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)