creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:21031-000002233583

공 학 석 사 학 위 논 문

모바일 뱅킹 시스템의 소프트웨어 보안성 개선을 위한 고장 트리 분석과 고장 유형 영향 분석에 관한 연구

PUKYONG NATIONAL UNIVERSITY 부경대학교

2016년 2월

부 경 대 학 교 대 학 원

정보시스템협동과정

김 소 영

공 학 석 사 학 위 논 문

모바일 뱅킹 시스템의 소프트웨어 보안성 개선을 위한 고장 트리 분석과 고장 유형 영향 분석에 관한 연구

지도교수 박 만 곤

이 논문을 공학석사 학위논문으로 제출함.

2016년 2월

부 경 대 학 교 대 학 원

정보시스템협동과정

김 소 영

김소영의 공학석사 학위논문을 인준함.

2016년 2월 26일

위 원 장 이학박사 이 경 현 (인)

위 원 공학박사 김 창 수 (인)

위 원 이학박사 박 만 곤 (인)

목 차

표 차례 ····· iii

그림 차례 ····· iv

ABSTRACT ····· v

1. 서론 ····· 1

1.1 연구의 배경 및 목적 ····· 1

1.2 연구의 내용 ····· 5

2. 관련 연구 ····· 6

2.1 모바일 뱅킹 시스템 ····· 8

2.2 모바일 뱅킹 시스템의 위험과 취약성 ····· 10

2.3 모바일 뱅킹 시스템의 소프트웨어 보안성 개선을 위한 결함 트리 분석(FTA)과 고장 모드 영향 분석(FMEA) ····· 12

3. 모바일 뱅킹 시스템의 정보 보안 통제 및 관리 프로세스 설계 ····· 18

3.1 모바일 뱅킹 시스템의 결함 메커니즘과 위험요소 분석 ····· 18

가. 사용자 인증 ····· 19

나. 접근 통제 ····· 22

다. 바이러스 탐지 및 통제 ····· 24

라. 네트워크 시스템 ····· 25

4. 모바일 뱅킹 시스템의 보안성 개선을 위한 결함 트리 분석(FTA)과 고장 유형 영향 분석(FMEA) ····· 28

4.1 모바일 뱅킹 시스템의 보안성 개선을 위한 결함 트리 분석 (Fault Tree Analysis) 적용 ····· 28

가. “사용자 인증” 단계에서의 FTA 적용 ····· 28

나. “접근 통제” 단계에서의 FTA 적용 ····· 30

다. “바이러스 탐지 및 통제” 단계에서의 FTA 적용 ····· 31

라. “네트워크 시스템” 단계에서의 FTA 적용 ····· 33

4.2 모바일 뱅킹 시스템의 보안성 개선을 위한 고장 유형 영향 분석 (Failure Modes and Effects Analysis) 적용 ····· 35

가. “사용자 인증” 단계에서의 FMEA 적용 ····· 35

나. “접근 통제” 단계에서의 FMEA 적용 ····· 37

다. “바이러스 탐지 및 통제” 단계에서의 FMEA 적용 ····· 39

라. “네트워크 시스템” 단계에서의 FMEA 적용 ····· 40

5. 결론 ····· 43

5.1 결론 ····· 43

5.2 향후 과제 ····· 45

참고문헌 ····· 46

Acknowledgement ····· 50

표 차례

<표 1> 모바일 뱅킹 등록 고객 수 ····· 2

<표 2> 모바일 뱅킹 서비스 이용실적 ····· 3

<표 3> 전자 금융 사기로 인한 피해 금액 ····· 4

<표 4> 모바일 뱅킹 내의 보안 위협 ····· 11

<표 5> 결함 트리 작성 시 사용되는 결함 트리의 기호 ····· 13

<표 6> FMEA 시트 ····· 15

<표 7> “사용자 인증” 단계 ····· 21

<표 8> “접근 통제” 단계 ····· 23

<표 9> “바이러스 탐지 및 통제” 단계 ····· 24

<표 10> “네트워크 시스템” 단계 ····· 26

<표 11> “사용자 인증” 단계의 FMEA ····· 36

<표 12> “접근 통제” 단계의 FMEA ····· 38

<표 13> “바이러스 탐지 및 통제” 단계의 FMEA ····· 39

<표 14> “네트워크 시스템” 단계의 FMEA ····· 41

그림 차례

<그림 1> 스마트폰 악성코드 수 ····· 4
<그림 2> 정보 보안 통제 및 거버넌스 프로세스 ····· 7
<그림 3> 모바일 뱅킹 시스템 구성도 ····· 8
<그림 4> 안드로이드 멀웨어의 증가 ····· 10
<그림 5> FT(Fault Tree)의 구조 ····· 14
<그림 6> FMEA 수행 알고리즘 ····· 16
<그림 7> 정보 시스템의 보안 결함 해결 프로세스 ····· 19
<그림 8> 사용자 인증(User Authentication) 단계 ····· 20
<그림 9> 사용자 인증 단계의 FTA 적용 ····· 29
<그림 10> 접근 통제 단계의 FTA 적용 ····· 30
<그림 11> 바이러스 탐지 및 통제 단계의 FTA 적용 ····· 32
<그림 12> 네트워크 시스템 단계의 FTA 적용 ····· 34

A Study on the Information Management Process and FTA, FMEA for Software Security of Mobile Banking System

Kim So Young

Department of Information Systems, Graduate School,
Pukyong National University

Abstract

As the information technologies and mobile communication technologies has developed, the use of internet and mobile banking is still increasing drastically. Especially, due to the convenience of mobile banking system which users can use anytime, anywhere, mobile banking service has become a major service on banking information systems. However, mobile banking system has been exposed to various security threats and risk factors. It is very important to improve the security of mobile banking systems. In this paper, first, we analyze risk factors and security vulnerabilities and suppose improved mobile banking security management process on the most important stages of mobile banking process. Second, we accomplish the analysis of FTA and FMEA for improving the security of mobile banking system. Hence, we can propose more improved, secure mobile banking system to users and prevent a lot of security threats regularly.

1. 서론

1.1 연구의 배경 및 목적

최근 정보기술의 발전과 모바일 디바이스의 발전으로 인해 언제 어디서나 모바일 단말기를 이용한 모바일 뱅킹 업무가 가능해지며 사용자들에게 편리함을 제공해주고 있다. 모바일 뱅킹은 무선과 온라인 그리고 뱅킹 서비스를 합한 개념으로써, 새로운 뱅킹 서비스로 자리 잡으며 많은 사용자들이 이용하고 있다. 표 1에서와 같이 모바일 뱅킹 이용자수가 급격하게 확대되고 있고, 앞으로는 더욱 더 모바일 디바이스를 기반으로 하는 모바일 뱅킹의 이용이 증가할 것으로 예상한다.[1][5]

그 중 IT 기술의 발달로 기존 오프라인 서비스가 모바일 서비스로 확대되면서 모바일 서비스의 형태도 다양하게 변화하게 되었다. 처음 2003년에 등장하게 된 IC칩 기반 모바일 뱅킹 서비스는 은행에서 발급을 받아 보안이 강화된 저장 기기로써 사용이 되고, 이 칩에는 은행 거래를 위해 쓰이는 사용자 계좌 정보와 같은 필수적인 정보가 저장이 된다. 그 다음으로 2007년에 등장하게 된 VM기반 모바일 뱅킹 서비스는 모바일 기기 내의 계좌를 이체하는 등의 거래서비스 기능을 가진 소프트웨어만을 사용한다는 점에서 IC칩 기반과는 다르다. 그리고 VM기반 모바일 뱅킹 서비스는 오직 모바일 뱅킹을 위해 생성된 'WIPI'와 같은 미들웨어를 사용하고, 공인인증서를 통해서 사용자를 인증할 뿐 아니라 보안카드와 같은 인증수단을 사용하여 사용자의 보안을 강화한다. 마지막으로 가장 많이 사용되는 모바일 디바이스 기반 모바일 뱅킹 서비스는 모바일 디바이스 내에 IOS나 안드로

이드 운영체제에 따라 구비된 모바일 뱅킹 어플리케이션을 이용하게 되며, 일반적인 뱅킹 서비스와 같은 수준의 뱅킹 서비스를 사용자들에게 제공하고 있다. 아래 표 1에서는 연도별로 모바일 뱅킹 서비스 형태에 따른 증가 추세를 보여주고 있다.[5]

[표 1] 모바일 뱅킹 등록 고객 수

	2010	2011	2012	2013
IC Chip	4,579	4,434	4,376	4,328
VM	8,561	8,946	8,749	8,421
Mobile Devices	2,609 (16.6%)	10,358 (43.6%)	23,966 (64.6%)	37,185 (74.5%)
Total	15,748	23,737	37,092	49,934

다음의 [표 2]는 한국은행이 발표한 최근 3년간의 모바일 뱅킹 이용서비스 현황을 보여주고 있다. 이와 같이 모바일 뱅킹 서비스 이용이 꾸준하게 증가하는 추세이다. 2012년 마지막 4분기에는 모바일 뱅킹 이용건수가 15,346 천건 그리고 스마트폰을 기반으로 한 이용건수는 15,017 천건을 나타내고 있다. 2013년에는 이용건수가 24,462 천건으로 작년에 비해 약 1.6배 증가한 것으로 나타난다. 마지막으로 2014년도에는 이용건수가 27,597 천건으로 2012년도에 비해 약 1.8배 증가한 것으로 기록되었다. 또한 이용금액도 마찬가지로 꾸준히 증가하는 것으로 나타나었다.

[표 2] 모바일뱅킹 서비스 이용실적

(천건, 십억원, %)

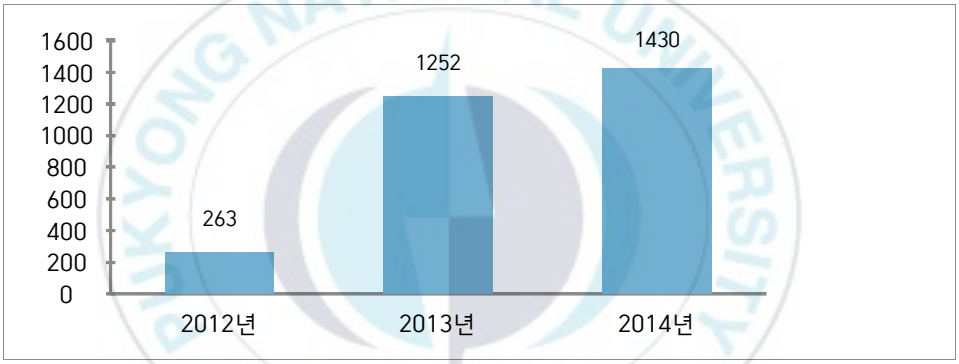
출처: 한국은행 (Bank of Korea)

	2012	2013	2014
이용건수	15,346 (15.4)	24,462 (9.7)	27,597 (12.8)
스마트폰기반	15,017 (17.1)	23,910 (7.5)	27,369 (14.5)
이용금액	1,134.0 (16.5)	1,573.2 (10.9)	1,663.4 (5.7)
스마트폰기반	1,071.9 (20.3)	1,525.2 (11.1)	1,627.6 (6.7)

그러나 모바일 뱅킹의 언제 어디서나 이용할 수 있다는 편리함 이면에는 다양한 형태의 보안위협과 보안취약점이 존재하여 사용자들을 위협하면서 개인정보 유출 및 금전적 피해를 일으키고 있다. 이에 따라 뱅킹 정보시스템이 등장하게 되어 보안성(Security)이 중요한 이슈로 떠오르고 있다. 아래의 [그림 1]은 2012년부터 2014년까지의 스마트폰 악성코드의 유입 수를 나타내고 있다. 2014년도는 약 1,430,246 건을 기록하며 2012년도에 대비하여 약 444%가 증가하였고, 2013년도에 대비하여 약 14.2%가 증가한 것으로 나타나었다. 또한 아래 [표 3]은 전자금융사기로 인한 피해금액을 사기형태별로 나타내고 있다. 최근 5년 동안 약 12만 건이 발생했으며 그 피해액만 4천억 원에 이르고, 보이스 피싱 피해는 해마다 줄고 있지만 피해액은 3천 7백억 원으로 피해규모는 점점 심각해지고 있는 상황이다. 신종 전자금융사기인 파밍, 스미싱, 메모리해킹 등은 최근 2년간 피해액이 약 30억 원 정도로 보이스 피싱에 비해 적지만, 발생건수가 매년 급격하게 증가하

고 있어 사용자들의 피해가 심각한 수준에 이르고 있어 대책이 시급하다. 이와 같이 심각해지고 있는 피해에 대처하고 뱅킹 시스템의 보안성을 개선하기 위하여 모바일 뱅킹 정보시스템의 보안위험요소와 보안 취약점을 도출해내어 보안 위협에 대한 대응을 하는 것이 중요하다. 따라서 본 논문에서는 모바일 뱅킹 프로세스 중 가장 보안성이 취약한 단계들에서 보안 취약점과 위험요소들을 파악하여 개선된 정보보안프로세스를 제안하고, 결함트리 분석과 고장 유형 영향 분석을 수행하여 모바일 뱅킹 정보시스템의 보안성을 개선할 수 있는 방법을 제안한다.[2][3][4]

(단위: 천 건)



[그림 2] 스마트폰 악성코드 수
출처 : Ahnlab Threat Research & Response Blog

[표 3] 전자 금융 사기로 인한 피해 금액
출처 : 경찰청 및 전화결제산업협회

	보이스피싱	파밍	스미싱	메모리해킹	총계
2012	59,500	-	-	-	59,500
2013	55,300	16,424	4,807	2,762	79,293
2014	36,900	6,842	276	522	44,540
합계	371,100	23,266	5,083	3,284	402,733

(단위 : 건/백 만원)

1.2 연구의 내용

모바일 디바이스를 이용하여 언제 어디서나 뱅킹 서비스를 제공해주는 모바일 뱅킹 시스템의 이용이 급격이 증가하고 있지만, 이러한 편리함 이면에는 모바일 뱅킹 시스템 내에 존재하는 다양한 보안 위협 및 위험 요소로 인한 금융사기 범죄 피해 수준이 심각해지고 있다. 이에 따라 보안성을 확보하고 개선하는 문제가 시급한 상황이다. 본 논문에서는 모바일 뱅킹 시스템의 보안성을 확보하고 개선하기 위하여 현 모바일 뱅킹 시스템의 보안 취약점과 위험요소들을 도출하여 분석해내고, 개선된 모바일 뱅킹 보안 프로세스를 제안하여 사용자들에게 안전한 모바일 뱅킹 서비스를 제공할 수 있도록 할 것이다.

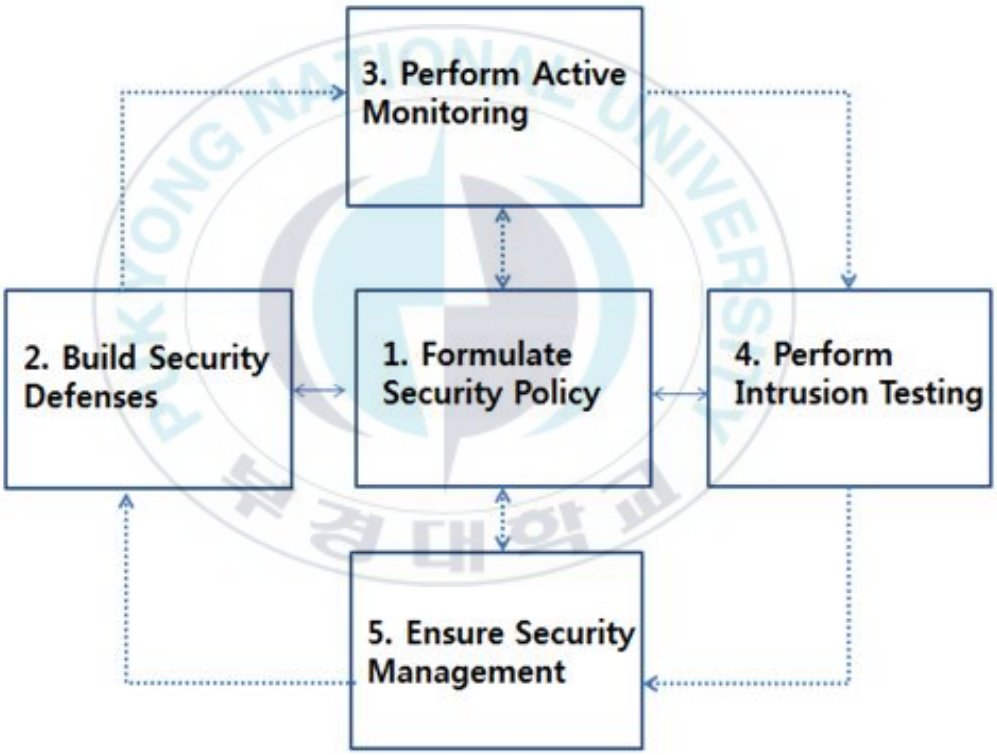
이를 위해 (1) 현 모바일 뱅킹 시스템의 모바일 뱅킹 프로세스 중 가장 보안성이 취약한 단계들에서 보안 취약점과 위험요소들을 분석하고, 보안성이 개선된 정보보안프로세스를 작성하고, (2) 이를 바탕으로 결함 트리 분석(FTA)과 고장 유형 영향 분석(FMEA)를 수행하여 모바일 뱅킹 시스템의 보안성을 개선할 수 있도록 한다. 결과적으로 (3)이를 통해 보안성이 개선된 향후 모바일 뱅킹 시스템이 갖추어야 할 사항을 제안한다.

2. 관련 연구

정보보안(Information Security)은 승인 및 허가되지 않은 접근으로부터 정보와 정보시스템을 보호하는 것을 말하고, 뱅킹 시스템 내에서의 보안성(Security)은 무결성(Integrity), 가용성(Availability), 기밀성(Confidentiality)등을 가짐으로써 보안성이 향상된다. 뱅킹 시스템의 정보 보안을 위해서는 정보 보안 통제 및 관리가 필수적이며, 구체적으로 정보 보안 통제와 관리는 정보의 가용성, 기밀성, 무결성과 관계된 위험요소를 관리하고 제어하는 과정을 뜻한다. 뱅킹 시스템 내의 정보 보안 통제 및 관리의 목적은 가장 중요한 기밀 정보 및 자산을 외부의 접근으로부터 보호하는 것이다. 그러나, 정보 보안 통제 및 관리의 결여로 인해 야기되는 주요 위험요소들로는 첫 번째, 정보 보안의 인프라 구조와 그 구성 요소의 파괴가 발생하게 된다. 두 번째, 미흡한 직원교육 및 도구의 미숙지로 인한 인적실패요소가 된다. 세 번째, 해커나 악성 바이러스와 같은 뱅킹 정보시스템에 가해지는 외부적인 공격이 된다.[3][4][5]

정보 보안 통제에는 세 가지 유형으로 분류되는데, 먼저 물리적 통제이다. 물리적 통제는 비허가된 접근으로부터 내부 시스템을 안전하게 보호하는 것이다. 예로는 파일 백업, 보안 경비시스템 가동 등을 말한다.
두 번째로, 정보 보안 통제의 핵심 부분인 기술적 통제이다. 기술적 통제는 컴퓨터 하드웨어 및 소프트웨어 등의 기술을 이용하여 정보 시스템을 보호하게 된다. 예로는, 접근 제어, 안티바이러스 소프트웨어 그리고 암호화 기술 등이 해당된다. 마지막으로는, 행정적 통제로 정보 시스템의 관리 제약, 수행 절차 및 보안 정책 등을 말한다. 이는 정보 시스템에 접근할 수 있는

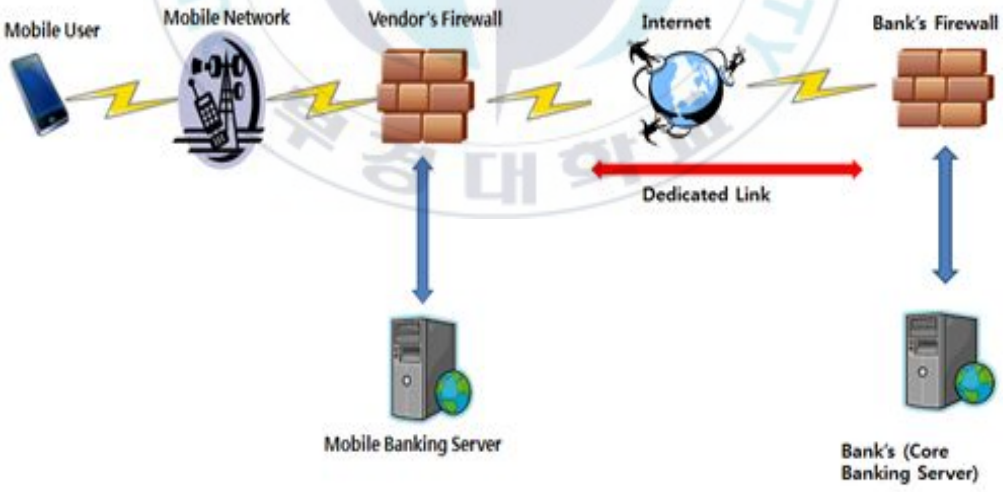
모든 사용자가 승인 및 허가를 받을 수 있도록 하는 것이 목표이다. 예로는, 시스템에 접근하는 사용자의 행동을 제어하는 사용자 중심 기술들인 보안 인식과 기술 트레이닝 등이 해당된다. 아래 [그림 2]에서는 일반적인 정보 보안 통제와 관리프로세스를 도식화하여 나타낸 것으로, 이를 통해 사용자들이 보안성이 개선된 뱅킹 시스템을 안전하게 사용할 수 있을 것이다.[1][4][5]



[그림 3] 정보 보안 통제 및 거버넌스 프로세스

2.1 모바일 뱅킹 시스템

모바일 뱅킹은 사용자들이 스마트폰, PDA와 같은 모바일 디바이스를 수단으로 이동통신사의 무선 인터넷을 이용하여 금융기관의 모바일 뱅킹 시스템과 연결하여 금융서비스를 이용할 수 있는 전자금융 서비스를 말한다. 모바일 뱅킹 서비스의 핵심인 모바일 뱅킹 시스템은 무선 네트워크를 이용하여 뱅킹 서비스를 처리하는 시스템을 말하며, 무선 네트워크를 사용할 수 있는 곳에서 다양한 전자금융서비스를 편리하게 사용할 수 있게 되었다. 각 은행별로 독자적인 혹은 공동 운영 및 개발을 통하여 모바일 뱅킹 시스템을 운영하고 있다. 아래 [그림 3]은 모바일 뱅킹 아키텍처를 설명하고 있다.



[그림 4] 모바일 뱅킹 시스템 구성도

먼저, 뱅킹 서비스를 하기 위해서는 웹 서버와 어플리케이션 서버와 데이터베이스를 설치하게 된다. 뱅킹 서비스를 사용하기 위하여 고객들은 모바일 네트워크를 구비한 모바일 기기를 사용하여야 하고, 금융 거래를 처리하기 위해 각 은행의 중앙시스템과 연결되어야만 한다.

모바일 디바이스를 이용한 모바일 뱅킹 서비스 구성 방식으로는 웹 방식, 어플리케이션 방식 그리고 웹-어플리케이션 방식이며, 주로 국내 금융기관에서는 대부분 어플리케이션 또는 웹-어플리케이션 방식을 채택하여 사용하고 있다. 뱅킹 서비스를 처리하기 위한 모바일 뱅킹 프로세스는 아래와 같다.[3][12]

- 사용자 인증 : 모바일 네트워크 상에서 사용자와 금융기관의 연결은 Pubilc/ Private키를 이용하여 암호화 되며, 모바일 뱅킹 시스템 서버는 사용자에게 인증을 요청하고, 사용자는 인적 사항들을 등록하게 된다. 그 다음으로 모바일 뱅킹 사용자는 인증을 받게 되고 모든 개인 정보들이 금융 기관으로 넘어가서 사용자를 최종 인증하고, 마지막으로 모바일 뱅킹 시스템 서버가 사용자들에게 필요로 하는 데이터들을 제공하게 된다.
- 사용자의 거래 요구 : 먼저, 사용자가 원하는 뱅킹 서비스를 선택하고, 서버는 뱅킹 서비스의 보안 강화를 위해 재인증을 요구하게 된다. 모바일 뱅킹 서버상에서의 재인증 단계는 뱅킹 서비스가 인증되었음을 보장하는 것을 목표로 한다.
- 금융 기관의 뱅킹 서비스 처리 : 금융 기관의 서버는 사용자가 요구한 뱅킹 서비스를 최종적으로 처리하게 된다.

2.2 모바일 뱅킹 시스템의 위험과 취약성

모바일 뱅킹 서비스가 널리 보급됨에 따라 뱅킹 보안 시스템도 취약해지고 따라서 사용자는 보안 위협에 쉽게 노출되어 개인정보노출, 신형 사기 등의 피해를 입고 있다. 사용자들의 대부분이 소지하고 있는 모바일 기기에서의 주요 위험요소로는 악성 소프트웨어(Malware), 보안 정책 위반, 취약한 무선 네트워크 구조, 취약한 지불 시스템 구조, SMS, 보안 수준이 약한 하드웨어 및 운영체제 등이 해당된다. 또한, [그림 4]에서는 모바일 뱅킹 시 모바일 디바이스 내의 운영 체제인 안드로이드 내에서 보안 위협 요소인 악성 소프트웨어(Malware)의 수가 2011년에 비해 2012년도에 급격하게 증가하는 것을 보여주며 모바일 뱅킹 시스템의 보안 위협 심각성을 보여주고 있다.[6][12][13][14]

[그림 5] 안드로이드 멀웨어의 증가
출처 : Kaspersky Security Bulletin 2012 Malware Evolution

모바일 디바이스 내의 보안위협형태는 공격 유형에 따라서 [표 4]와 같이 첫 번째는 모바일 디바이스 시스템 위협, 두 번째로 사용자 정보 위협, 세 번째로 악성코드 및 악성 소프트웨어(Malware) 위협, 네 번째로 네트워크 전송 위협 그리고 마지막으로 물리적 위협으로 나뉘어진다.[14][15]

[표 4] 모바일 뱅킹 내의 보안 위협

보안 위협 유형	보안 위협 요소
모바일 디바이스 시스템 위협	모바일 기기 시스템 위협 중 ▪ 플랫폼 변조가 됨에 따라 타 어플리케이션 프로세스와 메모리에 손쉽게 접근하거나 악성코드의 침투 그리고 기밀 정보 노출 등의 위협에 노출될 수 있다. ▪ 변조된 어플리케이션은 사용자의 개인 금융 정보가 외부에 의해 전송되어 노출될 수 있다. ▪ 인가되지 않은 파일 시스템의 접근은 관리자 권한을 획득한 후 파일정보에 접근하여 공인 인증서 파일 정보, 응용프로그램 파일 등이 노출될 수 있다. (예) MADDEN NFL 12로 위장한 악성 어플리케이션- 어플리케이션을 깔면 추가로 생성된 어플리케이션이 SMS발송하여 과금이 발생한다.
사용자 정보 위협	사용자 정보 위협 중 ▪ 사용자 시스템 내 메모리 중요 정보 노출은 타 프로세스 접근이 가능해져서 중요 정보가 저장된 메모리에 대한 위협이 발생할 수 있다. ▪ 사용자 정보 노출은 기법을 이용하여 입력 정보를 수집한 후 네트워크를 통해 전송되거나 모바일 디바이스에 저장되어 입력 기록을 알 수 있다. (예) 2013년 3월 10일, 국민연금 미납금 사칭한 악성 어플리케이션- 스마트폰에 있는 공인인증서, 사진, 메모 폴더 접근하여 압축시켜 원격지로 전송된다.
악성코드 및 악성 소프트웨어 (Malware) 위협	악성코드 및 악성 소프트웨어(Malware) 위협에서는 디바이스 간의 연결, e-mail과 SMS의 경로를 통해 위협 요소가 침투될 수 있다. 종류로는 악성 코드 및 악성 소프트웨어(Malware) 유포, 피싱, 파밍 그리고 스니핑 공격 등이 있다. (예) 스마트폰 소액 결제 노린 악성코드 체스트- 개인정보를 탈취하여 피해자에게 주기적으로 소액결제를 하도록 유도한다.
네트워크 통신 위협	네트워크 통신 위협에서는 전송되는 평문 형태의 기밀정보를 툴을 이용해서 수집하면 개인 정보를 얻을 수 있다. 또, 보안이 취약한 무선망을 이용하게 되면 모바

	일 DDOS와 같은 치명적인 공격을 받아 외부에서 침입하여 정보를 수집해 가게 된다. (예) 2014년 금융기관과 언론기관을 공격한 3.20대란- 대규모 악성코드 공격으로 금융권과 방송사의 전산망을 마비시켜 수많은 국민의 개인정보가 유출되었다.
물리적 위협	물리적 위협에서는 모바일 디바이스가 휴대성을 가지는 특성 때문에 다른 사람으로부터의 접근이 쉬워 도난과 분실로 사고가 이어지게 되고, 또 이동식 저장매체(USB)로 인한 감염도 발생한다. (예) 2008년 미국 아칸소 주의 맥도날드 직원이 어느 남성의 분실된 휴대폰에 저장된 부인 누드 사진을 인터넷상에 유포하였다.

위와 같은 보안 위협 형태에 따라서 한층 강화된 정보 보안 통제 및 관리를 시행함으로써 뱅킹 시스템의 보안성을 향상해야 할 것이다.

2.3 모바일 뱅킹 시스템의 소프트웨어 보안성 개선을 위한 FTA와 FMEA

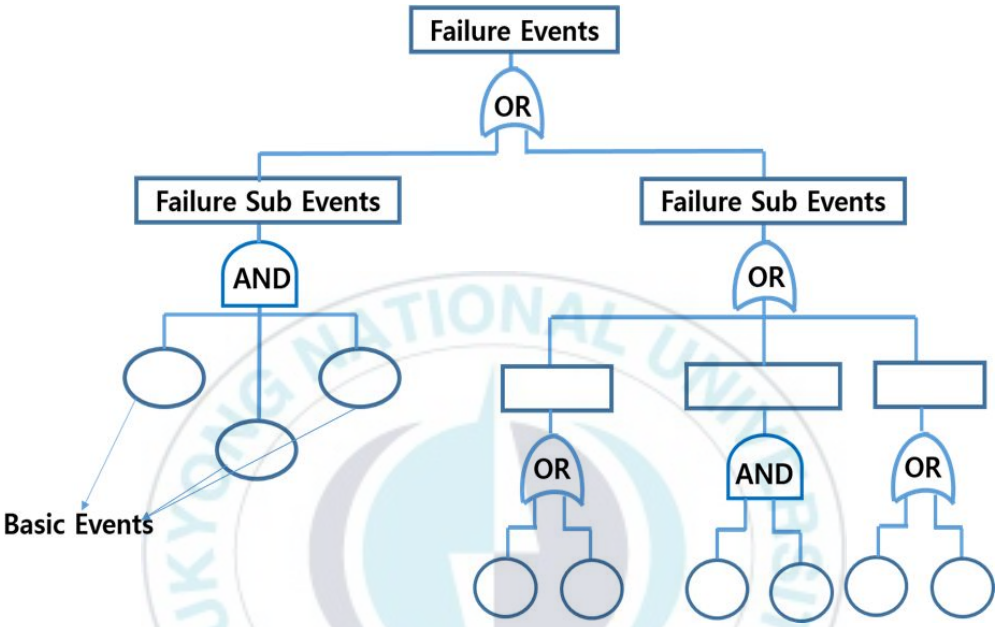
뱅킹 시스템과 같이 보안성(Security)을 중요시하는 정보시스템은 시스템 내에 존재하는 결함이나 취약점을 찾아내어 분석하는 일이 제일 우선시되어야 한다. 정보 시스템 내에 존재하는 결함은 하드웨어의 결함(시스템 설계 상의 실수, 부품의 오류, 하드웨어 자체 결함), 소프트웨어의 결함(분석 및 시스템 설계 오류, 코딩 오류, 구현상의 실수)과 마지막 운영인력(Operation Team)에서 발생할 수 있으며 그에 따른 시스템에 대한 통제도 하드웨어, 소프트웨어 및 운영인력을 중심으로 수행된다. 이를 위해서 현재 많은 분석기법들이 사용되고 있는데, 그 중에서 결함 트리 분석(FTA,

Fault Tree Analysis)은 결함원인들을 식별하고, 식별된 결함원인들을 분석하여 Fault Tree(FT)를 작성하고 이를 기반으로 하여 구성된 Fault Tree에서 정상사상이나 중간사상의 발생 확률들을 계산 하여 정보 시스템의 안전성 및 신뢰성을 분석하고 평가하는 도구로 사용되고 있다. 또한 FTA는 까다로운 정보 시스템에서 각 영역들의 위험요소들을 식별하기 위해서 정성적 및 정량적인 방법 모두에 사용될 수 있다. FTA의 결과물은 결함 원인들과 위험요소들을 나타내는 논리적 도식 표현의 결함 트리 다이어그램으로 나타난다. 결함 트리(FT)에 사용되는 기호는 아래 [표 5]와 같이 나타난다.[9][10][11]

[표 5] 결함 트리 작성 시 사용되는 결함 트리의 기호

기호		내용
	사상(Event)	보통 결함사상을 표시
	기본 사상 (Basic Event)	기본적 사상, 논리기호의 입력
	부전개 사상 (Undeveloped event)	데이터 부족에 의한 생략현상을 나타냄
	전입(In)	동일한 결함 트리 속에서 내용이 상이한 다른 부분과의—사이에 전이를 나타내는 기호. 삼각형의 상부선은 다른 부분에서의 전입을 의미하고, 삼각형의 측면선은 다른 부분으로 전출함을 의미한다.
	전출(Out)	
	AND Gate	하위의 사건을 모두 만족하는 경우에 사용하는 논리 게이트
	OR Gate	하위의 사건 중 하나라도 만족하면 사용하는 논리 게이트

결함 트리 기호들을 사용하여 결함 트리(FT)를 아래 [그림 5]와 같이 작성하게 된다.



[그림 5] FT(Fault Tree)의 구조

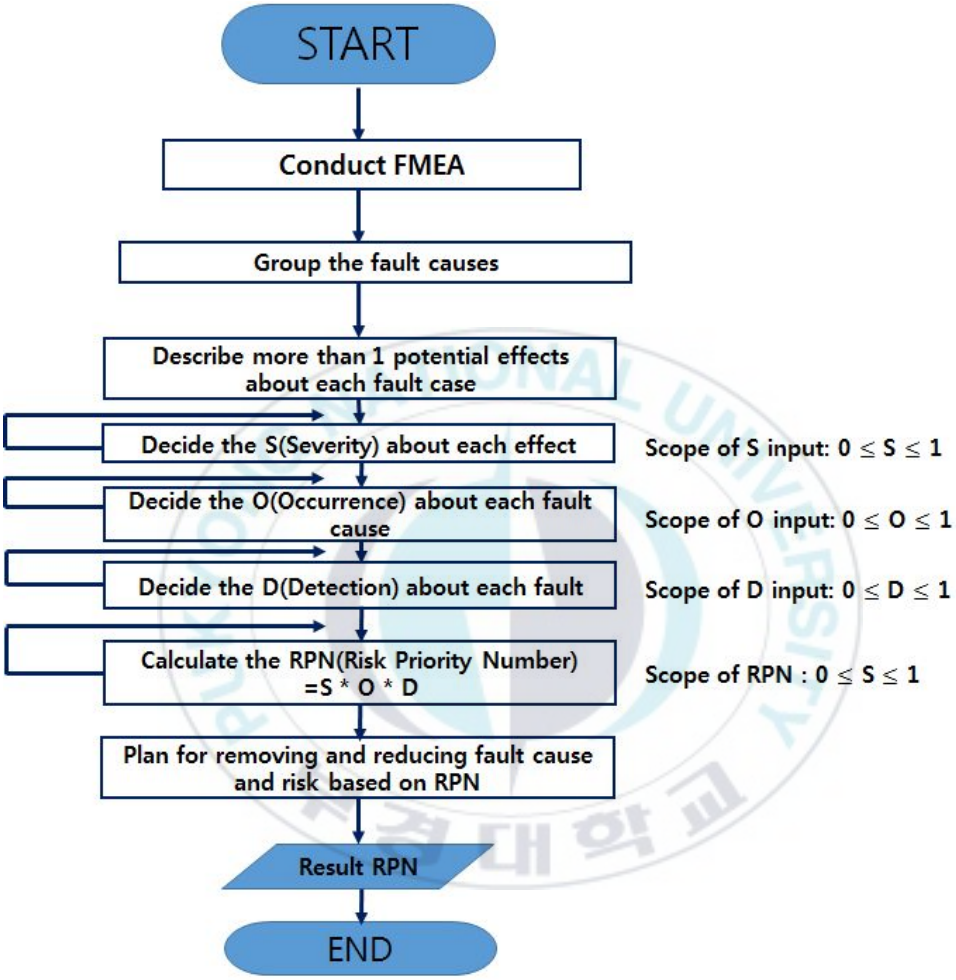
그 다음으로, 고장 유형 영향 분석(FMEA, Failure Modes and Effects Analysis)은 시스템의 잠재적 고장 모드를 발견하고, 시스템의 운영 중에 잦은 고장들이 발생하였을 경우에 임무 수행이 미치는 영향을 조사하여 평가하고, 영향이 큰 고장 모드들에 대하여 적절한 대책과 관리 방안을 세워서 향후에 발생할 수 있는 고장들을 미연에 방지하는 방법을 말한다. 시스템 내에서 발생할 수 있는 예상 결함 빈도, 결함의 영향도, 피해 수준 정도에 관하여 FMEA 시트를 작성하여 평가하며 보안 중요 정보시스템의 보안성을 확보하는 것이 매우 중요하다.[11][12]

아래 [표 6]에서는 FMEA를 수행할 때 사용되는 FMEA 시트를 보여주고 있으며, 이 FMEA 시트를 작성함으로써 수행할 수 있다.

[표 6] FMEA 시트

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*

또한, FMEA의 수행 알고리즘은 아래 [그림 6]와 같다.



[그림 6] FMEA 수행 알고리즘

FMEA 수행은 제일 먼저, 결함 원인들을 그룹화 하고 두 번째 단계는 각 결함의 경우에 대해 하나 이상의 잠재적 효과를 기술한 후 각 결함 원인에 대한 심각도, 발생도, 검출도를 결정한다.

세 번째 단계는 심각도, 발생도, 검출도를 가지고 위험우선순위 RPN(Risk Priority Number)을 계산한다. 여기서 RPN은 심각도(Severity) * 발생도(Occurence) * 검출도(Detection)로 계산된다. 구체적으로, 심각도(Severity)는 0과 1사이의 값을 가지게 되며 측정자가 0(None)에서 1(Most Severe)사이의 값을 임의로 정할 수 있다. 그 다음, 발생도(Occurence)도 0과 1사이의 값을 가지게 되며 측정자가 0(None)에서 1(Highest Probability)사이의 값을 임의로 정할 수 있다. 마지막으로 검출도(Detection)도 0과 1사이의 값을 가지게 되며 측정자가 0(None)에서 1(Highest Detectable Probability)사이의 값을 임의로 정할 수 있다.
마지막으로 위험우선순위를 바탕으로 결함과 위험을 줄이거나 제거할 수 있는 계획을 수립한다.[9][11]
현재 FMEA 수행은 과거 FMEA에 비해 심각도, 발생도, 검출도 값을 구체적이고 정확하게 계산 및 측정해낼 수 있음으로써 모바일 뱅킹 시스템의 보안성 개선에 더욱 초점을 두고 있다.
위의 내용을 바탕으로 본 논문에서도 FTA와 FMEA를 사용하여 모바일 뱅킹 시스템의 보안성 개선을 위한 분석을 수행하며, 이는 현 모바일 뱅킹 시스템의 보안 취약점 및 위험요소들에 대한 개선 사항을 바탕으로 한다.
이에 본 논문의 3절에서는 모바일 뱅킹 시스템 내에 존재하는 결함 원인 및 위험요소 도출을 통하여 정보 통제 및 관리 프로세스를 제안할 것이다. 제 4절에서는 3절의 모바일 뱅킹 시스템의 결함 원인 및 위험요소를 기반으로 하여 FTA 및 FMEA를 수행한다.

3. 모바일 뱅킹 시스템의 정보 보안 통제 및 관리 프로세스 설계

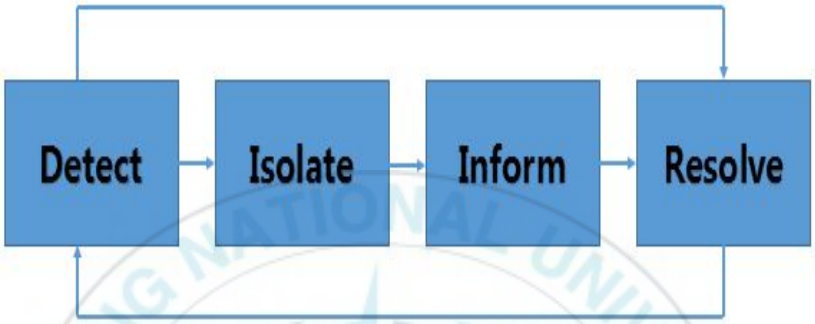
3.1 모바일 뱅킹 시스템의 결함 메커니즘과 위험요소 분석

모바일 뱅킹 시스템의 보안성(Security)을 개선하기 위해서는 각 모바일 뱅킹 시스템 내의 프로세스별로 보안 취약점과 위험요소를 찾아내는 일이 매우 중요하다. 이를 위해서는 모바일 뱅킹 시스템의 결함 메커니즘이 정의되어야 할 것이다.

정보 시스템 내에서 보안 결함 및 취약점들은 다음 네 가지 프로세스를 거쳐 해결될 수 있다.

- Detect(결함검출) - 결함을 탐지하고, 결함이 발생한 원인을 규명한다.
- Isolate(결함격리) - 발생 가능성이 있는 결함들을 분리한다.
- Inform(정보제공) - 관리 및 운영팀에 발생한 결함들에 대해 상세하게 보고한다.
- Resolve(문제해결) - 발견된 결함들을 최대한 빨리 대응하여 해결될 수 있도록 한다.

또한, 네 가지 프로세스는 아래 [그림 7]과 같이 계속 반복되면서 정보 시스템의 보안성을 개선할 수 있도록 한다.[8][14]



[그림 7] 정보 시스템의 보안 결함 해결 프로세스

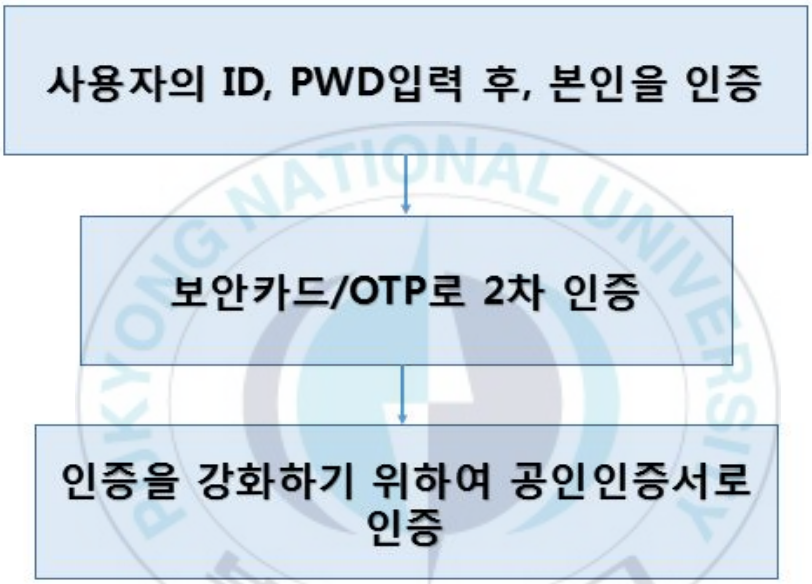
여기서 말하는 결함과 위험요소들의 상태가 'Active'한 상태가 되면 심각한 피해를 초래할 수 있기 때문에 이에 미리 대응하여 모바일 뱅킹 시스템의 정보 보안 통제와 관리를 효율적으로 할 수 있도록 해야 할 것이다.

모바일 뱅킹 서비스에서 각 기능 시스템에 따라 보안 취약점과 위험 요소가 존재하게 되는데, 아래에서는 모바일 뱅킹 프로세스 중 보안이 가장 취약한 4가지 단계(사용자 인증, 접근 통제, 바이러스 탐지 및 통제, 네트워크 시스템)에서의 보안 취약점과 위험요소에 대하여 상세하게 분류하고 정보 보안 통제와 관리 프로세스를 제안하고 있다.

가. 사용자 인증(User Authentication)

모바일 뱅킹 시스템의 뱅킹 서비스를 이용하기 위해서는 보안이 강화된 까다로운 절차의 사용자 인증 단계를 거쳐야만 한다.

여기서, 사용자 계정(User Account)과 비밀번호(Password)는 필수요소이다. 사용자 인증은 뱅킹 서비스 시스템에서 허가된 사용자인지 아닌지를 구분하며 아래 [그림 8]과 같이 세 단계로 진행된다.[7][14][16]



[그림 8] 사용자 인증(User Authentication) 단계

과거에는 뱅킹 서비스 인증을 하기 위해서는 사용자의 ID와 PWD 방식을 주로 사용하였지만, 최근에는 뱅킹 시스템의 보안을 더욱 강화하기 위하여 공인인증서(Accredited Certificate), 보안카드, OTP(One Time Password) 및 생체 인증(Biometrics) 방식을 도입하고 있는 추세이다. 아래 [표 7]에서는 "사용자 인증" 단계에서 발생할 수 있는 보안 취약점과 위험 요소들을 나타내고 있다.

[표 7] “사용자 인증”단계 - 보안 취약점, 위험 요소 그리고 정보 보안 통제 및 관리 프로세스

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	ID와 핀 번호, pwd 노출, ID와 pwd 해킹, 엑티브X 미설치	ID와 같은 pwd, 핸드폰 번호숫자, 개인 신상 정보 등	ID는 개인의 정보에 기반해서는 안되며, pwd는 다양한 문자 조합(대, 소문자, 숫자, 문자)으로 설정한다. ID, pwd 보안 수준을 알린다.	로컬장치 초기화 가상키보드 적용	관리자가 사용자마다의 ID/PWD 주기적으로 검사 및 보안성 검사	IP탐지 시스템, 방화벽,	보안 정책 평가 및 지속적 기술 관리
보안 카드	보안 카드 유출, 도난, 분실 및 보안 카드 이미지 파일 유출, 엑티브X 미설치	보안 카드 숫자, 보안 카드 이미지 파일	주기적인 보안 카드 생성 및 알고리즘 갱신, 보안 카드를 장기간 사용하지 않는다.	강화된 OTP기술 개발, 고정되지 않은 보안카드 숫자 이용	관리자가 사용자에게 보안 카드 갱신을 주기적으로 알림, 주기적인 보안성 검사	장기간 사용시 거래 차단 및 초기화, IP탐지 시스템, 방화벽	보안 카드 보안 정책 평가 및 지속적 기술 관리
OTP(One Time Password)	OTP해킹, OTP 사용 횟수의 제한, OTP 생성 알고리즘 조작, 엑티브X 미설치	OTP 토큰과 키	주기적인 OTP 생성 알고리즘 보완	현재 가장 높은 암호체계로써, 사용자의 OTP생성기 관리 주의	관리자가 주기적인 OTP 생성 및 관리 정책 수립, 주기적으로 보안성 검사	IP탐지 시스템, 방화벽	OTP 보안 정책 평가 및 지속적 기술 관리
공인인증서	공인 인증서 유출, 공인 인증서	개인 신상 정보,	공인 인증서 발급의 의무화, 공인 인증서의	보완된 Hardware Security Module	관리자가 사용자마다의 공인 인증서를	IP탐지 시스템, 방화벽	공인 인증서보안 정책 평가 및 지속적

	도난 및 분실, 엑티브X 미설치		주기적인 갱신 암호화키를 2048Byte로 증가	도입, 강화된 key 알고리즘	주기적으로 검사 및 보안성 검사 주기적인 공인 인증서 갱신		기술 관리
생체 인증 (지문, 홍채, 안면, 음성)	유출될 경우 복구 불가능, 엑티브X 미설치	정확한 인식 불가, 불확실한 매칭 임계치 설립	공유 불가능,	여러 가지 신체부위를 이용한 이중 인증	생체 인증을 통한 물리적 접근 제어, 생체인증 정보 암호화	IP탐지 시스템, 방화벽	생체 인증 보안 정책 평가 및 지속적 기술 관리

사용자 인증 단계에서는 주로 인증 방식에 관련된 개인정보 유출이 보안 취약점이 되고, 위협 요소는 사용자의 개인 신상 정보가 해당이 된다.

나. 접근 통제(Access Control)

접근 통제는 정보 시스템으로의 승인되지 않은 접근을 통제하기 위해 고안된 물리적 혹은 관리적인 통제 시스템을 일컬으며, 먼저 물리적인 통제는 일반적으로 특별한 보호가 필요한 시설 및 장비를 외부로부터 보호하는 것을 일컫는다. 다음으로, 관리적인 통제는 보안 정책에 의해 정의된 운영지침과 절차에 따라 승인되지 않은 접근을 통제하는 것을 말한다.

아래 [표 8]에서는 “접근 통제” 단계에서 발생할 수 있는 보안 취약점과 위험 요소들을 나타내고 있으며, 접근 통제를 위한 시스템인 운영체제, 미들웨어 그리고 하드웨어에서 발생할 수 있는 보안 취약점과 위험 요소를 나타내고 있다. 보안 취약점으로는 승인되지 않은 사용자의 접근과 악성코드 및 악성 소프트웨어(Malware)에 의한 위협들이며, 위험 요소로는 모바일 뱅킹 서비스 구현 환경인 모바일 운영체제와 그에 따른 접근 시도들이 해당된다.[14][15][16][17]

[표 8] “접근 통제” 단계 - 보안 취약점, 위험 요소 그리고 정보 보안 통제 및 관리 프로세스

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	금융고객 관련 파일 기록 도난, 개방형 모바일 환경으로 인한 외부 침입	개방형 API, 조작된 모바일 OS로 그 정보 악성코드	다른 사용자의 파일 읽기 금지 다른 사용자 메모리 사용 금지 다른 사용자의 디바이스 사용 금지	신뢰컴퓨팅 기술 구축, 프로세스 격리, 파일 시스템 권한 부여	파일 시스템 암호화, 보안 샌드박스 시스템 작동 원격 제어	코드 서명, 모의 해킹 시나리오 시연, IP탐지 시스템, 방화벽	보안 정책 평가 및 지속적 기술 관리
Middleware	데이터베이스 관리 파일 해킹, 외부침입	각 다른시스템마다의 로그온 시도	허가된 사용자만 접근 가능,	듀얼 컴퓨팅 기술 구축, 데이터베이스 접근 권한 부여	데이터베이스 시스템 암호화, 원격 제어	IP탐지 시스템,	
Hardware	모바일 기기 작동 오류, 사용법 미숙지, 기기 도난 및 분실	악성코드 및 악성웨어,	디바이스 암호화 패턴 및 비밀번호설정, 지문 인증 및 음성 인증	물리적 통제 기술 강화	모바일 디바이스 암호화 장치	감시 카메라, 엑스레이 검사	

다. 바이러스 탐지 및 통제(Virus Detection and Control)

최근 모바일 뱅킹 시스템에서는 다양해진 악성 바이러스와 악성 소프트웨어(Malware)의 공격으로 보안을 위협 받으며, 이에 따른 사용자들의 피해 수준도 심각해지고 있는 상황이다. 악성 소프트웨어(Malware)는 컴퓨터 및 모바일 디바이스에 설치되어 사용자 업무를 방해하거나 피해를 입히는 악성 소프트웨어를 말하고, 다양한 형태로 접근하여 사용자들에게 피해를 입히고 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.[14][15][17]

[표 9] “바이러스 탐지 및 통제” 단계 - 보안 취약점, 위험 요소 그리고 정보 보안 통제 및 관리 프로세스

<table>
<tr><th rowspan="2">Fault Mechanism</th><th rowspan="2">Security Vulnerability</th><th rowspan="2">Hazard Factors</th><th colspan="5">Information Security Control and Governance Process</th></tr>
<tr><th>1. Formulate Security Policy</th><th>2. Build Security Defense</th><th>3. Perform Active Monitoring</th><th>4. Perform Intrusion Testing</th><th>5. Ensure Security Management</th></tr>
<tr><td>웹사이트 방문</td><td>개인정보 유출, 금융 사기 발생</td><td>악성코드, 멀웨어</td><td rowspan="2">접근 통제를 강화한다. 악성코드로 인한 피해를 반드시 신고한다. 안티바이러스를 반드시 설치한다. 안티바이러스를 주기적으로 업데이트 한다</td><td rowspan="2">안티바이러스, 안티 멀웨어 설치, 달빅 가상머신 이용</td><td>주기적인 백신 프로그램의 업데이트</td><td>IP탐지 시스템, 방화벽</td><td rowspan="2">보안 정책 평가 및 지속적 기술 관리</td></tr>
<tr><td>디바이스 간의 연결</td><td>개인정보 유출, 금융 사기 발생</td><td>악성코드, 멀웨어</td><td>주기적인 백신 프로그램의 업데이트</td><td>연결 전 디바이스 바이러스 유무 검사</td></tr>
</table>

설치 경로 포함된 SMS, E-Mail을 통한 어플리케이션 설치	개인정보 유출, 금융 사기 발생	악성 코드 포함된 위조 어플리케이션			주기적인 백신 프로그램의 업데이트, 어플리케이션 검증 센터 구축, 스팸 메일 필터링	IP추적 및 탐지 시스템, 방화벽, 위조 어플리케이션 탐지 및 차단	

바이러스 탐지 및 통제 단계에서는 주로 웹사이트 방문, 모바일 기기 연결, SMS와 E-Mail을 통한 어플리케이션 설치에서 발생하는 개인 정보 유출이 보안 취약점이 되고, 위험 요소로는 악성 코드 및 악성 소프트웨어 등이 주를 이루고 있다. 향후에는 사용자들에게 점점 다양하고 치명적인 피해를 입힐 것으로 예상된다.

라. 네트워크 시스템(Network System)

네트워크 시스템은 모바일 뱅킹 서비스를 이용하기 위해서는 필수불가결한 존재로서, 다양한 네트워크 접속 환경을 지원하며 사용자들에게 편리함을 제공하고 있다. 그러나 많은 사용자가 모바일 뱅킹 서비스를 언제 어디서나 편리하게 사용함으로써 네트워크 보안 위협도 증가하고 있는 상황이다. 여기서 네트워크 시스템은 외부의 침입 신호를 감지하고 막거나 원격 접근을 허용하는 모든 시스템들의 총 집합을 말한다.[14][15][16][18]

[표 10] “네트워크 시스템” 단계 - 보안 취약점, 위험 요소 그리고 정보 보안 통제 및 관리 프로세스

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
네트워크 운영관리	데이터 손실 및 유출, 도청, 악성코드 유입 무선 구간 패킷 스니핑, 내부인트라넷 접속	해커의 접근, 악성코드, Wi-fi, GPS, 블루투스, 2,3G, Wibro DDOS 공격 무선망을 통한 노출된 위치정보	네트워크 접근 암호화 수행 모바일 플랫폼은 이동통신 망에서 전용회선으로 직접 연결	인증 및 암호화 기능 설정된 AP 사용, VPN 적용	트래픽 상시 감시, 무선랜 침입 탐지 시스템 구축	IP탐지 및 추적 시스템 작동, 방화벽	보안 정책 평가 및 지속적 기술 관리
네트워크 장비관리	데이터 손실 및 유출, 네트워크 장비 분실 및 도난	장비의 오작동, 장비 유지보수 미실시	내부 서버로의 직접연결은 차단, 이동통신 망에서 전용회선으로 직접 연결	호스트 기반의 방화벽 운용, 불필요한 포트 차단 및 통제 외부망과 내부망 분리 서버인 릴레이 연계서버 구축	무선랜 침입탐지시스템 구축, FMC관련 장비 구축,	네트워크 장비 위치 탐지 및 추적 시스템 작동	

위의 [표 10]에서와 같이, 모든 중요한 개인 신상 정보는 네트워크를 통해 암호화하여 전송하고 전송 중에 평문으로 복호화 되어서 외부 공격에 노출되지 않도록 해야 한다. 모바일 뱅킹 서비스를 위한 네트워크 통신 구간에서 암호 기술이 적용되어 사용자들의 개인 신상 정보가 전송되기 위해서 금융기관에서는 현재 다양한 암호 알고리즘 및 해쉬 함수 등을 개발하여 사용하고 있는 추세이다. 또한, 네트워크 시스템 단계에서는 주로 개인 정보 손실 및 유출이 보안 취약점에 해당되며, 위험 요소로는 네트워크로의 악성코드 유입과 네트워크 시스템 장비 자체의 오류가 해당된다.

위의 표들과 같이 모바일 뱅킹 서비스에서 각 기능 시스템에 따라 보안 취약점과 위험 요소들을 분석하고 이에 기반 하여 정보 보안 및 관리 프로세스를 수행할 수 있게 된다.

4. 모바일 뱅킹 시스템의 보안성 개선을 위한 결함 트리 분석(FTA)과 고장 유형 영향 분석(FMEA)

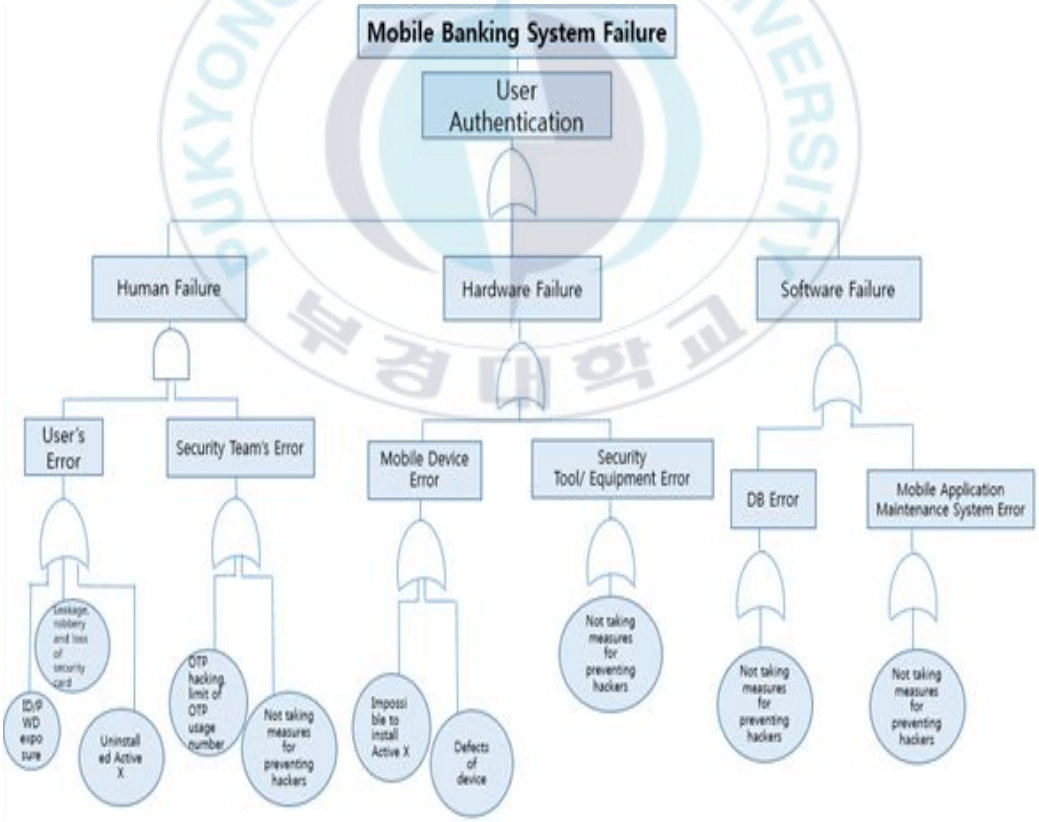
4.1 모바일 뱅킹 시스템의 보안성 개선을 위한 결함 트리 분석(Fault Tree Analysis) 적용

위 3절과 같이 모바일 뱅킹 시스템 내에 존재하는 보안 취약점과 위험요소들을 바탕으로 결함 트리 분석(Fault Tree Analysis)을 수행하여 모바일 뱅킹 시스템의 보안성을 개선할 수 있도록 한다.

가. “사용자 인증” 단계에서의 FTA 적용

사용자 인증 단계에서의 보안 취약점과 위험 요소들을 바탕으로 한 FTAs는 아래 [그림 9]와 같이 나타나고, 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 및 유출 그리고 Active X 미설치 등이 원인이 되고, 보안팀에 의한 오류는 크게 비인가된 외부 침입에 대한 대응 부족이 된다.

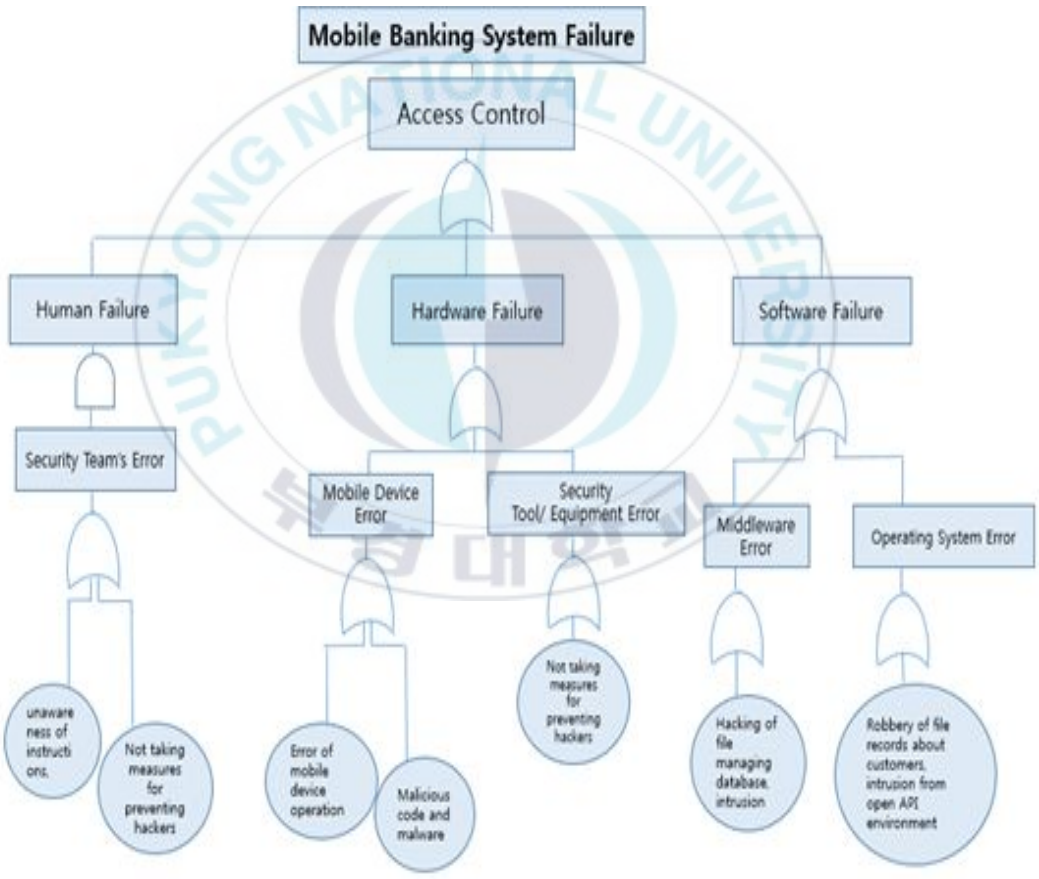
하드웨어에 의한 오류에서는 모바일 디바이스 오류와 보안 도구 및 장비에 의한 오류가 해당된다. 구체적으로, 모바일 디바이스 오류에서는 Active X 설치 불가 그리고 모바일 디바이스 자체 결함 등으로 나뉘어진다. 그리고 보안 도구 및 장비에 의한 오류로는 외부 침입 예방에 대한 대응 부족이 된다. 마지막으로, 소프트웨어 시스템에 의한 오류로는 데이터베이스 시스템 오류로, 이도 마찬가지로 외부 침입 예방에 대한 대응 부족을 말한다. 그 다음으로 모바일 어플리케이션 유지보수 시스템에 의한 오류에서도 마찬가지로 외부 침입 예방에 대한 대응 부족이 해당된다.[14][19]



[그림 9] 사용자 인증 단계의 FTA 적용

나. “접근 통제” 단계에서의 FTA 적용

접근 통제 단계는 모바일 뱅킹 시스템 내에서 핵심적인 부분으로 모바일 뱅킹 시스템 내에 다양한 형태의 결함과 보안 취약점이 존재하고, 그로 인한 보안 위협의 정도가 점점 심각해지고 있다. 아래 [그림 10]에서는 접근 통제 단계에서의 FTA 적용을 나타내고 있다.

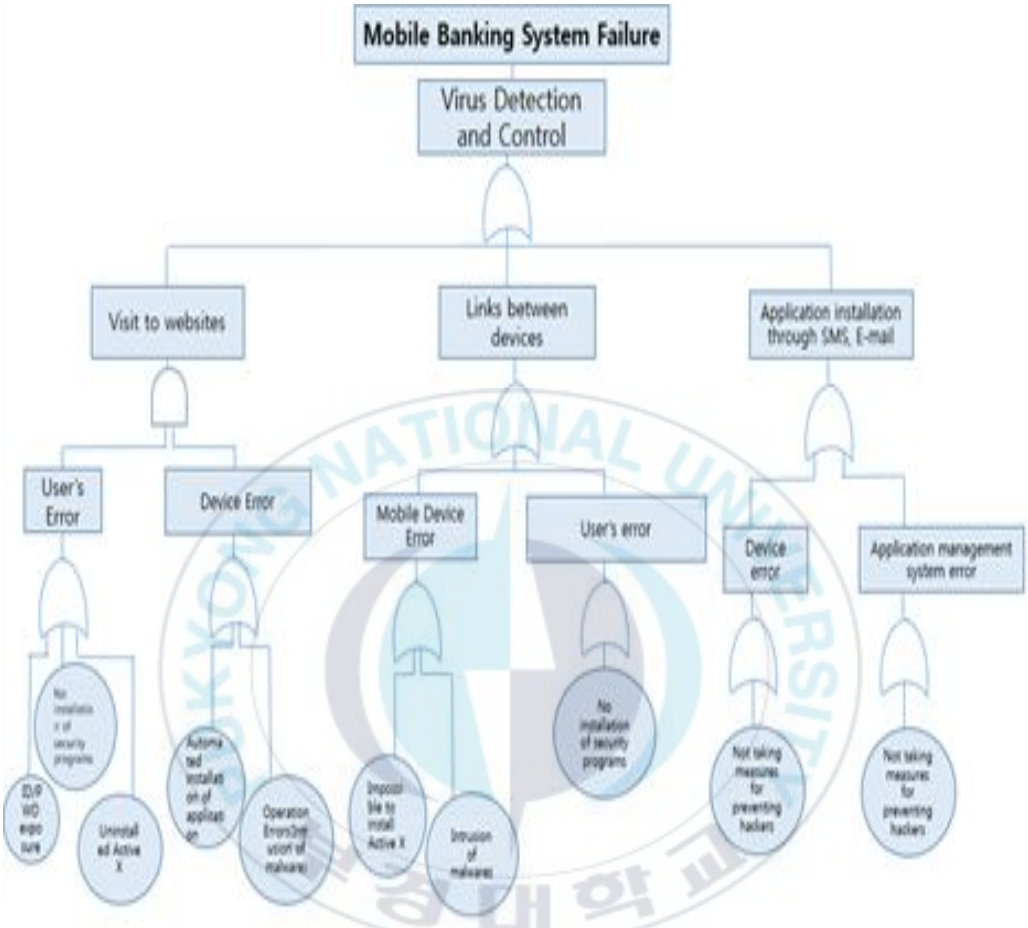


[그림 10] 접근 통제 단계의 FTA 적용

위의 [그림 10]에서는 접근 통제 단계에서의 결함을 사람에 의한 오류, 하드웨어에 의한 오류 그리고 소프트웨어 시스템에 의한 오류 이렇게 세 가지로 분류하였다. 먼저 사람에 의한 오류에서는 보안팀에 의한 오류로 교육 및 관리의 부재 그리고 외부 침입 예방에 대한 대응 부족이 해당된다. 그 다음, 하드웨어에 의한 오류로는 모바일 디바이스 오류 그리고 보안 도구 및 장비들에 관한 오류이다. 모바일 디바이스 오류는 모바일 디바이스 작동 오류와 악성 코드 및 악성 소프트웨어의 유입이 해당된다. 보안 도구 및 장비들에 관한 오류로는 마찬가지로 외부 침입 예방에 대한 대응 부족이 해당된다. 마지막으로, 소프트웨어 시스템에 의한 오류는 미들웨어 오류와 운영체제 시스템에 의한 오류로 분류되는데, 미들웨어 오류는 데이터베이스를 관리하는 파일로의 외부 침입과 미들웨어 침입이 해당된다. 마지막으로 운영체제 시스템에 의한 오류는 사용자 기록 파일 도난 및 유출 그리고 오픈 API 환경으로부터의 외부 침입이 해당된다.[15][16][22]

다. “바이러스 탐지 및 통제” 단계에서의 FTA 적용

바이러스 탐지 및 통제 단계에서 가장 많은 보안 취약점과 위험 요소가 발생할 수 있다. 현재 악성 바이러스 및 악성 소프트웨어의 형태가 다양해지면서 모바일 뱅킹 시스템의 보안 수준이 점점 약화되고 있는 상황이다. 여기서 말하는 악성 바이러스 및 악성 소프트웨어의 종류로는 바이러스, 애드웨어, 스파이웨어, 트로이목마, 스팸, 피싱 및 파밍 등을 말하게 된다. 또한 치명적인 수준의 악성 바이러스 및 악성 소프트웨어로부터 위협을 받게 되면 금융기관 전체 뿐 아니라 국가를 위협하는 정도의 피해를 받을 수도 있게 되므로 이에 대한 강력한 대응이 필요하다.



[그림 11] 바이러스 탐지 및 통제 단계의 FTA 적용

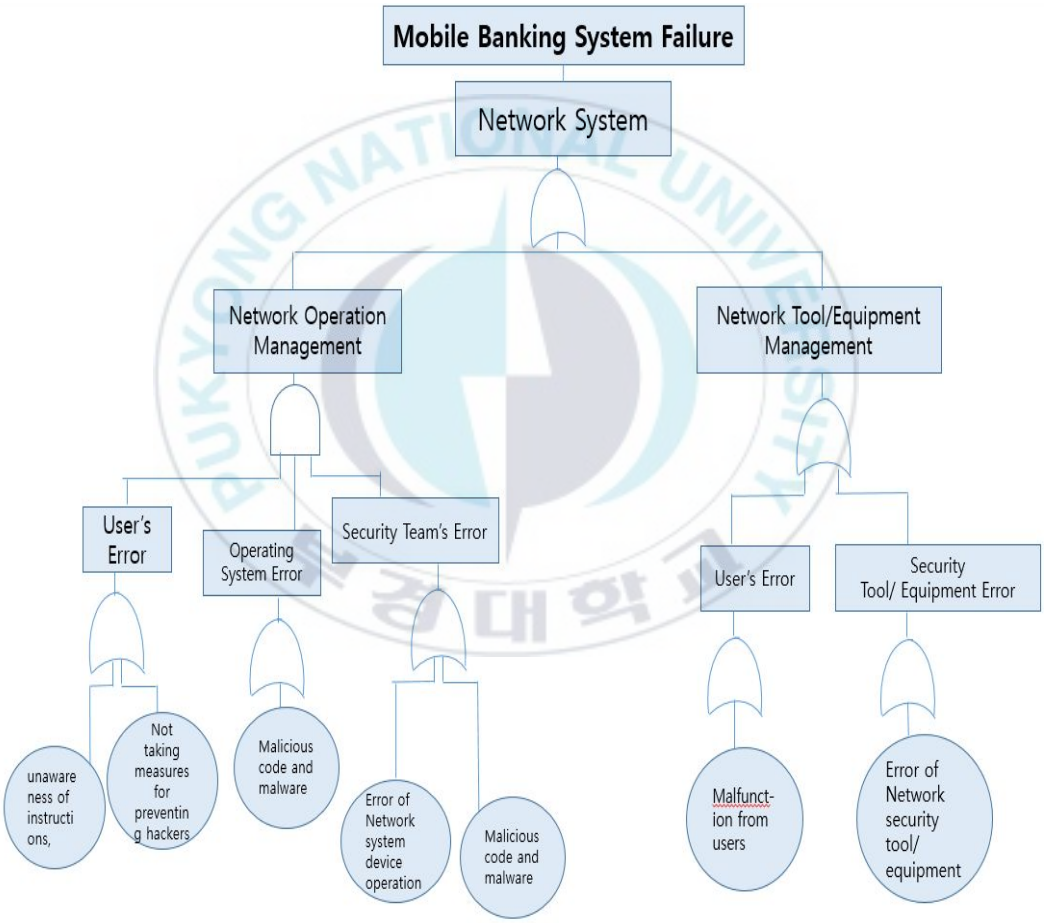
위의 [그림 11]에서는 바이러스 탐지 및 통제 단계에서의 결함들을 탐지되는 경로에 따라 웹사이트 방문, 모바일 디바이스 간의 연결, SMS 혹은 E-Mail을 통한 어플리케이션 설치 이렇게 세 가지로 분류하여 나타내었다. 먼저, 웹사이트 방문에 의한 오류로는 사용자에 의한 오류와 디바이스 오류로 나타난다. 사용자에 의한 오류에서는 ID/PWD 노출, 보안 프로그램 미설치 그리고 Active X 미설치가 해당된다. 그리고 디바이스 오류에서는

의도치 않게 어플리케이션의 자동 설치와 악성 소프트웨어의 침입으로 인한 작동 오류가 해당된다. 그 다음으로 모바일 디바이스 간의 연결에 의한 오류도 마찬가지로 모바일 디바이스 오류 그리고 사용자 에러로 나뉘어지며, 모바일 디바이스 오류에서는 Active X 설치 불가능과 악성 소프트웨어의 침입 그리고 사용자에 의한 오류에서는 보안 프로그램 미설치가 해당된다. 마지막으로 SMS 혹은 E-Mail을 통한 어플리케이션 설치에 의한 오류에서는 모바일 디바이스에 의한 오류와 어플리케이션 관리 시스템 오류로 나뉘어지며, 모바일 디바이스에 의한 오류는 외부 침입 예방에 대한 대응 부족 그리고 어플리케이션 관리 시스템 오류도 외부 침입 예방에 대한 대응 부족이 해당된다.[14][20]

라. “네트워크 시스템” 단계에서의 FTA 적용

네트워크 시스템 단계는 모바일 뱅킹 서비스 이용 시 네트워크 통신 사업자와 금융기관별 어플리케이션의 통신작용에서 중요한 역할을 하게 된다. 그러므로 더욱 허가되지 않은 외부 침입으로부터 보안을 쉽게 위협받고 있는 상황이다. 아래 [그림 12]에서는 네트워크 시스템 단계에서의 FTA 적용을 나타내고 있다. 발생하는 결함들은 네트워크 운영관리 그리고 네트워크 장비관리에 의한 오류로 2 가지로 분류하였다. 먼저, 네트워크 운영관리에 의한 오류에서는 사용자에 의한 오류, 운영시스템 오류, 보안팀에 의한 오류로 나타나게 된다. 구체적으로, 사용자에 의한 오류는 교육 및 관리정책 인지 부족과 외부 침입 예방에 대한 대응 부족으로 나뉘며 운영시스템 오류는 악성 바이러스 및 악성 소프트웨어 침입이 해당된다. 마지막으로 보안팀에 의한 오류는 네트워크 시스템 기기 작동 오류 그리고 악성 바이러스 및 악성 소프트웨어 침입으로 나뉘게 된다.

그 다음으로 네트워크 장비관리에서는 사용자에 의한 오류와 보안 도구 및 장비에 의한 오류로 나뉘게 된다. 먼저, 사용자에 의한 오류는 사용자의 기기 오작동이 해당되며 보안 도구 및 장비에 의한 오류는 네트워크 보안 도구 및 장비 자체 오류로 나타난다.[14][20][21]



[그림 12] 네트워크 시스템 단계의 FTA 적용

4.2 모바일 뱅킹 시스템의 보안성 개선을 위한 고장 유형 영향 분석(Failure Modes and Effects Analysis) 적용

위 3절과 같이 모바일 뱅킹 시스템 내에 존재하는 보안 취약점과 위험요소들을 바탕으로 고장 유형 영향 분석(Failure Modes and Effects Analysis)을 수행하여 모바일 뱅킹 시스템의 보안성을 개선하여 향후에 발생하는 잠재적인 결함을 예방할 수 있도록 한다.

가. “사용자 인증” 단계에서의 FMEA 적용

사용자 인증 단계에서의 보안 취약점과 위험 요소들을 바탕으로 FMEA를 적용한 것을 아래 [표 11]에서 나타내고 있다. 향후 사용자 인증 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 인증 수단인 ID/PWD, 보안카드, OTP, 공인 인증서 그리고 생체인증을 통한 사용자 인증 단계에 따라 분석하였다. 이를 기반으로 심각도(S), 발생도(O) 그리고 검출도(D)를 사용하여 위험우선순위(RPN)을 매김으로써 사용자 인증 단계의 보안성을 제고할 수 있도록 한다. 사용자 인증 단계에서의 위험우선순위(RPN)는 보안 강도가 가장 높은 생체인증에서 0.600으로 가장 높게 기록되었다. 또한 FMEA에서는 결함과 위험요소를 기반으로 작성한 관리 프로세스를 작성하여 나타내고 관리프로세스를 전후로 각 단계 내에서의 초기 심각도, 발생도, 검출도와 1차 심각도, 발생도, 검출도를 비교하여 나타내게 된다.[11][19]

[표 11] “사용자 인증” 단계의 FMEA

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
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	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 loca devices Apply virtual keyboard	Develop intensified OTP technologies, Use not fixed security card	Take notice the management of OTP generator IP Detection system	Institute complemented hardware security	Authenticate with dual factors using various parts of body

			numbers		module	
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
	RPN	0.14	0.128	0.18	0.225	0.40

나. “접근 통제” 단계에서의 FMEA 적용

접근 통제 단계에서의 보안 취약점과 위험 요소들을 바탕으로 FMEA를 적용한 것을 아래 [표 12]에서 나타내고 있으며, 향후 접근 통제 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 접근 통제 시스템의 핵심인 운영체제 시스템, 미들웨어 시스템 그리고 하드웨어 시스템에 따라 분석하였다. 이를 기반으로 심각도(S), 발생도(O) 그리고 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 운영체제 시스템에서 0.18로 가장 높게 기록되었다. 또한 결함과 위험 요소를 기반으로 작성한 관리 프로세스를 작성하여 나타내고 관리 프로세스를 전후로 각 단계 내에서의 초기 심각도, 발생도, 검출도와 1차 심각도, 발생도, 검출도를 비교하여 나타내게 된다. 특히나 접근 통제 단계의 보안이 중요시 되는 만큼 주기적으로 FMEA를 수행하여 관리 프로세스를 업데이트하여 모바일 뱅킹 서비스 이용자들이 심각한 피해를 더 이상 입지 않도록 해야 할 것이다.[11][18][21]

[표 12] “접근 통제” 단계의 FMEA

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 numbers	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

다. “바이러스 탐지 및 통제” 단계에서의 FMEA 적용

바이러스 탐지 및 통제 단계에서의 보안 취약점과 위험 요소들을 바탕으로 FMEA를 적용한 것을 아래 [표 13]에서 나타내고 있으며, 향후 바이러스 탐지 및 통제 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 접근 경로에 따라 웹사이트 방문, 모바일 디바이스 간의 연결 그리고 SMS, E-Mail을 통한 어플리케이션 설치로 분류하여 분석하였다. 이를 기반으로 심각도(S), 발생도(O) 그리고 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 모바일 디바이스 간의 연결에서 0.567로 가장 높게 기록되었다. 또한 결함과 위험 요소를 기반으로 작성한 관리 프로세스를 작성하여 나타내고 관리 프로세스를 전후로 각 단계 내에서의 초기 심각도, 발생도, 검출도와 1차 심각도, 발생도, 검출도를 비교하여 나타내게 된다.[11][13][18][22]

[표 13] “바이러스 탐지 및 통제” 단계의 FMEA

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	Malicious code	Malicious code and	Malicious code

Cause of Failure		and malicious software	malicious software	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

라. “네트워크 시스템” 단계에서의 FMEA 적용

네트워크 시스템 단계에서의 보안 취약점과 위험 요소들을 바탕으로 FMEA를 적용한 것을 아래 [표 14]에서 나타내고 있으며, 향후 네트워크 시스템 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 네트워크 시스템 구성 형태에 따라 네트워크 운영관리와 네트워크 장비관리로 분류하여 분석하였다. 이를 기반으로 심각도(S), 발생도(O) 그리고 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 네트워크 장비관리에서 0.441로 네트워크 운영관리의 RPN보다 높게 기록되었다. 또한 결함과 위험 요소를 기반으로 작성한 관리 프로세스를 작성하여 나타내고 관리 프로세스를 전후로 각 단계 내에서의 초기 심각도, 발생도, 검출도와 1차 심각도, 발생도, 검출도를 비교하여 나타내게 된다. 현재 각 금융기관별 모바일 뱅킹 시스템에서는 네트워크

시스템의 보안성을 향상시키기 위한 대책으로 다양한 암호 알고리즘들, 해쉬 함수 등을 사용하고 있는 상황이다. 또한 향후 모바일 뱅킹 시스템 네트워크 보안을 위한 대책을 지속적으로 개발해야 할 것이다.[11][12][14]

[표 14] "네트워크 시스템" 단계의 FMEA

Requirements		Network operation management	Network tool/equipment management
Potential Failure Mode		Leakage of personal information, Malicious code and malicious software, Access to internal Intranet, Packet sniffing with wireless section	Leakage of personal information, Loss and robbery of network tool/equipment
Potential Effects of Failure		Personal Information exposure	Personal Information exposure
S (Severity)		0.9	0.7
Classification			
Potential Cause of Failure		Malicious code and malicious software, Operation team's errors	Malicious code and malicious software, Operation team's errors
O (Occurrence)		0.7	0.6
Managing Process		Update vaccine program, IP detection system, Apply VPN, Monitor traffic regularly	Update vaccine program; Installation of security program, IP detection system, Build tools about FMC
D (Detection)		0.7	0.9
RPN (S*O*D)		0.441	0.378
1st Action Taken	S	0.7	0.5
	O	0.4	0.3
	D	0.5	0.5
	RPN	0.140	0.075

결과적으로 초기에 비해 1차로 다시 FMEA를 수행하였을 때 훨씬 심각도, 발생도, 검출도 및 위험우선순위(RPN) 수치가 줄어든 것으로 나타난다. 따라서 향후에는 모바일 뱅킹 서비스를 이용하는 고객들이 보안성이 향상된 모바일 뱅킹 시스템을 요구하기 때문에 이러한 분석기법들을 사용하여 잠재적인 결함 및 위험요소 발생을 예방하는 것이 필수 불가결적이다.

PUKYONG NATIONAL UNIVERSITY
부경대학교

5. 결론 및 향후 과제

5.1 결론

최근 정보 기술과 모바일 디바이스의 발전에 따라 모바일 뱅킹 서비스의 이용이 급격하게 증가하고 있다. 모바일 뱅킹 시스템(Mobile Banking System)은 사용자들이 스마트폰, PDA와 같은 모바일 디바이스를 사용하여 이동통신사의 무선 인터넷을 이용하여 금융기관의 모바일 뱅킹 시스템과 연결하여 언제 어디서나 편리하게 사용할 수 있는 전자금융 서비스를 말한다. 모바일 뱅킹 서비스는 무선 인터넷의 발달과 함께 기존의 오프라인 뱅킹 서비스가 온라인 및 모바일로 확대되면서 서비스 이용 고객, 거래 건수, 이용 금액 등의 이용 실적이 꾸준히 증가하고 있으며 전자금융서비스 형태 중 높은 비중을 차지하며 성장하고 있다. 그러나 이에 따른 보안 위협 요소들도 함께 발전되면서 모바일 뱅킹 시스템과 사용자들을 위협하고 있다. 이를 해결하고 보안성을 향상시킬 수 있는 연구가 중요시되고 있다. 따라서 본 논문에서는 모바일 뱅킹 시스템의 보안성을 확보하고 개선하기 위하여 현 모바일 뱅킹 시스템의 보안 취약점과 위험요소들을 도출하여 분석해내고, 개선된 모바일 뱅킹 보안 프로세스를 제안하여 사용자들에게 안전한 모바일 뱅킹 서비스를 제공할 수 있도록 할 것이다.

본 논문에서 제시한 현 모바일 뱅킹 시스템의 모바일 뱅킹 프로세스 중 가장 보안성이 취약한 단계들인 “사용자 인증”, “접근 통제”, “바이러스 탐지 및 통제” 그리고 “네트워크 시스템”에서 보안 취약점과 위험요소들을

분석하였다. “사용자 인증”에서는 주로 인증 방식에 관련된 개인정보 유출이 보안 취약점이 되고, 위험 요소는 사용자의 개인 신상 정보가 해당이 된다. 두 번째로 “접근 통제”에서는 보안 취약점으로는 승인되지 않은 사용자의 접근과 악성코드 및 악성 소프트웨어(Malware)에 의한 위협들이며, 위험 요소로는 모바일 뱅킹 서비스 구현 환경인 모바일 운영체제와 그에 따른 비인가된 접근이 해당된다. 세 번째로 “바이러스 탐지 및 통제”에서는 주로 웹사이트 방문, 모바일 기기 연결, SMS와 E-Mail을 통한 어플리케이션 설치로 인한 개인 정보 유출이 보안 취약점이 되고, 위험 요소로는 악성 코드 및 악성 소프트웨어 등이 해당된다. 마지막으로 “네트워크 시스템”에서는 주로 개인 정보 손실 및 유출이 보안 취약점에 해당되며, 위험 요소로는 네트워크로의 악성코드 유입과 네트워크 시스템 장비 자체의 오류가 해당된다. 각 단계들의 보안 취약점과 위험 요소들을 기반으로 보안성 개선을 위한 정보보안프로세스를 작성하고, 이를 바탕으로 결함 트리 분석(FTA)과 고장 유형 영향 분석(FMEA)를 수행하여 모바일 뱅킹 시스템의 보안성을 개선할 수 있도록 한다.

이와 같이 모바일 뱅킹 시스템은 다양한 뱅킹 서비스를 제공하기 때문에 각 단계마다 보안 취약점과 위험 요소를 가지고 있으므로, 보안성을 향상하기 위해서는 상세하게 보안 취약점과 위험 요소를 파악하고 해결할 수 있는 개선사항을 도출할 필요가 있다. 따라서 본 논문에서는 각 단계별 보안 취약점과 위험 요소들을 파악하여 도출한 후, 이를 개선하기 위하여 정보보안프로세스를 작성 및 결함 트리 분석(FTA)와 고장 유형 영향 분석(FMEA)를 수행함으로써 모바일 뱅킹 시스템의 보안성을 향상시킬 수 있는 방안을 제시하였다.

5.2 향후 과제

본 논문에서는 모바일 뱅킹 시스템 내에 존재하는 보안 취약점과 위험 요소들을 도출하여 분석한 후 이를 개선하기 위한 보안프로세스와 결함트리 분석, 고장 유형 영향 분석을 적용함으로써 개선방안을 제시하였다. 이러한 문제점들이 점점 발생할수록 이에 따른 보안 솔루션이 개발되고 있는 상황이다. 그러나 언제 어디서나 모바일 뱅킹 서비스를 이용할 수 있다는 편리함 뒤에는 사용자들을 위협하는 위협요소들이 점점 많아지고 그 피해수준도 점점 심각해지고 있기 때문에 이를 충분히 고려한 보안 솔루션에 대한 연구가 향후 과제로 남아 있다.

지금까지의 동향과 비슷하게 앞으로도 더욱 모바일 뱅킹 서비스뿐만 아니라 스마트 뱅킹 서비스의 사용이 증가할 것으로 예상되지만, 아직 해결하지 못한 보안 취약점과 위험 요소 그리고 점점 심각해지는 사이버 범죄 및 모바일 범죄 사기의 증가로 인하여 모바일 뱅킹 시스템의 보안성 향상에 관한 문제는 더욱 중요한 문제로 제기될 것이다. 따라서 효율적으로 모바일 뱅킹 시스템의 보안 취약점과 위험 요소들을 도출하고 분석할 수 있는 다양한 분석 기법의 지속적인 개발 및 연구가 필요할 것이다.

참고 문헌

[1] Hyu-Geun Shin, “2013 Predicted Analysis of Banking IT Information Security Trend”, Journal of the Telecommunication Technology Association, Vol. 133, pp. 23-27, 2011

[2] Chang-Kyu Guak, “Smartphone Security on Banking Parts Guide”, Journal of Financial Security Agency, Vol. 8, pp. 8-12, 2010

[3] Vanessa Pegueros, “Security of Mobile Banking and Payments”, 2013.01.04.
Retrieved on 12th Nov. 2014 from http://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062.

[4] Kyong-Hyung Lee, Yi-Young Kim, “The State of Mobile Banking Service in Domestic Banks”, Journal of Korea Information Society Development Institute, Vol. 18, pp. 2-7, 10-15, 2002.

[5] Hyu-Geun Shin, “2014 Predicted Analysis of Banking IT Information Security Trend”, Journal of Korea Financial Telecommunications & Clearings Institute, Vol. 55, pp. 93-124, 2014.

[6] Bong-Kyu Lee, “A Research on Discovering New Vulnerabilities and Analyzing Methods in Domestic Mobile Environment”, Journal of the Korea Internet & Security Agency, KISA-WP-2012-0009, 2012.

[7] Hee-Yeon Min, Jin-Hyung Park, Dong-Hoon Lee, In-Seok Kim, “Outlier Detection Method for Mobile Banking with User Input Pattern and E-finance Transaction Pattern”, Journal of Internet Computing and Services, Vol. 15, pp. 157-160, 2014.

[8] Jae-Chul Ryu, “A Research of Prevention Technique for Malignant Code Based on Mobile Environment”, KISA-WP-2010-0057, 2010.

[9] Myong-Hee Kim, Wildan Tyoib, Man-Gon Park, “An Integrative Method of FTA and FMEA for software Security Analysis of a Smart Phone”, Koren Information Processing Society Transactions on Computer and Communication Systems, Vol. 2, No. 12, pp. 541-552, 2013.

[10] Soo-Mi Jang, Man-Gon 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.

[11] Ubiquitous Management Academy Consulting, “FMEA(Potential Failure Mode and Effects Analysis)”. 2014.01.13

Retrieved on 1st April. 2015 from http://consulting.u-mac.co.kr/pds/quality/list.asp?sch_head=m_title&sch_string=fmea.

[12] Seong-Wook Na, Yoon-Hee Lee, Soon-Jeong Ji, "The Security Issue and Strategies of Smartphone an Mobile office", CIO Report of National Information Society Agency, Vol. 26, pp. 10-27, 2010.

[13] Jeong-Sook Seong, "A Research on Preventing for Security Threats", Journal of Security Engineering, Vol. 9, pp. 503-509, 2012.

[14] So-Young Kim, Myeong-Hee Kim, Man-Gon 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.

[15] Indian Institute of Banking and Finance, "Certified Information System Banker-Rules and Syllabus", 2007.12. Retrieved on 20th November. 2014 from http://iibf.org.in/documents/ceisb-module1.pdf.

[16] Michael Becher, Felix C. Freiling, "Mobile Security Cathcing Up? Revealing the Nuts and Bolts of the Security of Mobile Devices", IEEE Symposium on Security and Privacy, 2011.

[17] Kurt Biri, Giampaolo M. Trenta, "Corporate Information Security Governance in Swiss Private Banking", Master D

Thesis, Executive MBA Program of the University of Zurich, Swiss, pp. 5-64, 2004.

[18] Nie Jin, Hu Xianling, "Mobile Banking Information Security and Protection Methods", IEEE International Conf. on Computer Science and Software Engineering, 2008.

[19] Young-Sil Lee, "Online Banking Authentication System using Mobile-OTP with QR-code", Computer Sciences and Convergence Information Technology(ICCIT), Vol. 30, pp. 644-650, 2010.

[20] Ross J. Anderson, "Security Engineering 2nd Edition", pp. 93-126, WILEY, 2008.

[21] Indian Institute of Banking and Finance, "Certified Information System Banker-Rules and Syllabus", 2007.12. Retrieved on 20th November. 2014 from http://iibf.org.in/documents/ceisb-module1.pdf.

[22] FSC(Financial Services Commission), FSS(Financial Supervisory Service), "Implementation of Preventive Services For Electronic Financial Fraud", 2013.09.25. Retrieved on 20th November. 2014 from http://www.fsc.or.kr, http://www.fsc.go.kr

Acknowledgement

This thesis was supported by National Research Foundation (NRF) of Korea [2013K1A3A1A09076037].

PUKYONG NATIONAL UNIVERSITY
부경대학교

감사의 글

2012년도 학부 IT융합응용공학과로 편입을 한지가 엊그제 같은데 벌써 대학원을 입학하여 졸업을 앞두고 있습니다. 많은 생각들이 스쳐지나가면서 감개무량하고 한편으로는 아쉬운 점도 너무나 많은 것 같습니다. 먼저, 항상 따뜻한 애정과 관심을 가지고 저를 보살펴주시는 박만곤 지도교수님께 큰 감사를 드리고 싶습니다. 저에게 따뜻하고 진심 어린 조언과 때로는 따끔한 충고에 많은 배움과 깨달음을 얻을 수 있었습니다. 제가 있는 동안 저에게 주신 큰 가르침과 스승의 은혜는 절대 잊지 않고 멋진 사람이 되어 보답하겠습니다.

그리고 저희 지도교수님과 더불어 항상 가까이에서 저에게 많은 조언과 논문 작성에 도움과 격려를 보내주셨던 김창수 교수님, 이경현 교수님에게 감사드린다는 말 전해드리고 싶습니다.

대학원에 입학하기 전부터 SEMI 연구실에서 학부생부터 외국인 학생, SEMI 연구실 선배님들을 만나 많은 도움을 얻고 추억을 만들어서 감사의 인사를 드리고 싶습니다. 먼저, 많은 도움과 조언을 주셨던 김수도 교수님, 정말 감사드립니다. 항상 저에게 긍정적인 에너지와 많은 조언과 도움을 주셨던 김규아 교수님, 멋진 카리스마로 저에게 따끔한 충고와 많은 도움을 주셨던 장수미 교수님 너무 감사드립니다.^^ 그리고 늘 저를 응원해주시고 따뜻한 조언을 해주셨던 김명희 교수님 정말 감사드립니다. 그리고 항상 랩을 든든하게 지켜주시는 박현기 과장님에게도 감사의 말씀드리고 싶습니다. 다들 너무 보고싶을거에요!! 그리고 대학원 졸업을 같이하는 인도네시아 친구들 Vandha, Zhany, Diena 에게도 고맙고, 연구실에서 항상 힘들 일 수고해주는 성진, Bright, Sang, Rafael에게도 고맙다는 말 꼭 하고 싶습니다.

학부시절부터 대학원 중간까지 같이 한 은아에게도 고맙다는 말 전합니다. 모두에게 큰 감사의 말씀 드릴게요!!!

마지막으로 저를 이 자리까지 올 수 있게 해주고 항상 옆에서 든든하게 응원해준 우리 가족인 아빠, 엄마, 언니에게 너무 고맙고 너무 사랑한다는 말을 전하겠습니다.

감사합니다.

2016. 02

김 소영 드림

PUKYONG NATIONAL UNIVERSITY 부경대학교