A Practical Analysis of Smartphone Security*

Woongryul Jeon[1], Jeeyeon Kim[1], Youngsook Lee[2], and Dongho Won[1,**]

[1] School of Information and Communication Engineering, Sungkyunkwan University, Korea
wrjeon@security.re.kr, jeeyeonkim@paran.com,
dhwon@security.re.kr
[2] Department of Cyber Investigation Police, Howon University, Korea
ysooklee@howon.ac.kr

Abstract. Recent developments in mobile technologies have produced a new kind of device, a programmable mobile phone, the smartphone. Generally, smartphone users can program any application which is customized for needs. Furthermore, they can share these applications in online market. Therefore, smartphone and its application are now most popular keywords in mobile technology. However, to provide these customized services, smartphone needs more private information and this can cause security vulnerabilities. Therefore, in this work, we analyze security of smartphone based on its environments and describe countermeasures.

Keywords: Smartphone, Smartphone security, Security analysis, Security mechanism.

1 Introduction

A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone. Smartphones and feature phones may be thought of as handheld computers integrated within a mobile telephone, but while most feature phones are able to run applications based on platforms such as Java ME, a smartphone allows the user to install and run more advanced applications based on a specific platform. Smartphones run complete operating system software providing a platform for application developers[1].

Based on this feature, smartphone user can develop any programs which are customized in specific needs, and this is a most powerful advantage of smartphone. For example, smartphone user can search most popular restaurant, or nearest bus stop. Furthermore, smartphone user can trade their assets like stocks or use banking service with wireless network. Smartphone user can send or receive e-mails, too.

However, to provide these services, smartphone needs more private information than feature phone, thus, it is very important to keep smartphone secure. If smartphone user

[*] This research was supported by Basic Science Research Program thorough the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2010-0011279).

[**] Corresponding author.

M.J. Smith, G. Salvendy (Eds.): Human Interface, Part I, HCII 2011, LNCS 6771, pp. 311–320, 2011.

lost his/her smartphone, for example, every information like address, e-mail, log data in web browser, SMS(Short Message Service), MMS(Multi Message Service) or others, can be exposed if there is no appropriate security solutions.

In present, there are many researches on smartphone security, but there is lack of effort to analyze all security threats of smartphone. To establish smartphone security, security threats based on smartphone environment is necessary. This work is needed for design of security solution, either, to prevent potential vulnerabilities of smartphone.

Therefore, in this paper, we analyze security of smartphone and suggest countermeasures. This paper consists of five sections. In section two, we analyze smartphone environment and its assets. In section three, we analyze security of smartphone and derive vulnerabilities and threats of smartphone. In Section 4, we describe applicable security mechanisms for smartphone, and finally, in section 5, we end with a conclusion.

2 Security Environments of Smartphone

2.1 Environments of Smartphone

Smartphone can be connected various subjects, internet, PC, other mobile devices using wireless network. This feature makes smartphone useful and most popular mobile device. However, in other words, this feature means that malicious attacker or software can invade smartphone in various paths. Following figure 1 shows general environment of smartphone.

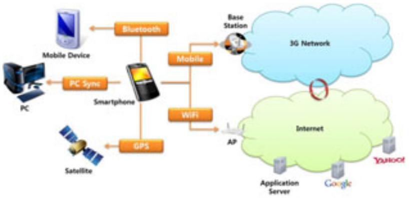

Fig. 1. Environments of Smartphone

The user can make a call or receive a call, manage his/her schedules, play game or use other functions by his/her smartphone. Some applications may need to connect web or other devices to provide customized service, and in this case, smartphone can connect others with various wireless network technologies.

The base station is kind of way to connect web and it is a basis of calling service. The base station relays phone calls, messages, e-mails or various data via 3G networks. If there is AP(Access Point)s around user smartphone, user also can connect to web using AP.

The satellite provide location information of smartphone, and this information can be used various services, for example, map, messenger, even if when user take a picture, location information is inserted in picture.

The PC(Personal Computer) can be connected to smartphone by cable or wireless network, and user may download files or update firmware through PC.

These entities can be regarded as both target and mean of attack. For example, an attacker can take denial of service attack on base station or web server and risk availability of smartphone. Furthermore, some entities like web server or PC can be used as a host to infect user smartphone with malware. Therefore we have to consider these entities in smartphone security.

2.2 Assets of Smartphone

Now we have to define smartphone assets, because the asset can be regarded by target of attack, and threats and vulnerabilities are basis of the attack. Following table 1 shows assets of smartphone in this paper.

Table 1. The Assets of Smartphone

Assets	*Description*
Private Information	Address book, Calling history, Location information, Notebook, Schedule, Cache file of web browser, password used in web, email and its attachments, and other information
Device	Smartphone device System resources of smartphone(CPU, RAM, Battery or etc.)
Applications	Smartphone applications user installed

First, information in smartphone can be defined an asset of smartphone. The information include all data both stored in smartphone and transmitted out to smartphone, for example, address book, calling history, location information, e-mail and its attachments, SMS(short message service), media files and so on forth. These information is managed by applications of smartphone, thus for security of smartphone, the application is an essential entity.

Second, smartphone itself can be defined an asset. Because smartphone can make a call or connect wireless network, thus malicious user who get smartphone someone lost, can cause overcharging by using smartphone. In addition, resources of smartphone can be regarded as an asset, because these resources ensure availability of smartphone. In fact, some malwares exhaust resource of smartphone on purpose to risk availability.

Third, applications on smartphone can be defined an asset. There are two kinds of applications, one is freely distributed by user or online application store, and another is commercially used with digital rights. The smartphone user has to pay some charge to use commercial applications and thus, application itself can be regarded as an asset.

Furthermore, the applications are closely related the information, thus it is natural to regard the application to an asset of smartphone. For example, most of smartphone web browser stores user's ID and password which can be used in online authentication process. Generally, smartphone provides QWERTY pad to input device and this device is implemented in touch screen about 3~4 inches, so, it is inconvenience to type ID and password every times. Therefore web browsers on smartphone store ID and password, and this feature is the reason why applications have to be regarded as smartphone assets.

3 Vulnerabilities and Threats of Smartphone

In this section, we derive vulnerabilities and threats of smartphone. All vulnerabilities respond specific threat.

3.1 Vulnerabilities of Smartphone

When to keep a system secure, we have to consider how keep system secure, and answer of this question is what kinds of threats can harm the system. To identify all existing threats, first, we have to confirm the assets and this is described above section. In this section, we determine security objectives for the system. In principle, the security of mobile devices deals with the same issues conventional computer security deals with confidentiality, integrity and availability. Table 2 shows the security objectives in this paper.

Table 2. Security Objectives

Issues	*Description*
Confidentiality	Confidentiality determines who is allowed to access what.
Integrity	Integrity identifies who is allowed to modify or use a certain resources.
Availability	Availability describes the requirement that a resource be usable by its legitimate owner.

Table 3. Vulnerabilities of Smartphone

Vulnerabilities		*Description*
Internal of Smartphone	V1. Implementation error	Malfunction caused by implementation error Malicious attacker can take advantages using implementation error(e.g. type safety, arbitrary code execution)
	V2. Incompatibility	Disabling application caused by incompatibility between applications Disabling application caused by incompatibility between application and platform
	V3. User unawareness	Unawareness of a device owner to risks of installing applications from un-trusted sources Unawareness of the device owner to the risk of connecting to un-trusted Wi-Fi networks and web-sites(e.g. Rogue AP, Phishing Site). Unawareness of the device owner to the risks posed by improper configuration (e.g., Bluetooth settings, browser settings). Unawareness of the owner to social engineering attacks. User can lose his/her smartphone.
External of Smartphone	V4. Vulnerabilities of Wireless Network	Corrupting, blocking or modifying information on the wireless network by sniffing, spoofing or eavesdropping
	V5. Vulnerabilities of External Objects	External objects of smartphone environment like web server, AP, base station or PC can risk smartphone security by its potential vulnerabilities, insecure management, or so on forth.

The threats can be divided in two groups, vulnerability and threat. Vulnerability means that it can risk security object potentially, and threat means that it can risk security object directly. In this paper, threats and vulnerabilities can be described based on this form, for example, resident malware can alter smartphone configuration without authority. This example includes subject – malware, object – system configuration, and action – altering. Now, we can derive vulnerabilities and threats of smartphone.

Table 3 shows vulnerabilities of smartphone. V stands Vulnerability in the table [2-11].

3.2 Threats of Smartphone

Threats of smartphone give shape to attack using vulnerabilities. In this paper, we divide threats in two groups, Threats caused by attackers and Threats caused by user unawareness or intention.

Table 4 shows threats of smartphone[2-11].

Table 4. Threats of Smartphone

Threats	*Description*	*Vulnerability*
Threats caused by attackers		
T1. Malware	Malware can alter or expose private information in smartphone Malware can risk availability by meaningless operation(e.g. arbitrary code execution) Malware can abuse costly services and functions(e.g. sending SMS/MMS, connecting wireless network)	V1 V3 V5
T2. Wireless Network Attack	An attacker can corrupt, block or modify information on the wireless network by sniffing, spoofing or eavesdropping	V4
T3. Denial of Service	An attacker can risk availability of smartphone to take denial of service attack to base station, wireless network, web server An attacker can risk availability of smartphone using radio interference	V4 V5
T4. Break-in	An attacker can gain partial or full control over the target smartphone by using flaw of code, code injection or abuse of logic error	V1
Threats caused by user unawareness or intention		
T5. Malfunction	The user can disable or malfunction his/her application by mistake or misappropriate configuration Smartphone application can malfunction by incompatibility between platform and application.	V2 V3
T6. Phishing	The user can expose his/her private information by accessing phishing site The user can expose his/her private information by messenger phishing The user can expose his/her private information by SMS phishing	V3
T7. Loss	The user can lose his/her smartphone	V3
T8. Platform Alteration	The user can alter his/her smartphone platform intentionally(e.g. jail breaking in iPhone, rooting in android phone)	V3

Figure 2 presents the results of a qualitative risk analysis that we conducted in order to identify and prioritize the threats. This figure is based on the report published in December, 2010, by ENISA (European Network and Information Security Agency)[11]. According to this report, main risk of smartphone is user unawareness. Although most smartphone applications have privacy settings for controlling how and when location data is transmitted, but many users are unaware that the data is being transmitted or data can be hided, even many users are unaware of existence of the privacy setting to prevent this. Other likely threat is malware. Smartphone user can install malware to his/her smartphone by unawareness, SPAM mail, SMS, MMS or other various ways. Lost or stolen smartphone is one of the main threats. However, the report cluster this threat in unlikely and medium, because only 2% of smartphone user are lost or stolen their smartphone last year. However, smartphone is a small and light mobile device, so user usually loses his/her smartphone, and when it lost, whole of information can be exposed.

Intentional platform modification also can cause security problem. However, according to this report, only 10% of iPhone users unlock their smartphone called by jail breaking.

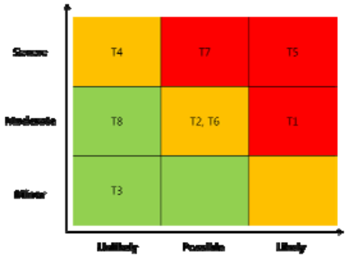

Fig. 2. Qualitative Threats Analysis

4 Applicable Security Mechanisms for Smartphone

Several security companies have already announced some security solutions for smartphone. These solutions include various antivirus software and intrusion detection systems that run on the smartphone and smartphone user can take these applications in online market. These applications can prevent attacks from outside like malware, but they can’t prevent attacks from inside caused by using implementation error or user unawareness. Therefore to keep smartphone secure, it is required to adopt other security mechanisms, for example, platform modification, regular update and so on forth.

When considering the applicability of a security measure, we have to determine who would be implementing it and how should be realized. According to this, we can cluster smartphone security measures into three types in terms of their realization approaches[12]. Following table 5 shows definition of security mechanisms.

Table 5. Types of Approach

Types	*Description*
System Modification	Require altering platform's core source-code including the kernel **Advantage :** available new functionalities **Disadvantage :** Relatively expensive in terms of man power and time
System add-on	Require modification of platform's core configuration file **Advantage :** more easier than system modification **Disadvantage :** To adopt this modification, smartphone user have to re-install all applications
Add-on Applications	Can be applied by any user by simply installing an application **Advantage :** easy to adopt **Disadvantage :** If user does not install this application, there is no improvement in security

Add-on application is easiest way, however, in this way, to improve smartphone security, smartphone users have to install appropriate applications to their smartphone. Thus, this way can't ensure security improvement.

System add-on means system updates, and platform manufacturer can improve functionality and security in this way. This way also needs user-self update, but updates are perfectly adopted in new smartphone.

System modification is most expensive way to improve smartphone security, because it needs kernel configuration. However, this way can improve entire security of smartphone platform.

Table 6 shows applicable security mechanisms for smartphone.

T8, Platform alteration, potentially, can cause various security problem, thus in the table 6, we denote it in parentheses.

Adopting security solutions like anti-virus or SPAM filtering from appstore is easiest way to improve smartphone security, however, to adopt this way, smartphone user have to install applications. There are many applications for smartphone security, thus to improve smartphone security, the user should install necessary security solution.

In addition, smartphone users have to update their smartphone and applications periodically. Platform manufacturer and application developer provide updates for their products and this update includes both improvement of functionality and security. So, the user may update their smartphone platform and applications for smartphone security.

To ensure confidentiality and integrity in smartphone, application developer and smartphone user can adopt cryptographic technology. Cryptographic technology can be implemented two types, application and APIs. In application store, there are many applications using cryptographic technology. Some application provides data encryption for data confidentiality and some application provides hash function for data integrity, thus smartphone user can keep their smartphone secure using these applications. APIs also are provided to application developer, for example, several smartphone OS includes security library thus the developer can use these APIs in implementation.

Table 6. Applicable Security Mechanisms

Mechanisms	*Types*	*Description*	*Related Threats*
Anti-Virus Solution	Add-on Application, System Add-on	Anti-virus solutions scan files, memory, SMS, MMS, emails and URLs Anti-virus solutions can prevent malwares and also prevent access to phishing site	T1, T6, (T8)
Firewall	System Modification	Firewall blocks and/or audit un-allowed connections from/to device Firewall can prevent network attacks by denying access to untrusted wireless network	T3, (T8)
Secure API	System Add-on	Secure API provide cryptographic functionalities for application developer Application developer can implement secure functionality using secure APIs	T1, T2, (T8)
Access Control	System Modification	Access control limits access of processes and user to resources and/or services Access control can limit risk from malicious/exploited application	T1, T7
Authentication	System Modification	User should be authenticated to use device Authentication process can prevent unauthorized use of device	T7
Spam Filter	System Add-on, Application Add-on	SPAM filtering applications blocks MMS, SMS, emails and calls from unwanted origin SPAM filtering applications can prevent SPAM	T1
Pre-Testing	System Modification	Pre-Testing guarantee applications and authorizes developer Pre-Testing can prevent malware and ensure security of applications	T1, T4, T5
Regular Update	System Modification	Regular update for platform and smartphone application	T5
Remote Access Control	System Modification	Remote access control includes remote configuration and management of smartphone(remote blocking, remote reset) When user lose his/her smartphone, remote access control can reduce damage by lost smartphone	T7

In present, access control model has been studied in many papers, and this technology can provide advanced user authentication[9]. According to this model, multiple users can be classified in groups by his/her rights and access rights can be determined attributes of each group. This model is based on platform of smartphone. However, many smartphone users take root permission by jail breaking or rooting, thus access control model should consider this situation.

Remote access control is also studied and adopted in many ways. Because smartphone is a small and tiny device, smartphone users usually can lose their smartphone. When users lose their smartphone, remote access control is necessary to prevent exposure of data in smartphone and illegal usage of smartphone. Remote access control includes remote locking smartphone and remote reset of smartphone.

5 Conclusion

A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone. Smartphones and feature phones may be thought of as handheld computers integrated within a mobile telephone, but while most feature phones are able to run applications based on platforms such as Java ME, a smartphone allows the user to install and run more advanced applications based on a specific platform. Smartphones run complete operating system software providing a platform for application developers.

Based on this feature, smartphone user can develop any programs which are customized in specific needs, and this is a most powerful advantage of smartphone. For example, smartphone user can search most popular restaurant, or nearest bus stop. Furthermore, smartphone user can trade their assets like stocks or use banking service with wireless network. Smartphone user can send or receive e-mails, too.

However, to provide these services, smartphone needs more private information than feature phone, thus, it is very important to keep smartphone secure. If smartphone user lost his/her smartphone, for example, every information like address, e-mail, log data in web browser, SMS(Short Message Service), MMS(Multi Message Service) or others, can be exposed if there is no appropriate security solutions.

In present, there are many researches on smartphone security, but there is lack of effort to analyze all security threats of smartphone. To establish smartphone security, security threats based on smartphone environment is necessary. Therefore, in this work, we analyzed security of smartphone and described applicable security mechanisms against threats.

References

1. Mulliner, C.R.: Security of Smart Phone, Master's Thesis of University of California (June 2006)
2. Guo, C., Wang, H.J., Zhu, W.: Smart-Phone Attacks and Defenses. In: HotNets III (November 2004)
3. Chen, J.V., Yen, D.C., Chen, K.: The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics. Information & Management 46(4) (2009)

4. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S.: Google Android: A State of the Art Review of Security Mechanisms, arXiv 2009 (November 2009)
5. http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
6. http://www.mt.co.kr/view/mtview.php
7. Monk, A., Fellas, E., Ley, E.: Hearing only one side of normal and mobile phone conversations. Behaviour & Informaion Technology 23(5) (September 2004)
8. http://threatcenter.smobilesystems.com
9. Ni, X., Yang, Z., Bai, X., Champion, A.C., Xuan, D.: DiffUser: Differentiated User Access Control on Smartphones. In: Proc. 5th IEEE Int'l. Workshop on Wireless and Sensor Networks Security, WSNS 2009 (September 2009)
10. Schmidt, A.-D., Schmidt, H.-G., Clausen, J., Camtepe, A., Albayrak, S.: Enhancing Security of Linux-Based Android Devices. In: 15th International Linux Kongress (October 2008)
11. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S.: Google Android: A State-of-the-Art Review of Security Mechanisms, Cornell University library (2009)
12. Smartphone: Information security risks, opportunities and recommendations for users, ENISA Report (December 2010)