Journal of Korea Multimedia Society Vol. 18, No. 2, February 2015(pp. 218-232)
http://dx.doi.org/10.9717/kmms.2015.18.2.218

A Study on the Information Security Control and Management Process in Mobile Banking Systems

So Young Kim[†], Myong Hee Kim[††], Man-Gon Park[†††]

ABSTRACT

According to the development of information processing technology and mobile communication technology, the utilization of mobile banking systems is drastically increasing in banking system. In the foreseeable future, it is expected to increase rapidly the demands of mobile banking in bank systems with the prevalence of smart devices and technologies. However, the keeping 'security' is very important in banking systems that handles personal information and financial assets. But it is very difficult to improve the security of banking systems only with the vulnerabilities and faults analysis methods of information security. Hence, in this paper, we accomplish the analysis of security risk factor and security vulnerability that occur in mobile banking system. With analyzed results, we propose the information security control and management processes for assessing and improving security based on the mechanisms which composes mobile banking system.

Key words: Fault Mechanism; Hazard Factors; Information Security; Mobile Banking Process; Risks and Vulnerabilities; Security Threats Factors

1. INTRODUCTION

Recently thanks to the development of information processing technology and mobile communication technology, it is possible for bank users to use mobile banking services anywhere and anytime with a big convenience. Mobile banking means banking services with wireless and online networks, it expanded as a newly emerged banking service and then received lots of attention gradually.

The IC chip-based mobile banking service started in 2003. A special embedded IC chip issued by the bank is used as a security enhanced storage device, and this chip stores essential financial information for bank transactions such as account information. A PIN is needed to access information inside the chip. The VM mobile banking service started in 2007. VM differs from the IC-based banking service in that it only uses software to enable the financial transactions such as balance inquiry, and transfer of funds on the mobile device. It uses middleware programs such as WIPI that are created specifically for mobile banking. The VM mobile banking service not only authenticates the user through accredited certificates and secure cards but also conducts mobile phone self-authentication through SMS, and downloads and installs VM mobile banking software via call back URLs. Now on mobile banking services, financial institutions conduct the transactions through mobile banking application equipped with mobile operating system such as iOS and android in smart devices, and offer a wide variety of services which are account inquiry, transferring, credit card, fund

※ Corresponding Author : Man-Gon Park, Address : (608-737) Yongso-Ro 45, Nam-Gu. Busan, Rep. of Korea, TEL: +82-51-629-6240, FAX : +82-51-628-6155, E-mail : mpark@pknu.ac.kr
Receipt date : Nov. 27, 2014, Approval date : Jan. 29, 2015
[†] Dept. of Information Systems, Pukyong Nat. Univ., Rep. of Korea (E-mail : jnny10@naver.com)
[††] Dept. of IT Convergence and Application Engineering, PuKyong Nat. Univ., Rep. of Korea (E-mail : mhgold@naver.com)
[†††] Dept. of IT Convergence and Application Engineering, PuKyong Nat. Univ., Rep. of Korea
※ This work was supported by National Research Foundation (NRF) of Korea(2013K1A3A1A09076037).

Table 1. The Trends of Clients Enrolled on Mobile Banking Services (Unit: 1,000)

Service Delivery Systems	2010	2011	2012	2013
IC Chip	4,579	4,434	4,376	4,328
VM	8,561	8,946	8,749	8,421
Smart Devices	2,609 (16.6%)	10,358 (43.6%)	23,966 (64.6%)	37,185 (74.5%)
Total	15,749	23,738	37,091	49,934

Source: The Bank of Korea (2013)

transactions same as general banking services. Table 1 shows the number of clients enrolled on mobile banking services are increasing more and more, in the future the use of mobile banking based on smart devices is soaring sharply.

However, on the back side of mobile banking conveniences, the threats of mobile banking security are increasing gradually due to personal information is saved on mobile devices. Moreover, as the security threats are intellectualizing, advancing, security technologies for preventing personal information leakage and monetary damages became inevitable. In domestic case, from 2011 second half year the appearance of malicious code on smartphone is expected and will be spread rapidly. According to 2013 predicted analysis of banking IT information security trend, malicious code and hacking technology for threatening financial information are detected in overseas country 2010, by expanding intrusion paths with Wi-Fi, blue-tooth, mobile communications services on mobile devices, more strengthened security counteracted system for improving confidentiality, reliability and integrity is required after making public scenarios about banking security threat, which reveal threatening factors and vulnerabilities in mobile environment, and countermeasures.

Hence, in this paper, we propose what future strengthened banking security system do after analyzing vulnerabilities and problems of current banking security system based on analysis of risk factors, information security control and management process in order to build strengthened information security management process of mobile banking. And we show visualized figures of information security control and management mechanism and propose that improved plan of information security control and management based on analysis of mobile banking security risk factors and vulnerabilities after classifying each function of mobile banking security system through fault mechanism.

2. RELATED WORKS

Information Security means that protecting information system from unauthorized access and by acquiring availability, integrity and confidentiality, information security can be improved. Information security control and management are essential for information security of improved banking system, here information security control and management mean controlling and managing risk factors which degrade availability, integrity and confidentiality, so goal of this process is to protect confidential information, asset from unauthorized access. But there are a lot of threatening factors due to absence of information security control and management. First, the destruction of component and infrastructure on information security. Second, the damage which from human failure factors due to insufficient staff training and in-acquaintance of tools. Last, the unauthorized attacks such as hacking or malicious virus which are on banking information system [1-3].

For preventing these risks, we can categorize three types of information security control. First, physical control which means prevention from in-

trusion of unauthorized access internally. For example, file backup, security guard. Second, core technical control which uses hardware/software technology. For example, access control, anti-virus software and encryption technology. Last, administrative control which are management restriction and security policy. It aims at assuring that user can get access authority. For example, security awareness, technology training, security policy and procedure, supervision, which all are user-oriented technologies controlling user's behavior.

Fig. 1 shows general information security control and management process, through this, we can improve the security of banking system and then offer secure banking services to users. However, these processes are totally different by financial institutions although they have similarities. Because financial institutions have each and their own risk factors considering their locations, features of their location, their services, their business goal and technical structure. Also there is an information security management system for improving information security. It manages risk factors which exist in banking system. This composes security management, security countermeasure, security maintenance, security analysis, security compliance and security training [3-4]. With these efficient security systems and policies, information security policy is being established and security technologies are developing constantly in order to improve and advance information security.

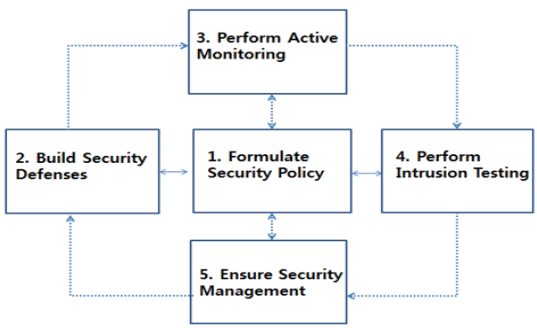


Fig. 1. Information Security Control and Governance Process Diagram.

2.1 Mobile Banking System

Recently with the consistent development of mobile devices and IT technology, mobile banking in banking industries is instituted and then now banking services using mobile devices is possible anywhere and anytime. Fig. 2 shows architecture of mobile banking and mobile banking system is based on two types of technologies. These are accessibility and remoteness.

For performing banking services, it needs web server, application server and database. Users of bank have to use their own mobile devices through mobile network for their transactions and communicate with core system of bank for processing these transactions as depicted in Fig. 3. The method how mobile banking system composes their services is that by using web, applications and web applications.

In domestic areas, mostly web-application meth-

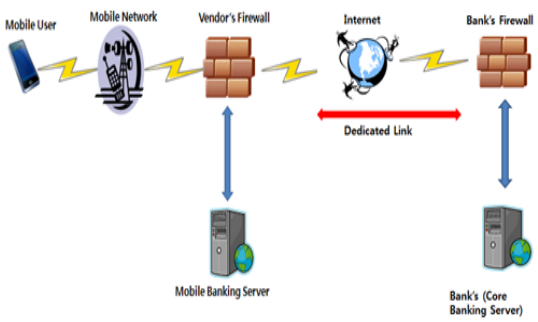


Fig. 2. Configuration Chart of Mobile Banking System

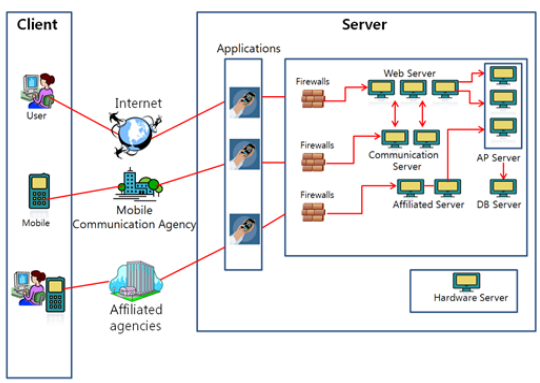


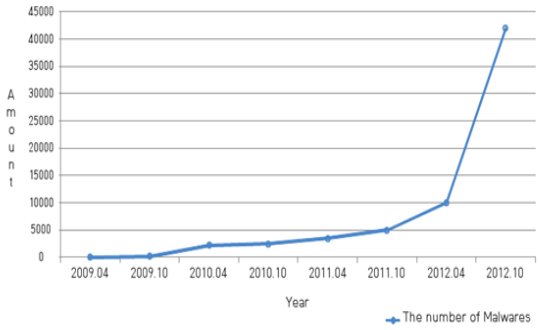
Fig. 3. Mobile Banking Operation System Configuration.

od is used. On web-application method, it transmits and processes transaction information on the web, it operates each and own security module on the application [3-4]. Then the mobile banking process is composed of three steps ([5-7]) as shown in Table 2.

2.2 Risks and Vulnerabilities on Mobile Banking Systems

Threats of security are increasing and security system in bank is very vulnerable according to prevalence of mobile banking. The damages such as a leakage of personal information and a new type of fraud are happening targeting mobile devices where personal data are loaded and so these are to be protected before being attacked from new type of threats. In mobile devices, major risks are malicious software, security policy violation, weak structure of wireless network, weak structure of payment system, SMS vulnerabilities, and Hardware/Software/Operating systems vulnerabilities. Fig. 4 shows that the number of malicious software which is risk factors in android operating system in 2012 are increasing sharply than in 2011. It also shows seriousness of security threats on mobile banking system [7-9].

Security threats in mobile devices are categorized mobile device system threat, user information threat, malicious code and malicious software



Source: Kaspersky Security Bulletin (2012)

Fig. 4. Increase of Android Malware.

threat, network transmission threat and physical threat like Table 3 by types of attack.

The researches about information security control and management are implementing continuously as an alternative preventing from security threats. Now, a lot of security systems are developed, however the stronger information security control and management are, the higher level of security threats and risks are. Therefore, it is urgent that we should improve information security of banking system through more enhanced information security control and process.

3. FAULT MECHANISM AND HAZARD FACTORS OF INFORMATION SECURITY CONTROL AND MANAGEMENT

It is very important to detect the security vul-

Table 2. Three Steps of Mobile Banking Process

Steps	Contents of Mobile Banking Process
User Authentication	The link with user and bank is encrypted using public/private key on mobile network. Server side on mobile banking requires authentication, user give personal information to bank and can enroll. And then, user on mobile can get authentication, bank confirms who is user passing on whole user's information. Lastly, server side on mobile banking can offer related data to users. Here, means of authentication is accredited certificate, account password and security card, One Time Password and so on.
Transaction request of user	User selects services which they want to transact. Server side on mobile banking requires re-authentication for confidential transaction. Here, re-authentication assures authenticated transaction.
Transaction processing of bank	Server side on mobile banking requires details about services which user asks for; also user passes on details to bank and transmits. Finally, the server requires re-authentication.

Table 3. Security Threats Factors in Mobile Banking ([10–15])

Type of Threat	Threat Factors
Mobile System Device Threat	Threats such as access to other application's process and memory, intrusion of malicious code and leakage of confidential information are exposed easily according to falsification of platform. Financial information of user is transmitted by outside attack in falsified application and exposed. File system without a permit accesses to file information and after acquiring authority of administrator, drains information of accredited certificate, application file. (Example) Malicious application which disguised it as a MADDEN NFL 12- If user installs this application, installed application sends message and incurs charge.
User Information Threat	A leakage of confidential information in user's system memory makes other process access easily, so threats of memory which has confidential information can happen. A leakage of user information is transmitted through network or recorded in mobile devices after collecting input data by using techniques. (Example) 2013 10th March, malicious application personating unpaid balance of national pension- After accessing to accredited certificate, photos, memo folders in smartphone and compacting, these are transmitted to remote site.
Malicious Code and Malicious Software Threat	Risk factors can intrude through linkage between devices, SMS route, and E-mail route through phishing, pharming, sniffing, and smishing. (Example) Malicious code 'Chest' targeting for small sum money payment in smartphone- After depriving user of personal information, it induces user to pay small sum money regularly.
Network Communication Threat	It can acquire personal information through transmitted plain text confidential data using tool. Moreover, it can acquire information through attacks, intrusion such as mobile DDOS from outside using network where security is weak. (Example) 2014 3.20 chaos- with big scale malicious code attacks, personal information of millions of people is leaked due to congestion of financial, broadcasting institution's computer network.
Physical Threat	A robbery and loss can occur because it is easy to access to other people's devices which have mobility. Also, infection from a removable disk can occur. (Example) In 2008, McDonald's crew in Arkansas State, America took a phone of man and spread nude photos which are saved on his phone.

nerabilities caused by faults from information security control and management. Also, the process of analyzing and resolving the security vulnerabilities should be handled importantly because faults can effect system and threaten the security. The security vulnerabilities get resolved with the following four processes as below.

- *Detect*: It detects events and investigate causes of faults.
- *Isolate*: It separates and isolates faults which are possible to happen.
- *Inform*: It informs happened faults to managing and operation system in detail.
- *Resolve*: It counteracts and resolves detected faults as fast as it can.

Here, risk factors mean factors which threaten, intrude into system and have a bad influence on system. If these states are 'Active', it causes serious situation. For this reason, we should find risk factors as well as faults and should analyze, counteract them. Through these procedures, we have to manage and control information security efficiently.

The security risk factors and faults exist by each function system in banking services. We classify security risk factors and faults in detail and suppose information security control and management process by tables as below [4].

3.1 User Authentication

User account and password are essential factors for user authentication as a first step in using banking services. Especially, password is very important to protect users in security system. Now when user uses banking service, account and password of user are formed according to policies about 'User account and Password'. Department where it manages these policies should have a conference about polices regularly and propose polices which have more improved contents of policies. The goal of this regulated polices is to build a strong security and then protect users. In <User Authentication> function, the most important thing is to authenticate user's identity. User Authentication is a procedure that makes sure whether user who is permitted access is or not, this procedure is progressing with 3 steps as below.

[Step 1] After entering ID/PWD, authenticate user.
[Step 2] Enter One Time Password as a second authentication.
[Step 3] Authenticate with accredited certificate for intensify authentication.

The way of ID/Password is commercialized normally, but nowadays the ways of accredited certificate, security card, OTP and biometrics are mostly used [3,11,16-18]. Table 4 depicts the information security control and governance according to security vulnerability and hazard factors under fault mechanism in user authentication phase.

3.2 Access Control

Access control is physical and electronic system to control access to network. Physical access control means normally locking the door, on computer, means controlling network security. Access control system which is spread to computer network has core center and core center operates system. Manager authorizes staffs to access using managing software systems.

For example, banking system which has many staffs and customers uses numerous access control system to block unauthorized user access. Here, access control classifies three parts on system: operating system, middleware and hardware as shown in Table 5. First, access control in operating system typically controls using mechanism such as 'Kerberos' algorithm which obtains security. Next, access control in middleware operates in database. Lastly, access control in hardware operates physical access control [3,11,19].

3.3 Hardware Systems

Each system on computer has more than 200 hardware/software systems and IT services. These are applied on banking system and banking services are processed. Each hardware system has its function and as the function operates, risk factors and vulnerabilities exist certainly. Vulnerabilities of information security in hardware systems occur at hardware platform, hardware operation and hardware maintenance steps as shown in Table 6. We say that as the role of mobile device is important, information security technologyand policy become inevitable on mobilebanking services [3, 11-12].

3.4 Operating System

Operating system on mobile device is open API, security vulnerabilities are exposed and it supports user connection environment of network. Operating system has the simplest interface between user and device while many steps are progressing through process management, memory management, device management, and storage management as shown in Table 7. Security vulnerabilities on operating system can occur at three types as below [11-12,20].

- Single-user, single task system: Normally, it allows one user each computer
- Single-user, multitasking system: It is basic

Table 4. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in User Authentication

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
ID/PWD	ID and PIN No., PWD exposure, ID and PWD hacking, and uninstalled Active X	PWD same as ID, Cellular Phone No. and Personal Info	ID should not be based on Personal Info; PWD should be set up as mixes of various characters (upper and lower case, no characters); Inform the level of ID, PWD security	Initialization of local devices, Apply virtual keyboard	Manager check each user's ID/PWD regularly and check security	IP detection system, Firewalls	Assess security policies and manage technologies continuously
Security Card	Leakage, robbery and loss of security card, leakage of security card image file, uninstalled Active X	Numbers of security card, security card image file	Create security card regularly and renew algorithm, Not use security card for a long time	Develop intensified OTP technologies, Use not fixed security card numbers	Inform user of security card renewal regularly; Check security regularly	Block off , initialize transactions when using for a long time, IP detection system, firewalls	Assess security policies and manage technologies continuously
OTP (One Time PWD)	OTP hacking, limit of OTP usage number, algorithm that makes OTP manipulation, uninstalled Active X	OTP token and key	Complement algorithm which makes OTP regularly	Take notice the management of OTP generator	Manager creates OTP regularly, establish management policies, Check security regularly	IP detection system, Firewalls	Assess OTP security policies and manage technologies continuously
Accredited Certificate	Leakage of certificate, robbery and loss of certificate, uninstalled Active X	Personal information	Oblige certificate issue, renew certificate regularly, increase security key size to 2048 byte	Institute complemented hardware Security Module, use intensified key algorithm	Manager checks each user's certificate regularly, check security, renew certificate regularly	IP detection system, Firewalls	Assess accredited certificate security policies and manage technologies continuously
Biometrics (finger prints, iris, face, and voice)	If it is leaked, it is impossible to restore, uninstalled Active X	Impossibility of accurate recognition, inaccurate matching threshold value	Not share means of authentication	Authenticate with dual factors using various parts of body	Control physical access through biometrics, encrypt information of biometrics	IP detection system, Firewalls	Assess biometrics security policies and manage technologies continuously

form, one user can perform many tasks

- Multi-user, multitasking system: Operating system manages requests of many users, a number of security controls are operating not to affect other users

3.5 Data Classification

Data classification is one of the control methods which protect confidentiality of information. Regardless of classification, all classification integrity and accuracy should be protected. Information can be categorized confidential information and public information as shown in Table 8. Confidential information has data which are very important or sensitive to handle. For example, personal information, system access information, file encrypted key file etc. Next, the other information is public information. Advantage of data classification is that risk management is easier and it is possible to shorten time which user accesses data. Therefore, although procedure of data classification is very complicated and takes a long time, it is very important task for information security on banking services [3,11,21].

Table 5. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Access Control

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Operating System	Robbery of file records about customers; intrusion from open API environment	Open API, information of rigged mobile OS log, malicious code	Prohibit from reading other user file; prohibit from using other user memory; prohibit from using other user device	Build trusted computing technology; isolate process; authorize file system	Encrypt file system; operate security sand box system; operate remote control	Code signature; rehearse simulation hacking scenario; IP detection system; Firewalls	Assess security policies and manage technologies continuously
Middleware	Hacking of file managing database; intrusion	Attempts of each system log-on	Only authorized user can access	Build dual computing technology; authorize access of DB	Encrypt database system, operate remote control	IP detection system	
Hardware	Error of mobile device operation; unawareness of instructions, robbery, loss of devices	Malicious code and malware	Set up the encrypted pattern; password on device; Finger-prints and voice authentication	Intensify physical access control technologies	Encrypt mobile devices	Surveillance camera, X-ray inspection	

Table 6. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Hardware Systems

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Hardware Platforms	Falsified platform; absence of communication with network	Link with weakly secure network, malicious code	Establish procedure to check whether falsified platform or not; analyze malicious code	Apply access blocking technology to falsified platform	Apply blocking technology when a new falsification technique created	Falsification detection procedural technology	Assess security policies and manage technologies continuously
Implementation	Leakage of confidential file; breakdown of device	Error of hardware operation, malicious code, forged application	Have access control to falsified application; access control of route authority; analyze malicious code	Analyze static application code and dynamic application code	Monitor malicious code detection	Real time access detection system	
Maintenance	Leakage of confidential file; device unavailability	Malicious code; device robbery	Have maintenance regularly, intensify function testing of hardware, analyze malicious code	Analyze static application code and dynamic application code; initialize remote device	Monitor detection through remote control	Surveillance camera	

3.6 Virus Detection and Control

Recently more and more malicious virus and malicious software affect information security system, they are threatening security system as form of them are diversifying. Malicious software means software which interrupts user's work and damages system after being installed on computer or mobile devices. They have damages from simple advertisement pop-ups to system intrusion. Types of malicious software are virus, adware, spyware, Trojan horse, spam, phishing, pharming, and so on. And intrusion routes are website visits, downloads

Table 7. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Operating System

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Processor Management	Authority threat by sharing with user ID; unseen process performance; malfunction of process function	OS log information; browser history	Prohibit other user from reading file, using memory; and using device	Authorize file system, isolate process; allow to eliminate potential risk factors	Operate security sand box system; encrypt file system; authorize route	Real time access detection system	Assess security policies and manage technologies continuously
Memory Management	unseen process performance; malfunction of process function	OS log information; browser history	Prohibit other user from using memory	Build virtual memory technology; encrypt file system	Operate security sand box system; encrypt file system	Real time access detection system	
Device Management	Falsified platform, leakage of confidential file; unavailability of device	Robbery and loss of devices; malicious code; forged application	Prohibit other user from using device	Protect key Chain data; remote wipe	Provide API of managing device by OS; encrypt file using SHA-1 and hash function	Surveillance camera	
Storage Management	Leakage of confidential file; disc space hacking	OS log information; browser history	Prohibit other user from reading file; prohibit other user from using memory	Encrypt disc access	Operate security sand box system; encrypt disc access	Real time access detection system	

Table 8. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Data Classification

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Confidential	Robbery and loss of data; fabrication of data contents	Hacker access; malicious code; data which are already infected	Perform encryption of access to database	Intensify security level of filtering; block unauthorized user access; encrypt database dually; Backup data regularly	Monitor traffic; detect based on heuristic	Real time access detection system	Assess security policies and manage technologies continuously
Public	Robbery and loss of data; fabrication of data contents	Hacker access; malicious code; data which are already infected	Perform encryption of access to database				

and installation of software, link with network as shown in Table 9. Through these routes, they deceive users, and then extract personal information and these routes are more diversifying. Financial institutions are extremely interested in information security, nowadays solutions of eliminating risk factors are released and interests about these solutions are rising gradually [3,7,11,13].

3.7 Database

Database is a storage area of all data; also it is one of the main systems which operate control for data security. Factors which affect database are access of unauthorized user, excess of user access, wrong system design and SQL performance and vulnerability of protocol. It is highly interested in database and database security because database in banking system handles sensitive, massive information as shown in Table 10. If database in-

Table 9. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Virus Detection and Control

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Website visits	Leakage of personal information; financial frauds	Malicious code; malicious software	Intensify access controls; Report damages by malicious code to the police; Install antivirus; Update antivirus regularly	Install antivirus, anti-malware; use dalvik virtual machine	Update vaccine program regularly	IP detection system, firewalls	Assess security policies and manage technologies continuously
Link between devices	Leakage of personal information, financial frauds	Malicious code; malicious software			Update vaccine program regularly	Check whether device has virus or not before link	
Application installation through SMS, E-mail including installation routes	Leakage of personal information, financial frauds	Forged application including malicious code			Update vaccine program regularly; build center where application is verified; filter spam e-mails	IP detection system; firewalls; detect and block forged application	

Table 10. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Database

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Plan database	Data leakage, violation of laws of personal information protection; spread a database security policy	False designed policies and disciplines	Define database security rules; compose organization of database security	Control access authority of database security policy and guidelines	Operate audit monitoring of internal security	Trace the collected data route and detect whether it has malicious code or not	Assess database security policies and manage technologies continuously
Design database	Data leakage, violation of laws of personal information protection; spread a database security design policy	False designed policies and disciplines	Define access control rules; define encryption key and algorithm; design simulated hacking scenario	Control access authority of database security policy and guidelines	Operate audit monitoring of internal security	Trace the collected data route and detect whether it has malicious code or not	
Build database	Data leakage, inflow of malicious code, DBMS source code leakage; Not implementation of examining environment which embodies database	Unauthorized access, false cipher text	Build environment which embodies database; examine and complement environment which embodies database; perform the test which applies simulated hacking;	Approve database tasks; encrypt key; prevent detour access; delete original data	Operate audit monitoring of internal security	Outside access detection system	
Operate and manage database	Inflow of malicious code, leakage of data, exposure of database security vulnerability	Impaired database; records of failed database services; unauthorized access	After maintaining, improving and complementing embodied technology factor; making operating reports	Authenticate user; control access of user log; backup database	Monitor operation state and result of technology	Outside access detection system	

cludes confidential information which classified by data classification, backup should be performed in order to prepare for instant changes of system, network periodically. Now institutions where it

handles personal information should oblige encryption of personal information and when they can save the data into local network of banking system, all data can be handled safely only if data meet standards of data encryption and various degree of risk analysis. However, if financial institutions where they deem speed as important encrypt, quantity of data will be increased greatly, performance of server will deteriorate and cost will increase. Also financial institutions could not find perfect solution until now, therefore it is essential to prepare a countermeasure about this problem [3, 11,22].

3.8 Network Systems

For using banking services, network systems became inevitable and it offers a lot of conveniences to users by providing network access environment. But while interest about network security is steadily increasing, threats are also increasing sharply. It is essential to build secure network between internet and user in banking information security. Here, network is all devices which block intrusion signal, allow remote access, block and prevent possible attacks.

Every personal information should be transmitted with encryption through network and should not be exposed to outside by decrypting to plain text while transmitting as shown in Table 11. Now financial institutions are using a lot of ciphering algorithms and hash functions in order to transmit data securely applying cipher technology at communication section [3,12,23].

3.9 Backup Restoration

It is very important to back up in advance in order to prepare for system failure and disaster in banking system. Recently after '3.20 Cyber Terror', financial institutions have greatly emphasis on urgency and necessity of backup restoration system. Backup system means all hardware, software and infrastructure systems for backing up, moreover its types and components are a lot [3,7,24-25]. Information security control and management process according to security vulnerability and hazard factors in backup restoration is shown in Table 12.

Now financial institutions build more than 300 virtual servers and dispersed 3,500 business use PC enterprise backup restoration systems at more than

Table 11. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Network Systems

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Network operation management	Robbery and loss of data; wiretapping; inflow of malicious code; Packet sniffing at wireless section; access to internal intranet	Hacker access; malicious code; Wi-Fi, GPS, Bluetooth, 2,3G, Wibro; DDOS attack; exposed location information through wireless net	Encrypt access to network; link mobile platform directly from mobile comm. to personal circuit	Use AP which function of authentication and encryption is set up; apply VPN	Always monitor traffic; build system which detects intrusion to wireless LAN	IP detection and tracking system, firewalls	Assess security policies and manage technologies continuously
Network equipment management	Robbery and loss of data; robbery and loss of network equipment	Malfunction of equipment; not implementation of equipment maintenance	Block direct link to internal server, link directly from mobile comm. to personal circuit	Manage firewalls based on host, Block and control unnecessary ports; build relay connected server which separates internal and external nets	Build system which detects intrusion to wireless LAN; prepare equipment related with FMC	Network equipment location detection and tracking system	

Table 12. Information Security Control and Management Process According to Security Vulnerability and Hazard Factors in Backup Restoration

Fault Mechanism	Security Vulnerability	Hazard Factors	Information Security Control and Governance Process				
			1. Formulate Security Policy	2. Build Security Defense	3. Perform Active Monitoring	4. Perform Intrusion Testing	5. Ensure Security Management
Design and build backup system	Leakage of confidential information due to inflow of malicious code when operating backup system	Analysis of false backup requirements; false operation management guidelines	Analyze backup requirements; do back up testing; train administrator	Control outside access, control with laws when spreading backup system design	Monitor design and build of backup system; examine backup system regularly	Track backup data routes; detect malicious code	Assess security policies and manage technologies continuously
Operate backup system	Leakage of confidential information; inflow of malicious code	Backup errors; backup infrastructure which are designed falsely	Have conference about backup operation; take action by backup error types	Design server which is exclusive use of backup; back up regularly	Monitor backup performance; Have simulated restoration training regularly	Operate system which detects and tracks internal and external accesses; detect malicious code	

200 branches all over the country. By doing this, they can improve stability, operational easiness, security of personal information for future banking systems. Based on analysis of risk factors and vulnerabilities through 9 departmentalization of each mechanism in mobile banking systems, we propose practical processes for information security control and management in mobile banking systems as above Tables 4-12 and visualize these processes as shown in Fig. 5.

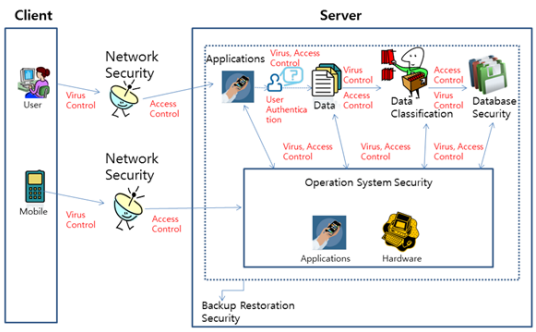


Fig. 5. Information Security Control and Management Process on Mobile Banking System.

4. CONCLUSIONS

Recently the use of mobile banking services is more and more increasing depending on the development of mobile devices and technologies. However, risk factors which intrude banking system are developed, expanded and they are threatening users gradually. Because users who use banking services want to get services securely, want their personal information to be protected safely anywhere and anytime with convenience, interests about information security are increasing steadily.

In this paper, we specifically find factors which threaten mobile banking security through the analysis of risk factors of mobile banking security by functions of banking services which information security should be applied and security vulnerabilities caused by these risk factor, the information security control and management process. With these, we can analyze problems and vulnerabilities of current mobile banking system. Also by analyzing risk factors and making the information security control and management process for managing, controlling mobile banking security system, we can find all causes of system defect occurrence easily and prepare a strong countermeasure about security threats and intruding factors.

Hence in this paper, we propose some important points which should be secured in mobile banking services. In the future, main task is to improve infrastructure security technologies of mobile banking systems. This means that we should build in-

tegration test and verify the security of mobile devices by mobile devices, platforms before developing applications. Next, we need a security-strengthened system in wireless LAN such as network intrusion detection or building a responding system for acquiring safety of wireless network. At the operational management side, operating security conference among security companies, mobile device manufacturing companies and telecommunication companies should be revitalized in order to build a well-organized security management system.

Lastly, it is greatly important to develop new security control and management methods which security protection level is advanced by researching and analyzing threatening factors and vulnerabilities of mobile banking security systems through risk analysis and fault analysis, also continuous control and management about current security services and technologies.

REFERENCES

[1] H. Y. Min, J. H. Park, D. H. Lee, and I.S. Kim, "Outlier Detection Method for Mobile Banking with User Input Pattern and E-finance Transaction Pattern," *Journal of Internet Computing and Services*, Vol. 15, No. 1, pp. 157-170, 2014.

[2] J. S. Seong, "A Study on the Prevention of Security Incident," *Journal of Security Engineering*, Vol. 9, No. 6, pp. 503-510, 2012.

[3] Certified Information System Banker-Rules and Syllabus (2007), Indian Institute of Banking and Finance, http://www.iibf.org.in/documents/ceisb-module1.pdf (accessed on Nov., 20, 2014).

[4] K. Biri and G. M. Trenta, *Corporate Information Security Governance in Swiss Private Banking*, Master's Thesis of Executive MBA Program of the University of Zürich, 2004.

[5] J. Nie and X. Hu, "Mobile Banking Information Security and Protection Methods," *Proceeding 2008 International Conference on Computer Science and Software Engineering*, pp. 587-590, 2008.

[6] H. G. Shin, "Year 2013 Predictive Analysis of Information Security Trends in Banking IT," *Journal of Payment Settlement and IT, Korea Financial Telecommunications and Clearings Institute*, Vol. 51, pp. 581-86, 2013.

[7] H. G. Shin, "Year 2014 Predictive Analysis of Information Security Trends in Banking IT," *Journal of Payment Settlement and IT, Korea Financial Telecommunications and Clearings Institute*, Vol. 55, pp. 90-126, 2014.

[8] Security of Mobile Banking and Payments, http://www.sans.org/reading-room/whitepapers/ecommerce/security- mobile-banking-payments-34062 (accessed on Oct., 24, 2014).

[9] K. H. Lee and Y. Y. Kim, "The State of Mobile Banking Service in Domestic Banks," *Journal of Information and Communication Policy, Korea Information Society Development Institute*, Vol. 14, No. 18, pp. 2-15, 2002.

[10] C. S. Park, "The Policy Direction of Smart Security," *Journal of the Telecommunication Technology Association*, Vol. 133, pp. 23-27, 2011.

[11] M. H. Kim, W. Toyib, and M.G. Park, "An Integrative Method of FTA and FMEA for Software Security Analysis of a Smart Phone," *Korean Information Processing Society Transactions on Computer and Communication Systems*, Vol. 2, No. 12, pp. 541-552, 2013.

[12] B. K. Lee, *A Research on Discovering New Vulnerabilities and Analyzing Methods in Domestic Mobile Environment*, KISA-WP-2012-0009, Research Report of the Korea Internet & Security Agency, 2012.

[13] J. C. Ryu, *A Study of Malware Detection Based on Mobile OS*, KISA-WP-2010-0057,

Research Report of the Korea Internet & Security Agency, 2010.

[14] S. W. Na, Y. H. Lee, and S. J. Ji, *Security Issue and Counterstrategies of Smartphone and Mobile Office*, CIO Report of National Information Society Agency, 2010.

[15] K. Streff and J. Haar, "An Examination of Information Security in Mobile Banking Architectures," *Journal of Information Systems Applied Research*, Vol. 2, No. 2, pp. 1-16, 2009.

[16] J. H. Lee, "Usage and Problems of Authentication Certificate on Smart Environment," *Journal of Internet and Security Focus*, *Korea Internet and Security Agency*, Vol. 3, pp. 23- 53, 2013.

[17] H. R. Yeom, *A Research on Security Criteria for Extension to Electronic Authentication Method Usage-Based*, KISA-WP-2011-0019, Research Report of the Korea Internet & Security Agency, 2011.

[18] S. M. Jang and M. G. Park, "A Study on the Fault Analysis and Security Assessment for Smart Card Management System," *Journal of Korea Multimedia Society*, Vol. 17, No. 1, pp. 52-59, 2014.

[19] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley Publishing, Indianapolis, Indiana, 2008.

[20] A. Silberschatz, P. B. Galvin, and G. Gagne, *Operating System Concepts*, 7th Edition, John Wiley and Sons, Inc., Hoboken, New Jersey, 2005.

[21] Data Classification of Information Security Glossary (2014), RUsecureTM Security Policy World, http://www.yourwindow.to/information-security/gl_dataclassification.htm (accessed on November 12, 2014).

[22] Database Security of Enterprise Risk Management (2010), http://www.emrisk.com/sites/default/files/newsletters/ERMNewsletter_March_2010.pdf (accessed on Nov., 12, 2014).

[23] Securing the Network Perimeter of a Community Bank, http://www.sans.org/reading-room/ whitepapers/firewalls/securing-network-perimeter-community-bank-33248 (accessed on November 12, 2014).

[24] W .C. Preston, *Executive Brief on VMware Backup and Recovery: Challenges and Solutions*, VMware® Partner, 2011.

[25] W. C. Preston, *Backup Hardware*, Backup & Recovery, O'Reilly®, Canada, 2007.

So Young Kim

She graduated with the B.E. in IT Convergence & Application Engineering at the Pukyong National University, Rep. of Korea in 2014.

She is a research member of the Software Engineering and Multimedia Information Systems Lab. as well as a master degree student of the Dept. of Information Systems, Graduate School, Pukyong National University, Rep. of Korea.

Her research interests are in Software Security, Software Safety, and Big Data Analysis Methods.

Myong-Hee Kim

She graduated with the B.E. in Information Communication Engineering at the Dongseo University, and received M.S. degree in Computer Science and Ph. D. in Information Systems from the Pukyong National University, Busan, Rep. of Korea. She was a Post Doctoral Researcher at the University of Colorado-Denver, USA. She is a lecturer of the Department of Information Systems, Graduate School, Pukyong National University. Also she was a lecturer of the Department of Computer Science and Engineering at the University of Colorado-Denver, USA. She served as an Assistant Faculty Consultant and a professional specialist in Information Communication Technology and Web-Based Multimedia Ttechnologies for CPSC which is an Inter-Governmental International Organization for Human Resources Development in Asia and the Pacific Region.

Man-Gon Park

He is a head professor of the Dept. of IT Convergence and Application Engineering, College of Engineering, Pukyong National University, Republic of Korea since 1981. Also he was the president and chairman of the Korea Multimedia Society (KMMS). He served as the Director General and CEO of the Colombo Plan Staff College for Technician Education (CPSC) from 2002 to 2007, which is an intergovernmental international organization of 29 member governments for Human Resources Development in Asia and the Pacific Region. He has been the visiting professor at the Department of Computer Science, University of Liverpool, UK; exchange professor at the Department of Electrical and Computer Engineering, University of Kansas, USA; and visiting scholar at the School of Computers and information science, University of South Australia; visiting professor at the Department of Computer Science and Engineering, University of Colorado, Denver, USA.

He was dispatched to Mongolia and People's Rep. of China by KOICA on various projects as information systems consultant. He has also embarked on consulting works and conducted training programs in ICT on individual capacity for Korean groups of companies, governmental and non-governmental agencies and other institutions in Korea. His main areas of research are software reliability engineering, software safety and security engineering, business process reengineering, Internet and web technology, multimedia information processing technology, and ICT-based human resources development