Advances in

Communications, Computing, Networks and Security

Volume 5

Editors
Paul S Dowland
Steven M Furnell

Advances in Communications, Computing, Networks and Security Volume 5

Proceedings of the MSc/MRes Programmes from the School of Computing, Communications and Electronics

2006 - 2007

Editors

Dr Paul S Dowland
Prof. Steven M Furnell

School of Computing, Communications & Electronics
University of Plymouth

ISBN: 978-1-84102-257-4

Preface

This book is the fifth in a series presenting research papers arising from MSc/MRes research projects undertaken by students of the School of Computing, Communications and Electronics at the University of Plymouth. These one year masters courses include a significant period of full-time project activity, and students are assessed on the basis of an MSc or MRes thesis, plus an accompanying research paper.

The publications in this volume are based upon research projects that were undertaken during the 2006/07 academic year. A total of 33 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. The expanded topic coverage compared to earlier volumes in this series reflects the broadening of our range of MSc programmes. Specifically contributing programmes are: Network Systems Engineering, Information Systems Security, Web Technologies & Security, Communications Engineering & Signal Processing, Computer Applications, Computing, Robotics and Interactive Intelligent Systems

The authorship of the papers is credited to the MSc/MRes student in each case (appearing as the first named author), with other authors being the academic supervisors that had significant input into the projects. Indeed, the projects were conducted in collaboration with supervisors from the internationally recognised research groups within the School, and the underlying research projects are typically related to wider research initiatives with which these groups are involved. Readers interested in further details of the related research areas are therefore encouraged to make contact with the academic supervisors, using the contact details provided elsewhere in this publication.

Each of the papers presented here is also supported by a full MSc or MRes thesis, which contains more comprehensive details of the work undertaken and the results obtained. Copies of these documents are also in the public domain, and can generally be obtained upon request via inter-library loan.

We believe that these papers have value to the academic community, and we therefore hope that their publication in this volume will be of interest to you.

Prof. Steven Furnell and Dr Paul Dowland

School of Computing, Communications and Electronics
University of Plymouth, May 2008

About the School of Computing, Communications and Electronics

The School of Computing, Communication and Electronics has interests spanning the interface between computing and art, through software, networks, and communications to electronic engineering. The School contains 61 academic staff and has over 1000 students enrolled on its portfolio of taught courses, over 100 of which are at MSc level. In addition there is a similar number of postgraduate research students enrolled on a variety of research programmes, most of which enjoy sponsorship from external sources.

The bulk of the staff in the School are housed in the Portland Square building, a purpose built state of the art building costing over £25million and situated near the centre of the historic city of Plymouth on the University campus. The laboratories are located in the newly refurbished Smeaton Building, and the Clean room for nanotechnology also recently refurbished courtesy of a Wolfson Foundation grant is situated in the nearby Brunel Building. All buildings are a short walk from each other, enabling a close collaboration within our research community.

This School sits alongside two other Schools in the Faculty of Technology, the School of Engineering (the merged School of Civil and Structural Engineering and Department of Mechanical and Marine Engineering), and the School of Mathematics and Statistics. There are research and teaching links across all three schools as well as with the rest of the University. The closest links are with the Faculty of Science, principally the Centre for Computational and Theoretical Neuroscience which started in Computing, and Psychology through Artificial Intelligence and Human Computer Interaction research.

Prof. Steven Furnell
Head of School

Contributing Research Groups

Centre for Interactive Intelligent Systems
Head: Professor E Miranda & Professor A Cangelosi
Email: eduardo.miranda@plymouth.ac.uk
Research interests:

1) Natural language interaction and adaptive systems
2) Natural object categorisation
3) Adaptive behaviour and cognition
4) Visualisation
5) Semantic web

http://www.tech.plymouth.ac.uk/Research/computer_science_and_informatics/

Centre for Robotics and Intelligent Systems
Head: Dr G Bugmann
Email: guido.bugmann@plymouth.ac.uk
Research interests:

1) Cognitive systems
2) Social interaction and concept formation through human-robot interaction
3) Artificial intelligence techniques and human-robot interfaces
4) Cooperative mobile robots
5) Visual perception of natural objects
6) Humanoid robots

http://www.tech.plymouth.ac.uk/socce/ris/

Fixed and Mobile Communications
Head: Professor M Tomlinson BSc, PhD, CEng, MIEE
E-mail: mtomlinson@plymouth.ac.uk
Research interests:

1) Satellite communications
2) Wireless communications
3) Broadcasting
4) Watermarking
5) Source coding and data compression

http://www.tech.plymouth.ac.uk/see/research/satcen/sat.htm
http://www.tech.plymouth.ac.uk/see/research/cdma/

Interdisciplinary Centre for Computer Music Research
Head: Professor E Miranda
Email: eduardo.miranda@plymouth.ac.uk
Research interests:

1) Computer-aided music composition
2) New digital musical instruments
3) Sound synthesis and processing
4) Music perception and the brain

http://cmr.soc.plymouth.ac.uk

Network Research Group
Head: Professor S M Furnell
E-mail info@cscan.org
Research interests:

1) Information systems security
2) Internet and Web technologies and applications
3) Mobile applications and services
4) Network management

http://www.cscan.org

Contents

SECTION 1 Network Systems Engineering

SECTION 2 Information Systems Security & Web Technologies and Security

SECTION 4 Computer Applications, Computing, Robotics & Interactive Intelligent Systems

Section 1

Network Systems Engineering

Mobile Devices Personal or Corporate providing a Mechanism for Security

D.Chaudhury and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

In last couple of years use of advanced mobile devices such as PDA and smartphone has become a regular practice in both office and home environment. This devices are capable of performing advanced operation such as storing information, downloading files, and transmitting and receiving information in both wired and wireless environments, they increases productivity of the organisation. On the other hand using these devices for the above application, without proper security measures provides potential risk to the user. There are current technologies such as on device authentication, encryption, antivirus software are available to provide security, but there no unified framework provided to describe which security mechanism is applicable to which users. In this project users have been divided into two basic groups, personal and corporate. The main aim is two develop a unified framework, which will provide security to all the personal and corporate users, using different technology and using the device for different application. In order to develop a security mechanism it is necessary to know what risk the devices provide and how they affect the user. It is also necessary to know the current technologies available, and the amount of protection they can give to the device, the in built protection mechanism of the device. In order to do this the current mobile technologies, protection mechanism, operating systems have been discussed. Some statistics have been also shown from the recent survey taken to show the amount of risk in practical. In the later part of this paper personal and corporate users have been divided into nine subgroups depending on their mobility (low ,medium, high) and type information they carry(less important, medium important, highly important). These users have been put into a security mechanism matrix/table. In this table each group of users have been assigned certain security controls which provides information security for the data stored in the device, data on process and data send to or from the device. A certain number of policies have also been also added to the mechanism, in order to unify different technologies and different users. The mechanism has been analysed and it's usefulness to minimise the threats and provide absolute security in both network level and to the device have been found out. Limitations of the mechanism have been found, the way to minimise them as much as possible have given.

Keywords

Mobile Devices, Personal, Corporate, Users, Security Mechanism, Security Policies

1 Introduction

According to the 2005 press release of GSM World, the number of mobile users were 2.2 billions and is expected to be 3 billions at the end of 2010. In order to attract more number of users mobile phone companies started producing mobile

phones with more advanced technologies such as smartphones or PDA in market. Mobile devices due to their small sizes, increasing functionality such as internet browsing, information storing and downloading have become a necessity in today's world for both personal and corporate users. The increasing complexities of mobile devices make them more vulnerable to security attacks such as virus threats, exposure of sensitive information stored. Due to their small sizes, they are also very vulnerable to theft or loss. This may lead to serious revenue loss to the organisation or the individual. Mobile users can be personal or corporate, they may use the mobile device with different features for different applications, they might use it for internet application, might carry sensitive data in it, might not, personal device might be used for corporate application. Each user has different requirement, mobile device with different security features, which makes the situation more complex. It is therefore needed to provide a unified frame work and certain policies which will protect all this users.

2 Background Information

In order to develop a security mechanism, it is necessary to know the recent threat scenario, the threats mobile devices are facing and how much and which way the latest technologies can protect the mobile devices. Some researches done in recent past give alarming results. According to a survey done in 2006 by the Economist Unit for Symantec, 7.29% major loss have been caused to the company due to loss or theft of a mobile device, For the same reason 21.05% to 26.05% medium to minor loss has been caused. The other reasons such as virus, exposure of information 3% - 5% major loss and. Minor losses caused varies between 13.36% to 21.46%. According to the same survey, only 30% of the senior management understands this risk and only 9% of them actually a new security policy for mobile devices. Another survey done by tech republic on CIO readers shows that 79% of them do not follow any security policy for mobile device and 27% says that security of their company was compromised due to a stole device. This survey also shows that only 14% of the companies provide encryption or access control on PDA and only 38% of them protects the employee owned PDA. Although these surveys are done within a small group are users, they give some idea about the global situation. According to the Security company by McAfee, "security threats to mobile devices are increasing and will reach critical proportions within 18 months" The company says "malware that targets devices such as smartphones, laptops and PDAs has increased 30 per cent since the beginning of 2006". After analysing the survey results we can conclude that the main threats is Lost or stolen devices, A survey from Pointsec supports it. 60% of the executives say that their business will be compromised if the device is lost or stolen. When it comes to home users most of them are not aware of security concerns. The main damage caused by lost device is, exposure of information which can cause serious revenue loss to the company or an individual, damage to the network by opening rouge access points, cost of replacement, cost to recover the lost data etc. the other concerns are mobile viruses, email viruses, other malwares like Trojans and spyware and spam messages. There are a number of security mechanisms available in the market to overcome these threats, antivirus software is available from several companies. (McAfee, Fsecure, Symantec etc) several

encryption technologies are available (disk encryption, file encryption, PKI) to protect unauthorised access to data. Password authentication and mobile devices with biometrics or smart card authentication mechanism is available is available to protect unauthorized access to the device. Mobile Operating systems also provide security features and some of them are open to additional security features, such as Symbian provides user authentication and an access control list, with the hep of this data can be synchronized with a certain server and can be protected by use from other servers. It also provides in built antivirus features. New version of Windows mobile provide memory card encryption, on device authentication etc., this operating systems are quite useful for storing sensitive information, but many times additional control is needed. Other operating several research institutes such as Forrester research Inc., Tech Republic, Searchsecurity.com has come up with guidelines for business users. Information security standards like ISO 17799 define a list of security controls for mobile devices. But there is no suitable security policy available defining and explaining, which group of business user needs which set of security controls and why? Suitable guidelines for mobile home users are very hard to find. In the next section of the paper a mechanism have been developed which covers the security need for both home and business users.

3 Security Mechanism

The fundamental aim of any security mechanism is to achieve absolute confidentiality, integrity and availability (CIA) with the help of authentication, authorization and accountability (AAA). This mechanism helps two entities, Mobile devices, and personal and corporate mobile users. In the first step, personal and corporate users have been classified into 9 subgroups depending on two parameters,

3.1 Mobility

It has been considered because many times chance of the mobile device being lost or stolen increases due to its mobility. The user groups depending on mobility are:

Low mobility: Personal or Corporate users who are confined within a building or campus most of the times. And do not carry mobile devices during work. E.g. Retail store employees, factory workers, Logistics employees, Administrative employees.

Medium mobility: Users who is based in the office and travels outside office less than 50% times. Primary remote access is from home. E.g. Students, Departmental managers, inside sales, System engineers.

High Mobility: Users who travel during work most of the time. More than 50%. E.g. Executives, consultants, Field sales, field Engineers.

3.2 Information content

It has been considered because protecting the mobile device means other way protecting the information in three stages, Data sent to or from the mobile device, data being processed on the mobile device, data stored on the mobile device.

Low Value: loss of information will have no material impact on the company profit or loss, will have minimal impact on user. Have a suitable back up for data or synchronization with the server. E.g. Field inventory data from retail outlets, service requests, Regular reports, Personal information which is not sensitive.

Medium value: Information which may lead the company to some loss, or an individual to harassments but not asset loss. Data back up is available but temporary loss can cause some block in the workflow. Information falling into competitors hand would be undesirable but not disastrous. E.g. Email, personal address or phone list, internal phone list of company, Market positioning, product or service road Map, customer lists, local or regional sales data.

High Value: Information falling into competitors hand may lead the company to significant loss or legal proceeding. Falling the data into competitors hand may violate the financial agreements. In case of a personal user it may lead him or her to money loss or loss of job. Temporary loss of data can be devastating to the company. E.g. Customer information with their account number and bank details, credit card number of an individual, emails with sensitive information, financial or revenue reports.

The nine user groups developed are: Low mobility /low information value:----*level 1*; medium mobility /low information value:-*level 2* ; high mobility /low information value:---*level 3*; Low mobility /medium information value:--*level 4*; medium mobility /medium information value:--*level 5*; high mobility /medium information value:---*level 6*; Low mobility /high information value:---*level 7*; medium mobility /high information value:--*level 8*; high mobility /high information value:--*level 9*.

The security mechanism will provide protection in three levels, Centrally protecting the network; Protecting the data travelling across the network, ;Protecting the data stored in the device. A Security control have been developed Matrix have been developed. Some security controls have been kept optional at each level; they can be changed or kept depending on the need of the organisation. In addition to the table, certain policies have also been included, in order to bring different technologies under a common mechanism.

Information			
	High	**Medium**	**Low**
Mobility High Medium Low	**Level 9** VPN, Antivirus, Password authentication, Fail Safe actions, Data back up and recovery, PKI or biometrics	**Level 6** VPN, Antivirus, Password authentication, Fail Safe actions, Data back up and recovery, encryption	**Level 3** VPN, Asset discovery, Password authentication, Antivirus, Fail safe Actions (remote device kill)
	Level 8 VPN, Antivirus, Password authentication, Fail Safe actions, Data back up and recovery, PKI or biometrics	**Level 5** VPN, Encryption, asset discovery, Password authentication, Fail Safe actions, Data back up and recovery, antivirus	**Level 2** Asset discovery, Password authentication, antivirus (optional), VPN (optional)
	Level 7 Antivirus, Password authentication, Smart card authentication Fail Safe actions, Data back up and recovery, encryption	**Level 4** Asset Discovery, Encryption, Password authentication	**Level 1** Asset discovery, Antivirus (optional), Password Authentication (optional)

Table 1: The security Matrix

Corporate Management: Management role; 1. Risk assessment 2. Forming a governing body who will address all the security issues and form a security policy. 3. Review of security policy at regular interval 4. Users should be educated about the risk. 5. Inventory of the personal mobile devices associated with network. 6. Reporting mechanism for lost devices should be included. 7. Easy to use security mechanism should be employed. 8. Disciplinary action should be taken for disobeying the rules. Data Protection mechanism: 1. Latest software patches for the operating system should be used. 2. Mobile devices with better operating system should be used for higher level users. 3. Unnecessary information stored on the device should be deleted. 4. Security mechanisms not required for a particular user should be turned off. 5. Devices which cannot be cannot be managed by company security policy should be restricted. 6. Specific way of synchronisation with desktop computers should be defined. 7. Corporate user not use third party ISP on his device without encryption. 8. Corporate user should not use his personal device to store corporate information without encryption. .	Personal users: 1. use a strong password (a password with special characters or alphanumeric password). 2. Install antivirus software if further protection is needed. 3. Use the device carefully and responsibly to avoid loss or theft. Beware of spam messages. 4. The security applications which are not in use should be turned off. 5. Avoid using mobile device for accessing sensitive information. 6. Connect VPN before using sending data over secured network. 7. Use the device carefully and responsibly to avoid loss or theft. 8. Be careful If a personal device is lost or stolen report the theft to police, if sensitive information is stored (such as banking PIN number, email password, account information or any sensitive information), also report the appropriate authority so that the data can be restored and any malicious use can be protected. 9. Please use encryption mechanism for sensitive data. 10. Avoid provide Credit card information while shopping online. 11. Use reliable sources for downloading or installing programs on mobile devices. 12. If Bluetooth is used, do not set it “discoverable” mode. 13. Should read and know the security and protection features on the device. 14. Barring and restriction services provided by the operators can also be used.

Table 2: Guidelines for personal and corporate

4 Analysis and Discussion

The mechanism has been designed to protect the device and protect the users by assigning several security controls to each user group, it also protect the network with the use of VPN and asset discovery mechanism. The data travelling across the

network is protected with the use of VPN and encryption. As information is more important within the two parameters, levels have been increased with the increasing importance of information. The levels 1, 2 and 3 which contains less important information has been given less number of security controls and some of them are optional. In level one mobility is low so it will be within the network most of the times, and their damage can cause serious damage to network due to this devices in this level do not need VPN. Asset discovery mechanism will be enough to protect attack on them. Encryption and antivirus can be added depending on the users wish, because virus might damage the battery also. Certain controls like fail safe actions and data back up are necessary in highly mobile environments to protect the network. That's why they have been given even if the information content is less important. The levels 4, 5 and 6 needs better security mechanism, because they carry more important information, they have been encryption, antivirus, data back up mechanism as has been provided so that even if the device is lost, malicious attackers will not be able to attack it. Level 7 8 and 9 contain users carrying highly important information, they have been provided best and advanced security mechanisms such as biometrics, PKI and smart card authentication with all the other control used in previous levels. This mechanism provides protection to personal and corporate with the help of assigning security mechanism to different user levels. Users at each level can be personal and corporate. Certain policy for the corporate user who uses their personal device to store corporate data has been described. A separate guideline has also been given for ease of use of home user. It also minimises all the security threats related to mobile devices, the threats due to lost or stolen devices can be minimised by, data recovery, encryption, authentication, fail safe actions (remote device kill) . Threat due to virus, malware and spam can be reduce with the help of antivirus software. The threats loss or exposure of information is minimised by authentication, encryption, VPN, recovery. In order to provide further development at network level a cluster based security approach can be followed, where network will be divided into three clusters, and the cluster which contains most important information will be most well protected. Advanced encryption mechanism such as PKI will be sued for the devices which will have access to that part of network and those devices will have better security features. In order to decrease the burden of enforcing security policy manually, a digital policy certificate can be given to the handheld devices.

5 Conclusion

The mechanism developed above is flexible; controls can be added or removed from each level depending on the need of the user. If any new control mechanism is implemented in future it can fit into a level according to the user need. It provides security at all the levels. The policies can also be added or from the given list of the policies users can choose the policies required for them. The main limitation of this mechanism is it has not been implemented practically; there are lot of difference when a mechanism is proposed or it is practically implemented. It is also difficult to decide for the users which level of the matrix they fit into. It is difficult to communicate the security guidelines to the personal users. A suggested solution of this problem can be, two questionnaires can be prepared separately for personal and corporate users, in which how much they move, what kind of information they carry

can be found out. Depending on their answers their level can be decided and security controls can be assigned to them. In order to alert personal users regarding security threats, mobile phone companies can provide security guidelines with the new device packages.

6 References

Ahonen J, PDA OS Security: Application Execution , http://www.tml.tkk.fi/Studies/T-110.501/2001/papers/jukka.ahonen.pdf (Accessed April 26 2007)

Bechler M,, H.-J. Hof, D. Kraft, Pählke F, Wolf L (2004) A Cluster-Based Security Architecture for Ad Hoc Networks http://www.ieee-infocom.org/2004/papers/50 1.PDF (Accessed April 26 2007)

Brenner B, 4 April 2006 Survey exposes lax mobile securityhttp://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1178468,00.html(Accessed 26 April 2007)

Brownlee T, Daley E, Christine E, august 14 2006 Create A Companywide Mobile Policy, available [Online] http://www.forrester.com/Research/Document/ Excerpt/0,7211,40085,00.html (Accessed 26 April 2007)

Carter, B. and Shumway, R. (2002) Wireless Security End to End, Wiley publishing, Inc., Indiana.Getsafe Online, http://www.getsafeonline.org/ [Accessed 26 April 2007)

GSM Association Press Release 2005, Worldwide cellular connections exceeds 2 billion http://www.gsmworld.com/news/press_2005/press05_21.shtml(Accessed 26 April 2007)

Information Technology-Security Techniques-code of practise for information security management, licensed copy, University of Plymouth, 15/2/2006 http://www.bsi-global.com (Accesed 26 April 2007) .

Lawson L, Survey respondents say companies are lax on mobile security, http://articles.techrepublic.com.com/5100-10878_11-1029682.html(Accessed 26 April 2007)

Meyer J. S. Desktop Security Policy Enforcement - How to secure your corporate mobile devices www.infosecwriters.com/text_resources/pdf/Desktop_Security_JMeyer.pdf(Accessed 26 April 2007)

Phifer L (25 April,2006), Policies for reducing mobile risk, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1184648,00.html (Accessed 26 April 2007)

Symbian OS, http://www.symbian.com/symbianos/index.html (Accessed April 26 2007)

Tech Republic , “Identify and reduce mobile device security risks”, July 19, 2004 http://techrepublic.com.com/5100-10878_11-5274902.html#(Accessed 26 April 2007)

Routing Over a Real Mobile Ad-Hoc Network – a Performance Evaluation

O.E.Dallokken and Z.Li

University of Plymouth, Plymouth, UK

Abstract

An ad-hoc network consists of mobile wireless nodes without any infrastructure. All data inside the network are transmitted over wireless channels from the source to the destination. As there is no infrastructure such as access points or routers, the mobile wireless nodes in the network have to act as routers. As the nodes are interconnected over the wireless channel, the nodes route the traffic using multiple hops. The nodes can move freely, and cause an arbitrary network topology. Studies of mobile ad-hoc networks are mostly restricted to simulation and theory, and few have been carried out in a real mobile ad-hoc network. This paper studies an experimental setup of a real mobile ad-hoc test bed using the ad-hoc on demand distance vector (AODV) routing protocol. The experimental study investigates the impact of having multiple hops, varying distance between the nodes and the mobility of nodes on the performance of the network throughput. In addition this paper investigates the complex interactions between TCP and UDP when they share the same hops in the network.

1 Introduction

Wireless networking has gained large popularity during the recent years due to its flexibility and the almost unlimited areas of use. With the use of wireless networks, computing can be accomplished almost anywhere and anytime. There has been a shift in the use of wireless networking which tends to shift over to a more mobile use. In this case, it has been necessary to have networks that are randomly organised and with nodes that can move freely, such as in a mobile ad-hoc network. A mobile ad-hoc network is a self organizing multi-hop network of wireless links independent of any infrastructure, and which communicates using wireless technology (Alonso *et al*, 2003). Mobile ad-hoc networks use each node on the network as a mobile router, which gives the network an arbitrary topology. The nodes can move freely and randomly which causes the topology to change rapidly and unpredictably. The minimal configuration and flexibility makes the ad-hoc network suitable for instant networking needs i.e. emergency situations such as emergency medical situations, natural disasters and other situations with crises management. Communication in mobile ad-hoc networks rely on distributed routing protocols such as the AODV, which can manage frequent changes in the topology caused by the mobility of the nodes (Royer, 1999).

The performance of a mobile ad-hoc network relies on the way the packets are routed due to the arbitrary topology and the mobility of the nodes. In an ad-hoc network the nodes share the same wireless channel which creates theoretical limits of the

performance in terms of throughput. The distance between the nodes and obstacles such as walls, body shadowing and body absorption, which make the signal quality poorer, are other factors that will have an influence on the performance.

Most of the studies in the area of mobile ad-hoc networking have been carried out with simulation and theories (Barron *et al*., 2005). It has been stated that the simulated experiments differ to the real tests, due to the complexity of simulating the physical and the link layers of the OSI model (Petrova *et al*, 2003). There are also problems with the real Ad-Hoc test beds. As the characteristic of an Ad-Hoc network is the use of multiple hops, all the wireless nodes to be used in the experiments cannot be in wireless range of each other. This means that large geographical areas have to be used. A large geographical area is exposed to changes, such as the wireless signal quality may not be identical in all the experiments. This makes it hard to redo experiments, and to ensure correct data.

This paper will investigate the performance of a real mobile ad-hoc network using the AODV routing protocol. The intention is to identify the effect of TCP and UDP throughput when adding the impairment factors, mentioned above, to the network. In addition, due to their complex interactions, the TCP performance will be tested to see the effect when sharing hops with an interfering UDP data stream. The results prove that the number of hops has a significant impact on the performed throughput. Furthermore the distance between the nodes and the mobility of nodes have been proved to have a surprisingly high effect on the achieved throughput. The interactions between TCP and UDP show that TCP greatly suffers in terms of throughput when sharing a wireless channel with an interfering UDP stream.

The paper is structured as follows. In section two, the related background information will be presented with emphasis the related work in the field. Further in section three the methodology will be introduced. This section contains experimental setup, and how the data was obtained in the experiments. The results of the experiments are provided in section four. Section five describes and discusses the findings. Finally there will be a conclusion in section six.

2 Background

Related work for the experiments consists of studies of performance evaluation done on mostly real mobile ad-hoc network test beds. However, as most of the work has been done with simulation there will be necessary to bring up some theories witch consists of imitations of the real ad-hoc networks.

Research has been done to test the throughput efficiency in multi-hop 802.11 networks. The main contribution of this paper is to report findings in a real test bed instead of simulation. The researchers have compared findings from simulation with real testing, to see if there is any difference to the simulated experiments. The results prove that there are differences with these two test methods, mostly due to a lack of good physical layer and link layer measurements done in simulations. In this paper, experiments have been done to determine the limitations of a mobile ad hoc network.

The main parameter for measure this is throughput. The research has reviled that the number of hops in mobile ad hoc networks are highly restricted due to the sharing of the wireless channel. It has also been proved that the number of hops has a great influence on the archived throughput (Petrova *et al*., 2003).

The mobility impact on nodes has been conducted by simulation (Bettstetter, 2002). It has been found that the mobility of nodes have a significant impact on the performance of the network due to the routing protocols ability to adapt to those changes.

The link quality has been found to have a considerable effect on the performance of the network (Cahill and Gaertner, 2004) .The effects of body shadowing and body absorption are rather high and causes the link quality to decrease significant. These problems cause packet loss and affect the throughput and performance of the network in general. Research has been done to analyse the link variability for an indoor stationary 802.11 networks external interference. The aim has been to characterise the relationship between packet loss versus signal to noise ratio and the link distance. The experiments they have done are measuring the ratio of packet loss when adding both interference and various distances to the receiver. It has been found that the interference of the signal has a more important impact on the performance compared to the link distance. However, Klein-Berndt *et al.* (2006) state that interference occurs more likely with long link distances.

Experiments in a real AODV ad-hoc test bed have been done to measure the impact on the throughput of the interactions between TCP and UDP, when sharing hops. TCP is known to have problems in wireless networks because the protocol erroneously understands packet loss as congestion (Holland and Vaida, 2002). Another problem for TCP that occurs in MANETs is when routes are lost, the TCP packets will get lost. To make this even more problematic, UDP is excessive in terms of throughput when it shares the same link as TCP traffic. TCP will back off for the UDP traffic adjusts its bit rate to the UDP traffic (Gunningberg *et.al*, 2004)

3 The Real Mobile Ad-Hoc Test Bed

To test the performance of a real mobile ad-hoc network, a test bed has been developed. The experimental setup consists of two desktop computers and two laptops. The hardware is as follows:

Computers	Wireless Cards
Asus A8F	Intel Pro 3945ABG
Toshiba Satellite Pro	Intel PRO/Wireless 2100 B
Dell C600 P3	Asus WL-167G USB2 Dongle
RM 1.7 GHz 512 RAM Desktop	Dynamode Wireless PCI 802.11b
RM 1.7 GHz 512 RAM Desktop	Asus WL-138g V2 54G Wireless PCI Adaptor

Table 1: Hardware used for the experiments

All the computers are using running Windows XP and are set to use 802.11b in ad-hoc mode. The desktops have been deployed as transmitters and receivers of traffic and the laptops are the mobile nodes and act as intermediate nodes. The tests have been conducted to measure the performance in different scenarios to reflect a real life use of an ad-hoc network. The scenarios are made to test the maximum throughput for TCP and UDP with different numbers of hops. Furthermore, tests of the impact of having varying distances between the nodes are done for one and two hops TCP. As the impact of having different link distances is determined in these experiments, different test scenarios for three hops TCP have been made. The impact of having obstacles to decrease the signal quality is done by using a wall in between the wireless link for a two hops TCP transmission. In addition to this, the effect of body shadowing and body absorption is tested in this experiment. Finally, tests have been conducted to determine the mobility effect on the performance and the interactions between TCP and UDP when sharing hops. The interactions have been done using a three hop UDP with one hop interfering TCP data stream to the same receiver as the UDP traffic.

All the tests involve transmissions of generated data. The data is generated by the Iperf (Tirumala *et al*., 2006) traffic generator. TCP throughput measurements have been done with an 8 Kb window size. UDP traffic has been generated at different transmission rates with frame size of 1512 bytes. To make it possible to do tests in a small area, a Factotum (aodv.org, 2006) MAC filter has been used. With the use of this tool the traffic from unwanted nodes is eliminated. This makes it possible to have all the computers within wireless range of each other and still make the routing protocol use multiple hops to reach other nodes. The implementation of the AODV protocol being used is WinAODV 0.15, provided by Intel (Intel Corporation, 2006).

4 Results

4.1 Maximum Throughput

	1 hop	2 hops	3hops
TCP	5.02 Mb/s	1.79 Mb/s	1.05 Mb/s
UDP	5.21 Mb/s	2.51 Mb/s	1.31 Mb/s

Table 2: Maximum throughput

The maximum throughput has been determined with having the nodes at a close distance. It has been found that the number of hops has a significant impact on the throughput (table 2). As expected the UDP achieves higher throughput compared to TCP.

4.2 Impact of having different distances between the nodes in TCP

Figure 1 shows the maximum throughput for one and two hops TCP traffic compared to varying distance between the nodes. The impact of increasing the distance between the nodes was surprisingly high and caused a drop of almost 1 Mb/s for one hop TCP and 0.87 Mb/s for two hops. They both show the same trend which is not

surprising. But in TCP with two hops proves that having more hops, decreases the impact of link distance, even if the link distance is the same.

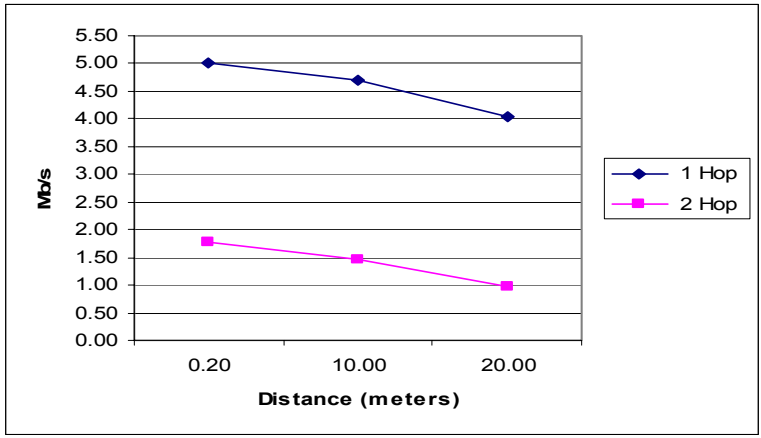


Figure 1: Impact of having different distances between the nodes in TCP

4.3 Impact of decreased signal quality over 2 hops TCP.

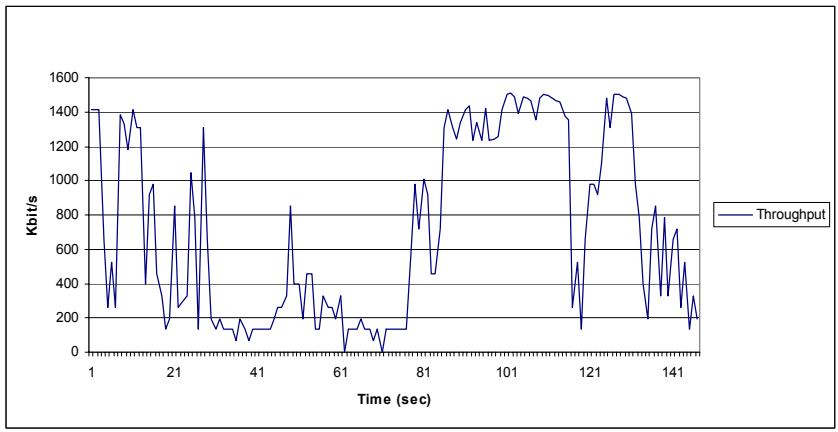


Figure 2: Impact of link hindrance over 2 hops TCP

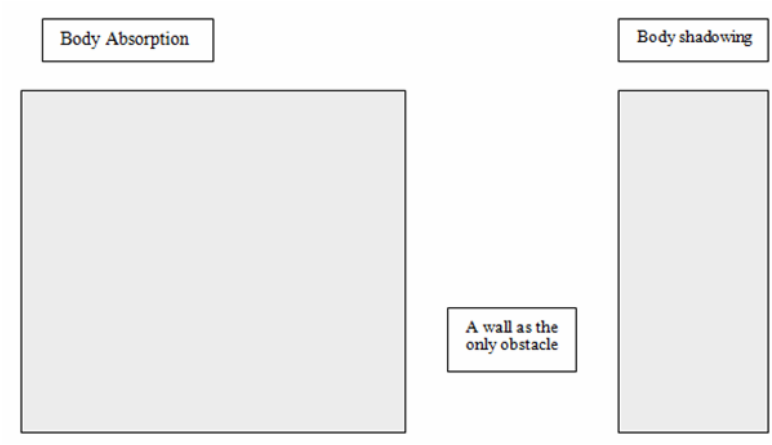


Figure 3: Impact of decreased signal quality over 2 hops TCP

Figure 2 shows that the body absorption and body shadowing has a large impact on the performance a make the throughput to drop significantly. The entire test has been done behind a wall, but having the wall as the only obstacle, the throughput is unexpectedly high compared to the body shadowing and body absorption of the signal. The body shadowing results varies a bit, but has nearly the same effect as the body absorption.

4.4 Mobility effect on TCP 3 hops

Without mobility	With mobility
1.01 Mb/s	0.82 Mb/s

Table 3: Results of mobility effect on TCP 3 hops

This test has been conducted to see the impact of having mobility of a mobile node, while transmitting TCP traffic. It was tested both with having the mobile node static, and with movement. The result with the node standing still gives a throughput of 1.01 Mb/s (table 3). When the node was in movement the achieved throughput dropped down to 0.82 Mb/s on average (table 3). This is a rather large fall of throughput and this proves that movement has a significant impact on the performance of a mobile ad-hoc network.

4.5 Interactions between UDP and TCP

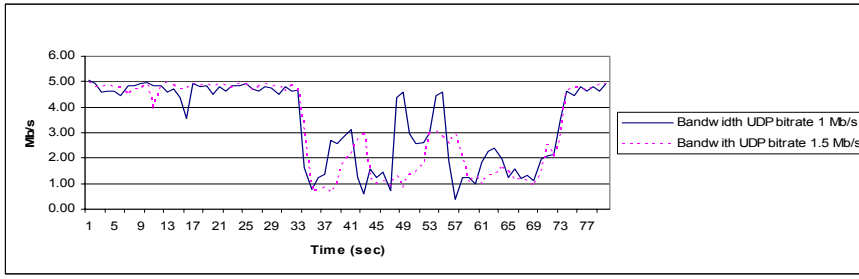


Figure 4: TCP with UDP interference

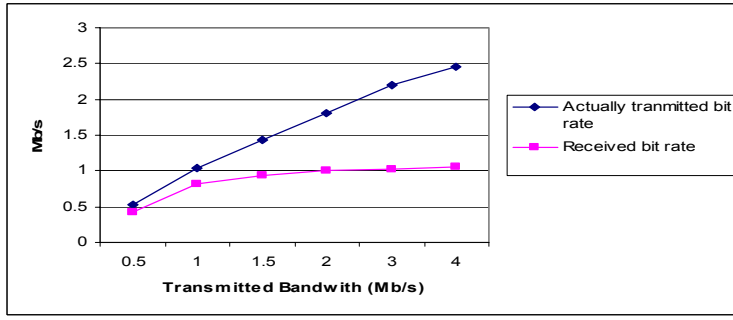


Figure 5: UDP with TCP interference

The TCP with UDP interference was done by having a UDP stream starting after 30 seconds, and lasted for 40 seconds. The TCP has one hop to the destination and the UDP has 3 hops. Figure 3 shows that TCP is highly affected by the interfering UDP stream and causes a large drop of throughput. The UDP with an interfering TCP has the same setup as the other test. The test proves that the UDP is not much affected of an interfering TCP stream in terms of maximum transmission data rate. But the rate of actually transmitted data rate, compared to the received rate differs even at rather low bit rates, which means that TCP causes packet loss on the UDP transmission.

5 Discussion

The impact of increasing the number of hops from a source to a destination is the factor that has the largest impact on the throughput in a multi hop ad-hoc network. This was not unexpected as the nodes in the network share the same wireless channel. For UDP it is found that the maximum throughput for a given number of hops can be determined by dividing the maximum throughput for one hop with the number of hops i.e.: ***maximum throughput 1 Hop / number of hops.*** This way of calculating the maximum throughput is not valid for TCP. The TCP has a maximum throughput of 5.01 Mb/s for one hop, and falls down to 1.79 for two hops. This is a

rather large decrease in performance which most likely is caused by the more complex interactions of the TCP. An unexpected observation was the difference from two to three hops using TCP compared to the drop from one to two. The fall of throughput was less significant then expected, and dropped from 1.79 to 1.05.

The distance between the nodes and the signal quality have a rather large impact on the TCP performance in a mobile ad-hoc network. The tests with one and two hops with distances from 20 cm to 20 meters prove that for one hop, the throughput decreases with 0.98 Mb/s and for two hops 0.87 Mb/s, which was a surprising observation. As these experiments were done over a maximum of 20 meters, it will be a significant factor in decreasing throughput when using longer distances, which also sets limits on the network size. The research identified that signal quality has a large impact on the performance of the network. This raises questions of how the mobility in ad-hoc networks can be obtained, as many of their use areas are for hand held and portable devices which will cause body absorption and body shadowing of the signal link. When having obstacles to reduce the signal strength, the test proves that the performance is highly affected by this. In fact the absorption and shadowing caused a drop in throughput from 1400 Kb/s to 200 Kb/s which can be said to be dramatic. The wall as an obstacle caused a lot less signal reduction, which is surprising.

TCP throughput is highly affected by a UDP data stream, competing for the same resources. The TCP was sent to a receiver over one hop, which has a maximum throughput of 5.02 Mb/s. The effect of the UDP data stream caused the TCP to drop down to a throughput of under 1 Mb/s which is a fifth of the maximum throughput. An additional observation here was that the bit rate of the UDP stream did not affect the TCP throughput much. It was about the same for 1 Mb/s and for 1.5Mb/s. This experiment proves that TCP suffers from a competing UDP data stream, as the TCP adjust its bit rate to the UDP bit rate. This is a well known issue, but in networks with limited resources, which a mobile ad-hoc network is, this phenomenon causes problems because network traffic contains both UDP and TCP traffic. The UDP test with an interfering TCP data stream was not much affected of the TCP stream. The throughput was slightly lower compared to experiments without any interfering TCP stream, but all in all this proves that the UDP will be “unfair” to the competing TCP transmission and captures the most of the bandwidth.

6 Conclusion

This research has proved that the major impairment factor is the number hops from a source to a receiver. An increased number of hops affect the performance dramatically. It has also been identified that this kind of networking is sensitive to mobility and signal problems. The interactions between TCP and UDP have been proved to have a significant impact on the use of the network. TCP suffers greatly when it has a competing UDP data stream, which largely decreases the TCP throughput. The UDP does not experience the same loss of throughput as the TCP when having a competing TCP data stream. As mobility and flexibility is the characteristics of an ad-hoc network these issues raise question of how to obtain

good performance. When adding all the impairment factors together there are limits of the use of mobile ad-hoc networks, and consideration should be taken before deployment. These considerations are dependent on the applications to be used in the network, due to different needs of network performance.

7 References

Alonso, G., Stuedi, P., Xue, J, (2003), *ASAP: An Adaptive QoS Protocol for Mobile Ad Hoc Networks,* Swiss Federal Institute of Technology, Zurich, Switzerland

Aodv.org, (2006), *AODV downloads* www.aodv.org/modules.php?op=modload&name=UpDownload&file=index&req=viewdownload&cid=2 (Accessed 3 January 2007)

Barron, P., Cahill ,V., Clarke ,S., Weber, S., (2005*), Experiences Deploying an Ad-Hoc Network in an Urban* Environment, Trinity College, Dublin, Ireland.

Bettstetter, C., Hoffmann, P., Wehren, (2004) *Performance Impact of Mobility in an Emulated IP-Based Multihop Radio Access Network*, DoCoMo Euro-Labs, Future Networking Labs, Munich, Germany

Cahill,V., Gaertner, G., (2004), *Understanding link quality in 802.11 Mobile Ad-hoc Networks*, IEEE Internet Computing vol.1089-7801/04/.

Gunningberg, P., Nordstrøm, E., Rohner, C., Tschudin, C., (2004) *Interactions between TCP, UDP and Routing Protocols in Wireless Multi-hop Ad Hoc Networks"* Uppsala University, Sweden and University of Basel, Switzerland

Holland, G., Vaida, N., (2002), *Analysis of TCP performance over mobile ad-hoc networks*, Wireless Networks (8): 275-288, 2002

Intel Corporation, (2006), *AODV for Windows*, moment.cs.ucsb.edu/AODV/aodv-windows.html (Accessed 3 January 2007)

Klein-Berndt, L., Miller, L. E., Moayeri, N., Souryal, M.,(2006), *Link Assessment in an Indoor 802.11 Network*, Wireless Communication Technologies Group, Gaithersburg, Maryland, US.

Petrova, M., Wu, L., Wellens, M, Mahonen, P., (2003) *Hop of No Return, Practical Limitations of Wireless Multi-Hop Networking*, Aachen University,

Royer, E.M., Toh, C.K.,1999, A Review of Current Routing Protocols for Wireless Ad Hoc Networks, IEEE Personal Communication Magazine, 1999: p 46-55

Tirumala, A., et.al., (2006) Iperf: The TCP/UDP Bandwidth Measurement Tool, dast.nlar.net/projects/iperf (Accessed 3 January 2007)

Mobile Devices- Personal or Corporate: Providing a Mechanism for Security

G.G.Eyetan and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

This research analyses the various security mechanism for both personal and corporate users and how we can secure these devices under both context. It classifies users based on the frequency of use for mobile devices, the breath of use and the multiplicity of tasks that the devices a put to in it's different contexts. User's profiles were analyzed and different statistics on the types of users and their characteristics was established. Based on previous research it is evident that a one security policy fits all will not suffice in this situation hence the classification of users into Novice, Intermediate, Advanced and expert users. Results obtained show that no single security mechanism is enough to address the issues of mobile device security; hence a multilayered approach was utilized leveraging the various security options for on-device security, security of communication channels and securing of the entire IT infrastructure. Controls in this model was derived from existing literature and the ISO/IEC standard 2005 which governs information security practice for organizations, but was applied to mobile devices context. Adverse issues that arise as a fall-out of security implementations and security of mobile devices as a whole was explained.

Keywords

Mobile Network, Security, Mobile Device

1 Introduction

The subject of mobile devices has generated a lot of interest because it is the area that has experienced the most phenomenal growth in Information and Communication Technology in recent years (Malykhina 2005). The support of internet services in a mobile environment is becoming an important topic (Pierre, 2001) this is encouraged by the possibilities of data communications over mobile phones. This is partly due to the fact that the capabilities of these devices have greatly increased in terms of their processing power, communication abilities, storage and the applications that interface with them are increasing such that most normal desktop functions can now be performed on a mobile device. Owing to its scalability and potential cost savings, mobile communication is being increasingly applied in the business and consumer communities to create innovative data and voice applications, which run over the internet infrastructure.(Olla and Atkinson 2004).

Ernest-Jones (2006) observed that part of the problem is that employees tend to see their mobile phones and PDAs as personal devices (even when they are paid for by their employers), while the lines between work and leisure use are more likely to be blurred. A scenario which creates security holes akin to that of ad-hoc networks where a device is simply brought into the organization, peered with another device usually a notebook or desktop, thereby rendering an organizations security policies and expensive firewalls totally ineffective. Most of their work included looking at the security threats and their counter measures for mobile portable computing devices, looking at the distinction between personal and business use for these devices. Furnell (2006) observed that unfortunately there is no simple answer to some of the problems, but it is at least relevant to recognize complications and constraints that are likely to be encountered, this paper will show that there no one security policy for personal and corporate use but a multi-layer, multi-user approach to information access and security, provides a more robust security architecture. Kim and Leem (2005) analyzed security threats of mobile devices, vulnerabilities of mobile platform and its application, attack on communication path and then suggested their countermeasures in terms of technical, manageable and physical aspects. Clarke and Furnell (2005) observed that "the popularity of mobile devices, increasing functionality, and access to personally and financially sensitive information, the requirement for additional and/or advanced authentication mechanisms is becoming more apparent", hence the use of simple password 4-8 digits is not adequate to secure devices like it used to, thereby creating room for more advanced methods like Biometrics.

Mobile systems fall into different categories depending on whose model you are looking at. Chou has categorized mobile systems into two categories: - vertical and horizontal applications (Chou and Yen, 2000). Vertical applications refer to the use of mobile technology in specific industries and application domains, some examples are packaging, monitoring, Public safety and Remote equipment monitoring which have application installed on this devices to give employees added functionality in performing their day to day activities . Horizontal applications refer to the mass market and domain-independent use of mobile technologies; these can be grouped into Personal Information Messaging (PIM) memory aids, document management, calenders, address books, messaging and electronic mail, and information services which tilt more to the personal user irrespective of where they are located and what their functions are. This is an approach taken by (King and Hart, 2002). Varshany provides a more pragmatic approach to mobile classification using the three groups (Varshany, 2001); business driven applications, consumer driven applications and state driven applications. Varshanys groupings offer more flexibility but could be considered to be slightly restrictive when considering the functionality of products registered. It was apparent from the examination of the registered applications that the categories proposed by Chou and Yen were no longer adequate as mobile applications have proliferated and fit into much broader groups.

2 Controls

Jendricke and Markotten (2006) observed that our users are the "weakest link" that our network has; hence to properly provide a mechanism for security we must first consider our users in our quest for a proper solution. So what was done was to divide our users into functional groups explained in the next section which are along the lines of the nature of information they processed on their device. This we noticed had a direct correlation to the type of devices they had and the applications running on them. We thereby created eight user profiles that cut across both personal and corporate use.

The researcher then took a number of controls from the BS ISO/IEC 17799:2005 which is the "Information Technology- Security techniques- Code of practice for information security management", which had a direct or indirect correlation with mobile devices and used these controls to create draft security policies for the different level of users that had already been created in the profiles above, assigning attributes, usage, access, to informational assets through mobile devices. This ensured a multi-layered approach to securing of the devices based on their classification. Hence the policy is not just about on-device security, or securing of communication channels or restricting access to corporate data or encryption or biometrics alone but combines all of the above valid security mechanism to provide one that looks at the user, determines what his requirements are and provides a security policy to match the criteria provided. The broad security clauses from BS ISO/IEC 17799:2005 include:-

- Information Security Policy
- Organization of Information Security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and Operations Management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Out of the 133 controls found in the BS ISO/IEC 17799:2005 document, 50 were used to provide security frameworks for all the users in our profiles. Some controls where already implied just by the user being in a particular environment while others where directly applied. Eckert, C. (2005) said "Security issues arise in three main areas:

(1) Secure management of assets stored in the mobile device,
(2) Secure communication within trusted and non-trusted environments (including privacy issues),
(3) secure interaction with critical IT infrastructures.

3 Results

This paper will now look at the research carried out by Seeley and Targett (1999) in which one hundred and three senior executives (board level or just below) from twenty very large organizations were interviewed. The organizations were all either ranked within the top 150 UK organizations, according to the Financial Times Index, or of an equivalent size, for example a government agency or a multinational listed on an overseas stock market. The purpose of their study was to elicit the encounters and episodes that caused any change and to determine what form the change took with respect to their personal use of the computer: hence, to generate a model of the process executives go through in developing their PC expertise. Of course we can apply user attitudes from the PC/Notebook to mobile devices as user attitudes in change environments are parallel. So how do we determine the end-user expertise? It can imply a range of applications, frequency, depth of expertise, tasks for which the computer or in our case mobile device is used, etc. so how broad are the applications installed, how frequently is the device used, what is the depth of expertise of the user and what tasks can these devices be put into. Recently, Seeley and Targett (1999) showed that `use' comprises at least three dimensions: frequency, depth of expertise with a software package and the breadth of software with which the executive was competent. They found that executives could be split into one of the four following broad end-user types: Novice, Intermediate, Advanced and Expert. The profiles to be created with the security mechanisms will be structured along these concepts of Novice, Intermediate, Advanced and Expert and the informational asset would increase in sensitivity as we move up our profiles.

The results obtained enabled the creation of profiles. The user profiles created are:-

- Security level I (User-1) Novice.
- Security level II (User-2) Intermediate
- Security level III (User-3) Advanced
- Security level III (User-4) Expert
- Security level IV (Corporate-1) Novice.
- Security level V (Corporate-2) Intermediate
- Security level VI (Corporate-3 Mobility) Advanced.
- Security level VII (Corporate-4) Expert

These cuts across both personal and corporate users and take the devices and their functions into consideration. Hence a user in SLVI has more security needs due to the applications running on his mobile device, the environment in which the device operates than one in SL1. The classification of these users also falls in line with the nature of information assets they process on their devices. Hence a user limited by

functionality in terms of the classes is not expected to access or process highly sensitive information. The classes are also hierarchical with the privileges increasing as the classification progresses.

The security controls are:-

Security level I (User-1)- Simple 4-digit passwords

Security level II (User-2)- Stronger password which will be alphanumeric, external authentication, Bit wiping

Security level III (User-3) - Stronger password which will be alphanumeric, external authentication, Bit wiping, Operating Systems (OS) patching.

Security level III (User-3) - Stronger password which will be alphanumeric, external authentication, Bit wiping, Operating Systems (OS) patching, and multiple applications.

Security level IV (Corporate-1)- Stronger password which will be alphanumeric, external authentication, Bit wiping, Operating Systems (OS) patching , directory access, internal authentication

Security level V (Corporate-2)-Stronger password which will be alphanumeric, external authentication, Bit wiping, Operating Systems (OS) patching, directory access, internal authentication, encryption, smartcard reader.

Security level VI (Corporate-3 Mobility)- Stronger password which will be alphanumeric, external authentication, Bit wiping, Operating Systems (OS) patching , directory access, internal authentication, encryption, smartcard reader, VPN tunnel, and any combination of (IPSEC, SSL, SSH and TLS)

Security level VII (Corporate-4)- Stronger password which will be alphanumeric, external authentication, bit wiping, Operating Systems (OS) patching , directory access, internal authentication, encryption, Smartcard reader, VPN tunnel, and any combination of (IPSEC, SSL, SSH and TLS),Dual authentication, key exchange, Biometrics.

4 Discussion

It is clear that securing Mobile Devices both personal and corporate is first and foremost about the user. Users determine the function the device will perform and the type of informational asset stored on or passing through the device. User attitudes and practices are therefore very essential in providing a security mechanism for the device. There is no one solution fixes all and an effective mechanism would have to comprise a number of individual solutions to make a proper and balanced framework for the device. Controls should be adhered to and properly applied especially in the corporate organization where breach of information security has very far reaching

effect for the organization in terms of legal, technical and regulatory frameworks. Policies should also be reviewed regularly as technological advances can make one strong policy today absolutely useless tomorrow, therefore proper monitoring of trends is a necessity.

Some implications of the security solutions were not considered as part of the scope of the research. The first is cost. The cost implications were not considered as some security mechanism provided in 3.0 would drive the cost way beyond an economically viable level for deployment within an organization, for example Biometrics. The next is speed. Implementing Dual authentication, alphanumeric passwords, encryption, IP security and VPN connectivity all slow down the speed of the device and the time it takes to access the information the user wants to process. This is usually unacceptable for most users as the whole purpose of the device for them from a functional point of view is quick access to the information, and finally is the device itself; some of the processes adversely affect normal mobile device functions like battery life. When encryption algorithms are being run they take up extra processing power and hence reduce the time the device can function without being connected to the mains. A situation which the user will rather not be in. So implementation should be holistic so that performance issues are not created while attempting to solve security issues.

Users are the focus of the classification and it is their attitudes how the market sways. They can “make or break” any technology. The fact that they have accepted the use of mobile devices is good the research has shown that they also are not too disposed to security especially on their devices. Selling the above proposal to them will most likely not be too easy a task but making it available to them will enable them to know what options are available to them in the event of their device getting compromised. Also when the information asset on the device increases in value the user knows what to do and how his/her risk has increased and the measures to take in ameliorating such risks.

The research also enables the user to see the implications of bringing their devices into a corporate environment and the fact that their data and corporate data should be protected when such a situation arises. Usually a user will not want to be bogged down with too much technicalities and this should be considered but measures that affect their battery life, speed and utilization is of importance to them.

The organization is an entirely different matter as a lot more enforcement can be implemented in the corporation. The research provides a very strong framework for corporate organization to either implement their security policy or draw up one similar to the one proposed in this research. The implications in terms of cost will be the most driving concerns here and the budget will be the quite high for corporations. Hence the gradual increase in features of the security complexity as the information asset increases on the device is a proposition that any organization will buy into any day, hence if the user has limited access to information asset, then limited features in terms of mobile device security should be applied and if the user has unlimited access to information asset then more money has to be spent securing their devices.

The issue of users bringing their devices into the network is one that given most administrators reason for concern hence the framework provides the organization the framework to help in the deployment of this devices in their network successfully. Institutional policies and should be developed and improved from time to time and in line with trends and changes in the types of users, the type of devices and their capabilities because it is inevitable that these devices will continue to improve in terms of capabilities and power and the applications run on them will continue to grow, organizations should position themselves in ways to harness the increases in technology.

Service providers including wi-fi operators and cellular have a special stake because they deploy these devices, sell them, support them and develop applications to improve their functionality. From this research they can analyze and see the types of users and the functions these users put the devices to. From the research they also can see that the security profiles is based on frequency of use, breadth and tasks that the devices can be put to, hence it is to the providers interest to build more functionality into their devices because the more the devices can do the more users they will have and the likelihood of the users using their devices for diverse tasks. The aspect of the research that shows the current age groups can also help providers know how to channel their marketing to the specified targets. As it stands from the research the provider will realize that the highest user group average age is 32 years, hence applications for this age group should developed but more marketing should be focused on the <19yrs to increase the users in this group and this is already being done as most Smartphone marketers have recently been focusing on music on the phone to entice more teenagers to purchase their devices. Development of security for the device itself, the communication channels and the data that the devices store are areas for which providers need to improve the security available. They also need to liaise with the organizations in developing proper solutions for mobile devices both on the corporate infrastructure and on the device itself. Security applications are also scarce in the field hence the development of security applications for mobile devices is an area that the research has shown is lacking seriously. All in all the providers' users and organizations are intertwined and must work together albeit indirectly to ensure that these devices serve the intended purpose for which they are produced.

5 Conclusion

Mobile devices are increasing in capabilities, functionality and use, users are currently deploying more and more applications to enable them perform normal functions more easily. Deployment of these devices is also growing exponentially hence security of the devices is generally lagging behind their deployments. Mobile devices pose a significant threat to traditional network security and policies, by virtue of their size and capabilities and because they use the "untrusted" internet as their main source of connectivity to external sources for information. There is no single solution to the security of mobile devices hence a multi-layered approach that looks at securing the device, communication channel and IT infrastructure gives a better security mechanism than just one security measure. The classification of users

based on frequency, depth and breadth of expertise with the mobile device being used. Solution and service providers have to take this into consideration as they design devices and products for the devices while organizations have to ensure that their users are properly equipped to get the most out of their devices without compromising security.

6 References

BS ISO/IEC 17799:2005 “Code of practice for information security management”, *Information technology- Security techniques*: 1-115

Chou, D.C and Yen, D.C (2000), "Wireless communication: applications and managerial issues", *Industrial Management & Data Systems*, 100:436-43

Clarke, N and Furnell, S. (2005). "Authentication of users on mobile telephones- A survey of attitudes and practices", *Computers and Security* 24 (7): 519-527

Donovan, J. (2006) “Support PDAs, but with caution” *Information Week – Manhasset*, (1072): 65-68

Eckert, C. (2005) “Security Issues of Mobile Devices” *Lecture notes in computer science,* 3450: 163

Ernest-Jones, T. (2006) “Mobile Security Strategy- Pinning down a security policy for mobile data” *Network Security,* 2006(6): 8-12

Furnell, S. (2006) “Securing mobile devices: Technology and Attitude”. *Network Security*, 9-13

Jendricke, U and D.Gerd tom Markotten. (2000) “Usability meets security – The identity-manager as your personal Security assistant for the internet,” in *Proceedings of the 16th Annual Computer security Applications Conference.* : 344-353

Malykhina, E (2005). “New Hacker Targets: Cell phones and PDAs”, *Information Week*, 1060:32

Kim, S. H. and Leem C. S. (2005) “Security threats and their countermeasures of mobile portable computing devices in ubiquitous computing environments” *Lecture notes in computer science,* 3483: 79-85

King, M, and Hart, T. (2002), "Trends and developments in wireless data applications - focus report (TCMC-WW-FR-0116)” *Gartner Report*, available at: www.gartner.com

Olla, P and Atkinson C (2004) “Developing a wireless reference model”. *Industrial Management & Data Systems* 104 (3): 262-272

Pierre, S (2001), "Mobile computing and ubiquitous networking: concepts, technologies and challenges", *Telematics and Informatics*, 18:109-31

Seeley, M and Targett, D (1999) "Patterns of senior executives' personaluse of computers," *Information & Management* 35: 315-330

Varshany, U. (2001), International Conference on mobile Communications and Networking, Proceedings of 1st workshop on Mobile commerce, Rome Italy.

Public Opinion towards RFID Technology

F.Li and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

RFID (Radio Frequency IDentification) is an automatic identification technique. A fundamental RFID device, often know as an "RFID tag", which is a tiny inexpensive chip with built-in antenna, can be attached on an item. By using radio waves, the tag's presence and its data can be recognised by the RFID reader. RFID technology can be used in many applications to provide the fast and convenient services. As the tag broadcasts its radio signal to all the dimensions in various distances, this raises the security and privacy concerns such as sniffing and tracking when people carry RFID tagged items. This paper examines the public's security and privacy awareness towards RFID technology. A total of 365 participants completed the survey. From an analysis of the results in was found that: 55% of the participants thought that wireless technology is not secure to use although numbers of security mechanisms have already been employed and 75% of them were worried about the fact that their privacy will be compromised (such as being monitored when they use their wireless devices). What was also found is that 36% of the participants have heard RFID technology before, and compared this with past consumer survey from 2003, here with an increased 13% in result, this indicates that there is still a strong need to educate people about the RFID technology to help them familiarise with the technology; furthermore, 67% of the participants chose their personal privacy over the specialised services which would be provided by the RFID technology, this demonstrates that people were more concerned about their privacy over functionality.

Keywords

RFID, Security, Privacy, Wireless

1 Introduction

In recent years, the use of wireless technologies has been dramatically increased as they provide the ubiquitous access to the telecommunication and data networks in the daily life. Currently, there are over 2 billion mobile phone users in the world (Cellular Online, 2006) and there are more than 130,000 public Wi-Fi hotspots available in 130 countries (Jiwire, 2006). While with the increasing market demand, the security and privacy issues should also need to be concerned. In 2003, the US researchers have pointed out the security flaws on WLAN (Wireless Local Area Network) and also have demonstrated number of attacks to compromise the security such as: by using the unauthorised packet to block the legitimate users to access the WLAN (Jackson, 2003).

One member of the wireless technology family is becoming more popular than ever before. The RFID (Radio Frequency IDentification) technology is an automatic identification method that can be used in any identification systems; by using radio signals, the RFID reader detects the tag's presence and accesses the tag's data, therefore the tagged item can be located and identified. RFID technology can be used in many applications such as: identification, tracking, payment system, inventory control, access control, and supply chain management. The RFID development never stops. In the U.S. retail supply chain, the RFID implementation has been estimated at $91.5 million in 2003 and this amount is expected to grow to $1.3 billion by the end of 2008 (Boone, 2004). As RFID technology is a member of the wireless family, it inherits many common security threats such as eavesdropping. However, due to its unique character, it also faces other threats (i.e. Clone attack on the RFID based biometric passport (Young, 2006)).

Privacy threats will be concerned when people use the wireless technology, according to The Times article, "by 2016, Britain is becoming a "Big Brother" surveillance society with millions of people being tracked.", also "shopping habits, travel movements and car and train journeys are being monitored increasingly as part of the fabric daily life" (Ford, 2006). These can be achieved by tracking/monitoring people's wireless devices such as mobile phones or RFID tagged train tickets. This research is aimed to find out the public security and privacy awareness level regarding to general wireless technologies and public opinion on RFID technology. The survey was structured so that information could be collected on demographics, general security and privacy aspects on wireless technologies and in particular for RFID technology. This paper's format is to outline the general security and privacy aspect of RFID technology, followed with introducing the investigation method which was a survey and analysing its results. The paper finishes by discussing the survey outcomes and predicting future directions for RFID technology development.

2 Security and Privacy for RFID

RFID technology has been used for over the last 60 years. It was mainly deployed for the military in the Second World War: the IFF (Identification Friend or Foe) system was used to identify the aircraft (Landt, 2006). In 1960s, the technology was first utilised for the public in an anti-theft system by using 1-bit tags to detect the presence or the absence of tagged items in retail shops (Roberts, 2005). Since then, it has been dramatically developed and it has been used in many applications. In 2004, Wal-Mart began to employ RFID tags to track products in their supply chain (Roberti, 2004); recently, European countries started to deploy the new biometric passport which uses the RFID chip to store the holder's personal information such as finger prints (Hoepman *et al.*, 2006). These shows that the use of RFID technology is changed significantly from 1-bit security tags to RFID chips based passport.

Security and privacy was never a major issue for RFID technology before; however, with the increased applications, security and privacy issues have become more important. For the security, in 2005, the researchers from John Hopkins University and RSA security have performed a spoofing attack on an RFID system; by using the

cloned RFID tag, they successful unlocked the car with the electronic immobilisation system (Bono *et al.*, 2005). In March 2006, the researchers who are from Vrije University Amsterdam have showed the vulnerability of the RFID system under the virus attack (Rieback *et al.*, 2006). With respect to the privacy, malicious users could build a hotlist to determine exactly location of the tagged item among thousands of others; this is an extremely dangerous threat to the people's privacy when carrying tagged items (Ayre, 2004). Although people may not heard these threats before, with the dramatic development and increasing usage, RFID security and privacy aspects should be concerned by people in the near future.

3 Methodology

The method used in this research was an online survey: by analysing the survey result, to predict the public's security and privacy awareness level when people use the wireless technology and especially public's view on RFID technology. After the draft version, a number of people were invited to form a focus group giving feedbacks to improve the survey quality. Survey invitation was sent out by using emails which contained the survey link and the research background information. The data collection process started from 25/08/2006 and completed on 30/10/2006, and the participants remained anonymous.

The survey was aimed to discover the public's view on wireless security and privacy and their attitudes on RFID technology; it was designed in two main sections: backgrounds: what RFID technology is and what it can be used for, and questions section which contained three subsections: demographics which required the participants' gender, age, nationality, education level and employment, general security and privacy for wireless technology which accessed what level of security and privacy awareness participants have when they use the wireless technology, and final section to predict what their opinions are on the RFID technology.

4 Results

A total of 365 participants completed the survey. According to the result, the participants were with a mix of gender (56% male and 44% female) and 77% were in the age group of 18-30. Given the skew towards higher educated persons who have a bachelor or higher degree (96% of the participants), it is suggested the results presented in this paper might reflect a more positive perspective of wireless and RFID technology than might be expected from the general public.

4.1 Security and Privacy on wireless technology

Wireless technology has been around for years, many people may have already experienced it in one or other formats, such as mobile phone. From the finding, a significant number of participants (87%) were aware of Bluetooth and WLAN both of them have only existed for few years; 72% were aware of GPS (Global Position System), GPRS (General Packet Radio Service) and 3G; only 34% were aware of RFID technology which has been survived for more than 40 years in the commercial

world; From figure 1, it shows that: the WLAN is the most frequently used wireless technology as 57% of the participants use it on a weekly basis compared to others, and the RFID technology is the least used one . This indicates the reason why most participants were familiar with WLAN as people regularly use it; compare with it, RFID technology is much less known as it is not a widely used yet and there is not much information about it even when people do use it such as the car's electronic immobilisation system is the RFID technology based, but it is very rarely people are informed about it.

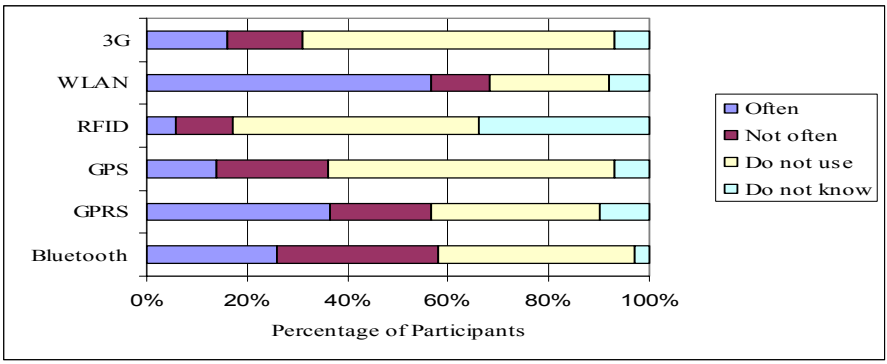


Figure 1: How often do participants use the wireless technology?

People can use many security mechanisms to protect various wireless devices. So what method(s) have been deployed by participants to protect their wireless devices? The results are shown in Table 1. On average, authentication is widely used as the ease of use and low requirement. 60% used firewalls and antivirus software to protect wireless laptops, but less usage of these methods on other devices. Due to those devices may not necessary need them at the moment and those devices have small amount of computer power to support those two mechanisms, but it is still possible for people to use these tow methods on those devices. Although biometrics method has been existed for many years, less than 5% used it as most of the devices do not support it; also, participants were aware switching off is an option, as some threats (i.e. the virus) can not harm devices when they are switched off.

	Mobile phone	PDA(personal digital assistant)	Wireless laptop
Physical secure(e.g. locks)	25%	7%	20%
Biometrics (e.g. finger print)	2%	2%	5%
Authentication(e.g. password/pin)	41%	16%	55%
Firewall	5%	7%	60%
Antivirus software	6%	7%	61%
Switch off when not using it	29%	10%	48%

Table 1: Security methods for various wireless devices

Although various methods have been used, there are still 55% of the participants thought it is not secure to use the wireless technology with two thirds of the population felt their security awareness level was medium and above. In addition, a significant number of participants (86%) felt that they could be benefited from learning more about security.

As the wireless technology uses radio waves by transferring data through the ether, it becomes to a potential privacy threat when people use it. 75% of the participants were worried that they may be tracked or monitored by other people when they use wireless technology. Furthermore, participants were asked "which of the following wireless technologies do you believe can be used to monitor\track you?" and the result shows in Figure 2: 70% chose WLAN; around 55% believed GPS, GPRS, Bluetooth and 3G; only 38% picked RFID technology. In fact, all these technologies can be tracked\monitored; this result indicates that people are very familiar with the WLAN as they use it fairly often and they do not know about RFID technology that well as they do not use it that much.

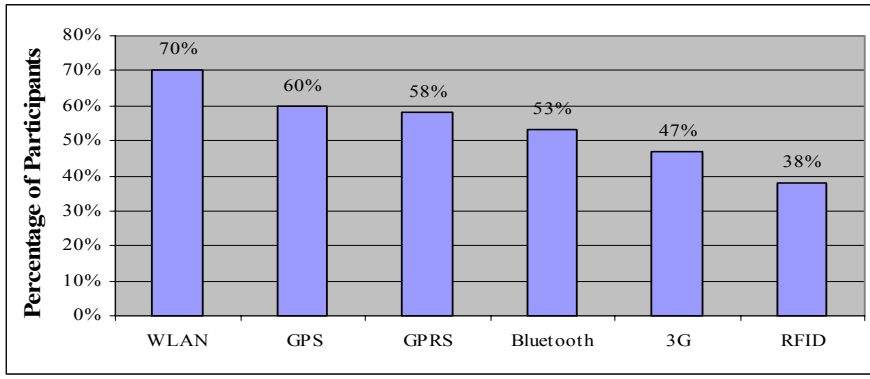


Figure 2: Wireless technologies they believe they can be tracked by.

In order to predict the public's privacy awareness level, a question was asked to scale their privacy awareness level when they use wireless technologies. From the Table 2, it shows that the skew towards to the very poor privacy awareness level (10%) from the very good privacy awareness level (4%), it may reflect that more participants do not know how to protect their personal information privacy, and even more they may not know whether their privacy is vulnerable or not when they use the wireless technology.

Privacy Awareness Level	Very poor	Poor	Medium	Good	Very good
Number of participants	10%	26%	41%	19%	4%

Table 2: Privacy awareness level when people use wireless technologies

4.2 RFID technology

RFID technology has been utilised by people for more than half century, much longer compared to other wireless technologies (e.g. WLAN). From the survey result, only 36% of the participants have heard about it before; this shows that actually participants' awareness of RFID technology is very low at this time, as it was mainly used for the military and then moved on for the business usage such as in the supply chain management. Further more, 37% of those who have heard about RFID technology have a job in I.T./Computing, 24% were full time students, and participants in education and engineering also took big portion of the total population; moreover, the result shows that individual's background does have an impact on their answers.

RFID technology has been deployed in many applications and it will be used in more areas. Figure 3 shows that applications which participants currently use and they would try with RFID technology in future. Only small portion of the participants use inventory control compares with majority of the population use the library system, passport, bus tickets and Visa debit card; on average, 38% of the population would use the RFID technology in aforementioned applications, this indicates that those participants would try new technology does not matter whether they use the current applications or not.

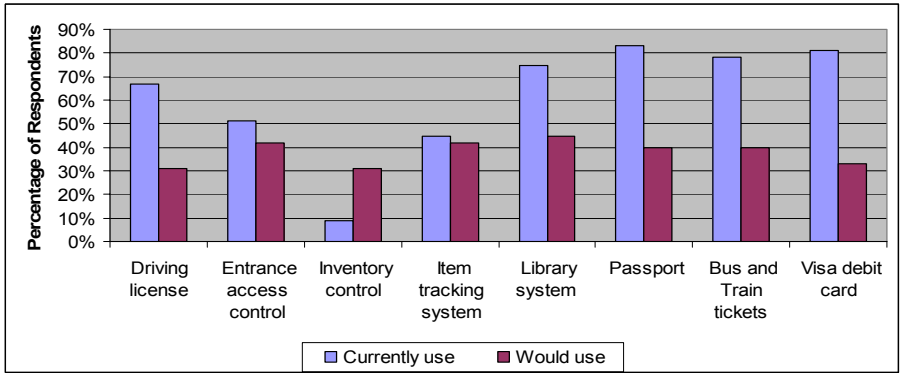


Figure 3: Applications people currently use, and they would try with RFID technology.

Various security and privacy threats are associated with RIFD technology such as sniffing, tracking, spoofing, replay attack, DoS (Denial of Service), man in middle attack and virus (Rieback *et al.* 2006). Participants were asked if they have heard those threats before, 68% said they have and the rest have not; for those who have heard the threats before, their answers were further analysed which is showed in Figure 5: among those who have heard the threats, 71% thought tracking may associate with RFID technology, around 30% thought the rest threats may relate with the technology and 8% thought none of the threats may have association with the RFID technology. As all these threats are related to the RFID technology, but

participants' responses are so different, it can be explained each participant has a different view about each threat for the RFID technology: participants understood more about tracking threat compare to others threats.

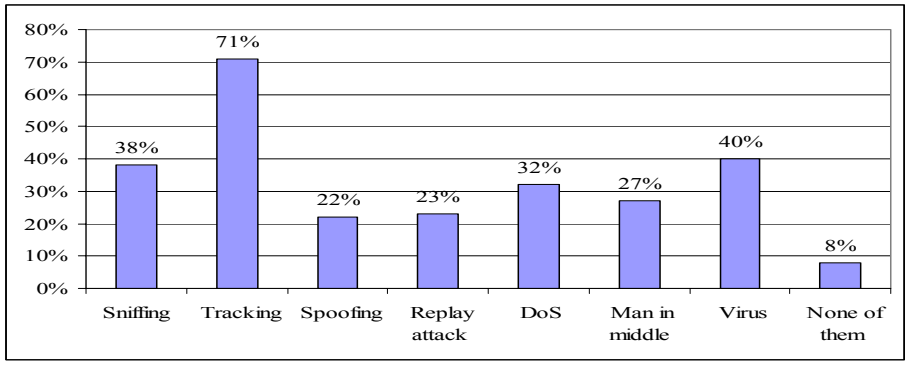


Figure 4: Attacks on RFID technology

RFID technology has some special futures such automatic warning which would be use in the daily life to provide the convenient, but at the same time, these futures may cause the personal privacy leakage. Participants were asked to give their opinions on these services and views about their information privacy when they use the services; for the services which would provided by RFID technology, 64% would like be informed by their washing machine if two different colour clothes cannot be washed together and 53% would like to be informed if the milk is low in their fridge. On the other hand, regarding to the privacy, 64% do mind that people know what they have in the fridge when others pass their home and 66% do mind taking off an item(s) such as jewelleries to protect their information against tracking. From these results, it shows that on average 59% liked the services and 65% wanted to keep their information privacy safe, this points out that there are some participants would like to have both at the same time; obviously, the participants can not have both at the same time at the moment; therefore a trade of question was asked to choose between personal specialised services (e.g. automate warning) and personal privacy information (e.g. current location). 67% of the responders chose their privacy and the rest prefer to the specialised services; this indicates that more people are concerned about their privacy than the services they would get.

5 Discussions

From the results, it shows that participants have a good level of understanding about wireless security. Participants use varies security mechanisms to protect their wireless devices to meet different security requirements: generally, authentication is used as it provides minimal protection; as the computer is vulnerable to the virus, therefore that is why 61% of the participants use antivirus software to provide with an extra level of security; in future, if the virus threats other devices, the antivirus software will be designed to fit them in order to protect the devices. It is very

interesting that although majority participants have a medium and above level of awareness on the wireless security, there are still 86% of participants thought they would gain more if they learn more about security, this indicates that how important people consider about the wireless security is.

Compared with the participants' security awareness, participants do have low privacy awareness level, as 77% of participants' privacy awareness level is the medium and below. 75% of participants were concerned that they would be tracked\monitored by their wireless devices; this indicates generally people are unfamiliar with the privacy impact when they use wireless technology, and they certainly do not know how to protect their privacy information. Therefore, relevant privacy protection methods should be introduced to erase people's fears when they use the wireless technology, this may take some time to develop as currently the systems' main concern is the security issue rather than people's privacy.

The result also shows that: only 36% of the participants have heard the RFID technology and the majority of them were IT/Computing professional and full time students; this compares with the 2003 US consumer survey (Capgemini, 2004) with an increased 13% in result. The result should be increased as most of the participants were higher educated persons whom received more knowledge compares to those general publics; this means that the public's view of the RFID technology has not changed much during the pass three years radically RFID development. Furthermore, for those who have heard the security and privacy threats before, 40% of them thought that virus associates with RFID technology; as the world's first virus infected RFID tag was created in earlier 2006 (Rieback *et al.*, 2006), this strongly indicates that those people presumed this only based on the virus is one of the common threats for IT systems, therefore it could be a threat for RFID technology as well.

From the results, it demonstrates that people are not familiar with the RFID technology although it has been around for very long time; there is certainly a need to educate those who have not got knowledge about it in order to help the RFID development; as from the survey result shows that 49% of those who have heard about the technology would use the RFID technology, in contrasts with 32% who have not heard about it before would use it. Once people start to use the RFID technology, then they can be informed with which security and privacy threats with the according protection methods. Also, from the survey results, 67% of the participant chose their personal information privacy over personal specialised services; this shows that although RFID technology would provide the convenient services, people still consider about their personal information as more important; this means in future, it will be desirable if the public's privacy is protected while they use the services.

6 Conclusions

Most of the participants do have a good level of security awareness on wireless technology, not only because what they have said, but also because people do use the

correct method to protect the right devices with the security needs; this still could be improved if they were informed more about security; On the other hand, participants' privacy awareness level is fairly low as people are not sure what the privacy threats are and how to protect themselves from these privacy threats; in order to improve this situation, people should be educated on what the privacy issues are and the industry should produce the according protection methods for the public to use. For the RFID technology, it shows that people's awareness level about it is pretty low as it was mainly used in the military and business, but not for the consumers, people should be informed about it before it is widely used by the consumers, as this can certainly boost the RFID development. Overall, as the increasing development of the wireless technologies especially for the growth of the RFID technology, both the security requirement and privacy impact should be considered by people and the sooner people receive the relevant information about them, the better for system security and the public's privacy.

7 References

Ayre, L.B (2004), "RFID and Libraries", http://galecia.com/included/docs/position_rfid_permission.pdf, (Accessed 02 October 2006)

Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A. and Szydlo, M. (2005), "Security Analysis of a Cryptographically-Enabled RFID Device", *In 14th USENIX Security Symposium*, pages 1–16, Maryland, USA, July-August 2005

Boone, C. (2004), "RFID: The Next Big Thing?", http://www.ftc.gov/bcp/workshops/rfid/boone.pdf, (Accessed 14 November 2006)

Capgemini (2004), "RFID and Consumers: Understanding Their Mindset", http://www.nrf.com/download/NewRFID_NRF.pdf, (Accessed 14 November 2006)

Cellular Online (2006), "Stats Snapshot", http://www.cellular.co.za/stats/stats-main.htm, (Accessed 09 November 2006)

Ford, R. (2006), "By 2016, they'll be able to watch you everywhere", http://www.timesonline.co.uk/article/0,,2-2433304_1,00.html, (Accessed 03 November 2006)

Hoepman, J.H., Hubbers, E., Jacobs, B., Oostdijk, M. and Schreur, R.W. (2006), "Crossing Borders: Security and Privacy Issues of the European e-Passport", *In Advances in Information and Computer Security*, vol 4266 of LNCS, pages 152-167, Springer Berlin / Heidelberg, 2006.

Jackson, W. (2003), "Wireless network attacks get a public airing", http://www.gcn.com/online/vol1_no1/23053-1.html, (Accessed 29 November 2006)

Jiwire (2006) Worldwide Wi-Fi Hotspots Hits the 100,000 Mark Online at: http://www.jiwire.com/press-100k-hotspots.htm date accessed: 14/11/2006

Landt, J. (2001), "Shrouds of Time The history of RFID" http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf, (Accessed: 02 October 2006)

Rieback, M.R., Crispo, B. and Tanenbaum, A.S. (2006), "Is Your Cat Infected with a Computer Virus?", *PerCom 06: 4th Annual IEEE International Conference on Pervasive Computing and Communications*, in Pisa, Italy, 13-17 March 2006

Roberti, M. (2004), "Wal-Mart Begins RFID Rollout", http://www.rfidjournal.com/article/articleview/926/1/1/, (Accessed 21 June 2006)

Roberts, C.M.(2005), "Radio frequency identification (RFID)", *Computer & Security*, Vol. 25, pp18-26

Young, T. (2006), "Biometric passports cracked", http://www.computing.co.uk/computing/news/2161836/kacers-crack-biometric, (Accessed 15 August 2006)

Web-Based Survey of Expert Marine Scientists

I.Tsitsikas and P.Culverhouse

University of Plymouth, Plymouth, UK
e-mail: pculverhouse@plymouth.ac.uk

Abstract

Plankton identification instruments are under development from various projects across the world. Most of them use image sets of labeled specimens in order to train their algorithms. A factor that affects the accuracy in their diagnoses is the lack of validated image sets. This paper introduces a hybrid version of a web-application created with the view to collect experts judgment's of plankton specimen's identification. It allows marine ecologists and contributors in general to offer their collections of specimen's images to an open study, enabling marine biologists and experts in taxonomy to offer their knowledge in identifying the specimens. The information which will be collected by this system will be of value to machine identification of plankton, training human taxonomists and gaining an understanding of the statistics of consensus on a large dataset.

Keywords

Plankton labeling, specimen validation, plankton taxonomy, expert consensus, expert consistency

1 Introduction

Scientists round the world are interested in categorization of plankton specimens and the discrimination of diversities plankton has. This process of categorization is carried out in two ways, by skilled taxonomists and with the aid of microscopes specimens are labelled manually (Culverhouse et. al, 2003); and automatically by machine. There is an active scientific community researching the topic of plankton identification by machines. Each automatic identification instrument may use a different technique in their implementation but typically they use techniques drawn from artificial intelligence. An example of this paradigm of is DiCANN (Dinoflagellate Categorisation by Artificial Neural Network; Culverhouse et. al, 2001).

What is common to many of these machines is their need for plankton image sets defined by accurate and non-disputable scientific names in order to train their machine learning algorithms, because incorrectly labelled specimen images can directly affect their diagnoses (Culverhouse, 2003). The collection of such image sets is not trivial, because although an identification of a specimen image by an expert is reasonably fast, their judgements may still be inaccurate especially in cases that an expert has to label a large sample of images. According to Culverhouse *et. al.* (2003)

the problem is caused by a series of cognitive effects such as 'Human short-term memory, fatigue and boredom, positivity bias and recency effects' that can dramatically reduce their labelling accuracies.

This study recognised these difficulties and set as an main aim to provide validated image sets to researchers developing systems for automatic labelling of marine plankton. In addition the aggregation of data might later reveal some aspects of how users label plankton images. The web-oriented database system, called Pleione, primarily serves marine scientists as an open-resource of machine-imaged plankton specimens. Secondly the image sets are offered to the oceanographic taxonomists and ecologists for labelling. And thirdly, whilst engaged in labelled these experts will be offered a subset of these images that have been flipped or rotated, as a means of studying expert consistency. The analysis of all the opinions for a given set of specimens will provide validated image sets and data on human expert consensus.

2 Background

Review of the literature selected showed that creation of web-based labelling system has to take into consideration the existing problems in the field of Taxonomy.

According to Paterson *et. al*. (2005) "Taxonomy is the branch of biology concerned with the classification of organisms into an ordered hierarchical system of groups (taxa) reflecting their natural relationships and similarities". The term taxa used in the previous definition is actually the plural form of taxon. A taxon is a group of organisms that have some key features in common or some genetic relatedness. Every taxon is assigned a rank in order to form a hierarchical order. Taxonomists are the creators of both taxa concepts and hierarchical classifications. In order for communication to be feasible among them, taxonomists apply Latin or Latinized Greek names to these taxa that conform to international rules of nomenclature (Sumich, 1999). These names referred are known as scientific names. Problems are immediately encountered because there are multiple scientific names that refer to the same taxon concept (Kennedy et al 2004). So taxonomists select one name to be the accepted/valid name and regard all others as synonyms (Sutherland, 1999). A second problem is homonyms that are scientific names written the same, but that refer to different taxon concepts (Sutherland, 1999). The third problem is that there are multiple classification hierarchies and revisions that occur frequently (Raguenaud *et al*. 2002). All these problems are common to any informational system that aims to store taxonomic data. There are already database models for example by Lindstrom (2006) that are designed to store this kind of information. An issue for systems implementers is not how these data will be stored, but how the problems of synonymy, homonymy and multiple classifications will be managed (Sutherland *et. al.,* 1999) (Kennedy *et al.* 2004).

For these reasons well funded taxonomic databases (like ITIS, NCBI, Species 2000 etc.) are seeking to aggregate all known scientific names and carefully manage the problems in taxonomy by examining and revising the aggregated names with the aid of their Taxonomic Work Groups (TWG). Typically they support a single

classification schema that accommodates all the segregated names (with exceptions Ubio, Prometheus). Also most of the taxonomic databases except from the web interfaces providing also and web services, (acting as the middle-ware) allowing with this way other web-systems to retrieve taxonomic information. The data exchange formats for these web-services are XML documents that are transmitted using HTTP or Soap protocols (Roderic, 2005; Kennedy et. al, 2004). But a problem still persists because even in these public databases there is not a single checklist that includes all the existing names and synonyms (Paterson, 2003). Also the concept of mixing names from multiple resources is jeopardizing the accuracy of the data since according to (Roderic, 2005) "there is no guarantee that taxonomic names stored in different databases will be mutually consistent". These approaches have also been characterized as 'naïve' from (Kennedy et. al, 2004). This sets a complex scene for the implementation of a web-based plankton labeling database.

3 Methodology

The Pleione web application is written in ASP .Net 2.0 (using C#). The Client side code is written in Javascript. And the RDBMS that is used is MS SQL server express edition. The methodology that is used to support marine ecologists to make available their collections of specimens to the community is the creation of a loosely coupled distributed system. It has been recognised that archiving images is a space demanding procedure and the aggregation of many image sets will require a huge amount of datastore that will be difficult to manage. Further more a problem is also generated in data acquisition and property rights because a contributor may claim misuse of his/her property. So the practice followed in this case is that the contributor setting up a web-server and putting his/her collections of images into an HTTP folder requires the same source folder is FTP enabled at the time of system upload. The contributor also specifies the HTTP_URL of the remote folder, the ftp address and the credentials of the same folder. By the aid of ftp protocol the list of image files are retrieved and by the aid of an iterative HTTP GET requests the validity of the distributed resource is checked. The system saves only the links of these images and the contributors undertake to maintain their web-servers. Contributors also may apply security restrictions allowing only Pleione system to communicate with their server since every file is passing through the application server without revealing the IP address of the contributor.

Both actual images (Data) and metadata are assigned equal importance. The metadata holds information that is closely associated with the capture of the image and provides answers to the questions of who, how, where and when where these images captured. Unfortunately there is a variation of detail that every contributor can provide. For instance one institute may be able to provide specific metadata concerning the geographical coordination (longitude, latitude) where some others may not. So elements of metadata classified into two categories according to their importance. The mandatory elements are the Collector Name (Agent), the Affiliation/ Institution, The date and time of collection, Country, Location and camera scale of the capture device expressed in microns. All the other metadata like

salinity and water depth are provided as a separate file that the user can upload using the same interface.

The metadata may be used later to allow Pleione users to select image sets according geographical criteria and date time attributes, for example. If more than 85 images are selected by the user then 5 of them are presented at four different poses at random, perhaps first it is presented normally, then again later it is presented rotated 180 degrees, in a third occasion it may be rotated 90 degrees and flipped on the axis of X and finally on the forth occasion the image may be presented rotated 90 degrees and flipped in both axes. So the total number of images that are presented is 100(80+5x4). In all cases the presentation sequence of any image set is unlikely to be the same since the application uses two random number generators iteratively to select two images at a time swapping their positions in the sequence. This iteration happens exactly for half of the number of images that are going to be presented. If the image set selected is less than 85 images then it is only presented in random sequence. This method is aiming to confuse the experts with the duplication of images. The purpose that this method is used is to extract inconsistent users. This measure may indicate the level of 'expert-ness' an expert can proffer on a plankton labeling task.

The entire database of ITIS has been downloaded and integrated into the system. The local copy of ITIS is used as the name thesaurus for the identification of specimens. The ITIS database is stored by compressing all taxa into a single table whilst making a clear discrimination between synonyms and valid/accept scientific names. Every record in this table is assigned a unique identifier named Taxonomic Serial Number (tsn). The records into this table also using an 'endogenous foreign key' (Mackey, 2002) that referencing the same table. This structure allows the storage of the whole taxonomic classification hierarchy something that is exploited by the application in order the taxonomic elements to be represented with a tree composition in the form.

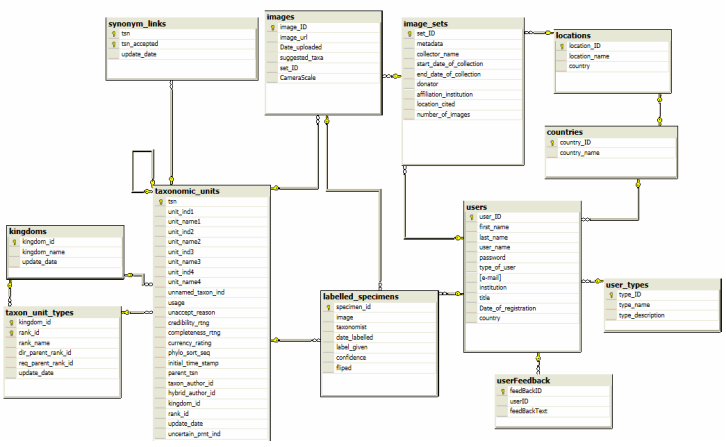


Figure 1: The database schema of Pleione: On the left the ITIS tables as are adapted, with the taxonomic units table to be the name thesaurus for the labelled_specimens table.

The "heart" of the database is the labelled_specimens table (see Figure 1) where all the experimental results are stored. It links an image and also the way that this particular image was presented with the judgment of a taxonomist as well as how confident the particular taxonomist was for his judgment. The confidence rate referred previously gives an extra clue about the accuracy of a label given by person basis.

4 Experimental results

The web application has been deployed to an IIS 6.0 web-server. Using the relevant user interface, 4 different image sets of plankton specimens were added: each sample contained 66, 38, 112, 63 images respectively (279 total). All the datasets were from samples taken from the Bay of Naples (collected by I. Bettino and imaged by P. Culverhouse, using HAB Buoy unit 0 underwater camera system). Three volunteer experts (one from the University of Plymouth, one from Plymouth Marine Laboratory and one from the Louisiana State University) provide the first experimental results for the system. The experts, using the interface in Figure 2, labeled in total 180 specimens (22, 99, 59 accordingly respectively). Each expert was free to select or make a combination of the four available image sets but in case the number of images was equal or exceeding the 85 the system was randomly selecting and duplicating some of them with the rules described in the methodology section.

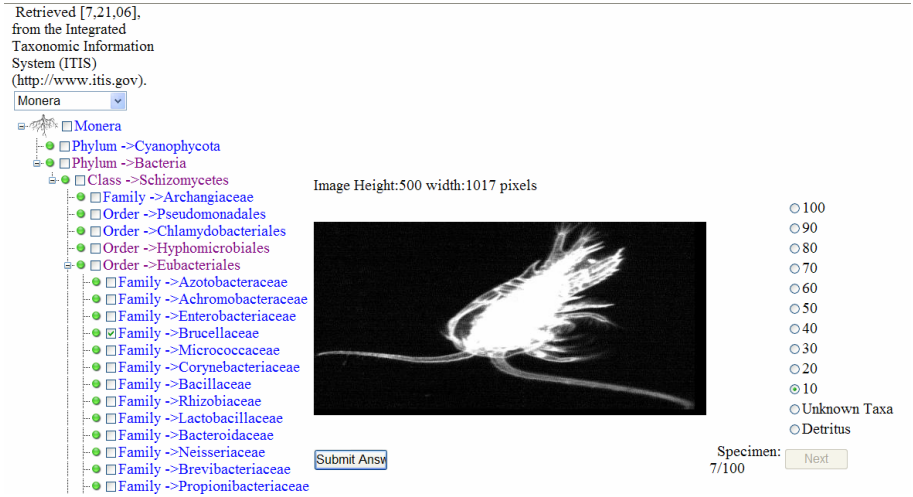


Figure 2: Specimen identification page

The average time taken for an expert to label a specimen using this interface was between 0.76 minute and 0.5. From the 180 labeled specimens there were 77 cases that two or more opinions of the same or different experts were referring to the same image. These occasions allowed self-consistency and consensus of opinions measurements. What can be noted from the total 8 available cases for measurements on self consistency is that although experts used different labels in different sittings

of the same image their opinion is self consistent. This happens because all the labels used for the classification of a given specimen were conforming to the same nested hierarchy without using another branch on the taxonomic tree. The study also noted that in all these cases only the first label was different whilst all the following labels were the same (for each expert). Since the sample is very limited the phenomenon will not be interpreted at the moment as it could be a small sample artifact.

Also, from the 23 available cases for measurements on consensus of opinions, there was only one case that had complete disagreement between the experts. In 12 cases the consensus of opinions was perfectly matching. In four cases the measurements of consensus were not feasible since there were only two experts that had labeled the same image and one of the two had answered as 'Unknown taxa'. In the other 6 cases the consensus of opinions had variations on the rank of the taxa given. For instance the first user was able to reach the phylum level were the other two the subclass and order level. But since all the cases were conforming to the same classification hierarchy are concerned as 100% consensus to the level (rank) that all opinions were matching.

Because there were no cases that experts showed inconsistencies in their judgements and the fact that all specimens categorized to the same kingdom (Animalia) the histogram in Figure 3 was produced. This diagram indicates the ability of experts to reach the desired outcome of labelling a specimen to the species level (as they were asked to do). For this purpose cases in which a taxonomist labelled more than one time the same image have been excluded leaving the best answer that he could provide (best effort).

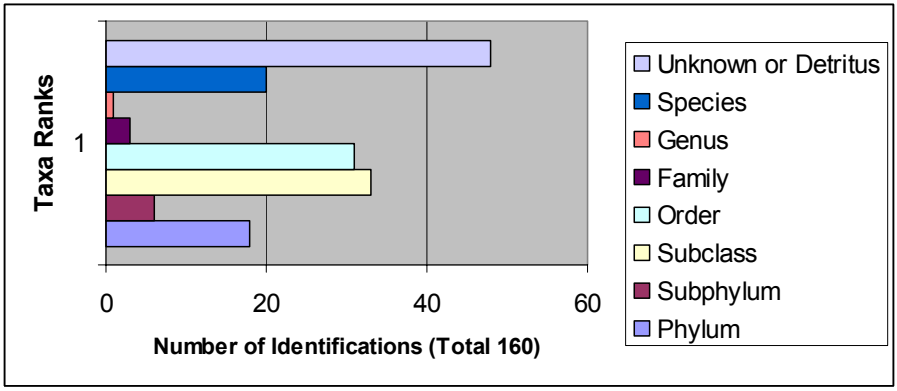


Figure 3: Ability of experts to reach the Species level

As it could be seen from Figure 3 histogram the ability of the users to reach the species level was only feasible 20 times out of the total 160 identification attempts (12.5%). Most of the times experts identified specimens as 'Unknown' or 'Detritus'. This has to do with two facts. The quality of images is varying from image to image and also the fact that the interface had not given a specific demarcation from these

two concepts led the users to categorize these two cases under the same label. Then the cases of Subclass and Order (33, 31 accordingly) are indicating that is the most likely level of identification if the image sets will keep to be selected with geographical region criterion only and the image-sets quality persist to be the same.

5 Discussion

On this limited sample of three experts and 160 expert opinions it has been shown that experts are self-consistent within taxonomic category. This is as expected, since experts of zooplankton were labelling images that fell within their specialisation. The sample size was small, and former research on the topic from Culverhouse et al. (2003) suggests domain experts can be up to 100% consistent at genera or taxon categorisation, but can drop to 85% for detailed species categorisations. It is hoped that a larger study can be completed using the system, revealing human performance variance across the world population of taxonomists and zooplankton ecologists.

A factor that may hinders the experts when attempting to give a species level label may be the lack of a mechanism to select an appropriate image set according taxa criteria, because every expert is specialized in a narrow range of taxa. Thus the system was unable to choose image sets that are optimal for an individual's expertise. This is a potential enhancement in future work.

The system produced by this research attends to the existing problems in taxonomy referred into the background section of this paper. Because if an expert uses a scientific name to label a specimen and a second expert uses a synonym that referring to the same taxon then measurement on consensus of opinions would be hindered. Also the problems of multiple classifications were in consideration. The scope of this research was not to produce a taxonomic database, which consequently has to confront all these problems, but only to collect expert judgments' as far as plankton identification is concerned. So the use of a checklist from a taxonomic database seems acceptable. The problem lastly concentrated to which one of these databases would best fit to the purposes of this study because retrieval from multiple resources as it mentioned may not be accurate. The ITIS database was finally chosen because according to the Institution standards it is not seeking to provide a cutting edge classification but rather a consensus of broadly accepted classifications (http://www.itis.gov/standard.html). The database also provides "quality indicators" for the records which can give easily a first look about the accuracy and completeness of a record. It makes an explicit demarcation between synonyms and Valid/Accepted names. It is funded by the Department of Agriculture in US and so probably it will continue evolving. Initial taxon data came from National Oceanographic Data Center (NODC) of US so the taxonomic information it is US-centred, but probably relevant to plankton from other parts of the globe. According to Hughes *et al.* (2004) it is used also by the British Oceanographic Data Center (BODC). And finally and more important can be download locally and is free of charge.

Another aspect of critical importance that directly affects this study is the fact that if specimen images labeled with scientific names alone (without referencing the authority of both name and taxonomic revision) then they will not have been precisely identified. Because a scientific name alone does not reflect the situation that a taxon concept has undergone a revision which have as a consequence changes into taxon boundaries (Kennedy *et al.* 2004). So a specimen labeled with a name alone may be linked to many different taxon concepts that arise from taxon revisions over the time (Kennedy *et al.* 2004). At the moment the best solution that can be given is the link of an image with a record of a reliable taxonomic database (for instance ITIS) which according to (Kennedy *et al.* 2006) is referencing to monographic treatments. So in this way the specimen is linked to a taxon concept and not to a name alone. This problem is well known to the scientific community and the solution that has been proposed by Kennedy *et al. (*2006) is the application of a data exchange standard (still under research) named Taxon Concept Schema (TCS). TCS is actually an XML schema that has designed to assist for data retrieval of both scientific names and their respective taxon concepts. If in the near future this data exchange format embraced by the scientific community the taxon concepts that will be available for representation by the TCS schema will be those exported from taxonomic databases like ITIS (Kennedy *et al.* 2006). Hence records of specimens identified using Pleione system will be able to be recognized globally referring to precise taxon concepts.

6 Conclusion

All in all, this research was an effort for the materialization of a system that will enable researchers to expose their plankton collections to an open study. This open study is including validation of plankton images that will later used as a feed for machine learning algorithms. From the beginning the standards that had been set for the creation of this system was to be as simple as possible but with the view to grow.

The conceptual design of this system had firstly to confront the existing problems in taxonomy. The study on this field which belongs to the new discipline of biodiversity informatics shows that the problems are well known to the scientific community but still there is no standard solution.

The solution has been given to this problem had consider the narrow time bounds of the implementation and the feasibility of the objectives in this bounds trying to do the best trade off between data quality and method selection. The method selected is the linking of a specimen with the records of the ITIS taxonomic naming system, that according to the literature presents a consensus of taxonomists opinions and at the same time providing a good handling of synonym problems. This has the potential for the Pleione-labeled specimens to be recognized globally. In case a taxon concept changed the labeled specimens can potentially associated with the new concepts since there is the opportunity of tracking the new records of ITIS and discriminate the changes. The testing results collected by the trial version of this system were encouraging and gave insights for further studies, but the system needs at least a mechanism of image selection according to taxa criteria.

7 References

Culverhouse, P., et al. (2001) '*Dinoflagellate 'Categorisation by Artificial Neural Network*', Final Technical Report, University of Plymouth. Available on:http://www.cis.plym.ac.uk/cis/projects/Reports/Final%20Technical%20Report.pdf(Last visited: 19-Nov-2006)

Culverhouse, P., Williams, R., Reguera , B., Herry V., and Gonzales-Gill S., (2003) '*Expert and machine discrimination of marine flora: a comparison of recognition accuracy of field-collected phytoplankton'*, in: IEE internation conference on visual information Engineering.

Culverhouse, P., Williams, R., Reguera, B., Vincent, H., Gonzalez-Gil, S. (2003) '*Do experts make mistakes? A comparison of human and machine identification of dinoflagellates*' Marine Progress Series, 247:17-25

Hughes, M. and Lowry, R. (2004) '*The BODC taxonomic browser-a powerful search tool to locate taxonomic information*' in proceedings of International Conference on Marine Biodiversity Data Management Hamburg, Germany: 29 November to 1 December 2004

Kennedy, J., Hyam, R., Kukla, R., and Paterson, T. (2006) 'Standard Data Model Representation for Taxonomic Information' OMICS: A Journal of Integrative Biology, 10(2):220-230

Kennedy, J., Kukla, R. and Paterson, T. (2004) 'Scientific names are ambiguous as identifiers for biological taxa: their context and definitions are required for accurate data integration' In , Proceedings of the 2nd International Workshop on Data Integration in the Life Sciences San Diego, USA:80-95. Available on: http://www.soc.napier.ac.uk/publication/op/getpublication/publicationid/8182971(Last visited: 9-Dec-2006)

Lindstron, J. (2006) '*Database Model For Taxonomic And Observation Data*', International Association of Science and Technology in: Proceedings of 2nd Iasted international Conference. Available on: http://www.cs.helsinki.fi/u/jplindst/dbarch_final.pdf (Last visited: 19-Nov-2006)

Mackey, A. (2002) '*Relational Modeling of Biological Data Trees and Graphs*' Available on: http://www.oreillynet.com/pub/a/network/2002/11/27/bioconf.html (Last visited: 19-Nov-2006)

Paterson, D. (2003) 'Progressing towards a biological names register' Nature,422:661

Paterson, T., Kennedy, J., Pullan M., Cannon A., Armstrong, K., Watson, M., Raguenaud, C., McDonald, S. and Russell, G. (2005) '*A Universal Character Model and Ontology of Defined Terms for Taxonomic Description'* Napier University Publications, Edinburgh, UK available on: http://www.soc.napier.ac.uk/publication/op/getpublication/publicationid/5941057 (Last visited: 21-Nov-2006)

Raguenaud, C. and Kennedy, J. (2002) '*Multiple Overlapping Classifications: Issues and Solutions*' In Jessie Kennedy (Ed),in 14th International conference on Scientific and Statistical Database Management - SSDBM 2002 :77-86. Available on : http://www.soc.napier.ac.uk/publication/op/getpublication/publicationid/931308 (Last visited: 9-Dec-2006)

Roderic, D., M. (2005) '*A Taxonomic Search Engine: Federating taxonomic databases using web services*' BMC Bioinformatics, 6(48) Available on:http://www.biomedcentral.com/content/pdf/1471-2105-6-48.pdf(Last visited: 21-DEC-2006)

Sumich, J.,L. (1999) 'An introduction to the Biology of Marine Life seventh edition', McGraw-Hill, London, UK

Sutherland, I., Embury, S.,M., Jones, A.,C., Gray, W., A.,White, R.,J., Robinson, J.,S., Bisby, F.,A., Brandt, S., M. (1999) '*LITCHI: knowledge integrity testing for taxonomic databases*' in: Eleventh International Conference on Scientific and Statistical Database Management:278-286

Network Intrusion Detection Systems Evasion Techniques – an Investigation Using Snort

J.A.Ytreberg and M.Papadaki

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Intrusion Detection Systems (IDS) provide an extra security precaution by detecting attacks that have bypassed the firewall. Snort IDS is one of the most widely used IDS (Siddhart, 2005). When a network is monitored by an IDS, attackers can send evading attack packets that will try avoiding detection. This research conducted experiments testing Snorts alerting capabilities when mutated attack packets where sent to a web server, using an IDS evasion tool called Nikto. It was found that Snort alerted for about half of the attack packets. Weaknesses in Snorts capabilities in detecting certain evasion attacks where found, which can be solved by creating customized rules. The research also proposes a new detection method for Snort, dividing large request strings into smaller ones, analyzing each of them against the rules. The total danger level of these combined strings could decide if Snort would alert for the request.

Keywords

NIDS, IDS, Evasion, Snort, Nikto, Rules, Detection, Networks, Monitoring

1 Introduction

As the world depend increasingly more on computer technology, so does the need for ways of securing these technologies. A network intrusion detection system (NIDS) usually lies behind the firewall of a security implementation, monitoring the network for attacking packets bypassing the security devices. Where malicious packets are found the NIDS will trigger an alert and log an event, it will not stop the packet in any way. Its purpose is to act like a smart network scanner, combining network capture packet techniques with a rule and alerting procedure. Intrusion detection systems is like a second line of defense (Anderson, 1980), and they all have their own strengths and weaknesses. Depending on configuration, placement, upgrade, etc. they all behave differently (Del Carlo, 2003).

NIDS are not 100% reliable and we do not expect it alerting all attacking packets, simply because this is a very difficult task. By configuring NID sensors to be too sensitive it would alert for too many packets which actually are legitimate network traffic (false positive). On the other hand, if the NID system is configured to be less sensitive we would most likely see attacking packets bypassing the NIDS unnoticed (false negative). What we do want is a balanced relationship between the number of

false positives and false negatives, also called Crossover Error Rate (CER) (Chapple, 2003). According to Sodiya et al. (2004) IDS systems still produce too many false positives and false negatives and lack the efficiency sorely needed.

Evasion techniques are ways of mutating packets, forcing the NIDS not to trigger off an alert, simply because it thinks the packets are legitimate traffic. There are many different evasion techniques all designed to evade the IDS in the best manner possible, still producing the right end results at the targeted node (i.e. web server).

The research has conducted a series of experiments using Snort IDS, one of the most popular IDS on the market (Siddhart, 2005). The purpose of the research experiments were divided into three parts:

- Evaluation on how well Snort IDS responded to evasion attacks from Nikto
- How well does Snort function when its processor is fully engaged
- Improvement needed areas of Snort rules and detection engine

This paper will present some of the prior work in the area of IDS, followed by the experiments methodology and results. Finally the findings will be analyzed and discussed, ending off with a concluding part of this paper.

2 Background

A research conducted by Richard Barber in 2001 found that IDS applications analyzing protocols and packet behavior were more efficient than applications utilizing pattern matching techniques. The research also discovered that if network load exceeds 35%, NIDS can suffer in its performance and start dropping packets. If the load at the Network Interface Card (NIC) on the NIDS get to high, packet will start evading it, simply because it does not have the capacity to analyze them all (Barber, 2001).

There has been a previous research including Snort, done by Vlasti Broucek and Paul Turner conducted in 2004. This research used Snort to observe the hit rate, and false-positives generated when monitoring a web server over a two month period. It was found that Snort using fine-tuned rules, still was a subject to a number of false-positives. When discovering attacks it was found hard tracing these attackers back using the Snort logs. Only IP addresses are available for inspection. Snort also had severe difficulties in analyzing encrypted communication, especially tracing packets back to the attackers (Broucek, Turner, 2004).

One way of increasing the performance on Snort was discovered by Ian Graham and his research on how to use multi-processors in combination with Snort. The performance on Snort was greatly improved by balancing the load over several processors. Traffic will vary from different networks, but there will always be a performance gain if using multi-processors (Graham, 2006).

Another method of improving an IDS is the use of a keyword selection method, with the intention of making the IDS smarter by counting keywords and calculating the risk of the attack probability. This technique improved the hit rate of an IDS, without increasing the false alarms (Lippmann, Cunningham, 2000).

3 Methodology

The experiments will have three essential components in use: a web server, an attacking computer running Nikto, and the NIDS installed on a monitoring computer. All these devices are connected to each other via a hub, enabling the NIDS to monitor all traffic between the attacking computer and the web server. The NIDS will also be configured to have a NULL IP. This because of two important factors:

The NIDS should stay hidden to prevent attackers noticing it

The NIDS should not be able to send packets through the monitoring NIC, only receive.

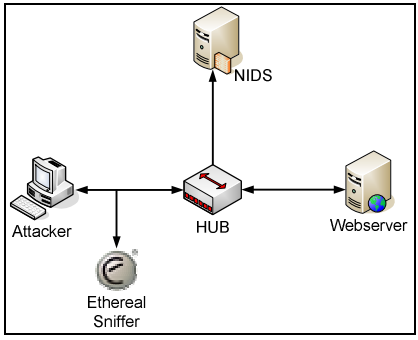


Figure 1: Experiment network topology and traffic flow

Figure 1 illustrates the network packet flow and the placement of the devices. The Ethereal sniffer is installed on the attacker computer for analyzing reasons. Notice that the NIDS will only receive packets, never allowed to send any. The NIDS will not have an IP address, but will still be able to sniff all traffic passing through the HUB (Kistler, 2003). The attacking PC will use the network tool Nikto, with its built-in evasion techniques. The NIDS will consist of a laptop installed with Snort IDS version 2.4.5. The research accomplished four different experiments, each one with dissimilar goals and test setup and configuration:

Test Description	Test Relevance
Test1 is an experiment where focus is upon Snort's detection abilities when submitted with mutated evasion packets.	Snort's performance can be compared to other IDS
Test2 is dedicated to finding out how Snort reacts when the CPU runs at maximum capacity (Snort recommends at least 300 MHz and 128 RAM for a low level traffic network) (Bull, 2002).	How would Snort perform if installed on a busy network or overloaded client?
Test3 is designed to find how new modified signatures affect the results. This experiment is much like Test1, with the exception of the adding of the new signatures.	Research upon writing own signatures and configuration options in Snort.
Test4 combines more evasion techniques to each attack packets using a method in Nikto which allows several evasion techniques at once. The goal of this experiment is to see if the research modified signatures still alert for complex packets involving several evasion techniques combined.	To what degree does several evasion techniques combined together affect the attacks, and the newly created signatures.

These experiments will be conducted in the same manner to produce the most accurate results. Where there are unexpected results, the tests will be run several times to produce more stabile results. This way we eliminate incidents with extreme results only occurring once.

4 Results

4.1 Results for Test1 – Snort's detection engine efficiency

Snort alerted differently based on the evasion attacks sent to the web server. The number of total attacks sent from Nikto varied by just a few packets per experiment, while the Snort detection varied much more frequently. Snort normally alerted for about 50% of the total evasion attack packets that where on the wire. The exceptions occured when Nikto used its evasion technique four "prepend long random string to request". Snort actually alerted for more than the total evasion packets sent on this occasion (see figure 2).

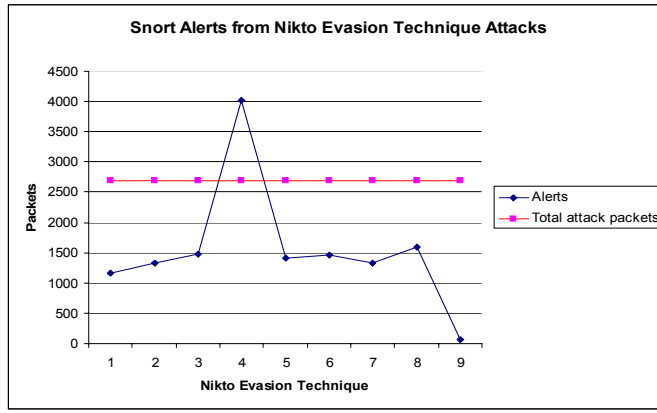


Figure 2: Snort's alerts compared to the total evasion attack packets sent

Figure 2 also show a relative small alert figure when Nikto used its evasion technique nine (9) "session splicing". This number is to be taken lightly, because of an incomplete experiment when testing this method (see chapter 5.1.9, NIDS evasion techniques - Thesis, Ytreberg, 2007).

4.2 Results for Test2 – Snort Detection under extreme conditions

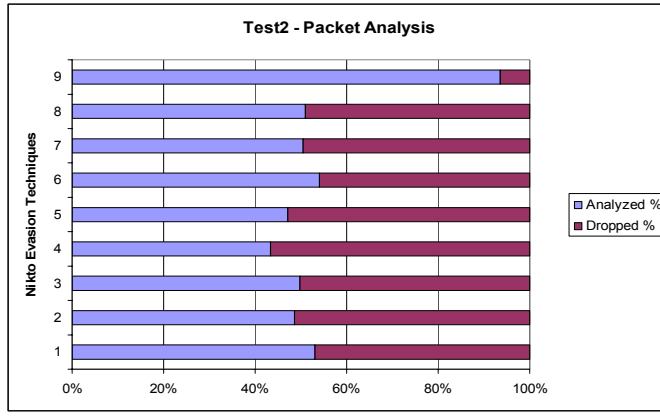


Figure 3: Snort's alerts compared to the total evasion attack packets sent

By using an option called verbose mode, making the NIDS output all packets received on its interface, the research stressed the CPU and memory of the NIDS. The goal was to see how Snort reacted when it had less processor capacity and memory than needed. As seen on figure 3, Snort started dropping packets after a few minutes of the experiment. Snort dropped around 50% of the packets when face upon the evasion attacks, with the exception of evasion technique nine.

4.3 Results for Test3 – Enhanced Signature Testing

The research created five (5) new signatures with the intention of improving Snort's hit rate. The signatures were created to improve areas where Snort usually alerts, but fails to do so because of some of Nikto's evasion techniques. The five new signatures looked like this (truncated):

```
content:"etc"; nocase; content:"/./"; content:"passwd"; nocase;
content:"/./"; content:"usr"; nocase; content:"bin"; nocase;
content:"etc"; nocase; content:"/./"; content:"hosts"; nocase;
content:"boot.ini"; nocase;
content:".passwd"; nocase;
```

After similar testing with the new signatures in place the results showed improved hit rate on the Snort detection (see figure 4).

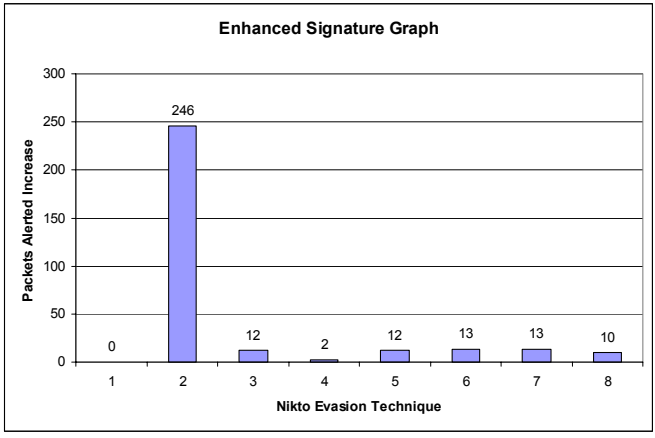


Figure 4: Alerts increase with new signatures

4.4 Results for Test4 – Combining Nikto Attacks

This test proved that the research's newly created signatures even work when Nikto mutates its attack packets by using several techniques per packet. Figure 5 illustrate a steep increase when Nikto combines method two and three, and a smaller increase when Nikto uses evasion method five (5) and six (6) combined.

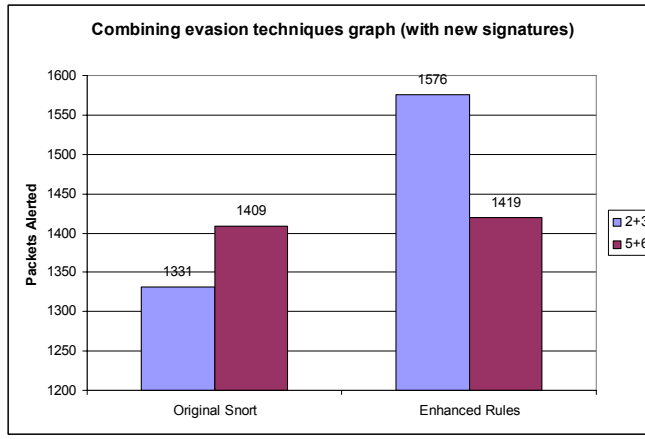


Figure 5: Packet increase alerts with new signatures

5 Discussion

The reason for Test1 - evasion technique four (4) triggering the high number of alerts, is because of two factors. Firstly, all packets look almost identical sending around 700 bytes of random strings before the actual request string in the end. This leads to Snort triggering off an alert per packet. Secondly, Snort will also alert on packets with malicious requests in the end, meaning each attack packet can get several alerts. This leads to the high number of alerts. When using evasion technique nine (9) the low number of alerts is simply because the experiments never ended. Session splicing requires many hours to complete, and the research had to abort after about five hours. Parallels can be drawn however, towards a NIDS on a busy network encountering session splicing attacks. If the NIDS is quite busy, it will not have the ability waiting for all session packets for reassembly, thus the packets will evade the NIDS.

If the NIDS is installed on a computer that is occupied with other duties as well as the intrusion detection system, it can be subject to dropping packets. As Test2 show the NIDS will drop packets if its resources are fully engaged. The most ideal placement of a NIDS would be on a separate node in a network, with no other applications and a processor of at least 1 GHz and memory of preferably 512 kb or more. With these resources the NIDS have the ability to withstand a high load on the network.

The area of which the research had focus on creating new signatures was towards Nikto's evasion technique two "add directory self-reference /./". These new signatures improved Snort's hit rate greatly when Nikto used this technique, and also when this technique was combined with most of the other evasion techniques. The command "nocase" were added to all signatures to prevent evasion techniques evading the signatures by using random casing. The problem occurred when Nikto

used its evasion technique one (1) “random URI-encoding”. The new signatures did not alert when this technique was used, or any other in combination with this one. This is why figure 5 shows no increase in alert using evasion technique one. All the other evasion techniques had an improved hit rate when using the new signatures (exception session splicing, not enough testing).

The work done by Lippmann and Cunningham in 2000 was a new way of thinking, trying to make the IDS smarter. The research find that there should be created some sort of system where Snort instead of scanning the requests for incidents, analyzes the whole packet in a different way. By dividing the request content into smaller strings, and then to analyze each string a danger level classification (see table 1) could be the answer. If the total level of danger for the entire request exceeds a limit, an alert would be raised. This method would eliminate any incidents where one attack packet gets several alerts, but most importantly it would make the Snort IDS more dynamic. More dynamic in the way it divides and conquers any mutated packet trying to bypass its systems, looking for known dangerous format patterns in its rules.

Content	Danger level (1-10)
/./	4
cgi-bin	2
/./	4
passwd	8
Total:	18

Table 1: Content separation and danger classification

6 Conclusion

The research experiments provided evidence of Snort’s capabilities for detecting mutated packets with evading features. It also answered these following questions:

To what degree is a Snort NIDS capable of detecting evading packets from an attacking computer?

Snort without any special customized configuration and new rules will detect around 50% of evasion-only packets sent from Nikto. This number is to be taken lightly as it only concludes how Snort reacts to these kinds of evasion attacks. There are many other techniques that can be used to evade Snort as well.

How well does the NIDS detect alerts when its processing power is fully engaged?

When Snort NIDS CPU was overloaded it started dropping packets, but it was consistent in all experiments around this. It processed all packets it could and alerted them, until it suddenly dropped all further packets. The results were exactly the same as on Test1 up till the point where the NIDS had to drop packets. This is better than

dropping a packet or two in between, because it would then be harder for administrators to notice that the NIDS CPU or memory was overloaded.

Is there a need for new and improved signatures?

Yes. There will always be a need for new signatures in Snort as attack tools and new techniques continue to develop and arise. Depending on the area of use, attack tools can be used to test a business IDS, and then to analyze the results. These results can then lead to new and customized rules that will protect the business optimally. Snort is very easy to configure and writing rules can be done in a couple of minutes. New signatures can improve a needed area greatly compared to the released Snort rules. Each NIDS has its own different network to protect, with all kinds of devices with lots of incoming requests. It is not an easy task to write common rules that is applicable for all these devices on Snort. The fact that Snort is an open source project means that it is the users that write the signature or the application would slowly die out.

7 References

Anderson, J.P. (1980), "Computer Threat Monitoring and Surveillance", (In Anderson, J.P. Technical report, Fort Washington, Pennsylvania)

Barber, R. (2001), "The Evolution of Intrusion Detection Systems – The Next Step", Computers & Security, Vol. 20, pp 132-145

Broucek, V., Turner, P. (2004), "Intrusion Detection: Issues and Challenges in Evidence Acquisition", Internal Review of Law Computers & Technology, Vol. 18 No.2, pp 149-164

Bull, J. (2002), "Snort's Place in a Windows 2000 Environment", www.snort.org/docs/snort-win2k.htm (Accessed 19 December 2006)

Chapple, M. (2003), "Evaluation and tuning an intrusion-detection system", searchsecurity.techtarget.com/tip/1,289483,sid14_gci918619,00.html?track=IDSLG, (Accessed 4 January 2007)

Del Carlo, C. (2003), "Intrusion Detection Evasion: How an attacker get past the burglar alarm", www.securitytechnet.com/resource/security/ids/1284.pdf#search=%22past%20and%20current%20work%20in%20evasion%20ids%20techniques%22, (Accessed 3 January 2007)

Graham, I. (2006), "Achieving Zero-loss Mutli-gigabit IDS – Results from Testing Snort® on Endace Accelerate Multi-CPU Platforms", www.touchbriefings.com/pdf/2259/graham.pdf (Accessed 3 January 2007)

Kistler, U. (2003), "Snort IDScenter 1.1 manual", www.engagesecurity.com/docs/idscenter/ (Accessed 30 December 2006)

Lippmann, R.P., Cunningham, R.K. (2000), "Improving intrusion detection performance using keyword selection and naural networks", Computer Networks, Vol. 34, pp 597-603

Rain Forest Puppy - rfp (1999), "A look at whisker's anti-IDS tactics", www.ussrback.com/docs/papers/IDS/whiskerids.html, (Accessed 30 December 2006)

Siddharth, S. (2005), "Evadion NIDS, revisited", www.securityfocus.com/infocus/1852, (Accessed 19 December 2006)

Sodiya, A.S, Longe, H.O.D and Akinwale, A.T. (2004), "A new two-tiered strategy to intrusion detection", Information Management & Computer Security, Vol. 12, No. 1, pp 27-44.

Investigation on Static Network with Network coding

P.Omiwande and L.Mued

University of Plymouth, Plymouth, UK

Abstract

The distribution of information from a source node to a large number of destination nodes over a communication network has attracted a lot of attention for more than a decade. The theory of network coding shows that achieving the optimal throughput is possible, and, moreover, computationally efficient (i.e. there are polynomial algorithms for computing the optimal routing). The basic idea is to send encoded information along the edges of graph; the nodes of the network process the information they receive and produce encoded packets that they forward to their neighbours. In comparison, the traditional store-and-forward paradigm, in which the nodes send bits of the original file without further processing, cannot achieve the optimal throughput; moreover, computing the maximum possible rate using store-and-forward is a known difficult problem.

Keywords

Network Coding, Multicast Networks.

1 Introduction

Network Coding is a field of information theory and coding theory in order to achieve maximum flow of information in a network. The idea of network coding is to allow and encourage mixing of data at intermediate network nodes. When a receiver sees these data packets and deduces from them the messages that were originally intended for the data sink. In contrast to traditional ways to operate a network that try to avoid collisions of data streams as much as possible, this elegant principle implies a surplus of surprising results. Not only is network coding a fresh and sharp tool that has the potential to open up stagnant fundamental areas of research, but due to its cross-cutting nature it naturally suggests a unified treatment of previously segmented areas.

The fundamental concept of network coding was first introduced for satellite communication networks in a paper presented by (Yeung *et al,* 1999). Thereafter, the concept was fully developed in a paper presented by (Ahlswede *et al*, 2000) where in the latter the term *network coding* was coined and the advantage of network coding over store-and-forward was first demonstrated, thus refuting the aforementioned tradition. The advantage of network coding cannot be over emphasised due to its generality and its vast application potential. Network coding has generated much interest in information and coding theory, networking, switching, wireless

communications, complexity theory, cryptography, operations research, and matrix theory.

Network coding treats information as mathematics entities that can be operated upon, rather than as unmodifiable objects to objects to be transported. It allows the network nodes to perform arbitrary operations on information from different incoming links. The aim of this is in network wide effects arising from coding across multiple links. Network coding has been proven to reach Min-cut Max-flow optimality at least in lossless network with directed graphs in adding to the theoretical attractiveness of the approach by (Chekuri *et al* 2006).

2 Project Aim

The aim of this papers research is to investigate the new area of network coding, in order to achieve optimal throughput in a network. This method has been shown to reduce bandwidth usage for multicast networks (Zhu *et al* 2004). The project also required an initial investigation, gathering and summarizing recent papers on this topic. Analytical studies are highly needed to understand the mechanisms of network coding, how coding and decoding takes place at various nodes which involves proper understanding of Galois field $GF(2^m)$ theory.

We focused on the term *network coding* aimed to establish an understanding of how this is essentially applicable to multicast which involves multiple sources and multiple destinations a type currently supported by so many networks, a typical example is video conferencing, where information and resources are being shared by various participants at various locations. This research on this topic will look at number of initiatives which are considering the delivery of a complete end-user experience as opposed to the traditional routing method which involves store and forward to the next node through an output link.

3 Network Coding Concept

The advantage of network coding over the traditional method of routing system can be shown by a simple butterfly method. The principle and concept of network coding could be demonstrated by a simple butterfly method as shown in the figure 1 below:

There are two different sources at the top, each having value *a* and value *b* to pass across to the destinations Y and Z at the bottom nodes of the diagram below. However, at the bottom each node wants to have knowledge of both values *a* and *b*. Each edge can carry only a single value considering an edge transmitting a bit in each time slot.

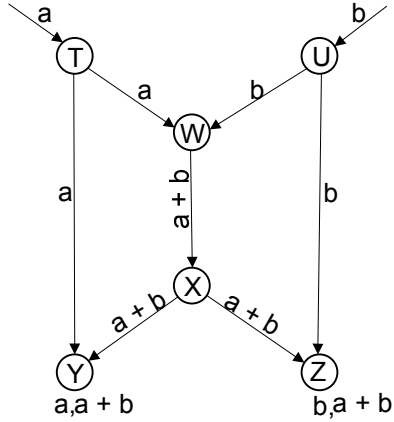


Figure 1: Shows network coding by simple butterfly method

With traditional routing method, the central line will either carry value *a* or value *b* but definitely not both values at the same time. Assuming we send value *a* through the centre line, the left destination Y would receive *a twice* and not know *b* at all, and if we send *b* right destination Z will equally receive *b twice*, without either of them having knowledge of each other. With that, we can say that routing is practically insufficient, since no routing scheme or method could transmit both value *a* and value *b* simultaneously to both destinations Y and Z.

Using a simple code, as shown above, we can get both value *a* and value *b* to both destinations simultaneously by sending the sum of the symbols through the center this implies that we encode both value *a* and value *b* using the formula "*a+b*" The left hand side which is Y destination receives *a* and *a+b*, and can find *b* by subtracting the two values. This is a linear code because the encoding and decoding schemes are linear operations.

With network coding, each node of the distribution network is able to generate and transmit encoded block of information. The randomization introduced by the coding process eases the scheduling of block propagation and thus makes the distribution more efficient (Gkantsidis *et al* 2005).

4 Methodology

We adopt a similar model of (Koetter *et al* 2003), which represents a network as directed graph *G*. The discrete independent random processes $X_1, \ldots, X_n$ are observable at one or more source nodes, and there are $d \geq 1$ receiver nodes. The output processes at a receiver node β are denoted by $Z(\beta, i)$. The multicast connection problem is to transmit all the source processes to each of the receiver nodes. There are *v* links in the network, where link *l* is an incident outgoing link of the node v =

tail (l), and an incident incoming link of v if v = head (l). We call an incident outgoing link of a source node a source link and an incident incoming link of a receiver node a terminal link. Link l carries the random process $Y(l)$.

We have chosen the time unit such that the capacity of each link is one *bit per unit time,* and the random processes X_i have a constant entropy rate of one bit per unit time. Links with larger capacities are modelled as parallel links, and sources of lager entropy are modelled as multiple sources at the same node.

The processes X_i, $Y(l)$ and $Z(\beta,i)$ generate binary sequences. We assume that information is transmitted as vectors bits which are of equal length u, represent as elements in the finite field $GF(2^m)$. The length of the vector is equal in all transmissions and all links are assumed to be synchronized with respect to the symbol timing. Considering a linear code, the signal $Y(j)$ on a link j is a linear combination processes X_i generated at node v = tail (j) and signals $Y(l)$ on incident incoming links l. When considering the delay-free case, we assume that G is a $GF(2^m)$ linear network, if for all links the random process $Y(j)$ on a link $j = (v, u, i) \in E$ represented by the equation below:

$$Y(j) = \sum a_{i,j} X_i + \sum f_{l,j} Y(l) \tag{1}$$

Note that (i: X_i generated at v) and (l: head(l) = v)

And an output process $Z(\beta,i)$ at receiver node β is linear combination of signals on its terminal links, can also be represented as

$$Z(\beta,i) = \sum b_{\beta_{i,l}} Y(l) \tag{2}$$

Note (l: head(l) = β)

For multicast on a network with link delays, memory is needed at the receiver nodes, but memory less operation suffices at all other nodes (Koetter *et al* 2003). We consider unity delay links, modelling links with longer delay as links in series. The corresponding linear coding equations are where μ represents the memory required is shown below:

$$Y_{t+1}(j) = \sum a_{i,j} X_{it} + \sum f_{l,j} Y_t(l) \tag{3}$$

(i: X_i generated at v) and (l: head(l) = v)

$$Z_{t+1}(\beta,i) = \sum \sum^{t} b_{\beta_{i,l_{t-m}}} Y_m(l) \tag{4}$$

The above coefficients $\{a_{i,j}, f_{l,j}, b_{\beta i,l} \in GF(2^m)\}$ can be collected into $n \times v$ matrices $A = (a_{i,j})$ and the $v \times v$ matrices $F = (f_{l,j})$ whose structure is constrained by the network. For acyclic graphs, we numbered the links ancestrally, which mean lower-numbered links upstream of higher-numbered links, so matrix F is upper triangular with zeros on the diagonal. A triple (A, F, B), where $B = \begin{bmatrix} B_1 \\ . \\ . \\ B_d \end{bmatrix}$ specifies the behaviour of the network, and represents a linear network code.

Considering a typical representation of point-to-point network connections, in which we develop some theory and notation necessary for us to be able to solve this complex equations involved in figure 2 shown below:

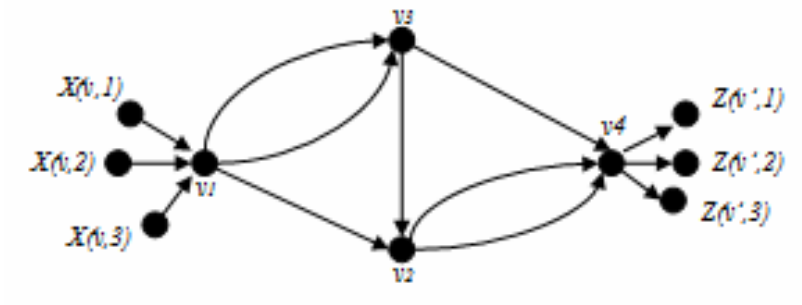


Figure 2: Summing the path gain in network coding

Let node v be the only source in the network. We let $\underline{x} = (X(v,1), X(v, 2),\ldots, X(v, \mu(v)))$ denote the vector of input processes observed at v. Also, let v' be the only sink node in a network . Let $\underline{z} = (Z(v',1), Z(v'2),\ldots, Z(v', v(v)))$ be the vector of output processes.

We need to consider the Galois Field $GF(2^m)$ of linear network so that we can give a transfer matrix so as to describe the relationship between and input vector x and an output vector with this simple equation $\underline{z} = \underline{x}M$ (Costello *et al* 2004).We consider the elements of matrix M as polynomials.

From Figure 4.1 above we are able to derive these sets of equations in the network and which enable us to absolutely understand the relationship between the input vector $\underline{x}$ and the output vector $\underline{z}$.

The outputs at node v_1 are shown below:

$$Y(e_1) = \alpha_{1,e_1} X(v,1) + \alpha_{2,e_1} X(v,2) + \alpha_{3,e_1} X(v,3)$$

$$Y(e_2) = \alpha_{1,e_2} X(v,1) + \alpha_{2,e_2} X(v,2) + \alpha_{3,e_2} X(v,3)$$

$$Y(e_3) = \alpha_{1,e_3} X(v,1) + \alpha_{2,e_3} X(v,2) + \alpha_{3,e_3} X(v,3)$$

The outputs at node v_3 are shown below:

$$Y(e_4) = \beta_{e_1,e_4} Y(e_1) + \beta_{e_2,e_4} Y(e_2)$$

$$Y(e_5) = \beta_{e_1,e_5} Y(e_1) + \beta_{e_2,e_5} Y(e_2)$$

The outputs at node v_2 shown below:

$$Y(e_6) = \beta_{e_3,e_6} Y(e_3) + \beta_{e_4,e_6} Y(e_4)$$

$$Y(e_7) = \beta_{e_3,e_7} Y(e_3) + \beta_{e_4,e_7} Y(e_4)$$

The output at node v_4 is shown below:

$$Z(v',1) = \varepsilon_{e_5,1} Y(e_5) + \varepsilon_{e_6,1} Y(e_6) + \varepsilon_{e_7,1} Y(e_7)$$

$$Z(v',2) = \varepsilon_{e_5,2} Y(e_5) + \varepsilon_{e_6,2} Y(e_6) + \varepsilon_{e_7,2} Y(e_7)$$

$$Z(v',2) = \varepsilon_{e_5,3} Y(e_5) + \varepsilon_{e_6,3} Y(e_6) + \varepsilon_{e_7,3} Y(e_7)$$

From the output at node v_4 we can compute our first matrix so as to show the relationship between input value $\underline{x}$ and output value $\underline{z}$. Let matrix $\boldsymbol{A}$ be as shown below:

$$\mathbf{A} = \begin{bmatrix} \alpha_{1,e_1} & \alpha_{1,e_2} & \alpha_{1,e_3} \\ \alpha_{2,e_1} & \alpha_{2,e_2} & \alpha_{2,e_3} \\ \alpha_{3,e_1} & \alpha_{3,e_2} & \alpha_{3,e_3} \end{bmatrix}$$

And from equation 4.57, 4.58 and 4.59 we compute the second matrix **B** as shown below:

$$\mathbf{B} = \begin{bmatrix} \varepsilon_{e_5,1} & \varepsilon_{e_5,2} & \varepsilon_{e_5,3} \\ \varepsilon_{e_6,1} & \varepsilon_{e_6,2} & \varepsilon_{e_6,3} \\ \varepsilon_{e_7,1} & \varepsilon_{e_7,2} & \varepsilon_{e_7,3} \end{bmatrix}$$

From the above matrix A and matrix B we can obtain our system matrix *M* which is

$$M = A \begin{bmatrix} \beta_{e_1,e_5} & \beta_{e_1,e_4}\beta_{e_4,e_6} & \beta_{e_1,e_4}\beta_{e_4,e_7} \\ \beta_{e_2,e_5} & \beta_{e_2,e_4}\beta_{e_4,e_6} & \beta_{e_2,e_4}\beta_{e_4,e_7} \\ 0 & \beta_{e_3,e_6} & \beta_{e_3,e_7} \end{bmatrix} B^T$$

From the above equation we can obtain our determinant of *M*.

The determinant of matrix *M* is equals to

$$\det(\mathrm{M}) = \det\mathrm{A}\,(\beta_{e_1,e_5}\beta_{e_2,e_4} - \beta_{e_2,e_5}\beta_{e_1,e_5})(\beta_{e_4,e_6}\beta_{e_3,e_7} - \beta_{e_4,e_7}\beta_{e_3,e_6})\,.\det(\mathrm{B}) \quad (5)$$

We are interested in nonzero determinant which we have gotten from equation (5) above. We can then choose our parameters in an extension field $GF(2^m)$ so that the determinant of *M* is nonzero over $GF(2^m)$. Therefore, we can choose matrix *A* as identity matrix and matrix *B* in order to have an overall matrix *M* as identity matrix also.

5 Linear Network Coding

We consider network coding approach for multicasting from several sources over a network in which nodes independently and randomly select linear mappings from inputs onto output links over some field. Let a network G be given together with a set C of desired connections. One of the fundamental questions of network information theory is under which conditions a given communication scenario is admissible. We make some simplifying assumptions:

The capacity of any link in G is a constant, e.g. one bit per time unit. This is an assumption that can be satisfied to an arbitrary degree of accuracy. If the capacity

exceeds one bit per time unit, we model this as parallel edges with unit capacity. Fractional capacities can be well approximated by choosing the time unit large enough.

Each link in the communication network has the same delay. We will allow for the case of zero delay, in which case we call the network delay-free. We will always assume that delay-free networks are acyclic in order to avoid stability problems.

Random processes $X(v, l)$, $l \in \{1, 2, \ldots, \mu(v)\}$ are independent and have a constant and integral entropy rate of, e.g., one bit per unit time. The unit time is chosen to equal the time unit in the definition of link capacity. This implies that the rate $R(c)$ of any connection $c = (v, v', X(v, v'))$ is an integer equal to $|X(v, v')|$. This assumption can be satisfied with arbitrary accuracy by letting the time basis be large enough and by modelling a source of larger entropy rate as a number of parallel sources.

The random processes $X(v, l)$ are independent for different v. This assumption reflects the nature of a communication network. In particular, information that is injected into the network at different locations is assumed independent (Koetter *et al* 2003).

In addition to the above constraints, we assume that communication in the network is performed by transmission of vectors (symbols) of bits. The length of the vectors is equal in all transmissions and we assume that all links are synchronized with respect to the symbol timing.

6 Project Conclusions

We focused on the term *network coding,* aimed to establish an understanding of how this is essentially applicable to multicast which involves multiple sources and multiple destinations a type currently supported by so many networks, a typical example is video conferencing, where information and resources are being shared by various participants at various locations. The studies on this topic revealed a number of initiatives which are considering the delivery of a complete end-user experience as opposed to the traditional routing method which involves store and forward to the next node through an output link. In the situation where an intermediate node is on the transmission paths toward multiple destinations, it sends one copy of the data packets onto each output link that leads to at least one of the destinations.

We show in this paper the analytical method on complex networks and it was proven to show encoding and decoding at different nodes. Because of the intrinsic broadcast property of wireless networks this linear combination might be received at several receivers resulting in new linear combinations when they are mixed with other packets. At destination, multiple linear combination are received through different paths resulting in a system of linear equations; if the number of independent equations exceed the number of combined packet the system of linear equation could be inverted leading to the initial packets. This is to compare with classical routing approach where only packets that validate routing criteria are forwarded or flooding

where each single packet is forwarded indifferently. Network coding is attractive for challenged networks because of its inherent unsynchronized operation; each node decides to forward a random linear combination without needing any global information about the topology or destination placement.

Our concerns for future work are area of selective placement of randomized coding nodes in networks where not all nodes have coding capability.

There are interesting problems in distributed resource optimization and scheduling algorithms for networks with con-current multicast and unicast connections. Another further work includes extensions of different applications, such as non-multicast. It would be of great interest to consider various protocols for different communication scenarios and evaluate the associated overhead, comparing this with traditional based approach.

7 References

Ahlswede R., Cai N., Li S. R. and Yeung R. W., "Network information flow," *IEEE Transactions on Information Theory,* IT-46, pp. 1204-1216, July 2000.

Chekuri C., Fragouli C. and Soljanin E. "On Average Throughput and Alphabet Size in Network Coding," *IEEE Transactions on Information Theory* vol. 52, no.6 pp.2410–2424 June 2006.

Costello D.J. and Lin S. "Error Control Coding," Pearson Education, Inc, USA 2004.

Gkantsidis C and Rodriguez P. R. "Network Coding for Large Scale Content Distribution," (*IEEE Infocom* pp. 1-11. 2005)

Koetter R. and Medard M. "An Algebraic Approach to Network Coding," *IEEE*/*ACM* Transactions on Networking, vol. 11 2003.

Yeung R. W. and Zhang Z. "Distributed Source Coding for Satellite Communications," *IEEE Transactions on Information Theory*, IT-45, pp. 1111-1120. 1999.

Zhu Y., Li B. and Guo J. "Multicast with network coding in application-layer overlay networks," *IEEE Journal on Selected Area in Communications, 2004.*

Analysis and Evaluation of IDS Alerts on a Corporate Network

C.Rousseau, N.L.Clarke and B.V.Ghita

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

More and more, organizations rely on their network (Lundin Barse, 2004). This makes them vulnerable and the actual security means are no longer powerful enough. In order to bring more security than the traditional firewalls, IDS came out. Unfortunately, they do not bring the expected level of security. As they generate a lot of false positive, they tend to makes administrator of such systems turn them off. This paper then tries to analyze the cost effective of IDS for organizations. They today do not have the same means to face threats and vulnerabilities. If some companies are willing to invest a lot in security, some others are not. This research work has been based on the University of Plymouth network. It pointed out that IDS had to be properly configured in order to involve less investment for the administrators. But it also underlined that designers of such systems have to improve their effectiveness. Today, considering the investment that IDS represent, they do not seem cost effective enough to be used by all organizations.

Keywords

Intrusion Detection System, False Positives, Log analysis

1 Introduction

These last years, corporate networks have seen a huge increase in network threats. “During the first half of 2006, Symantec observed an average of 6,110 DoS attacks per day” (Symantec Website, 2006). Where many variants of attack have been created, number of malware has also increased. The last year, there was a growth of 48% in viruses, worms, Trojan, and spyware (Sophos, 2005). In 2006, 41,536 new threats have been detected by Sophos. The actual security tools corporate networks use are not powerful enough. Firewalls cannot handle threats alone anymore. FBI recently underlined that “98% of organizations use firewalls, but that 56% of them had still experienced unauthorized network access” (Porter, 2005). A few years ago, the goal of the attacks was only the proud. Most of them are now designed in order to cause economical impacts The Financial Insights estimated in 2006 that the lost would be “$400 million or more due to phishing shemes”. Universities are also the target of attackers. The University of Oxford has recently been hacked. Two students have been able to “find out anyone's email password, observe instant messenger conversations and control parts of the university's CCTV system” (Slashdot, 2004). A quite similar attack also happened in the University of California where students’

personal information have been stolen (Hines, 2005). If universities are today facing the same threats than companies, they don't have the same means to face them. Indeed, universities do not have any security team to analyze generated events by security systems. Most of the time, their own law forbids them to monitor the traffic for confidential matters. Universities network are then more "open" and vulnerable to threats. Then for all these organisations, the need for security was obvious. Several security systems have come out but one has particularly attracted attention. Intrusion Detection Systems (IDSs) "inspect traffic inbound from the Internet for attacks against exposed Internet facing systems" (Stevenson, 2006). But as it is a quite new technology, IDS have some weaknesses in construction and configuration. They can sometimes generate much more than 1000 alerts per day. These alerts are, for most of them false positives (legitimate traffic tagged as attack by the system). This quite often compromises their effectiveness and makes the administrator of such system turn it off. But such system as presumed to be very powerful in attacks detection.

In order to test this effectiveness, this paper focuses of the efficiency of an IDS on the University of Plymouth campus network. It will first of all present a brief overview of the different IDS technology and will then present the methodology of the research. This will be followed by the findings of this research and a discussion of these results.

2 Overview of existing IDS

The IDS technology first started in 1987 with a generic IDS model presented by Dorothy Dening of the University of Georgetown. The model had to be independent from the environment in which it was evolving and its vulnerabilities. It also has to be independent of the types of intrusion.

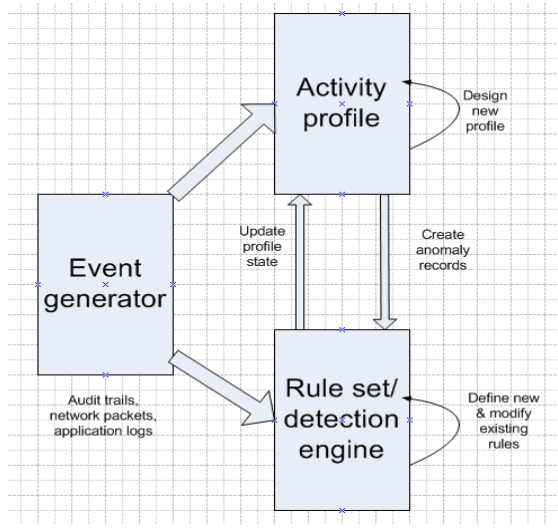


Figure 1: A typical IDS model (Escamilla, 1998)

From this model many others have come out and have implemented more accurate functions. Today, IDSs use the CIDF model (Staniford-Chen, 1998). However they are all based on this basic one. Briefly, the "Event generator" monitors the traffic. The "Activity profile" contains variables of the network and "defines" the environment. The last module, the "Rule set/Detection Engine" represents the engine used by the IDS to detect intrusion. Many engines exist and represent different IDS. A brief overview of the different IDS algorithms is given in this part.

IDSs have to face two issues. They have to be able to detect well known attacks but also to anticipate future attacks. That is why many different algorithms have come out. Unfortunately, no one can deal correctly the both matters and all have some advantages and disadvantages. The most popular are anomaly detection and pattern-matching engines. The anomaly detection is based upon thresholds. Statistics on users' behaviors are made during a defined period in order to record their "normal" behaviors. From these results, thresholds are set up. They can represent many parameters concerning users, group, servers, and files. The anomaly detection engine adjusts its thresholds in order to automatically update behaviors. Once these thresholds set up, each time a behavior will go over one of them, an alert will be triggered. This system presents a main advantage: it is able to detect new attacks because every variant of attacks will obviously differ from the normal behaviors. But two major problems remain in this system. First of all, an attacker can slowly insert an attack behavior inside the system as it automatically updates its thresholds. Secondly, the system will maybe trigger a lot of false positives because a user often changes its behavior. Another statistical method has been created: the Heuristic-based analysis. This algorithm does not work upon statistics about user's behavior but upon the attack's behavior (CISCO System, 2002). It looks at the requests' behaviors inside the network and where they come from. This algorithm can sometimes be the only way to detect malicious activity in a network

The pattern-matching engine works differently. It contains signatures that basically define a known attack. By this way they theoretically only generate a low number of false positives as they recognize a known attack. But this system is extremely vulnerable to new attacks. It has to have a rule for each new attack that makes it slowing down. Then, the aim of these rule is to, by changing their structure, be able to detect new variants of attacks. The definition of the rule can then represents an event but also a sequence of events or regular expressions. To improve the efficiency of the pattern-matching algorithm, the stateful pattern matching has been brought out. This algorithm considers that an attack can be hidden in different packets. For example, the commands the attacker sends to execute malicious code can be divided into two different packets. A default pattern-matching algorithm would not recognize it because it deals packet by packet. By memorizing previous packets, this system deals with a stream of data and not with only one packet. If this system is not difficult to implement, it can generate a high number of false positives. Indeed, by considering data as a stream, it multiplies the probability of misdetecting an attack. To limit the high number of false positives that could be generated by the stateful pattern matching, the protocol decode-based analysis algorithms are based on the protocol fields. Where the previous algorithm looks for a pattern matching

everywhere in the payload, this algorithm looks for a specific field of the protocol. By this way the detection of pattern matching is much more accurate. But the protocol has to be completely defined which is not always easy.

Many other systems do exist and try to implement advantages of two different systems. Emilie Lundin Barse (2004) cites some of them as example. RIPPER is based upon the anomaly and the pattern-matching detection. Briefly, it creates statistics of the previous data stored by data mining process. From these statistics and from the current intrusion, it defines rules. These rules fit much more the intrusions than hand created ones. A new type of IDS systems has also been brought out: the visualization systems. The Girardin's system (1999) is based upon a neural network and represents attacks as a map where the axes represent the different factors involved in the attack. The attack in then placed in this map according to the value of the different factors it represents. Erbacher and Frincke (2000) have created another visualization IDS. This one represents the entire network with nodes and links. The attacks are represented according to the different colors and different shapes that each node and link can take.

3 Methodology

In order to evaluate the need of an IDS for the University of Plymouth, an analysis of events has been made. When analyzing events, a methodology is essential. The methodology of this paper is based upon the incident handling procedure described in the Handbook for Computer Security Incident Response Teams (CSIRTs)" (West-Brown *et al.*, 2003). It describes the actions a CISRT has to take to deal with incident. Once an incident is opened for analyzing, an incident report has to be created. The incident report (or incident handling form) has been created upon the form described in the TERENA's Incident Object Description and Exchange Format Requirements (Arvidsson *et al*., 2001). This report has to contain a tracking number to follow the event throughout the analysis process. It also contains the basic information about the event such as when it occurred, the attackers and the victims. Once these basic informations are collected, the incident report goes to a deeper analysis state. It is then important to define the depth of analysis. This last one depends upon different factors. It first of all depends on the team's mission and technical capabilities but also on the severity of the incident, the chance of repetition of the incident and the knowledge the analysis can bring to the team. The amount of data collected was too important to deeply analyze every event. In order to be able to provide a great analysis, the six most popular events (which represented more than 96% of the entire data) have been deeply analyzed. Then, all the high-priority incidents have also been deeply analyzed in order to judge the efficiency of the IDS on high-severity threats. The deep analysis consisted of analyzing particular day, hour, source IP address, destination IP address, and so on. When possible, a justification of each deep analysis has been made. Then the deeper analysis was able or not to classify the incident. Four classes of results were possible. The "false positive" class represented the incident considered as mostly false positives. The class "depends on IP" represented incidents for which some events were probably false positives but some were potential attacks. The third class called "potential

attacks" represented incidents for which most of the generated events have been considered are potential attacks. Finally, the class "Unknown" represented the incidents for which it was not possible to give any hypothesis on their nature.

4 Results

To carry out this research, the data have been collected from the University of Plymouth network. It represented a common organization network and was then a relevant example for the cost effective of IDS for an "open" organization. The data have been collected two times. The first one was the 27th of March to the 11th of April and a second one from the 14th of June to the 23rd of June. TCPDump has been used to capture the traffic. Then Snort has been used as the intrusion detection system. Snort is a free signature-based NIDS (Network Intrusion Detection System). Scripts have been applied to the output alert file to anonymized the data

For the analysis of the different incidents, it has been presumed that a typical attack scenario was matching some essential criteria. First of all, the attempts occur grouped and are not spread out over time. Many other critera can be considered but mostly depend on the nature of the attack itself. Different source IP addresses can be used to launch an attack but no many different ones. Depending of the nature of the attacks, many or only one IP destination could be considered as a typical attack scenario.

As explained in the methodology, each event has been classified in one of the four categories. The chart below represents the classification of all the high-priority events analyzed.

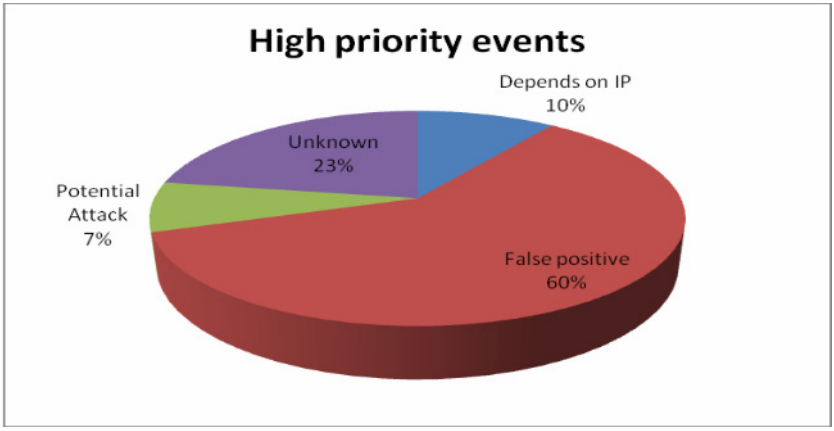


Figure 2: Classification of the high-priority events

More than the half analyzed events (60%) have been classified as false positives. Only 7% of these high-priority events have been classified as potential attacks. But quite a lot of events have not been classified and represent 23%.

%	No	Attack	Priority	Severity
51.72	6945449	SNMP request udp {udp}	2	medium
23.68	3180194	SNMP public access udp {udp}	2	medium
14.24	1912385	BAD-TRAFFIC IP Proto 103 PIM {pim}	2	medium
2.50	335264	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited {icmp}	3	low
1.77	238052	RPC portmap status request UDP {udp}	2	medium
1.25	167197	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited {tcp}	3	low
1.16	155808	DDOS Stacheldraht agent->handler skillz {icmp}	2	medium
0.94	126086	ICMP PING NMAP {icmp}	2	medium

Figure 3: The six most popular attacks

According to Figure 3, the six most popular incidents have been analyzed as well. Five of them are medium-priority and one is low-priority.

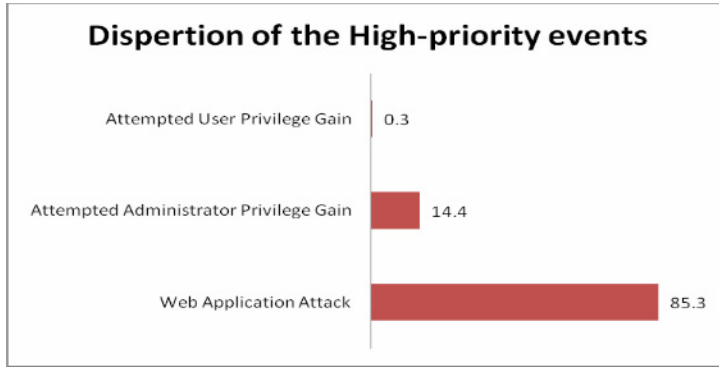


Figure 4: Dispersion of the high-priority events

Among the high-priority events, it was expected to find out a lot of injecting worms attempts. Surprisingly, only one has been potentially identified as so. For quite a few incidents, the evolution of the events over time looked the same as the global traffic. As it appeared that most of the high-priority events were web application attacks, the false positives hypothesis has been made in most cases. Indeed, attacks should not have any correlation with the global traffic otherwise it is obvious that legitimate traffic is "wrongly" tagged as attack.

The results of these analyses in addition to the results of the high-priority incidents gave the overall proportion of category class in the alert file. The graph below shows these proportions.

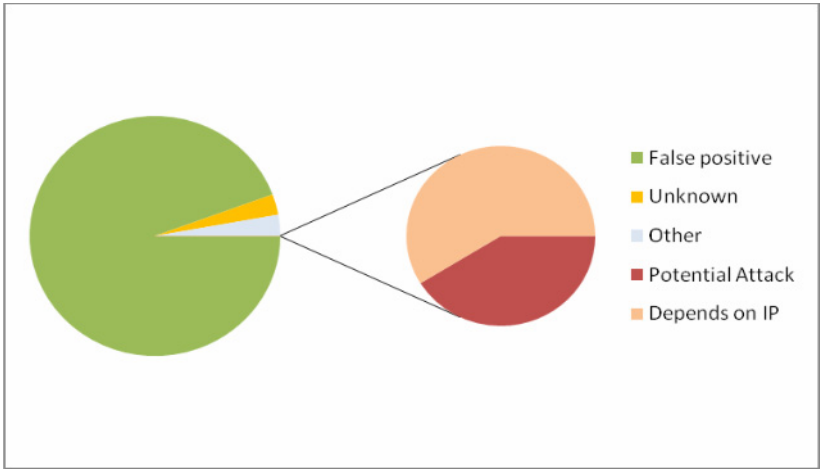


Figure 5: Dispersion of the events in the alert file

The number of potential attacks looks insignificant. But it still represents a number of potential attacks between 31 and 4300 per day by considering the "Unknown" events and the "Depends on IP" events. If it is not negligible in term of attacks attempts, it is in term of effectiveness. Indeed, five of the six of the most popular incidents have been classified as false positives. They are categorized as either medium or low priority and represent 94.8% of the entire alert file. In addition with the high-priority false positives, the entire proportion of false positives in the alert file represent more than 97%.

Several causes have been identified to these false positives. Many times it appeared the source or the destination IP addresses did not match the rule correctly. The rule that matches an attack can require an external or an internal IP address as source or as destination. Quite a few times the IP addresses involved in the generated events were incorrect according to the definition of the rule. It has been found out that the problem was in the operating system and the IDS configuration. The variables used by Snort could be substituted by the operating system variables, generating a lot of false positives.

It also appeared that the events generated by the http_inspect pre-processor of Snort have generated a lot of false positives. Briefly, the http_inspect pre-processor is a HTTP decoder implemented in Snort that can do the work that 1000 rules would do (Sturges, 2007). To work properly, the http_inspect pre-processor has to be accurately configured. The hypothesis of an incorrect configuration has been reinforced by the fact that similar incidents to those triggered by the pre-processor have also been triggered by a rule. Moreover this first version implemented in Snort does not handle the stateful processing. This can lead evasion attacks to bypass the system.

A few times, it appeared that the evolution of an incident over time looked surprisingly the same as the opposite of the global traffic. The number of events was slightly evolving to reach the highest in the middle of the night and to reach the lowest in the middle of the afternoon. Unfortunately the research did not come up with any hypothesis for that. A few times, a relationship between incidents have been seen and analyzed. Some incidents had a common source/destination IP address or generated events at the same time the same day. No certitude has been brought concerning a real link between these incidents. They could show a real attack as they could confirm a false positive hypothesis. However this way of research has shown a potential to bring more information concerning events.

5 Discussion

These results obviously show that too many false positives have been generated by the IDS. The proportion of false positives in the alert file represents an average of 142 763 false positives per day. These false positives are parasites for the quality of the collected data and make more difficult for administrators to find out attacks. Obviously the analysis of each incident could be deeper. To be more accurate, rather than analyze events as one incident, each event should be analyzed. However these results give a good overview of the composition of what the alert file likely is. The high-level priority events represent only 0.3% of all events and contain only 7% of potential attack. Even if 23% of events have not been classified as false positive or potential attack, this percentage is still low. In order to bring more reliability on the IDS, solutions have been proposed for most of the problems outlined in this work. This paper underlines the need for users of such system to configure it. They cannot do it properly without a good knowledge of the network and its need. Indeed, the resolving of IP address can bring answers on the legitimacy of traffic only if the potential communication of the University network with an external organization is well known. But this paper, across the http_inspect pre-processor, also showed that some weaknesses still remains in the design of IDS. So far, attackers have always had a step ahead the administrators and designers of such system. Security updates and patches come out after the attacker has already had the time to exploit the vulnerability. This main problem makes IDS focusing more on the detection of new variants of attack as quickly as possible. But by focusing on the efficiency, the effectiveness is maybe slowing down. This is maybe one main reason for the high rate of false positive generated.

6 Conclusion

From these results, the use of IDS seems to need a lot of investment. Their efficiency has to be much improved. The percentage of potential attacks detected represents indeed a real threat for organizations. But considering the huge number of parasite that can be generated in the log, it would cost a lot of time to really detect attacks. The percentage of false positives is definitively too high to show the effectiveness of such system in a network. However, a better configuration would definitively improve the quality of the alert file and could let think of a future with an IDS for every organizations. But so far the cost investment it represents is too much

important. Only organizations that deal with high confidentiality data will be ready to invest a lot in that system. For organizations that do not have the same means, such as the University of Plymouth, it does not seem essential to set up an IDS.

7 References

Arvidsson, J., Cormack, A., Demchenko, Y., Meijer, J. (2001), "TERENA's Incident Object Description and Exchange Format Recquirements", http://www.ietf.org/rfc/rfc3067.txt (Accessed 11 July 2007)

CISCO System (2002), "The Science of IDS Attack Identification", http://www.cisco.com/en/US/netsol/ns731/networking_solutions_white_paper09186a0080092334.shtml (Accessed 02 August 2007)

Dorothy Denning Web Site (1996), "An Intrusion-Detection Model", http://www.cs.georgetown.edu/~denning/infosec/ids-model.rtf (Accessed 20 July 2007)

Erbacher, R.F. and Frincke, D. (2000) "Visualization in Detection of Intrusions and Misuse in Large Scale Networks", http://www.cs.usu.edu/~erbacher/publications/SecurityVisPaper1-Mar2000.pdf (Accessed 03 May 2007)

Girardin, L. (1999), "An eye on network intruder - administrator shootouts", http://www.usenix.org/publications/library/proceedings/detection99/full_papers/girardin/girardin.pdf (Accessed 09 August 2007)

Hines, M. (2005), "Security Threats", http://news.zdnet.co.uk/security/0,1000000189,39192114,00.htm?r=2 (Accessed 08 August 2007)

Lundin Barse, E. (2004), "Logging for intrusion and fraud detection" http://www.cs.kau.se/~simone/Swits-IV/lundin.pdf (Accessed 08 August 2007)

Porter, T. (2005), "The Perils of Deep Packet Inspection", http://www.securityfocus.com/infocus/1817 (Accessed 06 May 2007)

Slashdot Web Site (2004), "Oxford Students Hack University Network",http://it.slashdot.org/article.pl?sid=04/07/16/021200(Accessed 08 August 2007)

Sophos, (2005), "Sophos Security Threat Management Report", http://www.sophos.com/security/whitepapers/SophosSecurity2005-mmuk (Accessed 05 August 2007)

Staniford-Chen, S., Tung, B., and Schnackenberg, D. (1998)," The Common Intrusion Detection Framework (CIDF)", http://gost.isi.edu/cidf/papers/cidf-isw.txt(Accessed 06 May 2007)

Stevenson, T. (2006), "Extrusion Detection: Security Monitoring for Internal Intrusions ",http://www.windowsitlibrary.com/BookReviews/BookReview.cfm?BookReviewID=95(Accessed 20 July 2007)

Sturges, S. (2007), "HTTP Inspect",http://www.snort.org/docs/snort_htmanuals/htmanual_2615/node61.html (Accessed 11 July 2007)

Symantec Web Site (2006), “News Release - Vulnerabilities in Desktop Applications and Use of Stealth Techniques**”,**http://www.symantec.com/en/hk/about/news/release/article.jsp?prid =20060926_01(Accessed 24 January 2007)

A Generic Information Security Framework for Mobile Systems

A.Sharma and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Mobile devices have faced tremendous changes in the past few years. Mobile devices are now tending to blend in to the category of PCs. While providing a bundle of services such as email, calendar, managing appointment and contacts, these mobile devices can also connect to a network via wifi. The risk caused by this is tremendous as there is no proper security framework at place. Many organizations being aware of this fact implement few add-on such as user authentication, virus protection, firewall, intrusion detection, etc. but these add on provide solution in a very different way. Many solution provided take action after the problem has occurred. This paper suggests a framework which can be incorporated in to the security mechanisms so as to avoid the above mentioned problems.

Key words

Mobile security, user authentication**,** security framework, ISO 17799, levels of users, Organizational user, General users

1 Introduction

Mobile device are becoming to be one of the most vital devices in not only corporate network but also they are turning out to be one of the most powerful devices for commutation with many networks on the move. It can be recognized that mobile devices are becoming one of the most vital tool for business, but there has not been a standard framework to protect the data. The mobile devices are not connected single network but they are connected to multiple networks at the same time, which means that the risks to the mobile devices and the network they are connected increases with these connectivity.

There has also been consideration on the authentication methods, the efficiency of authentication provided by PIN, and the impact of security on the mobile network as well as the mobile device. A look at the connectivity of the mobile network is also taken which provides the various risks by the various connectivities.

According to a survey by Frost & Sullivan there are more than 50 million workers whose jobs required them to perform work outside the office, in the near future with a growth of 6%, its going to be 72 million, and the number of mobile professionals using mobile devices to store data is going to be more than 37 million in the year

2007. According to this survey, Executives directors and midlevel managers make up to 57% of the enterprise professionals using mobile devices, field services employees conduction installation, service and repair comprise 17%, mobile sales employees 16% and vehicle operators make the remaining 10% (Frost, 2006)

According to another survey 36% of their employees carry laptops and mobile devices containing sensitive customer information. 98% of respondents say their organizations allow remote access to their corporate networks. As a result of recent world events and varying airline travel restrictions, 73% of respondents now believe more laptops and mobile devices may be lost or stolen during air travel. While 37% of respondents indicate they have already experienced some form of data breach due to loss or theft of mobile devices, a staggering 68% of respondents indicate it is likely they too could experience a data breach in the future. In fact, during a recent Entrust webinar, 60% of attendees noted that someone on their immediate team had a mobile device lost, misplaced or stolen. 64% of respondents have implemented specific policies and/or procedures instructing employees on how to avoid a sensitive data breach. Over 90% of organizations indicate they are reliant on their employees to take specific actions to help comply with these policies, with 37% indicating they are "very reliant" on employees. This reliance, coupled with the fact that 84% of respondents indicate a degree of difficulty in trying to influence employees' behavior in adhering to these policies makes policy alone an ineffective means to mitigate the risk of a data breach. (Etrust, 2006)

2 PIN Authentication

In the past few years we have noticed the number of mobile phones being used grow exponentially. According to a recent survey the mobile phone subscribers in the world has exceeded more than 2.14 billion (Mobiletracker, 2006). According to CIA fact book there are more number of mobile than the population of people in UK (CIA, 2006). Escalating number of mobile phones are lost or stolen each year, indicating valuable information of the user is at threat. In a second generation mobile phones (GSM) the security from unauthorized usage is achieved by combination of 2 secure radio encryption interfaces, SIM (Subscriber Identity Module) and IMEI (International Mobile Equipment Identifier). This enables the legitimacy of the devices before allowing it to utilize the network. The two identification numbers being used, they are mainly concerned to service provider. However the user vastly depended on the Personal Identification Number (PIN) authentication. This facility is enabled by the user before any level of protection is provided. It can be noticed that the security provided by the PIN is arguable, since the mobile devices contains a considerable amount of information of the user. (gsmworld, 2006)

In contrast, the 3rd generation mobile phones are not merely devices for communication. The advancements in the mobile have changed drastically in the past few years with easier ways effective ways of communication, the authentication methods of the mobile phone have not changed a bit for the pas 15 to 20 years. Since the introduction of the mobile phone the only authentication methods that is being used is "PIN" (Personal Identification Number). Mobile phones previously

were only used to make and receive calls and for texts. But the whole idea of mobile phones has changed, they are not just phones they are devices which whole bunch of entertainment and connectivity, they are having more processing speed than normal PC 5 to 6 years before. Loss of Mobile phone is loss of valuable information

In a survey conducted to determine the attitude of the user on security of mobile device 89% of the users knew about PIN authentication, but only 56 percent actually used it. It was also observed that only 76 percent of the users used only single lever PIN security (at power on). Of those 76 percent of users only 36 percent of them used the PIN to protect at the standby mode.The other key finding were that more than 11 percent of the users didn't even know about the PIN facility which can be more than 84 million user in real world, Of those 44 percent of the user who did not use PIN facility, 65 percent of the users gave the reason as it being incontinent. A large number of respondents, 41 percent have little confidence offered by the pin authentication. (Clarke et al. 2002)

3 Connectivity of Mobile Devices

These latest handheld devices are connected in more than one way which are

- traditional network, the service provider
- GSM or 3G depending on the connection
- Infrared
- Bluetooth
- IEEE 802.11 (Wifi)

Which make the device 5 times more vulnerable than the traditional PC.

The focus of this paper is mainly on Bluetooth and Wifi as they are more susceptible to attacks.

3.1 Impact of Bluetooth on mobile security

According to security advisor Kaspersky Lab, reports that Russia had earned the dubious distinction of becoming the ninth country with a confirmed infection of a virus targeted at Bluetooth devices called "Cabir.a" worm, which had already been stricken handheld devices in many country.(Kaspersky, 2007). The devices can also be attacked by Bluebug, and Bluesnarfing.

3.2 Impacts of IEEE 802.11(Wifi)

In Wifi there are mainly 2 different types of attack Denial of Service and Man in the Middle. Denial of service attack mainly prevents user from accessing network resources, it simply denies them from the service, hence the name denial of service. The usual method that triggers DoS is to flood a network with degenerate or faulty packets, crowding out the legitimate traffic causing the system not to respond.

Similar to DoS attacks, man-in-the-middle attacks on a wireless network are significantly easier to mount than against physical networks, typically because such attacks on a wired network require some sort of access to the network. Man-in-the-middle attacks take two common forms: eavesdropping and manipulation

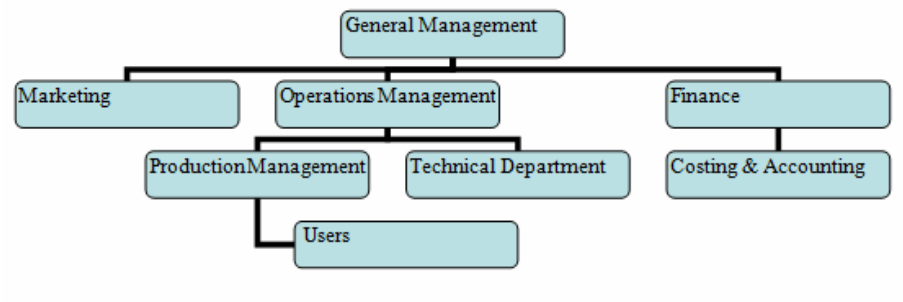
4 BS ISO/IEC 17799 Applicability to Mobile devices

In the following section these standards have been analyzed and they are applied mobile devices, most of the controls specified in this standard are universal which can be applied to any kind of devices and networks. The controls have been directly taken from BS ISO/IEC 17799 to check the applicability for mobile devices

Out of 11 categories, 39 control objectives, and 133 controls in ISO 17799 almost 99of the controls can be applicable to mobile devices and 9 being applied in special cases. A mobile device in some senses is similar to a normal PC and in more senses similar to a Laptop either of them can be connected via Wifi in a network. More over a Laptop has more similarities to a mobile device as it is more flexible to take from place to place. Most of these controls were defined to stationary devices like a standard PC. With a bit of similarities between a PC and mobile devices being there these Controls can be applicable. In the below section the applicability of each control has been explained.

5 Organizational Hierarchy

Given below is a simple model of organizational hierarchy, which gives most of the departments and users working.



The chart given above is a typical hierarchy of any organization. The best named companies such as Spryance Inc. and Acusis India. These companies are basically into ITES (Information technology enables services), health care business processing outsourcing. These companies are into outsourcing the healthcare services business to developing countries such as India, Pakistan, and Philippines due to low cost labor.

The general management is at the top of the chart followed by operations management. General management is directly connected to finance and costing &

accounting. Production management, technical department are directly below operations management, and users are directly under production management.

The process of work activity a is done in the following fashion

- The operation management plans the whole activity of the team as per the requirement.
- The operation management provides tasks to production management team
- Technical staff is directly under level operational management as it can take orders directly from them and do the necessary changes in the network
- General management is provided with reports by operation management on the tasks achieved.
- Marketing team gives the status of the market to operations management to provide with future implementations, and operation management does the task with the help of all other staff.
- The general management has a direct control over finance, cost & accounting. Marketing is under operations which give suggestions on strategies to operation management.
- The planning is done by operational management to be implemented by production management.
- These plans are implemented by production management team and users. The technical department is directly under operational management as well as general management

It can be seen from the above hierarchy that the user here can easily be divided in to 4 different levels.

- General management and operational management can be considered under highest level as they have most of the rights in the organizational network.
- Marketing finance, accounting & costing and other departmental management come under this second highest level.
- Technical department and production management team come under this level as they take orders from highest level, operational department and management.
- The rest of the users come under lowest level as they don't have much of rights and they have to work under the production team

From the above discussion it can be understood that there are more than 1 level of users, each block has different priorities and right.

6 Introduction to levels of users

In a corporation there are many different job descriptions with different works. In securing the mobile devices there must be different levels of authorization to different users.

For example a manager has the highest level of security as this user might be holding a tremendous amount of information on their mobile devices. A salesperson might be in medium security level as they might be holding most of the sales information and so on.

Levels of users in corporate network: When a corporate section is considered, there are many numbers of users. Each with different priorities and different usage. All these different users can be broadly classified in to 4 different levels. The basic definition and properties of these levels are given below

Level 1: This is the topmost level. This has the highest security and also the highest right.The user in this level can access to any file of any branch in that corporation.. The user has the rights to Update, modify and also delete certain files according to his\her priorities. As shown in the heirarcy the General management and operational management come under this level. For example the General Managemt of the company can come under this level, as they have many right in the network, they can access update, modify and delete the files according to the managers will. As this is the topmost level, this level must have the highest level of security. They can be considered as the highest percent of users as indicated in survey discussed in the previous section.

Level 2: This level user also has access to any files, but their access is limited to their own department. In this level the user can have all the rights specified in the above level, but their access is limited to their branch or department. As shown in the hierarchy departmental manager come under this level such as finance, costing and accounting and marketing users come in this level. The users in this level have access to all the files available in the network. They can update the document with the permission of the manager of the other department. For example HR manager can access only specific set of files which are under them. To access any other files which do not come under them they have to have proper accessing right from the other department they are accessing. This level has a security framework close to that of level 1. They can be considering at the 17% of the users as indicated in the survey.

Level 3: This level the user has access to their own profile. They can access modify, update delete information in their profile. They have access to browse files get information from any of the departments but they cannot edit the information. The users in this level can modify files in their own department, if required, this modification can only be done with the permission of the users in level 2 (as per the concerned departments). For example the staff in a sales department can access to the files in his department, if he/she needs to update the information in their department, he needs to get permission from the manager of that department, and only then can he do the necessary update. They do require the security framework, but not as users in level 1 and 2 need. They could come under the 16% of the users that were shown in the surveys discussed above.

Level 4: This level of users are similar to that of level 3. But the users in this level do not have any right to modify the files. They can modify their own profile, access files in their department and other department. For example students in the university can only access their files, modify their profile. That's all they can do. They do not require higher security frame work because of their access rights. As they are in a corporate network they will need a proper security frame work. They can be considered as the 10% of the users in the survey discussed above.

Levels of users in General sector*:* The non corporate users generally do not require the level of security as the corporate users need, although they have vital information to protect. They can be classified in to three levels which are given below

Level 1: This level user has the highest level in non corporate users. They are the people who have home offices, and users who are connected to their house network. They are mainly the people who use the Hotpoint where the service is available. For example users who sell products on eBay or even a stock broker who need constant update of market to do better business. They are not a big corporation. They are people who do their business. They check their update on the market and also do the banking on net. Their service is mainly dependent on their network service provider. Like the users in level 3 of corporate network who are governed by the rules and regulation of that certain corporate network these users have certain policies by the service provider. Level3 users in corporate have to follow rules of the corporation, here they are give certain policies which should be followed for their protection, following not following is their choice. Here the user is independent unlike corporate user.

Level 2: This level users are the users who do not get connected to any network. They only access the check their mails and surfing the net. They are also the users who use the Hotpoint to get connected to the network. They mainly use the internet for fun rather than work. For example the user access net where they don't have any computer to access their mails and surfing. They are in some way similar to user level4 in corporate users.

Level 3: The users in this level are the users who do not have any access to any of the connectivity. They use their mobile devices only to send and receive calls and also SMS. These are the users who do not need any protection. They are the users who either do not have device which is not advanced enough or either they are ignorant of the functionalities of a device or even both

Applicability of ISO 17799 Standards to each Level:

Corporate user:

- 99+9 controls can be Applicable Level 1 users
- 58+1 controls can be Applicable to Level 2 users
- 33+3 controls can be Applicable to Level 3 users
- 31+2 controls can be Applicable to Level 4 users

General User:

- 15+15 controls can be applicable to Level 1 users
- 9+9 controls can be applicable to Level 2 users
- 5 controls can be applicable to Level 3 users

Note: + X are the controls which can be applied to the users depending on the situation.

Similarities between level:

- 21 controls are similar between level 3 and level 1 in both the levels.
- 16 controls are similar between level 4 and level 2 in both the levels.

7 Conclusion

Mobile devices as known are changing. With new versions and new features included in to the mobile devices, making it more and more advanced each day. As they are becoming more and more indispensable devices, both in organizational and general level. All though mobile devices provide wide varieties of benefits they are at threat and pose a great danger both to the network as well as the device. The PIN authentication lacks in security. By the observations done in the above sections about the authentication of the mobile devices by PIN is quite questionable. The connectivity of the mobile devices are given an importance as they are the main cause for any kind of attack occurring. The important bits of those concepts were taken in to consideration to provide a framework. A deep analysis of ISO 17799 revealed that most of the standards were applicable which helps to make the base of this framework.

Studies have reveled that there are different levels of users who use a network, both in organizational and general level. The concept of different levels of users which gives a new dimension of security, each level user would need different security standards, by applying this ISO 17799 Standards appropriate policies needs to be applied. The framework suggested may provide a possible solution to many security issues.

8 References

Acusis India, 2007 - organizational hierarchy http://www.acusisindia.com/AIP0302/AcusisCompany/Associations.asp

Bitpipe, 2006 – Mobile device Security http://wp.bitpipe.com/resource/org_1108588893_863/Mobile_Device_Security_11579_edp.pdf?site_cd=bp

CIA, 2006 https://www.cia.gov/cia/publications/factbook/index.html

Clarke, Furnell, Rodwell, Reynolds, 2002 – "Acceptance of subscriber authentication methods for mobile telephony devices", Computers & Security

Etrust, 2006- Mobile Workforce Security Survey www.entrust.com/resources/download.cfm/22721/Entrust%202006%20Mobile%20Workforce%20Security%20Survey.pdf

Frost, 2006 – Frost & Sulivan, mobile office report 2004 www.frost.com

GSMworld, 2006 http://www.gsmworld.com/technology/glossary.shtml

Kaspersky, 2007 http://www.technewsworld.com/story/40124.html

OstermanResearch, 2006 www.ostermanresearch.com

Spryance.inc, 2007 – organizational hierarchy, http://www.spryance.com/aboutus/team.html

Section 2

Information Systems Security

&

Web Technologies and Security

Implementing a Visual Network Management Console

O.C.Agbai and P.S.Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Network management is implemented using a variety of tools. It delivers an automated method of managing network devices and resources. It controls the performance and availability of network services. The aim of this research is to demonstrate that a set of network monitoring tools can be used to show the geographical location of a network problem. It was conducted using the network monitoring tools PolyMon and NetMaCon. PolyMon uses its monitors to monitor different parameters of management information. It generates an alert when a specified threshold is reached and stores the data in the database. NetMaCon uses the stored data to generate a visual display of the location of the network problem.

Keywords

Network monitoring, alerts, notification, network management, trend analysis, PolyMon, NetMaCon

1 Introduction

The potential impact of this research is that it will aid in stabilizing the performance of networks ensuring network availability to users. It will provide an appropriate method of response to network problems. This can be made possible by using a range of network monitoring tools.

The tools used are PolyMon Network Monitor and NetMaCon. A combination of these two tools will be used to monitor a network, generate alerts and respond to the alerts by showing the location of the faulty device on the network. The PolyMon network monitor monitors devices and generates alerts when the monitors fail. These alerts are stored in the PolyMon database. NetMaCon on the other hand interacts with the database to show the visual and geographical location of network problems.

The aim of this research is to implement appropriate network monitoring tools that will display the network problems visually. These tools can be implemented from a single management location on the network. The network monitoring tools should be able to:

- Keep the network alive. Keep-alive tests the connectivity between network components.
- Identify network problems.

- Generate alerts and respond to alerts.

The next section explains the concept of network monitoring and network management followed by an analysis of some network monitoring tool. Section 3 explains the research methodology used. The functionalities of the monitoring tools PolyMon and NetMaCon are described in section 4 while the implementation process is explained in section 5. Section 6 is the conclusion.

2 Network Monitoring and Network Management

Network monitoring is a part of network management that involves accessing and gathering information about networked components (computers, routers and other peripherals) that are being monitored. It also involves generation of alerts when an abnormality is encountered. Network Management on the other hand involves accessing and gathering information, generating alerts and responding to the alert. The response can be either by executing code, shutting down the workstations, rebooting workstations or visual display.

Network monitoring is an automated approach to network management and it consists of three major design areas as suggested by Chiu and Sudama (1992): access to monitored information, design of monitored mechanisms and application of monitored information. In other words, the monitored information needs to be available, a technique for retrieving it should be devised and finally this monitored information should be utilized.

The network information on the system can be accessed in two ways: (Shin et al, 2007) the first is the centralised approach and the other one is the distributed approach. In the centralised approach, the entire network is managed from a single location. This location can be referred to as the management station. A central control is established from here to manage and maintain control over the network configuration, balance and optimise the network resources (Stallings, 1999). The distributed approach involves management from different departmental locations on the network. The control is no longer centralised but distributed across different management stations.

2.1 Network Monitoring Tools

A Network Monitoring Tool examines the functionality of a network and generates alerts when a problem occurs. Network monitoring tools can be classified according to their functionality. Some monitoring tools are designed to monitor based on the performance of the system while others monitor the security of the network, the configuration or the fault. Thus, the choice of network monitoring software solely depends on the reasons for monitoring. The tools can be grouped into:

- Application & Host Based Monitoring Tools
- Flow Monitoring Tools

- Packet Capturing Tools
- Bandwidth Analysis Tools
- Wireless Network Monitoring Tools
- Integrated SNMP Platform Tools

(Moceri, 2006; Keshav, 2006)

2.2 Analysis of Existing Network Monitoring Tools

There are numerous network monitoring tools available with varying features and functionalities. Their unique features however render them inflexible to satisfy the various aims of network monitoring. For instance, a packet capturing tool may not be able to generate alerts. A few monitoring tools are discussed briefly in order to establish their uniqueness, various functionalities and limitations.

PIKT

Problem **I**nformant/**K**iller **T**ool is an open-source Unix/Linux based network monitoring and configuration tool. It is used to manage networks and to configure systems security. PIKT has the ability to report faults and fix them, by killing idle user sessions and monitoring user activities. It uses command line and not a GUI (Graphical User Interface).

FLAME

Flexible **L**ight-weighted **A**ctive **M**easurement **E**nvironment is a Linux based network monitoring tool used for performance and security. FLAME is flexible in the sense that it is possible for users to inject codes that handle packets and get the information that is needed.

SysUpTime

SysUpTime checks for failure and it has automated monitoring capabilities which supports network performance and availability. Failure detection triggers an alert signal either by running a script, sound, email, rebooting, restarting, executing Windows commands, or by posting a web site. It displays graphically and has a map editing function which allows the administrator to add or remove components from the network.

In summary, PIKT and FLAME are both Linux based tools while FLAME is a commercial product. PIKT uses a command line execution which is not graphically interactive but it is capable of reporting faults. SysUpTime on the other hand works on Windows and Linux but it is however not freely available. It is capable of generating notifications and responding to them. It also has a graphical user interface.

The next section will explain the research methods used to discover and develop the tools used in this implementation.

3 Methodology

3.1 Investigation

This research began with investigation to find academic information and documents related to the network monitoring and network management. It was important to find out how network monitoring can be implemented from a single location. This led to further investigation to discover management or monitoring tools.

The next stage of the investigation involved finding the appropriate network monitoring tool to implement. The features of this tool should be able to assist in achieving the objectives of this research. Numerous monitoring tools were discovered in the process as well as the discovery of PolyMon network monitor.

3.2 Software Development and Rapid Application Development (RAD)

The decision to develop a software was considered in order to support the functions of the network monitoring tool PolyMon. This software is intended to be used to give a graphical representation of the networked components. It should make it easier for the network administrator to access information about the network while being monitored in real-time.

Rapid Application Development is a development process that is used to generate software quickly. It adjusts the System Development Life Cycle (SDLC) and reduces development time by using recommended tools and techniques to speed up the analysis, design and implementation steps. Visual Basic 6 programming language can be used to achieve RAD and thus, was used for developing the software NetMaCon.

4 The monitoring software: PolyMon and NetMaCon

PolyMon is an open-source Windows based network monitoring tool. It has three (3) main components: SQL Server Database or the PolyMon Database, PolyMon Executive and PolyMon Manager. The PolyMon Database stores information about the *monitors* and monitored stations. The PolyMon Executive operates in the background by running the *monitors* periodically and storing the results in the database. The PolyMon Manager on the other hand is the Windows-based GUI interface where the settings are organised. The monitors are also defined from this interface. The *monitors* in PolyMon refer to the plug-ins that the software uses in monitoring. For example: the Ping Monitor and TCP Port Monitor.

NetMaCon is a visual basic application which communicates with the information stored in the PolyMon Database to present the visual and geographical location of

the monitored network and of alert notifications. This alert can be viewed on a Virtual Earth Map when problems occur showing the area where the fault has occurred. NetMaCon uses the Virtual Earth Map to display a 3-dimensional view some buildings in the University of Plymouth. This map is interactive and responds to click events to display a view of the floors in each building. The click events also reveal the internal network of each floor. The networked devices like the computers and the connecting routers are display. This map responds also to the entries retrieved from the database to display a red sign beside the building whose network has been detected to have a problem.

Both monitoring tools used for this research were chosen because they: work on the Windows Operating System, are freely available (Open – Source Software & developed), have an interactive Graphical User Interface (GUI), monitor in Real-Time and generate alerts and alert responses. Real-time monitoring is the ability to monitor network traffic at the exact time the network traffic is being transmitted. This feature is very important when monitoring a network for network administrators to receive the exact traffic being monitored at the time. It will enable the quick analysis of traffic and rapid responses to faults. The Windows Operating system was chosen against the Linux operating system because Windows being a Microsoft product is the largest operating system used worldwide and is more compatible with other software. Microsoft provides security patches for their products more than any other operating system, therefore, it is considered to be a more secure operating system to use.

PolyMon network monitor was chosen because of its ability to log all information and setting of its monitors in the database. NetMaCon serves as a medium that extracts this information from the database and presents them visually. Due to the lack of funding and resources the open-source tool PolyMon has been chosen coupled with the developing software NetMaCon which also costs nothing to implement. How both tools work together is explained in the Implementation stage.

5 Implementation of PolyMon and NetMaCon

5.1 Structure of this Centralised Management System:

This section will be used to show how the tools PolyMon and NetMaCon will be used to achieve the objectives of this research. The figure 1 below is being used to illustrate the network used for this implementation. The devices being used are two computers named COMPT 1 and COMPT 2 and a router named GATEWAY.

The network management station: is a station on network from which the management activities are performed. In this implementation, the management station is COMPT1 and it comprises of a *manager* (that is the PolyMon Executive) and *Management Information Base (MIB)* or Database (that is PolyMon Database).

The managed device on the other hand is the device which is being monitored by the management station. These devices include hosts and routers. In this case, the

managed devices are COMPT 2 and GATEWAY. In conventional Network Management Systems, a managed station will usually have an agent and a MIB, but in this case, because of the nature of the monitoring tool PolyMon, the managed devices are agent-less, thus, they do not have agents and MIBs. Rather, the management station gathers and stores the management information. This information is obtained by the *manager* in the management station by "polling" the managed devices. Polling is a request-response interaction between a managed device and the management station (Stallings, 1999).

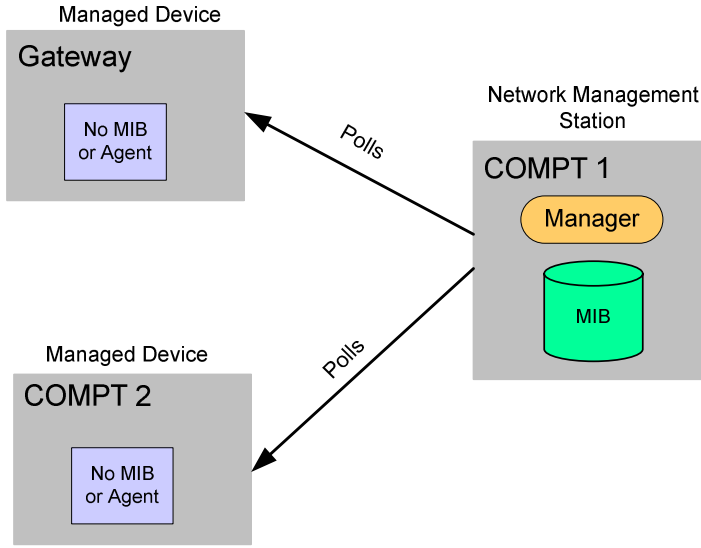


Figure 1: The Management System

PolyMon accesses the monitored information from the managed device using its Monitors. The Monitors controlled by the PolyMon Executive are design to make poll requests from the monitored stations. The poll requests retrieve monitored information from the monitored devices and stores them in the PolyMon database. The monitored information that generates problem notifications is used by NetMaCon to show visually where and when a problem has occurred.

5.2 Implementation Steps:

For the implementation the following are the required hardware and software.

- Processor: 133-MHz (recommended 550-MHz)
- Memory: 128MB of RAM
- Hard Disk: More than 2.9 GB
- Display: VGA that supports console redirection; higher resolution monitor
- Software:

- Microsoft Windows XP operating system (or Windows Server 2000/2003)
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2000 Developer Edition

The first step is to open NetMaCon and run PolyMon to define the PolyMon Monitors. PolyMon can be opened from within NetMaCon (see Figure 2). This implementation will use PolyMon's Ping Monitor to illustrate how the system works. The Ping Monitor works just like the command line tool *ping*. It sends ICMP (Internet Control Message Protocol) echo requests to the devices on the network. The managed devices should respond to this by sending an echo reply. This confirms the connectivity of the network devices. The Ping Monitor is configured for each device on the network (COMPT2 and GATEWAY). After the configuration, the status of the monitor is tested. This is to confirm that the monitor works properly. The test will return either an **OK** or a **FAIL** indication. The information about the configured monitors is stored in the database. As the PolyMon Executive run these monitors, and OK is stored against the monitor when it works well while a FAIL is stored when the monitor fails. In this example it will mean that the device did not respond to the Ping request.

The PolyMon interface is minimised but it continues to run in background. From the NetMaCon Window, the **Start Reporting** button (see figure 2) triggers the connection to the PolyMon Database. As the PolyMon Ping monitors run, NetMaCon checks the status of the monitors. When FAIL is detected from the database, the background of the affected device changes to RED. This signifies that the device has failed to respond. The device's background turns green when the monitor status is OK.

NetMaCon will show a red alert on the Map against the building whose network has been affected to notify the administrator visually. This signal is shown when NetMaCon receives twenty (20) consecutive FAIL records from the database. Figure 2 gives an illustration of how the alert is being displayed. It shows a red sign near the Babbage building on the map, one on the affect floor labelled "Fault!!!" and then on the background of the two computers on the network. The red alert on the Map directs the administrator to the source of the problem.

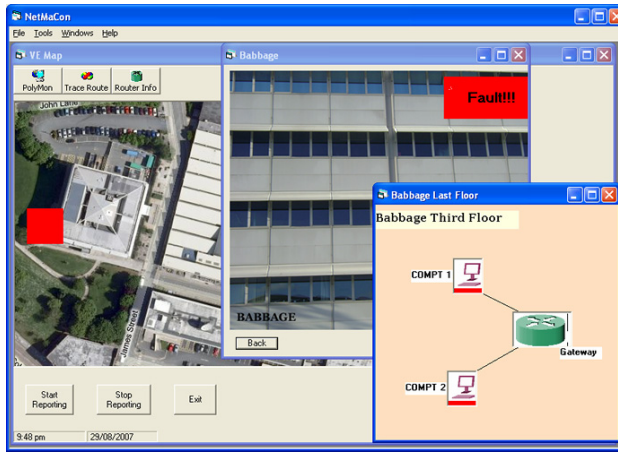


Figure 2: NetMaCon Interface

5.3 Trend Analysis

PolyMon is capable of providing historical trend analysis based on the activities of the monitors. The statistics can be used in the future to prevent the reoccurrence of such faults and failures. Figure 3 below shows the historical analysis of the Ping Monitor for COMPT 1.

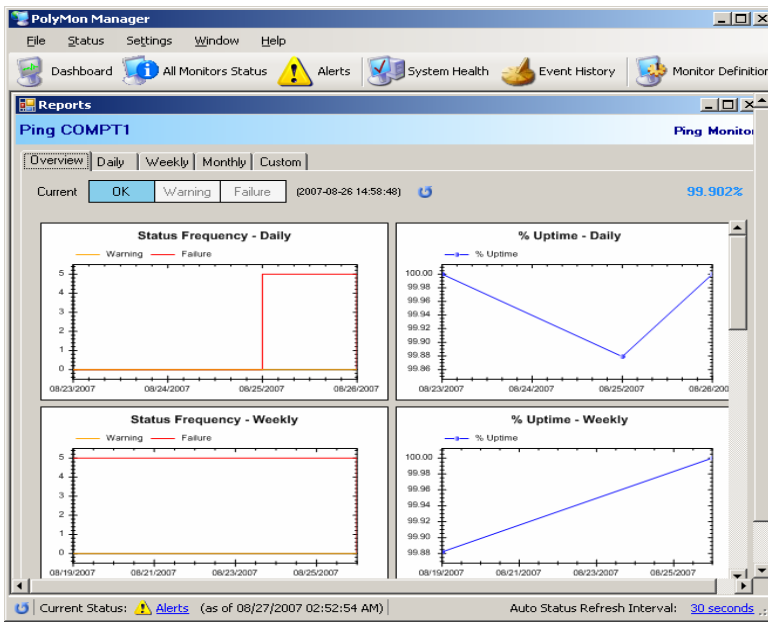


Figure 3: Historical Analysis of Ping Monitor for COMPT 1

The figure shows an overview of the frequency of the monitor's daily and weekly status. The daily status shows that the monitor failed between 23rd and 25th of August. From the 25th, there is a rise in the performance of the monitor. The weekly summary shows that the monitor has been working the whole week from the 8th to the 25th of August. The daily percentage uptime shows that the monitor's highest points were the 23rd and 26th of August with 100% uptime, while the lowest point was on the 25th with percentage of 99.88%. The weekly summary shows a continuous rise in the uptime of the monitor. Such information can be used for future references about the performance of the device.

6 Conclusion

6.1 Evaluation

The implementation above demonstrates how PolyMon and NetMaCon attempt to help achieve the objectives of this research. It has been used to keep the network alive using the Ping Monitor which tests the connectivity of network devices. Thus, the tools can be used to effectively identify network problems. However, they have some inadequacies. Firstly, these tools cannot populate the network devices by themselves. Thus, installing new devices to the network will mean manually changing the static networks presented. Secondly, each monitor in PolyMon needs to be configured for individual devices. The configuration stage can therefore be a tedious task.

It is recommended that in future research, a tool that populates the network devices is used to complement the ability of visually displaying notification alerts. This will enhance the functionality of the system. In addition, the visual display of the actual network can also be enhanced when this feature is incorporated. In 3D, the physical location of a faulty network device can be discovered.

6.2 Summary

In summary, network monitoring is a part of network management that uses network monitoring tools to gather information about networked components. Implementing monitoring tools can be done from a single centralized location on the network. The type of monitoring tool used depends on the reasons for monitoring the network. The Windows-based tools used for this implementation are PolyMon and NetMaCon. The conjunction of both tools has provided an effective interactive GUI tool that monitors the network for problems and generates visual notifications. The tools are used effectively to report alerts generated when faults occur on a network and can be used to predict device failures.

7 References

Chiu, D. M. and Sudama, R. (1992) *Network Monitoring Explained: design & application,* Ellis Horwood Limited, England, ISBN: 0-13614-710-0.

Keshav, T. (2006) *A Survey of Network Performance Monitoring Tools* [Online], Available: http://www.cs.wustl.edu/~jain/cse567-06/net_perf_monitors1.htm (21/01/07)

Moceri, P. (2006) *SNMP and Beyond: A Survey of Network Performance Monitoring Tools*, http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors2.pdf (15/01/07).

Shin, K. S., Jung, J. H., Cheon, J. Y. and Choi, S. B. (2007) 'Journal of Network and Computer Applications' *Real-time network monitoring scheme based on SNMP for dynamic information*, 30 (1): pp 331-353.

Stallings W. (1999) *SNMP, SNMPV2, SNMPV3, and RMON 1 and 2,* Addison Wesley Longman: Massachusetts, ISBN: 0-20148-534-6.

Security Risks Associated With the Use of Web Browsing, Instant Messaging and File Sharing software

D.Bitsanis and M.Papadaki

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

This research has been conducted in order to associate the security risks of the computers with the use of applications of Web-Browsing, Instant Messaging and File Sharing. The research has been conducted by isolating the traffic that these applications have generated, allowing accurate results. Each type of application has generated isolated traffic for forty hours, leading to a one-hundred-twenty hours of research. The results from this research have indicated that the Web-Browsers are submitted to a large number of attacks while the Instant Messengers and the File sharing applications are much safer since they are only submitted to very few attacks.

Keywords

Security Risks, File Sharing, Instant Messaging, Web-Browsers

1 Introduction

This paper introduces the research which has been conducted in order to reveal the security risks that the Web-Browsers, the Instant Messengers and the File Sharing applications are vulnerable to, when they generate traffic. The security risks of each application are introduced from other authors, which have already conducted their research on this sector. This paper introduces the way that the research has been conducted, including the setup of the network and the applications which have been used. Finally the results of the research and their meaning are explained.

2 Applications Existing Vulnerabilities

The File Sharing applications, the IM (Instant Messengers) and the Web-Browsers are all vulnerable on attacks through the Internet. Some of the attacks are based on the traffic that these applications generate, while others are based on the actions of the user. The experiment was based on the vulnerabilities that the applications are exposed to, because of the traffic that they generate.

2.1 Web-Browsing

Denial of Service

The applications which connect to the Internet are vulnerable to DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks. When an application is submitted to such an attack, it fails to establish connections to other hosts or servers. Web-browsers cannot be submitted to DoS and DDoS attack directly. They can still be submitted to one through a server that provides critical services, such as the server of a web-site, e-mail or a DNS (Domain Name System) (Moseley, 2007). If one of these servers is submitted to a DoS or a DDoS attack, it will also render web-browsers useless since they will not be able to establish a connection with them and use the services that they provide.

Cross Site Scripting / Buffer Overflow

A XSS (Cross Site Scripting) attack occurs when a malicious script is executed in a trusted web-site. A script is composed from a combination of small commands, which are executed immediately upon the loading of a web-page. The attackers can place such scripts in the web-pages through the user input fields, when their size is not restricted, or when some symbols are not forbidden from the users. These scripts can have various functions, such as redirecting the input of the other users to the attacker, or capturing the session ID, that a user uses in order to connect to the web-site, so that the attacker can use it and pretend to be the legitimate user (Moseley, 2007).

Spoofing

A spoofing attack occurs when an attacker uses a fake IP (Internet Protocol) address, in order to pretend to be a legitimate user. The attack is successful when the attacker intercepts the traffic between a user and a server (Moseley, 2007). If that happens, the attacker can capture the messages that the user sends to the server and use them in order to communicate to the server as the legitimate user. Doing so, the attacker bypasses the security of the server and has the access rights that the legitimate user has.

Session Hijacking

A session hijacking is taking place when an attacker takes over control the session ID, of the application that a user uses in order to connect to the Internet with. Having the session ID, the attacker can control the users' application. The ID codes can be captured in different ways. One of them is a brute force attack, where the attacker is using every possible combination of letters, numbers and symbols (Moseley, 2007).

2.2 Instant Messaging

Denial of service

The IMs are also vulnerable to DoS attacks. The IMs can only process a limited number of messages that they accept from the users. A DoS attack can succeed when a large number of messages are sent to a user. Even though some IMs have a function that protects them against such attacks, there are ways to bypass it. The attacker can use many different accounts in order to launch the attack. If the number of messages that the IM is trying to process exceeds the limit, then there is a very high possibility that the IM will crash. In an even worst scenario, the IM will consume a large amount of CPU (Computer Processing Unit) that will cause the whole computer to become unstable and maybe crash. (Hindocha, 2003)

Eavesdropping / Spoofing

An eavesdropping attack occurs when an attacker intercepts the communication between two users. This kind of attack is possible because by default, the communication between two IMs is not encrypted (Piccard, 2003). This means that anyone who is tracking the traffic of the Internet will be able to capture and read the conversation between two users. The attacker knowing the IP (Internet Protocol) address from both the sender and the receiver can redirect the messages to each other and even send fake messages. (Moseley, 2007; Sagar, 2003).

2.3 File Sharing

Denial of service

In order for the File Sharing applications to function properly, they require to establish a connection to a server and then to other hosts over the Internet. On the other hand, the File Sharing application will accept connections from other hosts as well. However the number of connections that the application can establish is set. This feature creates a vulnerability to the File Sharing applications. By trying to establish a large number of connections, an attacker will launch a DoS or DDoS attack. If these attacks succeed, then the application will not operate properly and it may even crash. In an even worst scenario the application will consume a large amount of CPU and will cause the PC (Personal Computer) to become unstable and even crash. (Piccard, 2003)

Reveal of IP / Port

An attacker requires the IP address of a host and the ports that the host has unblocked, in order to launch an attack. Hiding these two pieces of information is enough protection for the user, in order to limit the number of attacks. The File Sharing applications neutralise this protection. When the File Sharing application connects to a server and then to a similar application on the Internet, the IP address of the host as well as the ports that the application is using is revealed on the other end of the communication (FaceTime, 2005; Piccard, 2003). This exposes the computer to attackers which can launch more sophisticated attacks.

3 Research Method

The experiment took place at the NRG (Network Research Group) lab, at the University of Plymouth. The purpose of the experiment was to determine what kind of Internet attacks a PC is exposed to, while using Web-Browsers, IMs and File Sharing applications. Two PCs have been used for the experiment. The First PC, the Host, has been used to generate traffic using the Web-Browsers, the IMs and the File sharing applications. The second PC has been used along with the first as a Firewall, in order to allow only traffic from specific ports to be generated and in order to capture all the traffic the Host has generated. The experiment has lasted for one-hundred-twenty hours in total. Forty hours have been spent on Web-Browsers, forty hours on IMs and forty hours on File Sharing applications. The duration of the experiment has been selected according to the number of hours that an average user connects to the Internet for, based on different authors and statistics (ComScore, 2007; JCMC, 2002 and Oxford, 2006).

3.1 Network Setup

The Host and the Firewall have formed a network. The Host was located to the Intranet (Internal Network) of the network which was formed for the experiment. In order to connect to the Internet (External Network), the Host first had to go through the Firewall and then if the rules allowed it, it would connect to the Internet. The Firewall was placed between the Internet and the Intranet. It was the PC which was providing to the Host, access to the Internet. Also the Firewall had the rules which allowed the traffic from all the ports to be allowed or denied. The final function of the Firewall was to capture all the packages which went through it, whether they were headed from the Intranet to the Internet or from the Internet to the Intranet.

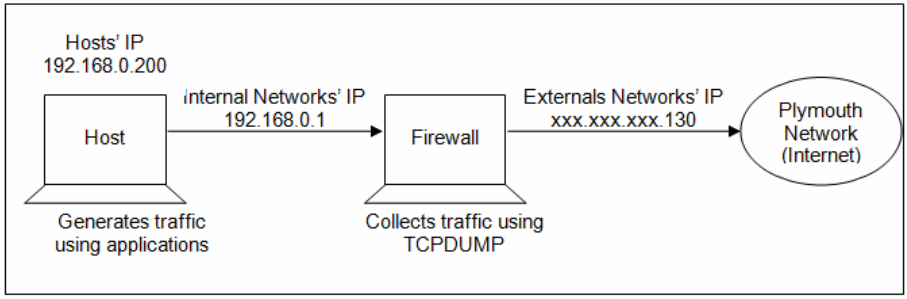


Figure 1: Experiments' Setup

The local IP of the Host, within the Intranet, was 192.168.0.200. However this has not been the IP that appeared in the Hosts' packages. When the packages were going to the Firewall, in order to be redirected to the Internet, the Firewall was changing the source IP, from the local IP of the Host, to the external IP address of the network. The external IP address was replaced with xxx.xxx.xxx.130 for security reasons. When a server was receiving the package, or when an attacker was encountering the

package, the IP which would appear on the package was the external IP of the network (Figure 1).

3.2 Hardware

The hardware that the host has been consisted of was a processor 'Intel Pentium III' in 701 MHz (Megahertz) and 256 MB (Megabyte) RAM (Random Access Memory). The Host had one network card installed, which was using in order to connect to the Firewall.

The firewall had a bit stronger hardware than the host, since it had more demanding applications installed and it would be used for more demanding processes. Its' processor was an Intel Pentium III in 800 MHz. The RAM was 190. The Firewall had two network cards installed. One card was used to connect the Firewall with the Host, and create the Intranet. The other network card was used to connect the Firewall, and the Host through it, to the Internet.

3.3 Software

Web-Browser

Two Web-Browsers have been selected for the experiment. The first one was Microsofts' Internet Explorer and the second was the open source software, Mozilla Firefox. Both of these applications, had been selected as the most popular web-browsers that users prefer to use, according to the statistics that the web-site W3Schools (2007) has released. The Web-Browsers establish connections to other servers that provide web-sites through port 80, while they use other ports in order to connect to other services. Port 443 which has been used in the research is used for the e-mail service of the University of Plymouth (Table 1).

Application	Direction	Port No	Protocol	Action
Web-browser	Host->Firewall	80	HTTP	Allow
e-mail	Host->Firewall	443	HTTPS	Allow
General	Host->Firewall	All	All	Deny

Table 1: Rules setup for Web-Browsers

Instant Messenger

MSN has been the first application selected for the experiment for the IMs. MSN is Microsofts' messenger. MSN had been selected because according to the web-site FreebieList.com (2007), MSN is one of the most popular web-browsers of the Internet therefore it is probably targeted by attackers more often than other messengers. The main port that the MSN uses in order to connect to the server is

1863, using the TCP protocol. In order for two users to communicate, their communication goes through the server, and the server redirects the messages to the users (Hindocha and Chien, 2003) (Table 2).

Yahoo! Messenger has been the second application for the IMs. Yahoo! Messenger was also one of the most popular messengers according to FreebieList.com (2007). The ports that Yahoo! Messenger uses are 5000 using the TCP protocol for the voice chat, and port 5050 using the TCP protocol for the chat messages. The user connects to the server in order to register in the network. While it is connected to the server, the users' messages go through the server first and then are redirected to the contact (Hindocha and Chien, 2003) (Table 2).

Application	Direction	Port No	Protocol	Action
MSN	Host->Firewall	1863	TCP	Allow
Yahoo!	Host->Firewall	5050	TCP	Allow
Yahoo!	Host->Firewall	5000	TCP	Allow
General	Host->Firewall	All	All	Deny

Table 2: Rules setup for IM

File Sharing

eMule had been selected to represent the File Sharing applications. In eMule, the application first connects to server through a port that the server has specified. Usually each server has different ports, which will accept connections from. While in the server, the user can search for a file, by providing a name for the file. The server then provides a list of files, according to the word that the user provided. When the user selects the file/s to download, the server provides directly to the eMule application, the IP addresses of the hosts over the Internet which have and share the selected file/s. The eMule then connects to all the PCs directly, not through the server, and starts downloading the file/s.

Application	Direction	Port No	Protocol	Action
eMule	Firewall->Host	12679	TCP	Allow
eMule	Firewall->Host	12689	UDP	Allow
eMule	Host->Firewall	4242	TCP	Allow
General	Host->Firewall	All	All	Deny

Table 3: Rules setup for P2P

However in eMule, the user has to specify the ports from which the traffic will go through. A port has to be set for TCP (Transmission Control Protocol) and a port for UDP (User Datagram Protocol). eMule will communicate with other applications, sending the traffic through these ports. However the application at the other end might not have the same ports open. In this case eMule will redirect the traffic towards that application from another port, matching the applications open port (Table 3). During the experiment though, the firewall was setup to allow traffic from specific ports only. Because of this configuration, only a few other applications have been able to connect to the Host. It is not certain whether this has affected the results or not.

4 Results

4.1 Web-Browsers

Analysing the captured traffic from the Web-Browsers, has revealed one alert of 'MS-SQL Worm propagation attempt', one alert of 'MS-SQL Worm propagation attempt OUTBOUND', one alert of 'MS-SQL version overflow attempt', three alerts of 'DNS SPOOF query response with TTL of 1 min. and no authority', two alerts of 'ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited', three alerts of WEB-CLIENT Adobe Photoshop PNG file handling stack buffer overflow attempt, forty-five alerts of 'ATTACK-RESPONSES 403 Forbidden' and one-hundred-fifty-six (156) alerts of 'ATTACK-RESPONSES Invalid URL'.

4.2 Instant Messengers

After analysing the captured traffic from the IMs, the following alerts have been revealed. Eight alerts of 'MS-SQL Worm propagation attempt', eight alerts of 'MS-SQL Worm propagation attempt OUTBOUND', eight alerts of 'MS-SQL version overflow attempt' and three alerts of 'ICMP redirect host'.

4.3 File Sharing

Analysing the traffic generated by File Sharing applications has revealed twelve alerts of 'MS-SQL Worm propagation attempt', twelve alerts of 'MS-SQL Worm propagation attempt OUTBOUND', twelve alerts of 'MS-SQL version overflow attempt' and one alert of '(portscan) TCP portscan'.

5 Discussion

Web-Browsers

The analysis of the Web-Browsers' traffic has revealed that these applications are vulnerable to a variety of attacks. Within the forty hours of experiment, the Web-Browsers have accepted attacks of DoS, Cross Site Scripting/Buffer Overflow and

Spoofing. The MS-SQL related alerts that have been detected are not based on the traffic that the applications have generated, rather they are based on the random selection of an IP address by the 'Slammer' worm (CAIDA, nodate)

The users need to be very careful when they are using Web-Browsers because there are a lot of ways for an attacker to compromise their PCs and steal private information about or from them. Many of the attacks are easy to launch, especially because of the variety of tools that are freely available and from the fact that anyone from any place of the world can setup a fake server and use it for attacks. Most importantly the Web-Browsers are vulnerable to attacks which are not visible by the users hence there is no way to protect themselves from them.

Instant Messengers

The IMs have only accepted an eavesdropping/spoofing attack. The MS-SQL related alerts have not been generated by the traffic that the IMs have generated. The IMs are submitted to a low number of attacks because they communicate to other IM indirectly through the server, hence it becomes hard to detect and launch an attack on the traffic they generate.

According to the results of the experiment, the users have few reasons to be afraid of the attacks that are based on the traffic that the IM applications generate. What they need to be careful of is adding new users to their buddy list, and accepting files even when they are sent from contacts of the buddy list.

File Sharing

The File Sharing application has only been submitted to a portscan attack, which is based on the reveal of the IP/ports. Despite the fact that the reveal of such information should have increased the number of attacks, there has only been one alert of this kind. The MS-SQL related alerts have not been generated by the traffic that the application has generated.

According to the analysis of the results, the users who use File Sharing applications are not potential victims of an attack. The attackers do not appear to be interested on hosts which use such applications. There is a possibility that the outcome of the File Sharing applications has been affected by the fact that only a few ports have been opened, hence the application has established connections with a few other applications and has not generated enough traffic.

6 Conclusion

This paper has introduced the vulnerabilities that the users are exposed to when they are using applications of Web-Browsing, Instant Messaging and File Sharing. The results have revealed that the average users do not accept many attacks while using Peer-to-Peer and Instant Messaging applications. However the number of attacks and the level of aggressiveness are increased while they are using Web-Browsers. The

data have been collected by isolating the traffic of the network, allowing only traffic by these applications to be generated. Any future work to improve the quality of the research would be to use more applications from each type, in order to increase the chances of an attacker detecting their traffic. Also adding more files to File Sharing applications could help. A last suggestion would be to allow the applications to generate traffic for more time than the time which had been allowed in this experiment.

7 References

CAIDA (nodate) "The Spread of the Sapphire/Slammer Worm" http://www.caida.org/publications/papers/2003/sapphire/sapphire.html (date accessed: 24/08/07)

ComScore (2007) "Press Release" http://www.comscore.com/press/release.asp?press=849 (date accessed: 06/04/2007)

FaceTime (2005) "Real-time Security for the Real-time Enterprise" http://www.spywareguide.com/whitepapers/wp_rtg500.pdf (date accessed: 29/11/2006)

FreebieList.com (2007) "Free Chat Programs and Chat Freeware Tools" http://www.freebielist.com/chatprograms.htm (date accessed: 01/06/2007)

Hindocha N. (2003) "Threats to Instant Messaging" http://www.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf (date accessed: 29/11/2006)

Hindocha N. and Chien E. (2003) "Malicious Threats and Vulnerabilities in Instant Messaging" http://www.symantec.com/avcenter/reference/malicious.threats.instant.messaging.pdf (date accessed: 29/11/2006)

JCMC – Jounral of Computer-Mediated Communication (2002) "User Behaviour and the 'Globalness' of Internet: From the Taiwan Users' Perspective" http://jcmc.indiana.edu/vol7/issue2/taiwan.html (date accessed: 06/04/2007)

Moseley R. (2007) "Developing Web Applications" John Wiley & Son, Ltd, Middlesex University, ISBN-13: 978-0-470-01719

Oxford University (2006) "Entwined in the network of networks" http://www.ox.ac.uk/publicaffairs/pubs/annualreview/ar05/02.shtml (date accessed: 06/04/2007)

Piccard P. (2003) "Risk exposure: Instant messaging and Peer-to-Peer Networks" documents.iss.net/whitepapers/X-Force_P2P.pdf (date accessed: 29/11/2006)

Sagar A. and Chakrabarty S. (2003) "Common attack methods" http://www.cert-in.org.in/knowledgebase/presentation/Commonattackmethods.pdf (date accessed: 12/03/2007)

W3Schools (2007) "Browser Statistics" http://www.w3schools.com/browsers/browsers_stats.asp (date accessed: 01/06/2007)

Analysis of Wireless Local Area Network Web Based Information

J.W.Elston and A.D.Phippen

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Wireless security education to all types of user form a major part in the implementation of secure WLAN networks. Lack of education is a barrier to security and many users like to obtain security information from the Internet / Web using major search engines such as Yahoo! and Google. This paper provides an original evaluation of WLAN security information found on the major search engines. The findings are that there are many good sources of WLAN security information available if the correct search is performed. Users should look out for signs of poor information and poor website quality.

Keywords

Wireless, Local, Area, Network, WLAN, Web, Security, Education, Information

1 Introduction

There have been many issues with the security of wireless networks, the user education of such technologies, current product availability, current developments, and the effective implementation of secure networks.

The knowledge and education play a vital role. Not surprisingly, the Internet is regarded as a prime source of direct information for network security. It is very simple and efficient for a network installer / administrator to use a popular search engine to retrieve practical security information, by entering keywords.

A user may want information on a specific WLAN hardware with instructions for setting up, administration, current industry developments, security information, security standards, or just plain curiosity. A user may want a more predefined education programme or online learning approach.

This information is readily available but, just how reliable is this information? Is the information suitable, correct, relevant and accurate? How useful are the Internet resources for someone who wants to find out about WLAN and security? Are the

sources biased? Are there any costs involved? Is the information clearly presented? Is the website easy to use? These factors need to be considered.

The overall quality of a website may be very good in terms of presentation and information content. However there are some cases where information might be uniformed, inaccurate and biased. The information might be quite low in volume, and not that useful. So this poses the question, just how good are the online resources for WLAN?

This paper is intended to propose an evaluation methodology and a summary of assessment of WLAN information websites, found from popular search engines. It is intended that the paper provide a starting point of the current state of WLAN security information on the web, that has not been widely and critically evaluated as of yet.

2 Evaluation Method

The main data collection medium was the Internet and fifty websites were evaluated. This number was decided due to the fact a user is unlikely to go beyond the first few search pages and only take the top few. A factor of user convenience was considered.

The two most popular Internet search engines were used to locate the web pages, these being Google (www.google.com) and Yahoo (www.yahoo.co.uk). The keywords entered in the search were, wlan security information, as the primary term.

Yahoo was the first search engine used with the websites given a number from 1 to 25 in order of their occurrence on the search engine. Google was used second and any repeating websites / pages will be ignored. They were given a number of 26 to 50, in order of precedence.

Websites containing WLAN information were assessed by the following criteria.

a) Information Quality

This table concerns the quality of the information provided in terms of the text and the information contained within. The table contains the following fields where a mark out of ten is given for each one.

- Authority – Does the work have a visible, qualified author with relevant credentials?
- Objectivity – Does the work have a clear objective?
- Authenticity – Where does the work originate? Is it authentic?
- Reliability – Is the information source trustworthy with evidence?
- Timeliness – Are the information and links up to date and current within the existing field?
- Relevance – Is the work is sufficient depth? Is the work usable and readable?

- Efficiency – Is the information well organised?

Total – The total mark of all information quality criteria. This is an overall mark out of 70 and gave an overall picture of the website's information quality.

b) Presentation

This table relates to the purely visual aspect of a website or webpage. It asks a range of usability and visual questions. Is a website pleasing and self-explanatory to a user?

- Search – Was the webpage / site easy to search with little effort?
- Navigation – Is the webpage / site easy to navigate around?
- Clarity – Is the webpage / site clearly presented and straightforward to understand?
- Style – Is the webpage style relevant and effective? Is the style pleasing on the eye?
- Colour Scheme – Is the colour scheme pleasant and easy to see? Do the colours clash?

Total – The total presentation criteria mark out of 50. This provided an overall figure for the presentation of the site.

A mark for each criterion, for each site was awarded the following banding was decided:

0 – Not useful at all or non existent. This is awarded when virtually no useful content or feature(s) are provided. This is of no usefulness to a potential end user.
1-3 Poor usefulness. This mark is given when a criterion presents very low, poor feature standard. This is of little usefulness to a user.
4-5 Some usefulness. The criterion is satisfied, providing some usefulness to a user.
6-7 Good usefulness. The criterion is assessed as being good usefulness to a user, with substantial evidence to back it up.
8-10 Excellent usefulness. The criterion is assessed as being excellent usefulness to a user, with substantial evidence to back it up.

It was agreed to have a second maker in order to provide a fairer mark and offer a second opinion. Each criterion was assessed on a rating of 0-10. With 0 being extremely poor, and 10 being excellent.

Each website was given a type classification number:
1. Retail Websites – Sites that sell products direct to a customer.
2. Company Product Websites – Sites detailing company product details.
3. Technical Information Websites – Sites aimed at providing a user with technical information, industry developments, technical news or useful information.
4. Help Websites – Websites with questions, answers, forums and trouble shooting websites. There has to be an element of interaction with the intention to help an end user specifically solve a problem.

5. User Websites – These are websites set up by individual users or groups of users from a non-corporate / profit making background with the intention of providing information to fellow users.
6. Academic Websites – This are websites provided from established, genuine educational establishments. They should provide some from of real world technical information.
7. Online Magazine / Subscription Websites – Online magazines or sites that require some form of subscription fee in order to access the information.
8. Other – These are websites that cannot be clearly classified in the above categories.

It was hoped that the classification and assessment scheme presented an adequate assessment method. It should be noted this was solely based on the evaluators' perceptions. The solid classification provided should also give a good picture of the type of information provider that is widely available.

3 Summary of Results

The following section provides a summary of the results found during the research and the key findings. Figure 1, shows the average criteria marks for the information quality. The precise marks were as follows: Authority – 5.76, Objectivity – 6.04, Authenticity – 6.76, Reliability – 6.48, Timeliness – 6.5, Relevance – 6.4 and Efficiency – 6.88. All criteria, apart from authority, on average produced a good level of usefulness and fell in good usefulness banding. The Authority criterion was on average 5.76 denoting some usefulness.

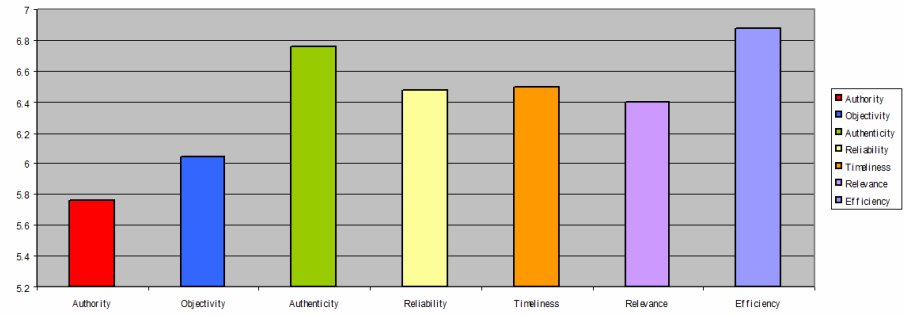


Figure 1: All Data Mean Information Criteria Marks

Figure 2, is a pie chart that presents the results in terms of the proportion of sites in a particular range. As can be seen, the 40 to 49 range were the most common aggregate marks. The average overall Information Quality mark was 44.82 or 64%. This denotes that on average the websites were awarded a good level of information quality. The frequency occurrence of the results were: Less than 10 – 3, 10 to 19 – 0, 20 to 29 – 1, 30 to 39 – 8, 40 to 49 - 20, 50 to 59 – 12, 60 to 70 – 6. Expressed in

percentages: Less than 10 – 6%, 10 – 19 – 0%, 20 to 29 – 2%, 30 to 39 – 16%, 40 to 49 – 40%, 50 to 59 – 24%, 60 to 70 – 12%

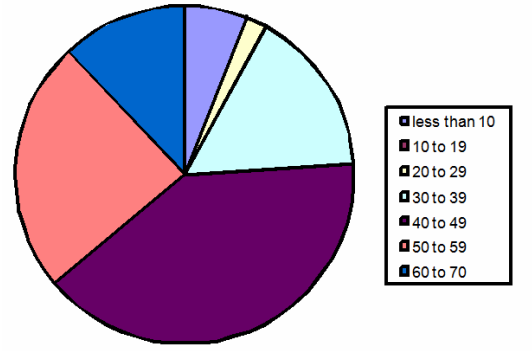


Figure 2: Pie Chart Breakdown of All Information Quality Overall Marks

Figure 3, summarises the mean Presentation Criteria results for all data in a bar chart. The precise results were as follows: Search – 5.72, Navigation – 7.42, Clarity – 7.4, Style – 7.2, and Colour Scheme – 7.14. All presentation criteria were awarded a good level of usefulness / quality on average, apart from the criterion Search which was awarded some usefulness on average. However at 5.72 this was very close to being of good usefulness. Figure 4 is a pie chart that presents the results in terms of the proportion of sites in a particular range. As can be seen, the 30 to 39 range were the most common aggregate marks, with an occurrence of 25 sites in that band. The average overall Presentation mark for all the data was 34.88 or 69.76%. This indicates that the presentation marks awarded were good, bordering on excellent. The frequencies of the overall presentation results are as follows: Less than 10 – 0, 10 to 19 – 2, 20 to 29 – 6, 30 to 39 – 25, 40 to 50 – 17. Expressed as percentages: Less than 10 – 0%, 10 to 19 – 4%, 20 to 29 – 12%, 30 to 39 – 50%, 40 to 50 – 34%.

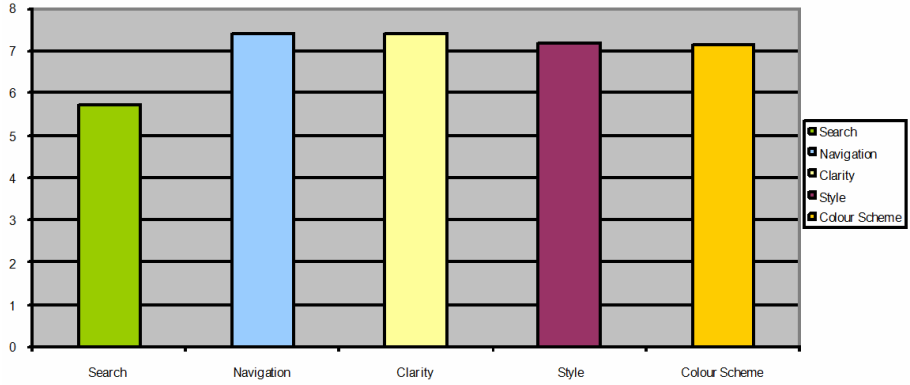


Figure 3: All Mean Presentation Criteria Marks

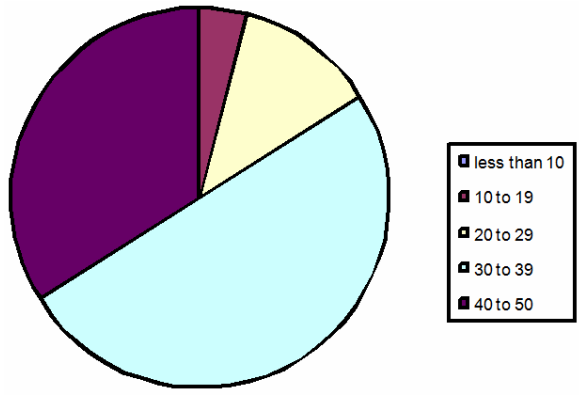


Figure 4: Pie Chart Breakdown of All Presentation Overall Marks

4 Method Effectiveness

To summarise the evaluation method had the following effective points:

- Easy to implement
- Easy to understand
- Breakdown to Information Quality and Presentation
- Tables defined by evaluation criteria
- Marks out of 10 and an aggregate mark
- Comparative
- Adaptable
- Real world type model

The method could be improved by:

- More time to gather data
- Larger volume of website data
- Many markers / evaluators
- User feedback
- Specific modification of evaluation criteria according to information analysed
- Derived information metrics (e.g. number of pieces of useful information per page)
- Derived presentation metrics

5 Conclusions

At present the main search engines (Google and Yahoo) provide an excellent source of high quality WLAN security information. The search engines are easy to use and

only require a few keywords and a click to produce a results page. A user does not necessarily have to go beyond the first few pages for generic WLAN information.

There are many useful URLs that cover topic areas such as general information to more specialised information. Much is dependant upon what the user is looking for. Some websites / pages are of very poor quality; many (especially those first encountered) provided a good-to-excellent source of information.

What makes a good WLAN information site is open to debate, especially the visual aspect of a website. What one person sees as clear another may see as unclear. The project has particularly identified that quite often WLAN information sites are lacking objectivity and in particular authority. In many cases no authors, credentials, or organisations are cited. This may have an impact upon the user's perception of the information and the confidence they hold it in. It is unlikely a user will take note of information they think is unsubstantiated.

User education is a vital weapon to improve security and knowledgeable people can place hardware and software safeguards to protect their WLANs from intruders / attackers / eavesdroppers. If a user is ignorant of issues it is unlikely they will be addressed, perhaps compromising the WLAN security. While some websites have been evaluated as being of good quality their effects on large numbers of WLAN users remains to be seen.

A method for WLAN security information evaluation has been presented in this paper. Ultimately it's usefulness depends on the accessibility, accuracy, correctness, application potential, understandably and information conveyance to the end user. Websites can also change frequently in terms of content and visual style

6 References

Bahli, B., Benslimane, Y. (2004) 'An exploration of wireless computing risks: Development of a risk taxonomy', Information Management and Computer Security, 12(3): 245-254

Beck, S. (2006) The Good, The Bad & The Ugly: or, Why It's a Good Idea to Evaluate Web Sources, http://lib.nmsu.edu/instruction/evalcrit.html (Accessed July 2006)

Bergström, L., Grahn, K., Karlström, K., Pulkkis, G., Åström, P. (2004) 'Teaching Network Security in a Virtual Learning Environment', Journal of Information Technology Education, 3: 189-217

Cohen, F. (1999) 'Managing Network Security: Security Education in the Information Age', Network Security, 1999 (10): 7-10

Cresswell, J. (2003) Research Design Qualitative Quantitative and Mixed Method Approaches Second Edition, Sage, California USA

Evaluating Internet Resources (2006) http://library.albany.edu/internet/evaluate.html (Accessed July 2006)

Evaluating Internet Resources (2006) http://eduscapes.com/tap/topic32.htm (Accessed July 2006)

Google Remains Number One Search Engine (2006) http://findarticles.com/p/articles/mi_m0BNG/is_2005_Sept_26/ai_n15634183 (Accessed July 2006)

Hardy, M. W. (2005) 'Online Learning Concepts, Strategies and Implications: Book Review', Elsevier

McGrath, N. (2004) Spread the Word, http://www.computerweekly.com/Articles/2004/11/09/206552/Spread+the+word.htm (Accessed July 2006)

Noll, C., Wilkins, M. (2002) 'Critical Skills of IS Professionals: A Model for Curriculum Development', Journal of Information Technology Education, 1(3): 143-154

O'Callaghan, J. (2003) 'Implementing wireless communications', Sensor Review, 23(2): 102-108

Potter, B. (2006) 'User education – how valid is it?', Network Security, 2006(4):15-16

Reisslein, J., Seeling, P., Reisslein, M. (2005) 'Integrating emerging topics through online team design in a hybrid communication networks course: Interaction patterns and impact of prior knowledge', Internet and Higher Education, 8: 145-165

Salmon, G. (2002) E-tivities the key to online learning, RoutledgeFalmer, Oxford UK

Steffora, A. (1994) 'User education critical to effective network security', Network Security, 1994(6): 2

Ten C's For Evaluating Internet Sources (2006) http://www.uwec.edu/library/Guides/tencs.html (Accessed July 2006)

When Wireless Works, PC Pro (2006) http://www.pcpro.co.uk/realworld/44895/when-wireless-works/page3.html (Accessed July 2006)

Tracking Botnets

M.Freydefont and M.Papadaki

Network Research Group, University of Plymouth, Plymouth, United Kingdom
email:info@cscan.org

Abstract

Botnets are not only a threat for companies under the pressure of Distributed Denial of Service (DDoS) attacks, but also at the origin of massive information theft, targeting the banking credentials of home-users. It is widely accepted that nowadays, botnets are the most challenging threat available on the Web. This paper is an attempt to study the feasibility of a tracking system which would shut botnets down in an automated fashion. The study is realized with a review of botnets monitoring techniques as well as a trend analysis in bots specifications. The results show that it is not realistic to imagine such automated "botnet-killer" system. Instead, an end-point defense strategy should be applied, putting the accent on educating people and improving the usability of security products.

Keywords

Bot, monitoring, trend analysis, defense

1 Introduction

These last years, malicious activity on the Internet has moved from the hackers community, motivated by technological challenges, to well-structured criminal associations (Ilet, 2005). Distributed Denial of Service (DDoS) attacks, spamming, phishing, information theft ... all these frauds have merged and are now embodied by a single entity: *the botnet*. The latter has become the favourite tool of cyber-criminals and at the same time one of the most challenging threats available on the Internet (Abu Rajab *et al*, 2007). Their distributed nature makes them hard to eradicate. The wide range of services they offer to their controller, moreover, the opportunities to make easy money, contribute to the professionalization of the underground economy. As a result, bots are getting more and more sophisticated, so hard to eliminate.

This paper investigates existing work that has been done to monitor botnets as well as the new trends in botnets specifications. The aim is to recommend areas where the efforts should be focused and propose ways to defend against them.

2 Background

A *bot* is a piece of malware that can perform tasks requested by a remote user. A *botnet* is the name given to a group of computers infected by a bot that enables a third body to perform malicious and distributed activity. The victim hosts are also

sometimes called *zombies*, *slaves* or *drones* and the controller of the botnet, *master* or *herder* (Myers, 2006).

There are three aspects that define bots:

- *Communication:* how the bot interacts with the master and how the bots are linked together. A *Command and Control* (C&C) server is the host where all the slaves connect to wait orders from the herder.
- *Propagation:* the way the botnet gets bigger. This includes the reconnaissance and the contamination phases.
- *Services:* the actions a bot can undertake and that make it interesting for the cyber-criminal.

At the beginning, IP addresses of C&C servers were hard coded in bot's code (Schonewille et al, 2006). The herders soon realized the obvious limitations of such practice: when a C&C server is taken down, all the clients are simply lost. They fixed this problem replacing the IP addresses by dynamic domain names (Schonewille et al, 2006): a domain name associated with an IP address that can be changed. This provides a great flexibility in the sense that when a C&C server is shut down, the herder just has to relink the domain name with the IP address of the new server for displacing all the zombies to their new headquarters.

IRC is an old protocol for text-based conference (Kalt, 2000a). It allows users to connect to a server and join a chat-room called *channel*. Hackers have found an application of this protocol to botnets. The slaves and the master meet up in a channel hosted by a server (the C&C server) where they can receive the commands sent by the master. IRC is considered as the legacy protocol for botnets (Myers, 2006).

3 Monitoring botnets

Reseachers have studied different approaches to monitor botnets, both from the inside, infiltrating the botnet or from the outside, analyzing visible traffic.

3.1 Honeynets

The honeynets enable researchers to gather information about botnets (Honeynet Project, 2006). However, they have two main drawbacks:

- Honeynets only enable local observation, it is not possible to get a broad view of the entire botnet. In an IRC botnet for instance, all the members are not always visible, due to IRC server options, RFC 2811 (Kalt, 2000b).
- Honeynets doesn't not allow to choose which botnet to monitor as the researcher has to wait to capture malware first.

A comparison of the DDoS attacks detected by incident reports (Peakflow SP statistic system) and honeynets (ShadowServer Foundation) showed that 13% of the attacks were detected by Peakflow against 2% for ShadowServer (Nazario, 2007). This demonstrates that botnet can not be tracked efficiently *only* using honeynets, a more global approach is required.

3.2 DNS Traffic analysis

In their paper entitled *"DNS as an IDS"* , Schonewille et al (2006) studied the potential of DNS servers for acting as detection systems. The hypothesis is the following: infected systems sometimes give information about themselves when making DNS queries. Information about the infection and the source may be extracted with analysis of those queries. The researchers of this study drew the conclusion that the DNS traffic analysis is limited is terms of botnet detection capacity, mainly due to the false positives raised. Also the analysis of the data is highly cpu-intensive and the cache on the client obscurates the real activity.

Another interesting study concerning DNS monitoring has been made, this time in the context of spamming botnets *"Revealing Botnet Membership Using DNSBL Counter-Intelligence"* (Dagon et al, 2006). DNSBL (DNS Black List) databases are normally used by regular mail servers (mail transport agent) to reject or flag spam messages (Wikipedia, 2007a). Nevertheless, they are also used by botmasters who perform lookups to check whether their spamming bots are blacklisted or not. Indeed, to rent a botnet for spamming purpose, the herder must insure that the bots are "clean"...(Dagon et al, 2006). The researchers used graphical analysis to distinguish legitimate lookups from reconnaissance queries. The origin and targets of suspicious queries are likely to be bots. *"With the ability to distinguish reconnaissance queries from legitimate queries, a DNSBL operator might be able to mitigate spam more effectively."* (Dagon et al., 2006).

3.3 Distributed Detection Systems and Algorithms

In their paper entitled "*A Distributed Host-based Worm Detection System"*, Cheetancheri et al (2006) present a distributed system for detecting large-scale worm attacks using only end-host detectors: End-host detectors monitor the traffic they can see and determine if there is an attack or not. But because of the limited view they have on the traffic, we cannot assume their detection quality is high. Therefore, information from many detectors is correlated and a Likelihood Ratio is then computed (probability that an attack actually occurs). In order to make the collaboration working, a complete protocol has been developed for exchanging the alert messages. It is a completely distributed approach with no single points of failure. Nevertheless, the system, while promising, is not finalized yet as it remains aspects to address. For instance, the system has only been tested using simulations and within a local area network; it does not take in account the worm traffic from outside (Cheetancheri et al, 2006). Moreover, this distributed system only relates to the early step of botnet construction (worms, whether they are mass-mailing or

propagates by exploiting vulnerabilities are the main vector for bot spreading). It is not designed to monitor existing botnets' activity.

Finally a team from the Portland State University in USA has developed an anomaly-based algorithm for detecting IRC-based botnet meshes (Binkley, Singh, 2006).Their system combines an IRC parsing component with a syn-scanner detection system. The algorithm is not signature-based and doesn't rely on any known port number or IRC command string. The system can clearly show the presence of botnets but there are more fuzzy cases where further analysis is necessary to determine whether the activity is actually suspicious or not. The technology employed here relies on attackers launching attacks (scans), therefore, there is no guarantee for every infected system to be detected. Also, one could argue that anomaly detection is "too late" (a host has already been exploited)

4 Trend Analysis

Bots' specifications evolve constantly and it is important to follow them to make sure for instance that the monitoring techniques developed do not become obsolete. This section presents the tendencies in terms of propagation, communication and services.

4.1 Methodology

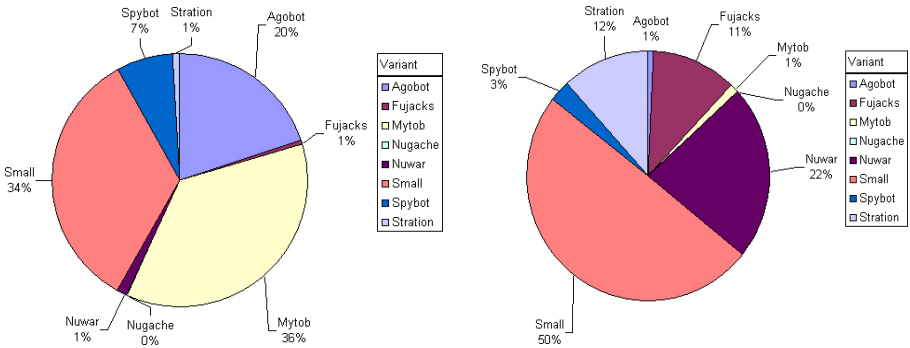
The antivirus vendor Trend Micro provides a comprehensive Virus Encyclopaedia (Trend Micro, 2007a), of malware variants, either caught by sensors or submitted by antivirus users. Trend Micro has been chosen because of the section *Statistics* available for any variant's description. It summarizes the number of infections made by the variants since it was firstly reported to Trend Micro. A program written in Java has been designed to crawl the website and collect information in an automatic fashion. This program receives as input a list of malware families and produces for each family, a file listing all the variants repertoried, their date of release and their total number of infections. The program also computes the number of days between the date of release of a variant and another specified date (6th of July, date chosen arbitrarily). The files generated by the Java Malware Crawler are used as sources of data imported in Excel sheets. This way, it is easy to sort the data following various criterions and create charts that give sense to the numbers collected. Seven families have been selected (the family names used come from the Trend Micro naming system):

- **PE_FUJACKS**: a recent family of profit-driven pieces of malware that have the particularity to propagate mainly infecting files.
- **TROJ_SMALL, WORM_NUWAR**: TROJ_SMALL.EDW aka Storm worm was the first outbreak of the year 2007. This variant creates botnets communicating with a peer-to-peer scheme. Moreover, it is an example of collaboration with another recent threat, WORM_NUWAR.
- **WORM_STRATION**: Stration is an HTTP-based botnet used mainly for spam.

- **WORM_NUGACHE**: Nugache is another example of peer-to-peer botnet but which also use encrypted communications.
- **WORM_AGOBOT:** probably the most popular malicious code since it first gave the possibility for hackers to assemble and thus to create their own variants, selecting modules through a user-friendly graphical interfaces.
- **WORM_SPYBOT, WORM_MYTOB:** other veteran families that have been on the front stage in the past years (i.e. often referenced in the literature).

4.2 Results

Each family has a total number of infection related which is equal to the sum of infections performed by all variants. The diagram shows the shares of infections amongst the families selected since 2001. The diagram on the right, on the other hand shows the infection shares only performed by variants released in 2007.



Since 2001 *In 2007*

Figure 1: Evolution of the infection shares amongst the selected families

Both statistics of infections and variants released (see table 1) demonstrate that the focus of the hackers' community seems to have moved from the legacy families Agobot, Mytob to new families such as Nuwar or Stration. The peak of interest in Small family is certainly explainable by the "success" of the variant Small.EDW, aka Storm worm, released in January 2007.

These recent families propagate by email, as for recent variants of Small family. Email propagation is not new but this channel is now prevalent. Talking only about emails is nonetheless passing by the real trend that stands behind: the social engineering attacks. Indeed, the choice of propagating over SMTP protocol is only relevant to bypass firewalls as well as IDS/IPS systems (of course when the mail has not been dropped by anti-spam counter-measures). But the human user still has to

fall in the social engineering scheme to trigger the infection. Unfortunately, the choice made by the malware creators seems to prove that it is more efficient to target the humans than software vulnerabilities for instance.

Family	2001	2002	2003	2004	2005	2006	2007
AGOBOT	0	3	68	644	423	38	26
FUJACKS	0	0	0	0	0	6	49
MYTOB	0	0	0	0	310	57	64
NUGACHE	0	0	0	0	0	2	2
NUWAR	0	0	0	0	0	7	716
SMALL	1	8	11	315	315	258	2931
SPYBOT	0	0	24	265	188	62	307
STRATION	0	0	0	0	0	148	293

Table 1: Number of variants released each year

Another recent strategy that has emerged is the collaboration with other pieces of malware, either from the same family or not. The best example of such strategy is the collaboration between Nuwar.CQ and Small.EDW (aka Storm worm).

A spam attack started at the beginning of January 2007. Recipients received emails with, as an attachment, a so-called video of the storms that hit the Europe in December 2006. Of course the attachment was not a real video but a Trojan TROJ_SMALL.EDW (Trend Micro, 2007b). So far, a classic scheme. What is less common however is that the Trojan Small.EDW downloads another mass-mailer worm, NUWAR.CQ which in its turn drops Small.EDW: this way they help each other to propagate.

The two pieces of malware have different goals and use two completely different topics as social engineering attacks. Small.EDW exploits the European storms while NUWAR.CQ used the incoming (at the time of the attack) Valentine's Day to fool the recipients (Trend Micro, 2007b): one can think he avoided the first trap but can still fall then into the second one!

A growing change concerns the topology and protocols for botnet communications. Specialists agree to say that the traditional IRC C&C servers are not trendy anymore. Instead, the shift has operated towards peer-to-peer architecture (Symantec, 2007a). Phatbot, Nugache or Small.EDW are examples of bots that has adopted peer-to-peer architecture. Small.EDW even use an open network, eDonkey (Dagon et al, 2007), that makes it harder to monitor since the activity is mixed with the rest of the users. Nevertheless, peer-to-peer botnets studied so far keep a failure point as they use static resources (hard coded list of hosts, cache servers, etc…) for the initial peer discovery. Their topology is not completely de-centralized yet and therefore, remains detectable and vulnerable.

In terms of services, DDoS attacks have decreased *"Symantec recorded an average of 5,213 DoS attacks per day, down from 6,110 in the first half of the year."* (talking

about year 2006, see Symantec, 2007a).The fact is DDoS have been studied and counter measures now exist like the Cisco Guard products (Cisco, 2007). Another possible explanation is that cyber-criminals try as much as possible to avoid direct contact with the victim. This is incompatible with the concept of extortion. It is also noteworthy to highlight that recent families amongst the ones that have been selected for this chapter (Stration, Nuwar, Fujacks), are not firstly designed to perform DDoS attacks (Trend Micro, 2007a).

On the other hand spamming and information theft are very active (Symantec, 2007a). Recent families such as NUWAR or STRATION make spamming their main goal:

- NUWAR broadcasts "pump-and-dump" spam to create artificial demand on financial stocks owned by the zombie network's creators (Trend Micro, 2007b).
- STRATION sends out pharmaceutical spam. It uses spam images in order to evade anti-spam rules (Trend Micro, 2007c).

Spam will certainly remain a privileged activity for the coming years.

5 Taking botnets down

An important question that motivated the authors to undertake this research was: is it possible to design a system that tracks and dismantles botnets in an automated fashion?

So far, it is does not seem possible, the challenges are far too numerous. Indeed such system should have a global view of the Internet (i.e. distributed and/or located at ISP level), detect accurately botnets, not affect legitimate traffic and act in agreement with the legal and ethical issues.

The monitoring techniques reviewed present good qualities but still suffers of limitations in terms of visibility (honeynets and distributed sensors), reliability (DNS as an IDS) or adaptability (the Portland University's botnet detector only works for IRC botnets). The use of fast-flux DNS (Lemos, 2007) makes even more complicated botnets takedown since the C&C servers are highly redundant. Finally, is the Cox Communication case (McKeay, 2007) well illustrates the problem of legal and ethical issues: this internet provider decided to re-route IRC traffic towards its own servers with the aim to uninstall the bots trying several commands. Whether the uninstallation attempt works or not, the bot is at least disconnected from its network. The idea would be nice if it did not also affect legitimate IRC traffic and thus the activity of some professionals using this protocol within their business. Moreover, as it is pointed out by Martin McKeay, we can wonder about the "intrusion" of the ISP in its customers system (McKeay, 2007).

The monitoring systems can prove useful to collect intelligence that will feed the security community and vendors but a lot of obstacles prevent actions to be undertaken afterwards to shut down botnets.

6 Conclusion

To defend against botnets, end-point defence strategy should be rather adopted: unfortunately, it is unrealistic to imagine cleaning the Internet of botnets given the state-of-the-art of monitoring technique as well as legal and ethical issues. Vendors offer products and services that can help to mitigate the threat, like Trend Micro's Botnet Identification Service (Trend Micro, 2007d) or Norton AntiBot (Symantec, 2007b). However, usability of security products in general should be improved again and again to foster their use by non-skilled people.

Educating/training users is essential: bots are first of all malware. As for any malicious pieces of code, the best way to be protected is not to execute them. The trend analysis showed that privileged propagation methods use social-engineering schemes. We could imagine a certification in "IT security awareness" that employees in a company, must pass. This certification would ensure that employees will not misbehave under social engineering attacks. Such certification could be required by the companies as a basic but should be light and quick to take. The simpler the certification is, the more chances there are that the certified people educate their family or friends afterwards. Communication through mass-medias can complete the population training.

Finally, working on new security architectures and/or protocols is certainly the key to make bots unusable. A fundamental difference between a bot and a human user is that the latter is...human. As a result, he is capable to pass very simple challenge while a program cannot, such as a CAPTCHA test (Wikipedia, 2007b). This difference should be exploited and integrated in new security architecture for operating systems.

7 References

Abu Rajab, M., Monrose, F., Terzis, A., Zarfoss, J. (2007) *My Botnet is Bigger than Yours (Maybe, Better than Yours)* [online] Available:http://66.102.9.104/search?q=cache:oeiQ7caR1E0J:www.usenix.org/events/hotbots07/tech/full_papers/rajab/rajab.pdf+prevalence+of+IRC+botnets&hl=en&ct=clnk&cd=2&gl=uk [Date accessed: Thursday 1th February 2007]

Binkley, J., Singh, S. (2006) *An Algorithm for Anomaly-based Botnet Detection* [online] Available: http://web.cecs.pdx.edu/~jrb/jrb.papers/sruti06/sruti06.pdf [Date accessed: 2nd March 2007]

Cheetancheri, S., Agosta, J.M., Dash, D., Levitt, K., Rowe, J., Schooler, E. (2006) *A Distributed Host-based Worm Detection System* [online] Available:http://delivery.acm.org/10.1145/1170000/1162668/p107-

cheetancheri.pdf?key1=1162668&key2=1411867711&coll=&dl=ACM&CFID=15151515&CFTOKEN=6184618[Date accessed: 27th April 2007]

Cisco (2007) *Cisco Guard DDoS Mitigation Appliance* [online] Available: http://www.cisco.com/en/US/products/ps5888/index.html [Date access: Wenesday 4th April 2007]

Dagon, D., Feamster, N., Ramachadran, A.(2006) *Revealing Botnet Membership Using DNSBL Counter-Intelligence* [online] Available: http://www-static.cc.gatech.edu/~feamster/papers/dnsbl.pdf [Date accessed: 17th March 2007]

Dagon, D., Grizzard, J., Nunnery, C., Kang, B., Sharma, V. (2007) *Peer-to-Peer Botnets: Overview and Case Study* [online] Available:http://www.usenix.org/events/hotbots07/tech/full_papers/grizzard/grizzard_html/ [Date accessed: Thursday 10th May 2007]

Honeynet Project (2006) *Know Your Ennemy: Honeynets* [online] Available: http://www.honeypot.org/papers/honeypot/index.html [Date accessed: Wednesday 10th January 2007]

Ilet, D. (2005) Official: Cybercrime is growing [online] Available: http://news.zdnet.co.uk/security/0,1000000189,39193449,00.htm [Date accessed: 22nd March 2007]

Kalt, C. (2000a) *RFC 2810 Internet Relay Chat: Architecture* [online] Available: http://www.irchelp.org/irchelp/rfc/ [Date accessed: Tuesday 16th January]

Kalt, C. (2000b) *RFC 2811 Internet Relay Chat: Channel Management* [online]Available: http://www.irchelp.org/irchelp/rfc/ [Date accessed: Tuesday 16th January]

Lemos, R. (2007) *Fast flux foils botnet takedown* [online] Available: http://www.theregister.co.uk/2007/07/11/fast_flux_botnet/ [Date accessed: 19th August 2007]

McKeay, M. (2007) *Should your ISP protect you from yourself ?* [online] Available: http://www.computerworld.com/blogs/node/5908?source=NLT_VVR&nlid=37 [Date accessed: Saturday 11th August 2007]

Myers, L. (2006) *AIM for Bot Coordination* [online] Available:http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_vb2006_myers.pdf [Date accessed: 22nd March 2007]

Nazario, J. (2007) *Botnet Tracking: Tools, Techniques, and Lessons Learned* [online] Available: https://www.blackhat.com/presentations/bh-dc-07/Nazario/Paper/bh-dc-07-Nazario-WP.pdf [Date accessed: 25th April 2007]

Schonewille, A. ,Van Helmond, D-J. (2006) *The Domain Name Service as an IDS* [online] Available: http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf [Date accessed: 2nd March 2007]

Trend Micro (2007a) *Virus Encyclopedia* [online] Available: http://www.trendmicro.com/vinfo/virusencyclo/default.asp [Date accessed: Tuesday 17th July 2007]

Trend Micro (2007b) *TROJ_SMALL.EDW Storms into Inboxes, Teams Up with NUWAR to Create Unique Network* [online] Available:http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VNAME=TROJ%5FSMALL%2EEDW+Storms+into+Inboxes%2C+Teams+Up+with+NUWAR+to+Create+Unique+Network&Page= [Date accessed: Monday 9th July 2007]

Trend Micro (2007c) *The STRATION Strategy* [online] Available:http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VName=The+STRATION+Strategy [Date accessed: Wenesday 11th July 2007]

Trend Micro (2007d) *Botnet Identification Service* [online] Available: http://us.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/botnetidentificationservice/ds03_bis_070725us.pdf [Date accessed: Thursday 9th August 2007]

Symantec (2007a) *Symantec Internet Security Threat Report Trends for July-December 06* [online] Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf [Date accessed: Wenesday 4th April 2007]

Symantec (2007b) *Symantec Arms Consumers Against PC Hijackers with Norton AntiBot* [online] Available: http://www.symantec.com/about/news/release/article.jsp?prid=20070717_02 [Date accessed: Sunday 12th August 2007]

Wikipedia (2007a) *DNSBL* [online] Available:http://en.wikipedia.org/wiki/DNSBL [Date accessed: Tuesday 12th June 2007]

Wikipedia (2007b*) CAPTCHA* [online] Available: http://en.wikipedia.org/wiki/Captcha [Date accessed: Saturday 18th August 2007]

Investigating, Implementing and Evaluating Client-Side Keystroke Analysis User Authentication for Web Sites

C.G.Hocking and P.S.Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

In today's electronic information society security is certainly the challenge of the 21st century. Driven by the need to counteract ever more determined cyber criminals, focus is turning upon biometric security as a means of ensuring protection and privacy of the most sensitive information. Keystroke dynamics and the analysis of the way people type their password is one method drawing significant attention because of its non-invasive nature and lack of requirements for expensive additional hardware. The majority of research has been executed in a local area network environment but this paper examines the possibility of implementing a solution for web sites and whether refinement of comparison data over time would lead to increasing improvement. Although the web site solution is not conclusive further investigation into profile refinement indicates that this may not have a significant impact on authentication rates. The observed typing characteristics of subjects at the beginning, throughout and at the end of the testing period offer little evidence for implementing a profile refinement strategy.

Keywords

Keystroke, authentication, biometric

1 Introduction

Telephones, computers and other electronic gadgetry have evolved from office-based machinery into household necessities, fashion accessories and even symbols of status. Reliance upon them has proportionately grown and as everyday financial and business activities move evermore into cyberspace, the temptation for others to misuse the trust we place in such devices has correspondingly increased.

Protection of software systems and the information they hold has generally relied upon the ubiquitous user identification and password security concept. Although this is not necessarily a bad idea human beings are inherently forgetful creatures and have tendencies to trust others. Passwords are often written down, placed in desk drawers, left attached to computer monitors on post-it notes or even or divulged for a bar of chocolate (BBC, 2004), and so the search to either replace or bolster this method of authentication is underway.

Electronic communication stretches back as far as the 1830s when Samuel Morse invented the electric telegraph and enabled messages to be transmitted from one side of a country to the other. Since this time expert users have always anecdotally been reported as being able to identify other operators via the style and rhythm with which they sent their communications. Extrapolating the principle this work investigates the possibility of using keystroke dynamics and the way in which people type as a secondary tier of user authentication on web sites. Biometric authentication using a keyboard is an ideal candidate because it requires no expensive additional equipment; it can be implemented in nearly any situation and does not rely upon specific knowledge but rather an individual's natural characteristics.

Biometric systems such as this are generally measured by three factors; the False Rejection Rate (FRR), the proportion of times an authentic user is rejected as being an impostor; the False Acceptance Rate (FAR), the rate at which an impostor successfully passes the authentication procedure; and the Equal Error Rate (EER), the point at which the FRR and FAR are identical. As figure 1 indicates the tolerance or threshold setting directly influences both the FRR and FAR; any solution aims to achieve an EER as near zero as possible with the ultimate system yielding a zero rate.

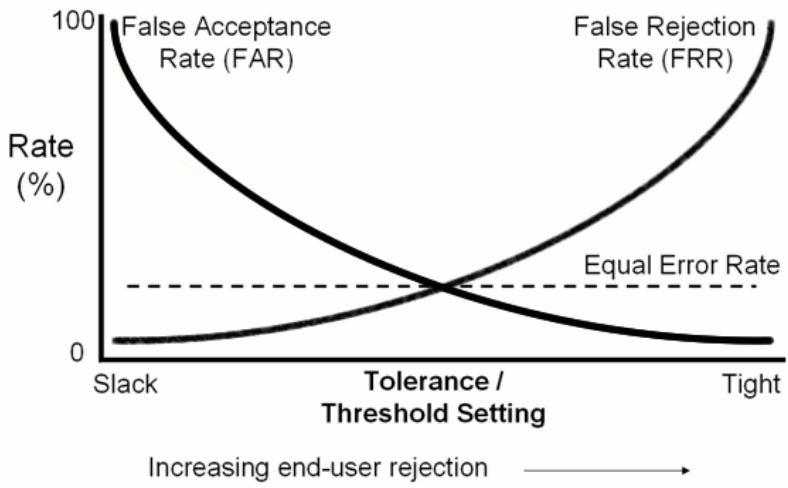


Figure 1: Biometric system result rates

A web site will be developed that allows individuals to register themselves and create a personal timing pattern that can then be tested against other subjects typing the same pass phrase. Once a period of testing has been completed the captured data will be retrieved and analysed off-line to establish if this is indeed a viable method of identity confirmation and whether further refinement over time would improve the observed success rate.

2 Background

Classification of typing characteristics or keyboard dynamics is generally based upon the analysis of consecutive keystroke (digraph) timings; the interval between key depressions, the gap between the release of the first key and the pressing of the second, and the total digraph length. In some instances the inter-key latency can be negative as a fast typist will depress the second key before releasing the first. Figure 2 outlines the significant events when typing the word 'the' where $K2_D$ represents the precise time of the depression of key two and $K3_U$ the release (key up) of key three.

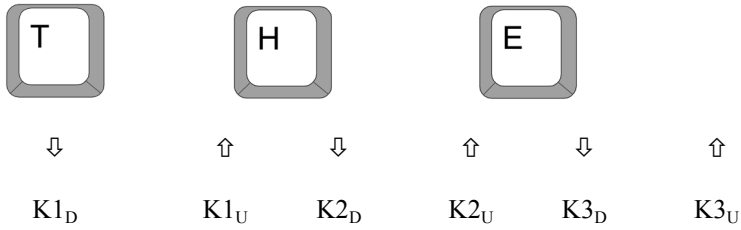


Figure 2: Sequence of events when the word 'the' is typed

This leads us to understand that for the digraph 'th', 't' was held down for $K1_U - K1_D$ time intervals, the inter-key latency was $K2_D - K1_U$ and the entire digraph took $\max(K1_U, K2_U) - K1_D$ to type.

The first study into keystroke analysis was in 1980 and involved the observation of a secretarial pool of seven typists. Each typist provided two typing samples, the digraph means of which were examined to see if they had come from the same subject using a T-test. An EER of around 5% was achieved in this preliminary study suggesting that keystroke analysis was a viable method for user identification and authentication (Gaines et al, 1980). First Leggett and Williams (1988) and then Joyce et al (1990) extended this early work by introducing the classification technique when comparing sampled timings with a mean test pattern synthesised from eight master samples. Although probability of digraph occurrence was not found to have a significant impact upon lowering the EER, the use of structured text during a training cycle was identified as being of greater benefit (Monrose et al, 1994). More recently neural networks have been used to identify typing patterns and have returned observations as low as 1% across 21 subjects (Cho et al, 2000).

Many researchers have also established the suitability of using such a technique to identify and authenticate (Bartolacci et al, 2005; Bergadano et al, 2003; Dowland and Furnell, 2004; Napier 1995) but in all of these cases the testing and data capture has been performed either on stand-alone PCs or across a local area network. Ngo et al (2006) successfully performed authentication across the Internet and it is with these and similar works that research is now turning towards refinement of a solution provision as opposed to proof of concept.

3 Research Detail

This work has involved the creation of a web site using a mixture of HTML and JavaScript with the server processing being undertaken by PHP and the data written to an Access database. The site required subjects to register a personal timing template which was synthesised from the 10 best entries of 12 attempts. Details of each digraph punched were stored in readiness for data analysis which was to occur off-line. Following registration individuals took part in the testing phase during which they were repeatedly requested to enter their own and a mystery user's password. Digraph timings were captured using HTML events such as 'onKeyDown', 'onKeyUp' and 'onBlur' to trigger appropriate JavaScript routines which used the internal PC clock to record the precise time. If at any time during typing of a password a mistake was made or inappropriate keys pressed the entry was entirely rejected and the individual requested to resubmit.

The approach to analysis was based upon proposals made by Magalhães and Santos (2005) but this work parameterised some of the settings and thresholds to investigate the impact upon the results. Additional work beyond the normal FRR, FAR and EER analysis was designed to investigate whether refinement of an individual's profile over time would indeed impact and improve the results. Upon validation of an entered password the timing of each character pair would be tested to see if it lay between an upper and lower bound, calculated from the password owner's profile. For each success 1 point was scored and for each failure zero. The average point score was then calculated and if this exceeded a specified 'acceptance' threshold the user was deemed to be authentic. The lower (b_l) and upper bounds (b_u) are calculated as shown below, using the profile mean ($\overline{p}$), profile median (p_m), a lower threshold (T_l), an upper threshold (T_u) and the profile standard deviation (σ).

$$b_l = \min(p_m, \overline{p}) \times \left(T_l - \left(\frac{\sigma}{\overline{p}} \right) \right) \quad \text{and} \quad b_u = \max(p_m, \overline{p}) \times \left(T_u + \left(\frac{\sigma}{\overline{p}} \right) \right)$$

The two thresholds are to be varied in the range (0.900-0.975) and (1.025-1.100).

4 Results

The web site and all appropriate data capture routines were developed and implemented. During a 12 day testing period 16 users fully registered their details and performed suitable amounts of testing to deem them significant candidates. The testing process was incentivised by the display of a 'Top 10 Testers' league table on the data entry webpage, with each scoring one point for the entry of a mystery password. In all 6999 tests were recorded, 4083 'own' and 2916 'mystery' passwords. Off-line analysis of this data using combinations of acceptance=0.40,0.45,0.50,0.55,0.60; lower bound threshold=0.900,0.950,0.975;

upper bound threshold=0.900,0.950,0.975; produced the following summarised results:

Acceptance	Lower Threshold	Upper Threshold	Self Failed	Other Passed	FRR	FAR
0.40	0.950	1.050	434	820	10.62944%	28.12071%
0.45	0.950	1.050	986	544	24.14891%	18.65569%
0.50	0.950	1.050	986	544	24.14891%	18.65569%
0.55	0.950	1.050	1226	290	30.02694%	9.94513%
0.60	0.950	1.050	1882	173	46.09356%	5.93278%
0.40	0.900	1.050	191	1142	4.67793%	39.16324%
0.45	0.900	1.050	517	833	12.66226%	28.56653%
0.50	0.900	1.050	517	833	12.66226%	28.56653%
0.55	0.900	1.050	668	526	16.36052%	18.03841%
0.60	0.900	1.050	1229	331	30.10042%	11.35117%
0.40	0.900	1.100	87	1351	2.13079%	46.33059%
0.45	0.900	1.100	264	1044	6.46583%	35.80247%
0.50	0.900	1.100	264	1044	6.46583%	35.80247%
0.55	0.900	1.100	378	717	9.25790%	24.58848%
0.60	0.900	1.100	863	479	21.13642%	16.42661%
0.40	0.950	1.100	279	1064	6.83321%	36.48834%
0.45	0.950	1.100	668	751	16.36052%	25.75446%
0.50	0.950	1.100	668	751	16.36052%	25.75446%
0.55	0.950	1.100	864	458	21.16091%	15.70645%
0.60	0.950	1.100	1508	275	36.93363%	9.43073%
0.40	0.975	1.025	687	595	16.82586%	20.40466%
0.45	0.975	1.025	1315	364	32.20671%	12.48285%
0.50	0.975	1.025	1315	364	32.20671%	12.48285%
0.55	0.975	1.025	1632	162	39.97061%	5.55556%
0.60	0.975	1.025	2283	92	55.91477%	3.15501%

Table 1: Summarised testing results

The combination of bounds that exhibited the lowest EER was 0.900 and 1.100 and the graphical representation of these is shown in figure 3.

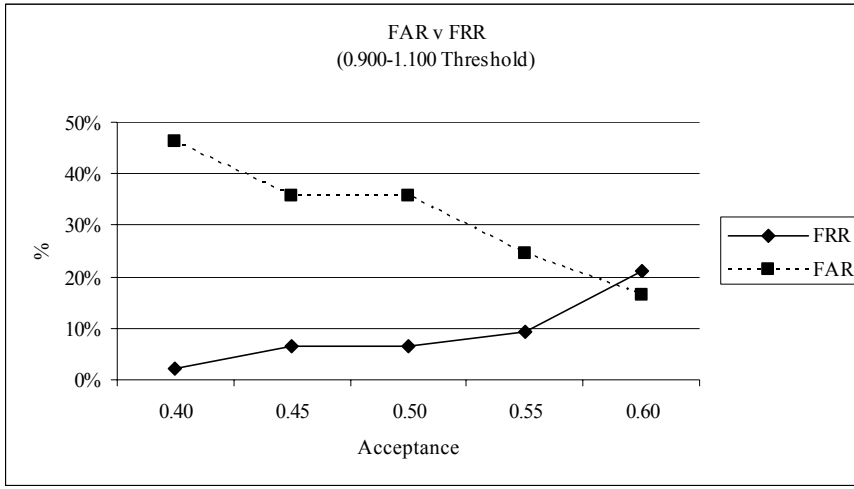


Figure 3: Graph of best results from table 1

Investigation then continued into the longevity of profiles; for this purpose the 'self test' data for the most prolific tester was isolated. This particular subject completed 2004 entries of their own password which consisted of nine single case alphanumeric characters (ilewamh04) and the data provided the following results:

	Mean				Standard deviation			
Digraph	Profile	All entries	First 10	Last 10	Profile	All entries	First 10	Last 10
i-l	238.600	254.880	251.000	264.300	7.031	56.902	29.833	20.174
l-e	223.100	266.605	221.500	333.900	20.940	88.799	61.136	32.191
e-w	244.800	246.415	249.500	245.400	15.465	73.758	18.511	30.771
w-a	262.200	254.624	260.600	247.700	33.409	114.204	30.474	15.963
a-m	197.900	198.471	208.900	200.500	31.297	70.080	25.324	28.218
m-h	284.000	264.134	271.400	284.400	11.498	42.525	17.374	14.678
h-0	426.000	428.607	480.300	555.400	81.884	120.599	140.155	173.959
0-4	276.200	225.124	255.700	259.800	39.364	67.979	29.678	76.349

Table 2: Results of the most prolific tester over time

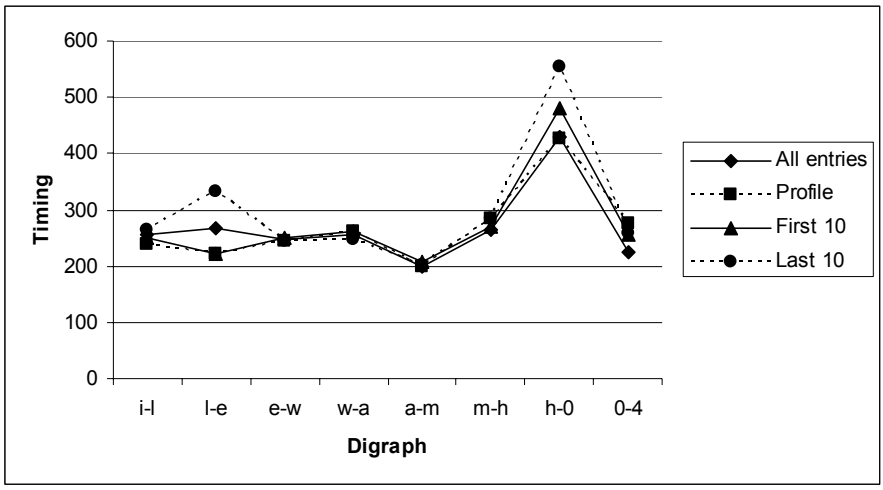


Figure 4: Mean timings of the most prolific user

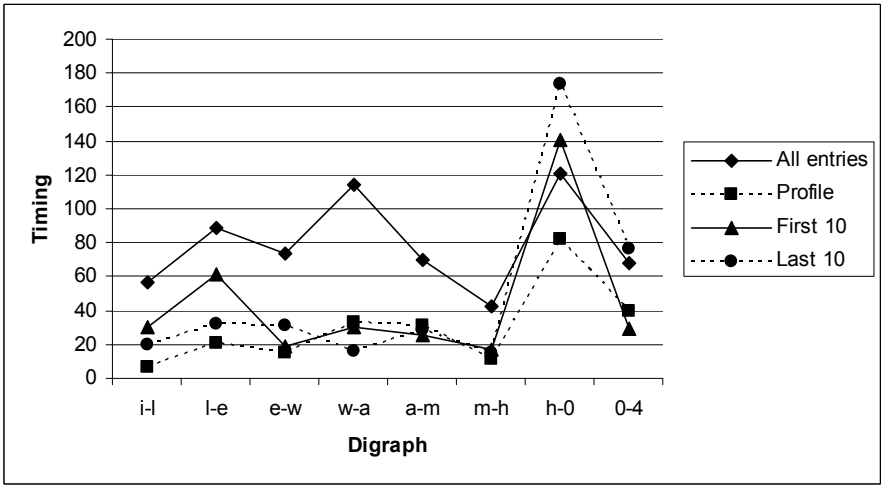


Figure 5: Timing standard deviation of the most prolific user

5 Discussion

Analysis of the keystroke timing results yields a plot (figure 3) which suggests an Equal Error Rate of approximately 18%, much higher than desired. This is certainly not low enough to conclude that keystroke analysis during this testing cycle was sufficiently accurate to be employed as a method of user authentication. It should be noted that the testing phase was compressed into a 12 day period and with the nature of the competition some subjects submitted a large number of tests. Of course the

quantity of data was welcomed to enable some meaningful calculations to be undertaken but contrary to this with so many repetitions passwords become familiar. Indeed at the outset because passwords were being openly displayed to other users, individuals were encouraged to select an unfamiliar password rather than pick one that was in regular use. Consequently at the beginning the only experience they had of using a particular pass phrase was their 12 repetitions during profile registration. Nearly everybody was as inexperienced as anybody else and one would expect a high standard deviation to be exhibited leading to higher FRR and FAR indices.

Typing expertise is a factor in exhibited results although it is not suitable to be used as a metric during the evaluation process. Anecdotally one of the subjects, a touch typist who uses all 10 fingers, reported they had trouble typing one of the test passwords, the name 'rebecca'. This for them was solely left-handed typing because of the position of the keys on the keyboard and the transition between 'e-b-e' was an "unnatural finger spread" which caused a disruption to fluency. A trait that was clearly visible in the captured data.

More meaningful results were exhibited by the investigation into user profile improvement. The two graphs produced by the results (figures 4 and 5) provided some very interesting results. Figure 4 exhibits the diagraph mean timings for the profile, all tests, the first 10 tests and the last 10 tests of a user who submitted 2004 individual entries of their own password. There is very little variation between the four profiles but the biggest change is noted in the 'l-e' diagraph combination which worsens by approximately 50% over time. This is perhaps related to the number of executed cycles and although the subject stated they are a 'good' typist the distance between the letters 'l' and 'e' on a keyboard is relatively large indicating that tiredness and perhaps the use of few fingers impacted on the timings. With a touch typist the digraph combination would be completed using both hands and so the distance to travel eliminated as a factor. The tiredness theory is further supported by figure 5 which shows an increased standard deviation across 'all tests' from the lowest set, the profile.

These findings suggest that to refine the profile as time goes on would not significantly tighten variation and is therefore of little benefit. It may be argued that with a high repetition rate apathy increases and concentration wanes leading to the observed discrepancies.

6 Conclusion

This research was carried out under time constraints and the development of the web site with the complexities within impinged upon the testing phase and the quantity of data gathered. Sixteen significant users are less than would be ideally chosen and so the results are a little unclear. Reflection upon self testing and the improvement exhibited over time appears to suggest that profile refinement would not impact upon the investigated user. Further work would ideally be targeted at this stronger vein of enquiry and compare the effects of time and repetition on other subjects.

The quantity of data would provide reasonable scope to refine the algorithms used in an attempt to identify typing patterns. An Equal Error Rate of 18% is too large to conclude this is a viable form of user identification and authentication with the techniques employed but eminent research and anecdotal reports compound to dispute this and further investigation is certainly required. Some of the fuzziness maybe due to JavaScript being employed to capture the precise timings and comparisons should be executed using alternative methods of timing to clarify this dilemma.

7 References

Bartolacci, G., Curtin, M., Katzenberg, M., Nwana, N., Cha, S. and Tappert, C. (2005), 'Long-Text Keystroke Biometric Applications over the Internet' *Proceedings of Student/Faculty Research Day, CSIS, Pace University*

BBC (2004), 'Passwords Revealed by Sweet Deal' available: http://news.bbc.co.uk/1/hi/technology/3639679.stm [accessed 14 Mar 2007]

Bergadano, F., Gunetti, D. and Picardi, C. (2003), 'Identity Verification Through Dynamic Keystroke Analysis' *Intelligent Data Analysis,* vol. 7 pp. 469–496

Cho, S., Han, C., Han, D. H. and Kim, H. I. (2000), 'Web-Based Keystroke Dynamics Identity Verification Using Neural Network' *Journal of Organizational Computing and Electronic Commerce,* vol. 10 no. 4 pp. 295–307

Dowland, P. S. and Furnell, S. M. (2004) 'A Long-term Trial of Keystroke Profiling using Digraph, Trigraph and Keyword Latencies' *Proceedings of IFIP/SEC 2004 - 19th International Conference on Information Security*, pp. 275-289

Gaines, R., Lisowski, W., Press, S. and Shapiro, N. (1980), 'Authentication by Keystroke Timing: some preliminary results' *Rand Report R-256-NSF. Rand Corporation*

Joyce, R. and Gupta, G. (1990) 'User authorization based on keystroke latencies' *Communications of the ACM,* vol. 33 no. 2 pp. 168–176

Leggett, J. and Williams, G. (1988) 'Verifying identity via keystroke characteristics' *International Journal of Man-Machine Studies,* vol. 28 no. 1 pp. 67-76

Magalhães, S. T. and Santos, H. D (2005) 'An Improved Statistical Keystroke Dynamics Algorithm', Proceedings of the IADIS Virtual Multi Conference on Computer Science and Information Systems, 2005

Monrose, F., Rubin, A. D. (2000) 'Keystroke dynamics as a biometric for authentication' *Future Generation Computer Systems*, vol. 16 pp. 351–359

Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M. and Wagner, M. (1995) 'Keyboard user verification: toward an accurate, efficient, and ecologically valid algorithm' *International Journal of Human Computer Studies*, vol. 43 pp. 213-222

Ngo, G., Simone, J. and St. Fort, H. (2006) 'Developing a Java-Based Keystroke Biometric System for Long-Text Input' *Proceedings of Student/Faculty Research Day, CSIS, Pace University*

The Dark Side of Google

T.Ly and M.Papadaki

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Google is the most popular, powerful searching tool and is used by pretty much all the web community. However, it is so powerful that Google can easily be turned into a very useful hacking tool, if misused by ill-intentioned people: in fact, by deliberately searching for confidential and sensitive information that the search engine may have inadvertently picked up, Google clearly shows us its dark side and it will indeed be possible to locate and exploit several targets across the web thanks to Google.Thus, lots of sensitive data, such as passwords, credit card numbers or even social security numbers are readily accessible to hackers, who would simply make use of Google to find them. In that way, Google is nowadays considered as a real double-edged tool and some alternatives should quickly be implemented to counterattack the Google Hacking phenomenon.

In that way, our project work would be to explore and analyse the general threat posed by Google hacking. The outlines of our work would then include the investigation through different real cases of security intrusions that involved Google hacking and would also propose some ways of detecting and responding to these types of attacks. Therefore, the preventive solution that we suggested would be to set up a GHH (Google Hack Honeypot), which would allow security specialists to study the profile of attackers, in order to anticipate their next move.

Keywords

Google Hacking, Google Hacking DataBase, Google Hack Honeypot

1 Introduction

Nobody can deny today that the company Google nearly controls all the majority of the huge web market, especially concerning the web search engines. In fact, the search engine Google gives us results and queries, which are so relevant and precise that it is certainly the most used in the world. Furthermore, searching web pages with the help of keywords is not the only ability of Google: in fact, the web search engine also makes the inventory of all images of websites, videos and message groups (such as USENET), etc. Thus, Google is growing everyday and becoming an unavoidable tool for all web users.

However, ill-intentioned people, such as hackers, are capable to misuse the web search engine, in order to exploit its powerful search algorithms, such as PageRank. As the web cache of Google is huge (the web cache represents all the data of web

sites registered by Google), the web search engine Google can deliberately become a hacking tool by searching for confidential information, such as passwords, credit card numbers, social security numbers or even FOUO (**F**or **O**fficial **U**se **O**nly) documents.

This amazing phenomenon is called the **Google Hacking** and it grows pretty fast those days. It is indeed a recent term that refers to the *art of creating complex search engine queries in order to filter through large amounts of search results for particular information* (Bausch, Calishain and Dornfest, 2006). At a more simple level, the Google hacking techniques would simply allow pirates to use/misuse powerful tools of Google in order to find sensitive information.

As it were, the more the web search engine Google grows, the more Google hacking also grows… In fact, even some trickiest tools appeared on the web market, such as the active **Google Hacking Database (GHDB)**: it is indeed a reference database in the field, which makes an inventory of all new Google hacking techniques. The database currently contains 1468 entries, included in 14 categories (GHDB, 2007), such as advisories and vulnerabilities, files containing passwords or pages containing network or vulnerability data. When a new Google hacking technique is discovered, people could add it in the database and it is everyday updated.

In that way, as Google is not ready to stop soon, the Google Hacking will not be willing to give up as well... and there will always have much more Google attackers... such as the master in the field, Johnny Long (see figure 1).

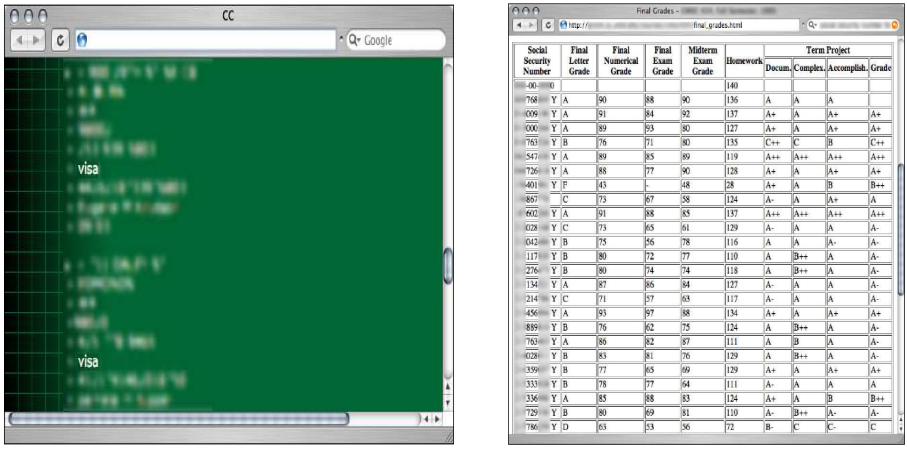


Figure 1: Credit card numbers & Social security numbers found by J. Long Source: Google Hacking for Penetration Testers (2004)

The main objective of this paper was to study the dark side of the search engine Google: the phenomenon as know as Google Hacking, mostly unknown to the general audience.

That is why the main purpose of this project will be to warn the general public, but rather people who build websites, i.e. the webmasters, of the threat posed by Google hackers. By the way, in order to better target the main aim, the project will be divided in 2 smaller objectives, which could also be compared to the main outlines of the project:

1. Reveal to all web users and especially to webmasters the real dangers of Google, which are generally unknown to the general public. The best way to achieve will be to explore the main techniques of Google Hacking and its latest trends.

2. Propose ways of detecting and responding to Google attackers: it will allow webmasters to better counterattack and also better understand Google's dark side.

2 Google Hack Honeypot, the reaction

2.1 The concept

The Google Hack Honeypot is not strictly speaking a real solution against Google hacking techniques. In fact, it is rather a 'reaction' to Google hackers (also called search engine hackers): the idea behind a Google Hack Honeypot (GHH) is that it places an invisible link onto your web site. Just like the case with a poorly constructed application, visitors to the web site will never see this link, but Google will. However, instead of providing access to confidential data, the link will conduct Google hackers to a PHP script that logs their activity.

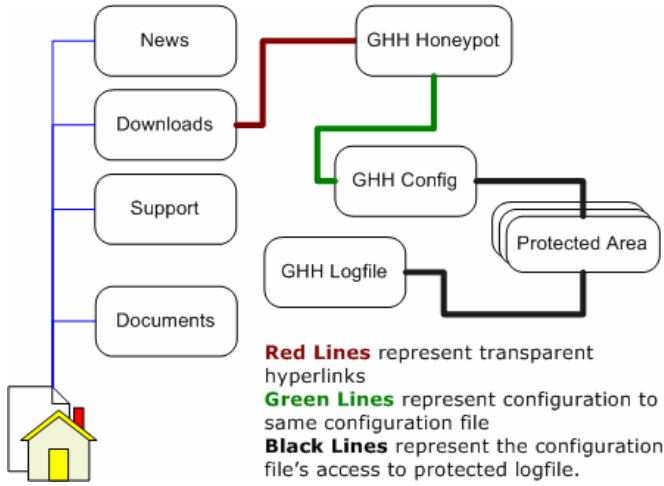


Figure 2: Google Hack Honeypot (GHH)
Source: http://ghh.sourceforge.net

In that way, security researchers and specialists would be able to draw an accurate profile of the attacks/attackers, in order to prevent and anticipate their next move.

At a simple level, a honeypot (hardware or software) will emulate vulnerabilities, or will deliberately contain some flaws and even some (false) confidential information: hackers will be attracted by this kind of information, and will fall in the trap: web administrators could also block hackers (IP address) and monitor how they launched their attacks (source of the attack), in order to prevent the next ones.

Therefore, GHH appears to be the perfect tool to better analyse and understand the Google Hacking phenomenon.

2.2 Experiments tested

Three different GHH experiments were launched through January to May 2007:

- Honeypot 1: GHDB Signature #935 (inurl:"install/install.php")
- Honeypot 2: GHDB Signature #1064 (filetype:sql ("passwd values" | "password values" | "pass values"))
- Honeypot 3: GHDB Signature #1758 "The statistics were last updated" "Daily"-microsoft.com

The honeypots were implemented in the same time and into a same hosted website. As it were, their set up was pretty easy to execute: there were indeed no specific need to install a hardware solution, nevertheless only few knowledge in PHP (the honeypots are coded in that web language) were necessary to manipulate them, but otherwise their implementation was quite simple to install. However, it is worth noting that the indexing into the Google search engine was a lot more challenging and it involved several steps; identification of the website, listing of all web pages with Sitemap (XML), implementation of the accurate META tags into the source code, waiting for a validation from a Google bot, which has to list all the webpages of the website, etc. In fact, in order to be seen by the hacker community, the opened vulnerabilities that the honeypots suggest and the website in itself as well have to clearly be visible on the web and particularly directly on the Google search engine. It is also important to that the website did not contain any confidential data (it was not a commercial website to be clear but rather a personal one, such as a blog). The purpose of potential attackers was then not financial. Perhaps, the website would have attracted more attacks, had it contained financial data.

The results were conclusive, as we caught all the same around 200 attacks the first month. However, the number of total attacks decreased month to month. The reason of this is probably that the 3 honeypots were hosted in the same website, so that the hackers did discover the traps. This suggests that the average life for a honeypot is about 1 to 2 months: after that ‘hackers’ begin to lose interest.

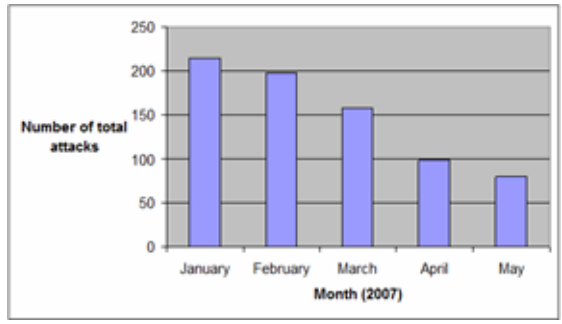


Figure 3: Number of total attacks

2.2.1 Honeypot 1: GHDB Signature #935

Collected data from the first honeypot reveal that the attackers were mainly script kiddies (inexperienced newbies in hacking). There is one thing to prove it: in fact, we remarked that the same IP consecutively appeared twice to four times, and even 5 times. When some script kiddies indeed fall in the honeypot, they stay in the same page, whereas they thought that they made a great exploit and are waiting for a new page with juicy information, but there is nothing for them, as they are in the honeypot! So, their reflex would be to hit again, by refreshing (actualizing) another time the webpage, and that is why we often caught the same IP in the results. Also, a large number of IPs belongs to some anonymous proxies, which is indicated by the fact that there was no specific response from whois queries (Whois, 2007). The attackers are then considered as anonymous. The IP addresses of those proxies are mainly from networks in Russia, Germany and China (see the graph), where lots of anonymous proxies' lists could even be rent. Moreover, as the website is hosted in Europe (from a French web host company) and then on Google France, the 'Other' IPs mostly did correspond to French IP addresses

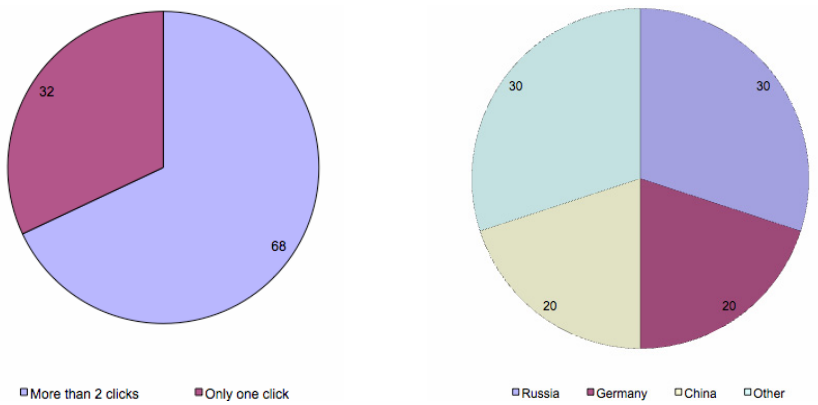


Figure 4: Script kiddies vs experienced hackers, Country of origin

2.2.2 Honeypot 2: GHDB Signature #1064

After a deep investigation, i.e. whois and traceroute (Whois, 2007)(Traceroute, 2007), most of the attacks come from a free tool called SiteDigger (the IPs are flagged with the SiteDigger signature, i.e. with a specific IP address). This software was created by Foundstone, a division of the famous antivirus company McAfee and was originally developed for helping security professionals to find (Google Hacking) web vulnerabilities (Foundstone, 2006). However, as it is the same issue for a lot of security tools, these are some double-edged weapons. In fact, SiteDigger also allows hackers to search for vulnerabilities, errors, configuration issues, proprietary information and interesting security nuggets on websites through Google. And icing on the cake, SiteDigger enables to directly look for vulnerabilities and signatures belonging to the unavoidable Google Hack DataBase (GHDB), which is a real incubator for Google hackers. In that way, the tool is always updated with the latest trickiest signatures of Google hacking.

Therefore, SiteDigger also allows hackers to automate their juicy information's searches thanks to Google (such as passwords) and this tool then appeared to be really dangerous. Nonetheless, the reaction of Google was, for once, quite effective: in fact, for activating SiteDigger, a Google API (Application Programming Interface) Key is requested, and it is the assault course to get the precious key: a large number of complex (and deliberated) registrations are required. Those were necessary to let Google to trace every query that SiteDigger will request (and by the way, the queries are limited to 1000 a day).

Furthermore, what it will be interesting to notice is that for the other honeypot, it was possible for hackers to hijack their identities by spoofing their IPs with some anonymous proxies. But for this specific case, all hints of identification through SiteDigger are logged and traced and it is not possible to be anonymous.

Nevertheless, many (good) black hat hackers asserted that it is very easy to create a tool such as SiteDigger: there is incidentally some unofficial tools which are distributed within the hacker community and that could easily be downloaded on the web.

As it were, despite the general Google's precautions, Site Digger is obviously used to look for unauthorised purposes. The evidence to support this claim is the fact that they searched your site for vulnerabilities, without your authorisation.

2.2.3 Honeypot 3: GHDB Signature #1758

It is really hard to draw a profile of the real attackers. Then what it would be interesting to study here is the kind of browser that the 'attackers' used. And results were pretty amazing: 40% of the users were using Internet Explorer (version 6 or 7), 35% (Mozilla) and 5% for the others (Opera, Netscape).

Mozilla is a browser that is said to be more secured (Zdnet, 2005), and people are more and more using it (Slate, 2004). However, what we could notice is that people did not update their version as we might do it, and that is pretty dangerous, as we know that old versions of browsers are subject to many attacks (Symantec Internet Security Threat Report, 2006).

Regarding now the country of origin of the attacks, they are coming by a majority from Europe (45%), US (20%), China (15%), Russia (15%) and others (5%). The reason why there are more attackers in Europe is because the website was hosted in France and will then be subject to more queries from European Google servers.

Basically, here are the other conclusions that we draw after analysis of the results:

- Many attacks appeared to come from scripts kiddies (inexperienced newbies in hacking). In fact, the Google hacking techniques through the GHDB for instance are likely very easy to use (such as making of use of Google itself).
- A large number of IPs belongs to some anonymous proxies and the attackers are then considered as anonymous. The IP addresses of those proxies are mainly from networks in Russia, Germany and China, where lots of anonymous proxies' lists could even be rent.
- Many IPs are coming from the strange same domain and networks. (e.g. x.x.x.1/20 with 10 IP addresses). This indicates that the IPs might belong to a potential botnet, as the time of the attack is very close to each other (even a simultaneous attack). The potential assumption is also that those particular IP addresses are probably all infected with a specific worm and then are hosted behind a specific ISP with DHCP (Dynamic Host Configuration Protocol) that keeps getting online/offline
- 40% of the users were using Internet Explorer (version 6 or 7), 35% (Mozilla) and 5% for the others (Opera, Netscape). We did noticed that the users did not update their version as we might do it, and that is pretty dangerous, as we know that old versions of browsers are subject to many attacks (Symantec Internet Security Threat Report, 2006).

To conclude this section regarding the Google Hacking experiments, what we could say is that the experiments were a great success: we caught many attacks and attackers, and it was pretty easy to draw conclusions (even if they were not as deep as we could expect). As it were, the honeypot is still an unknown technology, but it begins to be used more and more: in fact, its techniques are closely linked with the intrusion detection systems (Honeypots.net, 2007) and it is obvious that large companies will need it for their corporate website.

It is sure that those experiments were not perfectly raised at all: in fact, what it could be a potential improvement for better and more detailed analysis would be to set up one honeypot into one only hosted website: their shelf life (i.e. the honeypots were too easy to spot by hackers) would be surely longer and the collection of data would probably be more accurate.

Furthermore, what we noticed is that the average life for a honeypot is about 1 to 2 months: in fact, after catching attacks in the net, 'hackers' begin to understand that there noting really juicy in the website. In that way, they begin to give up and that is why we got less attacks during the last months.

Anyway, the honeypot technology is a good prospect: the next generation of honeypots would have to be more active and responsive. That is what the third generation of honeypots, as know as GenIII (honeywalls), recently appeared.

3 Conclusions and future work

This paper, which concluded 6 months of work on the topic, generally introduces the dark side of Google and its main concept based on some tricky Google Hacking techniques.

By the way, the study of the phenomenon was complete, as we get through different angles of attack. In fact, we addressed some deep theoretical points, by discussing the main techniques and also by reviewing some past incidents involving the Google hacking and we analysed with a practical viewpoint some (Google Hack Honeypot) experiments, in order to directly understand the purpose of the attackers.

As for a potential future work, there are plenty of choices: in fact, the Google Hacking phenomenon is not ready to stop for a good while. In fact, as the web search engine Google keeps growing, its dark side would keep increasing as well.

4 References

Dornfest, R., Bausch, P. and Calishain, T. (2006). "Google Hacks". Publisher: O'Reilly Media, U.S.A

GHDB (2007). "Google hacking DataBase", http://johnny.ihackstuff.com/ghdb.php [Accessed 30/08/2007]

Google Corporate History (2006). http://www.google.com/intl/en/corporate/security.html [Accessed 30/08/2007]

Google Hack Honeypot (2007). http://ghh.sourceforge.net/ [Accessed 30/08/2007]

Long, J. (2005). "Google Hacking for Penetration Testers". Publisher: Syngress Publishing, U.S.A

Symantec Internet Security Threat Report (2006). Trends for January 06 – June 06. Volume X, Published September 2006

Feasibility Study into the use of Service Oriented Architecture within the Atlantis University Portal

F.Mountford and A.D.Phippen

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Atlantis University is an ambitious e-learning project employing new pedagogical research to develop an e-learning system, currently the system has many heterogeneous applications in its portfolio that need to be integrated into one online based portal, the use of SOA is proposed to integrate the systems together. SOA is very complex to implement, it needs a completely new framework and strategy. Other more technical issues surround lack of maturity and some issues regarding performance. With regards to the Atlantis project the following needs to be considered:- What evaluation and feasibility studies can be carried out on Atlantis; An in depth analysis of the Atlantis applications and potential business processes and bottlenecks; How can the overall SOA project be managed; The project concludes that a SOA management committee be setup and distinctly more work in business process needs to be carried out.

Keywords

Service Oriented Architecture, Web Services, e-learning,

1 Introduction

The Atlantis University project is creating a software system in the area of e-learning to provide a learning environment based on extended blended learning.

The project involves the use of a portfolio of different applications of differing vendors and programmed using different languages and interfaces; the project needs to integrate all these applications together so that they can be used effectively.

Work conducted by Huang (2006) indicates that the proposed means to do this is by SOA and has suggested that some sort of feasibility study / prototype be developed.

This paper shows shortcomings in the literature review and therefore the SOA evaluation methods are used to create a new framework for Atlantis as part of the experimental work for this project. The framework details the need to look closer at the Atlantis applications and business processes in order to give some recommendations for the way forward for Atlantis.

2 Atlantis University

The Atlantis University Project is an international project in the area of learning; it is an ambitious and innovative project, introducing new concepts based on pedagogical research on order to provide a three tier learning package as shown in figure 1 below.

Atlantis is an international partnership involving nine universities; these include the Fachhochschule Darmstadt Germany, University of Plymouth UK and the Warsaw Technical Institute Poland.

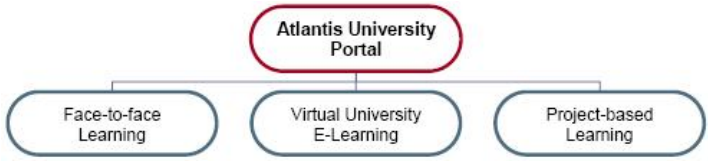


Figure 1: Atlantis University Portal (Bleimann, 2004)

The learning process hierarchy, shown in figure 2, shows how a student learns, starting off at the bottom with data and information applied to this forms knowledge, soft skills such as teamwork and communication make up to capability, E-learning does not address the capability part of the pyramid.

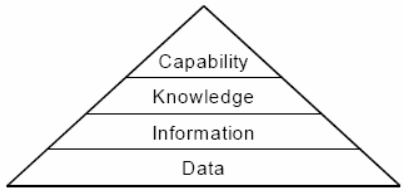


Figure 2: Learning Process Hierarchy (Bleimann, 2004)

Standalone e-learning packages have failed for this reason and therefore Atlantis has come up with extended blended learning, its aims is to outweigh the advantages and disadvantages of each learning method and to help provide all four tiers of the hierarchy by blending them all together.

3 Integration technologies

The Atlantis portfolio of applications need to be integrated together. The intended way to do this is by SOA and using Web Services as the underlying technology to provide it.

"Service Oriented Architecture is an architectural style as opposed to a technology in order to reuse and integrate subsystems of existing systems in order to reuse them for

new systems. Such systems are kept separate but are coupled loosely to each other as needed."

(Wada and Suzuki, 2006)

Web Services is a software system identified by a URI, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems.

These systems may then interact with the Web service in a manner prescribed by its definition, using XML based messages conveyed by Internet protocols. Web Services are frequently application programming interfaces.

(Austin et al, 2004)

4 Justification for SOA

In previous Atlantis work by Huang (2006), a consideration was made as to how the Atlantis Portal can be integrated. Two architectures were proposed based on complete theory work and these appear below in figures 3 and 4.

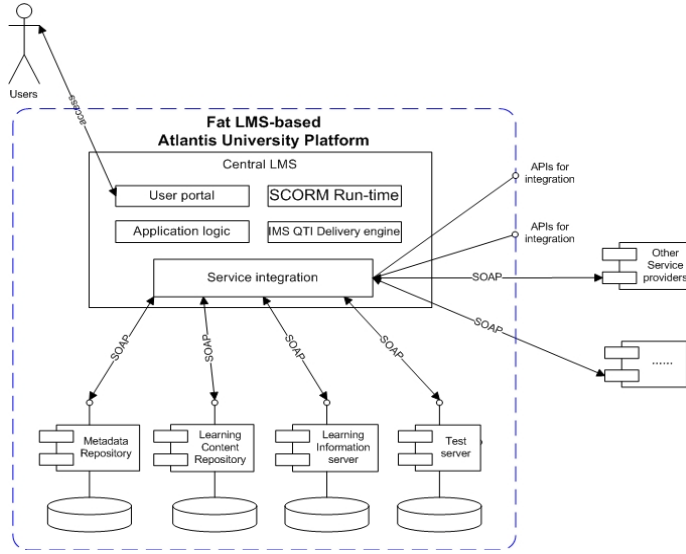


Figure 3: Fat LMS (Huang 2006)

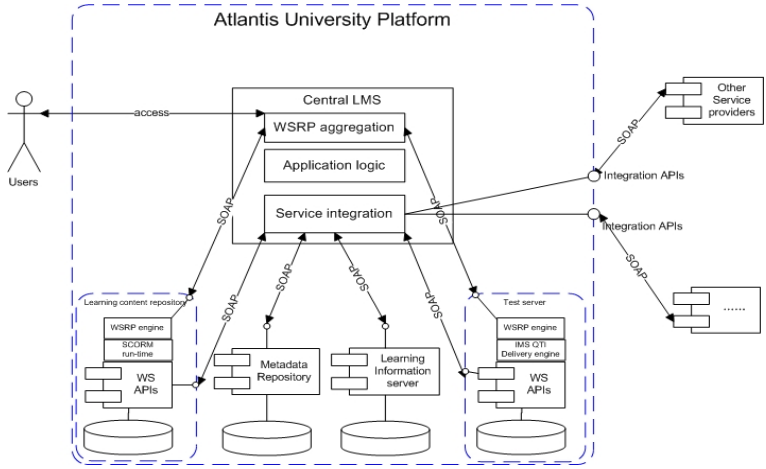


Figure 4: Thin LMS (Huang 2006)

The problem with the work of Huang is the fact that the thesis appears to be very descriptive and lacks critical justification through evaluation for the decisions.

The architectures and service platforms proposed by Huang also do not seem to resemble the project as it stands at the present time, and looks more to a futuristic outlook to the system in several years to come.

5 Technical Testing

Other work in this area concerned another Masters thesis which uses an experimental approach to investigate the readiness of web service standards to be applied to business processes. The work reveals many issues and concludes that such technology needs time to mature before they can be used realistically plus services seem to work best based around automatic tasks such as travel agent scenarios.

In the early stages of the project the idea was put forward to create some sort of technical testing of the use of SOA within Atlantis. The problem with doing this is the fact that some sort of analysis on the current Atlantis setup was needed before it can be established what exactly to test, a different approach is needed.

6 SOA Evaluation Methods

It was decided to give more thought about where this project is heading and a decision was made to look at some in depth research into how to evaluate and mange a SOA project.

Four main frameworks were investigated:-

- Evaluation framework

"The Evaluation framework is a conceptual framework for evaluating the applicability and viability of Web Services, examining economic, technical and organizational contexts." (Estrem, 2003)

- SOA project plans

Balzer (2004) presents a SOA Governance model which looks at the need for more management based skills as well as technical skills, the Governance model defines

  - What to do
  - How to do it
  - Who should do it?
  - How should it be measured?

- B2B Web Services design

This focuses issues regarding process-based integration of services, dependable integration of services, support of standardized interactions security and privacy. (Hogg et al, 2004)

- Migrating to SOA

Channabasavaiah et al (2003) discusses how organizations can better understand the value of SOA, how to evaluate the current infrastructure in order to develop a plan for migration to SOA.

Additionally Oracle (2005) looks at SOA Governance and Orchestration including the need for a SOA Strategy; it reveals a SOA Life Cycle and looks at consideration for the more challenging aspects of SOA.

Overall these frameworks look at very much the same sort of thing. The problem with them is they reflect the use of SOA on corporate based projects whereby formally Atlantis is a University research project; therefore, as part of the experimental work these frameworks have been translated into a usable model for Atlantis.

The use of the frameworks has established the need for the following:-

- The need for a Governance / Management Strategy
- Using the SOA Life Cycle and an Evolutionary Strategy
- Defining the SOA Architecture
- Definition of APIs

Plus looking at benefits predicted vs. those gained, Quality of Service Issues, defining Critical success factors, Security, Functional and Non Functional requirements

7 Atlantis Applications

The research above revealed that more awareness is needed about the current Atlantis applications before work on how to manage and evaluate the Atlantis SOA begins; this work is based on the following questions.

- What they do
- What data and information they communicate
- Potential bottlenecks / issues
- What other applications they interact with

- Plans for the future

The following is a list of Atlantis applications

- Learning design – Learning based on telling a story
- Collaborative Content Manipulation – Collaborative based Presentation Client
- Document Management System
- XML database
- Semantic Wiki
- LDAP
- Portal
- VOIP
- Generic Storytelling Engine
- Plus other applications

The work revealed that Learning Design is the strongest candidate for business processes and most applications will need to interface with the DMS and LDAP.

8 Integration of Diverse applications into a new Portal Based on SOA

A thesis by Reinbold (2007) looks at how to integrate the Atlantis applications into a new portal, research work was carried out into the business processes of Atlantis, evaluation of portal software and an architecture proposal.

Analysing the work conducted in this thesis reveals many flaws; first of all it is not believed that the business process work has been done properly the survey was very small and in itself was flawed due to the fact that the Learning Design system was omitted.

Because the work on Learning design was omitted, which we have learned is a key element of Atlantis it meant that a conclusion was made that there is little business processes happening in the system and therefore an architecture was proposed which

was purely to integrate. Functionality to provide business processing was missing from the architecture.

9 Business Processes

The work by Reinbold and the experimental work on SOA management shows serious shortcomings with regards to Business Process work and it is learned that this work is vital in ensuring success of a SOA system.

Work carried out into analysing the applications of Atlantis have revealed some potential business processes, particularly within Learning Design that has potential for reengineering and automation.

10 Atlantis SOA Architecture

The work on the Atlantis SOA Architecture by Reinbold shows some major shortcomings in the analysis carried out and therefore the proposal for the new Atlantis SOA architecture is not accurate particularly with regards to Learning Design

Figure 5 below illustrates a new proposal for the Architecture along with the Business Process flows, compared to the diagrams Reinbold created with respect to the Business process work flow engines it differs slightly in that these are missing; further research is needed to decide if a separate technology such as workflow or BPEL is needed to orchestrate these as it is unclear at this time. Additionally any interactions between the XML database and the other systems are not present simply because the research is not ready for this area yet.

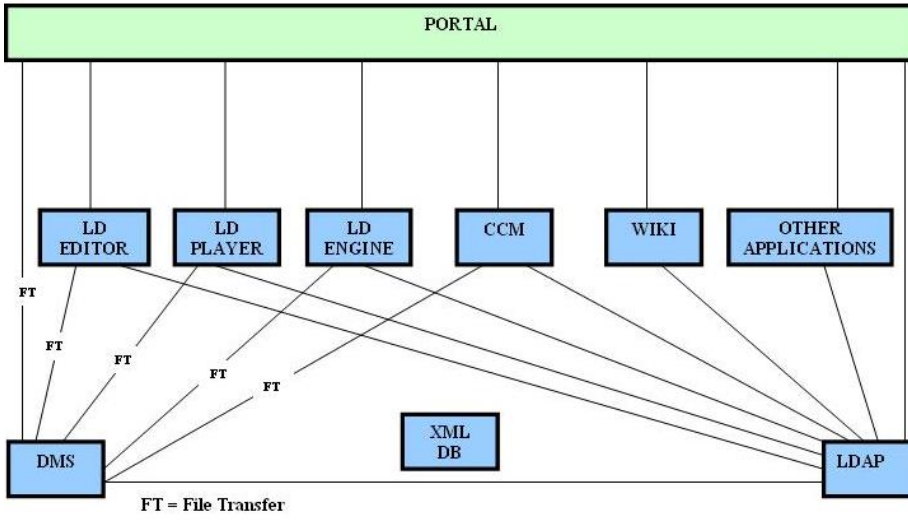


Figure 5: Proposed Atlantis Architecture

11 Recommendations and Conclusion

The initial idea of the project was to perform a feasibility study into the use of SOA within Atlantis.

It was quickly realised that as long as the fundamental reasons for having SOA are present, such as the need to integrate a set of heterogeneous applications, then SOA should in general be used. The real question is how to go about creating a SOA and this paper has revealed that this is a huge task and this paper has merely skimmed the surface.

Experimental work in the literature review was used to establish a SOA evaluation framework for use with Atlantis and therefore there are several recommendations that Atlantis should strongly adopt in the next semester of the project and these are listed below in order of importance.

A separate sub topic should be setup examining the Atlantis business processes more thoroughly with respect to the Atlantis SOA

Each development team for each sub system should support this team by producing process maps for them

The work on evaluating each Atlantis application needs to be completed, particularly for the new systems such as the XML database.

A SOA Management Committee should be setup

Findings in the work has revealed many shortcomings to parts of the Atlantis project that need to be completed, ideally before any more work is stated on the project.

Participating in the Atlantis project has been a huge experience in terms of communication and team work and the experience of cross boarder interactions. In the past university projects have been based on mock up of a business IT scenario but as Atlantis is a real life scenario it has given a more realistic experience in this area.

12 References

Austin D, Babir A, Ferris C, Garg S, 11th February 2004, Web Services Architecture Requirements, http://www.w3.org/TR/wsa-reqs/, Date accessed 16th January 2007

Balzer Y, 16th July 2004, Improve your SOA project plans, http://www-128.ibm.com/developerworks/webservices/library/ws-improvesoa/, Date accessed 12th March 2007

Bleimann U, 2004, Atlantis University – A new pedagogical approach beyond e-learning, http://www.aida.h-da.de/projects/atlantis_university/veroeffentlichungen/Atlantis_University_Paper_INC_2004.pdf, Date accessed 08th January 2007

Channabasavaiah 16th July 2003, Migrating to a service-oriented architecture, Part 1 http://www-128.ibm.com/developerworks/library/ws-migratesoa/, Date accessed 12th March 2007

Estrem W, 28th May 2003, An evaluation framework for deploying Web Services in the next generation manufacturing enterprise., http://www.sciencedirect.com/science?_ob=MImg &_imagekey=B6V4P-49H6XPJ-1-9&_cdi=5764&_user=10&_orig=search&_coverDate= 12%2F31%2F2003&_sk=999809993&view=c&wchp=dGLbVzz-zSkWb&md5= b2af6ce86ea1c0f4edcc3697fb28d87a&ie=/sdarticle.pdf, Date accessed 12th March 2007

Hayward J, 23rd September 2005, The application of Web Services within a business process framework, (MSc Thesis)

K Hogg, P Chilcott, M Nolan, and B. Srinivasan 2004, An Evaluation of Web Services in the Design of a B2B Application http://crpit.com/confpapers/CRPITV26Hogg.pdf , Date accessed 12th March 2007

Huang H, 19th October 2006, Concept of an E-Learning platform with respect to integration

Oracle, December 2005, Strategies for SOA Success, http://www.oracle.com/technologies/soa/strategies-for-soa-success.pdf, Date accessed 29th March 2007

Reinbold D, 2007, Integration of diverse applications into a new portal based on SOA, Masters Thesis

Wada H, Suzuki J, 2006, Modelling Non-Functional Aspects in Service Oriented Architecture, http://dssg.cs.umb.edu/projects/soa.html/, Date Accessed 22nd August 2007

Novel Single Sign On Architecture Based on the Subscriber Identity Module for Web Services

D.S.Stienne[1], N.L.Clarke[1] and P.L.Reynolds[2]

[1] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2]France Telecom R&D UK Ltd., Bristol, UK
e-mail: info@cscan.org

Abstract

The need to authenticate in Internet services has increased considerably over the past years. Every time the user wishes to access his web services, he has to prove his identity by providing his credentials. Therefore, knowledge based authentication methods (e.g. password) are inadequate, and bring in weaknesses in the security authentication chain. As a result, novel solutions are required to avoid the burden of repeated re-authentications and enhance authentication methods (e.g. strong authentication).

In order to solve the first point, the research has investigated an existing solution called Single Sign On (SSO). SSO is a concept which exonerates the user from re-authenticating. There are different ways to provide SSO, and the research has chosen to study different Authentication Authorisation Infrastructure (AAI), on one side the Liberty Alliance project and on the other side the Shibboleth project.

However these infrastructures do not improve the authentication process and consequently this paper has introduced a new component in the AAI architecture: the Subscriber Identity Module (SIM) which brings a strong authentication capability. In order to create such a concept, the research has developed a novel framework where web services can interact with the SIM card to authenticate the user.

Keywords

SSO, federation, Liberty Alliance, SIM

1 Introduction

Internet plays an important role in the day to day activities of the users who may use Internet for checking e-mails, buying books, looking for information or selling personal belongings. Each kind of activity is proposed by different web services. As a result, the user may have to create an account and remember a set of different passwords and identifiers in order to get the required connection. Therefore, the knowledge based authentication technique (e.g. password) does not provide a relevant level of security. Consequently, investigations are required to reduce the growing need to re-authenticate, and improving authentication methods.

The research starts by considering the Single Sign On (SSO) concept. By definition; SSO is a concept where a user authenticates one time to a trusted entity which provides at its turn information to other services requiring user authentication. The idea of SSO has already been developed by several Authentication Authorisation Infrastructures (AAIs). In an AAI, a user authenticates only once to an identity provider (IDP) and this one authenticates the user on his behalf in his web services (i.e. the IDP provides user's credentials information to web services).

Considering AAIs, the research proposes a novel approach, using the Subscriber Identity Module (SIM) card as a trusted module to authenticate the user. The SIM will be issued by the IDP and some credentials information will be downloaded into the SIM card. When credentials get in the hand of the SIM, the user is then able to authenticate in his web services independently from his IDP (i.e. once the user has identified himself to the SIM, he will be able to access his web services without having to re-authenticate repeatedly).

Nowadays, many Internet users have a mobile phone close to their computer and, therefore, this new way of working can be extremely valuable. In addition; the SIM will provide a strong authentication solution where credentials are stored in a tamper resistant area, protected by a secret knowledge.

This paper will describe the SIM card approach based on an existing AAI. It is laid out as follows: Section 2 gives a quick review of two existing AAIs, Section 3 describes the selected AAI in order to develop the concept (i.e. Liberty Alliance federation framework). Section 4 presents the proposed novel federation framework based on the SIM card to connect the user to his web services. Section 5 details several technical requirements involving the web browser interacting with the SIM card. Section 6 discusses the proposed solution and the paper finishes with a conclusion and the need for future research works.

2 Review of AAIs

This research study has chosen to review two well-known AAIs, which have been developed by different groups in order to provide web SSO. These AAIs are Shibboleth (Shibboleth website, 2007) and Liberty Alliance (Liberty Alliance website, 2007).

2.1 Shibboleth

Shibboleth is an Internet 2 project which has developed an open solution to solve the problem of sharing resources between different organisations. These organisations are called Service Providers (SPs) which have their own authentication and authorisation policies which impede sharing resources between them. The Shibboleth project chose to develop a novel idea where a home organisation is available to authenticate the user in different SPs. In addition, the home organisation manages the identity of the user. This identity is composed of different attributes which could be disclosed to SPs for authentication purposes. Consequently, when a user requests an

access to resources stored by an SP, the SP sends his attributes rules to the home organisation and the home organisation supplies the necessary information to the SP. The SP chooses to grant or deny the access to the resource. The advantage of such an architecture is that SPs do not have to manage the authentication of the user; this task being delegated to the home organisation and authorisation decisions performed by the SP.

2.2 Liberty Alliance

The Liberty Alliance project is a European project which has been created in 2001. It involves important organisations such as IBM, France Telecom and others companies working as a consortium. They cooperate in order to write open standards and define requirements to provide federated identity management. By definition, the concept of federation allows the user to manage his identity across different SPs and to navigate directly from SP to SP without to re-authenticate (SSO). This situation is possible when SPs are part of a circle of trust where an Identity Provider (IDP) authenticates the user in his federated services. Both IDP and SP parties must comply with the Liberty Alliance federation framework in order to get common protocol common protocols to exchange their information (Liberty Alliance, 2004a). Whereas Shibboleth is an open source software (i.e. released under apache software licence), the Liberty Alliance does not provide any software, but releases specifications draft, defining abstract protocols and delegating the task of implementation to organisations which wish to implement the federation framework.

3 The Liberty Alliance federation framework

As mentioned in the introduction part, the research has chosen to develop the SIM idea using one AAI. The Liberty Alliance AAI has been selected, and this part gives a quick overview of the Liberty federation framework and define terms and protocol.

3.1 SSO and Federation definition

The SSO and federation are two key concepts of the Liberty Alliance federation framework. As mentioned previously, the circle of trust is composed of an IDP and various SPs. Each party is independent and can authenticate the user through its own methods. However, the Liberty Alliance introduces the concept of federation which allows the user to login to his SP with a simplified sign on. This simplified sign on is made possible by the IDP which authenticates the user on his behalf in the SP. As a result, once the user is authenticated to his IDP, the SSO mechanism is available, and the user can navigate seamlessly in his federated SPs.

Prior to benefiting from the SSO, the user has to federate his accounts between the IDP and SP. If both the IDP and SP parties support the Liberty federation framework, the federation process is possible. By definition, the federation process links two accounts, and enables the IDP to authenticate the user on his behalf to his SP (Liberty Alliance, 2004b).

3.2 SSO and federation protocol

The Liberty consortium defined an SSO and federation protocol, part of the federation framework (Liberty Alliance, 2004c). This protocol is an abstract protocol which can perform both operations: federation and SSO through a same single message exchange. Figure 1 illustrates this protocol where one SP and one IDP exchange information.

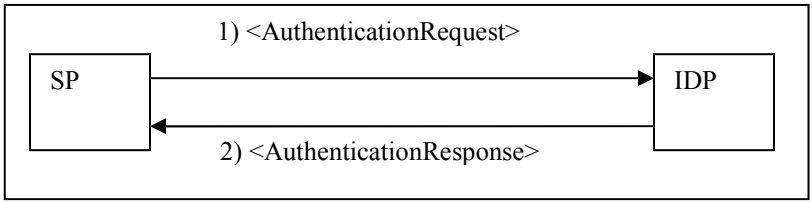


Figure 1: SSO and federation protocol

When a user decides to federate his SP account with his IDP, the SP sends an authentication request to the IDP specifying a federation subject. The IDP must respond with an authentication reply. Once the account has been federated, the user can enjoy SSO experience. SSO utilises the same protocol; as a result, when a user requests an access to his federated SP, the SP sends an authentication request to the IDP. The IDP should response with an authentication reply which gathers necessary credentials to connect the user to his federated SP.

4 Novel SSO architecture based on the SIM

The previous part presented the Liberty Alliance federation framework which permits to enable SSO. This part presents the novel SSO architecture based on the SIM.

4.1 Requirements

The research wants to develop a novel SSO architecture based on the SIM. One of the first objectives is to provide SSO to the user when he navigates through his web services. As a result, this research has elected to retain the Liberty components which are IDP and SP. Consequently, the federation and SSO concepts are maintained. However, the research wants to add the SIM in the framework, allowing the user to connect to his web services directly without his IDP. Then, the research must define new federation and SSO protocols which are not the same as the Liberty ones. The next paragraph defines these protocols.

4.2 New federation and SSO protocols

In the Liberty architecture, the federation and SSO protocols are part of the same protocol (Cf. section 3.2). In the novel architecture, the research has chosen to develop separately two different protocols: On one side, the federation protocol is

used to link two accounts of the user, one from the IDP and the other from the SP. On the other side, the SSO protocol is used by the IDP to authenticate the user to the SP on his behalf.

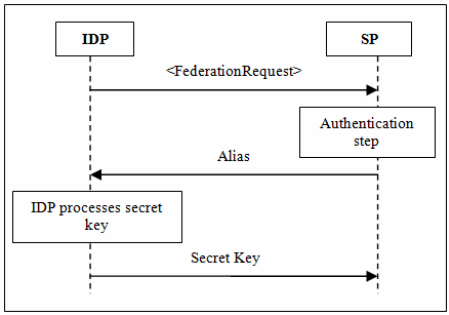


Figure 2: Federation protocol

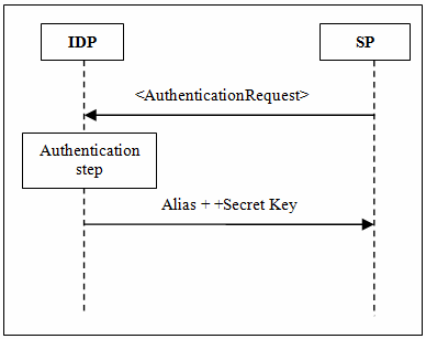


Figure 3: SSO protocol

Figure 2 illustrates the federation protocol where one SP and one IDP interact. When the user decides to federate his SP account with his IDP account, the IDP must be able to authenticate the user to his SP on his behalf. In order to achieve this operation, the SP and IDP have to agree on two criteria, an alias of the user and a secret key for authentication purposes. By definition, both providers must keep the alias and secret key in their directory or databases. The alias and the secret key constitute a profile which is called the federated profile.

The federation protocol is designed to allow this information exchange and will work as follows: First, the IDP sends a federation request to the SP. The SP authenticates the user and generates an alias corresponding to the user's local account. This alias is sent back to the IDP for storage purposes and the IDP generates a secret key and shares it with the SP.

Later on, when the user requests an access to his SP, the IDP will be able to authenticate the user on his behalf by using the alias and secret key previously agreed. The alias and secret key work as credentials to authenticate the user on the SP. Figure3 shows the SSO protocol where the SP issues an authentication request to the IDP. As a result, the IDP retrieves the alias and the secret key information in its database and sends them to the SP.

4.3 SIM card interaction

The research study proposes to add the SIM to the novel SSO architecture. By definition, the SIM is used in the global system for mobile communication network and designed to authenticate the user in this network (3GPP, 2007). This paper shows how the SIM will be able to authenticate the user in his federated services independently from the IDP. This challenging goal can be achieved only if the SIM gathers the federated profile of the user.

In order to do that, the SIM must be involved in the federation protocol. As seen previously, during the federation protocol, both IDP and SP parties exchange an alias of the user and a secret key. They store this information for authentication purposes. As a result, when a user decides to federate his account by use of his SIM card, the SIM must get the necessary information (i.e. federated profile).

Figure 4 illustrates the federation protocol interacting with the SIM. Now, the federation protocol involves three players, the IDP, SP and SIM. The flow of the protocol is the same as described earlier; however, in this case, the IDP does not generate the secret key. This task is delegated to the SIM card because the SIM must be able to authenticate the user in his federated service independently from the IDP. The SIM shares the secret key information with the IDP and the SP.

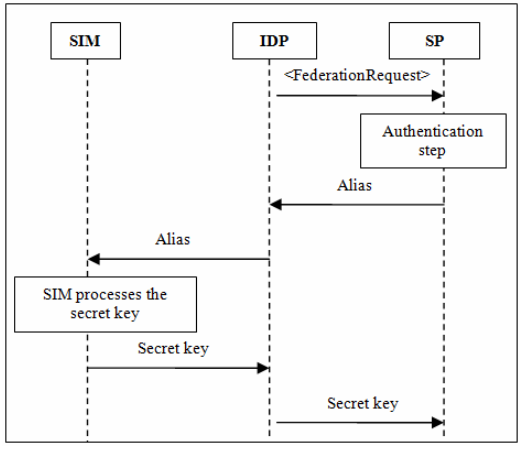


Figure 4: SIM based federation protocol

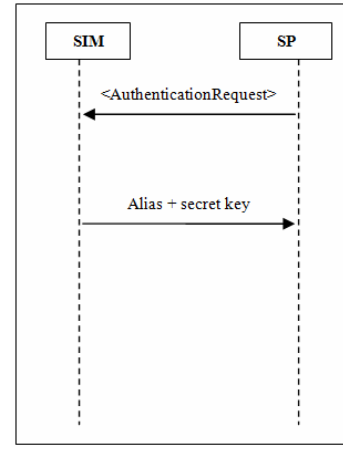


Figure 5: SIM based SSO protocol

Each party stores a federated profile; the IDP and the SP store this profile in their database, and the SIM stores the profile in its memory. Figure 5 illustrates the SSO protocol between the SIM card and the SP, which is the same protocol as described in Figure 3, but the SIM has now taken the place of the IDP.

4.4 Summary

This novel SSO architecture allows the user to navigate seamlessly from SPs to SPs with an IDP. The research adds a new component to the architecture which is the SIM card. In this new architecture, if the user decides to federate his accounts by use of his SIM card, he will have two possibilities to connect to his federated services. These two possibilities are the SIM card which can work independently from the IDP, and the IDP which can authenticate the user through his services. The described novel protocol implies several technical requirements as, for example, the issue of

communications between the SP and the IDP as well as security problems. The following paragraph gives an overview of the technical requirements.

5 Technical requirements

5.1 Web browser interactions

The web browser (i.e. user agent) is an application, part of the operating system of the computer, which permits the access to Internet. When a user requests an access to his web services, part of the federation framework, the IDP authenticates the user on his behalf. This situation is possible because the IDP communicates with the SP through the user agent.

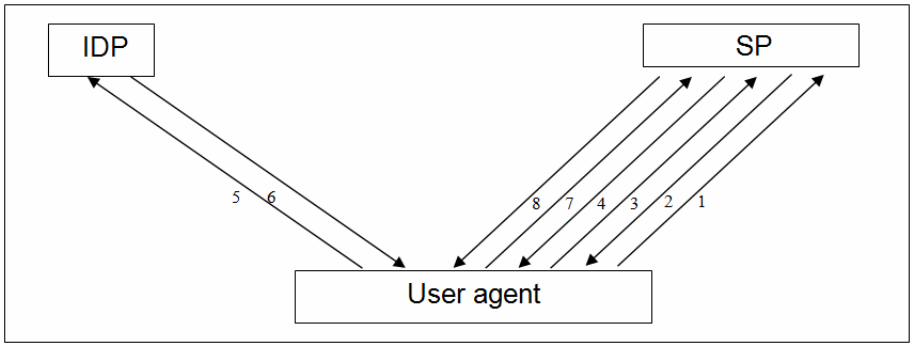


Figure 6: User agent used as a channel of communication

Figure 6 gives an example of the communication taking place between the IDP and SP. In this situation a user has one account to the IDP and one to the SP. Both accounts have been federated together, and SSO is enabled.

When the user requests an access to his SP (step 1), the SP responds with a web page listing IDPs which are part of the circle of trust (step 2). The user chooses the IDP which will authenticate him at the SP (step 3). Then, the SP issues an HTTP redirection request to the user agent which forwards the authentication request to the selected IDP (step 4 & 5). In response, the IDP must send back all necessary credentials (i.e. alias and secret key) to authenticate the user at the SP. This is achieved when the IDP sends an HTTP redirection request containing the required user's credentials (step 6). In final, the user agent forwards this information to the SP (step7) and the SP then decides to grant or deny the access to the user and displays a web page (step 8).

Figure 7 illustrates another situation where the user uses his SIM card to access his federated services. The protocol flow is the same as illustrated above. However, the user agent must be provided with a plug-in permitting an interaction between the SP and the SIM card.

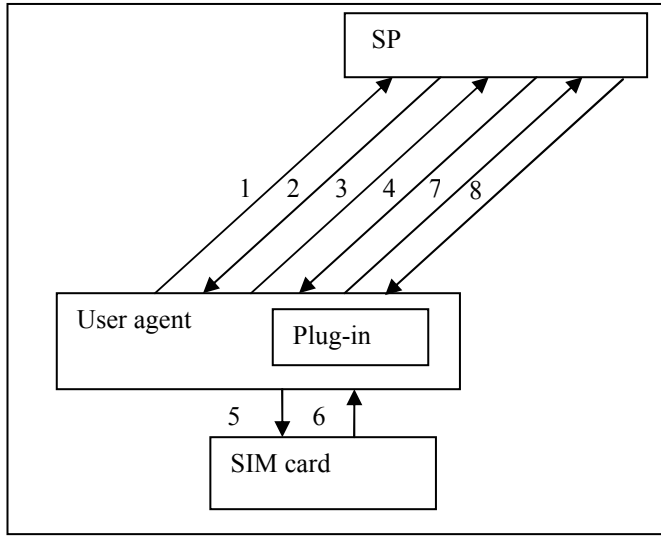


Figure 7: authentication to SP with the SIM card

5.2 Transport of information

During the federation or authentication step, parties exchange several critical information, like the secret key. Consequently, the information has to be protected, avoiding a user to misuse the credentials. As the communication between the IDP and the SP is achieved through the user agent, this research study has decided to use the SSL protocol to secure the transport of data. For being able to use it, providers must have an SSL certificate as advised by the Liberty Alliance Bindings and Profiles Specification draft paper (Liberty Alliance, 2004d).

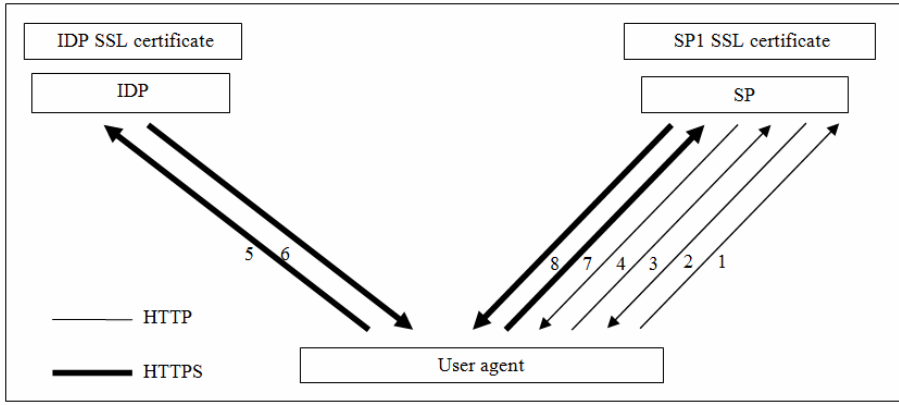


Figure 8: Use of SSL to securely transport the information

Figure 8 illustrates the situation where the SSL protocol is used to secure the exchange of information between the IDP and SP through the user agent. This situation has been described previously in Figure 6 where the user accesses his federated service with his IDP. As shown in Figure 8, steps 1, 2, 3 and 4 do not require using the SSL protocol while steps 5, 6, 7 and 8 use it for sending the credential data.

6 Discussion

This research intends to propose a novel federation framework using the SIM card. An advantage of this solution is that SPs (e.g. banks) which desire to benefit from this strong authentication solution will not have to involve an entire infrastructure for managing and updating the SIM component as it is under control by the IDP which provides the necessary credentials. Typically, the IDP and SP will have a business agreement, where the SP trusts the SIM as an authentication token to authenticate the users. In addition, the SIM based concept work independently from the IDP which results in a faster operation during the authentication process with the SP and avoiding the IDP being overloaded by SSO requests**.**

However, this approach shows several limitations as it has not defined how trust takes place between different elements. A solution can be to utilise a Public Key Infrastructure (PKI) where entities authenticate to each other by use of public key certificates (OASIS, 2004).

7 Conclusion and future work

This paper has introduced an approach in which the SIM card is used as a strong authentication solution. During the development of this concept, the research has reviewed the current AAI architectures which propose different federation frameworks allowing the user to navigate seamlessly to his web service without re-authenticating (SSO). To achieve the desired goal it has been selected to use the Liberty Alliance federation framework which, however, has not been designed to work with SIM cards. Consequently, the research has been driven to create a novel federation framework while keeping the architecture of Liberty and the federation and SSO concept. This paper has described how the new federation and SSO work and listed several technical requirements brought by the exchange of data process. The future work will have to define how trust can be generated between entities though the use of PKI.

8 References

3GPP (2007), "Specification of the Subscriber Identity Module -Mobile Equipment (SIM - ME) interface (TS 11.11 V8.14.0)", (Accessed 3 May 2007)

Liberty Alliance website (2007), "The liberty alliance project", http://www.projectliberty.org, (Accessed 27 March 2007)

Liberty Alliance (2004a),"Liberty Specs tutorial", (Accessed 27 March 2007)

Liberty Alliance (2004b), "Liberty ID-FF Architecture overview" Thomas, W., eds., (Accessed 5 April 2007)

Liberty Alliance (2004c),"Liberty ID-FF Protocols and Schema Specification", Cantor, Scott, Kemp, John, Eds., (Accessed 16 April 2007)

Liberty Alliance (2004d), "Liberty ID-FF Bindings and Profiles Specification,", Cantor, Scott, Kemp, John, Champagne, Darryl, eds., (Accessed 15 April 2007)

OASIS, (2004), “Trust model guidelines” Linn eds. [Online]. Available at http://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-draft-01.pdf (Accessed 24 July 2007)

Shibboleth website (2007), "Shibboleth project", http://shibboleth.internet2.edu, (Accessed 15 March 2007)

Online Security: Strategies for Promoting User Awareness

M.Vikharuddin and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

This Research paper describes various threats and vulnerabilities the home users face whilst using the services offered by the World Wide Web. It describes the common threats and the way the home users perceive them. Several aspects on online security are discussed that helps home users learn and understand the threats they are posed to. Reports from previous surveys are presented that gives a clear understanding on how the users perceive online security. More the online security perception, the better is the level of security achieved by the home internet users. The main outcome of this research is that the Security guidelines for home users are vast over the internet. Many websites offer simple and very easy to understand guidelines and yet the users are not able to reach those websites. Publishing security information on certain websites is not going to help users and previous survey results shows that the existing media awareness techniques are not succeeded in promoting awareness among home users so it is very important how the cybercrime and online security is presented to the open world. This paper makes a sincere attempt to recommend some new set of online security techniques that could be used to increase the user perceptions and also a solution to improve the existing media awareness techniques so that the governing bodies and software application vendors could reach more users educating them on online safety aspects.

Keywords

Internet Security, Home Users, Security Perception, Media Awareness

1 Introduction

The Internet has become a part of our daily life offering us online banking, shopping, electronic mail, businesses and education. It is a powerful means to establish connections to other computers and users. With the increased use, the internet is no more a safe playground to be dealt with. Information transferred through the Internet could be compromised by various means. Computer security is a vital issue for both home users and business users. Many software applications are available to protect the computers that are connected to Internet. Antivirus applications and Firewall are commonly used to protect computers from hacking, viruses, malicious codes and information theft. The way the home users perceive and protect against the odds plays an important role. Media presentation on the other hand is equally vital as it makes the users aware of the security updates, virus information and protection against them. The governing bodies, software vendors and banks should often perform awareness programs in such a way that the security information reaches

every user. The need for better understanding of the security aspects from a home user point of view was the main motivation to consider this research. This research paper discusses the existing methods on how the home users reach the security guidelines and about the media presentation methods adapted by various banking organizations and software vendors. The research also suggests possible improvements for both user perceptions and awareness programs.

2 Common threats the home users face

Home users often confront threats over the internet that includes viruses, worms, spam, spyware, phishing and hacking. Any of the mentioned threat will lead to the user information being tampered or misused or even the computer being hijacked/attacked.

The most recent noticeable incident in cybercrime is the Trojan attack on the online recruitment website Monster.com. The Trojan used credentials probably stolen from a number of recruiters. It then logged on to the website, searched for resumes and personal details of applicants such as name, surname, email address, home address and telephone numbers were uploaded to a remote server which was under the control of the attackers. 1.6 million job seeker's personal information was stolen (Symantec Report, 2007). Spam mail are unwanted mail the users get which could possibly leads the users to websites involved in installing malware and spyware applications in to the user's computer. The common type of spam in the online threat was related to 'Health products' and 'Commercial products' totaling to 32 % and 30% respectively (Symantec Corporation, 2007). There are many different kinds of threats such as phishing, viruses /worms and Instant messaging are that seriously posing threats to home users. Security is a major concern for home users when they are using the internet services like electronic mailing system, banking, shopping and instant messaging. Protecting home users from this kind of threats personal and drives to discuss the need for online security

3 The Need for Online Security

A survey conducted by comScore in June 2007 concluded that the United Kingdom has the most active online population. On an average, 21.8 million users access the internet everyday and the highest average time spent is 34.4 hours per user per month (comScore, 2004). With the vast number of users connected to the internet, securing their information and computer from being misused is very important and safety measures must be considered to ensure optimum protection. We shall consider the number home users using insecure computers before we talk about the way the users perceive the concept of online security. NetSafe's Home Computer Security Survey conducted in 2005 reveals that 41% of the respondents have an updated firewall and 59% do not use a firewall for computer security at all. 70% of the respondents do not have updated firewall and anti-virus applications (The Internet Safety Group 2005).

According to a survey report from Message Labs conducted in June 2006, one in 101 emails in June contained malware and one in 531 emails comprised a phishing

attack. The global Spam rate was identified to be 64.8% (Message Labs Intelligence, 2006).

According to a survey conducted by AOL and National Cyber Security Alliance 81% of home computers are lacking important computer security applications like Anti-Virus and Firewall applications out of which 64% users were using broadband Internet connection (American on Line/ National Cyber Security Alliance, 2004).

Home computers lacking core protections (recently-updated anti-virus software, a properly-configured firewall, and/or spyware protection)	81%
Home computer users who have received at least one phishing attempt via e-mail over the prior two weeks	23%
Home computers lacking current virus protection (not installed or not updated in prior week)	56%
Home computers lacking properly-configured firewall	44%
Home computers lacking any spyware protection software	38%

Table 1: Home users lacking security features (AOL/NCSA Survey Report, 2005)

Above shown table is a summary of the AOL/NCSA survey conducted in 2005. The survey included 225 broadband users and 129 dial-up users. It is apparent from the figures that not many users are able to configure the security software applications. Only 17% of the respondents understood the concept of firewall and how they work and 92% were unaware of spyware applications that were installed in their computers. This survey results discussed above shows the importance of security for home users. From the above results it can be analyzed that most of the home users are not completely aware of how to handle their personal computers. To make the home users aware of how to use the internet, some organizations are trying to provide security guidelines.

4 Security Guidelines

Security guidelines are helpful to reduce the risk of protecting home user's computer, personal and confidential information. Security guidelines for online safety can be found of many websites that educate the users to deploy security principles. Governing bodies and legislation should make sure that the security guidelines are effective and are up-to-date to the present level of threats and vulnerabilities that home users are exposed to. Security principles are useless if they do not reach the home users and media presentation and awareness programs should be tactically presented to educate the users. There are plenty of advisory website where users can

find information about online security including banking websites and security software vendors. Few of the well known sources that offer security information are presented below.

4.1 Get Safe Online: 10 Minute Guide for Beginners (Gets Safe Online, 2007)

This website provides information for home users on how to upgrade the Operating System; it provides series of advices on topics such as firewalls, antivirus, spyware, spam, backups and identity theft etc.

4.2 Symantec Best Practices for Consumers (Symantec Corporation, 2007)

Symantec Corporation has designed a set of guidelines for consumers/home users ensure optimum online security. The following are some of the guidelines that are provided by Symantec. Passwords should be made secure by mixing upper and lower case alphabets and numbers and should not be chosen from a dictionary. Vulnerability checks should be regularly done by using Symantec Security Check at www.symantec.com/securitycheck and user can report cybercrime incidents to get themselves involved in fighting crime.

4.3 Microsoft (Microsoft/ NSCA, 2006)

The National Cyber Security Alliance with the support of Microsoft Corporation has come up with Online Security and Safety Tips, they are as follows. Home users should make use of a firewall application if they did not get it along with the operating system they are using. Along with the firewall application, it is recommended to keep a back up of important documents and files for safekeeping. Parental control applications should be considered if kids are able to access the internet. Anti-spyware applications should be installed to prevent/remove spyware applications. These are some of the safety tips mentioned by Microsoft.

4.4 Discussion

The following tables give a clear picture of the level of information that is offered by Getsafe, Symantec and Microsoft. This table explains how far the users can educate themselves using these sources and decide on which source to rely for future security guidelines.

	Anti-virus	Anti-Spyware	Spam Sense	Backups	Wireless Networks	Online Auction	Identity Theft	Linux/ MAC Users
Getsafe	✓	✓	✓	✓	✓	✓	✓	✓
Symantec	✓	✓	X	X	X	X	✓	X
Microsoft	✓	✓	✓	✓	X	X	✓	X

	Passwords	Parental Control	Intrusion Detection	Vulnerability Assessment	Crime Reporting	OS Updates	E-mail Attachments	Firewall
Getsafe	✓	X	X	X	X	✓	✓	✓
Symantec	✓	X	✓	✓	✓	✓	✓	✓
Microsoft	✓	✓	X	X	X	✓	✓	✓

Table 2: Comparison of Security Guidelines

Getsafe perhaps offers a clear and easily understandable set of guidelines for home users and the website cares for Linux and MAC users too which Symantec and Microsoft fail to. Getsafe and Microsoft guidelines do not concentrate on reporting the security incidents and Microsoft amongst the three sources talks about parental control applications. Getsafe offers assistance in protecting wireless networks and tips for users who do online shopping whereas the other two sources does not mention about it. On the bigger picture, all three sources concentrated on the main aspects that include OS Updates/Patches, Firewall, Anti-virus, Anti-Spyware, Identity Theft, Password Management and Email attachments

5 User awareness

Security information is vast and easily available on the internet but how many users are aware of them or at least aware of threats they are posed while connected to the internet? According to the survey by AOL/NCSA in the year 2005 (225 broadband users and 129 dial-up users), only 22% of the respondents felt safe from online threats and 61% were somewhat safe. Some of the other key results of the survey are as follows they are 56% of the respondent had never heard of the word “Phishing”,

61% of them received phishing attempt, 70% felt the phishing mail as legitimate, only 23% knew the difference between a firewall and anti-virus application and only 56% had anti-virus application and 44% had updated within past one week (American on Line/ National Cyber Security Alliance, 2004). The main reason behind this lack of awareness among home users is because of media awareness programs. The organizations are mainly focusing upon the websites to promote awareness, there are no proper TV programs and the security awareness issues are not published in news papers normally, unless or until any attacks on identity thefts has occurred. The only way to learn user about internet security is internet itself, there should be more than one way to know about internet security this should be either mass awareness media such as news papers, posters, which should be displayed in public places. The results shown clearly indicate the need to improve security awareness techniques.

6 Security improvements

Effective ways of making users aware of the internet threats is perhaps the only way to fight the battle against cybercrime. Unfortunately, users are failing to reach the online resources that are meant to help them protect their own information/computer. Unaware of the threats, users are easily being trapped with which cybercrime is rapidly increasing. The role of governing authorities should be more than just making websites to promote awareness amongst the users and create security posters/leaflets. The Information security awareness program should be such a way that it should reach all sorts of home users including the ones who use the internet only to send and receive mail.

According to the European Network and Information Security Agency, information security awareness programs will (European Network and Information Security Agency, 2006):

- Communicate and motivate users to deploy security guidelines/ practices.
- Offer general and specific information about information security risks and controls.
- Make users aware of the responsibilities in securing their information.
- Minimize security breaches and create a stronger culture of information security.

Communication techniques should be very effective so that the users are forced to learn the security guidelines and making them aware that there is nothing important more than securing themselves from online threats. Examples of past security breaches/incident should be presented which users often remember easily and it spreads faster with word of mouth. The effective security awareness program should have the following set of qualities (European Network and Information Security Agency, 2006)

- Reach as much as users as possible ranging from novice users to IT professionals.
- Awareness should not be alarming; users should be educated in a simpler manner.
- It should bring users a good level of confidence.

The awareness being delivered, the media used and the person who is promoting the awareness must be influential and credible. If not, the users may not show good interest in listening.

More than one communication media must be used so that the users can reach the awareness easily.

Banks, community centres, computer dealers, educational institutions, libraries and universities can be used to deliver user awareness.

7 Recommendations

Based upon the following set of principles mentioned by European Network and Information Security Agency, this paper recommends new ways to improve home user perception on online security aspects and the ways the media presentation could be improved by the governing bodies and security software application vendors.

7.1 Perception Improvements

There are several ways in which the existing media awareness techniques can be improved thereby educating the users and making them aware of threats and vulnerabilities they are at which in turn changes the way the users perceive the trends of online security. This paper has made an effort to make some more media awareness methods apart from the ones mentioned by European Network and Information Security Agency, some of the guidelines are as follows:

Text Messaging: Mobile phone service providers should offer regular updates about the latest threats through text messages upon agreeing with the users. This could either be offered free of cost or at a nominal price. Text messages should be short, informative and educative and for more information, users must be advised to check advisory websites like Symantec or McAfee. There are 45 million (84% of the population) mobile phone users in the UK [Mobile ownership in the UK] and upon an agreement with the users and ISP, governing authorities should be able to spread a good awareness on information security as this will reach 84% of the population in the United Kingdom.

Public transport: Public transport vehicles should present the security tips in a simple and easily convincible way so those users who are commuting could have a glimpse of them if they are interested.

Bank Websites: Banking websites should offer security tips just before the users log-on to online banking website. Users should be forced to go through the security guidelines before entering into the website. This however will become annoying for users when they become familiar with security measures. This could be overcome using the *"skip"* option so that the users who are aware of security guidelines can skip the section and process with log-on process.

Comics: Comics usually attract younger generation and this will be an ideal way to implant security awareness from childhood. However, comics will have difficulties to convey complete messages but it is possible to design comics in such a way that it offers complete awareness. Children would read comics and discuss them with their parents through which there is a possibility that the older generation will learn too.

The proposed methods to improve the existing media awareness techniques will reach more audience at all age and with varying knowledge on computers and information security. The governing bodies, security software vendors and the media should come to a common understanding in promoting internet security amongst home user and implement them so as to bring the cybercrime activities down.

7.2 Security Guidelines

The research paper would like to present few improvements that could perhaps increase the level of user awareness about online security. Some of the improvements are mentioned below:

Shareware/Freeware/File sharing applications: These applications are often bundled with viruses, worms and Trojan horses which will get installed along with the application the user is looking for. This will be usually mentioned in the end-user agreement that is displayed during the installation process. User must read the agreement completely, carefully and if they feel they are at risk the application should not be used and instead look for a similar application from a well known source that is free from threats.

Phishing websites: User should clearly understand the techniques used in phishing attacks and be able to easily differentiate legitimate and phishing websites.

Spam: Users should learn what spam and how spam mail looks like. They should be careful whilst dealing with mail that may be spam and delete them if the mail is not from a known source.

The above mentioned set of security guidelines will serve the need to secure user's information that are exposed to the internet threats and also to help protect their computer system. Users will learn the security aspects when they make themselves available for the media that are promoting security awareness. The mixed combination of security applications like anti-virus, anti-spyware and firewall will offer a highly secure internet experience

8 Conclusions

Security guidelines for home users are vast over the internet. Many websites offer simple and very easy to understand guidelines and yet the users are not able to reach those websites. The relatively new threat Phishing, is getting unnoticed among home users and they are tactically forced to submit their personal and banking details. Home users have their own perception theory when it comes to submitting their banking details over the internet. Trust plays an important role in online transactions and some users are even ready to take risk. Media presentation and awareness plays an important role for users to understand the "Do's and Don'ts". The recommended security guidelines would perhaps strengthen the existing levels of security the home users deploy. Users should educate themselves from the resources available as it is their own responsibility to secure their information.

Future work would be to implement the recommended set of media awareness methods that will help users learn and educate themselves with online security techniques that are mentioned earlier in the report. Knowledge on Phishing could be made aware of into a greater depth to a group of people and later conducting a survey to evaluate their perception on phishing websites. A similar approach could be used to evaluate the home user's perception on spyware and malware after they are made aware of them. Key points for future are, making users aware of spyware applications and phishing websites and evaluate their perception, media awareness can be implemented with the new methods proposed and evaluate the effectiveness of the same and Web applications like the Internet Explorer and mail clients like MS Outlook could be designed in such a way that they are more secure and flexible giving the users more freedom and security.

9 References

American on Line/ National Cyber Security Alliance, "*AOL/NCSA Online Safety Study*", 2004. www.staysafeonline.info/pdf/safety_study_v04.pdf. Date Accessed 18/03/07

BBC Presentation, *"Life of Crime Part 5"*, 2001. http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm, Date Accessed: 21/05/07

ComScore, *"Review on pan-European Online Activity"*, 2007. http://www.comscore.com/press/release.asp?press=1459 Date Accessed: 18/07/07

European Network and Information Security Agency: "A User's guide: How to Raise Information Security Awareness", 2006.

Gets Safe Online, *"10-minute guide for beginners"*, 2007. http://www.getsafeonline.org/nqcontent.cfm?a_id=1179 Date Accessed: 23/06/07

The Internet Safety Group, *"NetSafe Survey"*, 2005 http://www.netsafe.org.nz/Doc_Library/download/2005_ISG_home_computer_security_survey_summary.pdf. Date Accessed 12/05/07

Message Labs Intelligence, "*Going Up, Going Down!", 2006.* http://www.messagelabs.co.uk/mlireport/2006_annual_security_report_5.pdf Date Accessed: 16/06/07

Microsoft/ NSCA, "Online Security & Safety Tips", 2006 http://www.staysafeonline.org/basics/resources/MicrosoftHomeUserGuidebook.pdf Date Accessed: 13/06/07

Mobile ownership in the UK, http://www.dhaliwalbrown.com/knowledge/UK_Mobile_Market_Statistics_2006 Date Accessed: 20/07/07

Symantec Report, *"A Monster Trojan"*, 2007. http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html Date Accessed: 20/08/07

Symantec Corporation, *"Symantec Internet Security Threat Report"*, 2007. http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf Date Accessed: 26/07/07

Cyber Terrorism – Electronic Activism and the Potential Threat to the United Kingdom

A.Wareham and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

The recent rise of anti-terrorist action in response to deemed terrorist organisations has been a major international concern, prompting military action as well as domestic reforms by the United Kingdom since the attacks of 2001. In addition to the physical threat of terrorist activities, the utilisation of computer systems and services to promote a further threat has also become a point of significant interest. Dubbed 'Cyber terrorism' by government groups, media agencies and specialist software and hardware manufacturers the potential risk of 'e-activism' has seemingly increased, most notably of all due to widespread adoption of the Internet.

However, it is relevant to ask what we actually know about 'cyber terrorism', and whether it actually poses a realistic threat to the United Kingdom. This paper discusses the various aspects of activism online, utilising analysis of cited attacks to examine the methods and impact of direct pressure at both the corporate and national level.

Keywords

Electronic Activism, Cyber Terrorism, Terrorism, Activism, Hacktivism, UK Threats, Intimidation & Influence

1 Introduction

The issue of cyber terrorism has grown considerably in the public eye since the events of 9/11, the issue of security and the potential for the spread of Internet-based threats receiving further attention as the issue of 'home grown' activism continues in the current public media. The motivation of such threats is not purely limited to religious idealism; the considerations of moral, ethical and political standpoints have their own parts to play, with examples of such efforts giving rise to this current paper.

The presence of activism on the Internet is a problem that requires more than simply analysing the potential technical attack methods, with considerations on social factors, legal issues and present legislation, the current UK defence policy to electronic attack and numerous other factors. We shall briefly look at a few core areas in order to draw a more informed opinion.

2 The Reach of Electronic Activism

Since its inception, the Internet has been a natural conduit for the exchange of ideas, evolving from the early ARPANET into a global phenomenon. The widespread acceptance of the web into the public spectrum has created a universal resource for business, community support, education, finance and the handling of the affairs of government; a link to the outside world which is becoming increasingly important in everyday life.

So what does this essentially offer online groups who wish to promote themselves and their ideals, and who may find it difficult to do so due to the exposure of potentially illegitimate activities? The rise of 'public' Internet provides a number of opportunities for any group who wishes to centralise their activities online, both in terms of services and environment:

- *Operations Support* - The ability to build and maintain the necessary 'command network' from which to operate as a cohesive group, a consideration especially important when considering the large global geographical and transnational spread of potential large-scale efforts.

- *Anonymity* - The ability to "hide in the anonymity of cyberspace" (Jones, 2005), allowing potential planning, co-ordination and actions to be overlooked until the goal has been completed.

- *Personal 'Safety'* - The ability to use considerations of anonymity from which to operate, a potential benefit and incentive to less 'driven' orchestrating groups or lone individuals.

- *Publicity* - The ability to publicise objectives, viewpoints and motivations for the purpose of informing, persuading and the incitement of propaganda, coupled with the maintaining of a desired 'public image' to validate or support operations and ideals.

- *Financing* - The ability to maintain continued operations through continued financing, through both donations and the utilisation of legal or illegal credit transactions

2.1 The Community

The Internet has a substantial capacity to further and support community elements in commerce, entertainment and academia, with social networking sites and privately managed communities forming to focus on innumerable topics of interest. The majority of these groups offer a benign and harmless outlet for the free exchange of ideas. However, the online community can offer its own potential dangers, and the ways in which services can be utilised depend largely on the needs of the group in question. For many the ability to publicise information regarding their goals and

aspirations, if only in a few brief paragraphs, is a basic component of web presence; perhaps even their main or only point of contact with the 'outside world'. A further necessity for many established communities is a need to authenticate users in order to view more pertinent information of interest, commonly in the form of membership or some other standardised process so that access to key services can be achieved. The same considerations also are in existence when considering the issue of activism, the balance of organisation and co-ordination processes with the presentation of intended material for the general public, whilst ensuring that sensitive and potentially incriminating information is secured. The overall cost provisions in terms of infrastructure are for the most part negligible, with tools such as IRC, phpBB and instant messaging systems providing flexible and free options for communication. The introduction of secure data using such tools as PGP adds further credence to the management of 'closed' community environments, systems which can cause significant headaches for policing and the security services. As a case in point, in 2006 the Serious Organised Crimes Agency (SOCA) found itself essentially foiled by the use of encryption during the raid on an ID theft ring, the estimated time to break the encryption "taking 400 computers twelve years to complete" (Espiner, 2006).

2.2 Influence and Intimidation – the Power of 'Reality'

The ability to influence the viewing audience effectively is a significant issue when considering the nature of electronic activism. The ability to 'prove' or 'disprove' specific information, as well the legitimising of actions, provides activists a certain amount of validity to justify intent, such as the committing of actions that may otherwise be viewed to be entirely inappropriate in the public spectrum.

Influence Type	Approach	Influence Strategy
Propaganda	Wide-scale	Sociological principles reinforcing cultural or social values
Persuasion	"Personal"	Psychological principles and arguments

Table 1 : A table denoting the differences between the two primary classifications of influence (Hutchinson, 2007)

Hutchinson (2007) explains the basic considerations of *propaganda* and *persuasion* in the common presentation of ideas, the subtle difference between the two methods highlighted in Table 1. The processes of each are self evident in numerous online publications and on a range of media, with services such as *YouTube* providing an ideal host to portray supportive material to capture the global audience. The ability to create 'realities' through the submission of convincing and relevant material allows for the swaying of public opinion, enhanced further by the provision of community groups to strengthen given perceptions. Arguably this is not a new concept; indeed the reinforcement of values, ethical principles, ideology and given

arguments can be seen in virtually every current mainstream religion and Government across the globe. The main difference we can see when considering electronic activism is that the adoption of full media web services allows for the presentation of emotionally driven material that can both support activist efforts and separate the target from perceived legitimate protection.

2.3 Utilisation of electronic activism in offensive scenarios

The following is a brief review of two separate acts against corporate and national entities, in order to highlight the scope and capability of electronic activism.

2.3.1 National Considerations - The Estonian Dispute

An example that highlights the potential threat of a national attack is provided by events in April and May 2007, which demonstrated the potential impact of activism on a national scale. The relocation of a Soviet war memorial in the City of Tallinn sparked a high profile conflict with both the Russian Federation and ethnic Russians living within Estonia; the apparent catalyst for the later attacks on Government services and infrastructure. The attack sustained for a number of weeks, with Table 2 emphasising the range frequency of attacks committed during a monitored period.

Attacks	Destination	Address or owner	Website type
35	"195.80.105.107/32″	pol.ee	Estonian Police Website
7	"195.80.106.72/32″	www.riigikogu.ee	Parliament of Estonis website
36	"195.80.109.158/32″	www.riik.ee	Government Information website
		www.peaminister.ee	Estonian Prime Minister website
		www.valitsus.ee	Government Communication Office website
2	"195.80.124.53/32″	m53.envir.ee	Unknown/unavailable government website
2	"213.184.49.171/32″	www.sm.ee	Ministry of social affairs website
6	"213.184.49.194/32″	www.agri.ee	Ministry of agriculture website
4	"213.184.50.6/32″		Unknown/unavailable government website
35	"213.184.50.69/32″	www.fin.ee	Ministry of finance website
1	"62.65.192.24/32″		Unknown/unavailable government website

Table 2 : Figures highlighting a range of targeted websites over a captured period (Nazario, 2007)

The thought that Estonia is heavily dependent on the Internet to support government, civil and financial institutions is indeed concerning, considering that Estonians "pay taxes online, vote online, bank online (and that) their national ID cards contain electronic chips" (Applebaum, 2007). This means that an effective *Denial of Service*

attack increases in the potential effect on a target as the sophistication of the target increases (a concerning trend due to a similar embracing of technology in the UK).

The sheer fact that the Estonian government brought the issue before NATO as a legitimate attack on its sovereignty highlights the validity and seriousness of the incident, not merely as an annoyance but most certainly as a full blown attack in its own right. The response from NATO Secretary General was that of voiced condemnation over the incident (Estonian Government, 2007), although further action was not clearly identified.

2.3.2 Corporate Considerations - Huntingdon Life Sciences

Animal research and testing has long attracted the attention of animal rights activists on both a national and transnational level. One such group, the *Stop Huntingdon Animal Cruelty* activist group (Affiliated with the international group PETA), has been involved on numerous occasions with illegal activity, primarily in terms of physical actions such as the storming of target offices and direct intimidation methods of targeted personnel.

Analysis of legal case reports from March and May 2004 highlights a variety of offences against the HLS facility and its personnel, with the documents demonstrated a joint campaign of both physical and technical threats to continued operations. The usage of phone, fax and email blockades, the interruption of mobile phone services and the harassment of affiliates were identified as the primary forms of technical attack, and although extremely basic, these methods proved enough in conjunction with physical efforts to drive away a number of investors. Indeed, the intended "impacting (on) Huntingdon's bottom line" (QB, 2004) as voiced by one of the defendants was an important part of many of the highlighted public comments, with the viewpoint of potential prison sentencing being "a small price to pay". (QB, 2004). This highlights understandable concerns over legal steps when attempting to deal with persistent or repeat offenders, especially when considering that one of the defendants in the reviewed cases highlighted legal action as being "laughable because we will find a way around it" (QB, 2004).

3 Defending the Realm

The primary recourse against actions committed has been that of the law, specifically in the case of terrorism (and thereby potentially most applicable to defined activism) three laws in particular, namely the *Terrorism Act 2006*, the *Prevention of Terrorism Act 2006*, and the *Anti-Terrorism, Crime & Security Act 2001*. Table 3 highlights the powers that these deliver, with the Terrorism Act in particular referencing *Internet* activities. This is a significant tool when combating potential aggressive forms of electronic activism, referencing key issues that (especially in terms of the HLS example) can be applied to situations where a particularly aggressive threat may be present. Further to the list in the Table, the RIPA Act 2000 further requires the handover of all keys and information relating to encrypted data for investigation, with a potential prison sentence for up to 5 years should there be any issues of

National Security (Home Office, 2007). As highlighted by the example of encryption employed against SOCA investigations, this may not be a large enough incentive should the potentially discovered information lead to a greater sentence. However, this covering period provides a mechanism to legally charge and detain potentially disruptive or dangerous elements.

Act	Focus
Terrorism Act 2006	Designed to combat: • Planning of Terrorist Acts • Encouragement of Terrorism • Dissemination of Terrorist Publications • The Training of Terrorists
Prevention of Terrorism Act 2006	Designed to: • Impose sanctions on specific suspects including the introduction of control orders • *Note: carried out in accordance to the EHCR and authorised directly by the Home Secretary*
Anti-Terrorism, Crime & Security Act 2001	Designed: • Combat Terrorist funding operations • Extend police powers

Table 3 : An overview of key UK anti-terrorism laws

3.1 The Structure of National Defence

The overall defence of UK infrastructure and interests is largely under the jurisdiction of the Home Office, assisted by independent groups such as the Joint Intelligence Committee (JIC) in the development of a suitable overall strategy. This structure is illustrated in Figure 1.

The four core groups that deal with the main body of the UK infrastructure and assets (CSIA, 2007) are as follows:

- CESG: a cabinet body catering primarily to the advisory of government groups and departments,
- CSIA: an arm of GCHQ which primarily focuses on the protecting of national information systems,
- CPNI: an arm of MI5 which focuses on protecting the UK's infrastructure from Electronic Attack

- SOCA: a progression from the now defunct National High Tech Crime Unit which deals with primarily high level crime / high impact crime.

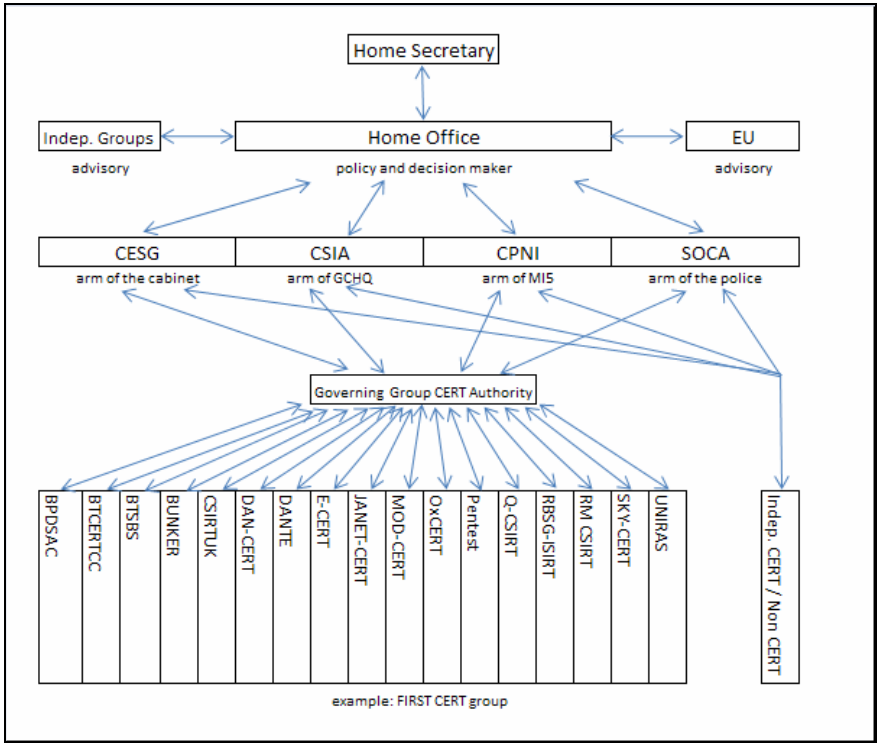


Figure 1 : A Basic Overview of UK Defence structure

These groups work together in order to protect against potential attack, as well as to ensure that information policy is maintained. Below these groups operate the various CERT and CSIRT teams that operate to protect key areas such as banks, infrastructure businesses, educational facilities or government concerns. These operate either independently or operate in mutually beneficial co-operative organisations such as FIRST. Overall this gives a reasonable level of infrastructural security, operating on a tiered basis in which each party can consult others for mutual support, development, education and protection whilst alleviating stress on Government groups.

4 Discussion and Conclusions

Overall, the considerations of activism highlight an embrace of basic attack methods in order to *deny* the target its communication capability, either in conjunction with defamation attacks as used in the Estonia, or by the usage of intimidation as prescribed by the events of the HLS case. The utilisation of electronic activism as a communication method provides opportunities for the conversion of others to a

similar way of thinking, facilitating both potential recruitment as well as an escalation of the impact of activities due to greater public support. The natural qualities of the Internet and the provision of free products and services mean that implementations for activist groups require little financial input, with the potential of utilising financial services such as *Paypal, Western Union* and even online virtual environments such as MMOGs (Massively Multiplayer Online Games) and *Second Life*. The nature and protection afforded by authenticated 'closed' community environments means penetration by law enforcement can be difficult, and even further impacted by the possibility of free encryption methods.

The more aggressive forms of activism could be charged under anti-terrorism laws, with national infrastructure measures in place to counteract any wide-scale attack. However, these methods are for the most part reactionary responses rather than proactive methods, essentially waiting for the activist to make the first move. We have identified that legal consequences may not be a silver bullet to activist attacks, especially when the attacker feels that they report to a 'higher authority' based upon moral, ethical or religious grounds. The issue is compounded when considering that the previous head of MI5 Dame Eliza Manningham-Buller highlighted the nature of the UK's proactive surveillance activities, citing a lack of manpower in relation to the threat (BBC, 2006). Following the bombings of 2005, the question over the sacrificing of certain civil liberties highlighted the difficulty in balancing measured security with effective security over the general 'terrorist' threat.

We have identified that, although technical methods have been provided for, the issue of human-orientated attacks are a far harder issue to combat. The problems of intimidation and threats, although far smaller in terms of the potential target radius, can negate common methods of protection. With the focus of the attack on the user, the threat of disseminating personal information to friends, family and business relations in order to invoke an emotional response is a common tactic; and one that was used against key directors and target business partners within the HLS example. With the impracticality of segregation and the screening of emails and similar forms of contact (one of the only real defences against the human side of activism), an effective solution would seem to require a blend of protective considerations:

- The implementation of an effective security policy for staff, assets and information systems at both a corporate and government level,

- The confirmed civil and government enforcement of contraventions regarding either security breaches or acts of an activist nature,

- The assigning of responsibility to service providers for the usage of the services they provide

One of the best potential solutions to the issue of electronic activism is the alerting of consciousness and the enabling of dis-inhibitors; key principles initially defined in a UK Home Office report on the future of net crimes. The ability to influence the general public that the *action* of vigilantism (even if justified by some moral, ethical

or religious concept) is wrong will potentially offer a solution, either by directly influencing the potential activist or by inciting peer pressure through others to search for a more peaceful solution to grievances. Although this is an unlikely solution outside of the UK bar that of a global initiative, such steps could help on a more local level though the pacification of UK activist groups.

It is perhaps unsurprising that utilising the same tactics that threaten national interests also seemingly offer a potential solution to future attacks.

5 References

Applebaum, A (2007), "For Estonia and NATO, A New Kind of War", *The Washington Post*, 22 May 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101436.html (accessed 28/07/2007)

BBC (2006), "MI5 tracking '30 UK terror plots'", BBC News online, 30 November 2006, http://news.bbc.co.uk/2/hi/uk_news/6134516.stm (accessed 19/07/2007)

CSIA (2007), "Key organisations", Central Sponsor for Information Assurance, Cabinet Office, http://www.cabinetoffice.gov.uk/csia/key_organisations (accessed 12/08/2007)

Espiner, T. (2006), "ID theft gang thwarts police with encryption", ZDNet News, 18 December 2006, http://news.zdnet.co.uk/security/0,1000000189,39285188,00.htm (accessed 17/10/2006)

Estonian Government (2007), "NATO Secretary General to the President of the Republic: the alliance supports Estonia", Government Communication Office Briefing Room. 3 May 2007. http://www.valitsus.ee/brf/?id=283225 (accessed 27/07/2007)

Home Office (2007), "Frequently Asked Questions", Regulation of Investigatory Powers Act, http://security.homeoffice.gov.uk/ripa/encryption/faqs/ (accessed 28/08/2007).

Hutchinson, W. (2007), "Using Digital Systems for Deception and Influence", in *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2007)*, Plymouth, UK, 10 July 2007, pp79-86.

Jones, A. (2005), "Cyber Terrorism: Fact or Fiction", *Computer Fraud and Security*, June 2005, pp4 – 7.

Nazario, J (2007), "Estonian DDoS Attacks: A summary to date", 17 May 2007, Arbor Networks, http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date (accessed 27/07/2007)

QB (2004), EWHC 493 *'Chiron Corpn Ltd and Others v Avery and Others'*, section 21

Section 3

Communications Engineering and Signal Processing

Radio Optimization in GSM Network

M.H.Chu and M.Z.Ahmed

University of Plymouth, Plymouth, United Kingdom
e-mail: m.ahmed@plymouth.ac.uk

Abstract

The main aim of this paper is investigating radio optimization in GSM network. Radio optimization includes four phases which are building radio quality indices, monitoring network performance, identifying and analyzing network problems and applying proposed solutions to existing network. Optimization procedure is investigated and illustrated by one practical case study. That case study is implementing optimization in Haiphong city in the North of Vietnam by using real data and statistics provided by Vinaphone Company. Three main problems are found out together with corresponding solutions.

Keywords

GSM, radio optimization, drive testing, network, monitor, coverage, capacity, quality, mobile, interference, handover

1 Introduction

Radio optimization is one of the most challenging works in network maintenance. Many factors in cellular environment affect radio network such as interference, multi path problems or raining and temperature. Optimization procedure is produced to well organize optimization activities and should be adapted with network development and state of the art technology. This paper concentrates on optimization procedure and its main problems as well as general solutions. Paper uses data and statistics of Vinaphone network provided by Vinaphone Company in Haiphong city in the North of Vietnam to illustrate one typical example of optimization.

The paper includes four main parts which are introduction, background, analysis and conclusion sections. Introduction section reviews the scene of radio optimization together with problems mentioned in this paper. Background section provides general knowledge about radio optimization works, from procedure to common problems and solutions. In analysis section, a typical optimization work is described together with real data, graph and solutions. Conclusion section is in the end to summarize key points in radio optimization.

2 Background

Radio optimization are defined as all activities to better improve radio network, it can include deploying relevant techniques in particular phase of network deployment

or identifying and solving quality problems. In a certain context, optimization also contains radio planning functionalities to effectively integrate new radio element to existing network.

In general, radio optimization can be divided into four continuous phases. In first phase, key performance indicators (KPI) are built in agreement between network operator and vendor to exactly reflect network performance. Typical indicators are dropped call rate (DCR), call setup success rate (CSSR), handover success rate (HSR) and TCH (traffic channel) blocking rate. KPIs are then used in monitoring phase to compare desired values with real ones to find out network problems. In monitoring phase, there are some useful methods to monitor radio network. Computers in operation and maintenance centre (OMC) are used to online monitor network. Signaling between OMC and network elements allows operator to monitor network performance as well as make a change to radio parameters by using man machine language (MML) software. However, this method cannot bring any field information about network problems. Driving test is issued to solve that problem. Driving test uses the field investigation tool (TEMS), positioning tool (GPS), laptop, mobile phone and relevant software to investigate radio problem at particular location. Another method is using network analyzer tool to trace network messages in radio interface. Alarm monitoring can be used to detect hardware problems (Mishra, 2007).

Network auditing is a third phase and also the most important one. Network auditing includes data analyzing and solutions producing. Input data for analysis is statistics from online monitoring and driving test. Two main problems in radio network are frequency and coverage. Almost attention is concentrated on handover problems, dropped calls, interference and call setup success rate. Co-operation with another team such as core and transmission teams is required to better analyze problems. Network upgrading phase is followed to implement proposed solutions from network audit to existing network together with permanent monitoring to observe follow-up network response. Adding new feature is proposed as new phase to well integrate new feature such as GPRS and EDGE on top of GSM network to compete with other GSM operators and satisfy customer demand.

Many techniques can be used to improve network performance in terms of coverage, capacity and quality. Frequency re-use is commonly used to make efficient use of frequency resource; same frequencies are deployed after certain distance to avoid interference. The more close the re-use distance, the higher the network capacity and interference. Frequency hopping is used to reduce interference, thus enables more close frequency re-use pattern which in turn increases network capacity. Frequency hopping schemes including base band hopping and synthesizer hopping are deployed depending on network development and equipments. Synthesizer hopping is a new scheme and has more advantages than base band hopping. However, some old equipment does not support synthesizer hopping. Antenna solutions are used to combat with interference and improve radio coverage. Space diversity and polarization diversity are used in antenna system to combat with multi path problems and interference. Polarization diversity is preferred because it uses less antennas and

space occupancy than space diversity system. Down tilting, azimuth and other parameters fine tuning are considered to improve radio coverage. Another solution to increase coverage quality is using multi layer system. Multi layer system uses three types of cells which are macro cells for remote areas, micro cells for city areas and pico cells for indoor areas. To improve radio quality, multi rate is used to combat with interference and error transmission. In multi rate solutions, full rate, half rate and adaptive multi rate (AMR) solutions are commonly used. Half rate can be used to reduce congestion because it provides a double number of voice channel in compared with full rate mode. AMR is used in high interference environment; bit rate of channel coding is increased to combat with higher interference and error (Chu, 2007).

3 Analysis

An example of optimization in reality is shown to illustrate optimization theory and background. This case study is optimization in Haiphong city, one small modern city in the North of Vietnam. The data is provided by Vinaphone Company, the owner of Vinaphone network in Haiphong city. Solutions are proposed and highly dependent on data and statistics availability.

Case description

- Optimization location: Haiphong city and its city centre
- Time: the middle of September 2004
- Operator: Vinaphone Company.
- Hardware equipments: BTS from Motorola vendor including Horizon, Horizon-II and M-cell 6 types.
- Investigation tools: TEMS W600i, TEMS investigation 7.1.1 software, laptop, two mobile phones, two Vinaphone SIM cards, GPS tool, MapInfo 7.0 software, OMC monitoring software.
- Route of drive testing: main roads of Haiphong city and high traffic areas.

(Chu, 2007)

Table 1 shows the network performance of BSC102M which serves overall coverage of Vinaphone network in Haiphong city. Three biggest problems of BSC102M at given time are low call success rate, high dropped call rate and low handover success rate. Statistics at cell level are produced to determine those problems at BSC102M are on small area or large area. Hardware alarm monitoring is investigated to exclude hardware fault.

Table 2, 3, 4, and 5 list cells having bad quality regarding to call setup success rate, handover success rate, dropped call rate, TCH blocking rate, respectively. The geographical location of those cells is identified in Vinh-Bao, Tien-Lang, An-Lao and Thuy-Nguyen district in Haiphong city. Bad quality in handover and dropped call performance suggests coverage investigation and frequency review; interference is another main cause of high dropped call rate therefore frequency review can

identify and reduce interference. High TCH blocking rate suggests network re-configuration. Low call setup success rate requires further analysis about signaling messages of call establishment. In scope of this paper, only frequency review, coverage and handover investigation are expected. Driving test is used to investigate network coverage in overall city and handover performance in wanted areas (Vinh-Bao, Tien-Lang, An-Lao and Thuy-Nguyen districts).

Date	Call setup success rate (%)	Call success rate (%)	Dropped call rate (%)	Handover failure rate (%)	Handover success rate (%)	Handover failure recover (%)	TCH blocking rate (%)
07/09	93.55	91.77	1.90	0.38	93.21	5.70	2.41
09/09	93.49	91.54	2.10	0.42	93.02	5.86	2.71
10/09	93.50	91.30	2.35	0.50	90.32	8.48	2.02
12/09	92.93	90.57	2.53	0.59	87.22	11.27	0.97
13/09	93.31	90.97	2.51	0.54	87.98	10.91	1.66
14/09	93.40	91.11	2.45	0.53	88.06	10.74	1.00
15/09	93.26	90.99	2.44	0.55	88.16	10.64	1.60
Average	93.35	91.18	2.33	0.50	89.71	9.09	1.77

Table 1: Network health check at BSC102M (BSC level) (Vinaphone Company, 2007)

Cell name	Cell ID	Call setup success rate
Kien-An_1	2051	86.04
Kien-An_2	2052	89.28
Doi-66_3	2123	75.63
An-Hai_1	2221	82.39
Phan-Boi-Chau_1	2241	86.41
No-Mu-Ra_3	2113	90.95
Ngo-Gia-Tu_2	2372	91.56

Table 2: Cells having low CSSR (Vinaphone Company, 2007)

Cell name	Cell ID	Handover success rate (%)
Vinh-Bao_1	2151	56.73
Vinh-Bao_2	2152	61.18
Vinh-Bao_3	2153	44.55
An-Lao_1	2171	86.70
An-Lao_2	2172	56.93
An-Lao_3	2173	76.93
Tien-Lang	2280	39.90
Thuy-Nguyen_1	2091	87.21
Thuy-Nguyen_2	2092	90.68
Thuy-Nguyen_3	2093	91.44

Table 3: cells having bad handover performance (Vinaphone Company, 2007)

Cell name	Cell ID	Dropped call rate (%)
Doi-66_1	2121	5.51
Doi-66_3	2123	8.32
Vinh-Bao_3	2153	5.81
Cat-Hai	2279	5.35
Tien-Lang	2280	5.88
Kien-An_2	2052	5.13
Van-Cao_1	2181	2.47
Phan-Boi-Chau_1	2241	3.33
Phan-Boi-Chau_2	2242	4.14
Ngo-Gia-Tu_2	2372	3.56

Table 4: cells having very high dropped call rate (Vinaphone Company, 2007)

Cell name	Cell ID	TCH blocking rate (%)
Kien-An_1	2051	43
Kien-An_2	2052	22
Kien-An_3	2053	14.75
Minh-Duc	2160	40.18
An-Hai	2221	21.52
Doi-66_3	2123	33.65
Van-My	2062	21.2
Ngo-Gia-Tu	2371	26.6

Table 5: Worst cells having high TCH blocking rate (Vinaphone Company, 2007)

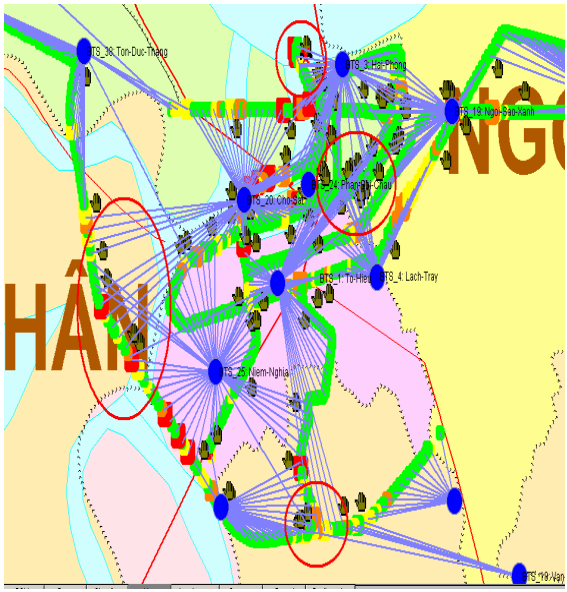


Figure 1: Coverage snail trail in Haiphong city (Vinaphone Company, 2007)

Figure 1 represents network coverage on main roads and high traffic areas in Haiphong city. Red circle areas show the overlapping and overshooting between cells coverage. Overshooting means signals from one site are shot to far sites coverage. In frequency re-use system, frequencies from overshooting site are probably similar to victim sites frequencies therefore cause co-channel and adjacent channel interferences. Overlapping is the two ways overshooting between source site and their neighbors, overlapping can increase handover requests and measurement report in overlapped areas which in turn degrade handover performance. General solutions to reduce overlapping and overshooting are fine tuning antenna parameters such as reduce antenna height, down tilting and reduce transmitted power.

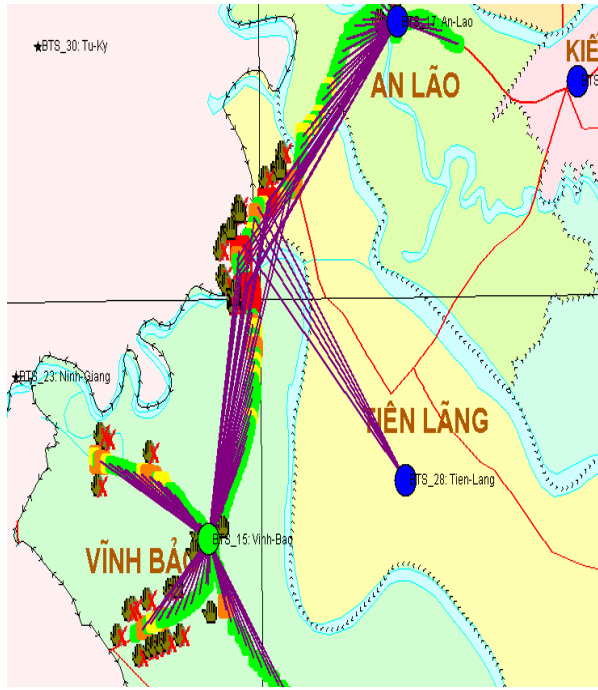


Figure 2: Handover of Vinh-Bao, Tien-Lang, An-Lao (Vinaphone Company, 2007)

In this paper, only handover investigation in Vinh-Bao, Tien-Lang and An-Lao is issued. Similar analysis can be applied to another area. Figure 2 shows many handover failures between those areas. Handover failures on large areas are mainly due to interference and bad coverage. Interference can be identified via driving test and statistics. Frequency review can reduce interference. Hardware-based solution is fine-tuning antenna parameters, power control parameters and adding new cells to improve coverage quality.

Source cells	Neighbour cells	Similar frequencies
Van-Cao_1	Lach-Tray1	18
Van-Cao_1	Lach-Tray1	20
Van-Cao_3	Niem-Nghia_3	26
Van-Cao_2	Do-Son	24
Ngoi-Sao-Xanh_1	Hai-Phong_1	514
Hai-Phong_3	Lach-Tray_3	30
Hai-Phong_3	Lach-Tray_3	32

Table 6: Cells and neighbours having same frequencies (Vinaphone Company, 2007)

Table 6 shows cells and their neighbor using similar frequencies which can cause severe interference between them. Frequency planning tool should be used to correctly change them. Adjacent optimization should be implemented to add necessary neighbor relation and delete unnecessary ones. It can be done via computer tools in database storage system. Frequency review and adjacent optimization can improve handover performance and reduce dropped call rate.

In configuration optimization, high TCH blocking cells should add more TRX or more cells in those areas whereas low traffic cell should dismantle unnecessary hardware and reinstall to high traffic cell as well. For example, table 5 shows 40.18% TCH blocking rate in cell Minh-Duc meanwhile it is Omni cell and has few carriers. That cell now must be configured in sectored cell with many carriers. Table 7 shows some cells having low usage of hardware in compared with designed values. Those cells must dismantle their inefficient TRX such as cell Cat-Ba_1 has 3.66 Erlang max usage in compared with 20.23 in design.

Cell name	Cell ID	Number of	Erlang max	Erlang design
Cat-Ba_1	2021	4	3.66	20.23
Hoa-Nghia_1	2361	4	6.02	20.23
Lach-Tray_3	2043	6	12.64	32.74

Table 7: Cells making inefficient usage of hardware (Vinaphone Company, 2007)

4 Conclusion

Optimization is defined as all operations to improve network performance in terms of radio, core and transmission network. Permanent works in radio optimization are monitoring radio quality, analyzing data and statistics about radio problems, and applying recommendations to network together with re-monitoring. Driving test and statistics are two key schemes to monitor and collect data about network performance. In above example of optimization, three main problems found are low call success rate, bad handover performance and high dropped call rate. The corresponding solutions are frequency reviewing to reduce interference and call drop, drive testing to investigate coverage quality which in turn improve handover performance. Call setup problems requires further analysis about signaling messages regarding to call establishment. Frequency and coverage are currently two biggest problems in radio optimization.

5 References

Chu, H. M. (2007) *MSc thesis about radio optimization in GSM network*. Plymouth: University of Plymouth.

Mishra, R. A. (ed.) (2007) *Advanced Cellular Network Planning and Optimization 2G/2.5G/3G...Evolution to 4G*. West Sussex: John Wiley & Sons Ltd, ISBN: 0-470-01471-7 (HB).

Mishra, R. A. (2004) Fundamentals of Cellular Network Planning and Optimization 2G/2.5G/3G...Evolution to 4G. West Sussex: John Wiley & Sons Ltd, ISBN: 0-470-86267-X.

Vinaphone (2007) *Private communication*. Vinaphone company, 57A Huynh Thuc Khang Street, Hanoi, Vietnam.

GSM Backhauling Over VSAT

M.H.Ghazanfar and M.Z.Ahmed

University of Plymouth, Plymouth, UK
e-mail: m.ahmed@plymouth.ac.uk

Abstract

Backhauling over satellites has become a customary and imaginative way to bring GSM services in geographically challenged areas where conventional terrestrial solutions are either not available or not suitable. This paper shall look at how GSM Network operators can save their OPEX (Operation Expenses) and bandwidth by incorporating the VSATs on SCPC and SCPC-DAMA. In addition to this, the impact of weather conditions on the overall connectivity. The paper will conclude on the benefits of what has been presented and the future of upcoming technologies such as DVB-RCS for satellites and WiMax.

Keywords

GSM, VSAT, Cellular Communications, Backhauling, Satellite

1 Introduction

This paper titled "GSM Backhauling Over VSAT" derives its concept from two technology white papers. The first was published by Alcatel as an Alcatel Telecommunications Review – 1st Quarter 2003. The paper titled as "New Opportunities for Satellites in Telecommunication Systems" discusses that how the new generation telecommunication networks may present the satellite industry with new tasks and markets. The second technology white paper comes from Comtech EF Data, Revision 2 published on December 21, 2005. The paper is titled as "GSM over VSAT: Choosing the Right Backhaul Solution". It discusses the Point-to-Point and Point-to-Multipoint GSM backhauling options. In the first former the SCPC access scheme is taken into consideration and in the latter two hybrid technologies based on two access schemes are well thought-out. Keeping into account the matters presented in the above mentioned papers, this project shall converse about certain aspects of the blending of such networks. Before proceeding on the integration of the two technologies, a detailed over view of the both GSM and VSAT architectures is carried out.

2 The GSM Network

It is quite well known that a European group known as CEPT, began the development of the GSM network back in 1982 (Lee, 2006). This new digital system offered certain advantages over AMPS in terms of efficient use of the radio spectrum, security for voice transmission, possibilities of data transmission, VLSI

components allowing cheaper and smaller handsets and of course compatibility with terrestrial ISDN based networks. So, with incorporation of the concept of cellular structure and frequency re-use patterns, the digital systems developed to include Multi-Layer cellular patterns i.e. micro-cells and macro-cells (AIRCOM, 2002).

2.1 The Architecture and Interface

A GSM Network consists of three sub-systems:

1. The Mobile Station (MS)

2. The Base Station Sub-system (BSS)

3. The Network & Switching Sub-system (NSS)

Currently, GSM uses the Open System Interconnection (OSI). As discussed in the literature report (26/01/2007), the three common interfaces based on OSI (Figure 2) are the Air Interface (Um – a common radio interface between the MS and BTS), Abis Interface (Between the BTS and BSC) and A interface (Between MSC and BSC)

2.2 Cell Design Objectives

In accordance with Catedra and Arriaga 1999, whilst designing a cell for the radio networks the following objectives must be taken:

The guarantee of the electrical coverage of the cell area. Figure 3 shows the typical power coverage for a cell.

We want to reach a level that provides enough channels in each cell so as to satisfy the traffic demands for new calls and handoffs.

The design approach must be flexible in order to locate the BTSs at available sites.

2.3 OSI Model for GSM

The OSI model of GSM comprises of five layers namely: Transmission (TX), Radio Resource management (RR), Mobility Management (MM), Communication Management (CM) and Operation, Administration & Maintenance (OAM).

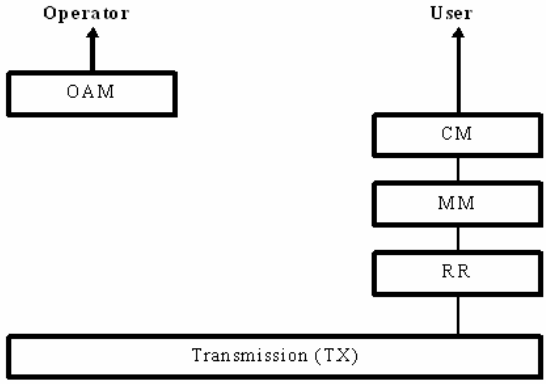


Figure 2 – The Functional planes of GSM (Lee, 2006)

2.4 Transmission layer (Tx)

Since the radio spectrum is a precious and limited resource, therefore using less bandwidth per channel provides more channels within a given radio spectrum. As such, an analogue speech signal of 4 kHz converts to a 64 kbps digital signal, then down converts to a 13 kbps digital signal before it is modulated. In this way the 13 kbps data rate transmission can easily take place over a narrowband channel. The modulation technique used is GMSK Gaussian Minimum-Shift Keying with $BT = 0.3$ as the normalized Bandwidth. Here B is the Baseband bandwidth and T is the transmission rate. The channel spacing is 200 kHz and the modulation data rate is 270 kbps (Abu-Rgheff, 2007).

3 The VSAT Network

VSAT technology is a telecommunication system based on wireless satellite technology. The term 'VSAT' stands for 'Very Small Aperture Terminal'. The advantage of a VSAT earth station, versus a typical terrestrial network connection, is that they are not limited by the reach of buried cable. The research is mainly focused on the SCPC-DAMA architecture due its unique capability of providing flexible bandwidth and intercommunications between remote locations on a network.

3.1 SCPC

In SCPC, to activate the career by speech of the signal dedicated equipment is used. On the concerned channel, when speech is present, the use of a speech detector allows commencement of the transmitted carriers. A syllabic compressor (ITU-T Rec. G.162) is used on each transmission channel and an associated expander on the receiving end provide a subjective improvement in the quality of the transmission.

Interestingly, the response of the expander to the amplitude of the received signal is the inverse of that of the compressor (Maral and Bousquet, 2001).

3.2 DVB-RCS

The DVB-RCS is an open standard and is based on the DVB standard. It is published and maintained by the European Telecommunications Standards Institute (ETSI standard EN 301 790). The DVB-RCS standard accommodates a wide range of commercial requirements and options, in order to define a future-proof standard for many applications. It also specifies the air interface and user terminal requirements and allows more freedom and flexibility in the implementation of systems and networks (Satlabs Online Brochure).

3.3 DAMA

Demand Assigned Multiple Access (DAMA) is a method that increases the sum of users which is supported by a limited "pool" of satellite transponder space. DAMA assigns communication links or circuits based on requests issued from user terminals to a network control system. When the circuit is no longer in use, the channels are immediately returned to the central pool, for reuse. This technology saves satellite users money, optimizes use of scarce satellite resources, and can increase service provider revenues (ViaSat, 2007).

3.4 PSK Modulation

Phase Shift Keying is a particular form of phase modulation which gives good performance while occupying the modest bandwidth. Each possible symbol has a selected phase. Conventionally, two or four phase alphabets are used but there is increasing interest in six and eight phase schemes (Ungerboeck, 1987; Heron, 1989). Digital techniques give a number of advantages that allows multi-rate data capability to be realized (Everett, 1992).

3.5 Channel Capacity Equations Used

Over all Channel Capacity

$$\frac{C_{sat}}{N_o} = \frac{1}{\frac{1}{C_{up}/N_o} + \frac{1}{C_{down}/N_0}} \qquad \text{Eq 1}$$

Uplink Channel Capacity:

$$\frac{C_{up}}{N_o} = P_{T1} \times \eta_{T1} \frac{(\pi D_{T1} f_1)^2}{c^2} \times \frac{c^2}{(4\pi r_1 f_1)^2} \times \eta_{R1} \frac{(\pi D_{R1} f_1)^2}{c^2} \times Rain_{loss} \times \frac{1}{kN_{temp1}} \quad \text{Eq 2}$$

Downlink Channel Capacity

$$\frac{C_{down}}{N_o} = P_{T2} \times \eta_{T2} \frac{(\pi D_{T2} f_2)^2}{c^2} \times \frac{c^2}{(4\pi r_2 f_2)^2} \times \eta_{R2} \frac{(\pi D_{R2} f_2)^2}{c^2} \times Rain_{loss} \times \frac{1}{kN_{temp2}} \quad \text{Eq 3}$$

4 Error Correction and Coding

The modus operandi of error correction coding is purely based on the information coding theory (a field developed from work by Dr. Claude Shannon in 1948). Theoretically speaking, we should be able to devise a coding scheme for a particular communication channel for any error rate, but no one has been able to develop a code that satisfies Shannon's theorem (Wells, 1999).

4.1 Turbo Codes

Turbo codes, also known as parallel concatenated convolutional codes, were first introduced in a paper by Berrou, Glavieux, and Thitimajshima in 1993. These codes combine a convolutional code along with a pseudorandom interleaver and maximum *a posteriori* probability (MAP) iterative decoding to pull off a performance very close to the Shannon limit (Costello, 1998).

4.2 LDPC Codes

LDPC (Low Density Parity Check) codes are also known as Gallager codes, after Robert G. Gallager, who developed this concept in his doctoral dissertation at MIT in 1960. Impractical to implement when developed in 1963, LDPC codes were forgotten. It was rediscovered (Neal and McKay, 1996) that LDPC codes employing iterative decoding to achieve turbo-like performance. During recent developments, an LDPC code beat seven turbo codes to become the error correcting code in the new DVB-S2 standard for the satellite transmission of digital television (HNS, 2003).

5 The Cellular Backhauling Concept

In order to minimize the total cost of ownership for a GSM operator and to augment the solution for the deployment of a given site, a well-designed satellite network should be laid out that can balance the elements like the antenna size, antenna gain and power budget. Antennas with more diameters and high gain require less power, on the other hand, it is not always economically viable to use a huge antenna, as such, an increment in the power budget may be essential.

VSAT Topologies

There are two main topologies that are used when a VSAT network is designed. The commonly implemented topology is the Star architecture, Figure 4, and can be well thought-out as a massive frame relay arrangement above the earth. Implementing a VSAT network in a star configuration also incurs the similar budget investments that can transpire over a dedicated circuit such as an E1.

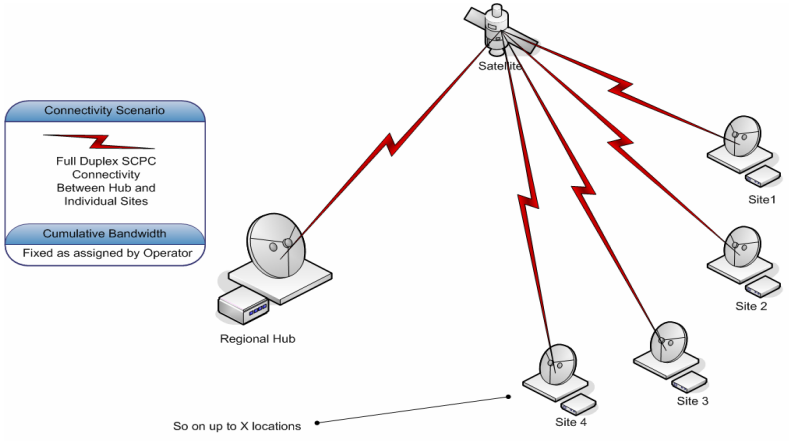


Figure 4 – SCPC Star Topology

In a star topology all the remote BTS locations will be connected to the BSC and the BSC will be connected to them via particular network element knows as the Regional Hub (in this case the MSC). Furthermore, all remote locations in a star topology are independently connected to the satellite, as a result of which the total bandwidth is subdivided amongst them in an equally fixed quantity. For instance, if the total allocation is 1 Mbps and there are 8 locations, then each site will be utilizing 125 Kbps of pre-assigned bandwidth. This leads to one major draw back of using the star topology and that is when a customer (in this case a GSM operator) procures a traditional circuit, then that customer pays a price for the full bandwidth that is allocated by a satellite operator, whether or not it is used. This is not the case required by a GSM operator who is looking to optimize the network.

There is another option in which the allocated bandwidth can be pooled and so that it can be utilized by each of the remote sites, mutually. The introduction of this concept yields a massive savings in the price tag. This is the Demand Assigned Multiple Access scheme that is implemented on a mesh topology, Figure 5. The mesh topology will allow any BTS site, which has lost the connection with its BSC, to link up to another BSC via another remote site near to its location. The hub allocates two channels to the designated VSAT and informs it of the call. The two channels serve as a bi-directional connection linking the two VSAT locations. Once the information is swapped, the call is terminated and the allocated channels are then returned to the pool for the next call. This is somewhat similar to a dial up network (Heifner, 2004).

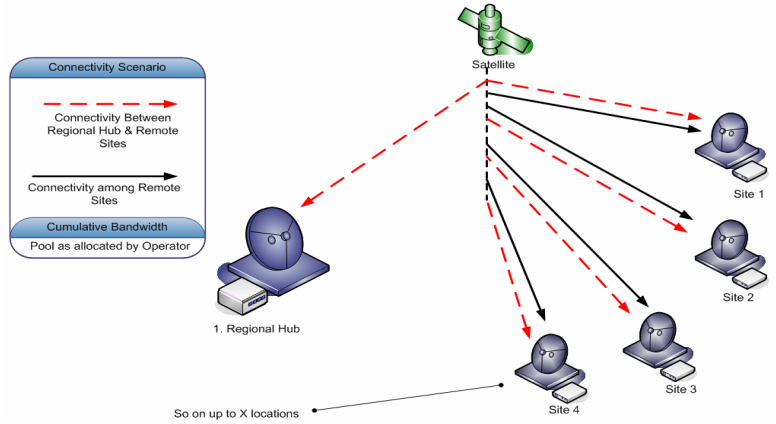


Figure 5 – DAMA Mesh Topology

Since this DAMA mesh scheme is based on CSC, it requires a data management hardware and software, which can be under the control of the BSC or preferably shared amongst the all terminals. This distribution will reduce the delay that occurs between call linking and also provides a major redundancy against hub failure (which in a star SCPC becomes a living nightmare for a GSM service provider).

6 Integration of GSM with VSAT

Based on the mentioned Star topology, the connectivity calculations can be done as follows:

OPTION 1: Satellite Bandwidth Requirement Without Compression For 40 BTS

Assuming QPSK Modulation with FEC ¾ a single E1 will occupy 3.7 MHz in full duplex mode. Thus for 40 BTS the bandwidth required will be 3.7 MHz X 40 = 148 MHz. Consequently two 72MHz transponders will be required for 40 E1 operations.

OPTION 2: Satellite Bandwidth Requirement With Compression For 40 BTS

At the A-bis interface there are five timeslots that are always unused. Furthermore the GSM radio channels can be optimized at each BTS. Thus by using D&I compatible satellite modems (Logitech, 2006) the satellite bandwidth can be compressed.

GSM RF Channels	GSM Voice Timeslots	A-bis data rate (Kbps) D & I	Duplex Satellite Bandwidth (MHz)	Total Satellite Bandwidth for 40 BTS (Mhz)
1	8	320	0.6	24
2	16	512	1	40
3	24	704	1.3	52
4	32	896	1.7	68
5	40	1088	2	80
6	48	1280	2.4	96
7	56	1472	2.7	108
8	64	1664	3	120

Table 1 – Bandwidth Savings

6.1 Weather Impact

Whilst designing a VSAT network a number of factors resulting from atmospheric changes have to be considered in order to evade impairment of unnecessary signals. Usually, a margin in the relevant channel to noise ratio is integrated to cater for such effects. For instance, the considerable impact of rain attenuation can cause a major decrease in the overall link performance. We know from Eq 1, 2 and 3 the overall channel capacity of a system as well the uplink and downlink capacities. With the help of these equations we can mathematically predict the effect rain attenuation has on the overall link performance whether it occurs on uplink channel or the downlink channel.

7 Future Research

In this era the technology that is on hot wheels is the DVB-RCS standard. It will be very much interesting to investigate in to the fact that how the DVB-RCS standard can be incorporated as a backhaul solution on a DAMA star or mesh architecture. As predicted by Alcatel in 2003, this leads to the understanding of savings on the bandwidth on both forward and return channels. Using Demand Assignment Multiple Access (DAMA) and greater compression at the Abis interface (typically by eliminating silences in the GSM frame) this technology may provide a 65% saving on both the forward and return channels. The DVB-RCS with DAMA capabilities may be able to support the remote connection of GSM and GPRS i.e. General Packet Radio Service networks. Subsequently, it can incorporate support for the new 3G networks, premeditated to the UMTS i.e. Universal Mobile Telecommunications System and CDMA i.e. Code Division Multiple Access standards.

In areas where the geographic conditions are suitable and redundancy is still required then an upcoming technology known as WiMax (Worldwide Interoperability for Microwave Access) can do the job. Working as a long range WiFi, this technology

promises to be an added advantage not only as a redundancy option but also as a tough competitor for GSM as it incorporates VoIP itself.

8 Conclusion

In this paper it has been seen how two major industries can be linked with each other to provide services to areas that are inaccessible or mainly how the VSATs can act as a redundancy option for the GSM operators thereby cutting their OPEX and enhancing the overall cellular, call and network performance. It was shown how VSATs are superior to the microwave links in terms of reliability, availability and error detection, correction and coding techniques. In addition to this the effect of rain attenuation in the atmosphere on the bit rate and the channel capacity of the VSAT gave an idea as to what measures must be taken in order to resolve this issue. Most importantly, the edge of a DAMA mesh technology over the SCPC star was laid out in a straight forward manner, leading to the fact that how the choice of the configuration and topology greatly affect the information traffic on a GSM network at the physical layer.

It can be concluded that satellites can become an integral part of telecommunications around the globe. And with research on the DVB-RCS standard and WiMax it can further reduce the operating expenses of GSM backhauling and provide a more effective means of redundancy not only on a 2G network but also on a 2.5G (GPRS) and 3G (UMTS/WCDMA) network.

9 References

Abu-Rgheff, Mosa A., 2007, *Lecture notes*, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, U.K.

AIRCOM International – Training Manual 2002.

Alcatel – Technology White Paper on *New Opportunities for Satellites in Telecommunication Systems*, Review 1st Quarter, 2003.

Comtech EF Data – White Paper on *GSM Over VSAT: Choosing The Right Backhaul Solution*, Rev 2, December 21, 2005.

Costello, D J., Jr.; Hagenauer, J; Imai, H; Wicker, S B., (1998) "Applications of Error-Control Coding.", *IEEE Transactions of Information Theory*, October 1998, vol. 44, no. 6, p. 2531 - 2560.

Evans, B. G., 1999, *Satellite Communication Systems*, IEE Communications Series 38, 3rd Edition, The Institute of Electrical Engineers, London, United Kingdom.

Everett, J., 1992, *VSATs – Very Small Aperture Terminals*, IEE Communications Series 28, The Institute of Electrical Engineers, London, United Kingdom.

Heifner, G, 2004, *Introduction to VSAT Technology*, Orbital Data Inc. http://www.broadbandproperties.com/ (accessed on 26/07/2005)

Hughes Network Systems (Oct, 2003), LDPC Codes, Application to Next Generation Communication Systems, Presentation.

Lee, W C. Y., 2006, *Wireless & Cellular Communications*, Third Edition, McGraw Hill, Singapore.

Lin, S., and Costello, D.J., Jr., (1983), *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, Englewood Cliff, New Jersey, USA.

Logitech Pvt. Ltd. – *Introduction to VSAT*, Training Manual 1998.

Logitech Pvt. Ltd. – *Technical Case Study*, 2006.

Maral G., Bousquet M., 1998, *Satellite Communications Systems,* 3rd Edition, John Wiley & Sons, Chichester, England.

NORSAT – MITH-2001 Discussion of Open Standards for Satellite Multimedia Services.

Satlabs Online Brochure http://www.satlabs.org/pdf/Satlabs_brochure.pdf (accessed on 20/06/07)

Shannon, C. E., (1948), 'A Mathematical Theory of Communication', *BSTJ*, vol. 27: pages 379-423, 623-657.

ViaSat Website http://www.viasat.com/technologies/dama/ (accessed on 13/06/07)

Wade, G., (2000), *Coding Techniques, An Introduction to Compression and Error Control*, Palgrave, Hampshire, UK and NY, USA.

Wells, R. B., (1999), *Applied Coding and Information Theory for Engineers*, Upper Saddle River, Prentice-Hall, New Jersey, USA.

On Interleavers Performances for Turbo codes

V.Olivier and M.A.Ambroze

University of Plymouth, Plymouth, United Kingdom
e-mail: mambroze@plymouth.ac.uk

Abstract

This paper deals with the role and performances of interleavers for Turbo codes. Several interleavers have been developed and can be classified into two main categories, random interleavers and structured interleavers. For the moment the dithered relative prime (DRP) interleaver offers the best performances and can be implemented with few parameters in the memory in comparison to random interleavers. High spread and high minimum distance with low multiplicity are necessary to design a good interleaver.

Keywords

Interleavers, DRP, HSR, Turbo code, Spread, Distance

1 Introduction

Turbo codes (Berrou et al. 1993) are one of the most powerful error correcting codes and allow amazing performances in data rate transmissions with a minimum of errors acceptable. The survey was restricted to Turbo codes with parallel concatenation as shown in Figure 1. Turbo encoder uses two recursive systematic convolutional (RSC) encoders to compute parity bits that are additional bits that will be sent with the information sequence. However, in order to have two different parity bits, we need to have different inputs containing the same information. This is done by the interleaver 'I' that scrambles the original information sequence. The resulting codeword will be sent through an Additive White Gaussian Noise channel and then decoded by a turbo decoder. The iterative decoding of Turbo codes uses two maximum a posteriori (MAP) decoders that, given a sequence of bits, calculates the a posteriori probability (APP) of a bit to be 0 or 1.

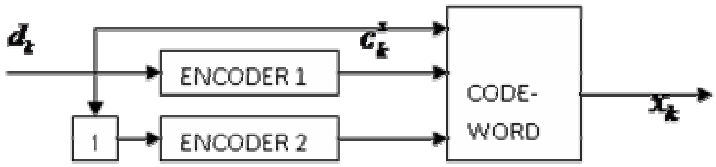


Figure 1: General Turbo Encoder with parallel concatenation

The survey concentrated on a parameter previously evocated: the interleaver. It is a key component of Turbo codes that provides, for a given length N, a reordered sequence of the information to the second encoder. This operation is done with a permutation vector I(i) where i goes from 0 to N-1 that characterizes an interleaver. If we call x the information sequence given as input of the interleaver and y the output, we can formulate this scrambling with y(i) = x(I(i)). So the purpose of interleavers design is to create the best permutation vector as possible in order to obtain more suitable extrinsic information at the decoder side. It is easy to understand that the more permuted the information is, the better will be the result. In fact it allows struggling against bursts or packets errors. By spreading close errors in the information sequence along the permuted sequence we separate them and we facilitate the decoding process. Therefore we could think that the more we spread, the better will be the results. But it is not always true and an explanation will be given in section 5 of this paper. Interleaving design has also to take into consideration that encoding and decoding have to be used for several lengths of sequences to increase the modularity and interleavers have to be implemented on components with restricted memory. The set of interleavers for a range of lengths given is called interleavers bank. If we have to store all the coefficients for each length it becomes memory greedy especially for long interleavers (thousands of bits).

This paper presents several interleavers by talking about their design and their performances. Sections 2 and 3 review and describe main interleavers such as S-Random, HSR and DRP interleavers. Section 4 presents simulations results and section 5 is a discussion about their performances and introduces the concept of distance of codes to explain the observations.

2 Randomly designed interleavers

Since the purpose of interleavers is to scramble the information sequence, it is interesting to define this permutation phenomenon. To do it we have to measure the dispersion or spread. First the representation of an interleaver is given in Figure 2. Two kinds of indexes are considered both from 0 to K-1 where K is the length of the interleaver. Write indexes are those used at the output of the interleaver, and read indexes are those used at the input. The output at write index i is the input at read index I(i), where 'I' is the permutation vector that fully described the interleaver. Two definitions exist to measure the spread and they don't give the same results. The first one is the most natural, because it is expressed as the distance between two read indexes, | I(j) – I(i) | where i and j are two different write indexes. By the way we define the minimum spread, with this definition, as $S_{old} = \min |I(j) - I(i)| \quad \forall i, j \;\; i \neq j$. The second definition of spread is more recent and not only considers distance between read indexes but also write indexes. It is defined by $S_{new} = \min(|I(i) - I(j)| + |i - j|) \;\forall i, j \;\; i \neq j$ (Crozier, 2000).

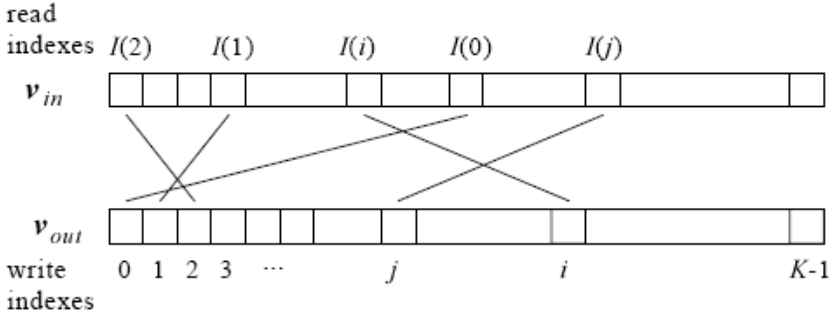


Figure 2: Illustration of interleaver definition (Crozier, 2000)

These two definitions lead to the so-called S-Random (Divsalar, 1995) and High Spread Random (Crozier, 2000) interleavers. The first one uses the following criteria $S_{old} > S$ for $|i - j| < S$ where the parameter S is theoretically lower than floor($\sqrt{K}$) where K is the interleaver length. However, practically we set S < floor($\sqrt{K/2}$) to be sure to obtain a solution in a reasonable amount of time. The second interleaver uses the same criteria but with the new definition of spread and with real indexes, for more details see Crozier's paper. The new theoretical limit of S becomes floor($\sqrt{2K}$) and we set S < floor($\sqrt{K}$) to be sure to obtain a solution in a reasonable amount of time.

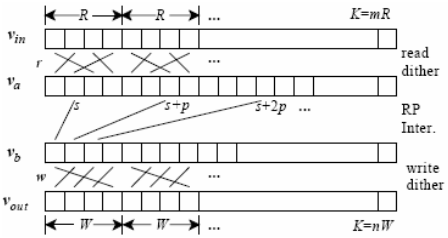
Unfortunately these two interleavers lead to two major drawbacks. First they are time consuming if we set the parameter too high, we are not even sure to obtain a result, and it become longer when we increase the size of the interleaver. A second drawback is that we need to store the entire permutation vector so it requires a huge amount of memory if we want have a large bank of interleavers.

3 Structured interleavers

To cope with these problems, researchers tried to find algorithms that could produce high spread while storing only few coefficients. Golden, relative prime (RP) and dithered interleavers (Crozier, 1999) are those investigated first. For further information about their algorithm see Crozier's paper. For golden and RP interleavers few parameters need to be stored because they are highly structured by their algorithm. Concerning the dithered interleaver it is the dither vector (local permutation) that has to be stored so the amount of memory required varies with the size of the dither. The latter two are important because they lead to the dithered relative prime (DRP) interleaver (Crozier and Guinand, 2001) that is the best one for the moment.

The DRP interleaver is the concatenation of three intermediate interleavers, two little dithered interleavers I_a and I_c and one relative prime interleaver I_b as shown in Figure

3. The interleaver is completely defined by $I(i) = I_a(I_b(I_c(i)))$. The relative prime interleaver offers a high spread performance and the two dithered interleavers introduce a little pseudo-randomness without affecting to much the spread. Contrary to the interleavers presented in the previous section, we don't need to store all the index values to define the interleaver. Since an algorithm is behind it, we just need some parameters such as two little dithered vectors and the starting index and the p parameter of the RP interleaver. Moreover this DRP interleaver can be implemented recursively and it reduces again the required memory to implement it.



$$v_a(i) = v_{in}(I_a(i)), \quad I_a(i) = R\lfloor i/R \rfloor + r(\lfloor i \rfloor_R), \quad i=0\ldots K\text{-}1$$

$$v_b(i) = v_a(I_b(i)), \quad I_b(i) = \lfloor s + ip \rfloor_K, \quad i=0\ldots K\text{-}1$$

$$v_{out}(i) = v_b(I_c(i)), \quad I_c(i) = W\lfloor i/W \rfloor + w(\lfloor i \rfloor_W), \quad i=0\ldots K\text{-}1$$

Figure 3: Ditered relative prime (DRP) interleaver (Crozier and Guinand, 2001)

4 Simulations Results

Simulations results given on Figures 4 show the frame error rate (FER) in function of the ratio Eb/No that is linked to the signal to noise ratio (SNR). These results are presented for Turbo codes with a block length of N=512, 8-state constituent codes with feedforward 15o and feedback 13o polynomials, no puncturing matrix so the rate is 1/3. At the encoder side the first encoder only is terminated. The decoding uses MAP decoders with modified BCJR algorithm (Bahl et al., 1974) since the boundaries conditions are: $\beta_N(m) = 1/n$ for every m, $\alpha_0(m) = 1$ if m=0 and $\alpha_0(m) = 0$ for $m \neq 0$, where m is the state of the encoder and n is the number of possible states, 8 in our case. The number of iterations is restrained to 3.

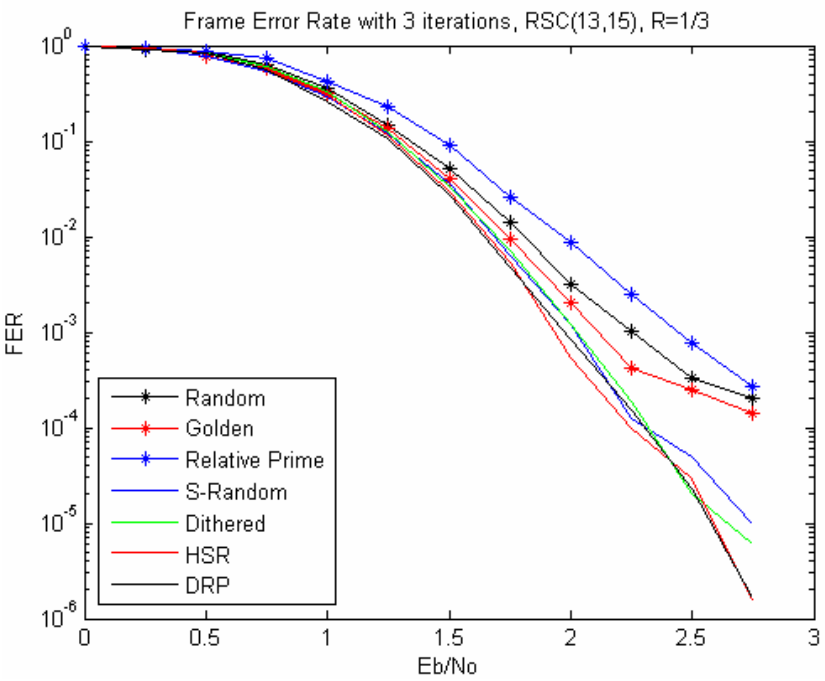


Figure 4: Comparison of FER results for several interleavers

with K=512, 3 iterations and a code rate of 1/3

As expected, the FER decreases when the SNR increases. However an error floor occurs for high Eb/No excepted for HSR and DRP interleavers. With these two interleavers obtaining the best and the same performances for a rate of 1/3, what tallies with Crozier's results (Crozier and Guinand, 2001). However the DRP interleaver is much more interesting because it only needs a few data to be stored to be completely defined without a lost in performance.

5 Interpretation of the results

Using the new definition of spread the minimum spread S_{min} is calculated for each interleaver. You can see these figures in the Table 2, and you can notice that best interleavers have a high S_{min} but some bad interleavers too. So a high spread is necessary but not sufficient.

As discussed in Section 2 the aim of the spread is to split bursts into scattered errors to make the decoding easier but it seems that it does not always give the best results.

	Relative Prime	Random	Golden	S-Random	Dithered	HSR	DRP
S_{min}	14	2	30	14	25	23	26

Table 1: Minimum Spread for different interleavers

The reason is that not only bursts are annoying but also some patterns that are more difficult to decode than others. The Hamming weight of a code that is the number of '1' in the case of binary data and the Hamming distance that is the difference between two codewords. For example a = 110101 and b = 100111 have both a weight w = 4 and a distance $d_H = 3$. The larger the difference between codewords is, the easier is the decoding, so it seems obvious that we have to make to have a high minimum Hamming distance d_{min}. Several algorithms have been developed to compute this true d_{min} and approximations. With this approach it appears that transforming two close input sequences into two completely different codewords is the purpose.

Using a program provided on Internet (Ould-Cheikh-Mouhamedou, 2004) the distance spectrum is calculated of un-punctured tail-bitten Turbo codes in order to observe the three lowest distances, their multiplicity A_d and the average weight w_d of input sequences that lead to these distances. In Table 2, the interleavers have been sorted according to their performances to facilitate the influence of distances on performances. This table has to be related to the performances curves of Figure1.

Interleavers	S_{min}	d_{min}	A_d	w_d	d_2	A_d	w_d	d_3	A_d	w_d
Relative Prime	14	27	2048	9	28	512	4	29	512	3
Random	2	13	1	3	14	4	2	17	2	3
Golden	30	27	1904	9	28	407	4	30	1802	6
S-Random	14	18	8	2	22	10	2	25	3	3
Dithered	25	22	21	2	26	33	2	27	33	9
HSR	23	22	16	2	26	12	2	28	11	4
DRP	26	42	243	6	43	491	5,5	44	513	4

Table 2: Distance Spectra for different interleavers

The first remark that we can make is that when d_{min} is high we generally obtain better interleavers but it is not always the case. So it is a necessary but not sufficient condition to obtain good performances. The other important parameter is the multiplicity. It has to be small if we want to have good performances. Since these three minimum distances are related to the worst input sequences the Turbo codes has to deal with, it is obvious that the highest the multiplicity is, the most often information sequences that generate low weight codewords will be encountered. That explains why relative prime and golden interleavers are weak. They have very good minimum distance but their multiplicities are very high. It comes from the fact that

they are highly structured and so a repetition of bad patterns in the information sequence will stay a repetition of bad patterns. We can notice that randomly designed interleavers have a very low multiplicity compared with structured interleavers, but it is the opposite if we consider the value of d_{min}.

We can now explain why HSR and DRP interleavers have the best performances. The HSR interleaver has an average d_{min} with a very low multiplicity so most of information sequences will generate average weight codewords and, at the end, a very good performance. The DRP interleaver has a very high d_{min} with a quite high multiplicity so several information sequences will generate low weight codewords and, at the end, a performance similar to the HSR since a low weight codeword for DRP interleavers is an average weight codeword for HSR interleavers.

6 Conclusions

Dithered relative prime (DRP) and high spread (HSR) interleavers obtain the best performances. However DRP interleavers are much more interesting to consider because they don't need much memory to be stored. In the case of a large bank of interleavers it is a huge benefit. Performances results obtained can be explained by the nature of the message process and by the kind of errors encountered. On one hand a high spread of information prevents it against packet errors, on the other hand a high minimum Hamming distance of Turbo codes insure that codewords will be different in many points even for close information sequences.

The very good performances of DRP interleavers can be explained by the fact they are based on relative prime interleavers, highly structured for a high minimum distance d_{min} and a high spread performances, and on small dithered interleavers adding the pseudo-random touch that reduces the multiplicity of low weight codewords.

7 References

Bahl, L.R., Cocke, J.,Jelinek, F. and Raviv, J. (1974) "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate" *IEEE Transactions on Information Theory*, 20 (2): 284-287

Berrou, C., Glavieux, A. and Thitimajshima, P. (1993) "Near Optimum Error Correcting Coding and Decoding: Turbo codes" IEEE Transactions on Communications, 44 (10): 1261-1271

Crozier, S.N. (2000) "New High-Spread High-Distance Interleavers for Turbo codes", Proceedings of the 20th Biennial Symposium on Communications, Queen's University, Kingston, Ontario, Canada, pp. 3-7, May 28-31

Crozier, S.N. and Guinand, P. (2001) "High-Performance Low-Memory Interleaver Banks for Turbo codes", Proceedings of the 54th IEEE Vehicular Technology Conference (VTC 2001 Fall), Atlantic City, New Jersey, USA, pp. 2394-2398, October 7-11.

Crozier, S.N., Lodge, J., Guinand, P. and Hunt, A. (1999) "Performance of Turbo codes with Relative Prime and Golden Interleaving Strategies", Proceedings of the 6th International Mobile Satellite Conference (IMSC '99), Ottawa, Ontario, Canada, pp. 268-275, June 16-18

Divsalar, D. and Pollara, F. (1995) “Multiple Turbo codes”, MILCOM’95, pp. 279-285, November 6-8

Ould-Cheikh-Mouhamedou, Y. (2004), “Distance Spectra for dual-terminated and tail-biting single binary Turbo codes”, www-mmsp.ece.mcgill.ca/Documents/Software/Channel-Coding/Distance_SB_TC/DS-SB-TC.htm, (Accessed 27 July 2007)

Evolution of Wi-Fi and Security Issues

A.Zaman and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Wi-Fi technologies are evolving with quick pace providing high speed broadband access to users at places where it was not possible before using wired technologies. Although, there are several benefits of Wi-Fi over wired technologies, there are several security issues that expose Wi-Fi technologies to hackers and intruders. This paper discusses about adoption of Wi-Fi technologies among users and security threats that can be harmful to Wi-Fi technologies.

Keywords

Wi-Fi, War driving, DoS, Malware, E-mail, Spoofing

1 Introduction

Wi-Fi technologies were introduced around a decade ago with devices providing data rate comparatively low as compared to modern Wi-Fi standards. The utilization of Spread Spectrum (SS) techniques for low power signal transmission over license-free wide band was an important feature of these wireless devices. Although, SS techniques were effectively employed for military-purpose communication during Second World War, it was not unitl mid-1990s that wireless devices were introduced for Internet and local network applications. The elimination of wires between devices for transmission purposes is considered as an attractive aspect of Wi-Fi networks.

2 Benefits of Wi-Fi technologies

Perhaps the biggest advantage of Wi-Fi technologies is the communication without any physical medium between wireless devices. This freedom of Wi-Fi communication provides mobility to the users so they can use their devices at remote locations. However, mobility offered by Wi-Fi devices is not the only benefit of this technology. Wi-Fi technologies also provide high speed broadband facility to their users who can access Internet through wireless connection to infrastructure devices. Wi-Fi solutions are also cost effective as compared to wired technologies for several reasons. There is no need to setup cables for connection between wireless devices and Internet access that reduces the cost of installation of these devices. Wi-Fi technologies are reasonably easy to use and it is not difficult to configure and manage these devices. Wi-Fi technologies are also suitable for providing network access to enterprise users at locations where wired solutions are not feasible. Figure 1 is showing the results of a survey to illustrate the use of Wi-Fi technologies at

various locations with respect to enterprises. It is interesting to observe that around 80% of Wi-Fi usage in enterprises is in guest areas, lobbies, and conference and meeting rooms.

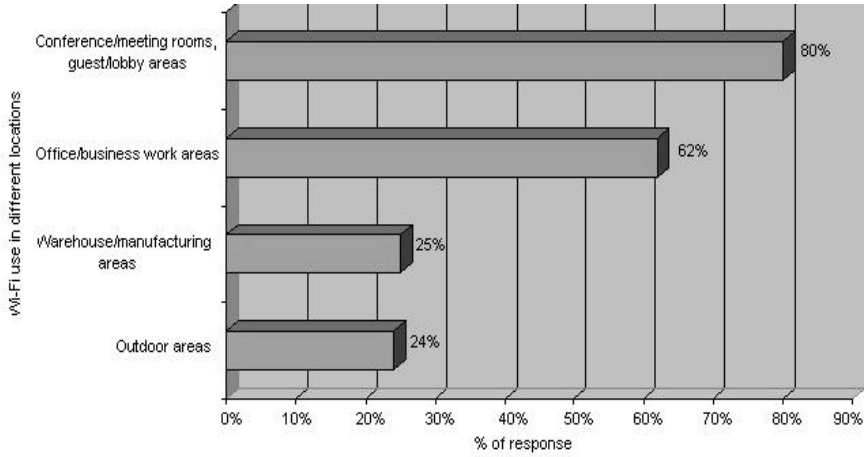


Figure 1: Wi-Fi usage at various locations in enterprises (Wexler, 2006)

3 User Attitude towards Adoption of Wi-Fi Technologies

Earlier Wi-Fi devices were comparatively expensive with respect to data rate support provided on these devices. However, with quick decline in cost of Wi-Fi devices and more data rate support with advanced techniques, users moved quickly towards Wi-Fi technologies. The flexibility provided by Wi-Fi in terms of mobility and ease of use has attracted residential users especially towards this technology. According to IDC, the overall Wi-Fi market value for Western Europe reached to $1.2 billion for first half of 2006 with 22% increase from second half of 2005 (IDC, 2006). The main factor behind this growth is the adoption of Wi-Fi technologies from residential sector that contribute major share of overall Wi-Fi market. The main reason behind this huge popularity of Wi-Fi technologies among residential users besides other factors described above is the lack of technical knowledge of home users. Wi-Fi technologies are generally easy to configure and manageable that requires little or no technical knowledge for installation and configuration purposes. Figure 2 below is also showing predicted increase in Wi-Fi users in different regions of the world from 2004-2009.

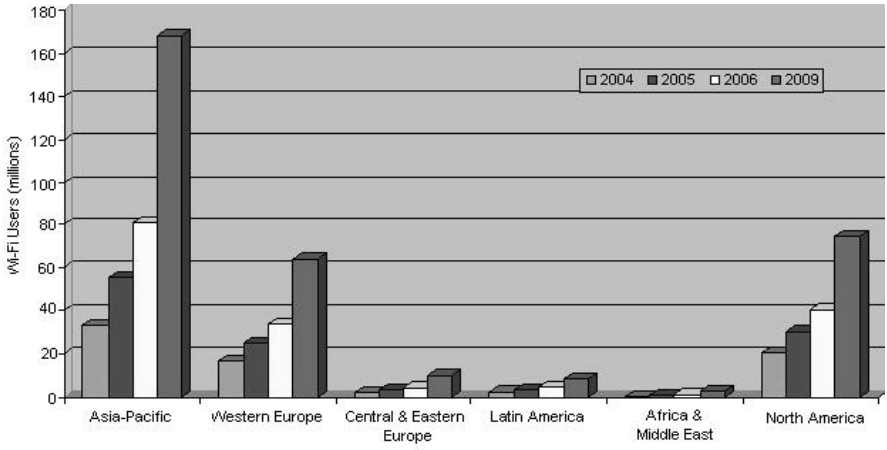


Figure 2: Expected Wi-Fi users with respect to different regions from 2004-2009 (Pyramid Research, 2005)

The introduction of new Wi-Fi solutions from manufacturers for better performance through centralized management and control capabilities is also attracting enterprise users to Wi-Fi technologies. WLAN switches are the example of centralized Wi-Fi solution for better management. According to Infonetics Research, wireless LAN switch market is expected to reach $4.1 billion by 2008 (ITFacts Wireless data, 2005). This figure clearly illustrates the interest of enterprise users in Wi-Fi technologies.

4 Security Issues of Wi-Fi Technologies

Although, mobility and flexibility provided by Wi-Fi devices to the users have many benefits and Wi-Fi can be useful in many situations. Wireless communication between Wi-Fi devices without any physical medium between these devices leads to many problems. There is no guarantee that the communication that occurred between Wi-Fi devices cannot be received by unauthorized users. Wi-Fi provides no mechanism to detect that the transmission of signal is secure in the air and no intruder or attacker is receiving wireless signals. Many enterprise users have concerns over security of Wi-Fi devices for these reasons. According to Wexler, 70% enterprise users have concerns about security of Wi-Fi devices that is preventing these users to deploy Wi-Fi technology (Wexler, 2006). Another important factor about the security of Wi-Fi devices is the lack of expertise in technical users who manage these devices. Some of the important security issues related to Wi-Fi technologies are discussed below.

4.1 War Driving

War driving is among one of the top security threats for Wi-Fi technologies. It is carried out by people who travel from one place to another in order to discover open

or insecure Wi-Fi networks. These people utilize various types of tools such as Airopeek, NetStumbler, AirMagnet to gather information of Wi-Fi networks (Moerschel et al., 2007). The information obtained from these applications is usually uploaded on some websites for other war drivers. War drivers also use special symbols to inform other war drivers and hackers about Wi-Fi networks near that sign. Figure 3 is highlighting some important statistics about war driving for 2002 & 2004. The increasing number of Wi-Fi networks in 2004 clearly shows user interest in Wi-Fi technologies.

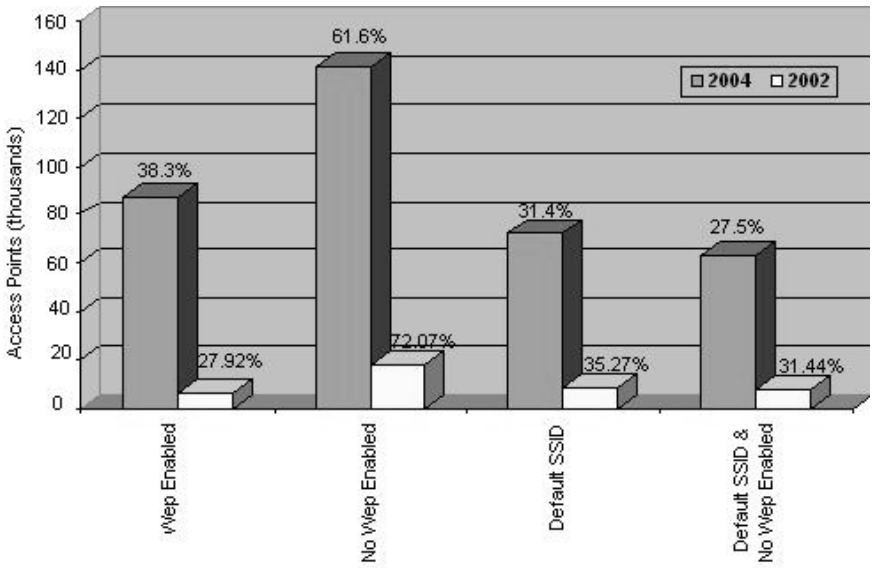


Figure 3: War Driving statistics for 2002 & 2004 (Audin, 2003; Wigle, 2007)

4.2 Denial-of-Service (DoS)

Another security threat to Wi-Fi networks is the Denial-of-Srvice attack against Wi-Fi devices to cause delay and interruption in the network. DoS attacks on Wi-Fi networks are usually carried out at physical or MAC layer. According to Internet security threat report, 38% ISPs were affected by DoS attacks for the period of Jan-Jun 2006 (Symantec, 2006). Most of the Wi-Fi networks are used by residential users for Internet access through ISPs that were also expected to be affected by these DoS attacks. DoS attacks on Wi-Fi networks are easily carried out through packet generators that are easily available in market such as Tamosoft's Commview (Tamosoft, 2007). These packet generators are easy to use applications and provide options such as packet size, packet transmission rate, and source and destination MAC addresses. Table 1 is showing top wireless attacks with highlighting different types of DoS attacks against Wi-Fi devices contributing 15% of overall attacks.

Rank	Threat	Percentage
1	Device probing for an access point	30%
2	MAC address spoofing	17%
3	Unauthorized NetStumbler client	16%
4	Rogue access point	8%
5	Unauthorized association DoS attack	6%
6	RF jamming DoS attack	4%
7	CTS DoS	3%
8	Illegal 802.11 packet	2%
9	Honeypot access point	2%
10	Authorized DoS attack	2%

Table 1: Top wireless attacks for the period of Jan-Jun 2006 (Symantec, 2006)

4.3 Viruses, Worms, and Malware

Name	Type	Operating System
Brador	Trojan	Windows Mobile
Cabir	Worm	Symbian
Commwarrior	Worm	Symbian
Dampig	Trojan	Symbian
Duts	Virus	Windows CE
Fontal	Trojan	Symbian
Lasco	Worm	Symbian
Locknut	Trojan	Symbian
Skulls	Trojan	Symbian

Table 2: Malware threats to wireless devices operating systems (Furnell, 2005)

Modern wireless handheld devices such as smartphones and PDAs are now coming with Wi-Fi support. Most of these mobile devices are equipped with widely used operating systems such as Windows Mobile and Symbian OS. These operating systems provide many benefits to the manufacturers and vendors who develop variety of applications for these operating systems. However, it is also easy for malware developers to penetrate wireless devices running these operating systems. Mobile device users usually left their Wi-Fi connections open while they are not

using it. These high speed hidden paths can be very useful for malware penetration into Wi-Fi devices and network that are providing services to these Wi-Fi devices.

Table 2 is showing some malware applications designed for mobile devices running Windows Mobile and Symbian OS. A careful analysis of table reveals that most of the Trojans and worms are used against Symbian OS. It is due to the fact that Symbian OS is the most used operating system on mobile devices. However, manufacturers are now introducing different versions of Windows Mobile family operating systems. Windows operating systems are widely supported on most of the devices and users are more familiar with Windows family of operating system. However, due to its wide use in different types of devices including Wi-Fi technologies, it is also easy for malware writers and hackers to launch viruses and worms attacks on Wi-Fi devices running Windows family operating system.

5 Protection Mechanisms for Wi-Fi Technologies

There are various types of security methods in order to secure Wi-Fi devices from threats and attacks from intruders and hackers. Wi-Fi enabled mobile devices such as smartphones and PDAs can be better protected through personal firewalls and antivirus applications. These handheld devices usually have low processing power and limited power resources that restrict these devices from using other security methods. Although, most of the Wi-Fi devices including Wi-Fi enabled mobile devices provide WEP for protection, it should never be use to secure Wi-Fi devices due to the known weaknesses in its implementation (Boland & Mousavi, 2004).

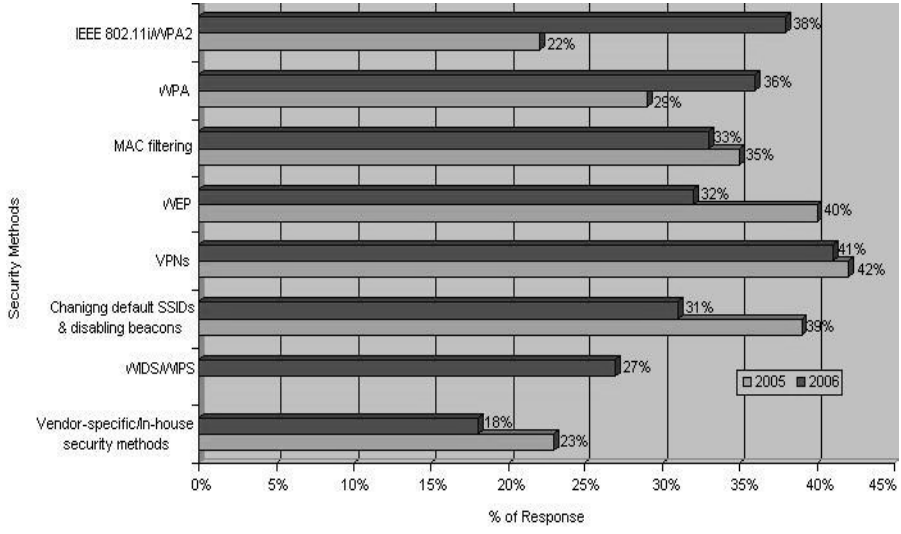


Figure 4: Users preference towards various protection methods (Wexler, 2006)

WPA and WPA2 are more secure security solutions for protection of Wi-Fi devices compared to WEP as these methods offer better authentication and encryption

support. There are various other protection methods as well that can provide better security to Wi-Fi devices. VPN solutions such as provides flexibility to users due to its vendor neutral nature for security purposes. However, it is not a good choice in case of residential and small office users due to the cost involved with this solution. It is also not suitable for real time applications such as voice and video especially when large amount of traffic is moving across VPN. Figure 4 is showing preference of enterprise users towards various protection methods.

6 Conclusion

As Wi-Fi technologies are coming with better data rate support for broadband Internet access, users are attracting to Wi-Fi devices due to many benefits provided by Wi-Fi devices. Residential users are more adopting Wi-Fi technologies compared to enterprise users due to mobility, flexiblilty, and ease of use they are getting from these devices. However, due to the nature of Wi-Fi devices to communicate with each other through wireless signals, Wi-Fi devices and users are becoming victim of various security attacks. These security threats can only be addressed through better security solutions to protect Wi-Fi devices in a layered manner.

7 References

Audin, G., (2003), 802.*11: Are You Sure You're Secure?*, Delphi Inc, http://www.webtorials.com/main/resource/papers/delphi/paper1.htm, (Accessed 15 December 2006).

Boland, H., and Mousavi, H., (2004), *Security Issues of the IEEE 802.11b wireless LAN*, IEEE Electrical & Computer Engineering Conference, Volume 1, pp. 333-336.

Furnell, S., (2005), *Handheld hazards: The rise of malware on mobile devices*, Computer Fraud & Security, May, 2005.

IDC, (2006), *Western European WLAN market generated $1.2 bln in January-June 2006*, ZDNET. http://blogs.zdnet.com/ITFacts/?p=11971, (Accessed 3 Feburary 2007).

ITFacts Wireless data, (2005), *WLAN switch sales up 52% in Q2 2005*, ITFacts. http://www.itfacts.biz/index.php?id=P4584, (Accessed 18 February 2007).

Moerschel, G., Dreger, G., and Carpenter, T., (2007), *Certified Wireless Security Professional-Official Study Guide*, Planet3 Wireless Inc., McGraw Hill, 2nd Edition.

Pyramid Research, (2005), *Wi-Fi Adoption*, BusinessWeek Online, http://www.businessweek.com/technology/tech_stats/wifi051003.htm, (Accessed 1st October 2006).

Symantec, (2006), *Symantec Internet Security Threat Report Trends for January 06- June 06*, Volume 10, http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport, (Accessed 5th January 2007).

Tamosoft, (2007), Tamosoft's CommView, http://www.tamos.com/products/commview/, (Accessed 15 January 2007).

Wexler, J., (2006), *Wireless LAN State-of-the-Market Report*, Webtorials, http://www.webtorials.com, (Accessed 14 January 2007).

Wigle, (2004), World Wide War Drive 4 Stats, http://wigle.net/gps/gps/GPSDB/stats/?eventid=1, (Accessed 22-03-2007).

Section 4

Computer Applications, Computing, Robotics & Interactive Intelligent Systems

Prototyping a Lightweight Robot Arm for Domestic Applications

A.Adra and G.Bugmann

University of Plymouth, Plymouth, United Kingdom
e-mail: gbugmann@plymouth.ac.uk

Abstract

This paper discusses the design of a light weight robot arm for domestic applications. It has four-degrees of freedom and a gripper driven by six electric dc motors controlled by an Atmega 64 microcontroller. Mechanical design is discussed as well as the electrical driving system. In addition, some material simulation results are presented, along with results made from experiments so far. The design shows a promissing load weight ratio of 3:1 but further analysis will be needed for improvement.

1 Introduction

Robotic systems mainly focus on mobility, in a place where human movements, security, and robot displacement are of an issue, it would be of a choice to think of a robot that can take care of all these problems and need to be light and simple enough for the user to control.

In a domestic environment, robotic arms should concern the most about safety issues; they should not cause any damages to their working environment neither to the arm operator. Here comes the need for a light robot that should be safe and not cause any damages.

However for a robot arm to be light, the design should be targeted to accomplish a specialized job. Pre-identified movements would help determine the strength on each joint, which help reduce the weight and make the arm lighter. In this paper, the design of a lightweight robot arm for clothes manipulation that could be mounted on robot legs for vertical motion will be presented, showing the idea behind it and the future plans that could be made, in addition to a brief study concerning the material used and its advantages. The idea behind this concept has been made available for years(e.g Michael et al, 1987) but has only recently been uncovered and made commercial like ‘Katana robot arm’(Neuronics, 2006) and ‘Manus’ (Assistive tobot manipulator 2007).

Figure 1: Clothes manipulation process

2 Design of the lightweight robot arm

2.1 Specifications

The following features permit the arm to be useful in different tasks. It has a maximum reach of 110 cm along the vertical axis, a 100 cm reach along the horizontal axis, and four joints that allow extra movement in all axes. Joint 2 can accomplish 360 degrees of rotation whilst joint 3 can accomplish only 180 degree of freedom (Figure3.b). An extension of 12 cm could be added to the arm using the prismatic joint with a possibility of removing the rotational joint having the same mechanical connectors. The desired motors speed is shown in table 1.

Joint	Speed
Joint 1	6 deg/s)
Joint 2	30 deg/s)
Joint 3	45 deg/s)
Joint 4	0.015(cm/s)

Table 1: Desired motors speed

While observing humans manipulating clothes; positions in the 3-D space were recorded. These positions represent the end of an action performed by a human arm

with a small error in measurements. They vary depending on the size of the piece being pulled and moved and the environment where the robot is placed.

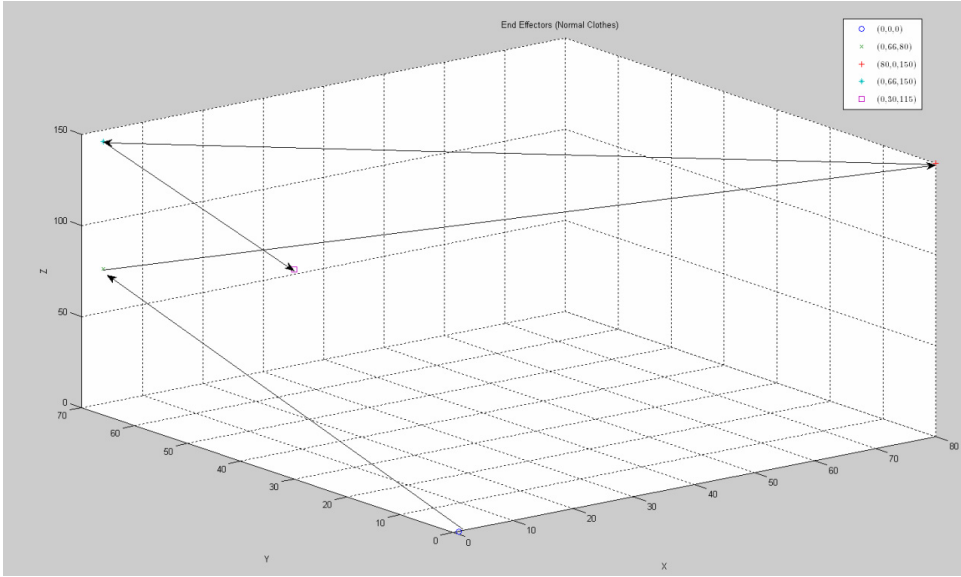


Figure 2: Robot end effectors way points

The arrows on the graphs represent the motion sequence of the arm showing the final positions the robotic arm should reach.

2.2 Design

The robot consists of 4 links; rotary on link one, two and three and prismatic on link four, in addition to a sliding joint on link one and rotary joint on the base (future plan) . The system consists of the robot arm, a washing machine in front and a table of the right.

This section presents Workspace as a simulation tool and a system for developing and execution of the model before being built. It is PC-based simulation software that has a 3D visualization, with collision and near miss detection.

The process of developing the lightweight robot arm consist of the following steps

Creating the part models

The part models are simple geometric entities (cube, sphere..) found in Workspace5. These entities form the robotic arm parts along with the environment such as the table and washing machine.

Building the model

This step consists of building the environment and the arm which is our interest. It consists of seven links which are; the base/link1, rotary1/link2, rotary2/link3, rotary3/link5, rotary4/link6, and prismatic/link7. These links are attached by their number using the feature in the software. They are linked as parent/child relationship.

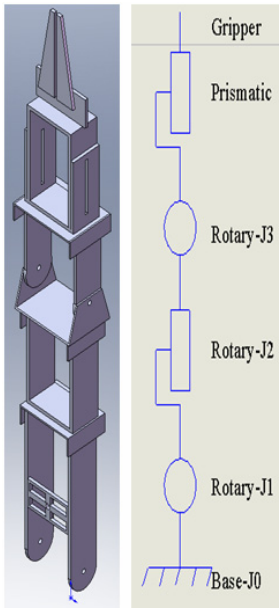


Figure 3: (a) Robot Arm Design, (b) Symbolic Diagram

Positioning the arm in the work cell

The work cell represents the environment where the arm should be placed. In this project, placement of the arm and washing machine are relatively similar to a human arm in action.

Defining the motion of the joints

The motion attributes of the device determine the limits, position, speed, and travel of the joints. Each joint is considered as part of the previous link. In this design, joint 1 links the base with the holder, joint 2 links the holder with the arm, joint 3 links rotary1 with rotray2, joint 4 link rotary2 with rotary3, joint 5 links rotary 3 with prismatic. Each of these joints has it own motion limits, and once they have been defined, workspace will calculate the kinematics of the robot.

Behaviour of the robot

The motion of the robot is defined by entering a series of geometrics positions that will create the path for the robot to follow. These GP's are defined by the motion the arm should do to accomplish the job.

These GP's are entered using the pendant feature of workspace. There are three ways to do so; by entering the value for each joint, by mouse clicking and by entering the X, Y, and Z coordinate for the joint. In this project, entering the coordinates of the joints was used which gives a better positioning for the arm.

Simulation

After defining the GP's , the simulation can be run overtime, which allows to view the movement of the robot arm, reach abilities, the cycle time and collision and near miss detection.

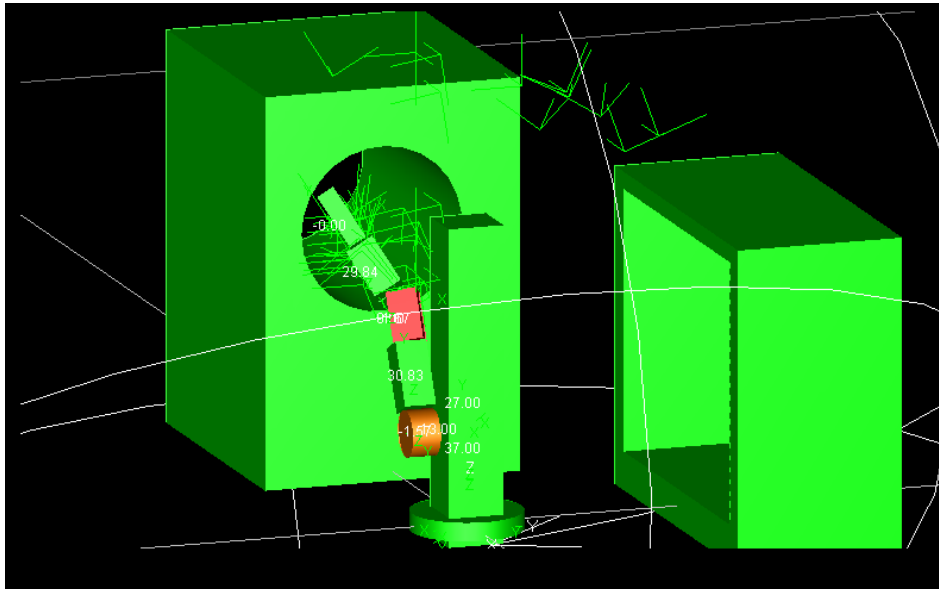


Figure 4: Workspace Simulation showing the robot arm, a washing machine and a work surface

2.3 Stress Analysis

The main features in prototyping the robot arm were being light, with high flexibility to allow maximum reach and grasp in a domestic area while keeping the safety factor elevated. It has to grasp clothes from basket, put in the washer and vice versa.

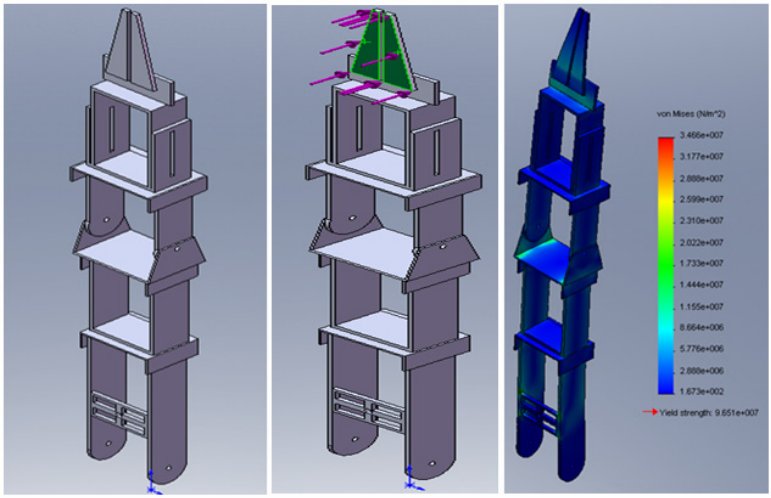


Figure 5: (a) mechanical parts,(b) force direction on the gripper (c) material strength simulation with a 4Kg load.

The arm was intended to be built using composite material such as carbon fiber, but since it is still in its development stages, aluminum was used instead to allow a real time simulation of the behavior and modification of the arm in small working areas.

2.4 Joints Design

Weights and pulling forces of various loads was done using a tubular spring to calculate the torque exerted on each joint of the arm on various positions. The arm was supposed to be pulled up and down on joint 1 using a threaded bar, but for simplicity a metallic cable was used for lifting. The arm is sectioned into four different joints; a rotary motion on joint1, 2 and 3 and a prismatic motion on joint 4. (Figure 3)

The gripper is very basic in design; it consists of two plates attached in parallel at a distance from each others. It is capable of lifting heavy items being only square or thin. An advanced design will not be needed, after multiple observations; humans only use their index and middle fingers which are grouped as one in the design.

2.5 Actuator system

The lightweight robot structure consists of two separate blocks; the arm and the holder (Figure 6.b). The arm is made of four aluminum blocks driven by five dc gear motors, gears, a thread and a cable at the base of the arm. The torque on the arm is maximal at its joint1 and 3. Having to pull from a short distance from the rotation center a heavy weight will require a high torque on the motor side, especially if the arm is parallel to the floor. To simplify the solution, since the arm won't extend more

than forty five degrees from the base, a smaller motor is used to minimize weight and cost.

The sliding joint uses the screw mechanism (Figure6.a), a block attached to a screw driven by a gear motor will slide in its counterpart forming a rectangular shape. The motor should be of high speed since the screw would act as a gear and its torque is calculated using the following equations for lowering and lifting the screw.

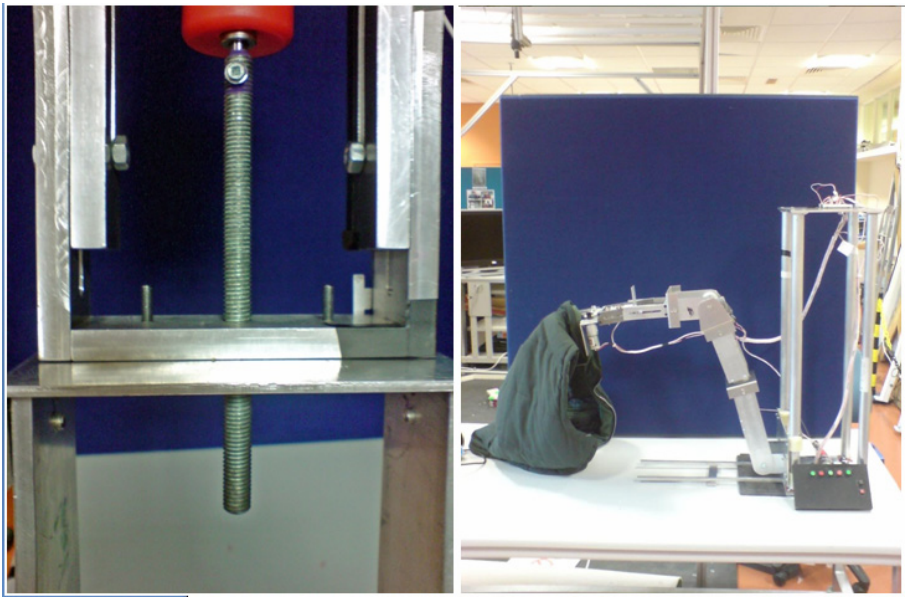


Figure 6: (a) Prismatic joint, (b) Lightweight arm

$$T = L \frac{(2\pi r - l)}{(2\pi r + \mu l)} \quad (r)$$

Where:

T = torque on the screw (in your case this is the torque that motor should exert), Nm
r = pitch radius of screw (for M10 X 1.25 it is 5.25 mm), m
l = lead of the screw, m (1.5mm)
L = load or weight on the screw (weight of your robot arm), N = 30
u = coefficient of friction for screw (its 0.17)
p = pi

2.6 Planned sensing system

The arm sensing system is in form of four potentiometers each placed on a joint in the arm. A sliding linear pot available on the upper part of the arm, to detect the extension distance, two rotary potentiometers placed on joints 2 and 3 and one additional potentiometer placed at the base to detect the distance the cable crossed.

3 Experiments

For the lightweight robot project, switches were used to control the arm. It had to manipulate with clothes, pick them from one side of the table and put them on the second side. Two sets of tests were carried on the robot arm; an experiment to measure the material strength and another to measure the arm handling with weights.

Experiments with weights

The arm was given a series of shapes and weights to work with before working with clothes. It started by picking hollow speheres having a minimal grip moving to water bottles and on shelf components. Having a simple gripper, rounded objects failed to be carried for a long time, they often slid from the gripper sides even when some rubber is placed to increase the friction between the two. Using 2 different types of gears, steel and delrin spur gears causes a corrosion of the plastic with time which let the arm jump over some teeth and start braking the joints.

Experiments on material strength

A set of tests was made before and during the arm creation, various materials were tested from steel, aluminum, composite materials and plastic. Needing a strong and light arm with a low budget design, the options were minimal as we were left with aluminum. The lightweight robot arm is powerful compared to previously designed ones. It can lift up to 1.5 kg having a total weight of 4.7 kg. One drawback is the low safety issue in the arm. Made from dangerous materials such as aluminum, it can hurt in case it brakes and falls, edges must be covered with protective materials that are to be used as shock absorbents.

4 Design Cost

The budget for this project was £150 initially and the part costs were:

PART	QUANTITY	PRICE
MFA940D100:1 motor	1	22.92
MFA940D516:1 motor	4	106.08
MFA950D810:1 motor	1	17.21
SPUR GEARS	-	32.16
TOTAL+VAT		**£209.58**

5 Conclusion

This project is a result of researches, designs and practical work that led to the process of building a robot arm. The mechanical part was built and testes successfully, the arm over all weight is 4.7 kg and is able to lift up to 1.5 kg having a load weight ratio of 3:1 . However, this arm could be better developed using another type of materials with a bigger budget.

A robot platform is now available, future students can benefit from it in future arm designs concerning domestic application and especially clothes manipulation. The need for a lightweight robot is now been understood, with a complete knowledge of the difference between different types of robot arms.

Future work could be done to the arm; the control code should be written and tested, a real time graphics robot simulator which consist of software simulating every movement of the arm on a pc with a system for obstacle detection and avoidance could be applied with material change from aluminium to carbon fiber.

6 References

Assistive Robotic Manipulator (2007) http://www.exactdynamics.nl/english/ index.html, (Accessed 25 August 2007)

Brown A. S.(2006) 'Nimble New Robot is Safe around Humans', *LiveScience* http://www.livescience.com/technology/061102_human_robot.html, (Accessed 20 August 2007)

Neuronics (2007) http://www.neuronics.ch/cms_en/web/index.php?id=244, (Accessed 25 August 2007)

Walsh R.A. (1999), *Electromechanical Design Handbook,* McGraw - Hill, USA

Personal Robot User Expectations

S.N.Copleston and G.Bugmann

University of Plymouth
e-mail: G.Bugmann@plymouth.ac.uk

Abstract

This is a report into the expectations of personal robots in the home using a survey of respondents from a combination of age groups. A questionnaire was designed using a "text open end" approach to the questions. The questions along with an introduction and sketch of a humanoid robot in a home were used to "paint the picture" of the subjects having a robot at home. They were then asked what they would ask the robot to do. 442 subjects from five age groups were questioned. The results were then normalized. The task category of "Housework" was the most popular out of a total of ten categories with 35% of the overall answers. "Food Preparation" and "Personal Service" were the second and third most popular categories with 20% and 11% respectively. The five most popular individual tasks from all categories were prepare tea, tidying, schoolwork, general cleaning, and make drinks. The overall attitude towards the robot from the respondents was that of a servant. The subjects would ask the robot to do tasks which enabled them to have more free time. The results point to areas of research that personal robot engineers could concentrate on.

Keywords

Personal robots, Expectations, Homes, Survey, Household tasks

1 Introduction

What tasks should a personal robot be able to do around the home? The question has no definitive answer and perhaps never will, however robots are becoming more advanced all the time and this evolution will bring robots into our homes. In the past the robotic market has been predicted to boom anytime now, especially in the personal and service sectors (Dan Kara, 2003). If this boom does in fact occur robot engineers need to be informed about what consumers want from personal robots in the home.

This research was undertaken with the aim to answer the question of "What household tasks should personal robot engineers be concentrating on?". A survey of varying age groups was carried out to attempt to answer this question. A questionnaire was designed to gather answers from people about what tasks they would ask a robot to perform.

2 Method

Surveys can be carried out using a variety of methods and a survey for robot tasks in the home was no different. After researching techniques of surveying it was decided

that the questions would be "text open end" questions (Creative Research Systems, 2006). These questions gave the subject freedom of expression and allowed for multiple answers per question. The level of detail gathered in each question was decided by the amount of information the subject wished to give. The in depth questionnaires induced the subject to imagine life with a robot and "day dream" interactions with the robot, and the working day of his or her robot. This approach bears some similarities with the "Information Acceleration" method used in market research for really new products (Urban et al., 1996), but gives more freedom of expression to the subjects. Multiple-choice questions were used to gather information on the subject's age, sex and if they have any help from helpers, nannies, cleaners or gardeners. The "day dream" method was used in the form of an introduction to the questionnaire. This introduction included a short sentence to describe how the subject has been given a robot and that it is theirs to instruct. In addition a sketch of a humanoid robot was supplied to enhance the subjects "mental picture" before answering the questions. The questionnaire was devised and is shown in Figure 1 below.

Personal robot user expectation survey

You have been given a robot as part of a trial program. It is yours to live with for one year.

1. You get up and get ready for your day, what will you ask your robot to do today?
2. The evening comes, what will you ask your robot to do during the evening?
3. You are going to bed, what will you ask your robot to do before you go to sleep?
4. It is Sunday morning. What will you ask your robot to do?
5. You have booked two weeks holiday and plan to go away. What will you ask your robot to do while you are gone?
6. You can "upgrade" your robot by teaching it new activities. 6 months have passed since you got your robot have you upgraded your robot by teaching it anything?
7. Instead of a robot you have been given a trial of an intelligent appliance. Which appliance would you choose and how would it be intelligent?

Sex: Male [ ] Female [ ]
Age: 18 – 20 [ ] 21 – 30 [ ] 31 – 40 [ ] 41 – 50 [ ] 50 and over [ ]
Nationality:_____
Do you have any of the following?
Cleaner [ ] Helper [ ] Nanny [ ] Gardener [ ]

Figure 1: The questionnaire form

Three surveying methods were chosen for this questionnaire, personal interviews, paper questionnaires and Internet survey. In total 442 subjects completed the questionnaire. 55 aged 6 to 7, 29 aged 10 to 11, 260 aged 11 to 17, 87 aged 18 to 60 and 11 aged 61 or above. 6 to 7 year olds and 10 to 11 years olds were children attending primary school. 11 to 17 year olds were children attending secondary school. 18 to 60 year olds were considered adults and 61 years or above were considered as Retired/Elderly. The data for 15 subjects were collected using the personal interview methods and all fell under the adult age group. Data for 21 subjects was collected using the Internet survey method and all were adults. The remaining 406 subjects were asked to fill out a paper questionnaire.

3 Results Analysis

Due to using the open-ended question method it was important to find the right approach to analysing the results. The subject's answers were very varied however there was some common answers. Therefore these common answers were recorded using a quantitative method. For example if a particular subject mentioned, "do the washing up" three times for questions representing different times of the day this task was recorded three times. They were counted three times to reflect the demand for the task. There has been an assumption made where tasks mentioned multiple times during the survey are therefore of most importance.

The number of subjects questioned in each age group was unbalanced. Therefore a normalization technique was utilised to scale the amount of answers for each task to a common level. All the answer data for the age groups were normalized to a population of 100 subjects. For example for 6 to 7 year olds, where the final respondent count was 55, the total number of answers for a particular task was scaled up by a factor of 100 divided by 55. If the scaling did not produced a round number the value was rounded to the nearest integer. The normalization process meant that all the age group data could be analysed side by side. To clarify, due to there being a total of five age groups there was a normalized total of 500 subjects, 100 subjects per age group. If all subjects in the survey had mentioned the same task three times each that would mean the total amount of data for that task would equal 1500. This therefore gave an indication of how popular tasks were.

4 Results

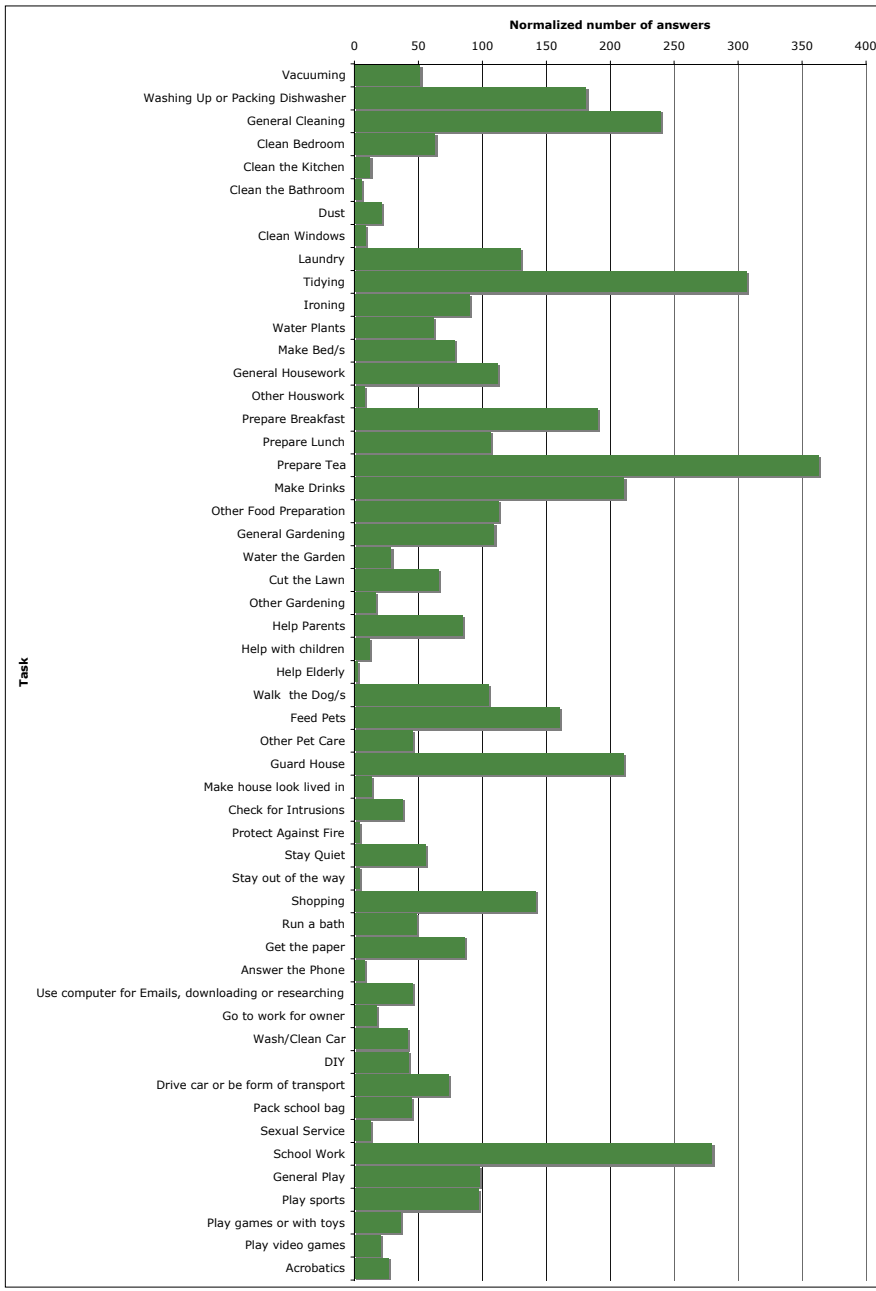


Figure 2: Quantitative results for all age groups showing the totals for all tasks

Figure 2 shows the normalized quantitative data recorded from the survey. It contains data from questions 1 to 6 from all age groups. The chart shows the most popular tasks and the amount of times they were mentioned in the survey by all subjects. General cleaning for example was given as an answer 240 times by the subject population of 500. As mentioned in results analysis this does not necessary mean that 240 separate subjects mentioned general cleaning. Subjects could have mentioned the tasks more than once during the questionnaire. The chart in Figure 1 gives a very clear indication of the most popular answers subjects gave. The five most popular tasks were; prepare tea, tidying, schoolwork, general cleaning, and make drinks with 363, 307, 280, 240 and 211 answers respectively

Housework
Vacuuming, washing up or packing dishwasher, general cleaning, clean bedroom, clean the kitchen, clean the bathroom, dust, clean windows, laundry, tidying, ironing, water plants, make bed/s general housework, other housework.
Food Preparation
Prepare breakfast, prepare lunch, prepare tea, make drinks, other food preparation
Gardening
General gardening, water the garden, cut the lawn, other gardening
Family Help
Help parents, help with children, help elderly
Pet Care
Walk the dog/s, feed pets, other pet care
Security
Guard house, make the house look lived in, check for intrusions, protect against fire
Stay Quiet
Stay quiet, stay out of my way
Personal Service
Shopping, run a bath, get the paper, answer the phone, use computer for emails, downloading or research, got to work for owner, wash/clean car, DIY, drive car or be form of transport, pack school bag, Sexual Service
School Work
School work
Play
General play, play sports, play games or with toys, play video games, acrobatics

Table 1: Tasks Categories

The tasks included in the chart are varied. Therefore this made it important to group them into categories. Categorising the data meant that an analysis could be done into the common areas which the robot would be asked to perform tasks in. The tasks were grouped into the following categories; Housework, Food Preparation, Gardening, Family Help, Pet Care, Security, Stay Quiet, Personal Service, School Work and Play. These categories came about by looking at the data once collected

and were not decided before the research was undertaken. Table 1 below shows which tasks came under which category.

The distribution of the tasks within the categories was then represented using the pie chart shown in Figure 3. The pie chart shows a very clear distribution of the categories within the data set. Housework had the largest amount of answers with 35%. Food preparation, personal service and play also had relatively high portions with 20%, 11% and 10% respectively.

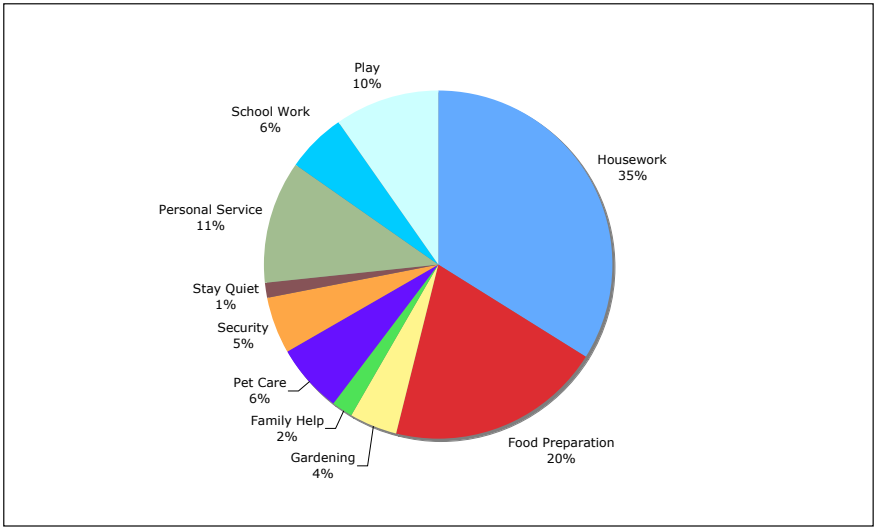


Figure 3: Popularity for each category

5 Discussion

The results show that people are able to think about living with robots with a positive attitude. Although there was no question to ask if the subjects would accept the robot into their homes, it is clear that they were all willing to give answers when asked what they would ask a robot to do for them. A previous survey conducted at a robotics exhibition in Switzerland backs up this fact (Arras and Cerqui, 2005). In the survey of 2000 people, 71% of them answered "yes" to the question "could you imagine to live on a daily basis with robots which relieve you from certain tasks that are too laborious for you?". It is shown from the popularity of the housework category that people are looking for solutions to the "laborious" jobs around the home. Another survey into the top ten most dreaded household chores highlights cleaning the kitchen, cleaning the bathroom and washing the dishes as the three most dreaded chores (CEA, 2007). This is very interesting when comparing the results from the data shown in Figure 2. Cleaning is most definitely the task most asked of the robot under the housework category. However it is general cleaning, which has been mentioned most often and subjects where not specific to exactly what rooms

they wanted cleaning. Some subject did state they wanted to kitchen or bathroom to be cleaned however this is a very low amount when compared to general cleaning. It is unclear whether the subjects had bathrooms or kitchens in mind when answering "do the cleaning". However for a task a household robot should be able to do, cleaning is of high priority. Washing up was very popular in the survey and is seen to be the third most dreaded chore. The survey results in this research seem to back up the attitudes to certain chores. However prepare tea was, by a high margin, the most popular task seen in the data in Figure 2. Cooking only ranked 9th out of the ten most dreaded chores. Perhaps many people like to cook meals, but it was also seen that an evening meal was very important for subjects when asking a robot to perform tasks for them. There seems to be a contradiction here, food preparation is again a priority task for household robots even though it is not as dreaded as others. To highlight another difference from the two surveys, tidying was not included in the top ten list but was mentioned 307 times in the housework category. People do not seem to dread this tasks very much but would still pass it off onto their robot.

There seems to be two types of tasks the robot could do for the owner. Tasks which remove labour from the owner and tasks which add to the owners life. Housework, gardening or food preparation all relieve work from the owner where as playing adds to the persons life through entertainment. The DIY task also adds something as it could be decorating and making the house environment a better place to live. In general however peoples attitudes to the robot seems to be strictly to help them by doing jobs. The subjects are benefiting from the robot by it giving them more leisure time that would otherwise be spent doing jobs around the home. There is an almost servant like attitude towards the robot. The questions never once said that the robot was there to do work for you. People just assumed that is what its purpose is. There were a percentage of subjects that did want to play with the robot. Whether it was sports, games or video games. These subjects were mostly children who have a more fun outlook on life in general. It could be said that adults have been given the impression that robots are going to be made to work for us and nothing else. This is distinctly a western view on robotics as a whole. If a robot does not have a use then it is deemed as unnecessary (Sparks, 2006).

There were some interesting results for certain tasks which should be mentioned. Schoolwork was the third most popular tasks overall and this is alarming. Schoolwork was only contributed to by children up to the age of 17, 300 of the 500 subjects. Therefore unlike the majority of tasks it is not an answer spread over all of the subjects. It is not surprising that children want to have help with schoolwork or in fact to have it done for them. The robot would be giving them less work to do and more leisure time. However these results could be highlighting a need for children to have more support when doing their schoolwork. What the support is this research does not cover but it was an interesting find. Another interesting task was sexual services. Whether subjects which answered a sexual service in their questionnaires were serious or not, the fact is sex was seen in the results. Sexual robots have already been seen in Hollywood (Spielberg, 2001) and it might just be a matter of time before robots made for sex become a reality. What is for sure however is these results show that there are many other tasks of higher priority to sexual services.

Playing with the robot was also seen in the results. The results for the child age ranges showed that they are very willing to play with a humanoid robot. The majority wanted to generally play with the robot or play sports with it. Males were the subjects that wished to play sports and also wished their robot to perform acrobatics. Playing video games was also solely a male answer. Females answered to generally play with the robot or to play games or with toys. Some adults also wanted to play with the robot. With sports, card games and video games all being mentioned. These results show that the tasks for the robot were not always considered "work".

Another interesting feature from the results was time frames. The questions were designed to guide the subject though their day and during a weekend and holiday. There was a definite relationship between the time of day and the tasks answered. Obviously food preparation was already governed by the time of day however other tasks like gardening or washing up were answered in the questions where the subject themselves would perform these tasks. For example, gardening was mentioned most often in the weekend question. The interesting thing here is the fact that the robot could perform these tasks at anytime but the subjects chose to ask the robot when they would normally do them. This trend could simply be down to how the questions were worded and the questionnaire design but it does show the thinking behind the respondents answers. It was decided to take a quantitative direction when collating the results. Was this the best method to take? To find the most popular tasks the answer is yes. On the other hand the results showed that they could be analysed qualitatively, especially when looking at attitudes towards the robot. Quantifying the results proved difficult for such open-ended questions and perhaps having a few multiple choice questions might have helped. On the other hand it was important not to influence the subject by giving them answers to choose from. In the end the quantitative results highlighted important tasks and trends from the "text open end" questions and therefore was a good analysis approach. Similarly the subjects were influenced by the introduction and sketch. It was decided that these were needed to put the subject in the "mind set" of having a robot at home. If this introduction was changed or removed entirely would that have affected the results? The answer is most probably. A possibility for a future survey would be to vary the introduction and sketch to see how the results change. For this survey however the introduction served its purpose and very few subjects questioned the robot being in their home or its functionality.

6 Conclusion

The aim of this research was to create a survey to obtain results regarding user expectations for personal robots in the home. The overall result was hoped to highlight tasks that personal robot engineers should be concentrating on to build solutions for. A questionnaire was created using open-ended questions and subjects ranging from age 6 to 60+ were questioned. The data was then quantified and it was discovered that prepare tea, tidying, schoolwork, general cleaning and make drinks were the most popular tasks. A servant type attitude was also found in the results where the subjects would ask the robot to perform tasks they did not wish to and therefore give them more leisure time. In terms of functionality it is suggested that

robot engineers should be concentrating on solution for cooking meals, tidying up, general cleaning and the preparation of drinks. Overall the research shows some very unique data and a sample of peoples expectations for robots in the home have been discovered.

7 References

Dan Kara (2003), "Sizing and Seizing the Robotics Opportunity", RoboNexus, www.robonexus.com/roboticsmarket.htm, Robotics Trends Inc, Accessed on 17/01/2007.

Creative Research Systems Corporation Web Site (2007), "The Survey System – Survey Design", http://www.surveysystem.com/sdesign.htm, (Accessed on 19 September 2007)

Urban Glen, Weinberg Bruce, and Hauser John (1996), Premarket Forecasting of Really New Products, *Journal of Marketing*, January 1996. Vol. 60, Iss. 1; p.47

Kai O. Arras and Daniela Cerqui "Do we want to share our lives and bodies with robots? A 2000-people survey", Swiss Federal Institute of Technology, EPFL, June 2005

Consumer Electronics Association (CEA) Market Research 2007, http://www.ce.org/, Accessed on 17/01/2007. (Technologies to Watch, Robotics 5, Winter 2006)

Mathew Sparks (2006), "Japanese Robotics", IET Computing & Control Engineering, Oct/Nov 2006

Steven Spielberg (2001), "Artificial Intelligence: A.I.", Producer Bonnie Curtis, 2001.

8 Acknowledgements

The following people are acknowledged for their contributions, informative discussions, support and advice during the project; Andy Phippen, Phil Megicks, Peter White and Liz Hodgkinson.

Pictocam: a Collaborative Game for Training a Language Learning System

M.Demarquay and T.Belpaeme

University of Plymouth, Plymouth, United Kingdom
e-mail: tony.belpaeme@plymouth.ac.uk

Abstract

We propose an exploration of language learning of simple words (nouns mapped to a visual representation) in a relatively innovative manner: through a computer game. As a matter of fact, children learn the meaning of words over many years and reproducing such a process in artificial life usually needs an important set of data which is not trivial to collect. As von Ahn and Dabbish (2004) already demonstrated, we can use the desire of people to be entertained in order to make them execute an implicit task in a game: in our case, training a memory-based learning system that associate words to their visual representation. Pictocam, our multiplayer game is accessible from a simple web page on the Internet. Users play in collaboration with other people and take pictures of objects with their webcam in their home environment. The object features calculated are then used to train a learning system. Once trained, the system is able to visually recognize hundreds of different type of objects.

Keywords

Distributed knowledge acquisition, Web-based games, Object Recognition, Computer Vision, Language Acquisition

1 Introduction

Language is unique to human kind. No other species have a communication system which rivals language either in terms of complexity or diversity. As numerous functionalities of our brain, using the language is spontaneous and natural for us; however, it intrigues and fascinates a lot of researchers in various areas. In neurobiology, anthropology or psychology, our linguistic abilities have been studied for years without having revealed all its secrets. More recently a part of the Artificial Intelligence research community is devoted to its study: now, it appears clearly that 'intelligence' and 'communication' and their respective complexities are inextricable and intrinsically linked.

For researchers in Artificial Intelligence who attempt to imitate and reproduce these linguistics abilities, a fundamental question concerns the way we learn language. It is believed that this acquisition is highly dependent on the manner we perceive our environment (Gallese and Lakoff, 2005). A popular model states that the meaning of words is deeply associated to symbols based on our perceptions (e.g. (Harnad, 1990; Glenberg and Robertson, 2000))

The purpose of this paper is to explore the language grounding by learning simple words (nouns mapped to a visual representation) in a relatively innovative manner: through a computer game. As a matter of fact, children learn the meaning of words over many years and reproducing such a process in an artificial system needs a huge set of data which is hard and tedious to collect. As von Ahn and Dabbish (2004) demonstrated, we can use the desire of people to be entertained by games to do such a task like labelling images on the web or, in our case, training a memory-based learning system to associate words to their visual representation. The success of our system lies in the fact that people participate not because they are involved morally or financially in the task but because they enjoy it.

The game, called Pictocam, is accessible by a simple web browser with a Flash Player plug-in installed (Adobe, 2007). People that possess a webcam will train a learning system just by playing it: the game is played collaboratively in groups of five and players are requested to take objects in pictures with their camera. Image features are extracted and sent to the server to be used in the game, but also to enrich the learning system database.

2 Related works

The idea of including the learning process into a game to feed the system with images is inspired by the work done by Von Ahn and Dabbish (2004). They have developed an online game named 'ESP game' in which players implicitly label images found on the web. They postulated that computer vision systems was not yet able to label images meaningfully, and current systems use text around images found on the web (their names, html tags near images…) are not accurate enough and meaningful. Google Image (Google Inc., 2007) is a good example of image search engine which does not use meaningful label for image retrieval. The only simple solution to do that for the time being is to manually label images with a human operator. However this process can be very expensive and long: they found a solution to involve people who will enjoy doing it. This system uses human abilities that computers do have not and their attraction to play games.

The game is online and hosted by a server, with a client (a Java Applet) available on a web page. The game associate players randomly by two and they cannot communicate. The two partners have only an image in common and they can guess words. To gain points, partners should agree on a word: to do that, they have to type a common word that describes the image for both of them. When players agree on a word, there is a strong probability that the word is meaningful for the image selected and independent of the player's personal perception.

Peekaboom is another web-based game using a similar concept. It has been designed to build a training set of located object in pictures for vision system algorithms (von Ahn, Liu, & Blum, 2006). The ESP game was labelling pictures with words: this new game use the set of labelled image created by ESP to precise where are located the objects referred by the word in pictures.

Pictocam use on the client-side an image feature extractor developed by Gousseau (2007). With a motion detection algorithm, the object region is detected and extracted from the background to calculate its low-level features (shape and colour).

The learning system developed by Coisne (2007) and used on the server-side is based on a memory-based learning system (see for an example: Nelson, 1996). It uses the object features extracted in clients and compare them to a word's model. If a feature is similar to one already known for this word, their similitude can be calculated and the knowledge of this feature will be increased through a weighting system; unknown features are simply added in the model base.

3 Description of the system

In a game, users play anonymously in group of 5 people which are created automatically by the server. At each new turn of the game, the server sends a random word that all players in the group have to find as fast as possible. They search an object in their home environment (e.g.: their house) representing this word and take a picture of it. Players try to obtain the best *match score* as it is possible without losing too much time. This match score increases when players in the group have taken similar objects and when the server recognises them (in the case of the learning system is trained for this word). So to play well, they have to implicitly agree on a common object representing the word. When they want to keep the picture they have taken and block their match score, they validate the turn. When they all have validated, the *team score and* players' *personal score* are increased, depending on all players' match scores.

The game is limited in time: it starts for a fixed duration and the timer is increased by a bonus every time players validate a new turn. The time bonus is calculated by a formula depending on the team score bonus of the turn and the number of turns elapsed (the time bonus decrease with the number of turns and increases with good team scores). If the team play well, they will have more time to continue and they will reach higher scores.

The main goal of players is to increase their rank in the game. The bests will be displayed in the 'top 10' boards. They can access to their own statistics to see their rank compared to all other players.

The Figure 1 shows the main screen of Pictocam (When the user is logged on the server). This screen displays the main statistics of the player: its rank relative to the day or since the account creation. The statistics concerning the best players are also available: the ten best players, the ten best players of the day, the best team (the group who reach the best team score) and the best team of the day. From this screen, the user can decide to join a game.

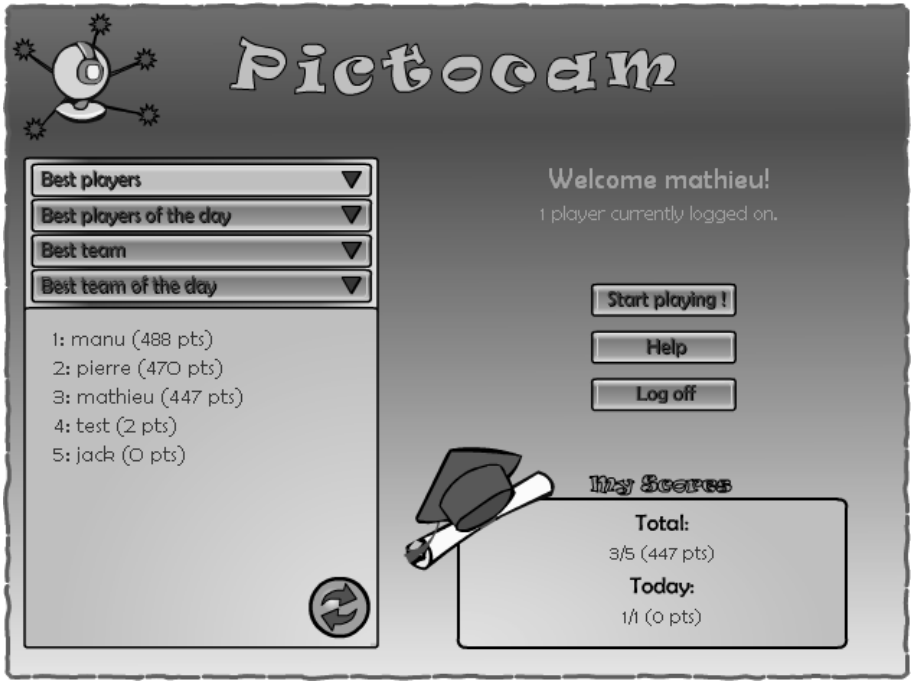


Figure 1: the main screen of Pictocam

When the server has found 4 other player, a group is created and the player can see a screen similar as the one presented on Figure 2. The 'hot word' is displayed and when a player has found in its environment an object representing it, he takes a picture of it by following the instruction given by the recognition feedback (e.g.: 'move your object', 'stand still' or 'remove your object'). When the picture is taken, features are extracted and sent to the server. Then, match scores are recalculated and updated in the table of each player (represented by progress bars in the 'match' column). When the user is satisfied with its own match score, he validates the turn with the button that is similar to ones in the column named 'next' in the table. When all the icons in the 'next' column are activated, the turn is ended and different scores are calculated by the server: the personal score of each player is updated, like the team score and the time bonus that will increase the total time of the timer. When the timer is over, the game is stopped and a summary containing the game scores is displayed.

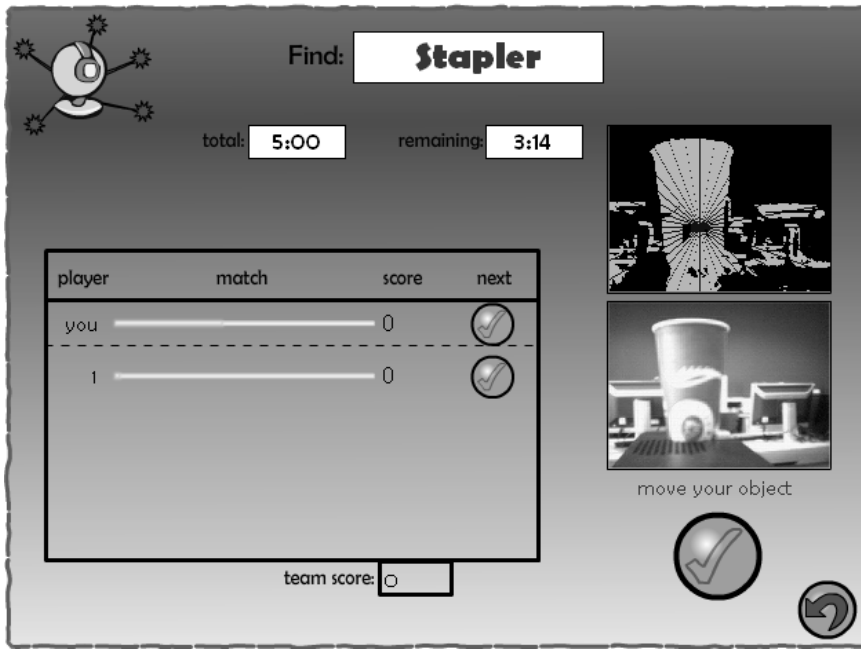


Figure 2: the game screen of Pictocam

Players interact together in collaboration: the fact that they play in a group of five anonymously is used to incite them to agree on a common view of the word requested. As they cannot communicate, this ensures that pictures taken can be trusted. The collaboration in a large group of players is also useful to ensure that the game recognition is also working with words that have not been learned very well. When the server estimates that the number of pictures taken for a given word is not enough, the server recognition importance is lowered for the calculation of the match score in order to rely more on the comparison between players' pictures.

The game is implemented on a client/server architecture. The Pictocam game is available at the URL http://www.pictocam.co.uk/. The client has been developed in ActionScript Flash (Adobe, 2007). The server is fully written in Java (Sun Microsystems, 2007) using the Oregano API, an extensible multi-user server dedicated to communicate in real time with client written in Flash (Spicefactory, 2007).

4 Evaluation

4.1 Assessment protocol

The aim of this research concerns the way we can transform a computing task (training a learning system) into an enjoyable game. Users involved must play to the

game because it is entertaining and not because it creates a valuable output generated for research purposes.

We need to assess if players enjoy the game. To do that, a survey has been designed and players have been invited to take it. The server is also providing game statistics that will be correlated and contrasted with results from the survey.

The second point to assess concerns the efficiency of the game as a trainer for the learning system. The first objective will determine if the learning system works by itself and permits to really learn object classes. Secondly, the game's initial objective will be checked: does the game really feed correctly the learning system? As the game does not store any image for ethical and network reasons (bandwidth and storage capacity of the server), the only way to know that is possible by asking to players through the survey and verifying if no cheating is done in the game.

4.2 Results

The data for this analysis has been collected between 1/09/2007 and 16/09/2007 (15 days). There are three sources of information: the game server statistics, the survey and the results from 'comments and bugs' web page. Approximately 700 emails have been sent to invite people to play the game. During this period, 69 accounts have been created and the server accepted 154 connections, 4 games have been played and 4 users at maximum were simultaneously logged on the server. No comments and no bugs have been logged through the 'comments and bugs' web page. Five individuals have taken the survey and for this reason, it is important to contrast results in regards to this little number of answers.

The interface design and its ergonomics are crucial in software, especially in computer games as they greatly impacts the user experience. According to results of the survey, all players have found the game screen intuitive and appreciate the style of the design. The word list also influences the gameplay: globally, words have to be nor too easy either too difficult to find and should not be repetitive. 0% of the answers find the word list too repetitive, 20% find it too hard, 0% too easy and 40% estimate they are originals. We had 2 comments saying that words to find were 'funny' and 'we are not expecting some words, it make works the imagination'. A good way to test if the game is appreciated is to monitor the time that players spend or would like to spend on the game. All players have answered that they would play Pictocam regularly, with 40% every week and 40% less often. 60% are willing to play between 15 and 30 minutes per day and the 40% of other players, less than 15 minutes. Finally, as players have been asked to play through the request of a friend or to a fellow student (the author), 60% of answers declare this is the main reason to play. However the other 40% play mainly because the game is enjoyable. 0% of people play because a research program is associated to the game.

During the 15 days test period, the server has collected 52 shapes and 15 colours for 11 words. According to survey's results, 60% of interrogated people feel that the system recognises the objects shown. Everybody also agrees that the recognition

feedback is useful. Concerning the data quality, 40% of players sometimes do not validate an object that is related to the word requested and these 40% do that once per game (or less).

5 Discussion

Before drawing any conclusions, it is important not to neglect that only few people have answered the survey and this number is not enough to act as solid evidences. The reasons of this little number of results are explained by the following facts:

On the 700 mails sent, 69 people have created an account over 15 days. We had 154 connections, so approximately 10 per days.

The game needs at least 3 people to start a game and we had 4 people maximum connected simultaneously. According to server statistics, players usually connect once to the game: they try to play and quit to never retry if they could not play.

To play the game, players need a webcam: even if this hardware becomes more and more present on home computers, this is not completely common (in 2003, 13% of French families had a webcam according to an IPSOS study (afjv.com, 2004))

To overcome this problem, the web site could be referenced in search engines like Google or Yahoo, or on specialized game sites. The implementation on the server-side of a bot (a simulated player imitating pre-recorded player action) could also provide a way for connected users to play even if there are not enough people.

Unfortunately, the lack of data does not permit to verify properly for the time being if the learning system is coming up to our expectations. For the moment, it is difficult to assess if players are naturally encouraged to take pictures related to the word requested: if the server does not discriminates object classes and the similitude between pictures is naturally high (Coisne, 2007), it is understandable that they can validate irrelevant pictures for the time being. However, results based on tests done by Gousseau (2007) shows that low-levels colours and shapes features are relevant for the study of the language learning. Coisne (2007) also demonstrates that the learning system discriminates different objects.

Despite the lack of data, analysed results concerning the gameplay are very promising. All results show that the interface design is ergonomic and users play because the game is enjoyable, not because they know that they help to a research program.

6 Conclusions

After 15 days of testing with real players, results provided by server statistics and the survey are really promising about the gameplay characteristics of the Pictocam. Even if few results have been collected, it is clear that players enjoy the game and

successfully provide valuable data to the system at the same time, which is the primary goal of this project.

This work could be extended by exploring other ways to learn words with visual recognition, other than simple nouns. The motion tracking used in the background detection could be generalized to learn actions, and the visual recognition could be improved to recognize faces for example. Children learn a language over many years by the intermediate of their senses. However this paper is clearly focused on the visual process. It could be interesting to test if the same game wrapping could be done to train a speech recognition system for example. A more ambitious project could consist of combining two different approaches to learn the meaning of words more efficiently: with the visual object recognition and also by using voice/sound recognition.

7 Acknowledgments

The authors would like to thank Emmanuel Coisne and Pierre Gousseau, for their supports and works. To Tony Belpaeme (project supervisor) for his availability and constant monitoring and to Marie-Thérèse Chevalier for her unconditional support and suggestions.

8 References

Adobe (2007), "Adobe Flash", http://www.adobe.com/products/flash/, (Accessed 13 August 2007).

afjv.com, (2004), "*Les* Français, les loisirs et les nouvelles technologies", http://www.afjv.com/press0306/030626_ipsos.htm, (Accessed 17 august 2007).

Coisne, E. (2007), *Learning System: learn word meaning from image processing*, Master Thesis, University of Plymouth.

Gallese, V. and Lakoff, G. (2005), "The Brain's concepts: the role of the Sensory-motor", *Cognitive Neuropsychology , 22* (3), pp455 - 479.

Glenberg, A. and Robertson, D. (2000), "Symbol Grounding and Meaning: A Comparison of High-Dimensional and Embodied Theories of Meaning", *Journal of Memory and Language , 43* (3), pp379-401.

Google Inc. (2007), "Google Image", http://images.google.com/, (Accessed 26 august 2007).

Gousseau, P. (2007), Extracting visual features using a web RIA technology for experiments on infant language learning, Master Thesis, University of Plymouth.

Harnad, S. (1990), "The Symbol Grounding Problem", *Physica D , 42*, pp335-346.

Spicefactory (2007), "Oregano", http://www.oregano-server.org/, (Accessed 13 Agust 2007).

Sun Microsystems (2007), "Java Technology", http://java.sun.com/ (Accessed 13 August 2007).

von Ahn, L. and Dabbish, L. (2004), "Labeling Images with a Computer Game", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp101-109.

von Ahn, L., Liu, R. and Blum, M. (2006). Peekaboom: a game for locating objects in images. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp55-64.

Stereovision for Navigable Space Mapping

R.Kabbara and G.Bugmann

University of Plymouth, Plymouth, United Kingdom
e-mail: gbugmann@plymouth.ac.uk

Abstract

This paper describes a complete design and implementation of a stereovision system, as being the only sensing device to guide the navigation of an autonomous mobile robot. Many sub-topics from the field of robotics and computer vision are exploited in details as an aid to achieve the desired objectives, under the main goal of accomplishing a successful stereovision-aided navigation. The focus is also on discussing an innovative idea for edge detection and the matching algorithm.

Keywords

Robotics, Stereovision, Navigation, Project, Mapping

1 Introduction

In order to ensure safe robot autonomous operation, the robot must be able to perceive its environment. Therefore, many sensors have been trying to serve this purpose for many years. Examples of those sensors are Infrared, Sonar (Ultrasonic), laser range finder, etc… Nevertheless, all of the listed sensors have disadvantages of a considerable effect on mobile robots. Some are very expensive and efficient; others are cheaper but have very limited range of sensing. Therefore, it is hard to equip a mobile robot with one of these sensors alone and make it fully aware of its environment. Obviously, another sensing breakthrough is needed.

This is where stereovision plays the crucial role. Building a stereovision system consists of using two image capture devices to produce pairs of images of the same scenes; having different but known positions and angles, the cameras provide a geometry which allow the calculation of the depth and position of each point in field of vision.

One other purpose of this paper is to prove that a successful stereovision system can be built with home-use devices, using simple and computationally cheap algorithms.

2 Background Research

2.1 Other sensors for mobile robotics

There exists other approaches to solve the navigable space mapping problem, mostly using combinations of previously mentioned active sensors, as in the work done by (Stolka et al., 2007) where they used sonar for automated surgical processes, guided by infrared. For instance these sensors serve well in applications requiring precision at fairly close distances. But when it comes to mobile robots operating at 1m/s as average speed, the required range for safety would be at least 2 meters. Infrared doesn't even reach this range, and ultrasound loses its angular accuracy at this distance.

2.2 Laser range finder

Laser range finders are much more accurate and reliable for mobile navigation than Infrared and Sonar. They can be used equally in indoors and outdoors applications, having a good sensing range. It works on the concept of laser beam reflection, which in its turn has many drawbacks, mainly safety. In an environment full of human beings moving around the robot, a laser beam may be harmful because of its focused and intense nature. Moreover, the reflection of this light beam can be affected by weather conditions (fog, humidity), as well as the type of the reflecting material. Once again, a more reliable sensor is needed.

2.3 Stereovision in mobile Robotics

Stereovision has a very unique property which allows it to acquire much more data from the environment than other sensors do, being a passive (receptor) sensor which has millions of preceptors (pixels). This gives the designer the privilege to have access to all sorts of information from the surroundings, and then apply the desired filters in order to obtain valid data relative to the application at hand.

2.3.1 Epipolar theory and disparity

Epipolar geometry is the basis for the concept of stereovision, because it provides geometric properties very convenient for matching features in stereo pairs.

The geometry states that, for every point M in space that has an image m_1 on the first camera's retina plane, there exists a line of points m_2 in the second camera's retina that are possible matches for m_1. This is a very important property, since it reduces the matching search space from two-dimensional to one-dimensional, saving precious time and computation. Figure 1 illustrates the geometry.

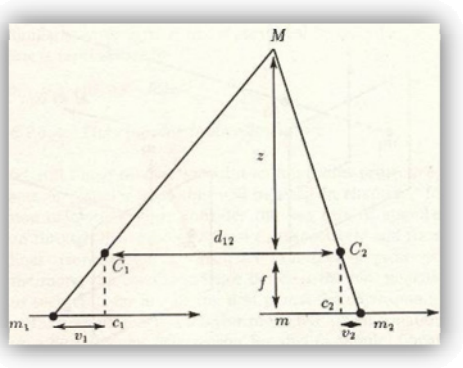


Figure 1: Relation between depth and disparity (Faugeras, 1996)

Thanks to this very crucial property of epipolar geometry, it was possible to extract depth and horizontal position of the point M from the system. The two equations representing relationships of system's different parameters are extracted from the geometry in details by (Faugeras, 1996):

$$Depth\ (m) = \frac{Distance_{Focal\ centres} \times Focal\ length}{Disparity \times Pixel\ Size}$$

$$Horizontal\ position(pixels) = \frac{Distance_{Focal\ centres} \times (v_1 + v_2)}{2 \times Disparity}$$

$$Horizontal\ Position\ (m) = -\frac{x \times Focal\ length}{Depth}$$

Where disparity is defined by: $Disparity = v_2 - v_1$

Provided that v_2 and v_1 are the horizontal coordinates of each image of M with respect to the retina centre it belongs to.

Having these properties at hand, one can estimate distances to objects by comparing their relative shift in pixels between the camera pairs.

3 The stereovision algorithm

The stereovision algorithm consists of several sub-algorithms and process studied separately then evaluated all together as a system.

Camera calibration is the process of rectifying a distorted image generated by a wide angle camera which introduces the fisheye effect. Straight lines are perceived as

curves on the camera's retina, which needs to be rectified before undergoing the next process in the stereovision algorithm. This is not the case for the Logitech Pro 5000 introduced in this paper.

3.1 Edge detection

The edge detection adopted in this paper is an innovative idea, where some of the properties of the pixel are still conserved, unlike other edge detectors. For instance, instead of producing a binarized image, the result is a greyscale image in which sharper edges are represented by lighter pixels and vice versa. This is realized by following these steps:

- Take a 3 x 3 square window, it will contain 9 pixels.
- Find the mean of those pixels' value (choosing Red, Green or Blue as a channel).
- Find the pixel of which the value represents the larger deviation from the mean.
- Represent the group of those 9 pixels in the square, with the value of the maximum deviation. Sharper edges are represented with a brighter pixel in the edge image.
- Move the square 3 pixels to compute the next 9 pixels' maximum deviation.
- The result is an edge image, having ninth the original size, thus ninth the resolution.

The concept is simple; an intense contrast corresponding to a sharp edge presents a group of pixels where the colour deviation is large. A graphical illustration and a produced image are shown in figure 2.

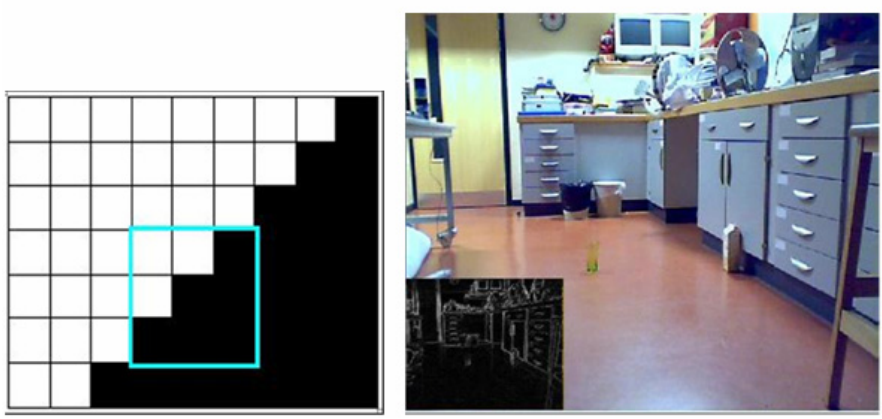


Figure 2: Edge window (left), the edge window generated from room scenery (right)

One way to minimize detection of reflections as an obstacle is setting a threshold. This is supported by the fact that surfaces valuable for finding navigable space and real obstacles are the sharpest, as observed. All other minor are edges either on the surface of an object or from reflections. Since these edges are not crucial for mapping, they can be eliminated. This is very simply done, right before writing the data to the buffer containing the edge pixels. If a pixel's value exceeds the threshold it's left intact, otherwise to black. Figure 3 shows different experimented threshold serving in optimizing the detection. As it is clearly observed, the threshold value is very critical to the stereovision process as a whole. In fact, one of the major key strength of stereovision is that it provides too much detail about the surroundings. It's a waste to lose too much of that information which may be critical for other algorithms. For this specific application, a threshold of 30 is found to provide a good balance (every pixel having a value greater than 30 is left intact, and every pixel having a value lower than 30 is set to black). Setting the threshold as high as 100 suppresses features of the picture that are important to the mapping algorithm such as the meeting edge of walls and ground.

To show the consistency of a threshold of 30, a sample of a light reflecting object is taken with the new setting, in Figure 3.

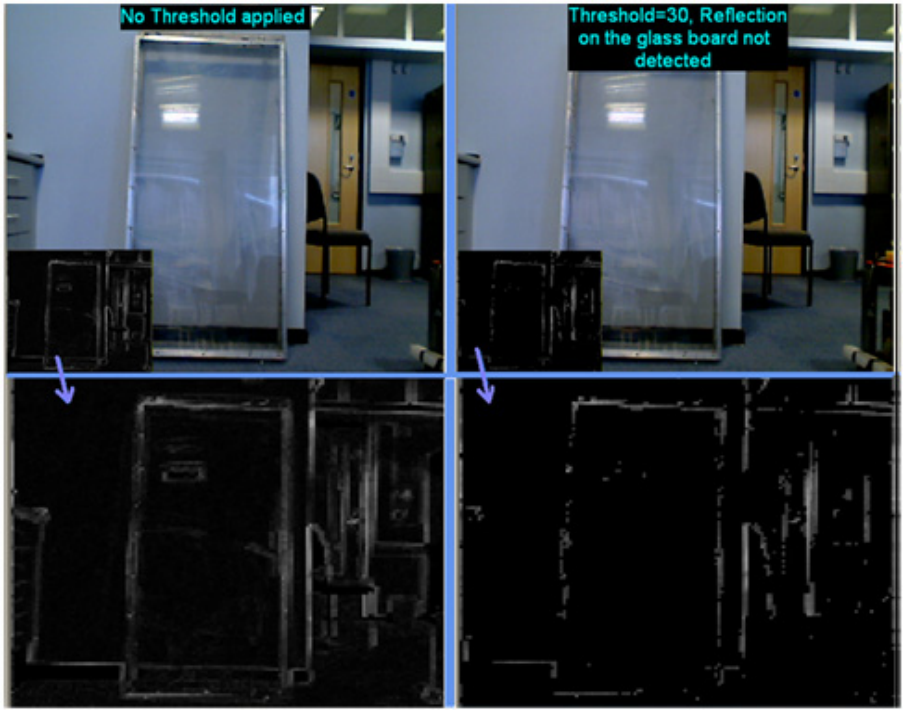


Figure 3: Reflection detection reduced in the edge detection window

After applying a threshold of 30, most of the reflection in the glass board is neglected, while sharp edges are still conserved.

3.2 Feature-based matching algorithm

In order to calculate the disparity, each edge pixel must undergo a matching process to find its corresponding pixel in the second image. (Gutierrez and Marroquin, 2003) described window-based algorithm for matching, on which the one used in this paper is based.

The algorithm is inspired by the innovative one-directional matching algorithm which is described by (Di Stefano et al., 2004). This algorithm, unlike traditional ones, compares pixels from the left image to the right image without the need to apply the process reversely too, to enhance the matching. Instead, a score is assigned to each matching attempt, and then a function finds the pair of pixels showing a minimum matching error.

The paper's matching algorithm introduces a blend of both discussed techniques to give reliable results, since no image rectification is being applied in the beginning. Hence, instead of trying to match the left pixel with the corresponding horizontal line in the right image, a window is considered in the right image to compensate for any non-rectified vertical tilt between the left and the right cameras. Figure 4 and the following steps illustrate how the algorithm is applied.

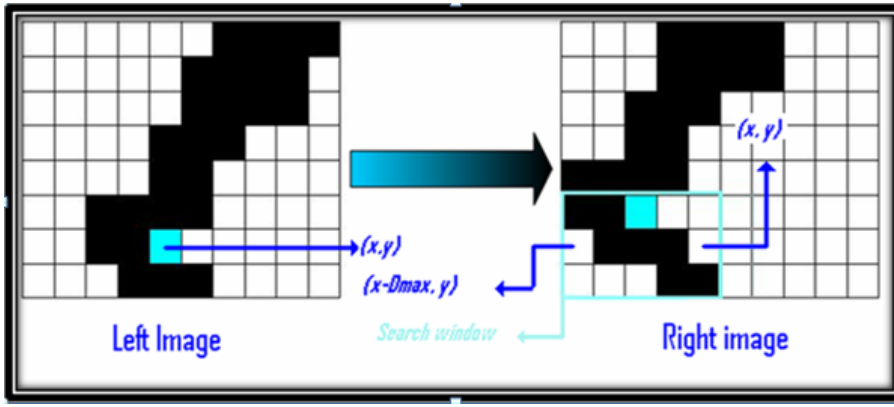


Figure 4: The stereovision matching algorithm graphically represented

Compute the value D_{max} which is the maximum disparity expected to be encountered. It is obtained from the equation described earlier, relating depth and disparity, by specifying the minimum depth before which the robot will be blind.

Find a pixel which value is above the threshold set earlier for edges filtering.

If the pixel's coordinates are (x, y) in the left image, place a search window in the right image of size D_{max} x n (where n is an odd number), centred vertically at y, having the width spread from $(x - D_{max})$ to x. This is logical since the matching right pixel is expected to be found at a position x_2 from x such that $0 < x_2 - x < D_{max}$.

Assigning a score to each matching attempt based on the difference of value between the left and the right pixel under investigation.

The matching is claimed a success corresponding to the pixel whose value minimizes the difference from the left pixel. The algorithm assumes that the pixel in the left image which passed the threshold in the edge detection stage will always find a match in the right image.

The above figure shows that, even though the second image is shifted up relatively, the matching window still contains the matching pixel. As expected, the performance is compromised for the sake of more accurate matching since the computation time is multiplied by the window's height, compared to a single line search presented in (Gutierrez and Marroquin, 2003). But with the processor at hand, this modification does not cause a noticeable delay and compensates for the possible vertical tilt between both cameras.

3.3 Mapping algorithm

The concept of mapping lies in transforming complex data coming from the stereo image pair into two dimensional simple data that the robot can process much easier, in order to assist it navigate autonomously. A very simple implementation of a mapping algorithm is introduced in this paper, since the main algorithm is present at the edge detection and matching stages.

The map is represented as a graph plotting all matched edges whose coordinates are (Horizontal position, Depth) described by the formulas earlier on.

Figure 5 shows the result from the mapping algorithm, where a piece of paper is tested in different positions:

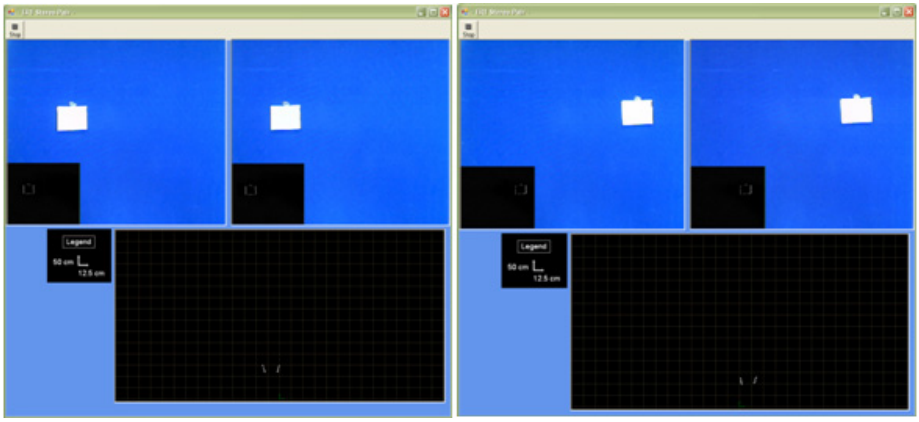


Figure 5: Mapping from a stereo pair

What's mainly noticed in the figure above, is that instead of getting just two points on the map representing both paper edges, the obtained result is two lines of points. This is due to the fact that an edge is not made of a single pixel, but rather of a group of pixels. In consequence, the matching algorithm matches all the pixels which belong to the edge in the left image with all the pixels which belong to the same edge in the right image. For instance, if an edge is made up of 3 pixels, there will be 9 successful matches generating depth and horizontal coordinate slightly different of each other, resulting in a line instead of a point.

3.4 Hardware

The hardware used is intended to show that a simple home-use webcams can provide a satisfying result using simple stereo algorithms.

The cameras are Logitech Pro 5000, mounted on an Evolution Robotics ER1 that supports a laptop as its processing unit. The specifications of the processor are as follows: Intel Centrino 2.0 GHz processor, 2GB of RAM and nVidia GeForce Go 7400 with 128 MB of video RAM. These are top notch specifications but a less powerful system can do the job as well. The system is shown below in Figure 6.

Figure 6: ER1 set up for operation

3.5 Implementation in C#

C# is a .NET framework managed language. With its garbage collector and evolutionary memory allocator, it was a nice to experience graphics programming and image processing in this environment. The libraries which served as basis for the image processing are DirectX's ones from the DirectX SDK 2.0 (August 2007).

The program structure is best described with Figure 7:

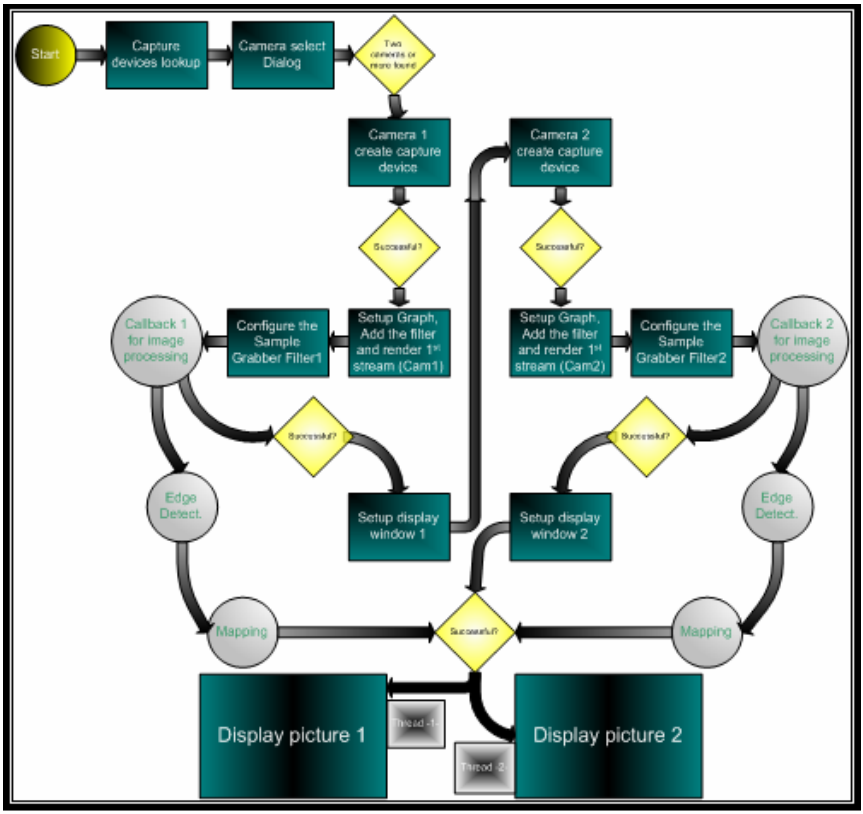


Figure 7: Application flow chart

The objective at hands is to capture two webcams' video streams simultaneously and then apply filters to them in a defined order. A line of data stream coming from the optical device is captured by different filters through pins, which process the picture and then upload it back to the stream.

4 Conclusion

The stereovision algorithm discussed in this paper doesn't produce as satisfying results as expected. This is due to the fact that the matching algorithm relies on the value of each pixel to find its match, which yields to false matches, hence unreliable obstacles map. The edge algorithm is a successful one which preserves the features of the pixels for better matching.

Future efforts are advised to be spent on improving the matching algorithm, which may improve the stereovision algorithm as a whole.

5 Acknowledgments

The author would like to take the opportunity to thank Dr. Guido Bugmann for all the support, help and guidance he provided throughout this paper and the whole Masters year. Thanks must be addressed to Dr. Phil Culverhouse for his valuable advice and help. Finally the author would like to dedicate this paper to his wonderful girlfriend for all the support and encouragement throughout a tough year.

6 References

Di Stefano, L., Marchionni, M. and Mattoccia S. (2004) 'A fast area-based matching algorithm', *Image and Vision Computing*, 22 :983-1005

Faugeras, O. (1996) *Three-Dimensional Computer Vision*, MIT Press, London: 188-189

Gutierrez S., Marroquin J. M., 'Robust approach for disparity estimation in stereo vision' *Image and Vision Computing,* Volume 22: 183-195

Stolka P.J., Waringo M., Henrich D., Tretbar, S. H., Federspil P. A. (2007) 'Robot-based 3D Ultrasound Scanning and Registration with Infrared Navigation Support' *IEEE International Conference on Robotics and Automation*

Impact of Leisure Internet use on Takeup of e-Government Services by Older People

J.D.Kneller and A.D.Phippen

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Considerable resources have been invested in the development of e-government services, including online facilities, in the UK. However, there is debate as to the effectiveness of such provision and in particular there is concern that uptake is not consistent amongst all demographic groups.
This paper discusses research carried out in conjunction with a District Authority in south-west England into attitudes and usage of the Internet in general and whether leisure use of online facilities has an impact on uptake on e-government services. Contrary to expectations based on the uptake distribution of general Internet use, analysis results were mixed and no overall significant difference between the rate of uptake of e-Government services amongst older people and other age groups was found. The most significant impact of leisure use on awareness of e-government is in users in the middle age group (45-64), rather than in the 65+ age group. However, in many areas additional statistical analysis will be required to further investigate the differences between leisure effects in each age group.

Keywords

Citizen engagement; e-government; technology adoption; citizen survey; older people

1 Introduction

There is increasing evidence that the uptake of Internet services is less amongst older people than amongst other demographic groups (Office of Communications, 2007). In the light of recent UK government initiatives to increase the volume and range of local and central government services available on-line, this research aimed to investigate whether, in reality, there is a significant gap in uptake of e-government services amongst older people in comparison with other age groups, and whether the rate of uptake is influenced by involvement in other on-line activities such as genealogy or local history.

What do we mean by the term “older people?” Hawthorn (2000) says that the ‘effects of age become noticeable from the mid forties onward’ but this research used the more common definition of 65 years and older (Eastman and Iyer, 2004; Fox, 2004).

The term e-government includes a very wide range of electronic governmental services including electronic transactions between government departments and from governments to supplier or customer businesses as well as interaction between authority and citizen. This research concentrates on the aspects of e-government that provide opportunities for interaction and transaction between central and local government organisations and citizens via facilities offered over the Internet.

2 Previous Studies into age disparity in IT use

Studies into Internet usage consistently show variations in uptake based on age. Table 1 summarises results from three studies across the globe.

Study	Young Users		Older Users	
UK, 2007, (Office of Communications, 2007)	18-24 years	65%	65+ years	16%
US, 2004, (Fox, 2004)	18-29 years	77%	65+ years	22%
China, 2000, Tan and Clark (2000)	21-30	51.3%	50+ years	1.6%

Table 1: Comparison of studies into Internet usage by age group

A large variety of reasons have been suggested for this disparity in usage and studies often produce contradictory evidence. There are four primary themes that run through the literature:

- Physical or Accessibility barriers
- Social or Domestic Barriers
- Personal Attitudes and Concerns
- Usability and Training Needs

2.1 Physical or Accessibility Barriers

Much of the research carried out in the 1980s and early 1990s into the use of computers by older people focussed on the physical barriers which they might encounter. Sourbati (2004), suggests that the mouse is a particular difficulty for some older people, and suggests that a heavier mouse might assist some users. The keyboard was also highlighted as a problem for patients with arthritis in their hands.

2.2 Social or Domestic Barriers

Many authors suggest that demographic factors have a strong influence on the uptake of regular Internet use amongst the older age groups. Morell et al., (2000) propose that education is a strong predictor of Internet usage amongst older people. Household income also seems to be closely related to Internet uptake (Eastman and Iyer, 2004) - the higher the household income, the more likely older people are to be Internet users. Other authors (Fox, 2004 and Sourbati, 2004) suggest that previous experience of computers can have both positive and negative impacts – positive first

experiences can increase future use, but a perception of computers as being a part of business life can have a negative impact amongst retired citizens.

2.3 Personal Attitudes and Concerns

Age Concern (2002) commissioned a report on the uptake and use of computers in a group of people aged 55+ in the UK. Their findings support the theory that, once using computers, most older people see a benefit to their lives – 55% of those using IT said the 'Internet had a positive effect on their lives'; only 2% said it had a 'negative impact'. However, the report still highlights a lack of interest in using the Internet amongst non-users - 41% of non-users said they were not interested and 8% 'expressed fear of modern technology and said they lacked the confidence to use IT'. This report reflects many others in that it shows the most common activities as contacting family and friends and referencing information about hobbies.

2.4 Usability and Training Needs

There seems to be a consistent theme running through all the literature that, given sufficient motivation, older people make regular use of personal computers and the Internet. However, in order for them to feel both competent and comfortable with the new technology, they must receive training tailored to their learning needs. (Eastman and Iyer, 2004). This means that the training must generally be at a slower pace than for younger learners, with plenty of time for repetition to reinforce the learning.

Thus, the factors influencing older people's uptake of IT generally and, specifically, Internet usage are complex.

3 E-government in the UK and the need for research

Services to the citizen are provided by public sector organisations at all levels of UK government – from central government departments, through government agencies to smaller local authorities. There has been a significant push towards alternatives to conventional face-to-face service delivery. The strategy for the move towards e-government in the UK was set out by the UK Government's Performance and Innovation Unit (2000) stating that "government's online activities must be driven by levels of use and by citizen preferences". Thus it was recognised early in the project that e-government could only be successful if it was accepted by the public. Since then the UK government has devoted huge resources to the development of on-line services but there seems to have been very little Government-sponsored investigation into differences of uptake between different demographics groups and the reasons behind this.

The Varney report on Service Transformation (Varney, 2006) identified areas of success in service provision and set out recommendations for future development of all aspects including e-government. However, it goes on to state that citizens will naturally compare e-government services with similar services provided by private sector organisations and consequently success will, in part, depend on the quality of

such services and the perceived benefit that the citizen gains from using e-government services rather than more conventional access channels. In turn, understanding the citizens' perspective is essential.

In order that all the resources put into their e-government services are not wasted, it is vital that local and central government understand what factors influence their citizens to use or not use the services they provide.

4 Experimental Design and Method

From the review of previous studies described above, two research hypotheses were defined:

H1: There is a significant difference between the rate of uptake of e-government services amongst older people and other demographic groups.

H2: Non-IT-focussed use of the Internet influences the uptake of e-government services amongst older people.

In order to gather data to inform research into the above objectives, the researcher decided to conduct a survey of citizens aged over 16 who might reasonably be expected to use a variety of services offered by local and central government. The research study was carried out in Devon, in the south-west of the UK. County-level government is provided by Devon County Council. This is divided in a number of District Authorities and Unitary Authorities including Teignbridge District Council which has a mix of small towns and rural areas, including parts of the Dartmoor National Park.

The average age in Teignbridge is 42.84 years, with people aged 65+ years making up 21.91% of the population (National Statistics Online, 2006). This shows a considerable difference from the UK average age of 38.6 years (65+ years: 15.89%), and so form a prime target population for studies of older people. Furthermore, Teignbridge District Council (T.D.C) is unusual in that the Council hosts two web sites - the official www.teignbridge.gov.uk Council web site (T.D.C. website, 2007) and www.teignbridge.info (Teignbridge.info website, 2007) which is a site hosted and content managed by T.D.C. but with most content contributed by local residents.

In order to inform research to fulfill the project objectives, the researcher specifically needed to the capture the views of and awareness information from non-Internet users as much as those of users. Therefore an Internet-based survey was not an option. Thus the most practical alternative approach was to distribute a postal survey. The Council agreed to issue the survey, on behalf of the researcher, to a sample of 1033 of the existing T.D.C "Citizen's Voice" Customer Panel and Youth Council.

The survey instrument investigated e-government uptake in a variety of ways. Firstly it offered respondents a selection of eight online government services and were asked to indicate which they were aware of and which they had used. The list was chosen

to be likely to appeal to a range of age groups, and to include a mix of transactional and informational services and central and local government responsibilities. The proffered options were: renew your passport, buy a fishing licence, tax your vehicle, submit income tax returns, find a doctor, register to vote, submit a planning application, check your local library account and an "Other" option was added. As a second level of investigation, respondents were asked which of the following government websites they were aware of and which had used: Teignbridge District Council website (2007), Teignbridge.info community site (2007), Devon County Council (D.C.C.) website (2007) and DirectGov (2007).

As a measure of their leisure use of the Internet, respondents who were Internet users were asked to indicate which of a list of online hobby activities they participated in (and how often). The list was chosen to appeal to wide range of age groups: Genealogy/Family History, Local History, Gardening Tips, Routes for walking etc, Education (e.g. University of the Third Age), Food and recipes, Making travel plans, Reading online newspapers, Booking theatre/cinema tickets, Online games (plus an "Other" option). Results for each respondent were combined to give a Variety score (how many of the activities they participated in) and a "Average frequency" score (a measure of the how often they participated in these activities). These two new variables were created to give a (somewhat subjective) estimate of the relative "sophistication" of the individual's Internet use.

5 Results

From the sample of 1033, 611 valid responses were received. Data was analysed using the SPSS statistical package and Chi-squared goodness of fit tests used to analyse the categorical data produced from the survey instrument. In order to get statistically valid results from the Chi-squared technique, results were condensed into three age groups: 16-44 years; 45-64 years; 65+ years.

A large number of different tests were carried out. For each test a null hypothesis was constructed that there was no statistically significant relationship between the two variables. The results are given in Table 2. Results were considered statistically significant and the null hypothesis rejected at SPSS significance less than 0.05. A number of tests did not meet the assumptions necessary for the Chi-squared test to be valid. These are marked as Invalid tests. The Cramer's V statistic was used to indicate the strength of association between variables. Cramer's V has a range of 0 to1, with 1 indicating a perfect association.

6 Discussion of results

The research set out to investigate the two hypotheses stated at Section 4. Null hypotheses were constructed as follows:

Null H1: There is no significant difference between the rate of uptake of e-government services amongst older people and other demographic groups.

Null H2: Non-IT-focussed use of the Internet has no impact on the uptake of e-government services amongst older people.

H1 was tested in two ways: by looking at the awareness and usage of 8 generic e-government services; and by looking at the awareness and usage of four selected e-government websites. As shown in Table 2, no statistically significant relationships were found between Age and Awareness of the 8 general e-government services; or Age and Usage of the 8 general e-government services (although the relationship is significant at lesser levels of confidence, $0.1<p<0.05$). Significant relationships were found between Age and Awareness of Teignbridge.gov.uk; and Age and Awareness of Devon County Council website. Furthermore significant relationships were found between Age and usage of all four specified sites.

Thus overall, it is suggested that there are some effects of age on both awareness and usage when considering individual websites. However, for the 8 general e-government services listed, initial results on the relationship between age and awareness are negative and additional research must be done to further investigate the suggested relationship between age and usage. Overall, **Null H1** cannot be conclusively rejected and it must be assumed that there is no significant difference between the rate of uptake of e-government services amongst older people and other demographic groups.

H2 was tested by looking at the impact of leisure usage and variety on awareness and usage of the generic e-government services and selected e-government websites above. Statistically significant relationships were found between both Age and Variety of leisure use and Age and Average Frequency of Leisure Use (when banded into low and high levels of usage).

Finally the number of generic e-government services were banded into low, medium and high awareness and usage, and the differences between leisure effects on e-government awareness and usage in each age group were investigated. All tests for both Usage and Frequency of leisure use were invalid based on the constraints of the Chi-squared test, and further more sensitive tests would need to be applied to investigate such effects. However, some valid results were achieved from the tests between Awareness and Variety of leisure usage. Although, the test was invalid for the 16-44 age group, it was valid for the 45-64 and 65+ age groups. The null hypothesis, **Null H2**, could not be rejected at the 0.05 significance level for the 65+ age group, but could be rejected for the 45-64 age group.

Thus there is an apparent impact of leisure use on awareness of e-government in the middle age group (45-64), but there is no such effect in the 65+ age group. The effect is such that where high levels of leisure use exist, the awareness of e-government sites is higher than might be expected by chance.

However, for results, the values of Cramer's V are relatively small and suggest that even where there are statistically significant effects, the size of the effect is not particularly large i.e. there may be more significant factors impacting usage.

7 Conclusion

Contrary to expectations based on uptake of the Internet generally, there is no overall significant difference between the rate of uptake of e-government services amongst older people and other age groups, although there may be some relationships indicated for individual websites. The most significant impact of leisure use on awareness of e-government is in users in the middle age group (45-64), rather than in the 65+ age group. However, in many areas the research has been inconclusive, and additional statistical analysis will be required to further investigate the differences between leisure effects in each age group. Furthermore, given the low values of Cramer's V, further research is required to investigate other factors that might impact awareness and usage of e-government sites.

Test	χ^2 (df)	Significance value from SPSS	Cramer's V	Comment
Age*LeisureVariety	23.129 (6)	0.001	0.160	Valid test – significant result
Age*AverageLeisureFrequency (4-Banded)				Invalid test
Age*AverageLeisureFrequency (2-Banded)	1.090 (2)	0.580	0.050	Valid test – not significant
Age*TDC.gov.ukAwareness	16.782 (2)	0.000	0.175	Valid test – significant result
Age*TDC.infoAwareness	0.776 (2)	0.678	0.038	Valid test – not significant
Age*DCCAwareness	14.575 (2)	0.001	0.163	Valid test – significant result
Age*DirectGovAwareness	3.710 (2)	0.156	0.082	Valid test – not significant
Age*4SiteAwareness	5.784 (2)	0.671	0.082	Valid test – not significant
Age*TDC.gov.ukUsage	27.497 (2)	0.000	0.245	Valid test – significant result
Age*TDC.infoUsage	7.308 (2)	0.026	0.145	Valid test – significant result
Age*DCCUsage	29.914 (2)	0.000	0.261	Valid test – significant result
Age*DirectGovUsage	12.805 (2)	0.002	0.194	Valid test – significant result
Age*4SiteUsage				Invalid test

Age*8-type egovAwareness	3.709 (4)	0.447	0.065	Valid test – not significant
Age*8-type egovUsage	8.226 (4)	0.082	0.132	Valid test – not significant
Age (16-44)*egovAwareness*LeisureVariety				Invalid test
Age (45-64)*egovAwareness*LeisureVariety	8.028 (2)	0.018	0.271	Valid test – significant result
Age (65+)*egovAwareness*LeisureVariety	1.941	0.379	0.159	Valid test – not significant t

Table 2: Results of statistical analysis of Teignbridge survey data

8 References

Age Concern (2002) *Management Summary: IT, Internet and Older People* Available HTTP: http://www.ageconcern.org.uk/AgeConcern/media/Quant_exec_report_ext.pdf (Accessed 28 Nov 2004)

Devon County Council (2007), http://www.devon.gov.uk/ (Accessed 3 February 2007)

DirectGov website (2007), ttp://www.direct.gov.uk/en/index.htm (Accessed 3 February 2007)

Eastman, J.K. and Iyer, R. (2004) 'The elderly's uses and attitudes towards the Internet' *Journal of Consumer Marketing*, 21 (3): 208-220

Fox, S. (2004) *Older Americans and the Internet* Pew Internet and American Life Project. Available HTTP: http://www.pewinternet.org/pdfs/PIP_Seniors_Online_2004.pdf (Accessed 13 Dec 2004)

Hawthorn, D. (2000) 'Possible implications of aging for interface designers' *Interacting with Computers*, 12 (5): 507-528

Morrell, R., Mayhorn, C. and Bennett, J. (2000) 'A survey of the World Wide Web used in middle-aged and older adults' *Human Factors*, 42 (2): 175-182

National Statistics Online (2006) *Key Statistics for local authorities in England and Wales Part 1* Available: http://www.statistics.gov.uk/downloads/census2001/KS_LA_E&W_part1.pdf (Accessed 18 March 2006)

Office of Communications (2007), Communications Market Report, Available http://www.ofcom.org.uk/research/cm/cmr07/cm07_print/ (Accessed 23 August 2007)

Performance and Innovation Unit (2000) *e.gov: Electronic Government Services for the 21st Century* Available HTTP: http://www.strategy.gov.uk/downloads/su/delivery/e-gov.pdf (Accessed 27 Oct 2006)

Sourbati, M. (2004) *Internet use in sheltered housing. Older people's access to new media and online service delivery* For the Joseph Rowntree Foundation. Available HTTP:http://www.jrf.org.uk/bookshop/eBooks/1859351697.pdf (Accessed 28 Nov 2004)

Tan, X. and Clark, T.H.K. (2000) *Internet as a Mainstream Communication Medium – An Empirical Study of User Demographics* Available: http://www.its2000.org.ar/conference/zixiang_clark.pdf (Accessed 13 Dec 2004)

Teignbridge District Council website (2007), http://www.teignbridge.gov.uk/ (Accessed 3 February 2007)

Teignbridge.info website (2007), http://www.teignbridge.info/ (Accessed 3 February 2007)

Varney, D, (2006) *Service transformation: A better service for citizens and businesses, a better deal for the taxpayer* Available http://www.hm-treasury.gov.uk/media/4/F/pbr06_varney_review.pdf (Accessed 3 August 2007)

Investigating Options of Securing Web Application

T.Meemeskul and P.S.Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

This research paper represents and explains the web application's major vulnerability as well as displaying easy functions to secure web applications. In the background it shows the brief internet threat report. The approach is based on the assumption of "Network Good – Application Bad". The Results of test show the reason why security options are not able to secure web applications.

Keywords

Security Awareness, Vulnerability, Web Attack, Security Option

1 Introduction

Web technology has enabled a new direct channel for communicating between client and server over Hyper Text Transfer Protocol (HTTP). Many visionary businesses take advantage of web technology to expand their network to users. It provides more alternative choice for developers selecting technology to operate their computer systems. In the same way, it motivates attackers to keep an eye on new web technologies and investigate loopholes of the application that enables port 80 to run all the time. Vulnerability begins with several developers, those who are inexperienced and have a limited knowledge of web technologies leaving them to remain unaware of security threats, more and more achieve various solutions to implement web systems but in limited time only. Without the principles of web security, the appearing gateway from failure in configuration and programming attracts attackers to break the web system. In addition, the limits of web technology itself raise the risks, the attackers approach is also more various than the protecting function.

Security options are designed to protect and defend as safeguard from unauthorised access which intends to break a web system. Many software vendors release security options for supporting unaware web developers, web administrators and web clients who are the key aspect involved with web security. However, security options unpreserved all the characteristics of web attacks even web applications and web servers run behind a firewall. HTTP port 80 is still enabling any HTTP request from web clients. The web application source code which interfaces with the web server and back-end database is available to be a device for attackers breaking into the web

system. The best options of securing web application has become security awareness from web developers, web administrators and web clients

2 Background

With web technologies, the communication service to the web is established when user's mention input into the Uniform Resource Locator (URL) in the Web browser, intern Web browsers running on the Application Layer open HTTP port 80, to send HTTP requests to web servers. User's input transforms to be a data packet to pass through the Transport Layer, Network Layer and Data Link Layer. The packet which runs inside a communication cable would be sent to the web server as mentioned in the URL. When web servers receive HTTP request, it would transmit them to web applications for executing data. Web applications would query data in database and return it back to the web server. Web servers would send the response to the users request back as hypertext or plain ASCII text and it would then terminate the connection after it receives an acknowledgement packet from the web client or after a server timeout due to 15 seconds without activity. If the connection is broken while the web server is responding, web servers would contribute an error message as text in HTML syntax (Cisco 2005).

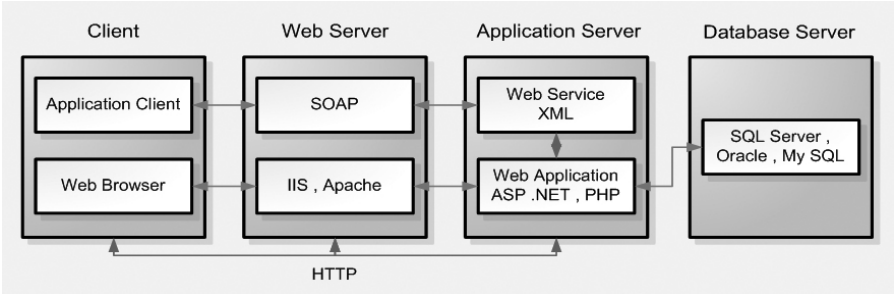


Figure 1: Web Mechanism

Now, many options are available for securing the connection between HTTP servers and the web clients. Secure Socket Layer (SSL) released to protect the private connection between web client and web servers by the use of cryptography protocol. In addition, the release of web application firewalls to also support HTTP servers for filtering HTTP request and controlling Buffer Overflow. In the same way, web developing tools released validation tools for validating input into the web application. However, more concentration from web developers focuses on other points rather than source code.

Basically, the major vulnerability of web applications is Invalidated Input (Huseby 2004). It is a vulnerability that web developers remain unaware about due to difficulty in determining input scope. Attackers are able to use input which affects the code in a web application attack of web system. This is because web developers do not determine the scope of input received from users. Attack can investigate

loopholes in source code and submit input which affects the commands in the source code to obtain data back. It is possible for this vulnerability to occur with all the web pages who provide textbox or textarea to receive data from users. Invalidated Input relates to forced browsing, command insertion, cross site scripting, buffer overflows, format string attacks, SQL injection, cookie poisoning, and hidden field manipulation vulnerability.

Rank July–Dec 2005	Rank Jan–June 2005	Port	Service Description	Percent of attackers July–Dec 2005	Percent of attackers Jan–June 2005
1	3	1026 UDP	Various dynamic services	17%	9%
2	1	445 TCP	CIFS/SMB (Microsoft Windows File Sharing)	12%	18%
3	5	443 TCP	Secure World Wide Web (HTTPS)	8%	7%
4	4	80 TCP	World Wide Web (HTTP) services	8%	7%
5	6	25 TCP	Simple Mail Transfer Protocol (SMTP) services	8%	6%
6	2	135 TCP	DCE-RPC (remote Microsoft Windows communication)	8%	13%
7	10	6346 TCP	Gnutella (file sharing)	5%	3%
8	9	139 TCP	NetBIOS (Microsoft Windows File Sharing)	5%	3%
9	7	4662 TCP	Edonkey (file sharing)	3%	5%
10	17	6881 UDP	BitTorrent (file sharing)	3%	1%

Figure 2: Top Attack Port from Symantec Internet Threat Report 2005

In the Internet Threat Report 2005 from Symantec represent HTTPS port 443 is ranked number 3 and HTTP port 80 is ranked number 4. However, the percentage of attacks for them are equal, they had 8% of overall attacks each (Symantec 2006). The result is possible to put into 2 points of view; Firstly, SSL is not secure, it might use self sign digital certificates and attackers can use sniffer software, to find the certificate code. Therefore, attackers are able to use man in the middle to attack web sites. Secondly SSL and networks are secure but web applications contain vulnerabilities. In this case the open loophole for attackers to use is Invalidated Input to attack the web.

3 Methodology

The vulnerability in the web application occurs because web developers are concern with the security of the connection between HTTP server and web client rather than source code. The vulnerability that's contained on web servers is difficult to solve. It is a big project that can be divided into many web developers programs. If only one web developer is unaware about security and leaves even one line of code that contains vulnerabilities, it means attackers are able to attack the whole web system. For web developers, they should be concerned with their source code before securing other applications or networks.

3.1 Approach

This research test is based on the assumption of "Network Good; Application Bad". The test would implement web systems by installing Apache HTTP server in Linux Fedora, all data would be stored in MySQL database connected with a PHP web application. All connection ports were closed by firewall except HTTP port 80 and HTTPS port 443. The authentication web page runs on HTTPS that uses OpenSSL certificate.

```
<?php
$con = mysql_connect("localhost","root","Timmy_21");
if (!$con)
  {
  die('Could not connect: ' . mysql_error());
  }
$user=$_POST['uname'];
$password=$_POST['password'];
$link = mysql_connect("localhost", "root", "Timmy_21");
mysql_select_db("timdb", $link);
$result = mysql_query("SELECT username,password FROM timusers
WHERE username='$user' and password ='$password'", $link);
$num_rows = mysql_num_rows($result);
echo "$num_rows Rows\n";
if ($num_rows == 0 )
   echo "Please enter the right password";
else
   echo "Found in database";
mysql_close($con);
?>
```

For the test, after entering input into the login form, form data uses the POST method to send data passed to the standard stream which is the connection for transferring input or output between computer applications. Form data would transform to $user variable, $password variable before sending variables into the SQL query command. If the data matches the data in the database, the web page would represent the number of rows which are matching. If the data is not matching, the result would be represented to users as "Please enter the right password".

The first test is sending the right username and password in there, the results found are normal. The Second time test is sending SQL code rather than username and password. The code is 'or '1' = '1. The results are in the following section.

4 Experimental result and Discussion

The results from previous section represent that the SQL code which entered was found in database. The SQL query in the source code executes input to be like this:

```
SELECT username,password FROM timusers WHERE Admin =  '  '  or
'1' = '1' and Timmy = '  '  or '1' = '1'
```

Actually, the database stores the username “Admin” and password “Timmy”. This code is following the tutorial online and some books. It means many authors aimed to teach new web developers how to understand to use the command only. They are not supporting any principle of security to web developers, not even easy functions such as preg_match. In PHP, function preg_match is used to compare matching input that passes to check it in function preg_match (Zandstra 2002). For example with the code below, before sending the code to query in the database, there should be input filtering such as character querying, for characters that possibly affect the source code.

```
<?php
function validateinput($uname2,$password2)
{
       if   (preg_match("/^[A-Za-z0-9_.=+-]+@([a-z0-9-]+\.)+([a-
z]{2,6})$/",$uname2))
       {
              if             (preg_match("/[A-Za-z0-9!@#%&*)(}{_-
]/",$password2))
              {
                     $uname3=addslashes($uname2);
                     $password3=addslashes($password2);
                     $link = mysql_connect("localhost", "root",
"Timmy_21");
                     mysql_select_db("timdb", $link);
                     $result        =        mysql_query("SELECT
username,password FROM timusers WHERE username='$uname3' and
password ='$password3'", $link);
                     $num_rows = mysql_num_rows($result);
                     if ($num_rows == 0 )
                            header("Location: 404.html");
                     else
                            header("Location:
http://www.plymouth.ac.uk");
                     mysql_close($con);
              }
       }
       else
       {
              header("Location: 404.html");
              die();
       }
}
$uname2=$_POST['uname'];
$password2=$_POST['password'];
validateinput($uname2,$password2);
?>
```

In the function preg match, it requires an email for the username. If the username those users enter is not an email, the web site would redirect users to an error page provided. Basically, the source code above uses double filter input, after passing function preg_match, it uses function addslashes before transforming user’s data into

a variable for querying. Better ways could web developers not sending any input to query in the SQL query command because most of attackers are able to break the basic code of SQL. Web developers should transform data that's queried in the database into variables and compare them with user's input rather than send user's input to query the data.
ASP.NET, Visual Studio 2005 provides a validation tool to filter the user's input (Ladka 2002). The RegularExpressionValidator from ASP.NET is able to validate input before submitting data to process. It works with object that web developers require to validate input. This method is better than the function from PHP because it is an automatic tool. For PHP, web developers still have to program it by hand.

```
<asp:RegularExpressionValidator
ID="RegularExpressionValidator1" runat="server"
ErrorMessage="Invalid Username"
Style="z-index: 101; left: 252px; position: absolute; top:
16px" ControlToValidate="txtUsername"
ValidationExpression='^[A-Za-z0-9_.=+-]+@([a-z0-9-]+\.)+([a-
z]{2,6})$'></asp:RegularExpressionValidator>
<asp:RegularExpressionValidator
ID="RegularExpressionValidator2" runat="server"
ErrorMessage="Invalid password"
Style="z-index: 100; left: 252px; position: absolute; top:
61px" ValidationExpression="(?!^[0-9]*$)(?!^[a-zA-Z]*$)^([a-zA-
Z0-9]{8,10})$"
ControlToValidate="txtPassword"></asp:RegularExpressionValidato
r>
```

The code above shows that in the txtUsername and txtPassword strict the input. The input for txtUsername should be an email only. For the txtPassword, it must be between 8 and 10 characters, contain at least one digit and one alphabetic character, and must not contain special characters. That is the recommendation from Microsoft. However, very strong passwords should include special character because they are not query character. The advantage of determining input is not only securing the web but when the web was attacked, it is easy to investigate the problem. Web developers are able to cut out the problems from input and find problems in other resources.

5 Conclusion

Obviously, all web vulnerabilities that occur are involved with security awareness. Many web developers misunderstand that options could secure their application even if it contains vulnerabilities. They are concerned more about options to secure their mistakes. They are not aware enough to improve their codes while programming. Actually, the first option to secure web applications is security awareness from web developers, and it's the best option and where they should begin. This research tries to investigate many options for securing web applications but the answer shows problems occur while programming web pages for testing. Security awareness from all the entities involved with the web application is the best option found from this research. To improve web security for future, it should start now. The first tutorial of

web developers should be basic concepts of web security rather than how to use connection string to connect with the database. For users, before teaching them to know how to use a search engine, change the ideas to how to set a strong password. In the authentication page they should provide a link for teaching users to set a strong password. That is the future plan for reducing the percentage of web attacks.

6 References

Cisco (2005), Cisco *Network Academy Program CCNA 1 and 2 Companion Guide*, Cisco Press, USA, ISBN 1-58713-150-1.

Huseby, S.(2004), *Innocent Code*, Wiley, England, ISBN 0-470-85744-7

Ladka, P. (2002), *ASP .NET for Web Designer*, New Riders, USA, ISBN 0-7357-1262-X.

Symantec (2006), 'Internet Threat Report July –December 2005', available from: http://www.symantec.com/enterprise/threatreport/index.jsp. date visited: 31 July 2006

Zandstra, M. (2002), *Tech yourself PHP in 24 hours*, SAMS, USA, ISBN 0-672-32311-7.

Implementation of a Content Management System for STEER Project at Port Isaac

M.Mudaliar and A.D.Phippen

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Port Isaac is a village in North Cornwall. The Port Isaac community is presently undergoing regeneration. The aim of this research to select an appropriate content management tool that facilitates in the regeneration of the Port Isaac community. In order to achieve this, the researcher has implemented the Drupal content management system for the community. The decision to implement Drupal is based on an investigative evaluation. The new website using Drupal is expected to offer more flexibility to the users. The complete implementation of the CMS in the community will help in evaluate its impact on the Port Isaac community.

Keywords

Virtual community, CMS, Drupal, Port Isaac, OpenSource

1 Introduction

Port Isaac, a village in North Cornwall, is a real world community that needs regeneration. The members of the community need a forum to interact with one another. The task in hand is to accommodate specific needs of the community as a whole that could enable it to regenerate its social and economic well being.

The purpose of this research is to select an appropriate content management tool that facilitates in the regeneration of the Port Isaac community. In order to achieve this it became imperative for this researcher to have a thorough understanding of two inter-related, yet conceptually separate topics, virtual communities and content management systems.

The first section of this research paper attempts to present a brief overview of virtual communities and content management systems. The second section provides information on the research methodology and experimental design adopted for the research and the third section states the results of the experiment, its implementation and the impact of such implementation. The paper ends with a few concluding thoughts from this researcher.

2 Virtual Communities

A community that is established in a cyberspace unlike societies in the real space is called virtual community. It is a community of people sharing common interests, ideas and more importantly human feelings over the Internet. Howard Rheingold coined the term virtual community.

3 Content Management System

By definition, it is a set of technologies and disciplines deployed in order to manage and exploit the unstructured information assets represented by any electronic or paper file, and delivered automatically and in a personalised form to web sites and other electronic and paper delivery channels. The information is used in support of organisational processes or goals, or as a container of the intellectual capital. (Strategies Partner International Limited, 2006)

4 Research Approach

The approach adopted by this author to suggest an appropriate content management tool is based on arriving at answers to some simple yet important research questions.

- What is the experience of being a member of a virtual community?
- Which CMS tools will participate in the investigative study and why?
- What are the parameters against which the tools are evaluated upon?
- Approach for addressing the questions

4.1 The experience of being a member of a virtual community

In an attempt to understand the experience of being a member virtual community, this author studied three existing virtual communities. By registering as a member, the author was able to identify the features of the community and evaluate the experience of being a member of that community. The communities that were a part of the study include ifood.tv (a video food community), myhealthbutler.com (website that offers information on preventive health) and wikipedia.org/ (popular online encyclopedia).

4.1.1 Choice of the CMS tools

The approach followed in this research to select a CMS tool is *Requirement-Driven*. The selection criteria in this approach are against a set of arbitrary requirements of the community in question. This approach reduces the risk of failure and also resolves the problem of comparing wide range of products against one another. It is a sensible way to begin the selection process.

4.1.2 Popularity as a Criterion

The idea behind using "popularity" as one of the criteria is to filter out any obsolete content management systems. While exploring the available CMS tools, the author came across two most popular CMS tools. As per the popularity list mentioned in the "opensourceCMS" site, the top two CMS tools are Drupal and Joomla. Since Joomla is a bi-product of Mambo, the author decided to choose Mambo instead of Joomla. The popularity was calculated based on a parameter called "ratio". Ratio is calculated by dividing the number of hits by the number of days that a particular CMS started its Demo. It should be noted that "hits" is the number of times a particular CMS was accessed and "Days" is the duration that a particular CMS was open for demo. As per this list, Drupal gets 1186.59 points (2125695 hits / 1793 days) and Mambo gets 600.48 points (1016610 hits / 1693 days). (OpensourceCMS website)

4.1.3 Experimental metrics

The author is of the opinion that the user friendliness of the new system and the flexibility it offers will have significant impact on its acceptability. Due to this fact, 'ease of use' was selected as one of the main parameters in the experiment. The nature of the occupations of the members and the availability of resources led to the decision of selecting 'time consumption' as a quantitative metric in the experiment.

5 Experimental Investigation

5.1 Aims

To compare two CMS tools, namely, Mambo and Drupal to select the most appropriate one for a virtual community (Port Isaac, North Cornwall)

Evaluate the selected tools on the basis of usability and performance (time taken to complete specific tasks)

Comment on the suitability of the tools for implementation on the above mentioned virtual community website

5.2 Set the stage

Ideally, to conduct this experiment, there are certain conditions that had to be met. For example, the system on which the experiment was to be done had to have PHP, SQL database and a web server installed. Since it was not possible to get such a system that had all these applications installed, the author decided to conduct the experiment on an online demo version. The steps that were taken to initiate the experiment are as follows.

- Go to http://www.opensourcecms.com

- Create an user account and log into the site
- On the left side of the screen, under "portals", click on either Mambo or Drupal.
- This will display the page where you should be able to log in as administrator.
- The following were the criteria for the experiment.
    - Upload content
    - Create new tabs
    - Create new user account
        - As a user
        - As an administrator

5.3 Experiment 1 – Uploading content

The first tool to test was Mambo. Although the interface of Mambo was impressive, its drawbacks did not escape the author's attention. The time taken to perform each of the above tasks took significantly longer as compared to Drupal. Please refer to the statistics below.

Description	Mambo	Drupal
Upload a page with few lines of content	6.217 sec	1.012 sec

In Mambo, with the existing settings, it was not possible to upload content directly. The author could only edit the existing files. However, to create and upload customized content, the author had to first create a section, then create a category for it and then link it with the section. Only then it would be displayed in the main menu. After the section was displayed, it was possible to upload the content. Uploading content on the Drupal was fairly simple. Another interesting point to note is that there were fewer clicks to upload content in Drupal. By default, the site had fewer menus displayed. There is an option to display or hide menus in the settings.

5.4 Experiment 2 - Creating a new tab

Description	Time taken in Mambo	Time taken in Drupal
To create new tabs	19.047sec	15.846 sec

Then the next experiment was to check creating new tabs. In mambo, when the tabs are created, it by default takes the content of the previous tab. So it would be an exact replica of the previous one. Incase this duplication is not desired, all content is to be deleted and then new content should be added. On the other hand creating tabs had a different approach and look in Drupal. The steps were very simple and self explanatory. Another interesting feature of this system is that the menus expand when you click on them. Unlike Drupal, Mambo would take the user to a different page to display submenus. In the process, the time delay in displaying the submenus is evident.

5.5 Experiment 3 - Creating user accounts

Description	Time taken in Mambo	Time taken in Drupal
To create user account	4.27.015 mins	1.08.953 mins

In this experiment, the ease of creating the user account was tested. The process went smoothly and about four user accounts were created in Drupal. The user accounts could be created either by the user or by the administrator. The administrator's interface is more advanced and he would be able to create users with different roles. But when a user is creating an account, it would be only the end user account. This exercise was difficult in mambo. The constant problem was the speed at which it would performs tasks. Secondly, since it would take the user to a different page for each operation, the time taken to create the user account was too long.

All the statistics of the above three experiments were recorded at the same time with two different browsers. This rules-out the possibility of any temporary problems with the site or the system. The author would like to conclude that although Mambo has a huge market share in the open source content management system industry it does not suit the requirements of the virtual community in question. The usability and user friendliness of these two applications vary enormously. The author found that the interface and ease of use in Drupal is far superior to Mambo. Even though the advantage in Mambo is that it displays all the features on all its interfaces (pages), Drupal scores higher in usability since it provides context-sensitive menu options, thus not confusing the user.

6 Drupal Experience

6.1 Installation

The latest version of Drupal is 5.2. To install Drupal, the system needs to meet the minimum requirements in terms of hardware and software. The minimum system requirements are mentioned below (source: www.drupal.org):

System Requirements	
Application Server	PHP 4.3.3 or above
Web server compatibility	IIS, Apache
Database	MySQL
Programming platform	PHP
Operating system	Any except legacy operating systems
Cost to buy Drupal	Free (open source)

Table 1: Drupal System Requirements

The installer file of Drupal can be downloaded from www.drupal.org. The size of the installer file is 733 KB. The author would like to bring to the reader's notice that due to limited resources, Drupal, for this project, was tested on a system that created a

simulated environment. This was done by installing WAMP, which is the abbreviated form of Windows, Apache, MySQL and any one of Perl, PHP and Python. WAMP can be downloaded from http://www.wampserver.com/en/ site. Also, it should be noted that WAMP need to be installed first and then Drupal.

6.2 Implementation of community requirements

Community requirements can be categorised into *Usage-Related, Feature-Related and Technology-Related requirements*. Most of the requirements are satisfied by Drupal. However, due to certain restrictions and limitations, some of the requirements are intentionally not implemented. For example, incorporating monetary transactions is not implemented owing to its liability factor.

Usage-Related Requirements: The first requirement is about the unused space on the left panel of the current website. This is because the current website is under utilised and secondly, the person in charge of the site does not have enough administrative rights to make necessary changes to the site to overcome this problem. This issue is not specific to any particular content management tool. This problem will be solved if appropriate rights are granted to the user.

Feature-Related Requirements: These requirements are more specific and it varies from one CMS tool to another. One of the main concerns was the flexibility of the tool that allowed creating content of different types. For example, uploading pictures in-between text was not possible in the current CMS tool. In Drupal, this can be done by the help of a module called “Image_Pub” that is specially designed for this purpose. All that needs to be done is to download this module from Drupal website and place it in the Modules folder.

Notice board or static pages are another feature-related requirement. This is one of the most important requirements. This can be achieved using Drupal by (a) Login as Administrator (b) Click on “Create Content” link (c) Click on “Page” link. In this page one can type the desired content to be published and click on Submit button located at the bottom of the page. Before submitting the page, appropriate option should be selected from the menus given in the same page.

User login or sign-in is not only a useful feature but also equally important for any community website. This feature makes the site dynamic and encourages member participation. Using Drupal, the “sign in” feature can be incorporated very easily.

Another requirement is that the site should have the ability to publish blogs that encourages users to pen down their opinions and views on topics concerning the village. By installing Drupal, this can be achieved by following the same steps as for creating a “Page”. The only difference is to click on “Blogs Entry” instead of “Page”.

Being able to advertising job vacancies, adding a link to useful information like recycling/free-cycling/re-using of commodities, etc. were other requirements. Even

though these are not specifically feature-related requirements, these can however be achieved by creating a separate pages and publishing them as explained above.

Technology-Related Requirements: These requirements are related more to the server location, appropriate rights and permissions, incorporating e-commerce for monetary transactions and assistance from an external entity to have network accessibility. The first one was to have a better profile for the Port Isaac community in Google search. The second requirement was to set up hot spots within the community to have Internet accessibility. These are not features of any CMS tool and hence cannot be achieved by implementing a CMS tool. Finally, the online monetary transaction feature to enable online business. Even though this can be incorporated in the website, it is intentionally not implemented considering the amount of risk involved.

7 Evaluation

The approach followed by the author has had both positive and negative sides to it. As far as the positives are concerned, the approach followed during the research has been systematic and methodical. The author first attempted to understand the features of virtual communities and then went on to conduct an experiment between the top two CMS tools. The experiments were based on tasks that were tested on both the CMS tools. This aided uniformity in the selection process.

The experiment was based on such criteria that were derived from the requirements of the community. Also, substantial consideration was given to the constraints in the community like the limited technical expertise of the users, limited resources and accessibility of the Internet. This author feels that adopting this requirement-drive approach is most sensible.

On the other hand, the approach adopted for implementation involved a few negatives as well. On hind sight, this author feels that although the experiments were based on some common content management tasks, it would have been far better if the author could have created a simulation of the website on the two CMS tools. These simulations could have been presented to a representative sample of the members of community. The members of community could then have played a significant role in deciding which CMS tool to use. The author feels that this approach would have yielded more participation and thus more acceptability as well.

Also, the author feels that research could have been conducted on websites of similar communities that went through successful regeneration. This would have aided the research by providing an understanding of the aspects of website design and implementation that led to the positive results.

8 Conclusion

The whole process of research brought to the author a mixed feeling of excitement, contentment, satisfaction, frustration and helplessness. The best part of the paper was the experiment and the selection of an appropriate CMS tool. Even though formulating the criteria and parameters for conducting the experiment was a tough task, there was a sense of satisfaction at the end of it. An extensive study of existing literature and writing the literature review for this paper gave the author an insight into the present situation and certain common mistakes most of the entities make. It also helped the author understand the importance of and thereby recommend the requirement-based approach to the selection process of a CMS tool. As far as the Port Isaac village is concerned, the author can safely say that Drupal is the best CMS tool to be implemented. There was enormous learning in the process and at the same time there were a number of hurdles during the whole process of research and experimentation. The fact that the experiments were being conducted on the demo version instead of the actual real-time version created a number of obstacles. This is also one of the reasons why Drupal could not be implemented immediately after its selection. Receiving numerous error messages during this process. Most error messages stated 'zero sized reply' on their screens. Also, at one point of time, the demo was logged out for more than 45 minutes. This was not due to the refresh time of the demo server, as would be expected. The reason for such behaviour is still unknown.

Secondly, gauging the impact of regeneration of the community was not possible as it takes time. If Drupal was implemented, it would have been most appropriate to check the difference in growth/regeneration after a certain period of time. The author feels that he could have done a survey to find out the statistics about the number of businesses, their magnitude and type, their income ratio etc and after certain duration of time, a fresh survey would have helped in drawing a graph to mark the changes in the social and economic growth process of the village.

8.1 Future Work

The author suggests that the first thing to do in the near future is to implement the selected tool for Port Isaac village. Also the server should be shifted to such a location which is convenient for the administrator of the Port Isaac community website. Secondly, the people of Port Isaac should be made aware of the new system. Simultaneously, having Internet Hotspots setup in the village is equally important so that the members of the community have easy and quick access to internet. Finally, there should be a mechanism that includes a specific time frame to measure the social and economic growth of the community. Interaction among the community members through the community website is referred to as social growth.

9 References

AOL Website (2007) http://www.corp.aol.com/whoweare/index.shtml

Browning, P and Lowndes, M (2004) 'Content Management Systems: Who needs them?' Ariadne [online] Issue 30 Available http://www.ariadne.ac.uk/issue30/techwatch/

Community Design: Building real communities in a virtual space? (2006) www.teladesign.com/ma-thesis/glossary.html

Creotec Website (2007) www.creotec.com/index.php

Michelinakis D, Open Source Content Management Systems: An Argumentative Approach 2004 [online] http://www.michelinakis.gr/Dimitris/cms/ (Accessed on 1 Aug 2007)

Drupal website (2007), www.drupal.org

Econtent Website (2007) http://www.econtentmag.com/Articles/ArticleReader.aspx ?ArticleID=7057&AuthorID=155, 2007

Emerald Website (2007) http://www.emeraldinsight.com/Insight/viewPDF.jsp?Filename =html/Output/Published/EmeraldFullTextArticle/Pdf/0291030905.pdf

Full Circle Associates Website (2006) http://www.fullcirc.com/index.htm

InternetWorld Website (2007) http://www.internetworld.co.uk/content-management.html

MobileMan Glossary Website (2006) www.mobileman.projects.supsi.ch/glossary.html

Preece, J Website (2001) Online Communities Designing Usability, Supporting Sociability Wiley England

SDA Asia Magzine Website (2007) http://www.sda-asia.com/sda/features/psecom,id,430, srn,2,nodeid,21,_language,Singapore.html

Slashdot Website (2007) http://slashdot.org/faq/slashmeta.shtml

Strategies Partner International Limited, Website (2007) http://www.internetworld.co.uk/pdf/ Exploiting%20Content%20Management%20in%202007.pdf

Sun Website (2007) http://dcb.sun.com/practices/howtos/selecting_cms.jsp

McKeever S, Understanding Web content management systems: evolution, lifecycle and market (2007) http://www.emeraldinsight.com/Insight/ViewContentServlet;jsessionid= 55DCD355E4229B10354D3729FA9AE315?Filename=Published/EmeraldFullTextArticle/Art icles/0291030905.html

The Well Website (2007) http://www.well.com/index.html

Usenet Website (2007) http://www.usenet.com/articles/history_of_usenet.htm

VirtualCommunities.com Website (2006) http://www.virtual-communities.com/modules/news /article.php?storyid=15

Wikipedia Website (2007) http://www.wikipedia.org

WorldWideLearn Website (2007) http://www.worldwidelearn.com/elearning-essentials/ elearning-glossary.htm

3D Confocal Image Analysis of Marine Plankton

M.C.Perryman and P.Culverhouse

University of Plymouth, Plymouth, United Kingdom
e-mail: pculverhouse@plymouth.ac.uk

Abstract

Part of understanding aquatic ecosystems requires that zooplanktons be studied; one such study of zooplanktons focuses on Harmful Algal Blooms (HAB's) in coastal waters. These HAB's are toxic and are often consumed accidentally with shellfish which can cause poisoning. The HAB Buoy project focuses on the automated recognition of these HAB's so that authorities can have advanced knowledge of their abundance.
This paper describes software whose aims are set by the HAB Buoy project to present confocal images of zooplankton as a 3D Image (Model), this Model is then to be used by the software to create multiple images of the Model from different angles for the recognition of these HAB's. Recognition of organisms requires taxonomic information; the software is designed to allow for this along with transparency in the Model for further taxonomic information.
This software was able to successfully create a Model from a stack of confocal images along with a partially completed feature of adding taxonomic information. The success of this project as a part of the HAB Buoy project was never tested.

Keywords

3D software, Confocal images, Zooplankton, Taxonomy.

1 Introduction

Most aquatic ecosystems performance can depend largely on the abundance of zooplanktons (Banse, 1995). To better understand these aquatic ecosystems, zooplanktons have been studied to gain a better understanding of their species interactions and their biogeochemical processes (Rogerson et al. 2000). To achieve this type of study, two-dimensional (2D) cameras have been used to capture images of the zooplankton under microscopic conditions (Rogerson et al. 2000).

Until recently there has been no method of capturing them in three-dimensions (3D), in 2000 a non-destructive metrological technique called holograммetry was developed to record the location of multiple zooplanktons without disturbing them (Rogerson et al. 2000). Another method of capturing them in 3D is to use stacks of confocal images; this process is to be used in the main project whereby the aim is to detect Harmful Algal Blooms (HAB's) in coastal waters, the choice of confocal images were made due to their image quality (HAB Buoy, 2007; Culverhouse et al. 2007). These HAB's are toxic and cause incidences of poisoning in people eating contaminated shellfish; this is in turn having a detrimental effect on the economic

factor of the shell fisheries of the European Economic Zone (EEZ) (HAB Buoy, 2007).

The recognition of these HAB's can be achieved very quickly by an expert in marine plankton; however the HAB Buoy project requires that it be automated, this requires machine recognition of digital images using the same method the experts use (Culverhouse et al. 2007). This machine recognition requires large clusters of image recognition data and is sensitive to the pose of the object, to overcome these problems the stacks of confocal images are to be used to create a Model of the plankton (Culverhouse et al. 2007).

From this Model, 2D images from any angle can then be taken and compared with 2D images taken from the camera on board the HAB Buoy equipment for recognition. This recognition can then identify the HAB's or non-HAB's present in the water. This process exists so that shellfishery staff can have an advanced warning of the HAB presence achieved through the use of the HAB Buoy equipment (HAB Buoy, 2007).

Software is needed to generate these Models from confocal images along with the ability to allow experts to use taxonomy on the Model so that automated recognition can occur; other features are required from this software, however no such software exists. This paper describes how this software was designed, implemented, and tested along with the results of the features implemented.

2 Aims and Objectives

The software described in the Introduction had objectives to complete so that the HAB Buoy project's recognition could take place. These objectives were to filter high-resolution 3D confocal images to make it look like lower resolution images and to analyse the texture of a plankton copepod from 3D confocal images. Then the image will be compared to a 2D version taken by Phil Culverhouse's underwater camera system (HAB Buoy).

From these objectives the following aims were devised:

- Input stacked confocal images and output to an interactive Model.
- Allow features of the plankton to be pointed out and labelled on the Model.
- Compare to 2D images taken from HAB Buoy.
- Allow for parts of the plankton to become transparent in the Model.
- Create a View Sphere (nine 2D images taken at different angles).

These aims satisfied the objectives and the main project supervisor, these aims then defined the progress of the project in terms of what had been achieved. These aims were then researched so that the software could be started and successfully finished.

3 Background

3.1 HAB Buoy Project

The HAB Buoy equipment that will be used in coastal aquaculture regions is a microscope coupled with natural object recognition software operated underwater suspended from a buoy, mussel-producing raft, or in a laboratory (HAB Buoy, 2007). This combination of equipment can then be used either in a laboratory, assisting government scientists to monitor the presence of HAB algae or out in the 'field' underwater where the potential contaminated shellfish are caught for consumption (HAB Buoy, 2007).

Once a sample of HAB algae has been detected it is to be further analysed to determine exactly which species of HAB algae is present, once the species of the HAB algae is known then the shellfishery staff, government health laboratories and water quality that are Small and Medium Enterprises (SMEs) can be informed (HAB Buoy, 2007). This information can then be used by government laboratories to focus their resources effectively (HAB Buoy, 2007).

3.2 3D Graphics Library

Before research commenced on how the Model and other subsequent features would work, a 3D graphics library (graphics library) was researched and chosen. A number of games specific software's were first researched to see if they could be used, when it was realised that the software's languages were too game specific and may not allow for the freedom needed to build the software to meet the aims, a programming environment (environment) was then looked into.

It was found that a new graphics library called Microsoft's XNA Game Studio Express (XNA) was available; this graphics library was researched further to assess whether or not XNA should be chosen for the project.

After following two 'How: To' guides for presenting a Model and adding user controls to interact with it, it was decided that XNA was to be used as the graphics library. In doing so the environment was already chosen; XNA was developed in C# (C sharp). This was not a issue due to the abilities of building a Graphical User Interface (GUI) that C# possessed.

3.3 How the Model System Works

Once the XNA graphics library was chosen, the modelling system was researched. It was found that to create a solid 3D object it must contain a number of Vertexes and Indices. A Vertex is defined as being a point from which lines form an angle, in XNA a Vertex can contain data for the location of that point, the normal, the colour, and the texture mapping value (Sykes, 1980). The Vertexes provide the framework of which the texture or solid is created with, to create the faces (Indices) of the object

the Vertexes must be connected together, however the order of which they are connected are important (Hill, 2001).

To create the framework of which to build upon, an indexed array (array) of Vertexes is needed; it is these indexes that are referred to by the Indices in order to join the Vertexes up (Hill, 2001). Each Indices in XNA is defined by three Vertexes, these Vertexes are joined counter clockwise as seen from outside the object to form a triangle, this helps the graphics process define the side that will be visible (Hill, 2001).

3.4 Confocal Images

The confocal image process used to capture the zooplankton are created by focussing light (commonly laser light due to its properties) onto an object; a pinhole aperture is used to filter out the out-of-focus light in front and behind the point of focus in the object (The Confocal Microscope, 2007). Using this process the microscope is able to move the point of focus through the object creating multiple images of the object, moving the point of focus through the object is essentially moving along the z-plane. This produces a stack of 2D confocal images that will be compiled into a Model in this project.

3.5 Image Research

Creating the Model from confocal images requires that the method of which they were acquired to be known. Figure 1 shows an original confocal image, this image contains the focussed light (green) and the unfocussed light. Removing the unfocussed light requires a filter to be used. An early filter attempt was found to be inadequate due to the image being stored in the Red Green Blue (RGB) colour space.

Figure 1: Original Confocal Image

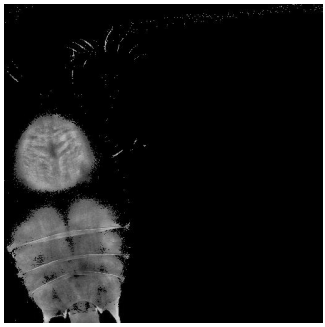


Figure 2: HSV Filtered Confocal Image (taken from the Confocal software)

An edge detection algorithm was tested on Figure 1 to explore if data could be extracted; it was found that too much data was being removed. Instead the Hue Saturation Value (HSV) colour space was tried, early testing found that the confocal images were made up entirely of a single Hue value; this meant that the Hue from

each image could be ignored or not calculated. Filtering of the Saturation and Value values resulted in a successful filtration method as shown in Figure 2. This method was subsequently used throughout the project.

4 Research Method and Experimental Design

Once the graphics library, Model system, and image filtration was researched work could commence on the design of the software, to start it was decided that the displaying of the Model created from confocal images was to be built first. From this first aim being completed, all other aims could subsequently be built using this software as a basis.

To design the software the usual formal methods were researched; waterfall model, incremental model, spiral model, and Boehm spiral model. Due to the project being built by a single programmer, there was a possibility that they wouldn't finish on time, for this reason and the reason that the software was to be demonstrated to the HAB Buoy project supervisor for feedback, the Boehm spiral model was chosen.

The Boehm spiral model was chosen due to its stages of development and the eventual creation of a prototype, each aim was to be sectioned so that the building of a prototype for each section could be made so that the latest prototype could be demonstrated once a week.

The initial plan was to build aims one in three main prototypes; the first was designed to make the algorithm that would create the Model from a 3D array. The second main prototype was designed to read in, view, convert, filter, and eventually compile the images into a 3D array, the third was to be used to join the first two prototypes together to form the first working example of aims one. Aims two was to then be built on top of the completed aims one software in a single main prototype.

4.1 First Main Prototype

The preliminary design stage for the prototype devised the flowchart diagrams that the algorithms would follow; each algorithm was implemented in turn whilst following the spiral model carefully. Each testing stage of a completed prototype was carefully checked so that the algorithms were implemented successfully and that they finished in the shortest possible time. One of the algorithms used to create the Indices was not completed; this was so that the next prototype could be started and that the incomplete algorithm could be finished more effectively in the third main prototype.

4.2 Second Main Prototype

Displaying the read in images required a GUI that allowed the user to view all the confocal images read in; the maximum amount of confocal images in a single stack were 25 images, displaying these images at the same time was not possible due the fact that the resolution of each image would be lost.

Instead the use of tabs was used; this allowed the user to select each image in full size, these tabs also allowed the possibility of a GUI for the filter so that the user can adjust it and see the results instantly. The following conversion of images and filter algorithms were already devised during the image research, the implementation of them however still followed the spiral model to ensure that they worked correctly in the new environment.

4.3 Third Main Prototype

Once the first two prototypes were complete, the integration was attempted. This was more difficult than previously thought due to the first main prototype using a thread along with the second main prototype using another thread, integrating the two meant that one had to finish before the other was started.

Once a solution was found, the algorithm used to create the Indices was continued, the completion of the algorithm was hindered due to a new and previously unknown error. This error was being caused by too many Vertexes and Indices being drawn at the same time, this was found to be a limitation of the graphics card.

A solution was attempted whereby the Indices were split up into smaller arrays so that the draw command could be used for each array along with all the Vertexes, this temporarily solved the error. This solution showed that multiple draw commands could be used to successfully draw a Model that could previously not be drawn due to too much data in a single draw command.

It was also realised that if the array of Vertexes was too close to the limit that the Indices would be split up in many arrays thus creating many draw commands and thus slowing the display of the Model down. To successfully solve this error the software needed to be rebuilt from scratch in a previously unplanned forth main prototype.

4.4 Forth Main Prototype

Completion of the forth main prototype required a solution to be built into the Indices creation algorithm. Due to the limit of the graphics card and the possibility that the array of Vertexes could become too big, the solution of creating a pair of Vertexes and Indices was used. Table 1 shows all the data needed to display four Vertexes, Tables 2 and 3 demonstrate the Vertexes paired with the Indices; this reduces the amount of data in a single array.

Vertexes	Indices
0	0, 1, 2
1	1, 3, 2
2	
3	

Table 1: Original arrays

Vertexes	Indices
0	0, 1, 2
1	
2	

Table 2: First pair

Vertexes	Indices
1	1, 3, 2
2	
3	

Table 3: Second pair

Once the pair of arrays reached the limit set by the graphics card, they were stored and new arrays were created. Once this had been achieved the algorithm used to create the Indices was continued to the point of completion, this led to the successful production of the first full size Model (Figure 4).

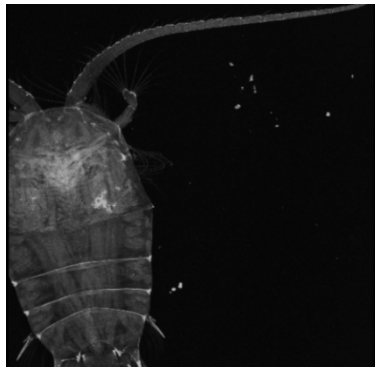


Figure 3: Compilation of the Confocal Images used

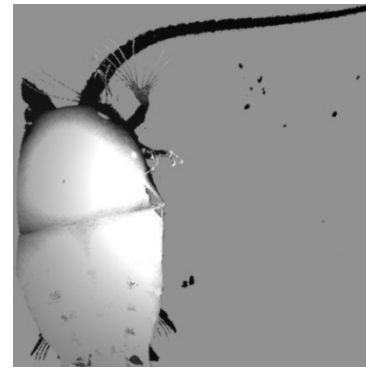
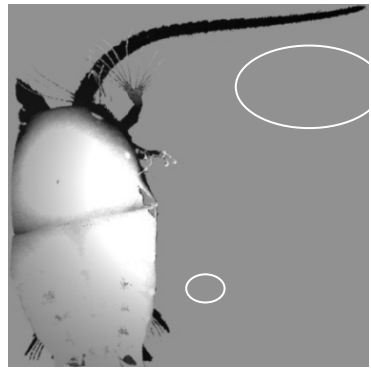


Figure 4: First Successful Model created from the Confocal Images used in Figure 3

The forth main prototype was then continued with the addition of separating the Model into smaller models, this requirement was designed, implemented, and tested according to the spiral model. Separating the Model into its individual models meant that the unwanted areas could be selected and deleted; this selecting ability was the next requirement in the forth main prototype and was implemented successfully (Figure 5), white dots surrounding the models were used to indicate the selected model by turning them all black (Figure 6).



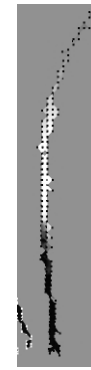


Figure 5: White Circles Indicate Deleted models **Figure 6: Selected model**

The results produced from the forth main prototype match aims one completely, this prototype could then be used to implement the subsequent aims so that the software could be completed.

4.5 Fifth Main Prototype

The fifth main prototype focussed on the completion of aims two; the labelling of the features of the Model. The aims' solution was to allow the user to 'cut' the Model up into smaller models so that they could be labelled; this solution required that an algorithm be made during the preliminary design stage along with a Tool object.

The Tool object was designed so that it could be placed at any angle by the user, once the user was satisfied with its placement they would then signify this by pressing the 'enter' button. This Tool object was then used to find the Vertexes that were intersecting it so that Vertexes on either side could be found; this would produce two Vertex arrays. The Vertexes would then require Indices to make it appear solid, it was decided that copying over the Indices from the intersected model would save time.

After all the algorithms were implemented and were successful with a smaller Model, the full size Model (Figure 4) was tested. This then caused the algorithms to take longer and subsequently cause a GameTime error. The GameTime object stores the software's elapsed time since it started (used in game software) and the actual time; after the algorithms finished, the GameTime object updated and due to the long amount of time taken by the algorithms, the update caused an error. The solution was to allow the GameTime object to update while the algorithms were run; this was achieved by running the algorithms on a separate thread.

Once the error was solved, it was found that the algorithms didn't work with the full size Model due to the Vertexes and Indices stored in different arrays due to the graphics card error, the solution was to compile the Vertexes into a single array. This resolution led to another error caused by the intersecting Vertexes being to 'thin', the algorithm used to find the Vertexes on one side was using a single Vertex and finding all the connected Vertexes, if the intersecting Vertexes had a 'hole' then the algorithm would find it. This was solved by 'thickening' the intersecting Vertexes.

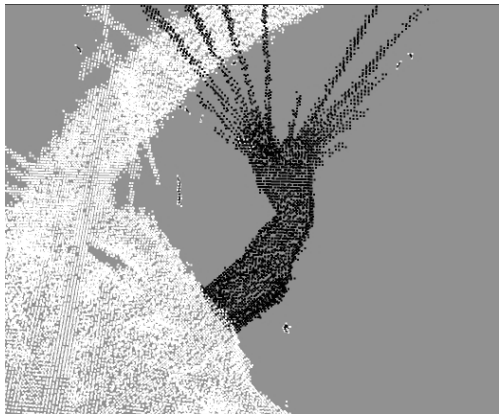


Figure 7: Successful 'cut' Performed

The copying of the Indices was never completed; however the completed algorithms did produce Figure 7 whereby the black dots represent one of the selected models.

5 Results

The software that completed aims one was reasonably successful; where the creation of the Indices based on the Vertexes was complete, other areas were not successful. Aims two was partially successful as demonstrated in Figure 7.

> The software is easy to use, the documentation understandable and accurate. The system does not crash. The menus are easy to understand and useful. The only problem is that the copepod being displayed appears more flattened that it should.
> I guess this is because the Z-axis parameters are not correctly set.

Figure 8: Phil Culverhouse's Feedback from using completed aims one software

The feedback from Phil Culverhouse (Figure 8) demonstrates aims one success in the project from a user's perspective; it also highlights the z-axis spacing problem that was quickly implemented with a lack of data, this lack of data is part of this problem.

6 Discussion and Evaluation

Thanks to the graphics card error, the solutions lead to a storage method that will allow for vast amounts of data to be stored without hindrance to the user. This has in turn produced an almost limitless Model size; methods used in the building of the software have hopefully lead to all limits of the software being removed. This has left only limits of the hardware, as most computers have the hardware needed to run the software these limits are almost non-existent.

6.1 Problems Encountered

Other problems encountered that were not errors, was a method employed in the forth main prototype whereby the spacing between the confocal images was added. This produced a more realistic Model; however the method employed was implemented incorrectly due to lack of information. Feedback received from the main project supervisor has pointed out this problem, although a solution will require more information on the images and a better filtration algorithm.

7 Conclusions

The project as a whole was not completely successful, the production of a Model from the confocal images, although complete, needs improvement on the image handling. The progress of aims two has been successful and upon completion no further work will be needed. The implementation of the GUI was also a success due to the feedback received.

7.1 Future Work

Once the fifth main prototype is complete, image handling needs to be enhanced; this requires research into confocal image extraction along with the required information for producing correct spacing between the images. Once these are complete a method could be implemented to solve the erratic drawing of the full size Model when it is interacted with, this can be achieved by drawing a wireframe version of the Model. Once these are completed the rest of the aims should be implemented.

8 References

Banse, K. 1995. Zooplankton: Pivotal role in the control of ocean production. *ICES Journal of Marine Science*, 52: 265-277.

Culverhouse, P., Williams, B., and Buttino, I. 2007. "Taxonomically driven recognition of features for visual categorisation of zooplankton." *4th International Zooplankton Production Symposium.* May 28 - June 1, Hiroshima: ICES Journal of Marine Science.

HAB Buoy. 2007. [Internet] Available from: <http://www.hab-buoy.apt-sites.com/main%20frameset.htm> (Accessed 13 August 2007).

Hill, Jr. F. S. 2001. *Computer graphics using Open GL, 2nd ed.* New Jersey: Prentice Hall.

Rogerson, A., Watson, J., Fang, X., and Krantz, E.P. 2000. Three-dimensional spatial coordinates of individual plankton determined using underwater holograммetry. *Liminology and Oceanology*.

Sykes, J. B. 1980. *The popular oxford dictionary, 6th ed.* Oxford: Book Club Associates.

The Confocal Microscope. 2007. [Internet] Available from: <http://www.gonda.ucla.edu/bri_core/confocal.htm> (Accessed 16 August 2007).

Analysing the Extent that Children are Made Aware of Internet Security Issues Within UK Schools

B.A.Richardson and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
email: info@cscan.org

Abstract

Home computer users are increasingly becoming vulnerable to the threats of the Internet. One major reason for this is a lack of crucial security awareness amongst the older generation. Considering that children learn many life issues from their parents, the question has to be asked, how safe are their children? This paper presents results from a survey of 71 ICT school teachers about the teaching of security aspects in secondary schools; their awareness of the issues; and their views on responsibility and the National Curriculum. The findings reveal that there is a void in the curriculum with regards to computer security, which teachers are fully aware of. In addition, teachers lacked awareness of specific security issues resulting in an inadequate level of information being provided. There is a brief discussion about the current curriculum review regarding the proposed amendments and who it will affect. Moreover, suggestions are made as to whether the review is likely to be sufficient.

Keywords

Child protection, Teacher survey, Internet security, Security awareness, Curriculum review

1 Introduction

Home computer users are frequently exposed to dangers when using the Internet. As the commercial sector is tightening its own security, the home user is becoming more vulnerable. The number of home Internet connections is rising all the time with the vast majority (69%) being high speed broadband (National Statistics, 2007). With more and more homes installing fast Internet connections the home user is becoming an increasingly attractive target.

Home users make themselves vulnerable further by having a fairly low level of awareness of security concepts. Furthermore, home users are largely unaware that their actions (or inactions) impact greatly on other internet users. Many types of malware will propagate through the Internet infecting each vulnerable machine as it goes. With Sophos claiming that, “there is now a 50% chance of being infected by an Internet worm in just 12 minutes of being online using an unprotected, unpatched Windows PC” (Sophos, 2005), it is no wonder that unprotected home users fall foul to such attacks. Recent surveys have revealed that home users appear to be wise to some Internet security issues with the majority taking key protective measures; 83%

use anti-virus software and 78% have a firewall (Get Safe Online, 2006). Nevertheless, despite the high usage of such tools there still remains a poor level of security awareness on how to use them effectively.

One threat that has been rising for the last decade is phishing. This is defined as a "type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information" (Microsoft, 2006). In the first six months of 2007 Symantec discovered 196,860 unique phishing attempts and blocked 2.3 billion phishing messages (Symantec, 2007). A study revealed that 40% of people failed to spot phishing websites and 90% failed to spot the most realistic website (Dhamija, 2006).

Particularly vulnerable when using the Internet are children. In many cases they begin using the Internet from the age of 7 or 8, either introduced to it at home by their parents or at school during lessons which involve using computers. Children are particularly vulnerable because they are much more trusting and naïve to possible dangers. Many children use file sharing programs and technologies such as BitTorrent for downloading music and films illegally. Some problems that arise from using file sharing programs include opening up the user's computer to the Internet making them vulnerable to attack, and studies have revealed that 45% of executable files downloaded from such networks contain malicious code (Zetter, 2005).

In addition children can be prone to bullying; exposed to indecent images; and online grooming. Online grooming is described by the Child Exploitation and Online Protection Centre (CEOP) as "a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes" (CEOP, 2007a). Although it may be expected that this is a relatively minor threat, in reality on average 50,000 paedophiles are online at any one time (Goodchild and Owen, 2006), and 1 in 4 children have met in person someone they had only previously met on the Internet (CEOP, 2007b).

This paper examines the extent to which children are taught about Internet security issues at school through a survey of Information and Communication Technology (ICT) teachers. The main discussion begins with an outline of the survey's methodology and the demography of the respondent group. The teachers' awareness and knowledge of certain security issues is analysed followed by explanations of what issues they are required to teach their pupils about. The final part of the main discussion analyses the respondents' views with regards to responsibility and the current state of Internet security education. The paper concludes with a summary of the findings and a brief discussion on the future of ICT security within schools.

2 A survey of ICT school teachers

The study was undertaken during July 2007 and was delivered to ICT teachers via emails to their schools. The only criterion for respondents was that they taught ICT to children in at least one of the key stages[1] between 1 and 4 (ages 7-16). Six hundred UK primary and secondary school email addresses were gathered from local council websites, and requests for respondents were sent out to them.

The survey was hosted on a free website (securitysurvey.brinkster.net), and received a total of 71 responses. Please note that percentages presented in this paper are rounded, therefore some questions' results may not total exactly 100%. The majority of teachers were male (77%) and the average age was fairly high (45) as shown in Figure 1. Figure 2 illustrates that almost all of the respondents taught at a secondary school level (key stage 3 or 4), with only four teaching at either key stage one or two. Due to the limited number of primary school respondents, the survey findings presented here are based on secondary school teachers only.

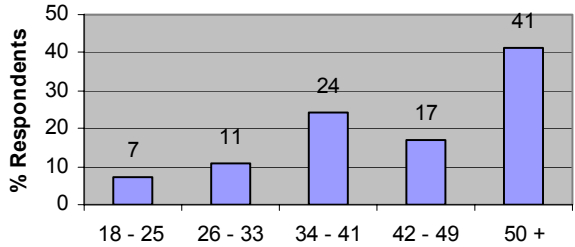


Figure 1: Respondents by age group

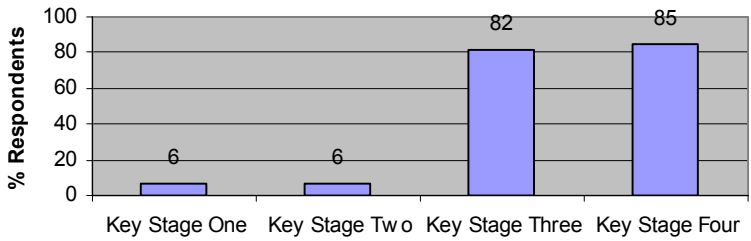


Figure 2: Respondents' teaching audience

[1] A key stage is a specific range of years of education in UK schools each ending with a formal assessment. Stages 1 and 2 form part of primary school (children aged 5-7 and 7-11). Stages 3 and 4 form part of secondary school (children aged 11-14 and 14-16).

The qualifications held by respondents were weighted towards Teaching Certificates (35%) and Degrees (49%), with a small number holding A-Levels (11%), one GCSE/O-Level and the remaining selecting other (3%). This included studying for a PHd and a post graduate degree. The spread of qualifications fit what was expected from a sample of ICT school teachers but with one surprising selection of GCSE/O-Level. This was unexpected considering the respondent taught at the same level as the highest qualification they held. However it could be the case that the respondent mistook the question for, "what level do you teach at?"

3 Awareness amongst teachers

The first section of the survey posed questions which would try to evaluate the respondents' knowledge about security issues, in order to understand the quality of the information they may give out to their pupils. Respondents were asked to state their level of awareness on a number of Internet threats as Figure 3 depicts. It is clear from the results of this question that the more recent threats are the ones that fewer respondents are aware of; botnets (19%) and pharming (12%). Surprisingly, around a tenth of ICT teachers do not know how to protect themselves against common threats such as Worms (9%), Trojan horses (10%) and spyware (8%).

The next stage of testing respondents' awareness of security issues was to give them six terms and six definitions which they were asked to match up. They were asked to pair up the terms file virus; macro virus; worm; Trojan horse; logic bomb; and botnet with the following definitions taken from BBC Webwise (2007):

- Malicious computer code that pretends to be a game or other interesting program that damages your PC as soon as you open it
- Waits and damages your computer when triggered by an event like a date
- Uses program files to get in and then copies itself
- A large number of compromised computers that are used to create and send spam or viruses or flood a network
- Infects your computer by using special codes found in word processing and spreadsheet files
- Does not damage files, but copies itself endlessly across computer networks and the Internet which slows them down

Not surprisingly, the correct definition for each term received the most responses. However, the number of incorrect answers was significant, given that the respondent sample consisted of ICT teachers. The threats that respondents previously claimed to be fully aware of received some of the lowest correct answers; file virus (64%), worm (36%), and Trojan horse (40%). Lesser known threats received middle of the range results; macro virus (87%), logic bomb (69%), and botnets (61%). The higher number of correct results for the less well known threats could be down to the fact that respondents were able to guess; this meant that some definitions could be easily assigned without any prior knowledge of the threat.

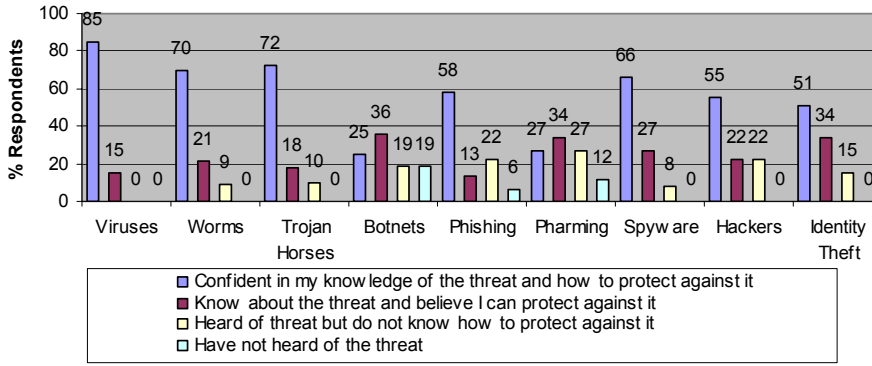


Figure 3: Respondents' awareness of Internet threats

The results from the awareness section of the survey were very worrying. It seemed that ICT professionals were unaware of key Internet threats and had false interpretations of ones that they were aware of.

4 Teaching practices

The second section of the teacher survey endeavoured to find out which security topics are taught in schools - respondents were asked to choose from a list of Internet security terms. As Figure 4 illustrates, the most common requirements (81%) were teaching about viruses, anti-virus software and safe online practices. Surprisingly, worms, Trojan horses and botnets which are just as dangerous as viruses if not more, were only required to be taught by 13% of respondents. Alarmingly, only 27% of teachers claimed that they are required to teach about updating software to patch security flaws. Another interesting finding concerns identity theft and phishing. 67% claimed that they teach about identity theft yet only 27% teach about phishing (i.e. one of the largest problems associated with online identity theft). Likewise, 40% of respondents taught about spyware but only 13% about its removal. It seems peculiar that related topics which are important for Internet security are not being linked in the classroom.

Of those who selected that they were required to teach about phishing (27%), all claimed to use visual examples of fraudulent emails and fake websites to get the issue across. Likewise, the respondents that teach about safe online practices (81%) shared similar views on what should not be disclosed when using the Internet. All advised not to give out your address; telephone number; send pictures of yourself; or meet in person. The vast majority (91%) recommended not to disclose your name and 83% advised against giving out the name of your school. Ideally, none of the information mentioned should be disclosed on the Internet whether it be on forums, social networking websites, in chat rooms, or on instant messenger. Oddly enough, some teachers were not advising children to keep their name or the school they

attend secret. These two pieces of information can be enough for children to put themselves in serious danger.

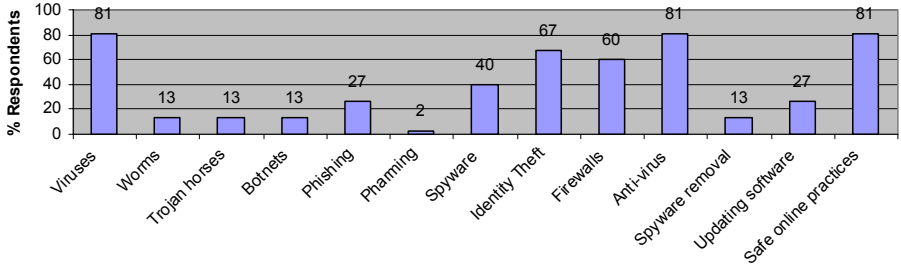


Figure 4: Respondents' teaching requirements

Those who taught about anti-virus software (81%) had a diverse view on updating virus definitions. As anti-virus software can only protect against viruses it knows about, and as new strains of malware are released every day, the only way to ensure maximum protection is to update the software as soon as an update becomes available. All reputable companies will release new virus definitions at least once a day. However as Figure 5 shows, only half of respondents advised updating this frequently. Thankfully, most of the remaining respondents (41% in all) selected once a week which should be the absolute minimum. Worryingly, 9% of ICT school teachers felt that updating anti-virus software once a month was sufficient to protect them from attack.

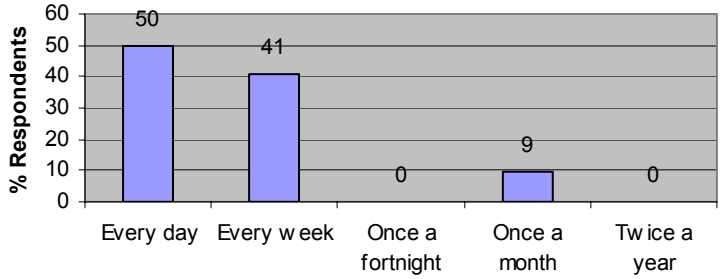


Figure 5: Respondents' recommendations for updating anti-virus software

Respondents were asked which websites they recommend to their pupils for receiving further information on Internet security issues. Amazingly, even with the apparent gaps in teaching security awareness, 57% of ICT teachers do not recommend any computer security information websites. The websites that are recommended by the remaining respondents are BBC Webwise (41%); Get Safe Online (9%); IT Safe (2%); and Wise Kids (2%). Note that the totals for this question total more than 100 percent as respondents were able to select more than one website. It is highly surprising considering the low level of security education being given that most teachers would not recommend any information websites to their

pupils. However, the failure to inform children of available help may be down to a lack of awareness that such websites exist.

Website	Visited	Aware of but not visited	Unaware of
BBC Webwise	54%	39%	8%
Get Safe Online	34%	0%	66%
IT Safe	13%	27%	60%

Table 1: Respondents' awareness of security information websites

Respondents were asked if they had heard of the major security information websites; table 1 shows their response. The majority of teachers had either not heard of them or did not know how informative they were as they had not visited them. The only website that was well known amongst respondents was BBC Webwise which only 8% had not heard of and 54% had actually visited. Government funded websites, Get Safe Online and IT Safe, had poor awareness with a large number of teachers having not heard of them, 66% and 60% respectively.

5 Respondent views

The final section of the survey asked respondents for their views on Internet security and teaching responsibilities. The teachers were asked how security focused they feel the current ICT curriculum is. As Figure 6 shows, the majority of respondents (48%) felt that there is very little focus on security issues with a further 13% believing that there is no focus at all. With that question in mind, respondents were asked if they teach additional information regarding Internet security which is not required of them under the curriculum; 46% agreed that they have taken it upon themselves to educate their pupils about particular threats. Some teachers explained that children receive additional information through an ICT Users Certificate that is taught at their school. Although a positive move to fill gaps in the curriculum, it is important to note that the majority of schools do not adopt this approach as they look to the curriculum for guidance on teaching.

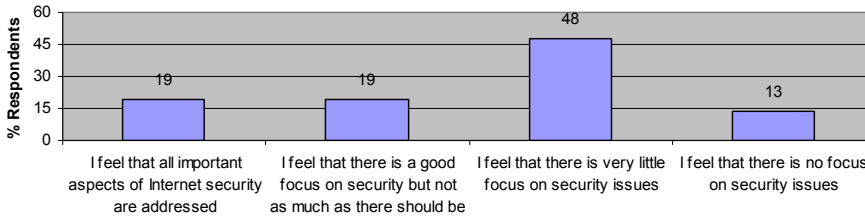


Figure 6: Respondents' views on the level of security focus in the curriculum

The final question of the survey asked respondents where they believe the primary responsibility lies in educating children about the threats of the Internet. Despite the fact that the survey has shown a low awareness amongst teachers and an inadequate coverage of the subject in the curriculum, the vast majority of teachers (70%) placed the responsibility with the schools. Almost all of the remaining respondents (25%) placed it with the parents. It seems extraordinary that so much expectation is placed on schools when next to nothing is actually delivered.

The respondents were asked if they had any further comments about the survey and the topic of Internet security. Below are two comments that sum up the situation within schools, with reference to educating children about the dangers of the Internet:

"The Key Stage 3 curriculum does not have a dedicated unit about security ... perhaps it should?"

"The National Curriculum and our exam spec (DiDA) do not require us to address these issues. We teach personal protection as part of our own take on duty of care, but so pushed for time to cover everything else that if it is not required we don't do it"

6 Curriculum review

The teacher survey has revealed a worrying lack of teaching about important security issues when using computers and the Internet. However, changes are on the horizon as an entire key stage 3 curriculum review is underway with key stage 4 in the pipeline. The changes are being made in all subjects to effectively update the National Curriculum (a framework that defines what children are taught in the UK), as it has not changed in around a decade. For subjects such as ICT this is extremely important as the rate of change is considerably higher than most other subjects (which tend to remain more consistent). Ideally, changes should be made to the ICT curriculum every few years to account for new technologies and threats. The new key stage 3 curriculum will roll out in September 2008 with key stage 4 the following year.

The current curriculum does not contain any security units and has no mention of security or protection at all. The most relevant reference made is in key stage 4 when pupils learn about the Data Protection Act 1998 and Computer Misuse 1990 Act. The revised key stage 3 curriculum will have a much larger focus on security with one of the key concepts being, "recognising issues of risk and safety surrounding the use of ICT" (QCA, 2007). The proposed syllabus also states that children will learn, "how to use ICT safely and responsibly … communicate and share information effectively, safely and responsibly" (QCA, 2007). They will also learn about "safe working practices in order to minimise physical stress" and "keeping information secure" (QCA, 2007).

The fact that the changes are only happening as part of an entire review of all subjects shows that the gravity of keeping children safe online has not yet been realised. The changes that are being made should help make a difference to the attitudes of children when using the Internet but how much is yet to be seen. One possible problem evident from the study is that many teachers are not fully aware of the issues. This means that unless they undergo training prior to the release of the new curriculum, they are likely to deliver inaccurate information which will only add to the problem.

7 Conclusions

This paper has examined a teacher survey, and has shown that there is a lack of education in schools about important security issues. Teachers openly admitted that there is very little focus on security in the secondary school curriculum although many of them made attempts to fill the gap of their own accord. The majority of teachers felt that schools are primarily responsible for educating children about Internet security issues, despite the fact that this is not currently the case. Many of the respondents lacked basic security knowledge that would be expected from an ICT teacher; the majority of respondents could not correctly identify the definition of a worm when presented with six very different answers. Perhaps most disappointing was that the majority of teachers did not advise pupils of any security information websites, even though they admitted that children do not receive enough on the subject at school. The survey has shown that there is a clear need for changes to be made to the curriculum, and that re-education of ICT teachers about old and new threats is required.

Thankfully, change is coming with the current review of the secondary curriculum. Security aspects are being added to key stage 3 to cover some of the basic issues. However, the quantity and quality of the delivery is yet to be examined as the new curriculum does not take effect until September 2008.

8 References

BBC Webwise (2007), “Online safety”, www.bbc.co.uk/webwise/course/safety/menu.shtml, (Accessed: 18 August 2007)

CEOP (2007a), “What is grooming and online child abuse?”, www.ceop.gov.uk/get_advice_what_is_grooming.html, (Accessed 18 August 2007)

CEOP (2007b), “Strategic Overview 2006-7”, www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf, (Accessed 1 September 2007)

Dhamija (2006), “Why phishing works”, people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, (Accessed 7 September 2007)

Get Safe Online (2006), “The Get Safe Online Report 2006”, www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf, (Accessed 18 August 2007)

Goodchild, S. and Owen, J. (2006), "IoS investigation: Children & the Net", news.independent.co.uk/uk/politics/article1216003.ece, (Accessed 7 September 2007)

Microsoft (2006), “Recognize phishing scams and fraudulent e-mails”, www.microsoft.com/protect/yourself/phishing/identify.mspx, (Accessed 18 August 2007)

National Statistics (2007), “Internet Access”, www.statistics.gov.uk/cci/nugget.asp?id=8, (Accessed 18 August 2007)

QCA (2007), “The secondary curriculum review”, www.qca.org.uk/secondarycurriculumreview/subject/ks3/ict/index.htm, (Accessed 18 August 2007)

Sophos (2005), “Virus writing on the up as average time to infection spirals down”, www.sophos.com/pressoffice/news/articles/2005/07/pr_uk_midyearroundup2005.html, (Accessed 18 August 2007)

Symantec (2007), “Symantec Internet Security Threat Report: Trends for January – June 07”, eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf, (Accessed 17 September 2007)

Zetter, K. (2004), “KaZaA Delivers More Than Tunes”, Wired Magazine, January 2004

Assessing Protection and Security Awareness amongst Home Users

V-G.Tsaganidi and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Home users have become the most attractive target for cyber criminals as they are more vulnerable and less protected than the rest of the users. As they constitute a mostly inaccessible group the only information they get originates from people in their environment and their exposure to media. Therefore, the amount of information they possess, their awareness about security issues and their security practices play the key role in their protection. This paper presents the findings of a number of interviews with novice UK home users of different ages, educational level and occupation. These interviews were conducted in order to assess their security perceptions, their awareness of threats and security mechanisms, their practices in regard to security and study their opinions and thoughts of security issues in general. The results revealed a satisfying level of threat awareness and security practices which however were not enough to make users feel adequately protected or confident about their actions. They are counting too much on their friends' advice, without wanting to search for more information on their own, thinking that they cannot afford the time and effort required. As a result, they feel somewhat at risk but believe they are taking all the necessary actions to prevent a bad ending.

Keywords

Home users, security practices, security awareness

1 Introduction

Users of the World Wide Web and its services are dealing with the prospect of fraudsters breaching their privacy. In today's online world, the amount of personal information that is exposed, exchanged and exploited is massive. In addition to that, an essential number of other threats is also a hazard for users such as malware including viruses, Trojan horses and worms, spyware and identity thefts by phishing, pharming or other Internet scams. Especially home users are starting to become the primary target for many cybercriminals nowadays. That is because the majority of them lacks the experience to protect their systems or neglect to do so considering themselves not to be possible targets. Since they do not protect their systems properly they are vulnerable to many threats and that makes them an easy pray for hackers and fraudsters. Therefore, security requires immediate attention and a first step to address it is studying the way users think, their actions, the reasoning behind them and how informed they are.

The number of attacks towards home users has been highly increased and the numbers speak for themselves. Symantec's Internet Security Threat Report showed that 93% of all attacks were targeting home users (Symantec, 2007). The equivalent result of the previous 2006 security threat report was 86% (Symantec, 2006). This difference of 7% within the period of 6 months cannot be overlooked as it is extremely forewarning and it indicates how important it is to protect home users. Public is not aware of this new trend, where home users have become the primary target, falsely believing that they are less vulnerable than companies and organizations. However, the threats are multiplying monthly and according to Anti-Phishing Working Group Report (2006) in December 2006 there were 28531 phishing sites, which was increased by two thousand from October. Jaeger et al. (2006) assessed the awareness and understanding of spyware of 205 home users. The findings showed that a high number of the respondents were aware of spyware, being able to define it correctly and identify its risk. However, the users could not accurately recognize which websites have the most chances to distribute spyware. That indicates that home users can be at risk even though they are aware of a threat such as spyware. Home users also have to deal with usability problems when configuring the security settings as it can prove to be very difficult and tricky, and they have to deal with it without help from an expert such as a system administrator (Furnell et al. 2006). From the latter relevant research (Furnell et al. 2007) it was deduced that although the respondents appeared to be aware of the threats and employing security policies and techniques a profound study showed a lack of serious knowledge and understanding. Thus, a more in-depth study was needed to assess not only what users do but also why they do it.

2 Interviewing novice home users

The research was conducted by 20 interviews where all the interviewees were UK citizens as the research aimed at studying the home users exposed to the UK media. Since the last research (Furnell et al. 2007) was focused on advanced users, this study to assess the way the novice home user thinks, feels and reacts with regard to computer security issues, the way they use the Internet, and their awareness of the role they play in the security chain. All the results aimed at studying the user's perceptions, attitudes and customs and what the users think they know and if they believe it is adequate for their protection.

All the interviewees were asked to participate either by word of mouth or by email invitations. They were notified that the research was about novice home users and all the users that classed themselves as such, accepted to participate. Each interview was adjusted to the particular interviewee depending on the answers they provided along the way. Thus, there was no predefined time duration. However, all the interviews lasted at least 15 minutes which was the minimum time needed for covering all the topics. These users did not know that much, did not look that interested in the security topic or they just were not aware of all the advancements in the threats and the security mechanisms. The topics that were chosen to be discussed during the interview were namely, the users' awareness of the various threats and security mechanisms, their knowledge about identity theft and any relevant experiences they

had and the sources they use for help and advice. At the end, there were questions regarding their overall opinion about what the interview offered them and if it affected them.

2.1 Internet Usage

Firstly, interviewees were asked about their Internet activities and then they were asked whether there is an activity they refrain from because it is not secure enough. Some respondents referred to buying online:

> *It does bother me sometimes, cause I think maybe it's not secure but I tend to stick because they have these little padlock symbol and I didn't have any problems with it so far so I just keep going. I wouldn't use sites I've never used before or things that look a bit dodgy and I tend to stay away from them.*
>
> *I always check when I buy things online that they've got the padlock, cause I know it's the secure way of buying things online. I'm quite happy with sites I know, I wouldn't use some random site if I hadn't heard of them or been recommended to them. I'm a bit cautious about using the Internet and paying with my credit card.*

Others were afraid of downloading files from the Internet or doing online banking:

> *I download songs and movies and I don't really think about that, because I think that when I am using the antivirus to scan my computer that this is enough but from what my friends told me it's not…I don't really pay much attention in which websites I am going to.*
>
> *I don't download anything because I am afraid of viruses.*
>
> *I'll buy things and I'll give them my credit card details but I'm still a bit worry about doing my banking online. I'll do it over the telephone but I'm still not too sure about actually doing it over the Internet.*

Even though people are afraid of doing certain things like for example buy things online or download files they will actually do them. Of course some of them will try to assure first that a level of security for that particular action like making sure a website has the padlock symbol or scan a file for malware before opening it.

2.2 Awareness of Threats

The users were asked what threats they know or have heard of, and after they had said all they could remember, they were prompt with some other threats to see if they know them. As the responds showed all the interviewees knew about or had heard of viruses. They all recognized the name, it was the first one mentioned when asked the question and most of them were able to define its impacts on the system and some

even identified ways by which a computer can get infected. However, none mentioned the potential data breach where their confidential data could be stolen if their computer was infected by malware. A Trojan horse was the piece of malware less known among the respondents and although most users had heard about phishing they could not provide an exact definition. All of the users receive or have received in the past some junk email but not all of them know its different name, spam. Another observation is that although users were familiar with spyware a couple of them thought that it was a program confusing it with an antispyware. The interviewees after talking about the threats they know or have heard about and learnt about other threats as well they were asked if they were ever faced with any. Fourteen respondents responded positively, with one of them referring to a phishing attempt, six to a Trojan horse and seven to a virus. Three of these 14 respondents were faced with both a virus and a Trojan. From the respondents that admitted having a virus in the past all of them reformatted their computer, with four asking for a friend or relative's help to do it. Only one took their computer to a professional and they reformatted it there. The three respondents that had a Trojan horse were able to solve their problems using their antivirus on their own.

2.3 Security Mechanisms

In order to protect themselves users should take some measurements and use some security mechanisms to do so. Therefore, it was advisable to ask the interviewees which security mechanisms they know, which ones they have and if they would not come up with many then they would be prompt to see if they know any more. The interviewer had in mind the following mechanisms: antivirus, firewall, antispyware and antispam. In order to assess the users' knowledge of other security controls within applications that are not security related they were asked if they have used any of those. None of the users was able to come up with any such security control and thus, they were asked in particular about the security options in Microsoft's Word and their web browser's security adjustments. The results were rather discouraging, as only two have used the first one and four the second one. Almost all of the respondents use an antivirus with only two out of 20 not using one. The rest of the respondents are certain that they have an antivirus where about the firewall, the antispyware and the antispam there were several users that were not sure if they do have them. Those that do not have an antivirus were asked to justify their choice and here is what they replied:

> *I am not cause I am not entering sites such as where you download programs or something. I am just reading newspapers or check things necessary for my coursework. As I said my C drive is totally empty so if something happens I just delete it and that's all.*
>
> *I just use certain sites to download stuff and buy things, they 2 of each one and I don't think I need an antivirus. I used to have one but it made my computer slow and I didn't like that.*

2.4 Identity Theft

Another important section of questions was referring to identity theft which has drawn a lot of media attention lately. The users that answered positively to the question if they use online payment methods were then asked how they think they protect themselves from identity theft. Since all the interviewees answered they know what identity theft is, they are all aware of it as a threat and therefore were expected to take some kind of a measurement to prevent it. The issue of trust was the first and most common one mentioned. Users interact with websites they trust as they think that if the site is trustworthy they will avoid loosing their identity details:

> *I just use the sites that I trust.*
>
> *If you know the site that you're using, I mean yeah I use different sites but when I want to put my credit card details usually it's a real loyal website like from a train company or an airline company, I don't use it everywhere.*

Others claimed that they only use sites that their friends have recommended and used in the past. Their friends' advice helped them to overcome their fears about identity theft and be able to shop online:

> *I learned from friends about two sites where you can buy things that they are safe and there will be no problem and I only use them.*

Others stated that in order to protect themselves they do certain things regarding the payment methods they use to buy stuff:

> *I use my credit card and we check our credit cards very regularly. We check the bill every month, we got all the receipts.*

Some choose to use cards that have a limited amount of money on them in order to lose the minimum amount of money in case of an identity theft:

> *I prefer not to use my credit card online and that means I have to se my debit card instead but I think that's safer because.. it's not like they're gonna steal a lot of money, it's less damage.*
>
> *The only good thing is that even if I use the credit card it has a low limit so he is gonna get a small amount of money.*

Unfortunately for e-commerce's bloom, there were some respondents that stated they refrain as much as they can from using their credit cards as they feel vulnerable to identity theft:

> *I don't use that much the credit card that's why* (identity theft) *because some day maybe someone gets my card and everything.*

> *I am not using it a lot* (the credit card) *because I'm afraid they can steal my passwords and they can charge me but ok, sometimes when I am obliged to use it, I use it.*

There was even a case where an interviewee stated refraining entirely from online shopping was his only option. An important observation is that none of the interviewees felt very confident in using their credit cards. From the 18 users reporting that they shop online, some of them tried to avoid shopping whenever they could and the rest tried to be as cautious as possible. However, there was not a single person saying that they were not at all afraid of identity theft. Despite their fear though, many of them were not discouraged and continue buying stuff online on a regular basis.

2.5 Social Engineering

The interviewees had various jobs and a scenario of using a computer at work did not apply for all of them. However, because all the users were familiar with using a username and a password for an account, they were able to picture a scenario of them working for a company, having a username and a password to login to their work computers. They were first described a case of a social engineering attack by the phone, using a similar example of that described by Granger (2001). Then they were asked how they would react and whether they would divulge their login details. Even though the majority of the respondents would at least think about it before sharing these details over the phone, there were 5 people that would:

> *Yes, I would provide my details, what can you say to someone superior? I won't tell you?*

> *I think I would that only if I knew the person* (even their name).

There were many respondents who said that in order to avoid divulging such important information they would use a number of ways to obtain some kind of confirmation about the caller's identity. There were a couple of respondents that were more negative about giving away such information and only one that looked certain about not divulging her login information. Some stated that they would ask the caller's number to call them back themselves or they would ask somebody else in their working environment or even ask the caller to come over himself to get the details:

> *I feel like giving away some information could be vital and important, so I may not give, I may ask some questions or ask to call back in a couple of minutes, so that I ask some other people that are working around.*

> *I don't think so. I would tell him I will be in the office in a while, I will give it to you myself or something, face to face I mean.*

2.6 Phishing

The interviewees were asked what they would do if they received a phishing email and also if they had any ideas about how they could tell if the email or the link or the website itself were legitimate. They were encouraged to share their thoughts in order to see if they possessed indeed the knowledge to spot a phishing attempt or at least a dodgy element that would prevent them from divulging their personal data. Some of the interviewees also talked about phishing emails they did actually receive but no one fall for them even if a couple of them almost did. Here are some of their thoughts:

> *I've never accepted any but I don't think I would know how to tell if it's legitimate so I would visit the website from the link.*

> *I would visit the website but on my own, not from the link.*

2.7 Sources for help

In order to evaluate at a small scale the advice shops offer when people buy their new computers the interviews were asked if they receive any advice when they bought their computers but none had. When it comes to if they felt they needed any at that time their answers differed. Some thought they did not and some others said they can always use some more information. Then the interviewees were asked who they turn to for help when they are facing a problem with their computer and 12/20 answered friends. However, one of those 12 answered that would also consult a relative, and three more would also visit websites. In addition three of those 12 would go to an expert if their problem insisted. Two of the rest answered they would ask for a relative's help only and two others mentioned a colleague from their IT department at work. As observed by their answers, there is a trust issue even with the professionals that solve problems with computers because users cannot judge for themselves if the price they pay for their services is fair or if they are being overcharged. Moreover, if they can avoid the whole procedure of finding the right person to fix it and then pay any price they will charge them, they prefer to ask friends who can always trust and rely on. After that the interviewees answered if they know about the websites that provide information about security topics and guidelines and they were given the example of Getsafeonline. From the 17 users that were asked this question, only two knew about their existence but have not visited them and four others stated they have used other websites like Microsoft's or AOL's. The respondents then were asked whether they would visit these websites if they knew their web addresses. Seven respondents replied that they would probably visit them with three rating free time as the only constraint. Additionally, four respondents explicitly expressed their refusal to visit these websites. Two of them said explicitly:

> *Because I don't care. I mean it's not that I had severe problems with viruses in the past, to be that afraid to look for information all day long.*

> *It's such a waste of time for me, it's a good thing though… but the thing is that I have a few friends in my circle, who are good in computers and if I ask them I know they are the best guides so there is no point.*

The interviewees were asked who they think is responsible for online security with 13 replying the end user is responsible too. It was really encouraging to hear that users think they have a share of the responsibility. Some respondents also mentioned companies and Internet or software providers and only 3 named the Government because they think the Internet is too wide, chaotic and shared across the world to be secured which is rather concerning.

2.8 The users' perception of their security knowledge

In order to assess the users' opinions about how much they know about security they were asked if they think they know enough about it. Eleven out of 20 answered that they do not know enough, seven answered that they do, although some were not very confident about it. Even the respondents that think they know enough are not blindly believing that they know everything. They are just happy with how things are so far, and they continue trying to be as cautious as they can, protecting their systems and their personal data. Here is what some of them said:

> *No I think I know a little it and I am aware enough not to give out passwords and usernames and give out too many like credit card details when I am not fully confident in what I am doing but I don't really know.*

> *I know preliminary stuff but at least I can secure myself.*

2.9 Impact of the Interview

A very important question was one of the last ones asked to the interviewee, whether the discussion informed them or changed their view in any way. It was expected that users, being novice, would think that the information provided in the interview, would be considered as a plus and could signal their quest for more information. However, only ten felt that it was informative, eight thought it was somewhat informative since it provided some definitions about threats or the reference to the websites and two thought it made no difference to them. Here are some of their opinions:

> *Yeah, it raises my awareness about what is there and how you have to be alert all the time, about how resourceful people can be in social engineering and in tricking you.*

> *Yes it made me think a little bit more about security on my computer.*

> *No, it's made me realize I am doing what I should be.*

3 Conclusions

Most of the respondents were aware of threats. Even though they did not know much about all of them, they knew that they could cause a lot of damage to their computers. However, none mentioned the probability of a loss of personal information. Still, if the user knows that there are a lot of risks it is more possible to protect more their system. That is why some of them, the ones that after the interview answered they were informed, decided to change some of their habits. If the user is uninformed and thus unaware, then they have a false sense of security that prevents them from protecting more their computer. During the interview, many respondents were keen on knowing more about the threats and listened carefully while these were being explained to them. Of course there were others that looked as if they did not care about knowing more and thought since they did not have so far any problems, they were alright with what they knew up until now. As it can be concluded from their answers, the respondents tend in general to avoid anything redundant because they want to cope with everything they have in their possession. Some of them would like to know more and act more but without having to search for themselves for information.

Regarding phishing emails the majority of the interviewees expressed even simple ideas on how to check the e-mail's genuineness which is really encouraging because as more people are getting aware of phishing, their checks will become more thorough and more demanding. Of course there were also users that would not check at all and they admitted it, even though the nature of the question encouraged them to think something and say it at that time. The interviewees did actually mention some important things that should be noticed but will they indeed think about them each time they go into their inboxes?

The fact that none of the interviewees received any advice when their purchased their computers is very concerning and should be the subject of a different research that will focus on the quantity and quality of the advice shops offer if they actually offer any. Shops could play a very important role in informing the users about the various threats and the risks associated with the use of computers and the Internet, as well as the ways of dealing with them. Overall, the interview provided some interesting findings that can be used to find the right way to approach the home users and help them in the difficult task of protecting their systems, themselves and thus, the other users. Especially them who are the most vulnerable since they are relying on their own power and actions to protect themselves. First of all they need to be educated, informed, alarmed and equipped with the right tools to ensure their computer's security. But the users have to understand why it is important to maintain their security and then what they should be careful about, what they should be afraid of and how they can achieve their protection.

4 References

Anti-Phishing Working Group (2006) "Phishing Activity Trend, Report for December 2006" http://www.websense.com/securitylabs/resource/PDF/apwg_report_december_2006.pdf (Accessed 26/07/2007)

Furnell, S. M., Bryant, P. and Phippen, A., D. (2007) "Assessing the security perceptions of Personal Internet Users" *Computers & Security*, Vol.26, Issue 5, p. 410-417

Furnell, S. M., Jusoh, A. and Katsabas, D. (2006) "The challenges of understanding and using security: A survey of end-users" *Computers & Security*, Vol. 26, Issue 1, p. 27-35

Granger, S. (2001) "Social Engineering Fundamentals, Part I: Hacker Tactics" Security Focus http://www.securityfocus.com/infocus/1527 (Accessed 24/05/2007)

Symantec, (2006) "Symantec Internet Security Threat Report- Trends for January 06-June 06" Volume X, Symantec Enterprise Security

Symantec, (2007) "Symantec Internet Security Threat Report- Trends for July-December 06" Volume XI, Symantec Enterprise Security

Author Index

Advances in Communications, Computing, Networks and Security

Volume 5

Edited by
Paul S Dowland & Steven M Furnell

This book is the fifth in a series presenting research papers arising from MSc/MRes research projects undertaken by students of the School of Computing, Communications and Electronics at the University of Plymouth. These one year masters courses include a significant period of full-time project activity, and students are assessed on the basis of an MSc or MRes thesis, plus an accompanying research paper.

The publications in this volume are based upon research projects that were undertaken during the 2006/07 academic year. A total of 33 papers are presented, covering many aspects of modern networking and communication technology, including security, mobility, coding schemes and quality measurement. The expanded topic coverage compared to earlier volumes in this series reflects the broadening of our range of MSc programmes. Specifically contributing programmes are: Network Systems Engineering, Information Systems Security, Web Technologies & Security, Communications Engineering & Signal Processing, Computer Applications, Computing, Robotics and Interactive Intelligent Systems

The authorship of the papers is credited to the MSc/MRes student in each case (appearing as the first named author), with other authors being the academic supervisors that had significant input into the projects. Indeed, the projects were conducted in collaboration with supervisors from the internationally recognised research groups within the School, and the underlying research projects are typically related to wider research initiatives with which these groups are involved. Readers interested in further details of the related research areas are therefore encouraged to make contact with the academic supervisors, using the contact details provided elsewhere in this publication.

ISBN 978-1-84102-257-4
90000
9 781841 022574