SECURITY ISSUES IN MOBILE DEVICES AND PREVENTION TECHNIQUES

Chinmaya Datta Parvathaneni, Jeevan Chandrashekar
Department of Computer Science
University of Alabama in Huntsville

Abstract— Mobile phones, to be more specific smartphones have become like a part of everyday life. They have become more than a device used for just communication, people use them almost for everything, starting from using like an alarm clock to the device which stores almost all of the important data and also a means to pay bills online using the account and card details stored in their phone's memory. With so much of sensitive data being stored on smartphones, many types of different attacks are done by hackers and cyber criminals to obtain the personal data and the account details for personal and monetary uses. This paper discusses of such possible attacks and vulnerabilities that allow means to infiltrate a mobile device. By highlighting some potential attacks, we have proposed some ideas on how to prevent such attacks and keep a mobile device and its data safe.

1. INTRODUCTION

Modern day society depends a lot on mobile devices such as smartphones and tablets for their everyday life. Development of smartphones created a revolution in technology, devices such as IPhones, blackberry, Microsoft, Samsung etc. brought a tremendous change in people's lifestyle. Earlier days, people used landlines for communication which restricted them to a particular location. To overcome this, mobile phones were developed and people could carry them anywhere and communicate even while travelling. Mobile phones had limited features like calling and texting etc. Users were not completely satisfied with its features and required more. Smartphones were then developed by adding many new features GPS, GPRS, Wi-Fi, Bluetooth etc. With the introduction of new and exciting uses, people got addicted to smartphones and began to use them for every purpose. Smartphones are being used in everyday life for very small uses to extremely high sensitive transactions. Starting from viewing time, entertainment uses like watching movies, listening to songs, playing games, utilities such as camera with capability of taking high resolution pictures to HD videos and also for doing online transactions such as paying bills, online purchases and also for transferring funds using general messaging and also by using specific apps. Since mobile communication and connectivity is wireless, there are many threats and risks. Earlier smartphones had a standardized and less heterogeneous operating system (OS). This led attackers to exploit a vulnerability and attack large number of similar devices and led to large number of security outbreaks [1]. New operating systems were implemented by different companies- iOS by Apple, Android by Samsung, Motorola, Sony etc. Blackberry OS by blackberry and windows operating system for windows phones. Even with new and different OS's deployed on a variety of devices, there are still many risks and issues that can affect the functionality of a smartphone. There are still many possible ways to attack a mobile system by any professional attacker by exploiting any vulnerability in the system or by introducing any malware.

This paper is categorized as follows- Section 2 covers Risks and Issues in Mobile Devices, section 3 covers Threats for Mobile Devices, section 4 covers Attacks on Mobile Devices, section 5 covers Defensive Mechanisms, section 6 covers Related Works, section 7 is the summary, section 8 enlists references.

2. RISKS AND ISSUES IN MOBILE DEVICES:

Though mobile devices seem to be perfectly safe and secure, there are many issues and faults that maybe in the OS or due to some design flaws [2]. Below are some of the many possible risks and issues that compromise the mobile device security.

Theft and loss:

Smartphones and tablets are like mini PC's with a lot of processing power and having a lot of storage space. Smartphones carry almost all the data of the user, which could be credit card details, personal files – photos and videos and important mails. There is a great chance that a mobile device can be lost or stolen by a thief. In either case, the smartphone with all the details of the user ends up in other persons

hand and the data can be misused causing a lot of damage to the owner.

Unsafe Data storage:

Data stored on mobile phones can't be assumed as highly secure. Mobile phones use wireless internet for connectivity and some devices even use cloud storage for data storage and easy retrieval. Though cloud storage is safe, there are many instances where secure cloud storage such as iCloud was hacked and personal files of many people are stored and released to the world. There is a very high risk of data confidentiality violation on a device as the modern mobile platforms implement built-in disk encryption technologies. These techniques do not block any attacks during runtime, if any malicious application that is capable of accessing clear-text files or if there is any user with privileged access to the target device attacks the device, successful data theft is possible [3].

Illegitimate updates:

Users always want newest updates and software's in their possession. Most of the users do not wait for the official release of a new software or application and tend to download from other sources over the internet without considering the consequences. This way they download malware or virus infected applications compromising the safety of the device.

Unencrypted channel communication:

Most of the mobile platforms implement transmission of data on unencrypted channels or poorly encrypted channels. A poorly encrypted channel is the one with a weak cryptography algorithms allowing hackers to decrypt the data transmission. Even if high encryptions are placed, certificate validation errors and returning back to plain text communication after a failure were ignored putting the security of the device in jeopardy. Malicious users or hackers can easily intercept Clear text communication by using Man in the Middle attacks and able to manipulate the data sent back to the application.

Data leakage:

Most of the mobile devices have some flawed programs or some insecure OS features. If these vulnerabilities are not removed in further updates, data leakage is possible and sensitive and personal data of the users end up in global OS logs, web caches and on World Wide Web. Some such vulnerabilities in the Apple's iCloud drove attackers to hack into iCloud and steal the stored information from their servers and released them into internet causing inconvenience to the users.

Broken cryptography:

This is a risk in the mobile system that is due to using poor cryptography techniques or by developing custom cryptographic algorithms based on standard cryptographic algorithms. Some mobile systems use these type of custom developed cryptography algorithms without realising that the encoding and complication are not equivalent to the encryption and cryptographic keys that are hardcoded into the application code. This results in failure of the cryptographic implementation leading to loss of confidentiality of data.

3. THREATS FOR MOBILE DEVICES:

A threat can be explained as a potential danger that can exploit a vulnerability for breaching the security of a system. There are wide range of threats for a mobile device. Threats to a mobile system are of two types, intentional and unintentional. Intentional threats can cause high damage as these are mostly targeted or untargeted attacks on a mobile system by various unethical sources to steal sensitive data of the users. Unintentional threats are mostly due to faulty software updates or due to defective components in a system.

Botnet Operators:

Botnets are a set of devices that are controlled by a user (botnet operators) remotely without the owners having any idea about that and are tasked to do various malicious activities such as sending spam mail and committing various Dos attacks. These botnet operators use botnets to attack websites and distribute phishing schemes, spam, and further malware attacks on mobile devices that access these attacked websites [4].

Cyber Criminals:

Generally, cyber criminals attack mobile devices and computers for various profits. They use spyware, malware, pishing and spam for gaining access to the information stored on the device and do many cybercrimes such as identity theft, computer extortion, online fraud and steal money as well from their bank accounts.

Hackers:

Hackers are two types, ethical and unethical. Ethical hackers stick to their ethics and use their skill for helping others, while unethical hackers use their skill to show off their talent by hacking into devices and cripple the device for fun or to gain various profits by using the personal data and account details on board.

Terrorists:

Terrorists' first goal would be to get hold of mobile communications and to destroying them, in order to cripple a country's communication and to spread chaos. Secondary goal would be gain access to other mobile devices to use them for obtaining peoples' personal details and do identity theft.

Foreign Governments:

Some foreign countries have intelligence agencies that are directed to hack and tap mobile communications of other countries to obtain general and classified information. Since communications is the crucial part of any society, these intelligence agencies try to sabotage the country's communication to create pandemic and chaos amongst people. These kind of measures are generally taken during the times of war or to cripple an economy and panic amongst the people is the best way to gain success.

4. ATTACKS ON MOBILE DEVICES:

As mentioned in previous sections, mobile devices are open to various range of threats. While unintentional threats can be easily resolved by modifying the software or the device settings, but intentional threats are from various sources and are mainly aimed at infiltrating the mobile device and using the details in them for either monetary gain or for online fraud etc., In march 2011, Google gave reports [5] stating that it had removed a large number of malicious android apps from the android market-play store, in some cases it had also removed those malicious applications directly from the users' devices remotely. Since android market is not so secure, anyone who is capable of developing an application is able to upload it into the market. Taking this as an advantage, hackers and cybercriminals are encouraged to attack android smartphones and online surveys prove this [6].

Malware:

Malware can be said as a software that is designed to carry out malicious activities on a device. Malware can generally be used to steal personal information off of a mobile device for personal gains such as to perform financial fraud and to perform identity theft. Malware is an application based and is downloadable through an applications right from a devices app store. Malwares are commonly masqueraded as a game, utility, patch, music app, social network app, connectivity apps etc. which are mostly third party applications generally developed by some untrustworthy third party developers. Malwares can comprise of virus, worms, Trojan and spyware. Soon after installed into a mobile device, the malware initiates a wide range of attacks and keeps spreading to other devices it gets in contact with.

Spyware:

Spywares are designed and tasked to collect user data from the mobile devices without user having any idea and without the users' approval. Spywares are most commonly directed to steal contact information, photos and videos, messages, emails, location and banking details.

Virus:

A virus is a software program with a piece of small code that can duplicate itself and spreads throughout a device. Using these replicas, the virus uses different replica to affect different part of the system and also affect other programs.

Worms:

A worm is a self-replicating program that creates new copies of itself and transfers them from one device to another with the help of different transport mechanisms from existing system without the knowledge of the user and infects healthy systems and keeps on spreading to newer systems. In 2009 a worm Ikee.B was found in iPhones and was used to obtain sensitive financial data from iPhones that were jailbroken [7]. In addition to that, according to a security report given by cisco [8] in 2010 July, U.S. Library of Congress has added jailbreaking of iPhones to the list of actions that doesn't come under the category of copyright violation. This made iPhone users free to jailbreak their devices and at the same made them vulnerable to various security attacks.

Trojan:

Trojans are used to gather private information and also installs other malicious applications such as, worms, virus, botnets etc. Trojans generally stay undetected in a device and transmits sensitive data to its owner.

Botnets:

Botnets are some compromised devices which are controlled remotely by a user and use them to do pishing attacks and denial of service (DoS) attacks on websites.

Rootkits:

Rootkits are malicious applications that gain rights to run in privileged mode masking their presence from the users by modifying the standard operating system functionalities. The below table displays some different kind of malwares in the form of virus, Trojan, worms and spyware that had affected many devices with different operating systems in the last decade [9] [10] [11] [12].

Name	Time	Type	Method of Infection	Effects	OS
Liberty Crack	2000	Trojan	Pretend to be a hack	Remove third-party software	Palm OS
Cabir	2004	Worm	Bluetooth connection and copies itself	Continuous scan of Bluetooth, drain phone's battery	Symbian OS
Dust	2004	Virus	File Infector	Infect all executables in root DIR	Windows Mobile
Skulls	2004	Trojan	Vulnerability in overwriting system files	DoS	Symbian OS
Doomboot	2005	Trojan horse	Doom 2 video game	Prevents booting and installs Cabir and CommWarrior	Symbian OS
Lasco	2005	Virus	File infection	Add itself to install packages	Symbian OS
Feakk	2005	Worm	SMS message	Send SMS to all contacts	Symbian OS
CardTrap	2005	Cross-Platform Virus	Auto-start of removable storage	Copy Wukill on the phone	Symbian/Windows OS
Crossover	2006	Cross-Platform Virus	CIL vulnerabilities	Copy to/from mobile/PC	Windows/Mobile OS
Letum	2006	Worm	E-Mail spreading	Infect registry	Windows Mobile
Mobler	2006	Cross-Platform Worm	Dropping Mechanisms	Disable antivirus and infect removable storage	Symbian/Windows OS
Wesber	2006	Trojan	Fake Browser	Send SMS to premium-rate numbers (Russia only)	OS-Independent (J2ME)
Acallno	2006	Spyware	Fake Commercial Software	Gather and send information about user's activities	Symbian OS
Feak	2007	Worm	Proof-of-concept worm	Sending SMS to contact list with URL	Symbian OS
Flocker	2007	Trojan	It claims to be an ICQ application to trick the user	Sending SMS to a hard coded phone number	Symbian OS
Beselo	2008	Worm	Via MMS and Bluetooth fake application	MMS charging	Symbian OS
InfoJack	2008	Trojan	Attach itself to installation packages	Disable security settings	Windows Mobile
Yxes	2009	Worm/Botnet	SMS containing malicious URL	Send contact lists to external server	Symbian OS
Ikee	2009	Worm	Scanning a IP ranges and SSH	Alter wallpaper	iPhone
FlexiSpy	2009	Spyware	Fake Application	Tracking/log of device's usage	Symbian
ZeuS MitMo	2010	Worm	Fake SMS	Steal bank account information	Cross-Plafrom
iSAM	2011	Multifarious malware	Scanning IP and connecting to SSH	Collect private information, send malicious SMS, DoS	iPhone

Types of malwares found in the last decade

Wi-Fi sniffing:

Most of the applications and webpages do not use proper security measures while transmitting their data i.e. they use clear texts instead of using encrypted texts for transfer of data over wireless networks. This leads to the compromising of data as many attackers take this as an advantage and intercept all the data listening to unsecure wireless networks [13].

Eavesdropping:

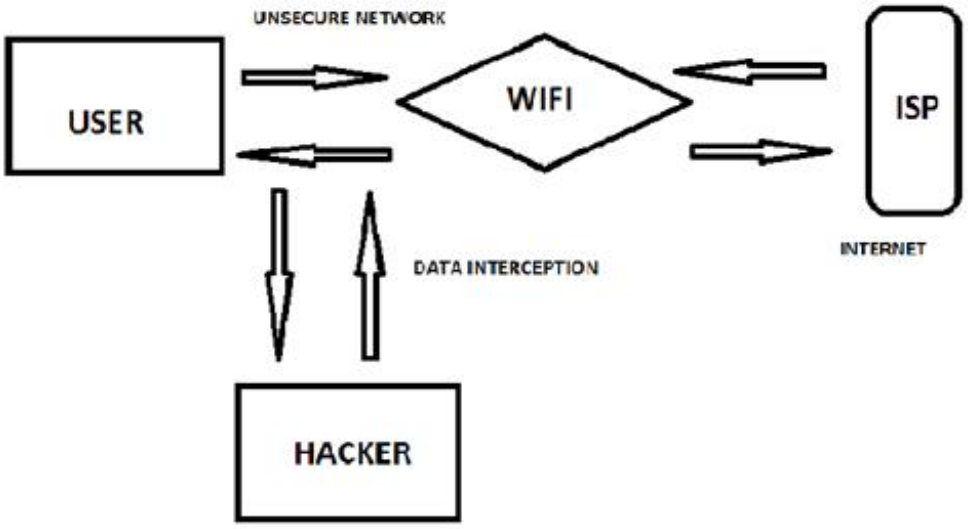
Any mobile device with an unsecure connection with its base station has a possible chance of getting intercepted by an attacker and the conversations can be heard by the attacker. Eavesdropping is a major problem in most of the developed countries where the government in the name of national security eavesdrops on civilians conversations.

Network Exploits:

Every mobile operating system has some minor or major software flaws. Minor flaws are not much of a problem, but if an attacker gets hold of any major exploit, he can attack a device with such flaws operating on a local or cellular network.

Bluetooth:

Bluetooth attacks focusses on spreading malware from one device to another. If Bluetooth settings are misconfigured in any device, an attacker will be able to access call history, phone contacts and other important information from the target phone. Immediately if two Bluetooth devices come in range, the compromised device connects and pairs with the target system with default passwords and access codes. Once pairing completes, the infected device transfers malicious data via Bluetooth and infects the other system.



WIFI SNIFFING

5. DEFENSIVE MECHANISMS:

After gaining some knowledge on the various types of threats, vulnerabilities and potential attacks on mobile systems like smartphones, it is of highest importance to implement and practice various defensive mechanisms and techniques.

User authentication:

Mobile devices like smartphones should be configured to require a password to provide access to any user. Password should be sound without using easy guessable passwords. Masking the passwords while entering is advisable in order to prevent anyone from observing while entering. Innovative techniques like biometrics can also be implemented for authentication such as fingerprint scans, face recognition and voice recognition etc. Research was done on Implementation of biometric techniques and were found to be a better solution to prevent unauthorized access to a mobile system [14]. Apple iPhones and Samsung phones from Galaxy s5 implemented fingerprint readers for a secure access to their devices. It is too costly to implement all these security features but it is worth to spend in order to save device from attacks. In addition to this, a security failsafe should be installed so as in case of theft of the device, the sensitive data in the smartphone can be prevented from falling into wrong hands by disabling the phone remotely and it should be able to track phones location online.

Checking authenticity of downloaded applications:

Since most of the malware gets into a device through some third party applications downloaded from the app stores, it is of utmost importance to verify each and every application that is downloaded before installation. Device should check the digital certificates of all the applications and only the ones with authentic certificates are allowed to download and installed.

Antivirus:

Antiviruses proved to be efficient in preventing intrusions and attacks on computer systems and laptops etc. Implementing antiviruses into mobile systems like smart phones will be a smartest choice. Number of studies prove that antiviruses are essential for a safe mobile device [15]. Many leading antivirus companies have already developed mobile compatible antiviruses and released them into market. Kaspersky, Norton and Avast are the best examples for the leading antivirus companies that have taken an initiative to develop and release antiviruses' for mobiles.

Securing app stores:

Most of the malwares that enter into mobile devices is due to downloading malicious or infected apps from the app stores. It is necessary for the owners of operating systems to closely monitor their app stores. Some highly trained and talented hackers can generate apps with fake certificates which are almost as perfect as the original ones. User devices will not be able to differentiate the authentic ones from the ones that are not. App stores owners should be very careful while accepting new apps to be released in their store. It is a well-known fact that the android play store owned by Google has a policy where anyone who can develop an app is able to add their app into the play store. Taking this as an advantage, many attackers chose this platform to install malware into user mobile devices. Apple's app store has also suffered malware infection to some of its applications and Apple had to take prevention steps to remove the malware to keep its device safe [16].

Encryption of mobile devices:

Encryption of mobile devices is aimed at encrypting the data stored in the device or the memory card of the device. Whenever a device gets attacked, the main goal behind that is to obtain the data stored in it. Encryption of data prevents an attacker from accessing the data even if he is able to break into the device. It is also necessary to introduce a mechanism where data is completely erased from the device if a certain user-defined number of failed attempts are made to access the data. Although this is mostly preferred by users if it the data doesn't end up in wrong hands.

6. RELATED WORKS:

Since mobile devices have become a part of daily life for all the people, the number of threats and attacks on these devices have also increased in a gradual manner. Similar kind of studies are made about the risks of increasing attacks on mobile networks by information warfare attacks [17]. This work focusses on the mobile security breaches from an information warfare perspective. Some surveys were also done on mobile device serve issues and some ideas were proposed focussed on IDS-based tools and models [18]. Considering such threats, four testing techniques were proposed- mobile forensic, penetration techniques, static analysis, and dynamic analysis [19].

7. CONCLUSION:

With increased number of Mobile phones usage, many hackers have discovered new vulnerabilities and ways to exploit those vulnerabilities. In this paper, we discussed a lot of issues in mobile device security, new found vulnerabilities and the possible ways of attacking the system to steal confidential and personal data. We also researched and proposed some methods and ideas on how to resolve the issues and ways to keep a mobile device safe from intrusion and also possible ways to keep the data safe inside the device even if it is infiltrated via some malware or at the times of theft of the device. Some of the ideas proposed are a little farfetched, but implementing them will bring a lot of change in the field of mobile phone security and we hope that there is a chance in the near future, where these techniques might be implemented.

8. REFERENCES:

[1] M. Kotadia, “Major smartphone worm by 2007,” Gartner Study, June 2005.

[2] Daniel , K. Foiling the Cracker: A Survey of,and Improvements to, Password Security, Proceedings of the 2nd USENIX UNIX Security Workshop, pp.5-14, August 1990.

[3] Luca De Fulgentis, "The Windows Phone Freakshow", Hack in The Box Conference, Amsterdam 2015 - Research Whitepaper v. 2.0.

[4] GAO-12-757,” INFORMATION SECURITY: Better Implementation of Controls for Mobile Devices Should Be Encouraged”,2012,[Online]. Available : http://www.gao.gov/648519.pdf

[5] Google Mobile Blog, “An Update on Android Market Security,” March 2011. [Online]. Available: http://googlemobile.blogspot.com/ 2011/03/update-on-an- droid-market-security.html

[6] Sophos, “Security Threat Report,” 2010. [Online]. Available: http://www.sophos.com/sophos/docs/eng/ papers/ sophos-security-threat-report-jan-2010-wpna.pdf

[7]https://www.fsecure.com/vdescs/worm_iphoneos_ikee_b.shtml.

[8] Cisco, “Cisco 2010 Annual Security Report,” Jan 2011.[Online]. Available: http://www.cisco.com/en/US/prod/collateral/vpndevc/security annual report 2010.pdf

[9] A. P. Felt, M. Finifter, E. Chin, S. Hanna and D. Wagner "Survey of Mobile Malware in the Wild", 2011

[10] https://en.wikipedia.org/wiki/Mobile_virus

[11] http://www.mobilemarketer.com/cms/opinion/columns/15296.html

[12] http://www.wikiwand.com/en/Mobile_virus

[13] Mingzhe Li, Mark Claypool, and Bob Kinicki, ``Wireless sniffing by example - how to build and use an ieee 802.11 wireless network sniffer,"Tech. Rep. WPI-CS-TR-05-19, Department of Computer Science at Worcester Polytechnic Institute, Nov. 2005,Online: ftp://ftp.cs.wpi.edu/pub/techreports/pdf/05-19.pdf.

[14] Sujithra M,” Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism”, International Journal of Computer Applications (0975 – 8887) Volume 56– No.14, October 2015