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.