International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013)

Android Mobile Security – Threats and Protection

Jiayi Mu[1], Ailing Cui[1], Jingyu Rao[1]
[1]Department of Computer Science University of Southern Polytechnic State University, USA
{acui & jrao& jmu}@spsu.edu

Abstract - In recent years, more and more users and businesses use smart phone as communication tools, but also use in our private life. In the meantime, hackers use the network exploits to attack users' smart phone. These attacks exploit weaknesses come from different kinds of access just like SMS, Wi-Fi networks and MMS. Here, we will show eight modules, which cover important mobile threats in most aspects of mobile security. Each module focuses on one type of mobile threats, such as Spyware, SMS Spam and Malware, and we will convey the threat analysis and protection in multiple ways. We will provide one lab in each module to explain the solutions that we get.

Index Terms – Mobile Security, Smart Phone

1. Introduction

There are 1.03 billion smart phones in use in the third quarter of 2012. It increased 47 precents from third quarter 2011. [1] When Google Company revealed the Android operating system in 2007; Android devices immediately became almost the most popular devices in the market and gained an unmatched prevalence in the mobile phone industry. Apple products are presented notable challenges in the smart mobile phone industry to Google Company and Android. However, Android is slowly gaining a stronger hold in the tablet and mobile phone market around the world due to its lower prices, faster operating system, and the fact that it is open source and thus is free to use. [2]

In this paper, we will introduce eight issues about mobile threats, and offer an examination for each issue. The examinations will include attacking tests and defending tests. We will provide one solution, which would avoid hacker attacking the smart mobile devices, for each threat. The threats that we will discuss about are as follows:

(1) Threats of Lost or Stolen Mobile Devices: people usually stored much personal information in their mobile phones, such as messages, contacts' number and daily reminders. A large number of personal information and sensitive data are stored in these devices. Once people lost their mobile phone, their personal information might be released.

(2) Unauthorized Mobile Resource Access: most sensitive information being accessed by the public network while at work. Connecting the device with public networks will cause some security issues. Most sensitive data could be hacked easily, if people store them in a mobile device.

(3) Mobile Device Cryptography Privacy: privacy threats might cause some applications, which are not necessarily malicious but can gather many personal data, become malicious applications.

(4) Mobile Malware: mobile malware is an application actually. However, this kind of application is malicious, and the number of the application is increasing quickly. Attacks of mobile malware usually include three phases: the infection of a host, accomplishments of its goal, and spread of the attack.

(5) Mobile Spyware: mobile spyware is a kind of malicious application, which is collects or steals data without user permission. It not only violates victims' privacy, but also allows hackers to get the importance data from the mobile device.

(6) Mobile SMS Security: there are three kinds of SMS threats that are mentioned in this paper: SMiShing, SMS Spam and Premium Rate SMS. To some extent, SMiShing seems like phishing that uses SMS instead of email. [10] SMS Spam is the unwanted messages that are sent into a person's account. [11] Premium Rate SMS is that hackers attack the victims in a very short time, and some victims might even have no idea.

(7) Mobile Phishing: Phishing attacks trick users into personal information to web pages that appear to be reputable sites or installing malware; they will masquerade as a trustworthy entity in an electronic communication. [4]

(8)Mobile Network Exploits: exploit means that hacker can gather privacy from victims' phones or even control their phones by their Wi-Fi.

2. Threats and Protection

Issue 1: Threats of Lost or Stolen Mobile Devices.

Smart phone and tablet play an important role in current social life, and has already become an essential tool in human activity. A large number of personal information and sensitive data are stored in these devices. The problem is that when the devices were stolen and lost, the personal data were exposed. If there is not defence machine system, the information will have the risk of being seen by other people. The password could be hacking, the private email content could be seen, and even the transaction results could be revealed. If the hacker attack enterprise network via VPN, the losses are terrible.

In order to avoid data losses, defence system is strongly needed.

1. It is necessary pre-installed auto-backup app, protecting our device through installing mobile tracking app. The Backup Manager handles all your data transactions with the cloud storage (using the backup transport) and your backup agent handles all your data transactions on the device. [5]

2. When you lost or stolen, you need to report the lost device immediately, prevent from malicious using the stolen device, and decrease the loss. Locking the device is the most efficient method to protect your device. Nobody can use your

© 2013. The authors - Published by Atlantis Press

device, without your access, even somebody exchanges the SIM card on your device. It will cut off abuse SMS fee, reading email, and personal information.

3. Located the lost device and display location on the Google map. Finally, you can remote your stolen device to wipe out your private information.

Issue 2: Unauthorized Mobile Resource Access.

Today's society exchange the information more and more frequently, such as wired and wireless device interact. The enterprise network can access most of corporative information while working. However, this kind of inter-operation exist security problem. Connecting the device with the public networks will lead in security issue. Most corporate data could be hacked easily, if they use and store mobile devices, especially android. And also, most users install the applications without knowing whether it credibility or not. The username and password in the active directory permit many business application accesses, and it will be easily hacked. Also, when the email usernames are published in the network resources, the hacker can easily get the credentials.

In order to resolve the security issue, device need to protect active directory.

1. Use the Two Factor Authentication in the mobile device. When a thief have access to your computer, he can boot up in safe mode, bypass the physical authentication processes, scan your system for all passwords and enter the data manually, thus -- at least in this situation -- making two-factor authentication no more secure than the use of a password alone. [5]

2. Custom logging has a special feature that protects corporate password by providing custom logging credentials for Active Sync.

Issue 3: Mobile Device Cryptography Privacy

Privacy threats may be caused by applications those are not necessarily malicious, but gather or use more sensitive information (e.g., location or user identity) than is necessary to perform their function or than a user is comfortable with [5]. In order to protect this data from dangerous, encryption is the most efficient way to save data security.

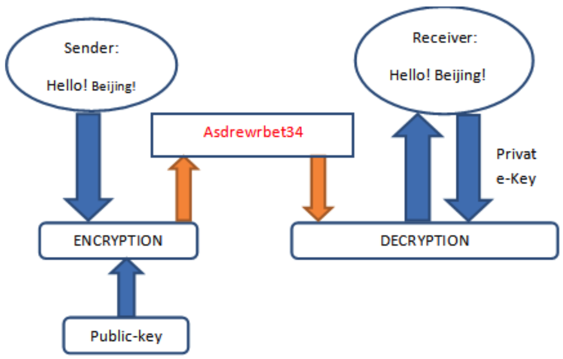

Figure 1. Mobile Device Cryptography Privacy

Cryptography is a technique transforms original data into a different and unique format, which cannot be read and understood, which is used to protect important information. RSA is a generally used public-key encryption algorithm. AES is a well-known private-key encryption algorithm. RSA is asymmetric encryption algorithm, need to two distinct keys for both encryption and decryption. AES is a well-known symmetric encryption algorithm standardized by U.S government. In AES, we used the same encryption and decryption keys.

Decryption algorithm is a reverse mathematical procedure for a specified encryption algorithm, such as RSA&AES.

Issue 4: Mobile Malware

With the development of the smart device, there are increasing number of malicious applications were developed, and the target is device and platform. These applications all called mobile malware.

An attack of mobile malware involves three phases: the infection of a host, accomplishments of its goal, and spread of the attack. The infection happened in many cases. When downloading a malicious file or visiting phishing website, user may be infected. When sharing applications peer-to-peer, sharing links on mobile network also made device infect. The infection also happened when the device synchronizing with Cloud services.

Once infected, the malware start to accomplish their goal, such as disrupting devices' operations. The most popular malwares are spyware, Trojan horse, adware, etc.

There are several ways of preventing from attacking in the following:

1. Install an antivirus application. Make a complete scan of installed applications, data, settings, and files for any infection.

2. Be careful of using battery and network. If you feel that have an unusual usage of network and battery, it might be infected by the malware application.

3. Check device setting. Be careful any suspicious behaviour in the device settings, such as when you turn off WIFI, 3G, GPS, and these will turn on automatically without user permission. In these case, the infected application will change the setting automatically.

4. Only accept and download from trusted and official applications providers. Do not download from unsecured or un-trusted third part websites.

Issue 5: Mobile Spyware

In general, mobile spyware is a kind of malicious application that is collects or steals data without user permission. Spyware application displays in adware. In the mobile device, spyware not only violate user privacy, but also allows the cyber criminal gets the importance information. The spyware steals the data from memory resources, and consumes bandwidth when it sends the data to the spyware home base. Spyware don't have to come with any other apps, because it installed surreptitiously. Cyber criminals design most of spyware, which is posted in the open market. And when you download these apps, your device will turn into a spy tools. Following is the method of protecting mobile device.

1. The most efficient way is install an anti-spyware or mobile security apps.

2. Checking the abnormal shutdown problems. If you shut down your mobile device without responding to the certain functionality, then this could be an indication that installed a spyware. In generally case, spyware program runs in the background, which could occasionally cause a problem when trying to shut down.

In order to avoid the same things happen again, we need to be careful in mobile application.

1. Making ensure that installed applications are clean and legit.

2. The requested permissions from the apps need to be carefully read and if the requests match the app's feature then download it.

Issue 6: Mobile SMS Security

Mobile message is one of the most popular functions in mobile devices, but it also provides many changes for hackers to attack user's mobile devices. Nowadays Mobile Short Message Service (SMS) threats are increasing. In this issue, we will explain the SMS-based threats and protection methods. SMiShing is similar to phishing that uses text messages on cell phones and smartphones instead of e-mails. [10] There are two kinds of SMiShing.

1. You receive a text that seems to come from a trusted source, and the text would instruct you to go to a specific Website to verify your account information. The text is actually from the thieves. They will use your information to steal money from your account. [10]

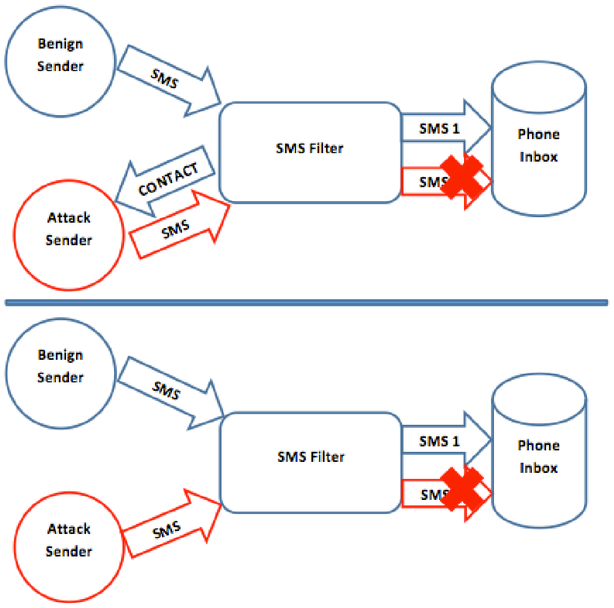

Figure 2. Mobile SMS Security

2. You receive a text with another urgent request, that contains an attachment. The attachment will include a virus or malware that allows the scammers to access everything on your phone even control it. [10] SMS Spam is used to describe electronic "junk mail" which is unwanted messages set to a person's email account or mobile phone. [11] Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. [12] Premium Rate SMS is that such attack can make the attackers a lot of money in a very short time and for the victims, they may even haven't realized that. In this lab, we created a fake attack that may cause privacy leaks, and then we provided a SMS filter to reduce the above attacks.

Issue 7: Mobile Phishing

Phishing attacks trick users into personal information to web pages that appear to be reputable sites or installing malware; they will masquerade as a trustworthy entity in an electronic communication, such as eBay and online banks. [5] These sensitive information includes usernames, passwords, credit card details, and beyond. [8] Although hackers use different forms of communication, such as the Internet and SMS, this can be also done. The hacker can send links via e-mail, using pop-up ads. When the victims access the malicious website, they will have no idea and continue entering in their private credentials. [5]

In recent years, because of the speed of the Android mobile operating system so quick, hackers have already started to target mobile users for attacking. For avoiding the mobile phishing, we need to know how to protect our mobile. To prevent any malware infections by phishing, when logging into a website with personal account, always check the URL of the website (the android device tends to hide the URL, but it can be accessed with a quick finger stroke). [9] Besides, install an effective mobile security app is necessary. [7] In this laboratory, we created a Fake Facebook application, which would take a victim's username, password credentials and other personal information.

This Fake Facebook would provide a button that links the user to fake Facebook.com, which maximizes data. In our defencing lab, we installed an app permission manager, which could help prevent the attack from the Fake Facebook, because it would scan the applications installed on the phone and report the permissions that an application has been assigned. In this case, Fake Facebook cannot be using the Send SMS permission, and the users would be alerted that the application might be malicious and should be deleted.

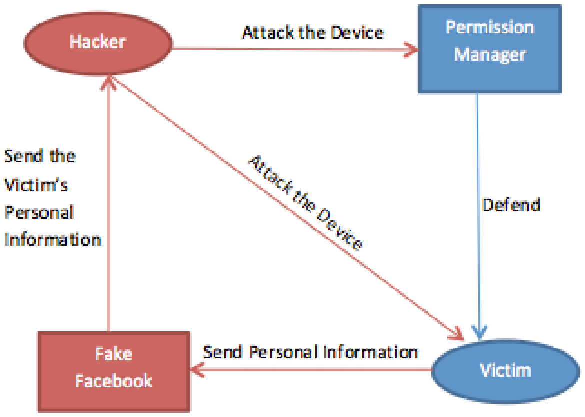

Figure 3. Phishing Defence

Issue 8: Mobile Network Exploits

In this issue, we will talk about network exploits. In computing, an exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders. Used as a verb, the term refers to the act of successfully making such an attack. [6]

For smart phones, Network Exploits mean that a hacker retrieves sensitive information from a victim's phone or even bugs a victim's phone by connecting to their Wi-Fi or Bluetooth. Here, we mainly talk about how to deal with network exploits a hacker carries out to a victim's phone by connecting to their Wi-Fi. In some applications, they will retrieve the Android user's password before encryption. Some applications can also allow a hacker view the user's private information, track the user's personal Internet history, and kick other users off public Wi-Fi by hacker's own mobile device.

These attacks seem to be out of victim's control. However, they can be eventually prevented by connecting to a secure network, or downloading a necessary firewall application. We used the android application, Droidsheep as our attacking application. When the spoofing function is started, Droidsheep will obtain an IP address and obtain cookies that are sent through the same Wi-Fi router. The user of this mobile device can then choose to view webpage data that was embedded in a cookie sent though the Wi-Fi. In the protection lab, we download a firewall application, Network Firewall.

3. Conclusion and future work

Mobile security has become a really big issue nowadays. More and more people, businesses use smartphones as communication tools, which also work everywhere in our daily life and private life. After the study of mobile security, defense and protection, we began to realize the growing importance of this topic. This paper presents our initial effort on exploring mobile threats and the ways to protect them. We did a lot of research and practices on the Android security labs. In the future, we plan to explore various aspects of communication security. We will improve our labs, and add several labs together to develop a bigger Android security project.

Acknowledgment

We appreciate the help from Dr. Qian, who contributes plenty of ideas for this project and educates us the mobile security knowledge. Moreover, the Technical Assistant of Mobile Security class gives us suggestions to solve various problems. We appreciate the help from all the people who help us.

References

[1] "Data Backup." *Developer.android.com.* Developers. Retrieved from http://developer.android.com/guide/topics/data/backup.html

[2] "Definition: Two-factor authentication." *Searchsecurity.techtarget.com.* Search Security. Retrieved from http://searchsecurity.techtarget.com/definition/two-factor-authentication

[3] Lookout, Inc., "Lookout Mobile Security Report 2011," August 2011, accessed on Oct 12, 2011, Retrieved from https://www.mylookout.com/mobile-threat-report.

[4] "Definition: Exploit." *Searchsecurity.techtarget.com.* Search Security. Retrieved from http://searchsecurity.techtarget.com/definition/exploit

[5] "Smishing, vishing- time for mobile phishing."*Bullguard.com*. Bulguard. Retrieved from http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/smishing-vishing-mobile-phishing.aspx

[6] Frak, Bodek. "Gone Phishing." Retrieved from http://web4.uwindsor.ca/units/its/insight/insight.nsf/0/d1b60efa750dfe21852573d7004cbbd8?OpenDocument

[7] "Phishing Prevention Tips." *Sis.pitt.edu.* Retrieved from http://www.sis.pitt.edu/~nophish/prevention.html

[8] Cooper, Alison. "What is SMiShing?" *howstuffworks.* Retrieved from http://www.howstuffworks.com/personal-finance/online-banking/smishing.htm

[9] "Smishing and Vishing." *FBI Gov*. Retrieved from http://www.fbi.gov/news/stories/2010/november/cyber_112410/cyber_112410

[10] "Spam."*Acma.gov.* Australian Government. Retrieved from http://www.acma.gov.au/WEB/STANDARD/pc=PC_310294

[11] "Number of Smartphones Around World Top 1 Billion –Projected to Double by 2015." *Finance.yahoo.com*. Retrieved from http://finance.yahoo.com/news/number-smartphones-around-world-top-122000896.html

[12] Bolton, M. (2011, July). "What is android? A beginner's guide." Retrieved from http://www.techradar.com/us/news/phone-and-communications/mobile-phones/what-is-android-a-beginners-guide-975482