Journal of Korea Multimedia Society Vol. 21, No. 1, January 2018(pp. 26-33)
https://doi.org/10.9717/kmms.2018.21.1.026

결함 어골도 분석에 의한 모바일 결제 시스템의 보안성 개선에 관한 연구

서진호†, 박만곤††

A Study on the Security Improvement for Mobile Payment Systems by the Fault Fishbone Analysis

Jin-Ho Seo†, Man-Gon Park††

ABSTRACT

As financial transactions using mobile devices have been activated, mobile payment services have appeared and many changes have been made to the existing financial service methods. Due to the simplified payment method of mobile payment service, security threats such as personal information leakage, phishing damage, and malicious code are increasing. Research that can solve this is needed. In this paper, we discuss the features and security factors of mobile payment system. In order to improve the security of mobile payment system, we propose a fault analysis method based on frequency of occurrence using Fault Fishbone Analysis(FFA) technique.

Key words: Mobile Payment System, Security Improvement, Fault Fishbone Analysis

1. 서 론

무선 네트워크의 발달로 인해 스마트폰과 태블릿 PC 등과 같은 모바일 기기들이 빠르게 대중화되면서 시간과 장소에 구애받지 않는 모바일 결제 서비스가 확대되고 있다. 기존의 금융서비스와 IT가 결합된 모바일 결제 서비스는 사용자 측면에서의 편리성을 고려하여 결제 과정을 간소화하였고 모바일 기기 사용자라면 누구나 빠르고 간편하게 금융서비스를 제공받을 수 있다. 국내의 금융서비스산업은 그동안 정부의 규제로 인해 뒤쳐져있었지만 최근 해외 모바일 결제 시장의 급성장으로 국내에서도 관심이 높아지고 관련 기술 연구와 규제 완화의 움직임이 본격화되고 있다.

금융감독원은 이러한 모바일 결제 서비스의 등장에 따른 금융 서비스 경쟁력을 발전시키고자 사전 보안성심의 제도를 폐지하였다. 이로 인해 공인인증서를 이용한 사용자 인증절차가 생략되었고 결제 애플리케이션을 통한 정보 유출과 같은 문제가 제기되고 있어 보안에 대한 우려가 높아지고 있다[1].

또한, 3G, 와이파이 등의 경로로 보안을 위협하는 공격들이 침입하여 스마트폰에 저장된 개인정보 및 결제정보를 외부로 유출하려는 시도가 계속 증가될 것으로 예상된다. 해킹에 의한 정보 유출 및 공인인증서의 탈취, 역공학 공격을 통한 키 변조, 악성코드 감염을 통한 결제 정보 탈취 등으로 유출된 정보들은

※ Corresponding Author : Man-Gon Park, Address : (48513) 45 Yongso-Ro, Nam-Gu, Busan, Rep. of Korea, TEL: +82-51-629-6240, FAX : +82-51-629-6230, E-mail :mpark@pknu.ac.kr
Receipt date : Nov. 6, 2017, Approval date : Dec. 7, 2017

† Dept. of Information Systems, Graduate School, Pukyong Nat. Univ., Rep. of Korea
(E-Mail: seo41777@naver.com)
†† Dept. of IT Convergence and Application Engineering, Pukyong Nat. Univ., Rep. of Korea
††† This work was supported by a Research Grant of the Pukyong National University (Year 2017).

전자금융사고로 이어질 수 있다.

모바일 결제 서비스가 활성화 되기 위해서는 결제 과정의 편리함도 필요하겠지만 개인정보보호와 보안에 대한 사용자의 불안 요소를 줄일 수 있는 시스템 환경으로 운영되어야 한다. 또한 전자금융서비스의 보안 위협 및 요구사항과 보안성 평가를 위해 기준이 되는 체크리스트를 이용하여 시스템의 결함을 분석하여 개선하기 위한 연구가 필요하다.

이에 본 연구에서는 모바일 결제 시스템의 개념과 보안 요구사항에 대해 알아보고 결함 어골도 분석(Fault Fishbone Analysis; FFA)을 이용한 모바일 결제 시스템의 발생빈도별 결함을 분석하여 보안성을 개선하는 방법을 제시하고자 한다.

2. 모바일 결제 시스템

2.1 모바일 결제 시스템의 특징

모바일 결제 시스템은 모바일 기기를 사용하여 상품 및 서비스의 결제가 가능하게 해주는 시스템으로 본인 명의의 신용카드, 계좌이체 등과 같은 결제 정보를 애플리케이션을 이용하여 최초 등록한 후 결제 시 마다 추가 정보를 입력할 필요 없이 사용자 인증을 통해 결제할 수 있도록 해준다. 모바일 결제는 서비스를 출시한 회사의 기술에 따라 서비스 유형이 다양한데, 서비스를 출시 회사로는 은행, 카드사, 전자지급결제대행(Payment Gateway; PG)사, 소셜 플랫폼사, 포털 사이트 등이 있다.

모바일 결제 시스템은 온라인뿐만 아니라 오프라인에서도 이용할 수 있으며 다양한 환경의 웹브라우저, 디바이스, 운영체제에서도 결제가 되는 호환성을 제공하고 있어 언제, 어디서든지 간편한 결제가 이루어지도록 하는 시스템이다[2].

신용카드를 이용한 일반 결제 서비스를 보면 신용카드 결제 정보 입력, 공인인증서를 이용한 사용자 인증까지 번거롭고 복잡한 결제절차를 거치도록 되어 있다. 그에 비해 모바일 결제 서비스는 사용자가 등록한 결제 정보가 전자지급결제대행사에 암호화되어 저장되었다가 결제 시 정보를 불러와 공인인증서 없이 아이디와 비밀번호 또는 비밀번호와 같은 간단한 사용자 인증으로 결제된다[3].

2.2 모바일 결제 시스템의 보안 요구사항

모바일 결제 시스템의 보안을 유지하기 위한 요소로는 기밀성, 무결성, 인증, 부인방지, 가용성 등이 있다.

첫째, 기밀성으로 사용자의 카드정보 및 결제내역 등의 결제 정보는 보호되어야 한다. 금융기관과 사용자만이 데이터를 공유하고 공격으로부터 카드정보 및 결제내역 등의 결제정보를 보호하는 것으로 사용자와 서버간의 암호화 통신 기술을 적용할 수 있다. 둘째, 무결성으로 결제 정보가 변경되지 않았음을 보장할 수 있어야 한다. 사용자와 금융기관 사이에 모든 메시지는 개방된 네트워크로 인하여 위조 및 변조될 가능성이 있어 전송되는 정보가 비인가자에 의해 변조 되었는지 해쉬 기법으로 확인한다. 셋째, 인증으로 정상적으로 카드결제가 승인된다면 사용자는 올바른 사용자다. 금융 거래 시 정당한 사용자인지 확인하는 것으로 무결성으로 보장된 해시값에 의해 인증 및 안전한 통신 연결을 보장한다. 넷째, 부인방지로 사용자에 의해 발생한 거래에 대하여 부인할 수 없어야 한다. 송신자와 수신자간에 전송된 메시지에 대한 분쟁을 해결하기 위한 것으로 사용자 및 기관이 금융거래 사실을 부인할 수 없는 수단으로 제공한다. 다섯째, 가용성으로 인가된 사용자가 원할 때 언제든지 결제 서비스의 연속성은 보장되어야 한다. 인가된 사용자가 허가 받은 정보에 대해 방해받지 않고 원할 때에 언제든지 접근할 수 있는 것으로 금융서비스를 중단 없이 사용할 수 있도록 보장한다[4][5]. 아래의 Table 1은 모바일 결제 시스템의 보안 요구사항을 나타낸다.

Table 1. Security requirements for mobile payment systems

Type	Contents
Confidentiality	The payment information of the user's card information and payment history is protected.
Integrity	Ensure that the payment information has not been changed.
certification	If the payment is accepted normally, the user is the correct user.
non repudiation	The user can not deny the transaction that occurred.
Availability	Ensure continuity of payment service whenever user wants.

3. 관련연구

3.1 결함 트리 분석(Fault Tree Analysis; FTA)

FTA는 인적오류, 하드웨어 및 소프트웨어 오류,

환경적 요인 등과 같이 시스템의 고장을 야기 시키는 사건들간의 연관성을 밝히기 위해 사용되는 기법으로 시스템의 고장 원인과 위험을 진단하여 시스템 성능을 개선하여 다양한 문제를 해결하는데 사용된다[6].

FTA는 위험들을 평가 및 통제하기 위한 표준화된 훈련방식을 제공하고 시스템 레벨에서의 바람직하지 못한 사건을 발생시키는 인간 오류, 하드웨어, 소프트웨어 등을 결정하여 결함 트리 다이어그램으로 나타낸다. 바람직하지 않은 정상사상(top event)을 시작으로 발생 원인과 발생 원인에 기여한 요소들을 찾아 시간적 흐름을 거슬러 분석하는 연역적 구조로 정상사상의 발생 확률을 예측하여 정상사상의 발생에 영향을 주는 원인을 파악한다. 정성적인 분석과 정량적인 분석이 가능하며 부울 대수로 수학적 논리를 나타낸다. 아래의 Table 2는 FTA에 사용되는 기호를 나타낸다[7].

Table 2. FTA diagram symbols

Symbol		Function
Event		Treated as a primary cause with no further resolution.
Basic Event		Basic error events that would not require the further development.
Undeveloped Event		An event which is no further developed.
In		If lines are coming to the top of the triangle, mean the transfer from other parts.
Out		If lines are coming from the side, means move out to other parts.
AND gate		Logic gate when all sub cases are satisfied.
OR gate		Logical gate when one of the sub-events is satisfied.

아래의 Fig. 1은 FTA를 이용한 결함 트리 분석의 예를 나타낸다. FTA는 정상사상을 설정하고 1차 원인과의 관계를 놀리 게이트로 연결하여 그 1차 원인에 대해 분석한 후 더 이상 분할 할 수 없는 기본 사상까지 반복해서 분석한다.

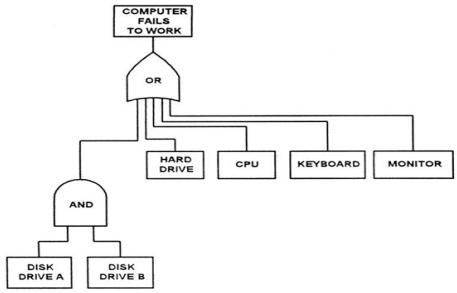


Fig. 1. Example of fault tree analysis using FTA.

3.2 결함 어골도 분석(Fault Fishbone Analysis; FFA)

FFA는 기존의 FTA에서 사용된 결함 트리에서 결함의 확률만 표현하는 한계를 극복하여 정규화 위험 우선순위 값 NRPV(Normalized Risk Priority Value)에 의한 치명도(Criticality)를 적용한 어골도(Fishbone)로 도식한다. 원인과 결과를 분석(Cause and Effect Analysis)하여 근본적인 원인을 찾는 방법으로 NRPV에 의한 치명도는 오른쪽 정상 사상에 가까울수록 높은 사상으로 배치한다. FTA와 마찬가지로 전체 집합의 부분 집합을 찾아가는데 유용한 도구로 본질적으로는 마인드 맵(mind map)이나 로직 트리(logic tree)와 같다. 아래의 Table 3은 FFA에 사용되는 기호를 나타낸다[8].

Table 3. FFA diagram symbols

Symbol		Function
Event		An event caused by a combination of events through the logic gate.
Basic Event		Basic error events that would not require the further development.
Undeveloped Event		An event which is no further developed.
In		If lines are coming to the top of the triangle, mean the transfer from other parts.
Out		If lines are coming from the side, means move out to other parts.
AND gate		Logic gate when all sub cases are satisfied.
OR gate		Logical gate when one of the sub-events is satisfied.

아래의 Fig. 2는 FTA를 이용한 결함 분석의 예를 나타낸다. 머리에서 꼬리로 이어진 주 골격을 중심으로 갈라져 나온 뼈대들에는 문제를 일으키는 각각의 원인들을 나열하고, 그 원인들의 원인을 찾는 방법으로 근본적인 원인을 찾는다[9].

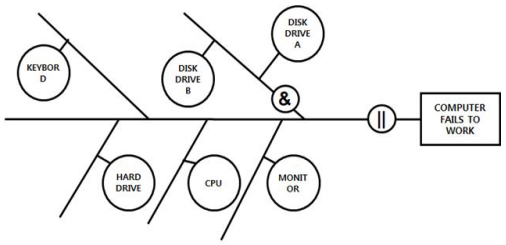


Fig. 2. Example of fault analysis using FFA.

4. 모바일 결제 시스템의 결함분석과 보안성 개선

4.1 모바일 결제 시스템의 기능 블록 다이어그램

모바일 결제 시스템은 크게 사용자 인증기관(User Authorities), 결제 관리(Payment management), 이상거래탐지 및 통제(Abnormal transaction detection and control)로 구성된다. 사용자 인증기관은 결제 단말기, DB 서버, 사용자 인증 시스템으로 구성되는데, 결제 단말기에서 결제카드를 인식하여 DB 서버를 통해 사용자의 정보를 저장하고 사용자 인증 시스템에서 사용자의 정보를 식별한다.

결제 관리 시스템은 키 관리, 애플리케이션 관리, 카드 관리로 구성되는데, 키 관리는 애플리케이션 관리와 카드 관리를 위해 요구되는 키에 대한 프로파일을 생성하고 관리하는 서버이다. 애플리케이션 관리는 애플리케이션의 추가 및 제거, 정보 조회 및 발급 처리 등의 프로세스를 관리한다. 카드 관리는 카드 발급, 데이터 입력 및 출력, 카드 형식 등의 프로세스를 관리한다[10].

이상거래 탐지 및 통제는 거래 내역 관리, 환불 내역 관리, 통합 애플리케이션 관리로 구성되는데 거래 내역 관리에서 거래 자료를 수집하고 분배 정산을 처리하며, 환불 내역 관리에서는 환불 내역 자료를 수집하고 수수료 지불 내역을 정산 처리한다. 아래의 Fig. 3은 모바일 결제 시스템의 기능 블록 다이어그램을 나타낸다.

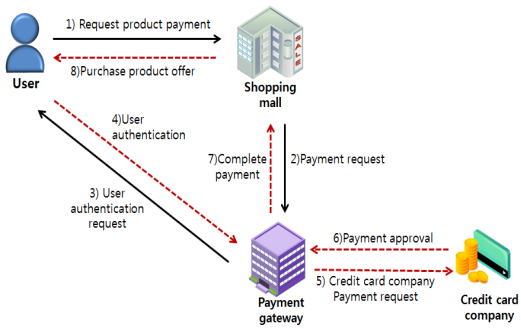


Fig. 3. Function block diagram for mobile payment systems

4.2 모바일 결제 시스템의 결함 리스트

아래의 Table 4는 모바일 결제 시스템의 기능 블록 다이어그램을 기반으로한 결함 리스트를 나타낸다. 추출 초반부에는 예상 기능별 결함을 리스트로 작성하여 사용하지만 운영과 시험을 거치면 보다 더 실제적이고 자세한 결함 리스트들을 구할 수 있다.

Table 4. Functional fault list of mobile payment systems

System		Function	Functional Fault
User authentication	Payment terminal	Recognizing payment card	Terminal operation error
	DB server	Saving user information	DB server error
	User authentication system	Identifying user information	User authentication error
Payment management	Key management	Definition of key values	No user transactions, User transaction history error, User authentication error
		Key process management	No user transactions, User transaction history error, User authentication error
	Applications management	Definition of applications	Card payment error
		Adding and removing applications	Card payment error
		Checking application issue information	Card payment error, No user transactions
	Card management	Issue request processing	Card payment error, No user transactions
		Card issuance process	Card issuance error
		Input and output of data	User data error
		Definition of Card Type and Type	Card payment error
Abnormal transaction detection and control	Transaction history management	Collection of transaction data	User transaction history error
		Distribution	User transaction

		settlement processing	history error
	Refund history management	Collection of refund history data	User transaction history error
		Settlement of fee payment	User transaction history error
	Integrated applications management	Security tool	User transaction history error
		Maintenance system	User transaction history error

4.3 발생 빈도(Occurrence)에 의한 FFA

모바일 결제 시스템의 결함 리스트를 FFA기법으로 분석하여 발생빈도를 계산하였다. 기본 사상의 발생확률은 기본사상의 오류 개수/전체 오류개수이고, 중간 사상의 발생확률은 기본사상의 OR 결합으로, 본 연구에서는 Noisy-OR gate를 사용하여 확률 F의 값을 결정한다. Noisy-OR gate에서 x_i는 원인, F_i를 x_i만 나타나고 나머지 원인은 나타나지 않았을 때, 결과를 나타날 확률 F는 다음과 같다[11].

$$F = 1-[1-F_1] \cdot [1-F_2] \cdot \cdots \cdot [1-F_n]$$
$$= 1-\prod_{i=1}^{n}(1-F_i)$$

아래의 Table 5는 모바일 결제 시스템의 결함 발생 빈도는 나타내는 것으로 Payment management의 중간 사상인 Key management의 발생 빈도는 다음과 같다.

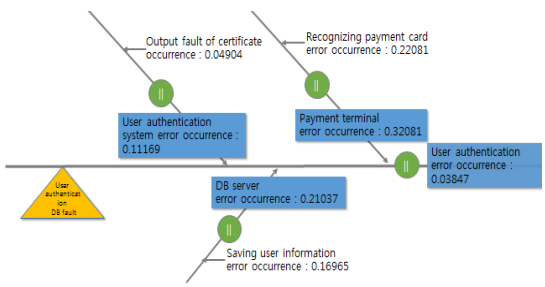
$$F = 1-[1-0.05668] \cdot [1-0.05890]$$
$$= 0.11224$$

Table 5. Occurrence for of mobile payment systems

System		Function	Functional Fault	Occurrence
User authentication (0.03847)	Payment terminal	Recognizing payment card	Terminal operation error	0.22081
	DB server	Saving user information	DB server error	0.16965
	User authentication system	Identifying user information	User authentication error	0.04904
Payment management (0.20336)	Key management (0.11224)	Definition of key values	No user transactions, User transaction history error, User authentication error	0.05668
		Key process management	No user transactions, User transaction history error,	0.05890
			User authentication error	
	Applications management (0.05630)	Definition of applications	Card payment error	0.01089
		Adding and removing applications	Card payment error	0.01886
		Checking application issue information	Card payment error, No user transactions	0.02757
	Card management (0.04913)	Issue request processing	Card payment error, No user transactions	0.04353
		Card issuance process	Card issuance error	0.00145
		Input and output of data	User data error	0.00435
		Definition of Card Type and Type	Card payment error	0.00007
Abnormal transaction detection and control (0.34821)	Transaction history management (0.07462)	Collection of transaction data	User transaction history error	0.00007
		Distribution settlement processing	User transaction history error	0.07456
	Refund history management (0.16075)	Collection of refund history data	User transaction history error	0.00703
		Settlement of fee payment	User transaction history error	0.15481
	Integrated applications management (0.16074)	Security tool	User transaction history error	0.00713
		Maintenance system	User transaction history error	0.15471

모바일 결제 시스템의 내부 시스템별 발생빈도에 의한 FFA는 Fig. 4와 같다.

각 시스템별 정상사상 발생 확률을 통합하여 모바일 결제 시스템의 정상사상 발생 빈도를 계산하면 Table 6과 같다.



(a)

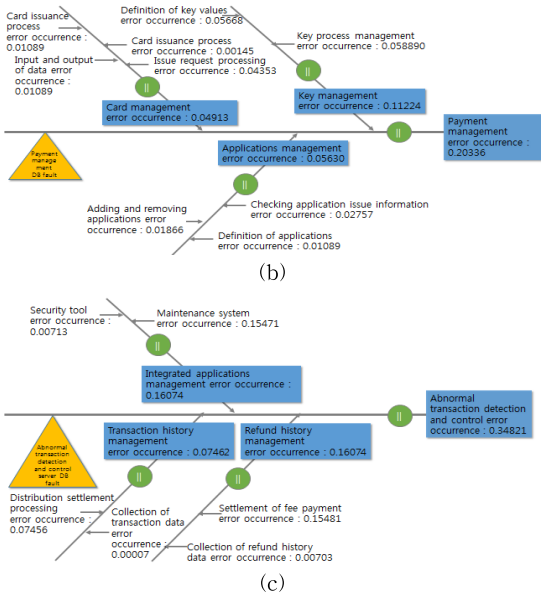


Fig. 4. FFA by (a) User authentication error occurrence, (b) Payment management error occurrence, and (c) Abnormal transaction detection and control error occurrence

Table 6. Occurrence of top event for mobile payment systems

Ranking	Top Event	Occurrence
1	User authentication error	0.03847
2	Payment management error	0.20336
3	Abnormal transaction detection and control error	0.34820

모바일 결제 시스템의 시스템별로 발생 빈도에 의한 User authentication, Payment management, Abnormal transaction detection and control을 통합한 모바일 결제 시스템의 발생빈도에 의한 FFA는 Fig. 5와 같다.

4.4 모바일 결제 시스템의 보안성 개선

Table 7은 모바일 결제 시스템의 실험 결과를 제시한 것으로 1차, 2차의 개선 지시에 따라 결함 발생 확률이 개선되는 가상의 예를 나타낸다. 개선율은 (개선 전 Occurrence - 개선 후 Occurrence) ÷ (개선 전 Occurrence)를 이용하여 구하였으며 개선 차수가 높아짐에 따라 최고 43.31%까지 보안이 개선되는 것을 알 수 있다.

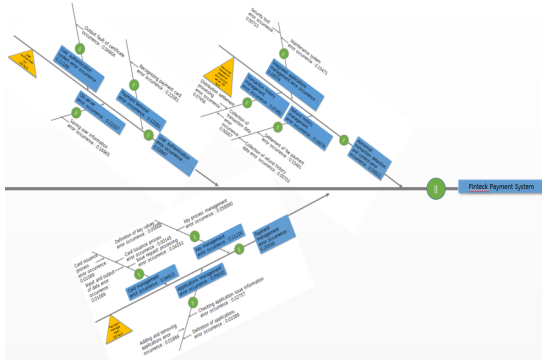


Fig. 5. FFA by mobile payment system error occurrence.

Table 7. Improved results of mobile payment systems by following the instructions of improvement

System	RPN parameter / Degree of improvement	Occurrence	Improvement rate	
			Improvement comparison	First comparison
User authentication	Before first improvement	0.03847	-	
	After first improvement	0.02798	27.27%	27.27%
	After second improvement	0.02181	22.05%	43.31%
Payment management	Before first improvement	0.20336	-	
	After first improvement	0.16013	21.26%	21.26%
	After second improvement	0.12714	20.6%	37.48%
Abnormal transaction detection and control	Before first improvement	0.3482	-	
	After first improvement	0.2657	23.69%	23.69%
	After second improvement	0.2185	17.76%	37.25%

5. 결 론

모바일 결제는 기존의 금융기관에서 공인인증서를 통해 제공해오던 결제 서비스를 사용자 입장에서 간소화하고 편리성을 발전시킨 것이라고 할 수 있다. 이러한 모바일 결제 방식은 기술적 측면과 관련 제도의 정비, 사용자 정보보호, 시스템의 안전성 분석 등 종합적인 시각으로 접근하고 개발 및 유지가 되어야 한다. 모바일 결제 시스템의 편리성으로 사용자가 점차 늘어가고 있으나 최근 들어 해외에서 대량의 정보 유출 사례가 계속해서 발생하고 있으며, 피해는 개인 사용자, 신용카드 결제서비스 사업자, 유통 업체 등 다양하게 퍼지고 있어 보안성 개선이 더욱 필요한

실정이다. 이에 결제 과정의 편리함을 보장해 줄 수 있는 보안 요소들이 반영되어 운영되어야 하고 이러한 보안성 평가의 기준이 되는 검토항목에 대한 연구가 필요하다.

모바일 결제 시스템의 보안성을 평가하기 위해서는 다양한 결함 분석 방법이 사용될 수 이루어 질 수 있으나 본 논문에서는 결함 어골도 분석을 이용하여 모바일 결제 시스템의 보안성을 평가하고 개선하는 기법을 제안하여 개선 차수가 높아짐에 따라 최고 결함발생확률의 개선율 43.31%에 도달됨을 보여주었다.

이에 모바일 결제 시스템의 보안성을 평가하기 위한 다양한 결함 분석 기법들간의 상호 보완적인 조합을 연구하고 분석하여 모바일 결제 시스템의 활성화를 위한 시스템의 안전성과 무결성을 보장할 수 있는 방안에 대한 연구가 필요할 것이다.

REFERENCES

[1] H. Yu, *A Study on Developed Security Check Items for Assessing Mobile Financial Service Security*, Master's Thesis of Chung-Ang University, 2017.

[2] E. Teo, B. Fraunholz, and C. Unnithan, "Inhibitors and Facilitators for Mobile Payment Adoption in Australia: A preliminary Study," *Proceeding of the International Conference on Mobile Business,* pp. 663-666. 2005.

[3] D. Kim, *An Easy Payment System Model with Using Mobile Devices,* Doctor's Thesis of Honam University, 2016.

[4] H. Choi and H. Kim, *Secure Mobile Credit Card Payment Protocol Based on Certificateless Signcryption*, Master's Thesis of Korea University, 2013.

[5] K. Nam, *A Study on the Mobile Credit Card Payment Protocol Based on Secure MicroSD Card and Certificateless Signcryption*, Master's Thesis of Soongsil University, 2015.

[6] E.J. Hemly and H. Kumamoto, *Reliability Engineering and Risk Assessment,* Prentice Hall, New Jersey, 1981.

[7] M. Kim, E. Jin, and M. 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.

[8] S. Jang, *A Study on the Fault Analysis and Security Assessment for Smart Card Management System,* Doctor's Thesis of Pukyong National University, 2014.

[9] H. Chang, "Evaluation Framework for Telemedicine Using the Logical Framework Approach and a Fishbone Diagram," *Healthcare Informatics Research*, Vol. 21, No. 4, pp. 230-238, 2015.

[10] P. Nam, *A Study on the Fault Tree Analysis Methods for the Security Evaluation of Fintech Payment Systems*, Master's Thesis of Pukyong National University, 2017.

[11] A. Oniśkoa, M.J. Druzdzelb, and H. Wasyluk, "Learning Bayesian Network Parameters from Small Data Sets: Application of Noisy-OR Gates," *International Journal of Approximate Reasoning,* Vol. 27, Issue 2, pp. 165-182, 2001.

서 진 호

부산외국어대학교 (경제학사)
부경대학교 교육대학원 전산교육 전공(교육학석사)
부경대학교 대학원 정보시스템학과(박사과정 수료)
관심분야 : 모바일 결제 시스템, 소프트웨어 안전성 및 보안성 공학, 멀티미디어기술

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 (콜롬보플랜기술교육대학교) 사무총장 (Director General and CEO)
2004년~2007년 Asia-Pacific Accreditation and Certification Commission (아태지역 인증검증위원회) 위원장
2005년~현재 유네스코 (UNESCO-UNEVOC) 자문위원, 아시아개발은행(ADB) 자문관
관심분야 : 소프트웨어 공학 및 재공학, 소프트웨어 신뢰성공학, 소프트웨어 안전성 공학, 비즈니스 프로세스 재공학 (BPR), ICT-기반 HRD, 전자정부 및 전자교수학습 시스템 구축