ISSN:2321-1156
International Journal of Innovative Research in Technology & Science(IJIRTS)

Issues, Solutions and Recommendations for Mobile Device Security

D. Roselin Selvarani, Department of Computer Science, Holy Cross College, Bharathidasan University, Tamil Nadu, India 1;
Dr. T. N. Ravi, Department of Computer Science, Periyar E.V.R. College, Bharathidasan University, Tamil Nadu, India 2.

Abstract

Security is a major concern for any mobile computing device such as Laptop, Notebook, Mobile Phone, Personal Digital Assistant (PDA), Smart phone etc. which 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. Now-a-days, business applications are going mobile and are using business data of an enterprise in a mobile context in order to improve the revenue by increasing the productivity. So there is a need to secure these devices from the various attacks. This paper presents the issues related to mobile device security in detail, in terms of Physical, Logical, Network and Personnel categories. It also offers simple solutions to overcome these issues and a table contains the recommendations to protect the devices from various problems. A new diagram that depicts the Issues of Mobile device security is also given.

1. Introduction

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. According to International Data Corporation (IDC), the total number of mobile workers using mobile devices to access enterprise systems is expected to reach 1.2 billion by 2013, which is more than 33 percent of the global working populace [1]. 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 the user wherever he goes. 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. Mobile devices have constraints such as limited battery power, low memory capacity and processing capability, small screen size and narrow bandwidth. These limitations may facilitate Denial of Service 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.

The remaining part of this paper is organized as follows. Section 2 reviews the various techniques used for securing Mobile devices in the literature. Section 3 discusses the Issues and Solutions related to Mobile device Security in terms of Physical, Logical, Network and Personnel categories. Section 4 provides the recommendations for the mobile device users as well as organizations and Section 5 Concludes the paper.

2. Review of Literature

A new wearable token system based on the idea of transient authentication, which provides more efficient security is discussed in [4]. In this system, the cost of transient authentication is reduced with the careful key management and prudent communication mechanism and the users enjoy the benefits of constant reauthentication without using their own efforts. The factors to be considered in selecting a mobile device to the corporate standardization are explained in [5]. The key factors are type of mobile wireless service, security and device level of enterprise application and platform support. Multimodel biometrics based user verification is suggested in [6]. In this method, unobtrusive biometric is used initially and if it fails, then explicit effort is applied. In [7], Voice Recognition and Fingerprint recognition are proposed as reliable security measures for cell phones. IBM Linux Wristwatch as a wearable token, which has a short range wireless link and modest computational resources is used

for authentication in [8]. The various security issues of mobile devices are discussed in [9]. This paper also recommended that there is a need for new approaches towards self-protecting and self-healing systems. Security threats and their countermeasures in technical, manageable and physical aspects of mobile portable computing devices are presented in [10]. In [11], the authors provide a review of mobile network security, attack vector classes and models. It also offers a survey on security of smart phones and the future direction in this area.

3. Issues and Solutions related to Mobile devices

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. Figure 1 represents the issues on Mobile device security.

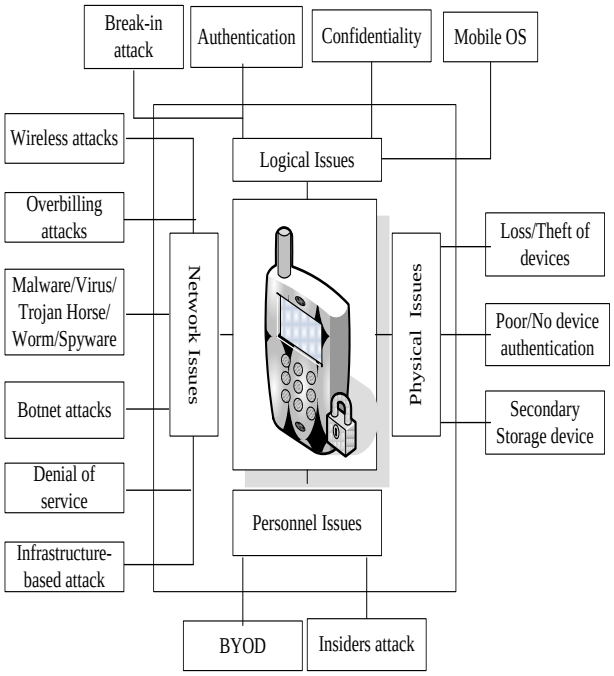

Figure 1. Issues on Mobile Device Security

3.1. Physical Issues and Solutions

3.1.1. Loss or Theft of devices

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.

3.1.2. Poor or No Device Authentication

Often mobile devices do not possess with password or personal identification number (PIN), or pattern screen locks or biometric security methods like fingerprint, voice recognition, etc. for authentication. Even if they possess, they are only simple passwords or PINs that can be easily identified or bypassed. Without proper device authentication mechanism, lost or stolen devices will face increased risk of accessing information by the unauthorized users. Complicated. Passphrase can be used as a solution. Also Screen Lock and Screen Timeout mechanisms can be utilized.

3.1.3. 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.

3.2. Logical Issues and Solutions

3.2.1. 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.

3.2.2. 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 in

the 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.

3.2.3. Break-In Attacks

In this attack, the attacker manages to gain partial or full control over the targeted device. Two types of Break-In attacks exist: Code-injection and the abuse of logical errors. Code-injection is achieved through exploitation of programming errors which lead to Buffer Overflow or format string vulnerabilities. The misuse of logical error is more delicate, because it depends on the application or the device that is being attacked. Confidentiality, Integrity and Availability of the data will be affected by this attack. Also it provides a way for the other attacks like overbilling, data/identity theft.

3.2.4. 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 extend.

3.3. Network Issues and Solutions

3.3.1. 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.

3.3.2. Malware / Virus / Trojan Horse / Worm / Spyware Attacks

Malware is a 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

3.3.3. Botnet Attack

A group of mobile devices (botclients) with malicious software facilitates an attacker / botmaster to control them remotely. These devices are within the established botnet. Through this botnet an attacker can steal information, launch a denial of service or perform any other malicious activities.

3.3.4. Overbilling Attacks

In this attack, the attacker sends random traffic to the IP-address 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.

3.3.5. Denial of Service Attacks

DoS attacks against mobile devices are mostly related to strong connectivity and less capability. Sending a large amount of rubbish matter traffic to a host over the network is an example for common attack. Due to the limited hardware of the mobile device, it may be easily become unusable by the traffic sent by the attacker.

3.3.6. Infrastructure-based Attacks

The service infrastructure, built of GSM networks and application servers, is the basis for important functionalities of mobile devices like placing/receiving calls, SMS and e-mail services [12]. In the cellular phone network structure, if an attacker sends messages simultaneously through the several available portals into the SMS network, the resulting aggregate load can saturate the control channels and thus block legitimate voice and SMS communications. An attacker can use the UMTS security architecture to launch DoS attacks. Through GPRS, an attacker can over bill users, disclose or alter the critical information, making the services unavailable, or the network breakdown.

Installing the Anti-Virus/Anti-Malware software and Firewalls can avoid maximum number of attacks related to Network Issues. Disabling all the connectivity such as Bluetooth and Wi-Fi, if they are not needed / used, downloading applications only from authorized vendor sites, avoiding attachments from the untrusted sources are some of the possible solutions.

3.4. Personnel Issues and Solutions

3.4.1. Insiders 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.

3.4.2. BYOD Attacks

Bring Your Own Device (BYOD) is a recent trend. Generally the organizations provide Mobile devices to the mobile workers for conducting businesses outside the boundaries of an Organization. But now-a-days they ask the workers to bring their own devices. This may also lead to security breaches as they may not be able to control the devices. The trend toward supporting corporate applications on employee's own notebooks and smart phones is already under way in many organizations and will become commonplace within four years [13]. The employees are also willing to use private consumer smart phones or notebooks for business, rather than using the organization devices. When they use their devices, they must be trust worthy to the corporate or the organization where they work. Leakage of sensitive corporate data is a crime and a person found to be involved in such activities needs to be penalized.

Implementing strong Security Policies, Installing Monitoring Software and educating the employees are the possible solutions to overcome these issues.

4. Recommendations

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.

Table 1. Security Recommendation Vs Security Need / Requirement / Justification

Security Recommendation	Security Need / Requirement / Justification
1. Ensure that data stored in the mobile devices are encrypted and audited.	The mobile devices are small in size and portable in nature and therefore they can be easily lost or stolen. To mitigate the risk of intentional or accidental disclosure of data, it should be encrypted.
2. Ensure that Mobile devices are configured with a power-on authentication to prevent unauthorized access if lost or stolen	The mobile users may switch off their devices in order to avoid the battery drainage as the mobile device has a limited battery power.
3. Ensure that anti-virus software is installed on the mobile devices.	Secured environment for software execution is needed so that attacks from the malicious software such as viruses or Trojan horses are prevented.
4. Ensure that firewall client is installed on the mobile devices.	If a mobile device has wired or wireless network access capabilities then use a mobile firewall to have a secure network access.
5. Ensure that Mobile devices are encrypted with strong password.	Authenticating users to a mobile device is a good security practice so that the unauthorized users will not get access to the device in the event of loss or theft.
6. Report the lost or stolen device to the Supervisor immediately.	The mobile workers should immediately report the lost or stolen devices to their supervisors so that they can deactivate the device or wipe away the sensitive data from the device.
7. Ensure that the data stored in the secondary storage such as Memory Sticks, Data card, removable USB drive are also encrypted.	Like mobile devices, the secondary storage devices can also be lost or stolen.
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.	Employees pose the greatest threat to the sensitive and confidential data of the corporate. Such insider threat can be avoided only by establishing the policies and enforcing penalty for the workers who disobey the policies.
9. Ensure that Bluetooth, Wi-Fi, etc. enabled mobile devices are turned off when they are not used.	It will minimize the device exposure to the potential malicious activities.
10. Ensure that periodic backups of mobile devices are done in data server.	Backup can minimize the damages causing loss or destruction of sensitive data.

5. Conclusion

The usage of mobile devices is increasing day by day in number and type as it makes life more convenient for users. 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. In future security threats may still become worse owing to the development and increased usage and it will be difficult for the IT Professionals to protect the mobile devices along with the personal and corporate data. 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.

References

[1] Sunil Lalvani, "Mobility for a dynamic workforce", The Hindu, Dec. 9, 2012. http://www.thehindu.com/sci-tech/gadgets/mobility-for-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] Sang ho Kim and Choon Seong Leem, "Security Threats and Their Countermeasures of Mobile Portable Computing Devices in Ubiquitous Computing Environments", Springer-Verlag Berlin Heidelbeg, LNCS 3483, Page 79-85, 2005.

[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] http://pewinternet.org/Reports/2011/Smartphones/Summary.aspx