Security Issues and Solutions in Mobile Computing

Naveen Kumar.K, Soniya.V

Students, Department of Computer Science,

Christ College of Science and Management, Bangalore University, Karnataka

naveenpura1@gmail.com,Soniyavenkatesh97@gmail.com

Abstract-"Mobile computing as a generic term describing ability to use the technology to wirelessly connect to and use centrally located information and application software through the application of small,portable and wireless computing and communication devices[1]". In recent years we can see that it has come a very long way of providing anytime, anywhere service and access to information needed.It is an interaction between human and computer which allows transmission of data, voice and video.Mobile computing involves mobile communication, mobile hardware and mobile software. Security is a major concern for any mobile computing device such as Laptop, Notebook, Mobile Phone, Personal Digital Assistant (PDA), Smart phone etc. As all our mobiles contains sensitive data and accesses the Internet. Due to the inherent nature of these devices such as Mobility and Portability, they encounter additional security issues compare to the conventional computing devices. So there is a need to secure these devices from the various attacks. In this paper we bring out some of the issues related to mobile device security in detail, in terms of Physical, Logical, and Network categories. Also have mentioned some simple solutions to overcome these issues and to protect the devices from various problems.

Keywords: Mobile computing,security issues, physical issues, logical issues, network based issues ,recommdations,secondary device

1. INTRODUCTION

Olden day's people were using hand phone which was very big and bulky and was used only for voice communication. In other words we can say that it was merely an extension of the fixed line telephony that allowed users to keep in touch with colleagues. Now the phone is not only used for voice communication, it is also used to send text and multimedia messages. Futuremobile devices will not only enable internet access, but will also support high speed data services.Mobile computing is taking a computer and all necessaryfiles and software to the next level.

Security is a major concern for any computing devices which contains sensitive data and accesses the Internet. It is still more mandatory in the case of mobile computing devices such as Laptops, Notebooks, Tablets, Mobile Phones, Personal Digital Assistants (PDAs), Smart phones etc. due to their inherent nature such as Mobility and Portability.

The security issues of mobile devices are different from the security issues of traditional Computer systems. The following are the key factors that make the difference between these two computing devices: Mobility, Strong Personalization, Strong Connectivity, Technology Convergence and Resource constraints [2].

The mobile device moves along with us wherever we go. Because of this Mobility, the chance of mobile theft or loss is increased. Unlike the computer system, the mobile device is not normally shared by more than one person. It supports multiple ways to connect to a Networks or Internet. Due to these strong Personalization and Connectivity threat of Privacy violation is increased. A single mobile device integrates with different technologies, which may enable an attacker to exploit different routes to execute his / her attacks.

Deployment of mobile devices in work place is increasing continuously as the demand increases in order to improve the productivity of the mobile workers. Therefore securing these devices become very important in the organizations. A recent Survey on the Impact of Mobile devices on Information Security [3] reveals the significance of securing Mobile Devices.

2. LITERATURE REVIEW

A new wearable token system based on the idea of transient authentication, which provides more efficient security [4]. The cost of transient authentication is reduced with the careful key management and prudent communication mechanism and the users enjoy the benefits of constant re-authentication without using their own efforts. The factors to be considered in selecting a mobile device to the corporate have to standardize [5].

The key factors are type of mobile wireless service, security and device level of enterprise application and platform support. Multi model biometrics based user verification is suggested in mobile computing [6]. In this method, unobtrusive biometric is used initially and if it fails, then explicit effort is applied.

Voice Recognition and Fingerprint recognition are proposed as reliable security measures for cell phones [7]. IBM Linux Wristwatch as a wearable token, which has a short range wireless link and modest computational resources is used for authentication [8]. The various security issues of mobile devices are increasing day by day [9].

3. OBJECTIVE

- To make aware of different security issues existing with respect to mobile devices today
- To know how to overcome those challenges easily to protect our devices
- To implement some security protection in the mobile computing environment in a standard way.

4. SECURITY ISSUES

Mobile devices must be protected from an array of issues/threats/risks in order to provide security. The issues can be categorized into 4 types namely Physical Issues, Logical Issues, Network Issues and Personnel issues

A. PHYSICAL ISSUES AND SOLUTIONS

1) LOSS OR THEFT OF DEVICE

If the device gets lost or stolen, the confidentiality of the data stored is also lost. After a period of time if the device is found, integrity may be lost. There is a possibility of installing spyware or adding a physical bug to the hardware that leads to tampering the system. Although this threat is common for any device, mobile devices are more likely to be lost as they are small and constantly moving along with their users. Once a device is lost, everything that is stored inside is also lost. Encryption and remote wiping are the possible solutions for this problem.

2) SECONDARY STORAGE DEVICES

Care should be taken to keep the secondary storage devices safe so that they are not lost or stolen. The sensitive information such as Passwords, PINs, Credentials, Corporate data like customers list, etc. may be stored in secondary storage (e.g., flash memory) of the mobile devices which must be secured from the attackers. If they are not properly protected, along with the personal information, the valuable corporate secrets also will be exposed. Encryption is the only way to protect these sensitive data.

B. LOGICAL ISSUES AND SOLUTION

1) USER AUTHENTICATION

The personal or corporate data stored in the mobile devices should not be read or modified by unauthorized people. Otherwise the confidentiality and integrity of the mobile data will be lost. The use of corporate data by the traveling people is increasing day by day and it creates more threats on data privacy. Proper Authentication mechanism such as Password / PIN/Token/Biometric factors like Fingerprint, Iris recognition, Voice recognition etc. should be implemented to protect the sensitive data stored in the mobile device.

2) CONFIDENTIALITY OF DATA

Personal data such as Bank account number, ATM password that are stored in the mobile device should not be known to others. Similarly the sensitive corporate data like customer list and their phone numbers are kept carefully inthe device. If others happened to see the data, the confidentiality and privacy of the data/organization will be lost. Unauthorized disclosure/modification/withholding of data should be prevented. Effective Encryption techniques and strong Access Control mechanisms are the possible solutions to maintain the confidentiality of the mobile data.

3) MOBILE OS

Mobile software vendors must take the responsibility of securing mobile operating system (MOS), which is not an easy job. Security relates not only to the data loss but also to the system downtime. If the lack of security prevents a user to make a single phone call on his/her mobile device, the user experience will be weakened immensely. The access control model used by majority of the mobile operating systems is fairly strong on the base device and it is fully supported by the MOS vendors. But the external SD cards are supported by FAT permission model, which is not highly secure. By providing proper Access Control Mechanism, data integrity is protected by limiting who can access/alter the data and to what extent.

C. NETWORK ISSUES AND SOLUTIONS

1) WIRELESS ATTACKS

There are varieties of attacks which leverage the wireless connectivity of the target. Since mobile devices support communication through wireless connection, they are often affected by eavesdropping to extract confidential and sensitive information, such as usernames and passwords. Wireless attacks also misuse the unique hardware identification such as wireless LAN MAC address for tracking or profiling the owner of the device. Malware often exploits Bluetooth as a medium to speed up its propagation. For example, Cabir is a worm that propagates through Bluetooth. Phishing/Spamming/Spoofing/Man-in-the middle attacks are also caused by wireless connectivity.

2) MALWARE/ VIRUS/ TROZAN HORSE/ WORM/ SPYWARE ATTACKS

Malware is software that is often masqueraded as a game, patch or other useful third party software applications. It passes into the mobile device as a Trojan which appears to provide some functionality but contains malicious program. Keystroke logging is another type of malware that records keystrokes on mobile device. Using these keystrokes, it captures the sensitive information and sends it to a cybercriminal's website or e-mail address. Malware also includes viruses, spyware etc. Once it is installed, it can initiate an array of attacks and multiply itself on other devices. The malicious applications can do the following functions: retrieving sensitive information, gaining control over user's browsing history, initiating telephone calls, initiating mobile device microphone or camera to secretly record information, and downloading other malicious applications.

Virus - It is a program that replicates itself and infects the mobile device without knowledge of the user. Initially it infects a mobile device and then slowly spreads to the other devices and finally to the server during the synchronization process. Security techniques configured only for detecting the external attacks can be easily bypassed by such type of viruses. One of the worst viruses targets the mobile phones and makes the infected phone unusable by locking it up completely. Most of the viruses enter into the devices by downloading a corrupted email attachment or visiting a phishing website. Ex. Dust, Lasco, Cardblock.

Trojan Horse - It is a program that embeds itself within an apparently harmless or trusted application. It depends on the action of the user to succeed, and requires successful use of social engineering rather than the ability to exploit flaws in the security design or configuration of the target.

Worm - Replicates itself to spread across networks. It can potentially overwhelm mobile devices and fixed computer systems, and does not need to be a part of another application in order to spread itself. Ex. CABIR, CommWarrior, Feak.

Spyware - It is a program which is secretly installed to log and report user activities and personal data. Ex. FlexiSpy.

3) OVERBILLING ATTACK

In this attack, the attacker sends random traffic to the IPaddress of the victim. The provider would not check if the traffic was requested by the victim or not, and bill the victim for it. The attack utilizes the 'always on' characteristics of GPRS, which is billed by the amount of traffic instead of the usage time. The goal of the attacker is to charge additional fees to the victim's account, and if possible, acquire these extra fees from the victim.

D. PERSONNEL ISSUES

1) INSIDER ATTACK

It is a non-technical attack. Due to the lack of awareness of security policies, many security breaches occur. Even though corporate has Standard Policies for mobile device security, employees don't understand the risks associated with it. In [3], it is found that careless employees pose greater security risks (72%) than hackers (28%), which reinforces the importance of implementing a strong combination of technology and security awareness throughout the organization.

5. SOLUTIONS

As the need for mobile device is increasing, the threats/risks encountered by the mobile users are also increasing in an exponential way. Table 1 provides a list of recommendations that can be followed by the mobile users to keep their mobile devices and the data stored in the devices in a secured way. For every Recommendation, the Security need / requirement / justification is also given.

1. Ensure that thedata stored in the mobile devices are encrypted and audited.
2. Ensure that Mobile devices are configured with a power-on authentication to prevent unauthorized access if lost or stolen
3. Ensure that anti-virus software is installed on the mobile devices.
4. Ensure that firewall client is installed on the mobile devices
5. Ensure that Mobile devices are encrypted with strong password.
6. Report the lost or stolen device to the Supervisor immediately
7. Ensure that the data stored in the secondary storage such as Memory Sticks, Data card, removable USB drive are also encrypted
8. Ensure that the mobile device policies are established in the organization and the users are informed about the importance of policies and t he means of protecting their information.
9. Ensure that Bluetooth, Wi-Fi, etc. enabled mobile devices are turned off when they are not used.
10. Ensure that periodic backups of mobile devices are done in data server

6. FINDINGS

The usage of mobile devices is increasing day by day in number and type as it makes life more convenient for users. Today's computing had rapidly grown from being confined to a single location. With mobile computing, people can work from the comfort of any location they wish to as long as the connection and the security concerns are properly factored. The improvement in the memory capacity has enabled people to store more corporate sensitive data and personal data in their mobile devices. But Mobile devices continue to be a source of security incidents. So the situation calls for more security methods.. .

7. CONCLUSION

In this paper the security issues of mobile devices, possible solutions and recommendations are discussed to an extent. Still there is a need to find an innovative techniques or methods or approaches to put an end to the threats and issues which will continue as a never ending process.

REFERENCE

[1] Sunil Lalvani, "Mobility for a dynamic workforce", The Hindu, Dec. 9, 2012. http://www.thehindu.com/sci-tech/gadgets/mobilityfor-a-dynamic-workforce/article4178905.ece

[2] Collin Richard Mulliner, "Security of Smart Phones", Master's Thesis, University of California, Santa Barbara, July 2006.

[3] "The Impact of Mobile Devices on Information Security: A Survey of IT Professionals", Dimensional Research | January 2012. www.dimensionalresearch.com

[4] Da-Zhi Sun, Jin-Peng Huai, Ji-Zhou Sun, Jia-Wan Zhang, "A New Design of Wearable Token System for Mobile Device Security", IEEE Transactions on Consumer Electronics, Vol.54, No.4, November 2008.

[5] Wesley Chou, Cisco Systems, "Considerations for an Efficient Mobile Workforce", Wireless Broadband Technologies, IEEE, Computer Society, 2008.

[6] Elena Vildjiounaite, Satu-Marja Makela, Mikko Lindholm, Vesa Kyllönen and Heikki Ailisto, "Increasing Security of Mobile Devices by Decreasing User Effort in Verification", Second International Conference on Systems and Networks Communications (ICSNC 2007), IEEE Computer Society, 2007.

[7] H.Abdul Shabeer Suganthi.P, "Mobile Phones Security Using Biometrics", International Conference on Computational Intelligence and Multimedia Applications 2007, IEEE Computer Society, 2007.

[8] Antony J. Nicholson, Mark D. Corner and Brain D. Noble, " Mobile Device Security using Transient Authentication", IEEE Transactions on Mobile Computing, Vol. 5, No. 11, November 2006.

[9] Benjamin Halpert, "Mobile Device Security", InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA, ACM, 2005.

[10] M Satyanarayanan, pervasive computing:vision and challenges, 2001.

[11] Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf, "Mobile Security Catching Up?Revealing the Nuts and Bolts of the Security of Mobile Devices", IEEE Computer Society, 2011.

[12] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra "A Survey on Security for Mobile Devices", Communications Surveys & Tutorials, IEEE, 2012.

[13] D.roselin selvarani, T.N ravi "issues, solutions and recommendatipons for mobile device security". Bharathiyar university, 2014.