IC카드 지불결제 시스템의 보안성 평가를 위한 고장트리 분석(FTA)과 고장유형과 영향 분석(FMEA)

김명희[†], 진은지^{††}, 박만곤^{†††}

요 약

IT융합 응용 기술의 발전으로 스마트 디바이스들의 활용이 증대되고 있고 지불결제 시스템에서도 스마트 IC카드의 사용이 급증하고 있다. 또한 무선 이동통신기술과 멀티미디어 처리 기술의 발전에 따라 언제 어디서나 IC카드 지불결제 시스템의 사용이 요구되고 있다. 이에 IC카드 지불결제 시스템의 보안성(security) 역시 중요한 이슈로 떠오르고 있다. IC카드 지불결제 시스템들과 같은 정보 시스템의 보안성을 평가하기 위한 여러 가지 결함 분석 기법들이 있다. 그러나 IT융합 응용 기술이 확대 발전함에 따라 정보 시스템의 종류와 특성이 다양해지면서 단지 하나의 시스템 보안성 평가 방법으로는 적절한 분석이 이루어 질 수 없다. 따라서 본 논문에서는 IC카드 지불결제 시스템의 보안성을 평가하기 위해서 두 가지 중요 결함 분석 기법인 결함 트리 분석(Fault Tree Analysis; FTA) 기법과 치명도(Criticality)기반의 고장모드별 영향 분석(Fault Modes and Effect Analysis/Criticality; FMEA/C)기법을 통합하여 사용함으로써 IC카드 지불결제 시스템의 결함 분석을 수행하여 보안성을 평가하고 개선하는 방법을 제안한다.

Fault Tree Analysis and Fault Modes and Effect Analysis for Security Evaluation of IC Card Payment Systems

Myong-Hee Kim[†], Eun-Ji Jin^{††}, Man-Gon Park^{†††}

ABSTRACT

The demands of IC card payment system has been increased according to the rapid advancement of the IT convergence application technologies. Recently IC card payment systems are in demands of the usage space at anytime and anywhere by developing the wireless communication technology and its related multimedia processing technology. Therefore the security of IC card payment system becomes more important and necessary. There are many fault analysis methods to evaluate the security and safety of information systems according to their characteristics and usages. However, the only assessment method to evaluate the security of information systems is not enough to analyse properly on account of the various types and characteristics of information systems by the progress of IT convergence and their applications. Therefore, this paper proposes an integrative method of the Fault Tree Analysis (FTA) and Fault Modes and Effect Analysis/Criticality (FMEA/C) based on criticality to evaluate and improve the security of IC card payment system as an illustration.

Key words: 결함트리분석(Fault Tree Analysis), 고장유형과 영향분석(Fault Modes and Effect Analysis), IC카드 시스템 (IC Card System or Smart Card System), 보안성 품질 개선(Security Quality Improvement)

※ 교신저자(Corresponding Author) : 박만곤, 주소 : 부산광역시 남구 대연 3동 부경대학교 대연캠퍼스 1호관(웅비관) 1308호실(608-737), 전화 : 051) 629-6240, FAX : 051) 628-6155, E-mail : mpark@pknu.ac.kr
접수일 : 2012년 8월 22일, 수정일 : 2012년 9월 29일
완료일 : 2012년 11월 8일

[†] 정회원, 부경대학교 교육대학원 전산교육전공
(E-mail : mgold@naver.com)

^{††} 준회원, 부경대학교 대학원 첨단 정보과학 및 정보기술학과
(E-mail : melissaly@naver.com)

^{†††} 종신회원, 부경대학교 공과대학 IT융합응용공학과
※ 이 논문은 2011학년도 부경대학교의 지원을 받아 수행된 연구임(PK-2011-2-32).

1. 서 론

오늘날 IT융합 (IT Convergence) 기술의 발달에 따라 내장 소프트웨어 (Embedded Software)의 사용이 확대되고 있으며 이제 대다수의 하드웨어 시스템들은 내장 소프트웨어들에 의해서 운영되어지고 있는 추세이다. 이에 따라 하드웨어에 내장된 소프트웨어 시스템이 정상적으로 동작 하는지에 대해서 대단히 민감한 안전과 보안 중심 소프트웨어 시스템들 (Safety and Security-Critical Software Systems)을 중심으로 하드웨어 또는 소프트웨어의 결함으로 인한 사고 또는 재난 발생을 예방하기 위한 시스템들의 보안성 평가와 개선방법에 대한 관심이 증가하고 있다. 현재 운영 중인 대다수의 시스템들이 안전과 보안을 보장해 줄 수 있는가에 대한 사람들의 신뢰는 낮아지고 있고 그에 따라 소프트웨어 공학자들은 이런 안전 및 보안 중심 소프트웨어 시스템들을 사고와 재난들로부터 안전성과 보안성을 확보하기 위해서 보다 개선된 방법을 찾기 위해서 노력하고 있고 그 대책들을 마련하고 있다[1-4].

안전과 보안 중심 소프트웨어 시스템들 중의 하나인 소프트웨어를 내장한 IC칩을 사용하고 있는 IC카드시스템은 현재 다양한 분야에서 지불결제 도구로 사용되어 이를 활용한 지불결제 시스템들이 지하철, 버스, 택시 등의 교통 서비스 시스템과 소액결제에 필요한 유통 서비스 시스템을 중심으로 T머니, 마이비, 하나로 카드 등과 함께 활용되고 있으며 다른 분야로 점차 확대 사용되어지고 있는 추세이다. 그러나 유비쿼터스 시대를 맞이하여 국민의 안전과 편익을 보장할 수 있는 IC카드 지불결제 시스템의 기반을 마련하고자 공공분야 IC카드의 플랫폼 표준화 추진을 위해 많은 연구를 수행하고 있지만 이를 실제로 차세대 전자금융산업을 추진하기 위해 적극적으로 연구하거나 활용하는 사례가 거의 없는 실정이다. 교통수단 및 유통산업을 통합하여 지불 결제하는 모델이 없으며, 사용자들의 보다 폭 넓은 활용요구에 대한 대책을 마련하지 못하고 있는 실정이다. 따라서 이러한 교통수단과 유통산업을 포함한 전 결제시스템에서 사용가능한 통합 IC카드를 이용한 전자지불결제 시스템을 개발하여야 할 필요성이 증대되고 있다.

그러나 이들 통합 IC카드를 이용한 전자 지불결제 시스템을 구축하여 사용을 확대하는 데에는 선결과

제가 있다. 이는 안전성과 보안성 평가(Safety and Security Evaluation)를 통하여 전자 지불결제시스템의 안전성과 보안성의 보증 (Assurance of Safety and Security)이 그것이다. 만약에 통합 IC카드를 이용한 통합 전자지불결제 시스템에 안전성과 보안성이 확보되지 못하면 엄청난 사회적인 문제를 야기하여 지불결제를 중심으로 금융질서를 교란시키는 심각한 재난이 발생할 수가 있다.

안전성이란 사고나 재난으로부터 자유로운 상태라고 정의할 수 있는데, 소프트웨어 시스템의 경우 소프트웨어가 개발될 때 내재해 있는 결함들이나 결함이 없다고 하더라도 외부로부터의 잘못된 입력이나 운영으로부터 시스템을 안전하게 지켜 주고, 사고 또는 재난의 발생을 막기 위한 통제 수행 가능성에 관심을 갖는 것을 말한다. 이와 관련하여 신뢰성과 안전성은 소프트웨어에 있어서는 매우 유사한 개념으로 사용되었으나 최근에는 그 개념이 분리되는 추세에 있다. 신뢰성은 특정한 환경 조건에서 준비된 기능이 특정 시간 내에 바르게 수행될 수 있는지에 대한 가능성을 말하는 것이라면, 안전성은 내부의 잠복 결함이나 외부에서의 잘못된 입력으로부터 사고나 재난이 일어나지 않도록 하는 조건과, 계획된 안전관련 기능이 제대로 수행될 가능성을 말한다[5,6].

이처럼 많은 시스템들에 내장된 소프트웨어의 안전성과 보안성에 대하여 사람들의 관심이 높아짐으로써 개발되고 있거나, 양도되어지거나, 사용 중인 내장 소프트웨어를 탑재한 시스템이 안전성과 보안성을 확보하고 있다는 보증이 필요하게 되었다. 따라서 소프트웨어 시스템이 가지고 있는 안전성과 보안성에 관련한 결함들을 분석함으로써 안전성과 보안성을 보증하거나, 발견된 결함을 제거하여 안전성과 보안성을 개선하는 기법에 관하여 보다 심도 있는 연구가 필요하다. 이는 안전성과 보안성 확보의 실패는 인간의 생명 또는 사회 시스템의 붕괴와도 관계가 있기 때문이다[5,6].

시스템의 보안성의 결함 분석 기법으로는 상태 기반 접근법의 Markov 분석, 표 기반 접근법의 고장모드별 영향 분석(Fault Modes and Effect Analysis; FMEA), 매개변수 기반 접근법의 결함 및 운영가능성 분석(Hazard and Operability Studies; HAZOP) 그리고 트리 기반 접근법의 결함 트리 분석(Fault Tree Analysis; FTA) 등이 주로 사용되고 있다. 본

논문에서는 시스템의 보안성 평가를 위해서 결합트리분석(FTA)을 바탕으로 하여 치명도 (Criticality)를 중심으로 고려하는 FMEA/Criticality분석 기법에 대해 초점을 둔다[5,6].

또한 소프트웨어 안전성 평가를 위한 소프트웨어 고장모드별 영향 분석에 관한 연구[5]에서는 내장된 또는 탑재된 소프트웨어 시스템의 크기가 비교적 작으며, 시스템 제어에 있어서 실시간 반응 시간에 민감하지 않는 안전중심 시스템들의 소프트웨어 안전성 평가를 수행하여 FTA와 FMEA를 결합한 소프트웨어의 결합분석 방안을 제안하고 유비쿼터스 헬스케어 시스템을 이용하여 사례연구를 수행하였다. Thomas Maier의 “안전성과 보안성에 핵심을 둔 시스템에 있어서 내장된 소프트웨어의 안전성 설계 지원을 위한 FMEA와 FTA” 연구에서는 FMEA를 통하여 아주 복잡한 제어 소프트웨어 내부의 가능한 모든 오류를 조직적으로 확인하고, 각각의 소프트웨어 요구사항의 모든 가능한 방법의 설정에 의하여 이러한 실패는 치유될 수 있고, 결합 트리의 구축을 통하여 완성될 수 있다고 하였다. 이 방법론은 전술한 목표들을 넘어서 안전 및 보안 필수 시스템의 설계자들을 위하여 안전성과 관련한 피드백을 준비할 수 있는 환경을 제시하고 있다. 그러나 이러한 결합 분석 기법들이 모든 시스템에서 그대로 적용될 수 있는 것은 아니며, 안전성과 보안성 관련 부품이나 시스템의 특성과 크기에 따라 가장 적절한 방법으로 활용되어야 할 것이다[7-15]

따라서 본 논문에서는 내장 소프트웨어들을 사용하는 IC카드시스템을 바탕으로 하는 통합 전자지불결제 시스템의 고장 원인과 고장메커니즘의 분류, 결합 트리 분석 방법의 적용, 보안성 평가를 위한 소프트웨어 및 하드웨어의 치명도 기반 고장 유형 및 영향 분석 방법의 적용을 중심으로 종래의 하드웨어 안전성 평가에서 보다 효율적인 소프트웨어를 포함

하는 통합시스템의 결합 분석 기법들의 실제적인 결합 보안성 평가 프로세스를 정의하고 그에 따른 실험적인 결과 분석을 수행한다.

2. 스마트 IC카드와 IC카드 지불결제 시스템

2.1 스마트 IC카드 및 IC카드 관리 시스템

IC카드(또는 스마트 IC카드)는 내장된 집적회로를 가진 포켓 크기의 카드를 말한다. IC카드에는 그림 1에서처럼 마이크로 프로세스[MPU], RAM, ROM 및 Flash와 같은 휘발성 기억장치들을 포함하고 있다. 또한 IC카드에는 양방향 무선 통신이 가능한 루프 안테나가 운영되어지고 있다.

IC카드에는 전기를 생성하는 유도 코일 및 콘덴서가 내장된 플라스틱 카드이다. IC카드 판독기는 항상 IC카드의 무선 통신 시스템으로 전파를 보낸다. IC카드와 IC카드 리더기 사이의 거리가 10cm정도가 되면 전파가 유도 코일에 충분한 전기를 생성 후 콘덴서로 저장할 수 있다. IC카드에는 이 전기를 사용하여 IC카드 판독기에 IC카드 메모리칩의 시리얼 번호를 보낸다. IC카드에는 IC카드 소지자에게 IC카드 관리 시스템에 대한 보안 요구 사항을 인증하는 보안 자격 증명 때문에, IC카드에는 안전한 전자 증명의 기반을 제공하고, 칩 운영체제(Chip Operating System)아래 각 장치, 네트워크 또는 컴퓨터에 대한 접근을 제어하는데 사용될 수 있다.

IC카드 관리 시스템은 도둑이나 물리적 손상 등의 손실의 경우 카드를 대체할 수 있는 보험과 같은 관리를 하는 시스템을 말한다. IC카드 관리 시스템은 세 가지 부분으로 나누어 질 수 있다. 이는 논리적 영역으로서 카드 관리 부분, 어플리케이션 관리 부분, 키 관리 부분으로 구성되어진다. 카드 관리 부분은 주로 카드 발행자의 필요성과 연관된다. 이는 카

그림 1. 스마트 IC카드의 구조

드 구조에서 카드의 전체적 기본적 사항과 각각의 카드를 관리하기 위한 것이다. 어플리케이션 관리 부분은 카드 상에서 특별한 어플리케이션 데이터의 전체적 어플리케이션 발행자를 지지한다. 키 관리 부분은 특정한 암호화된 키로 전체적 카드 과정에서 카드 발행자와 어플리케이션 발행자가 모든 카드나 어플리케이션을 생성하거나 관리하는 것을 허락하는 부분이다. 카드 관리 영역의 발행 과정은 어플리케이션 데이터를 카드로 적재하는 것이다. 예를 들면 디지털 서명과 홍채, 지문, 피부를 이용한 생체 인식 시스템이 있다. 카드 대체 활동은 카드가 이용 가능한 시설에서 카드의 손실이나 유실의 경우 이루어진다.

2.2 IC카드 지불결제 시스템

IC카드를 이용한 통합 전자 지불결제 시스템의 모듈들은 충전과 환불이 가능하도록 확장성을 고려하여 단위모듈들(서브시스템들)로 개발이 되도록 했다. IC카드 지불결제 시스템은 크게 수집 및 정산 시스템, 충전 및 환불 시스템, 카드 관리 시스템으로 구성되고 각 시스템의 모듈마다 내부연계와 외부연계는 실시간 및 일괄처리로 구성되어야 한다.

그림 2는 IC카드 수집 및 정산 시스템의 사례로서 IC카드 이용자가 IC카드 지불결제 단말기에서 이용한 지불자료인 거래 자료와 사용자충전 거래 자료를 수집하여, 해당 지불자료에 대한 분배 정산을 처리하는 과정을 보이고 있다. 즉, 수집 및 정산 시스템은 예를 들어 가맹점인 버스 운수사와 도시 철도 공사를 통하여 자료를 수신하고 이를 통해 정산시스템을 거쳐 데이터를 처리한다. 결제가 이루어져 정산이 완료된 데이터는 타 카드 거래나 해당 통합카드의 거래

그림 2. 수집 및 정산 시스템 구성도의 예

별로 데이터를 추출하고 이를 다시 최종적으로 해당 연계기관인 선불 카드사, 은행, 신용카드사와 VAN에 자료를 취합하여 전달한다. 해당 연계기관은 수집 및 정산 시스템의 거래 자료를 바탕으로 통계 및 대금결제가 이루어진다. 그림 3은 IC카드 충전 및 환불 시스템은 충전 및 환불 내역을 관리하며 해당 충전 및 환불 내역에 대한 수수료 지불 내역을 정산 처리하는 충전환불 시스템이다. 크게 이용자의 충전과 환불, 충전 거래점과의 충전과 환불 대행사와의 환불로 이루어진다. 또한 이는 충전 거래점에서 충전 및 환불 시스템에 LSAM 충전을 시행하며 금융기관에 사용자 충전 거래 자료와 CMS 거래를 요청하여 환불을 하는 시스템이다.

또한 그림 4에서처럼 IC카드 관리시스템은 통합 카드의 전자화폐의 개발 및 각종 PerSAM, LSAM/PSAM 등의 개발과 KMS(키 관리 시스템)을 통한 HSM의 키 생성, 각종 카드 발급, 거래기록 인증, LSAM 거래인증의 역할을 수행한다. IC카드 관리 시스템은 통합 IC 전자지불결제 시스템의 업무담당자가 카드운용 및 카드재고관리를 위해, 발주 및 입고 처리기능을 수행하고, 요청되는 사용자카드를 위해 발급 및 배포업무를 처리한다.

그림 3. 충전 및 환불 시스템 구성도의 예

3. 보안성 평가를 위한 결함 분석 기법들

FTA는 결함들을 트리 구조에 의해 표현하므로 시각적으로 우수한 표현 수단이며 FMEA/C에서 얻은 고장유형과 영향을 사용하면 더욱 상세하게 주요 원인을 논리적으로 분석할 수 있기 때문에 본 연구에서는 보안성 평가를 위하여 결함 트리 분석(Fault Tree

그림 4. 카드 관리 시스템 구성도의 예

Analysis; FTA)과 치명도 기반 고장 유형과 영향 분석(Failure Modes and Effect Analysis/Criticality; FMEA/C)을 다루고자 한다.

3.1 결함 트리 분석 (FTA)

결함 트리 분석 기법은 시스템 안전분석의 대표적 기법으로서 1962년 미국 벨연구소에서 개발되었다. FTA는 미사일 발사 제어시스템에서의 우발사고의 예측을 하는 기법으로써 후에 보잉사에 의해 컴퓨터를 사용하는 시뮬레이션이 가능한 항공 우주산업과 원자력산업을 시작으로 산업안전 분야에 넓게 사용되었다. FTA는 시스템의 고장 원인을 top-down 방식으로 추리해 가는 로직 다이어그램을 사용하기 때문에 보안성 관련 기능들의 결함들을 결함 트리의 형태로 만들어서 시스템의 고장 확률을 구하고 취약 부분을 찾아내어 시스템의 신뢰도를 개선하는 정량적인 보안성 평가 기법이다. FTA는 AND와 OR의 두 종류의 논리 게이트 조합에 의해 표현하므로 시각적으로 표현이 우수하다. 표 1은 결함 트리의 주요 기호들과 그 기능을 요약 설명하고 있다.

3.2 치명도 기반 고장 유형과 영향 분석(FMEA/Criticality)

치명도 기반 고장 유형과 영향 분석은 FMEA에서 치명도(Criticality)라는 것이 추가되어 FMEA를 치명도 중심으로 파악하기 위한 결함 분석 기법이다. 실패가 발생하기 이전에 실패들을 제거하고 위험을 최소화하기 위해서 잠재적 실패 요인들을 파악해서 제거해서 시스템의 보안성을 제고하는 기법으로 원래는 정성적 보안 예측 기법이었다. 이에 따라서 FMEA/C를 통하여 최종적으로 보안성을 향상할 수 있다. 일반적으로 FMEA는 프로세스 내의 고객 요구 사항을 만족하는데 장애가 될 수 있는 고장 유형의 형태를 모두 명시하고, 고장과 연계된 특정한 원인에 대한 위험 요소를 추정하는 용도, 고장 발생 원인을 제거하기 위한 현재의 관리 방법을 평가는 용도, 공정을 개선하기 위해 조치 내용의 우선순위를 정하는 용도, 지속적으로 유지 관리하기 위해 관리 항목을 도출하고 구분 및 관리하는 용도로 사용된다. FMEA/C의 수행은 모든 가능한 실패 모드를 알아내는 것으로 시작된다. 결함 모드의 발견에 따라 모든

표 1. 결함 트리의 주요 기호

기 호	기 호 명	설 명
	• 사상(Event)	• 논리 게이트를 통해 사건들의 통합으로 생겨난 사상을 나타내는 기호
	• 기본 사상(Basic Event)	• 더 이상 발달을 요구하지 않는 기본적인 오류 사상을 나타내는 기호
	• AND 게이트	• 하위의 사상을 모두 만족하는 경우에 사용하는 논리 게이트
	• OR 게이트	• 하위의 사상 중 하나라도 만족하면 사용하는 논리 게이트

표 2. FMEA/C의 치명도, 발생도 및 검출도 값의 범위

	값의 범위
치명도(C) (Criticality)	$0 \leq C < 1.0$: 치명도가 없음 $1.0 \leq C < 3.0$: 치명도가 심각하지 않음 $3.0 \leq C < 6.0$: 치명도가 중함 $6.0 \leq C < 9.0$: 치명도가 심각함 $9.0 \leq C < 10.0$: 아주 치명적임 $C = 10.0$: 재앙적임
발생도(O) (Occurrence)	$0 \leq O < 1.0$: 발생 가능성 없음 $1.0 \leq O < 3.0$: 발생 가능성 거의 없음 $3.0 \leq O < 6.0$: 발생 가능성 이따금씩 있음 $6.0 \leq O < 9.0$: 발생 가능성 높음 $9.0 \leq O < 10.0$: 발생 가능성 아주 높음 $O = 10.0$: 발생 가능성이 매번 있음
검출도(D) (Detection)	$0 \leq D < 1.0$: 검출도가 확실함 $1.0 \leq D < 3.0$: 거의 검출도가 확실함 $3.0 \leq D < 6.0$: 검출도가 빈번함 $6.0 \leq D < 9.0$: 검출도가 조금 있음 $9.0 \leq D < 10.0$: 검출도가 거의 불확실함 $D = 10.0$: 고장 검출 능력 없음

가능한 원인과 결과, 각각의 실패 위험도를 파악하는 단계가 뒤따른다. 이후에 각각의 실패 모드의 위험 우선순위(Risk Priority Number; RPN)를 계산하며 이는 각각의 실패에 대한 치명도(Criticality), 발생도(Occurrence) 그리고 검출도(Detection)의 곱이다. 마지막으로 최종 선택된 실패 모드에 대해 적절한 개선 지시가 뒤따른다. 다음 표 2는 FMEA/C의 정성적인 치명도, 발생도, 검출도를 정량적으로 표현하기

위해서 값의 범위를 설정하였다[5-6].

3.4 FTA와 소프트웨어 FMEA/C의 통합

FMEA/C는 bottom-up 분석 기법으로 소프트웨어 시스템에서 가능한 소프트웨어 실패 모드의 결과를 확인하는 기능인 반면에 FTA는 top-down 분석 기법으로 원하지 않은 사건을 유발하는 요소를 찾아내는 기법이다. FMEA/C는 표 형식의 자료이기 때문에 소프트웨어 결함의 원인 사이의 논리 관계를 설명하기 어렵다는 단점이 있다. 그리고 FTA는 최상위 사건의 선택을 고려하는 것이 어렵다. 따라서 두 가지 기법을 통합하여서 분석한다면 포괄적이고 효과적인 방법이 될 것이다. FTA와 FMEA/C를 통합하는 방법으로 본 논문에서는 그림 5와 같이 FTA를 기준으로 FMEA/C를 통합하는 방법을 고안하였다[8-15].

우선 소프트웨어 결함 트리를 만들기 위한 최상위 사건을 선택한다. 만약 결함 트리에서 부정확성이 나타나거나 고장 영향의 치명도에 따라 새로운 최상위 사건이 나타난다면 결함 트리를 수정할 수 있다. 그리고 FMEA/C에 의해 치명도 분석이 이루어진 후에 최상위 사건의 발생 확률은 계산되어 질 수 있다. FTA 기준 FMEA/C의 통합 기법 수행 순서는 소프트웨어 보안 요건이나 위험 분석에 따른 최상위 사건 선택과 결함 트리 제작, 해당 사건들을 질적인 분석

그림 5. FTA 기준 FMEA/C의 통합 기법

을 통해 확인, 고장 모드에 의한 해당 사건의 FMEA/C를 형성, 결함트리와 개선 지시 수정하거나 새로운 결함 트리를 만들고 다음의 분석을 수행하기 위한 최상위 사건의 결함 모드 선택으로 이루어진다[7, 14-15].

4. IC카드 지불결제 시스템의 FTA와 FMEA/C의 보안성 평가 및 개선

4.1 IC카드 지불결제 시스템의 기능 블록 다이어그램

IC카드 지불결제 시스템의 보안성을 분석하기 위해서는 기능 영역이 정의되어야 한다. 그림 6은 IC카드 지불결제 시스템의 기능 블록 다이어그램이다. IC카드 지불결제 시스템은 수집 및 정산 시스템, 충전 및 환불 시스템, 카드 관리 시스템으로 이루어져 있고 카드 관리 시스템은 키 관리 서버, 어플리케이션 관리 서버, 카드 관리 서버로 구성되어 있다.

키 관리 서버는 어플리케이션 관리 서버와 카드 관리 서버를 운영하기 위하여 요구되는 키들에 대한 프로파일 생성, 관리하는 서버로써 키 값의 정의와 키 프로세스 관리 등을 수행한다. 어플리케이션 관리 서버는 IC카드에 탑재되는 어플리케이션의 전체적 프로세스를 관리하는 서버로 어플리케이션의 정의,

어플리케이션 추가, 제거, 어플리케이션 발급정보 조회, 발급 요구처리 등의 기능을 수행한다. 카드 관리 서버는 IC카드의 전제적인 주기인 프로세스를 관리하는 서버로써 카드 발급 프로세스, 데이터의 입력과 출력, 카드 형식, 종류의 정의 등의 기능을 수행한다. 그리고 카드 회사에서 카드 발급을 위한 발급 데이터의 배치 프로세스 스케줄링 등의 기능을 처리하기도 한다. 어플리케이션 다운로드 서버는 다양한 네트워크인 인터넷이나 무선 랜을 통하여 요청되는 후발급 처리에 대해서 키 관리 서버, 어플리케이션 관리 서버, 카드 관리 서버와 연동하여 사용자의 IC카드에 다양한 어플리케이션을 동적으로 다운로드 시켜주는 역할을 수행한다.

4.2 IC카드 지불결제 시스템의 결함 리스트

IC카드 지불결제 시스템의 기능 블록 다이어그램을 사용하여 기능별 결함들을 추출한다. 초반부에는 기능별로 예상 결함을 리스트로 작성하여 사용하지만 시험과 운영을 거치면서 보다 자세하고 실제적인 결함 리스트들을 표 3과 같이 구할 수가 있다.

4.3 FTA에 의한 결함 분석

FTA는 결함 발생의 원인들을 한눈에 알기 쉽게

그림 6. IC카드 지불결제 시스템의 기능 블록 다이어그램

표 3. IC카드 지불결제 시스템의 기능별 결함 리스트

시 스템		기 능	기능별 결함
수집 및 정산 시스템		거래 자료 수집	사용자 거래내역 오류
		사용자충전 자료 수집	사용자 거래내역 오류
		분배 정산 처리	사용자 거래내역 오류
충전 및 환불 시스템		충전 및 환불 내역 관리	사용자 거래내역 오류
		수수료 지불 내역 정산 처리	사용자 거래내역 오류
카드 관리 시스템	키 관리 서버	키 값의 정의	사용자 거래 불가, 사용자 거래내역 오류, 사용자 인증 오류
		키 프로세스 관리	사용자 거래 불가, 사용자 거래내역 오류, 사용자 인증 오류
	어플리케이션 관리 서버	어플리케이션의 정의	IC카드 사용 오류
		어플리케이션 추가 및 제거	IC카드 사용 오류
		어플리케이션 발급정보 조회	IC카드 사용 오류, 사용자 거래 불가
	카드 관리 서버	발급 요구처리	IC카드 사용 오류, 사용자 거래 불가
		카드 발급 프로세스	IC카드 사용자 발급 오류
		데이터의 입력과 출력	IC카드 사용자 데이터 오류
		카드 형식 및 종류의 정의	IC카드 오류

표현한 순차적인 그래프 모형으로 4.1절과 4.2절에서 구한 IC카드 지불결제 시스템의 기능 블록 다이어그램과 IC카드 지불결제 시스템의 결함 목록 리스트에 의하여 그림 7과 같이 IC카드 지불결제 시스템의 FTA를 정의 할 수 있다. 이를 통해 IC카드 지불결제 시스템 결함 원인이 파악되어 설계된 시스템을 정성적으로 정략적으로 분석 가능하다.

4.4 FMEA/C에 의한 IC카드 지불결제 시스템의 보안 위험 우선순위 계산과 개선 지시

FMEA/C에 의한 IC카드 지불결제 시스템의 보안 위험 분석을 위해서는 적당한 워크시트가 필요하다. 아래의 표 4는 기존의 FMEA/C를 위한 워크시트를 축약 및 변경하여 나타내었다. 고장에 대한 위험

그림 7. IC카드 지불결제 시스템의 최상위 수준에 따른 결함 트리

표 4. 개선 지시에 따른 수정 계산된 RPN 값

개선 차수	개선 전후	치명도	발생도	검출도	RPN	개 선 율	
						개선 전 대비	최초 개선 전 대비
1차 개선	개선 전	7.5	9.3	10.0	697.5	20.9%	20.9%
	개선 후	7.5	8.0	9.2	552.0		
2차 개선	개선 전	7.5	8.0	9.2	552.0	46.1%	57.4%
	개선 후	7.5	6.1	6.5	297.4		
3차 개선	개선 전	7.5	6.1	6.5	297.4	61.2%	83.4%
	개선 후	7.5	4.4	3.5	115.5		

우선순위(RPN, Risk Priority Number)를 계산하여 RPN이 높은 고장부터 개선 지시 (Corrective Action)를 수행한다. 결함에 대한 개선 지시 (Corrective Action)에 의해서 결함은 줄어든다. 치명도(Criticality)는 고장 유형의 치명성의 정도 ($0 \leq C \leq 10$), 발생도(Occurrence)는 고장 유형의 발생 가능성의 정도 ($0 \leq O \leq 10$), 검출도(Detection)는 시스템이 사용자에게 양도하기 이전에 고장이 검출될 수 있는 가능성의 정도 ($0 \leq D \leq 10$)을 말한다. RPN의 값은 $RPN = \text{치명도(Criticality)} \times \text{발생도(Occurrence)} \times \text{발생도(Detection)}$ 로서 구할 수 있다.

본 논문에서는 IC카드 지불결제 시스템의 FMEA/C는 치명도, 발생도, 검출도, RPN의 이해를 돕기 위한 개선 지시의 1차, 2차, 3차에 따른 RPN이 개선되는 가상적인 예를 나타낸 것이다. RPN이 개선된 것은 결함에 대한 치명도, 발생도, 검출도 등을 최대한 탐지하여 개선한 것으로 차수가 높아짐에 따라 결함이 감소되어 3차 개선에서는 RPN 개선율이 최고 83.4%까지 도달됨을 보여주고 있다. 또한 표 4에서 치명도의 값이 1차, 2차, 3차에 있어서 동일한 이유는 치명도라는 것은 그 보안성의 위험은 시스템이나 소프트웨어가 개선됨에 있어서도 동일하기 때문에 본 논문에서는 각 소프트웨어 보안성 결함에 있어서 동일한 수치를 사용했다. 또한 표 4의 예에서는 개선 지시를 3차 까지 수행하였지만 안전성을 보장해야 하는 사용자의 요구사항이 있다면 그 조건을 만족시킬 수 있을 때까지 수차에 걸쳐서 개선노력을 수행해야 할 것입니다.

4.5 FTA와 FMEA/C의 통합에 의한 IC카드 지불결제 시스템 결함 분석

본 논문에서는 3.4절의 그림 5와 같이 FTA와

FMEA/C의 통합 방법을 FTA를 기준으로 FMEA/C를 통합하는 방법을 고안하였다. 이는 FTA를 중점으로 결함 트리 분석 수행 후 FMEA/C를 통하여 치명도, 발생도, 검출도, RPN을 계산하여 개선 지시를 통해 보안성을 개선하는 기법이다.

FTA를 기준으로 FMEA/C를 통합하는 방법을 사용한 이유는 FMEA를 기준으로 통합한 방법은 FMEA를 중심으로 소프트웨어의 보안 결함을 분석하는 기법이기에 소프트웨어의 보안적인 수치 판단의 정량적 분석이 주를 이루고 또한 FMEA를 기준으로 하기 때문에 IC카드 지불결제 시스템의 모든 결함 원인을 하나하나 분석해야한다. 하지만 FTA를 기준으로 FMEA/C를 통합하는 방법을 통하여 IC카드 지불결제 시스템을 분석하면 FTA를 기준으로 하기에 최상위 사건인 전자 교수학습 시스템의 고장을 결과로 선정하여 top-down 방식으로 IC카드 지불결제 시스템의 고장 원인을 파악할 수 있다.

본 논문의 4.3절에서 정의한 그림 7의 IC카드 지불결제 시스템의 최상위 수준에 따른 결함 트리에서 FTA를 기준으로 FMEA/C를 통합한 방법에 효율적으로 적용하기 위해 그림 8-10과 같이 세 가지 부분을 나누었다. 세 가지 부분은 수집 및 정산 시스템, 충전 및 환불 시스템, IC카드 관리 시스템으로 구성된다.

5. 결론 및 향후 과제

오늘날 IT융합 기술의 발달에 따라 내장 소프트웨어의 사용이 확대되고 있다. 이에 따라 하드웨어에 내장된 소프트웨어 시스템이 정상적으로 안전하게 동작 하는지에 대한 안전 중심 소프트웨어 시스템들을 중심으로 하드웨어 또는 소프트웨어의 결함으로

그림 8. 수집 및 정산 시스템의 FTA를 기준으로 FMEA/C를 통합한 분석

그림 9. 충전 및 환불 시스템의 FTA를 기준으로 FMEA/C를 통합한 분석

그림 10. IC카드 관리 시스템의 FTA를 기준으로 FMEAC를 통합한 분석

사고 또는 재난 발생을 예방하기 위한 소프트웨어 시스템의 보안성 평가에 대한 관심이 증가하고 있다. 소프트웨어를 내장한 IC칩을 사용하고 있는 카드시스템은 다양한 분야에서 지불결제 도구로 사용되고 있고 IC카드를 이용하여 지불결제 시스템을 구축하여 활용되고 있으며 다른 분야로 점차 확대 사용되어지고 있는 추세이다. 그러나 교통수단과 유통을 포함한 전 결제시스템에서 사용 가능한 통합 전자지불결제 시스템의 개발 필요성이 증대하고 있다. 이에 IC카드를 이용한 통합 전자 지불결제 시스템을 구축하여 사용을 확대하는 데에는 이들에 대한 안전성과 보안성 평가를 통하여 안전성과 보안성의 보증(Assurance)이 우선이다. 통합 IC카드를 이용한 통합 전자지불결제 시스템에 안전성과 보안성을 확보하지 못하면 엄청난 사회적인 문제를 야기하여 심각한 재난이 발생할 수가 있다.

본 논문에서는 IC카드 지불결제 시스템의 보안성 평가를 위해서 FTA와 FMEA/C를 이용하여 통합적

인 분석을 해보았다. IC카드 지불결제 시스템의 보안성 평가를 하나의 기법으로만 사용하는 것보다 두 가지 기법의 장점을 모두 이용함으로써 더욱 효과적인 평가를 수행할 수가 있었다. IC카드 지불결제 시스템의 보안성 평가 방법 중 FTA는 결함 발생의 모든 원인들의 연결과정을 한눈에 알기 쉽고, FMEA는 시스템의 고장 모드들과 그 영향들을 쉽게 파악할 수가 있기 때문에, 치명적인 시스템의 고장들에 대한 대책 수립을 통해 보안성을 개선할 수가 있다. 따라서 실제적인 적용 사례에서, IC카드 지불결제 시스템에서 (1) 먼저 결함들을 기능적으로 정의한 다음, (2) 결함트리분석(FTA)을 수행하여 결함의 구조들을 파악하고, (3) 그에 따른 결함들의 치명성을 중심으로 발생빈도 및 검출가능성을 정량적으로 분석하여 그 영향을 고려할 수 있는 고장모드 및 영향 분석(FMEA/C) 방법을 수행하며, (4) 그에 따른 보안성 영향평가 수치인 RPN을 계산하여 보안성 개선 지시 및 평가를 수행하는 일련의 정량적인 분석 방법과

프로세스를 제안하였다.

시스템의 결함 분석을 통해서 보안성을 평가하는 많은 기법들이 존재하지만 본 논문에서는 두 가지 이상의 기법들의 통합을 통한 시스템 결함 분석과 안전성 분석을 효율적으로 수행하고 그 프로세스를 실제적으로 제시하였다. 따라서 시스템의 결함들에 대한 FTA를 기준으로 FMEA/C를 통합한 방법이 IC카드 지불결제 시스템의 보안성을 평가하고 개선하는 데 상호 보완적인 최적 결함 분석 기법이라고 할 수 있다. 따라서 계속해서 특정 시스템의 보안성을 평가하기 위해서는 효율적인 결함 분석 기법들과 그 상호 보완적인 결함 분석 기법들의 조합을 연구하고 그 조합의 방법들이 더욱 보안성을 강화할 수 있도록 연구해야 할 것이다.

참 고 문 헌

- [1] Doo-Hyun Kim and Jong-Ho Lee, "Qualitative Assessment for Hazard on the Electric Power Installations of a Construction Field using FMEA," *Journal of the Korean Society of Safety*, Vol. 19, No. 14, pp. 36-41, 2004.
- [2] S.Y. Kim, W.Y. Yun, and H.G. kim, "Reestablishment of RPN Evaluation Method in FMEA Procedure for Motors in Household Appliances," *Journal of the Korean Society for Quality Management*, Vol. 35 No. 1, pp. 1-9, 2007.
- [3] Rajiv Kumar Sharma and Pooja Sharma, "System Failure Behavior and Maintenance Decision Making using, RCA, FMEA and FM," *Journal of Quality in Maintenance Engineering*, Vol. 16, No. 1 pp. 64-88, 2010.
- [4] Hyo Young Kim and Hyuk Soo Han, "A Defect Prevention Model based on SW-FMEA," *Journal of Korean Information Science Society*, Vol. 33, No. 7, pp. 605-614, 2006.
- [5] Myonghee Kim and Man-Gon Park, "A Study on the Software Fault Modes and Effect Analysis for Software Safety Evaluation," *Journal of the Korean Multimedia Society*, Vol. 15, No. 1, pp. 113-130, 2012.
- [6] Hyun Ki Park, *A Study on Methods of Fault Analysis and the Failure Effect Analysis for Security Improvement of e-Teaching and Learning System*, Ph.D. Dissertation, Pukyong National University, 2012.
- [7] Ik-Sung Lee, "A Study for Quality Improvement of Convention by Failure Mode and Effects Analysis," *Journal of the Korean Convention Society*, Vol. 5, No. 1, pp. 101-107, 2005.
- [8] Joong-Soon Jang, "A Study on Performing FMEA Effectively," *Journal of the Korean Institute of Plant Engineering*, Vol. 4, No. 4, pp. 69-77, 1999.
- [9] Joong-Soon Jang and Dong-Geun An, "How to Perform FMEA Effectively," *Journal of the Korean Society of Quality Management*, Vol. 25, No. 1, pp. 156-172, 1997.
- [10] Adem Sabic, jasmin Azemovic, "Model of Efficient Assessment System with Accent on Privacy, Security and Integration with e-University Components," *Second International Conference on Education Technology and Computer(ICETC)*, Vol. 3, pp. 128-131, 2010.
- [11] M. Ben-Daya and Abdul Raouf, "A Revised Failure Mode and Effects Analysis Model," *International Journal of Quality & Reliability Management*, Vol. 13, No. 1, pp. 43-47, 1996.
- [12] N. Snooke and C. Price, "Model-driven Automated Software FMEA," *Proc. Reliability and Maintainability Symposium (RAMS)*, pp. 1-6, 2011.
- [13] Rodrigo de Queiroz Souza and Alberto José Álvares, "FMEA and FTA Analysis for Application of the Reliability Centered Maintenance Methodology: Case Study on Hydraulic Turbines," *ABCM Symposium Series in Mechatronic*, Vol. 3, pp. 803-812, 2008.
- [14] Thomas Maier, "FMEA and FTA to Support Safety Design of Embedded Software in Safety-Critical Systems," *Proc. CSR 12th Annual Workshop on Safety and Reliability of*

- Software Based Systems*, pp. 351-367, 1997.
- [15] Zhang Hong and Liu Binbin, "Integrated Analysis of Software FMEA and FTA," *Proc. International Conference on Information Technology and Computer Science*, pp. 184-187, 2009.

김 명 희

동서대학교 정보통신공학과(공학사)
부경대학교 대학원 전자계산학과(이학석사)
부경대학교 대학원 정보시스템학과(공학박사)

2004년~2007년 정부간 국제기구 CPSC (콜롬보플랜기술교육대학) Assistant Faculty, 정보기술 및 통신학처장
2011년~2012년 부경대학교 교육대학원 전자계산교육 전공 강의전담교수
2012년~현재 미국 University of Colorado-Denver, Dept. of Computer Science and Engineering Post-Doc 연구원
관심분야: 소프트웨어 공학 및 재공학, 멀티미디어정보 처리기술, 네트워크성능평가, e-Learning and u-Learning

진 은 지

2011년 부경대학교 전자컴퓨터정보통신공학부 졸업(공학사)
2013년 부경대학교 대학원 첨단정보과학 및 정보기술전공 (공학석사 예정)

관심분야: 소프트웨어 공학 및 재공학, 멀티미디어정보 처리기술, 소프트웨어 안전성 및 보안성 공학, e-Learning and u-Learning 콘텐츠 개발

박 만 곤

경북대학교 수학교육(이학사)
경북대학교 전산통계학(이학박사)
Philippine Women's University (국제행정학석사)
University of Rizal System, Philippines (명예 기술학박사)

Dept. of Electrical & Computer Engineering, University of Kansas (Post Doc.)

1981년~현재 부경대학교 IT융합응용공학과 교수
2008년~현재 한국멀티미디어학회(KMMS) 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 자문관

관심분야: 소프트웨어신뢰성공학, 비즈니스 프로세스 재공학(BPR), 소프트웨어 공학 및 재공학, 멀티미디어정보처리기술, 정보시스템성능평가, ICT-based HRD System