International Journal of Fuzzy Logic and Intelligent Systems, vol. 11, no. 4, December 2011, pp. 229-237
http://dx.doi.org/10.5391/IJFIS.2011.11.4.229

A Security Reference Model for the Construction of Mobile Banking Services based on Smart Phones

Yong Nyuo Shin and Woo Chang Shin[+]

Department of Computer Engineering, Hanyangcyber University, Seoul 133-791, Korea
Department of Computer Science, SeoKyeong University, Seoul 136-704, Korea

Abstract

As smart phones have become widely adopted, they have brought about changes in individual lifestyles, as well as significant changes in the industry. As the mobile technology of smart phones has become associated with all areas of industry, it is not only accelerating innovation in other industries such as shopping, healthcare service, education, and finance, but is also creating new markets and business opportunities. The preparation of thorough security measures for smart phones is increasing in demand. While offering excellent mobility and convenience, smart phones can be exposed to a range of violation threats. In particular, it is necessary to make efforts to develop a security system that can preemptively cope with potential security threats in the banking service area, which requires a high level of reliability. This paper suggests a security reference model that is considered for the smart phone-based joint mobile banking development project being undertaken by the Bank of Korea in 2010. The purpose of this study is to make a security reference model for a reliable smart phone-based mobile financial service, by recognizing the specific security threats directed toward smart phones, and providing countermeasures to these security threats. The proposed mobile banking security reference model is useful in improving system security by systematically analyzing information security threats to the mobile financial service, and by presenting the guideline for the preparation of countermeasures.

Keywords: Smart phone; Multiple sensors; Mobile banking services; Security; Threats; Countermeasures; Reference model

1. Introduction

A smartphone is a next-generation mobile phone equipped with diverse functions such as internet information search, MP3, built-in camera, DMB(Digital Multimedia Broadcasting), GPS, and image information sending/receiving. It is based on the concept of a portable computer [1]. In the past, the term "smartphone" referred to a terminal named a "PDA phone," which physically combined PDA functions with phone functions. Today's smartphones, while phone-centered, have essentially absorbed PDA functions. Recently, smartphone-based mobile financial services have seen a rapid increase of users thanks to the convenience and fast speed they offer, in addition to the fact that they enable users to perform transactions at any time and from any place. Reviewing the Internet banking service use status in Korea at the end of 2010, the number of mobile financial service transactions showed a 65.4% increase from the previous year (2.85 million transactions), and the total transaction amount increased by 53.5% (408.7 billion won). Furthermore, there were 0.95 million smartphone-based financial service transactions, and a total transaction amount of 46.8 billion won [2]. The use of smartphone-based financial services seems to be increasing more rapidly due to a greater diffusion of smartphone terminals. H/W and S/W for existing Wi-Fi based feature phones are limited by each manufacturer. However, as the smartphone is a portable terminal loaded with an open platform, a smartphone-based business can be exposed to security threats more easily than any other business.

Today's smartphones include multiple sensors, such as proximity sensors, light sensors, accelerometers, Bluetooth, microphone, and GPS, and newer models are even equipped with fingerprint recognition sensors and Near Field Communication sensors. While some of these sensors are irrelevant to security, others can provide a means of coping with security threats.

Preparation of thorough security measures for the smartphone equipped with multiple sensors and loaded with open platform is more important than anything else, as smartphones, though providing excellent mobility and convenience, can be exposed to a range of violation threats [3]. In particular, it is necessary to make efforts to develop a security system that can preemptively cope with potential security threats in the banking service area, which should be based on the high level of reliability [4]. This paper suggests a security reference model that should be considered by the smartphone-based joint mobile banking development project of the Bank of Korea. The purpose of this study is to make a security reference model for the reliable smartphone-based mobile financial service, by recognizing the specific security threats directed toward smartphones, and providing countermeasures to these security threats. Following the introduction, Section 2 introduces the joint smartphone-based banking project. Section 3 describes the security threats to the smartphone platform. Section 4 presents the mobile banking

Manuscript received Oct. 25, 2011; revised Nov. 9, 2011; accepted Nov. 16;
[+]Corresponding author

security reference model. Section 5 introduces the mobile banking issues in Korea and utilization of the security reference model. The last section provides a conclusion.

2. Joint smartphone banking development project

Since the release of the iPhone on November 28, 2009, Hana Bank and the Industrial Bank of Korea announced the release of application-type smartphone banking services in Korea [5]. These banks seemed to be poised to re-arrange the structure of the existing feature-phone based mobile banking market, and occupy the smartphone banking market in its early stage. These smartphone banking services are implemented such that the free application is downloaded from iPhone AppStore, and the public certificate is moved/copied from the PC. Currently, account transfer and balance check of deposit, loan, fund, and foreign currency accounts are supported by these services. In addition to independent services provided by individual banks, the banking industry has been promoting the development of a joint smartphone-based banking system since early 2009. The joint smartphone banking service standard was prepared through discussions by the Mobile Finance Committee, which is composed of 17 commercial banks. In December 2009, the Finance Informatization Promotion Committee adopted the "joint development project for the smartphone-based mobile banking service" as one of the finance information projects, and commissioned the Korea Financial Telecommunications & Clearings Institution to implement the project. The joint smartphone-based development project is expected to minimize the investment cost and risk to individual banks by realizing economies of scale in the smartphone environment, in which applications and security modules must be developed for each Operating System type, and to prevent customers of smaller-scale banks from becoming an alienated service class, as those banks would unavoidably have to give up service provisioning. In addition, overall service stability can be improved by applying common security measures such as public certificate, security module, and information leak prevention. However, customization by each bank will be allowed in application development (customer contact segment) in order to reflect the service differentiation needs of each bank, so that the differentiation needs of participating banks and market needs for convenient services can be satisfied at the same time.

In application-type smartphone (iPhone) based mobile financial service, the digital certificate is copied from the PC and saved in the smartphone by downloading it through the service provider's server. However, the digital certificate is integrated in the application in question. As a result, other applications cannot use this signature in joint development project, and have to download it again. The application of the joint development project driven by the Bank of Korea can share the digital certificate with other applications. The Ministry of Public Administration and Security encouraged the joint use of the digital certificate by distributing the dedicated application that stores and manages the digital certificate. As a result, the digital certificate issued by the Korea Financial Telecommunications and Clearings Institute to use mobile banking service can also be used for e-Government or mobile e-Commerce services.

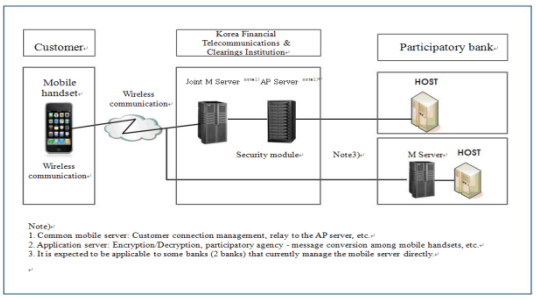

Fig 1. Configuration of the joint development project system for smartphone-based mobile banking services.

3. Security threats to the smartphone platform

The smartphone is a mobile handset equipped with computer functions, and has characteristics that make it similar to a PC. To attack a smartphone, hackers must have a prior understanding of the specific smartphone OS, as there are a larger number of smartphone OSs than PC OSs. In most cases, the scope of smartphone security incidents is limited to individuals, such as personal information leaks, device disabling, and financial information loss. As smartphones handle sensitive information and dedicated smartphone security software is not sufficient, it seems that security measures need to be established. Types of smartphone security incidents include personal information leaks, limited device use, illegal billing generation, and mobile DDoS. Table 1 shows the details of these various types.

Table 1 Types of smartphone security incidents

Violation incident pattern	Details
Personal information leak	Confidential information leak and privacy violation such as receiving message, phone directory, location information, and business files.
Limited device use	Terminal screen change, terminal breakdown (malfunction), battery consumption by malicious code, information (file, phone directory, etc.) deletion and program uninstallation.
Illegal billing generation	Financial loss due to spam SMS sending and small amount payments by the mobile handset.

Mobile DDoS	Causes illegal billing, web site paralysis, and terminal disabling by creating large amounts of traffic at a specific site and sending SMS to a specific terminal.

The most significant portion of smartphone security threats is caused by mobile malicious code. Mobile malicious code is a malicious program that is designed to perform malevolent actions on the mobile terminal, such as personal information leak, system breakdown, and remote connection, much like the malicious code found in the PC environment. Many mobile malicious codes have been reported, and the range of symptoms and damages caused by infection is quite broad. A total of 524 types of malicious code had been found as of June 2009, 60% of which were Trojans having the form of spyware, worm, or virus [6]. Mobile malicious codes perform the same behavior as malicious codes running in a regular PC. However, given that a smartphone usually contains e-mail addresses, text, and various files relevant for business, and processes diverse personal information including the user's phone book, personal information and company information, there is a high risk of the disclosure of sensitive information in a case of infection by mobile malicious code. In addition, smartphones are connected to the mobile communication network 24 hours a day, such as Code Division Multiple Access and High Speed Downlink Packet Access, as well as various Internet connection environments such as wireless LAN and Bluetooth. As a result, malicious codes can be dispersed quickly, using various methods such as Bluetooth, MMS, and e-mail. Mobile malicious codes are mainly diffused through social engineering. An example of mobile malicious code causing "illegal billing" is "Mosquit". It appeared in 2004. It masquerades as a hacking version of the popular game "Mosquitos" and is saved in the user's terminal that downloads it from P2P network. Then, an SMS is sent without the user's knowledge, leading to a high service charge to the user. Another example of mobile malicious code causing "limited device use" is "Stealwar". It appeared in 2007. Stealwar distributes several malicious codes to other terminals via Bluetooth, infects them, and then generates excessive Bluetooth traffic to use up the terminal battery.

As these codes attempt to infect the victim's terminal by masquerading as a free application or game downloaded through e-mail or a web site, users should be careful not to open unknown attachment files. In addition, the smartphone OS should be maintained in its most current version, by applying security updates and updating the application periodically, and important data should be encrypted before archival and backup to prevent the disclosure of important information even in the event that the terminal is infected. Mobile malicious codes in the smartphone environment can be diffused through synchronization with the PC, memory card, Wi-Fi, communication among smartphones, mobile data server, and mobile Internet. Most of the malicious codes identified up thus far have been diffused using Bluetooth and MMS. However, this only shows the numerical statistical data regarding the infection ratio by diffusion route, and security threats may exist in the open smartphone environment via various routes The simplest response to the spread of malicious code through the wireless interface is to deactivate the wireless interface function until the service is actually needed. Deactivating the wireless interface function not only protects the terminal from infection by malicious code, but also prevents unnecessary battery consumption. To protect the terminal from infection by malicious code via Bluetooth, the security setting for Bluetooth should be strengthened in such way that the user should be informed of any Bluetooth connection request from outside. In addition, if the function to selectively register trusted terminals is available, the user can block connections from malicious terminals by defining a list of trusted terminals in advance.

4. Mobile Banking Security Reference Model

This paper analyzes the security threats that can occur in the open type mobile-based electronic financial service, and describes countermeasures to analyzed threats. In addition, a mobile banking security reference model is suggested, which designers and developers can refer to when developing the mobile-based electronic financial system, in regard to security threats and security measures.

4.1 Security vulnerabilities in smartphone based mobile financial services

The preparation of thorough security measures for smartphones is more important than anything else, as smartphones, while offering excellent mobility and convenience can also be exposed to a range of violation threats. In particular, it is necessary to make efforts to develop a security system that can preemptively cope with potential security threats in the banking service area, which requires a high level of reliability. Figure 2 shows vulnerabilities on smartphone-based mobile financial service each component.

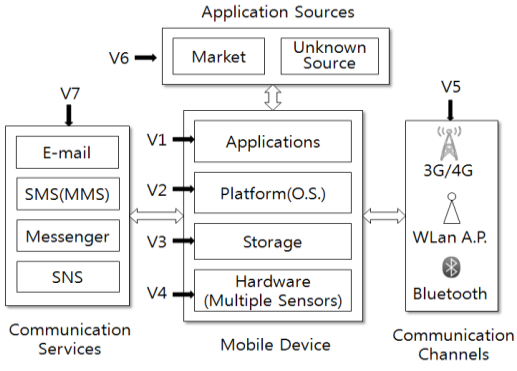

Fig 2. Vulnerabilities on the mobile banking service

Table 3 shows possible security vulnerabilities in smartphone-based mobile financial services.

Table 3 security vulnerabilities in smartphone-based mobile financial services

	Meaning	Threats
V1: Application	Attacks on vulnerabilities of an application that is recognized by users, unlike a virus.	T1.Phishing program
V2: Platform	Derivative attack is expected due to vulnerabilities or unique functional characteristics of the OS used in the open type mobile platform.	T2. Virus and malicious code T3. Keyboard hacking, T4. SMS hooking, T5.process memory dump
V3: Storage	Access to the file system loaded onto the internal/external memory of the mobile handset, confidential information extraction, and alteration attacks are expected.	T6. Confidential information extraction, and alteration attacks T7. S/W reverse Engineering
V4: Hardware	If the attacker obtains a stolen, lost, or disposed mobile terminal, the financial information can be extracted or disclosed accessing hardware directly.	T8. Acquisition by attacker (stolen, lost, or disposed mobile terminal)
V5: Communication Channels	Attacks using vulnerabilities of various types of communication channels.	T9. Rogue AP T10.Infection route
V6: Application Sources	Distribution the fake application or malicious code via several routes, such as the application store, black market, download site, and e-mail/MMS.	T10.Infection route (black market, internet download, memory card etc.)
V7: Communication Services	Attacks via communication services, such as e-mail, SMS, MMS, Messenger, and Social Networking Service.	T10.Infection route (mail or attached file of MMS) T11. Connection of the phishing site and receiving the phishing message through communication services

4.2 Security Threats and Countermeasures

4.2.1 Phishing Program

Attention should be paid to the following expected threat when designing the application for smartphone-based joint mobile banking system of the commercial banking industry, as an attack against the vulnerability of an execution application of which users are aware, unlike a virus. Applications containing malicious code can be distributed via the open smartphone application market, because anyone can produce and distribute the content and use it, and the application verification system is insufficient.

- Threat - T1

There can be a security threat in which the program containing the malicious code masquerades as a normal program and induces the user to install or use the program in question.

- Countermeasures – C1, C2

C1. The application is verified by the financial application verification institute, and verification is performed at the source code level, if needed.

C2. The code signature is generated in the application using the digital signature of the certification authority.

4.2.2 Virus and malicious code

The first mobile virus code was found in 2004 on a mobile terminal running Symbian OS [7], and since then, approximately 400 mobile malicious codes have been detected. A mobile malicious code (Trojan-SMS.Python.Flocker) was detected by Kaspersky Lab [8], which sends an SMS to the recipient registered in the phone directory of the mobile terminal that instructs them to transfer money to a certain account, using mobile malicious code.

- Threat - T2

- Modification, deletion, or disclosure of the user's personal information or stored application.
- Excessive traffic due to continuous requests for data, which were not initiated by the user.
- Sends large numbers of SMS using the user's phone directory.

- Countermeasures – C2, C3

C2. The code signature is generated in the application using the digital signature of the certification authority.

C3. Anti-virus installation is taken as the minimum measure to protect against virus and malicious code attack. Anti-virus software can be used to detect abnormal process execution in real time, and control unauthorized access to the resources saved in the mobile terminal.

4.2.3 Keyboard input value hooking

Keyboard input value hooking is a technique that snatches the user's keyboard input, and is exploited to find the password that the user inputs. This security weakness is most prominent in internet banking performed on a general computer, and financial damages related to this vulnerability periodically occur.

- Threat – T3

- It is known that hooking is possible for a physical keyboard like a QWERTY keyboard, but no such incidents have been reported thus far for a virtual keyboard.
- As the virtual keyboard accepts input with a fixed number of characters at a fixed location, which is integrated with the

terminal when it is shipped out, there is a possibility that the input character can be calculated by detecting mouse clicks or keyboard events.

- Countermeasures – C4, C5

C4. Technology is required that provides confidentiality of keyboard input values by making the data pass through the adapter (hardware that performs encryption) before connecting the keyboard device to the mobile terminal.

C5. The virtual keyboard can be used for the computer internet banking system.

4.2.4 Short message Service hooking

SMS is utilized for various financial services (e.g., personal information change), and the program that manages the SMS is implemented as an application. Due to different standards and localization problems, proprietary text engine programs are embedded and executed by each mobile operator.

- Threats – T4

- As commercial SMS programs equipped with convenient functions are sold online, an experienced developer can control the SMS through various approaches. The attacker attempts to make a mobile phone payment with his/her personal computer. The authentication code is sent to target's mobile terminal via the SMS. The SMS receiving event is created in the platform, and transfers the event or data to the SMS program. When the SMS related to the authentication number is received by filtering the string, the authentication number is sent to the pre-defined hacker's PC, and not to the original SMS program.

- Countermeasures – C2, C3

C2. The code signature is generated in the application using the digital signature of the certification authority.

C3. Anti-virus installation is taken as the minimum measure to protect against virus and malicious code attack. Anti-virus software can be used to detect abnormal process execution in real time, and control unauthorized access to the resources saved in the mobile terminal.

4.2.5 Process memory dump

Process memory dump means fetching the financial information by accessing the memory that is used by the operating system end in real time. Even though there have been no incidents reported of such a process memory attack on a mobile terminal, the smartphone environment is similar to that of a PC. Therefore, there is a possibility that this attack may occur.

- Threats – T5

The attacker dumps the memory by installing a virus or malicious code in the victim's PC in real time, or scans the major information in the memory only, and sends it to the attacker remotely via the network.

- Countermeasures – C3, C6, C7, C8

C3. Anti-virus installation is taken as the minimum measure to protect against virus and malicious code attack. Anti-virus software can be used to detect abnormal process execution in real time, and control unauthorized access to the resources saved in the mobile terminal.

C6. Delete the values and buffer immediately that was used to save the confidential information.

C7. Introduce the technology that controls access to other processes and memory.

C8. Programming with obfuscated codes is needed in order to make reverse engineering impossible, by declaring major variables separately at the development stage.

4.2.6 Extraction of financial and privacy information

Extraction of financial and privacy information refers to an attack that extracts and analyzes the application configuration file or the protection file that is internally encrypted by the application itself.

- Threat – T6

As it can be easily connected to the PC via a route such as Bluetooth or USB, the attacker can back up the victim's information to their PC using the interface function of the open-type terminal, and extract the user's financial information or privacy information[15].

- Countermeasures – C9, C10, C11

C9. Access control for the application layer and load for the file encryption technology.

C10. Process key generation and digital signature generation inside of the USIM card, when encryption operation is performed.

C11. Function of the digital certificate is basically loaded when distributing the financial IC card.

4.2.7 Software reverse engineering

For software used for financial settlement, this refers to an attack that identifies and misuses software vulnerability, such as the extraction of the encryption key through reverse engineering, or acquisition of the information that can be used to guess the encryption key.

- Threat – T7

Reverse engineering technology is used to find the user's password or analyze the encryption key built in the program, by analyzing the financial application when the encryption algorithm internally developed by the mobile communication service provider or the encryption key is included in the execution code.

- Countermeasures – C8

C8. Introduces the technique that prevents the attack via reverse engineering by making program source code difficult to read, using a code obfuscation technique.

4.2.8 Acquisition by attacker

If the attacker obtains a stolen, lost, or disposed mobile terminal, the attacker may acquire the financial information stored in the terminal without difficulty, or misuse the terminal for illegal financial transaction, if the terminal has an integrated NFC sensor.

- Threat – T8

Unlike a personal computer, a mobile terminal can easily be stolen or lost. In addition, due to the short product life cycle,

the terminal can be handed over to others after disposal, or re-sold on the used market. Once an attacker obtains the terminal, the attacker can extract or disclose the financial information stored in the terminal without difficulty.

- Countermeasures – C12, C13, C14, C15, C16, C17, C18

C12. The user should set a security system that requires a password when starting the mobile terminal or when the screen is displayed.

C13. The user should set the security password in the USIM.

C14. The user should not save any sensitive financial information in the terminal. If such information must be stored, use an information management application that provides security features.

C15. Install a remote management function in a PC that traces the location of the mobile terminal, and enables the remote deletion of major internal information. If the mobile terminal is lost, delete all important information saved in the terminal, and trace the terminal location to get it back quickly.

C16. When disposing of the mobile terminal or selling it as a used phone, initialize all information inside the terminal to completely remove all personal information.

C17. If the mobile terminal provides the financial settlement function using the integrated NFC sensor, install the function that can stop financial settlement function remotely. If the terminal is lost, terminate all financial settlement functions of the terminal, using this function.

C18. If the mobile terminal is equipped with a biometric sensor such as a fingerprint recognition scanner, use the sensor as a security device to identify the user.

4.2.9 Rogue AP

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator [9], or has been created to allow a hacker to conduct a man-in-the-middle attack.

- Threat – T9

General users may not consider which wireless access point they use for wireless communication, and simply use the wireless access point that is automatically selected. Taking advantage of these circumstances, the attacker installs a wireless access point that is not protected by encryption in a public place, and obtains information on the users who connect to the access point for data communication. In addition, the attacker guides the user to a phishing site by providing the phishing site address for the user's DNS query request.

- Countermeasures – C19, C20, C21, C22, C23

C19. Users should install a wireless intrusion prevention system that detects rogue APs, when using the terminal in public places like airport lounges.

C20. The user should use a security protocol that can prevent the MITM attack for finance-related services.

C21. The user should create a trusted wireless AP whitelist and allow registered APs only. (The user has to use the connection management application that manages the wireless AP whitelist.)

C22. The user should disable the automatic wireless AP connection function, and avoid connection to untrusted wireless APs.

C23. Install the phishing site blocking program in the mobile terminal.

4.2.10 Infection route

Mobile terminals can be infected with phishing programs, viruses, and malicious codes, via various routes. It is important to install anti-virus software or various security devices. However, it should be emphasized that the infection route of these malicious programs should first be identified and blocked completely.

- Threat – T10

- The attacker uploads a fake application to the application store by masquerading as a legitimate application.
- The attacker uploads the fake application on the black market.
- The fake application is distributed via the Internet download site.
- The fake application or malicious code is distributed as an attached file to e-mail, MMS, or Messenger.
- If the memory card used for the mobile terminal is connected to a PC infected with the malicious code, the malicious code can infect the memory card for the mobile device.
- If the user accepts a Bluetooth connection request from an external terminal infected with a malicious code, the malicious code spreads.
- The mobile malicious code waits on the PC for the user to synchronize his or her mobile terminal, then runs in background mode, infecting the smartphone when the PC is connected to the terminal.

- Countermeasures – C24, C25, C26, C27, C28, C29

C24. The application store administrator should perform a strong security review before uploading any application to the application store.

C25. The application store administrator should remove unsecure applications from user terminals using the remote application removal function.

C26. The user should not download and install applications from unidentified Internet sites or black markets. (Turn off the "Install unverified applications" option.)

C27. The user should not open unverified e-mail, MMS, and Messenger attachments.

C28. The user should turn off the automatic connection function to block unnecessary Bluetooth connection with external terminals.

C29. The user should try to avoid infection with malicious codes by strengthening the security of PCs connected to the mobile device.

4.2.11 Connection of the phishing site and receiving the phishing message through communication services

In addition to SMS and MMS, smartphones provides various types of communication services, such as e-mail, Messenger, and Social Networking Service. Threats can be caused when using these communication services, because the user can be guided to a phishing site, or financial fraud can be attempted using a phishing message.

- Threat – T11

- The user is guided to a phishing site, and the user's personal and financial information is disclosed.
- The user is misled into making a remittance, using the phishing message.

- Countermeasures – C23, C30, C31

C23. The user should install the phishing site blocking program in the mobile terminal.

C30. The user should double-check any such requests, using a secondary means of communication like a voice call.

C31. Be careful not to disclose the communication service address or personal profile information on an SNS article or Internet bulletin board.

4.3 Security Reference Model

System developers should be aware of the aforementioned security threats when developing the mobile-based electronic financial system, and prepare appropriate countermeasures. The mobile banking security reference model guides the developers of mobile-based electronic financial software to systematically check security threat factors and take preventive measures against them. Figure 3 shows the reference model proposed by this paper.

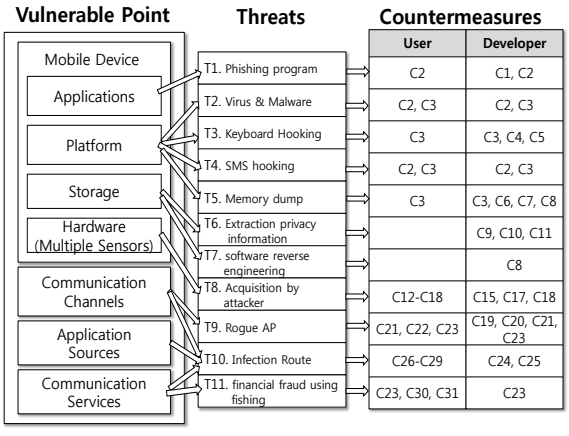

Fig. 3: Mobile banking security reference model

Components related to the security of mobile banking services are listed at the left side of the reference model, and possible threats to each component are mapped and described in figures. In addition, for each threat, countermeasures that could be taken from the standpoint of user and developer are listed at the right side. The "user" refers to the mobile terminal user, whereas the "developer" includes the financial service developer, terminal platform developer, and communication infrastructure developers. Various countermeasures can be taken both by user and developer. For example, when installing "C3 Anti-virus program," the user can install the program in his/her mobile terminal, or the developer can require automatic installation when the user accesses the financial site.

Table 4 below shows the example of a security development plan and checklist that the dedicated mobile development application team for a financial company applied to the mobile banking security reference model.

Table 4. Checklist for a financial company applied to the mobile banking security reference model

Component of mobile banking	Threats	Counter-measures	Application
Applications	T1.	C1.	N/A
		C2.	Use of code signature for dedicated application
Platform	T2.	C2.	*duplicated*
		C3.	Anti-virus installation automatically when server connected
	T3.	C3.	*duplicated*
		C4.	N/A
		C5.	Use of virtual keyboard in dedicated application.
	T4.	C2.	*duplicated*
		C3.	*duplicated*
	T5.	C3.	*duplicated*
		C6.	Delete the values and buffer immediately that was used to save the confidential information.
		C7.	Block the memory access form the other processes.
		C8.	Use of the code obfuscation technique.
Storage	T6.	C9.	Access control for the application layer and load for the file encryption technology.
		C10.	N/A
		C11.	N/A
Hardware	T8.	C15.	N/A
		C18.	If the mobile terminal is equipped with a biometric sensor such as a fingerprint recognition scanner, use the sensor as a security device to identify the user.
Comm.	T9.	C19.	N/A

Channels		C20.	The user should use a security protocol such as SSL that can prevent the SSL-MITM attack for finance-related services.
		C21.	The user should disable the automatic wireless AP connection function, and avoid connection to untrusted wireless APs, such as alert message.
		C23.	Install the phishing site blocking program in the mobile terminal.
Applicati on Sources	T10.	C24.	N/A
		C25.	N/A
Comm. Services	T11.	C23.	*duplicated*

5. Mobile banking issues in Korea and utilization of the security reference model

The joint service of the banking industry installs a different digital signature and security program for each smartphone model, which means that the security level is different for each smartphone. Korea Financial Telecommunications and Clearings Institute, which is developing the joint service on consignment, is considering a method that does not apply a firewall and antivirus program for its iPhone banking service. For keyboard security, it plans to install a virtual keyboard with enhanced security in the application. On the other hand, for the open OS Windows Mobile or Android-based smartphone [10], security technologies such as firewall, vaccine, and keyboard security will be applied. When Hana Bank and the Industrial Bank of Korea released iPhone [11] banking service in 2010, no security program other than the digital signature was applied. Hana Bank and others are also considering the installation of a keyboard security program, like the current joint smartphone banking service. Windows Mobile and Android-based smartphones are expected to apply a similar level of security. According to the analysis of Windows Mobile-based electronic financial service for general threats to Internet banking, such as file alteration and process memory dump, confidential information can be disclosed and files can be altered. For Windows Mobile, which was preferably selected as the target of the smartphone based joint mobile banking project in consideration of marketability, there is a high possibility that security threats to a regular PC can be transferred to the mobile terminal, considering that the regular computer environment is the Windows OS. In addition, as the software development environment is similar to the existing Windows environment, Windows hackers seem to be able to develop various hacking tools and produce and distribute malicious codes relatively easier than others. In addition, open-type mobile systems are likely to suffer from potential security threats due to the allowed access to internal files and execution of unauthorized application. An open-type mobile electronic financial service is likely to be vulnerable to the aforementioned security threats due to a lack of proven security products, such as keyboard security programs and anti-virus software [12]. Therefore, priority should be given to efforts to analyze security threats in advance and determine countermeasures. In addition, vulnerability analysis and the establishment of response plans are required for security threats implemented via the sensors of a mobile terminal that is equipped with diverse sensors.

Even though many security threats exist in the mobile banking service, the Finance Informatization Promote Committee has trouble balancing security and convenience. As the reliability of financial institutes can be significantly influenced, the security of the financial service takes precedence over convenience compared to other industries. However, convenience can be damaged and system development cost can be wasted if too great an emphasis is put on security without considering the current technology level. It is continuously pointed out that security is most important in electronic financial transactions, but convenience can be reduced if only security is highlighted without considering the characteristics of smartphones. Therefore, it is necessary to determine the proper security level, considering these issues. This paper recognizes the convenience and value of the smartphone equipped with multiple sensors, and also recognizes the security threat to mobile financial services, and presents countermeasures against these threats. The proposed mobile banking security reference model and benefits of this study can be summarized as follows.

- The proposed mobile banking security reference model is useful in improving system security by systematically analyzing information security threats to the mobile financial service, and by presenting the guideline for the preparation of countermeasures.
- It provides the foundation for finding and accumulating more threat factors and countermeasures, by presenting the initial model for the countermeasures as well as the threats that may occur in the open mobile-based electronic financial service.
- The proposed reference model can be effectively utilized when establishing security measures, which should be considered by the smartphone-based joint mobile banking development project implemented by the Finance Informatization Promotion Committee of the Bank of Korea.

6. Conclusions

Unlike a regular mobile phone, which provides voice call and message transmission functions only, the smartphone offers diverse functions, such as mobile settlement, MP3, camera, DMB, GPS, and Internet access, and includes various built-in sensors[13][14].

In particular, the smartphone has become an indispensable and useful Internet access tool in the ubiquitous environment, because data transmission via Bluetooth, Wi-Fi, and wireless network is supported at any time. Paradoxically, damage due to mobile malicious code can increase due to these changes, and it's time to take action to address this. As the performance of mobile terminals and software technology develops, the security threats to which electronic financial transactions on a PC are exposed may also occur in the open-type mobile terminal. This study explicitly presented the difference between PC and smartphone in terms of security, by reflecting these characteristics, classified the smartphone incident type, and analyzed mobile financial service threats and countermeasures against them. Also, the mobile banking security reference model was presented by making a model about mobile malicious code infection routes and mobile financial service threats, and countermeasures against these threats.

References

[1] Joris Claessens, Valentin Dem, and Joos Vandewalee, *"On the security of Today's Online Electronic Banking Systems",* Computers & Security, Elsevier advanced Technology, 2002, Vol 21, No 3, pp. 257-269.

[2] "*Utilization on internet banking service in korea"*, The Bank of Korea, 2010.

[3] Yung Fu Chang, C.S. Chen, and Hao Zhou, "*Smart phone for mobile commerce"*, Computers & Security, Elsevier advanced Technology, 2009, No 31, pp. 740-747.

[4] Paivi Heikkinen, "*A framework for evaluating mobile payments*", Financial Markets and Statistics, Bank of Finland , 2009.

[5] Jaewon kim, "*Smartphone banking gains popularity"*, the korea times, 2010.

[6] *Worldwide Mobile Security 2010-2014 Forecast and Analysis*, IDC, 2010.

[7] Symbian Developer Network, http://developer.symbian.com/

[8] Kaspersky Lab, http://www.kaspersky.com/news?id=207575728

[9] White paper of proxim corporation, "*Rogue access point detection: Automatically detect and manage wireless threats to your network, proxim wireless networks"*, 2004.

[10] Android Development, http://www.android-devs.com/?p=127

[11] Apple iPhone, http://www.apple.com/iphone/

[12] Giles Hogben, Marnix Dekker, "*Smartphones: Information security risks, opportunities and recommendations for users"*, European Network and Information Security Agency, 2010.

[13] Hahmin Jung, Dong Hum Kim, "*Control of a Mobile Robot Based on a Tangible Interface using iPhone"*, Journal of Korea Institute of Intelligent Systems , 2011, Vol 21, No 3, pp. 335-340.

[14] Yong-Hyun Cho, "*System Development for Guiding Job Information Based on Android Smart-Phone"*, Journal of Korea Institute of Intelligent Systems , 2011, Vol 21, No 5, pp. 588-594.

[15] Yong-Nyuo Shin, "*Standard Implementation for Privacy Framework and Privacy Reference Architecture for Protecting Personally Identifiable Information"*, International Journal of Fuzzy Logic and Intelligent Systems , 2011, Vol 11, No 3, pp. 197-203.

This work was supported by the research fund of Hanyang Cyber University(HYCU-2010-0017)

Yong-Nyuo Shin
Professor of the Hanyangcyber University
Research Area: telebiometric, mobile programming
E-mail : ynshin@hycu.ac.kr

WooChang Shin
Professor of the Seokyeong University
Research Area: Software engineering, formal method, mobile programming
E-mail : wcshin@skuniv.ac.kr