Journal of Korea Multimedia Society Vol. 18, No. 11, November 2015(pp. 1342-1350)
http://dx.doi.org/10.9717/kmms.2015.18.11.1342

모바일 뱅킹 정보시스템의 소프트웨어 보안성 개선을 위한 고장 트리 분석과 고장 유형 영향 분석

김소영[†], 김명희[††], 박만곤[†††]

Fault Tree Analysis and Failure Mode Effects Analysis for Software Security Improvements in Mobile Banking Information Systems

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

ABSTRACT

Due to rapid development of mobile device technologies, the mobile banking through Internet has become a major service of banking information systems as a security-critical information systems. Recently, lots of mobile banking information systems which handle personal and transaction information have been exposed to security threats in vulnerable security control and management processes, mainly software systems. Therefore, in this paper, we propose a process model for software security improvements in mobile banking information system by application of fault tree analysis(FTA) and failure modes and effects analysis(FMEA) on the most important activities such as 'user authentication' and 'access control' and 'virus detection and control' processes which security control and management of mobile banking information systems are very weak.

Key words: Software Security, Security-Critical Information Systems, Mobile Banking Information Systems, Fault Tree Analysis(FTA), Failure Modes and Effects Analysis

1. 서 론

최근 정보기술의 발전과 모바일 디바이스의 발전으로 인해 언제 어디서나 모바일 단말기를 이용한 뱅킹 업무가 가능해지면서 사용자들에게 편리함을 제공해주고 있다. 모바일 뱅킹은 이동통신단말기를 수단으로 무선인터넷을 통해 금융기관의 뱅킹 시스템(Banking System)과 연결하여 이루어지는 금융서비스를 말하며, 다양한 형태의 뱅킹 시스템 중, 앞으로 스마트폰을 기반으로 하는 모바일 뱅킹의 이용이 증가할 것으로 보고 있다. Table 1에서는 2010년부터 2013년 사이의 스마트폰을 이용한 모바일 뱅킹 등록 고객 수의 증가를 나타내고 있다. 2010년에는 스마트폰을 기반으로 한 모바일 뱅킹 등록 고객 수가 가장 적었지만 2011년 약 4.5배 정도 증가하고, 2013년에는 2010년의 수보다 14배가 증가하여 대부분의 고객들이 스마트폰을 기반으로 한 뱅킹 서비스를 이용하다는 사실을 알 수 있었다[1].

그러나 언제 어디서나 이용할 수 있다는 특징으로 인해 모바일 뱅킹 서비스는 다양한 보안 위협에 노출

※ 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 : Jul. 27, 2015, Revision date : Aug. 24, 2015
Approval date : Sep. 7, 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 the Pukyong National University Research Abroad Fund in 2012 (PS-2012-020).

Table 1. The Numbers of Customers who Enrolled in Mobile Banking

Classification \ Year	2010	2011	2012	2013	2014
IC Chip	4,579	4,434	4,376	4,328	3,645
VM	8,561	8,946	8,749	8,421	8,260
Mobile Devices	2,609 (16.6%)	10,358 (43.6%)	23,966 (64.6%)	37,185 (74.5%)	48,203 (80.19%)
Total	15,748	23,737	37,092	49,934	60,107

Source: The Bank of Korea (2014), Unit: 1,000

이 되기 쉽다. 보안 위협(Security Threats)은 주로 사용자 인증 (User Authentication) 단계와 접근 통제 (Access Control) 단계 그리고 바이러스 탐지 및 통제(Virus Detection and Control) 단계에서 가장 많이 발생한다. 그 외에도 뱅킹 시스템 내의 운영체제, 데이터베이스, 네트워크 등에서도 보안성이 위협당하고 있다. 장차 다양하고 고도화된 해킹 기법으로 모바일 뱅킹 시스템을 위협하여 사용자들에게 심각한 피해를 줄 것으로 예상된다[2].

따라서 본 논문에서는 모바일 뱅킹 정보시스템에서 가장 보안성이 취약한 사용자 인증 프로세스와 접근 통제 프로세스에서 결함 트리 분석(FTA)과 고장 유형 영향 분석(FMEA)을 수행하여 모바일 뱅킹 정보시스템의 보안성을 개선시킬 수 있는 방법을 제안한다.

2. 관련연구

뱅킹 정보시스템과 같은 보안 중요 정보시스템(Security-Critical Information Systems)의 보안성을 개선하기 위해서는 시스템 내에 존재하는 결함이나 취약점을 찾아내어 분석하는 일이 우선시되어야 한다. 이를 위해서 많은 분석기법이 사용되고 있는데, 그 중에서 결함트리분석(FTA, Fault Tree Analysis)은 결함 원인을 식별하고, 식별된 결함원인을 분석하여 Fault Tree(FT)를 작성하고 이를 기반으로 하여 구성된 Fault Tree에서 정상사상이나 중간사상의 발생 확률들을 계산 하여 시스템의 안전성 및 신뢰성 분석 및 평가하는 도구로 사용한다. Fig. 1에서는 FT 구조의 한 예를 보여주고 있다[3,4].

고장 유형 영향 분석 (FMEA, Failure Modes and Effects Analysis)은 시스템의 잠재적 고장 모드를 찾아내고 시스템의 운영 중에 잦은 고장들이 발생하

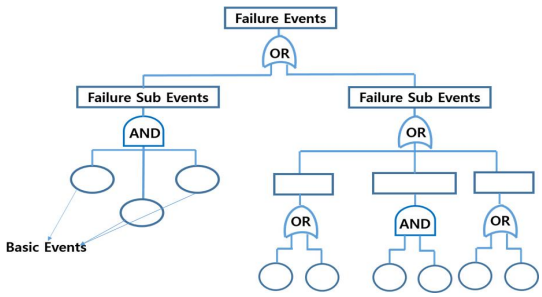

Fig. 1. A Structure of FT(Fault Tree).

였을 경우 임무 수행이 미치는 영향을 조사하여 평가하고, 영향이 큰 고장 모드들에 대해서는 적절한 대책을 세워서 고장들의 미연 방지를 도모하는 방법이다. 그래서 예상되는 결함 빈도, 결함의 영향도, 피해정도에 관하여 평가를 하며 보안 중요 정보시스템의 보안성 개선을 위해서는 이러한 기법을 통하여 보안성을 확보하는 것이 매우 중요하다. Table 2에서는 FMEA를 수행할 때 사용되는 FMEA 시트를 보여주고 있으며 FMEA 시트를 작성함으로써 FMEA 기법을 수행할 수 있다. FMEA의 수행 알고리즘은 다음 Fig. 2와 같다[3-6].

3. 모바일 뱅킹시스템에서의 위험요인과 취약성

모바일 뱅킹시스템에서의 사용자 인증과 접근 통제 단계 그리고 바이러스 탐지 및 통제 단계에서 보안이 취약하여 가장 많은 보안위험요소들이 발생하여 다양한 형태의 위협을 받게 된다.

3.1 사용자 인증(User Authentication)

모바일 뱅킹 정보시스템의 서비스를 이용하기 위해서는 까다로운 절차의 사용자 인증 단계를 거쳐야만 한다. 여기서, 사용자 계정과 비밀번호는 필수요

Table 2. FMEA Sheet

Function		*Dispense amount of cash requested by customer*		
Potential Failure Mode		*Does not dispense cash*		*Dispenses too much cash*
Potential Effects of Failure		*Customer very dissatisfied*		*Bank losses money*
S (Severity)		*0.8*		*0.6*
Potential Cause of Failure		*Out of cash*	*Machine jams*	*Bills stuck together*
O (Occurrence)		*0.5*	*0.3*	*0.2*
Current Process Controls		*Internal low cash alert*	*Internal jam alert*	*Loading procedure*
D (Detection)		*0.5*	*1.0*	*0.7*
RPL (S*O*D)		*0.200*	*0.240*	*0.084*
C (Criticality)=RPL/D		*0.40*	*0.24*	*0.12*
Recommended Action(s)		*Periodical refill cashes*	*Repair Bill Counting Part of Cash Machine*	*Repair loading part of bill stuck*
Responsibility and Target Completion Date		*Within 1 hour*	*Within 10 hours*	*Immediately*
Action Results	Action Taken	*Repair Bill Counting Part of Cash Machine and Periodical refill cashes*		*Repair loading part of bill stuck*
	S	*0.8*		*0.6*
	O	*0.1*		*0.01*
	D	*0.5*		*0.9*
	RPL	*0.040*		*0.054*
	C	*0.020*		*0.060*

소이다. 사용자 인증은 허가된 사용자인지 아닌지를 구분하며 다음과 같은 세 단계로 진행된다.

Step 1. 사용자의 ID와 PWD 입력 후, 본인을 인증한다.

Step 2. 보안카드/OTP로 2차 인증한다.

Step 3. 인증을 강화하기 위하여 공인인증서로 인증한다.

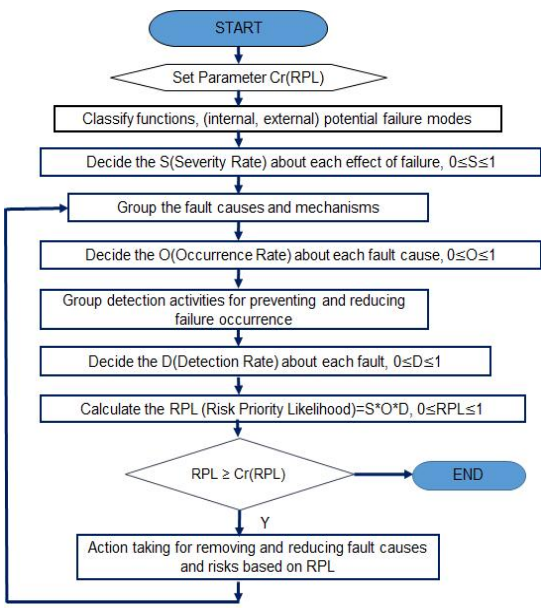

Fig 2. Flowchart of FMEA Process.

과거에는 사용자의 ID와 PWD 방식을 주로 사용하였지만, 최근에는 뱅킹 시스템의 보안을 강화하기 위하여 공인인증서, 보안카드, OTP(One Time Password) 및 생체 인증 방식을 도입하고 있는 상황이다. 아래 Table 3에서는 사용자 인증 단계에서 발생 할 수 있는 보안 취약점과 위험 요소들을 나타내고 있다[7-9,11].

3.2 접근 통제(Access Control)

접근 통제는 허가되지 않은 접근을 감시하고 차단하며, 접근을 요구하는 사용자를 식별하는 과정을 말한다. 아래 Table 4에서는 접근 통제를 위한 시스템인 운영체제, 미들웨어 그리고 하드웨어에서 발생할 수 있는 보안 취약점과 위험요소를 나타내며, 주로 비인가된 사용자의 접근과 악성 코드 및 악성웨어에 의한 위협이 주를 이루고 있다. 또한 이들이 진화하면서 그에 따른 피해 수준도 심각해지고 있다[9,10].

Table 3. Security Vulnerabilities and Risk Factors in User Authentication

Authentication Way	Security Vulnerability	Hazard Factors
ID/PWD	ID/PWD exposure, ID/PWD hacking, uninstalled Active X	PWD same as ID, Cellular Phone No, and Personal Info
Security Card	Leakage, robbery and loss of security card, leakage of security card image, uninstalled Active X	Numbers of security card, security card image
OTP	OTP hacking, OTP usage limitage, manipulated algorithm that makes OTP	OTP tokens and keys
Accredited Certificate	Accreditted Certificate leakage and robbery and loss	Private personal information
Biometrics (finger prints, iris, face, voice)	In case of being leaked, impossible to recover	Impossible to recognize accurately, inaccurate matching threshold values

Table 4. Security Vulnerabilities and Risk Factors in Access Control

Access Controls	Security Vulnerability	Hazard Factors
Operating System	Robberies of recorded file about customers, intrusions from open API environment	Open API, manipulated Mobile OS log information, malicious codes
Middleware	Managing DB file hacking, attempts of disapproved customers	Attempts to log on from outside
Hardware	Error of mobile device operation, unawareness of device instruction, losses of mobile devices	Malicious code and malwares

3.3 바이러스 탐지 및 통제(Virus Detection and Control)

모바일 뱅킹 정보보안시스템에서는 점점 악성 바이러스와 악성 소프트웨어의 영향을 받고 있고, 악성 바이러스와 악성 소프트웨어의 형태가 다양해지며 그 피해의 수준도 심각해지고 있다. 악성소프트웨어(Malware) 는 컴퓨터 및 모바일 디바이스에 설치되어 사용자 업무를 방해하거나 피해를 입히는 악성 소프트웨어를 말하고, 다양한 형태로 접근하여 사용자들에게 큰 피해를 주고 있다. 멀웨어의 종류로는 바이러스(Virus), 애드웨어(Adware), 스파이웨어(Spyware), 트로이목마(Trojan Horse), 스팸(Spam), 피싱(Phishing) 그리고 파밍(Pharming) 등이 해당되며, 이들의 침입 경로로는 웹사이트 방문, 소프트웨어 다운로드 및 설치, 무선 네트워크 연결 등이다. 금융 기관에서도 이에 대한 관심이 급격히 높아지면서 악성 위험요소를 해결하는 솔루션을 다양하게 제안하고 있다. 아래 Table 5에서는 침입경로인 웹사이트 방문, 모바일 기기 연결, SMS와 E-mail을 통한 애플리케이션 설치에서 발생할 수 있는 보안 취약점과 위험요소를 나타내고 있다. 앞으로는 점점 다양하고 치밀한 방법으로 사용자들에게 피해를 줄 것으로

Table 5. Security Vulnerabilities and Risk Factors in Virus Detection and Control

Access Controls	Security Vulnerability	Hazard Factors
Visits to web sites	Leakage of personal information, financial frauds	A lot of malicious codes, malicious softwares
Link between devices	Leakage of personal information, financial frauds	A lot of malicious codes, malicious softwares
Application installation through SMS, E-mails including installation routes	Leakage of private personal information,	Forged and manipulated application including malicious codes

예상된다.

4. 모바일 뱅킹시스템의 보안성 개선을 위한 FTA와 FMEA

사용자 인증 단계에서의 보안 취약점과 위험 요소를 바탕으로 한 FTA를 아래 Fig. 3에 나타나 있다. 결함은 크게 사람에 의한 오류, 하드웨어에 의한 오류, 소프트웨어 시스템에 의한 오류 이렇게 세 가지로 분류할 수 있다. 구체적으로, 사람에 의한 오류에서는 사용자에 의한 오류 그리고 보안팀에 의한 오류로 나누어지는데, 사용자에 의한 오류는 사용자의 실수 및 의도적인 행동인 ID/PWD 노출, 유출 그리고 Active X 미설치 등이 원인이 되고, 보안팀에 의한 오류는 크게 비인가된 해커들의 침입에 대한 대응 부족이 된다. 하드웨어에 의한 오류에서는 모바일 디바이스 오류와 보안 도구 및 기계들의 오류이다. 이들은 크게 디바이스에 존재하는 자체 결함이 원인이 된다. 마지막으로 소프트웨어 시스템에 의한 오류에서는 데이터베이스 오류와 모바일 애플리케이션 유지보수 시스템 오류이고, 이들은 주로 비인가된 해커들의 침입에 대한 대응 부족이 원인이 된다[4,7-9,11].

접근 통제 단계는 모바일 뱅킹시스템의 보안면에서 가장 중요한 부분이라 할 수 있어, 모바일 뱅킹시스템 내에 다양한 결함이 존재하고 그 결함들로 인하여 위협의 정도가 심각해지고 있다. 아래 Fig. 4에서는 접근 통제 단계에서의 결함을 사람에 의한 오류, 하드웨어에 의한 오류, 소프트웨어 시스템에 의한 오

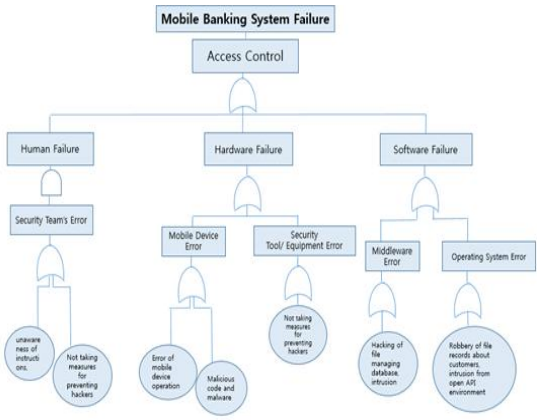

Fig. 4. FTA Diagram of Access Control.

류 이렇게 세 가지로 분류하여 나타내었다. FTA를 적용함으로써 모바일 뱅킹시스템에서 보안이 가장 취약한 부분의 결함 원인 규명을 간편히 할 수 있고, 보안성 중심 소프트웨어 시스템의 결함 원인을 알기 쉽게 분석하여 향후에 발생할 위험과 결함을 예방할 수 있을 것이다[4-5,9-11].

마지막으로 바이러스 탐지 및 통제 단계에서 가장 많은 위험 요소와 보안 취약점이 발생 할 수 있게 된다. 아래 Fig. 5에서는 바이러스 탐지 및 통제 단계에서의 결함을 경로에 따라 웹사이트 방문, 기기간의 연결, SMS 혹은 E-mail을 통한 애플리케이션 설치 이렇게 세 가지로 분류하여 나타내었다. 세 가지 모두 사용자에 의한 오류와 기기에 의한 오류로 나누어진다. 사용자에 의한 오류로는 사용자 실수로 인한 위험요소 설치 및 접근이 해당되며, 기기에 의한 오

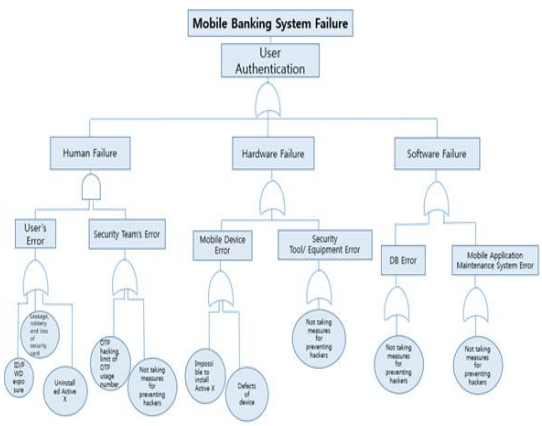

Fig 3. FTA Diagram of User Authentication.

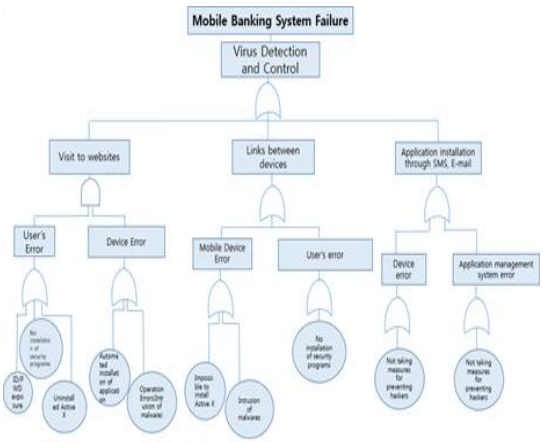

Fig. 5. FTA Diagram of Virus Detection and Control.

류로는 주로 보안프로그램 미설치 및 설치불가 그리고 바이러스 및 악성소프트웨어 침입에 대한 미대응이 해당이 된다[7-9,13].

Table 6에서는 향후 모바일 뱅킹시스템의 사용자 인증 단계, Table 7에서는 접근 통제 단계 그리고 마지막으로 Table 8에서는 바이러스 탐지 및 통제 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 나타내고, 이를 바탕으로 심각도, 발생도 그리고 검출도를 계산하여 위험우선가능성(RPL, Risk Priority Likelihood)를 계산한다. 모바일 뱅킹시스템의 고장과 연계된 특정한 원인에 대한 위험 요소를 추정하며 고장 발생 원인을 제거하기 위한 보안프로세스를 제안하고, 뱅킹시스템의 보안성을 개선하기 위해 조치 내용의 우선순위를 매김으로써 뱅킹 시스템의 안전성을 제고할 수 있도록 할 것이다. Table 6-8에서 측정된 심각도(S), 발생도(O) 그리고 검출도(D)를 사용하여 RPN 값을 계산하여 높은 RPN값을 갖는 위험 요소별로 고장 원인을 제거하기 위한 활동(Action Taking)을 수행하여 심각도(S), 발생도(O) 그리고 검출도(D)를 낮추고 보안성이 확보될 때까지 연속적인 고장 원인을 제거하기 위한 활동 (Action Taking)을 수행한다. 따라서 최근 정보기술의 발전에 따라 모바일 뱅킹 서 비스를 이용하는 고객들은 더 높은 수준의 보안성과 안전성을 갖춘 시스템을 요구하고 있기 때문에 FMEA 기법을 사용하여 잠재적인 결함을 예방하는 것이 필요하다[3,5,6,9,11-13].

5. 결 론

최근 모바일 뱅킹시스템의 등장으로 인한 편리함을 누리고 있는 반면에, 이에 따른 보안 위협 요소들도 발전되면서 뱅킹시스템 및 사용자들을 위협하고 있다. 이러한 문제로 인하여 안전성과 보안성을 갖춘 모바일 뱅킹시스템을 개발하고 생산하기 위하여 정확한 안전성 설계 및 예측을 통한 보안성 확보가 필수 불가결하다.

따라서 본 논문에서는 모바일 뱅킹시스템에서 보안이 가장 취약한 '사용자 인증'과 '접근 통제' 단계 그리고 '바이러스 탐지 및 통제' 단계에서의 보안 취약점과 위험요소를 작성하고 FTA 기법을 사용하여 결함 분석을 수행하였으며, 또한 FMEA 기법을 통해 위험 요소를 추정하고 위험우선순위를 매김으로써 향후 결함을 예방하는 목적으로 단계별 보안 프로세

Table 6. FMEA Sheet of User Authentication

Requirements		ID/PWD	Security Card	OTP	Accredited Certificate	Biometrics
Potential Failure Mode		ID and PIN No, PWD exposure, id and pwd hacking and uninstalled Active X	Leakage, robbery and loss of security card, leakage of security card image file, uninstalled Active X	OTP hacking, limit of OTP usage number, algorithm that makes OTP manipulation, uninstalled Active X	Leakage of certificate, robbery and loss of certificate	If it is leaked, it is impossible to restore
Potential Effects of Failure		Personal Information exposure	Personal Information exposure	Personal Information exposure	Personal Information exposure	It is impossible to restore
S (Severity)		0.7	0.8	0.9	0.9	1.0
Potential Cause of Failure		PWD same as ID, Cellular phone No, and personal Info	Numbers of security card, security card image file	OTP token and key	Personal information	Impossibility of accurate recognition, inaccurate matching threshold value
O (Occurrence)		0.9	0.8	0.7	0.8	0.6
Managing Process		Initialization of local devices, Apply virtual keyboard	Develop intensified OTP technologies, Use not fixed security card no.s	Take notice the management of OTP generator, IP Detection system	Institute complemented hardware security module	Authenticate with dual factors using various parts of body
D(Detection)		0.3	0.4	0.5	0.8	1.0
RPN (S*O*D)		0.189	0.256	0.315	0.576	0.600
1st Action Taken	S	0.7	0.8	0.9	0.9	1.0
	O	0.5	0.4	0.5	0.5	0.5
	D	0.4	0.4	0.4	0.5	0.8
	RPL	0.14	0.128	0.18	0.225	0.40

Table 7. FMEA Sheet of Access Control

Requirements		Operating System	Middleware	Hardware
Potential Failure Mode		Robbery of file records about customers; intrusion from open API environment	Hacking of file managing database; intrusion	Error of mobile device operation; unawareness of instructions, robbery, loss of devices
Potential Effects of Failure		Personal Information exposure	Personal Information exposure	Personal Information exposure
S (Severity)		0.9	0.1	0.7
Classification				
Potential Cause of Failure		PWD same as ID, Cellular phone No, and personal Info	Numbers of security card, security card image file	OTP token and key
O (Occurrence)		0.5	0.4	0.8
Managing Process		Initialization of local devices; Apply virtual keyboard	Develop intensified OTP technologies; Use not fixed security card no.s	Take notice the management of OTP generator; IP Detection system
D (Detection)		0.4	0.4	0.2
RPN (S*O*D)		0.18	0.16	0.112
1st Action Taken	S	0.9	0.1	0.7
	O	0.3	0.2	0.4
	D	0.3	0.3	0.2
	RPN	0.054	0.006	0.056

Table 8. FMEA Sheet of Virus Detection and Control

Requirements		Website visits	Link between devices	Application installation through SMS, E-mail
Potential Failure Mode		Leakage of personal information; financial frauds	Leakage of personal information; financial frauds	Leakage of personal information; financial frauds
Potential Effects of Failure		Personal Information exposure	Personal Information exposure	Personal Information exposure
S (Severity)		0.7	0.9	0.1
Classification				
Potential Cause of Failure		Malicious code and malicious software	Malicious code and malicious software	Malicious code and malicious software
O (Occurrence)		0.4	0.7	0.8
Managing Process		Update vaccine program; IP detection system	Update vaccine program; Installation of security program	Update vaccine program; IP Detection system
D (Detection)		0.7	0.9	0.5
RPN (S*O*D)		0.196	0.567	0.40
1st Action Taken	S	0.7	0.9	0.1
	O	0.2	0.4	0.4
	D	0.4	0.4	0.4
	RPN	0.056	0.144	0.016

스를 제안하였다. 머지않아 더욱 더 고도화된 기술의 등장으로 뱅킹 시스템 보안을 위협하여 피해를 입는 사례가 증가할 것으로 보인다. 앞으로는 이에 대비하여 뱅킹 시스템의 위험요소와 보안 취약점을 분석기법을 다양하게 개발하여 뱅킹 시스템의 보안성과 안전성을 증진시킬 수 있는 연구가 이루어져야 할 것이다.

REFERENCE

[1] H.G. Shin, "Year 2013 Predictive Analysis of Information Security Trends in Banking IT," *Journal of Payment Settlement and IT,* Vol. 51, pp. 581-586, 2013.

[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] 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.

[4] 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.

[5] M.H. Kim, E.J. Jin, and M.G. Park, "Fault Tree Analysis and Fault Modes and Effect Analysis for Security Evaluation of IC Card Payment Systems," *Journal of the Korean Multimedia Society*, Vol. 16, No. 1, pp. 87-99, 2013.

[6] Ubiquitous Management Academy Consulting, http://consulting.u-mac.co.kr/pds/quality/list.asp?sch_head=m_title&sch_string=fmea (accessed on April., 1, 2015).

[7] 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.

[8] 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.

[9] S.Y. Kim, M.H. Kim, and M.G. Park, "A Study on the Information Security Control and Management Process in Mobile Banking System," *Journal of the Korean Multimedia Society,* Vol. 18, No. 2, pp. 218-232, 2015.

[10] 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.

[11] 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.

[12] White Paper of FIS Consulting Services, http://www.fisglobal.com/ucmprd-pub/groups/public/documents/document/c028786.pdf (accessed on April, 1, 2015).

[13] 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.

김 소 영

부경대학교 공과대학 IT융합응용공학과(공학사)
부경대학교 대학원 정보시스템학과(공학석사 취득예정)
관심분야 : 소프트웨어 보안성 공학, 소프트웨어 안전성 공학, 비즈니스 프로세스 리엔지니어링, 빅데이터 분석기술

김 명 희

부경대학교 대학원 전자계산학과(이학석사)
부경대학교 대학원 정보시스템학과(공학박사)
University of Colorado-Denver, Dept. of Computer Science and Engineering (Post Doc.)
2004년～2007년 정부간 국제기구 CPSC (콜롬보플랜 기술 교육대학), Assistant Faculty 및 정보기술 및 통신학처장
2011년～2012년 부경대학교 교육대학원 전자계산교육전공 강의전담교수
2012년～2013년 University of Colorado-Denver, Dept. of Computer Science and Engineering, Lecturer
관심분야 : 소프트웨어 공학 및 재공학, 멀티미디어 정보처리기술, 네트워크성능평가, e-Learning and u-Learning

박 만 곤

경북대학교 수학교육(이학사)
경북대학교 전산통계학(이학박사)
Philippine Women's University (국제행정학석사)
University of Rizal System, Philippines(명예 기술학박사)
Dept. of Electrical and Computer Engineering, University of Kansas (Post Doc.)
1981년～현재 부경대학교 IT융합응용공학과 교수
1997년～현재 한국멀티미디어학회(KMMS), 초대 총무이사, 수석부회장, 회장 및 명예회장
2002년～2007년 정부간 국제기구 CPSC (콜롬보플랜기술교육대학) 총재 (Director General and CEO)
2004년～2007년 Asia-Pacific Accreditation and Certification Commission (아태지역 인증 및 검증위원회) 위원장
2005년～2007년 유네스코 (UNESCO-UNEVOC) 자문위원, 아시아개발은행(ADB) 자문관
관심분야 : 소프트웨어 공학 및 재공학, 소프트웨어 신뢰성공학, 소프트웨어 안전성 공학, 비즈니스 프로세스 재공학 (BPR), 멀티미디어정보처리기술, 정보시스템 성능평가 기법 및 도구, ICT- based HRD System