DOI: 10.3745/KIPSTC.2010.17C.3.223

인터넷 뱅킹 시스템 관련 표준 분석 및 보호프로파일 개발에 관한 연구

조 혜 숙[†] · 김 승 주[††] · 원 동 호[†††]

요 약

인터넷의 발달로 기존의 많은 오프라인 서비스가 온라인 서비스로 확장되면서 금융 거래 서비스 역시 편리성을 이유로 인터넷 뱅킹 시스템을 통해 서비스가 제공되고 있다. 하지만 인터넷 뱅킹 시스템 개발 과정에서 보안성에 대한 고려가 부족하여 여러 보안 문제점을 갖고 있고 실제로 인터넷 뱅킹 시스템에 보안 사건들이 빈번하게 일어나고 있는 실정이다. 이런 문제점을 해결하기 위하여 금융기관은 ISO 20022, ISO/IEC 27001, ISO/IEC 9789, ISO/IEC 9796 등의 국외 표준과 웹 환경 구축 및 운영을 위한 보안관리 지침, 전자상거래 표준화 로드맵 등 국내 표준을 적용하고 있지만 인터넷 뱅킹 시스템에 관한 보안요구사항 등이 제대로 고려되지 않아 여전히 취약성이 발생하고 있다. 본 논문에서는 기존 표준들에 대해서 설명하고 인터넷 뱅킹 시스템에 단일 표준 적용시 보안을 보증하지 못하는 이유에 대해서 살펴본다. 또한 인터넷 뱅킹 시스템의 취약성을 설명하고 보안기능을 분석해 그 특징에 맞는 보안기능 요구사항을 도출하고 이를 통해 공통평가기준 V3.1을 참고로 하여 인터넷 뱅킹 시스템의 보안을 강화하기 위해 특화된 보호프로파일을 제안한다.

키워드 : 인터넷 뱅킹 시스템, 보호프로파일, 공통평가기준

A Study of Protection Profile and Analysis of Related Standard for Internet Banking Systems

Heasuk Jo[†] · Seungjoo Kim[††] · Dongho Won[†††]

ABSTRACT

Due to the advance of Internet, offline services are expanded into online services and a financial transaction company provides online services using internet baning systems. However, security problems of the internet banking systems are caused by a lack of security for developing the internet banking systems. Although the financial transaction company has applied existing internal and external standards, ISO 20022, ISO/IEC 27001, ISO/IEC 9789, ISO/IEC 9796, Common Criteria, etc., there are still vulnerabilities. Because the standards lack in a consideration of security requirements of the internet banking system. This paper is intended to explain existing standards and discusses a reason that the standards have not full assurance of security when the internet baning system is applied by single standard. Moreover we make an analysis of a security functions for the internet baning systems and then selects the security requirements. In this paper, we suggest a new protection profile of the internet baning systems using Common Criteria V.3.1 from the analysis mentioned above.

Keywords : Internet Banking System, Protection Profile, Common Criteria

1. 서 론

인터넷 이용자 수가 증가하면서 은행을 직접 가지 않고 금융 업무를 보는 개인과 기업이 늘어남에 따라 국내 온라인 금융 거래 이용자 수는 5천만 명을 넘어섰으며, 계속 증가하는 추세를 보이고 있다. 이에 발맞춰 금융 기관에서도 구축된 인프라를 바탕으로 사용자에게 편의성을 제공하기 위한 다양한 서비스를 개발하여 제공하고 있다. 하지만, 인터넷 뱅킹 서비스의 개발에는 많은 노력을 기울이지만 보안성 측면에서는 그에 비해 간과되어지고 있다. 오히려 인터넷 뱅킹 서비스의 발달을 따라가지 못해 보안은 점점 더 취약해지고 있는 실정이다.

대부분의 인터넷 뱅킹 시스템을 서버와 클라이언트로 분류할 때, 서버 시스템의 보안은 공개 되어 있지 않지만, 훈

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업(NIPA-2010-(C1090-1031-0005))과 방위사업청과 국방과학연구소(UD100002KD)의 연구결과로 수행되었음.
† 정 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
†† 종신회원 : 성균관대학교 정보통신공학부 교수
††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2010년 1월 25일
수 정 일 : 1차 2010년 4월 26일
심사완료 : 2010년 5월 17일

련된 관리자에 의해 관리되기 때문에 보안 취약성이 적다. 반면, 클라이언트 시스템은 공개된 시스템이며, 다수의 다양한 사용자에게 사용되기 때문에 여러 취약성이 존재하고 있다. 따라서 소비자가 직접 사용하게 되는 클라이언트 시스템의 보안에 대한 고려가 필요하다.

또한 인터넷 뱅킹 서버 시스템은 악의적인 공격을 당할 경우, 개인적 또는 사회적으로 문제가 되고 그 피해가 크기 때문에 국내외에서 여러 표준과 제도를 통해 대비책을 제시하고 있다. 뿐만 아니라 금융 기관을 포함한 여러 기관 및 기업은 자사의 유형, 무형의 자산을 보호하기 위해 다양한 표준을 사용하고 있다. 사용되는 국외표준으로 ISO 20022, ISO/IEC 27001, ISO/IEC 9798, ISO/IEC 9796, Common Criteria 등이 있고 국내 표준으로는 웹 환경 구축 및 운영을 위한 보안관리 지침과 표준화 자료로 전자상거래 표준화 로드맵, 전자상거래 프레임워크 표준현황 및 적용 지침 등이 있다. 이러한 표준들은 인터넷 뱅킹 시스템을 안전하게 유지하기 위해서 적용되어 지기도 한다. 하지만 표준을 적용하고 있음에도 불구하고, 인터넷 뱅킹 시스템은 여전히 보안에 취약한 이유는 무엇일까. 예를들어 한 인터넷 뱅킹 시스템을 운영하는 기업이 ISO/IEC 27001 인증을 획득하였다고 하자. 물론 인터넷 뱅킹 시스템을 위해 보안이 유지될 수 있을 것이다. 하지만 적용한 표준은 정보보호 경영 시스템을 유지하는데 중점을 둔 표준이기 때문에 여전히 인터넷 뱅킹 시스템에서는 그 취약성이 존재할 것이다. 왜냐하면 적용 표준이 인터넷 뱅킹만을 위한 표준이 아니고, 또한 인터넷 뱅킹 시스템을 개발 할 때 표준 적용 범위는 개발자에 따라 달라지기 때문이다. 즉, 기존에 제안된 표준이나 제도들이 인터넷 뱅킹 시스템에 적절한 보안요구사항을 제시하고 있지 못하고, 실제 시스템에 충분히 적용되지 못한다는 것이다.

따라서 본 논문에서는 인터넷 뱅킹 시스템의 보안을 강화하고 보증하기 위해 적용 가능한 표준과 제도를 설명한다. 이를 통해 인터넷 뱅킹 시스템에 단일 표준을 적용했을 때의 취약점을 해결할 수 있는 요소를 취하고 보완하여 인터넷 뱅킹 시스템 보호프로파일을 제안한다. 제안하는 보호프로파일은 현재 세계적으로 잘 알려진 제품과 시스템에 대한 보안성 평가기준인 ISO/IEC15408 공통평가기준(CC, Common Criteria)[8-11]을 사용한다.

본 논문의 구성은 2장에서 금융 산업에서 사용하고 있는 관련 표준들을 서술하고 인터넷 뱅킹 시스템의 구성 및 취약성에 대해 설명한다. 3장에서는 인터넷 뱅킹 시스템에 특화된 보안기능 요구사항을 도출하여 보호프로파일을 제시하며, 4장에서는 결론을 맺는다.

2. 관련 연구

현재 금융 관련 산업 보안을 위하여 국제적 또는 국내에 많은 표준이 제시 되어 있고, 활발하게 개발이 이루어지고 있다. 하지만 이러한 표준의 적용은 인터넷 뱅킹 시스템의 보안을 보장하기에 현실성이 부족하다. 본 장에서는 금융기관에서 적용하고 있는 관련 표준들을 분석하여 인터넷 뱅킹 시스템의 보안에 적합하지 못한 이유에 대해 고찰하고 인터넷 뱅킹 시스템 구성에 대한 설명과 구성 요소들이 가지고 있는 취약점에 대해서 살펴본다.

2.1 금융기관의 적용 표준

2.1.1 ISO 20022

금융기관 간 금융 정보의 송수신을 위한 표준 ISO 20022 [1](UNIFI, UNiversal Financial Industry message scheme)는 ISO/TC68 Financial Services에서 개발한 표준으로 표준화된 XML 구문규칙(모델링방법론, XML디자인규율 등)에서 메시지를 개발하기 위한 플랫폼을 금융 산업에 제공한다. UNIFI는 MDDL, FIX, FinXML, VRXML, RIXML, XBRL, FpML, IFX, TWIST, SWIFT, RosettaNet, OAGi, ACORD, CIDX, 등과 같이 XML 금융 메시지 분야의 수많은 중복된 표준들을 통합하고, 개선하고자 개발되었다. 모든 금융관련 표준 기관들에서 사용할 수 있도록 금융 분야의 방법론, 프로세스, 저장소 등에 관한 하나의 통합된 표준이다.

UNIFI는 ISO 15022 표준으로부터 발전되어, 다음과 같이 5개의 부분으로 구성되어 있다.

- Part1. : International Standard: Overall methodology and format specifications for inputs to and outputs from the ISO 20022 Repository
- Part2. : International Standard: Roles and responsibilities of the registration bodies
- Part3. : Technical Specification: ISO 20022 modelling guidelines
- Part4. : Technical Specification : ISO 20022 XML design rules
- Part5. : Technical Specification: ISO 20022 reverse engineering

하지만 ISO 20022는 금융 기관 간 상호운영을 위해 금융 정보의 송수신에 대한 표준이므로 결제와 보안 기능에 중점을 두고 있다[17]. 따라서 전송 및 저장되는 정보를 보호하기 위한 기능은 표준에서 제시하고 있지만, 하나의 시스템 안에서 여러 모듈이 상호 동작하는 기능 및 객체에 대한 보안은 제시하고 있지 않다. 현재 인터넷 뱅킹 시스템은 서버와 클라이언트간의 동작에서 구체적인 보안요구사항이 필요하며, 특히 클라이언트에게 강화된 보안기능의 제공이 필요한 실정이다. ISO 20022 표준에서는 이러한 보안요구사항을 제공하지 못한다.

2.1.2 ISO 27001

ISO 27001[2]은 BSI(British Standards Institute)가 제정한 국제표준으로, 기업이 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적 경영시스템인 정보보호경영시스

템(Information Security Management System, ISMS)에 대한 요구사항을 규정하고 있다.

ISO 27001은 BS7799 표준에서 파생된 것으로, BS7799의 1부는 ISO/IEC 17799로, BS7799의 2부는 ISO/IEC 27001로 전환되었다. ISO/IEC 27001에서 규정하는 통제항목은 11개 조항으로 구성되어 있다.

ISO 27001 표준은 기업의 전체 시스템에 대해 인증이 이루어지기 때문에, 조직의 핵심 정보자산을 보호 관리 할 수 있으며, 시스템의 취약점을 파악하고, 운영상의 위협에 따른 손실을 예측하여 보완할 수 있다. ISO 27001은 시스템의 위험을 관리하기 위한 일반적인 접근방법의 사례를 제시한다. 이러한 특징은 ISO 27001에서 제시하는 모든 통제항목이 모든 정보시스템에 적용할 수 없다는 단점을 갖는다. 악의적인 공격의 시도가 잦은 인터넷 뱅킹 시스템의 경우, 다양한 공격에 대한 높은 수준의 기술적인 보안이 요구된다. 또한 인터넷 뱅킹 시스템은 보안을 위해 다양한 정보보호제품과 연동이 되고 있어, 이에 대한 구체적인 보안 요구사항이 필요하다. 하지만, ISO 27001 표준은 시스템 구성요소의 기술적인 측면에 대한 요구사항이 부족하기 때문에 높은 수준의 기술적 보안을 제공하지 못한다.

2.1.3 Common Criteria

CC[8-11]는 IT제품에 대한 보안성 검증 및 평가하기 위한 국제 기준(ISO 표준)으로 미국, 영국, 프랑스 등 선진국이 참여하여 각국의 보안평가기준을 하나로 통합 및 일원화하여 개발하였다[7]. 1996년 CC V1.0 발표를 시작으로 1998년 CC V2.0, 2005년 CC V2.3, 2006년 8월에 CC 3.0 개발 및 공개 검토가 이루어졌고 2009년 7월에 CC V3.1, Revision 3이 공식 평가기준이 되어 2010년 현재 까지 사용되고 있다. CC는 보안기능이 구현된 IT 제품이나 시스템의 보안성을 평가하기 위한 공통의 요구사항을 제시한 기준이다. 현재 국내의 경우 2006년에 국제상호인정협정 (Common Criteria Recognition Arrangement, CCRA)에 가입하여 국제용/국내용 평가 인증제도를 실행하고 있다.

CC는 기본개념, 보안기능요구사항, 보증요구사항으로 총 3부로 구성된다.

- 1부 소개 및 일반모델: 용어정리, 개요, 보호프로파일 (Protection Profile, PP) 및 보안목표명세서(Security Target, ST)의 구조
- 2부 보안기능요구사항: 보안기능 요구사항(11개항목) 정의 및 설명
- 3부 보증요구사항: 보증요구사항 및 평가보증등급 등 정의

CC V3.1은 특정 유형의 소프트웨어 또는 운영체제 등을 조합하여 개발할 때 발생할 수 있는 문제에 대해서도 합성 클래스를 통해서 적용 가능하다. 하지만 기존 국가기관용 침입차단 및 침입탐지 시스템 보호프로파일, 역할기반 접근통제 시스템 보호프로파일 등을 기준으로하여 많은 업체와 국가기관이 이를 활용하고 있지만 인터넷 뱅킹 시스템의 안전한 운영 관리에 관한 보호프로파일이 없기 때문에 그 개발이 필요하다.

2.1.4 웹 환경 구축 및 운영을 위한 보안관리 지침

한국정보통신기술협회의 정보통신단체표준 (TTAS.KO-10.0090, [16])으로 웹 환경 구축 및 운영에 필요한 보안 요소 파악을 위해 웹 보안요구사항, 안전한 운영의 접근 기법, 메시지 교환 보안기법, 해킹을 방어하기 위한 프로그래밍 기법 등을 제공한다. 이 표준은 전자상거래, 인터넷뱅킹 등 웹서비스를 제공하는 모든 분야의 웹 관리자가 웹 환경 구축 및 운영에 활용할 수 있는 표준이다. 웹 보안관리 지침으로 크게 세 가지로 나눠 <표 1>과 같이 설명하고 있다.

웹 환경 구축 및 운영을 위한 보안관리 지침은 안전한 시스템을 위해 개발되었지만, 인터넷 뱅킹 시스템의 경우에는 인터넷 뱅킹에 특화된 위협에 대응하기에 이 지침에서 제안하는 보안 요구사항이 충분하지 않다. 또한 이 지침은 웹 환경 구축 및 운영에 대한 최소한의 간단한 사항만 제시할 뿐, 시스템이 어떠한 위협에 대응해야 하고, 이를 위해 어떤 보안 기능을 갖추어야 하며, 시스템 설계과정이나 이로부터 도출되어야 하는 기능에 대한 요구사항이 부족하다.

2.1.5 기타[1]

앞에서 언급한 표준 외에 전자상거래, 정보시스템 등의 보안을 위한 여러 표준들이 존재하고 있다. 하지만 이러한 표준의 대부분은 암호화, 전자서명과 같은 하나의 보안 기능을 위한 표준이며, 안전한 시스템의 구축 및 운영에 대한 요구사항은 제시하지 않고 있다. <표 2>는 인증, 암호화, 전자서명에 관한 표준이다.

<표 3>은 앞서 제시한 관련 표준의 특성을 분석하여 인터넷 뱅킹 시스템에 단일 표준으로 적용 시 나타날 수 있는 취약점을 나타낸다[17].

〈표 1〉 웹 환경 구축 및 운영을 위한 보안 관리 지침

분야	설 명
웹 보안 기법	네트워크 주소를 이용한 접근제어, 사용자 이름과 패스워드에 대한 접근관리, 로그파일 관리, 메시지 교환 보안 기법
안전한 웹 프로그램 제작 기법	SQL Injection 공격 보안 기법, SQL Injection을 이용한 사용자 인증 우회 공격 및 대책, 업/다운로드 공격 보안기법, XSS 공격 보안기법
웹 서버 및 브라우저 별 보안대책	웹 서버 및 웹 브라우저 보안대책

〈표 2〉 기타 표준

분야	표준	설 명
인증	ISO/IEC 9798	- Information technology - Security techniques - Entity authentication
암호화	ISO/IEC 18033	- Information technology - Security techniques - Encryption algorithms
전자 서명	ISO/IEC 9796	- Information technology - Security techniques - Digital signature schemes giving message recovery
	ISO/IEC 14888	- Information technology - Security techniques - Digital signatures with appendix
	ISO/IEC 10118	- Information technology - Security techniques - Hash-functions
	ISO/IEC 15946	- Information technology - Security techniques - Cryptographic techniques based on elliptic curves

〈표 3〉 각 표준 특성 및 취약점

표 준	특 성	단일 표준으로 적용 시 취약점
ISO 20022	금융기관 상호 운영을 위한 표준	- 모듈간 상호보안 부족 - 클라이언트의 행동에 관한 보안기능 부족
ISO 27001	기업 시스템 인증 및 정보자산 보호관리	- 모듈간 상호보안 부족 - 기술적인 보안 부족
Common Criteria	IT 제품의 개발, 평가, 조달 지침	- 현재 인터넷 뱅킹 관련 보호프로파일 없음
웹 환경 구축 및 운영을 위한 보안 관리 지침	웹 환경 안전을 위한 기술	- 특화된 위협에 대한 대응 부족 - 기능 요구사항 부족

2.2 인터넷 뱅킹 시스템 구성 및 취약점

인터넷 뱅킹은 사용자의 웹 브라우저, 인터넷 뱅킹 서버, 인증기관, 데이터베이스 요소들로 구성된다. 각 구성요소 사이에 안전한 서비스를 위하여 보안을 위한 여러 방법들이 사용되고 있다. 각각을 살펴보면 사용자의 웹 브라우저는 인터넷 뱅킹 서버에 접속할 때 금융기관에서 제공하는 보안 프로그램과 안전한 금융거래를 위한 공인인증서를 사용하여 접속하게 된다. 인터넷 뱅킹 서버는 사용자와 서버 사이에 안전한 통신을 하기 위하여 침입탐지시스템 또는 방화벽을 설치하여 안전을 보장한다. 또한 안전한 인터넷 뱅킹 서비스를 위하여 개인키 관리, 암호 및 전자서명 알고리즘, 인증서 처리 등의 업무를 처리한다. 인증기관은 사용자의 인증 요청시 인증 업무를 처리하고 관련 데이터를 보관함에 있어서 전용회선이나 가상사설망 등을 통하여 안전을 보장한다.

하지만 이러한 노력에도 불구하고 인터넷 뱅킹 시스템은 다양한 해킹 기법 등을 이용하여 개인 정보보호 유출 사고로 인한 손실[18] 및 침해사고가 지속적으로 발생되고 있다. 이러한 인터넷 뱅킹 관련 취약점을 대처하기 위한 방편으로 우리나라 에서는 전자금융거래 안전성 강화 종합 대책[12]이 마련, 전자금융거래법[13] 시행, 국제 웹 보안 협회인 OWASP (Open Web Application Security Project)에서 발표한 2010년 주요 웹 취약점 항목[6]을 통해 시스템의 안전성을 유지하고 사용자를 보호하고 있다. 현재 인터넷 뱅킹 시스템의 사용은 웹 기반 서비스 사용자가 다수기이 때문에 웹 기반 시스템에서 발견된 취약점[6]은 인터넷 뱅킹 시스템에서도 발생한다고 할 수 있다. 실제로 금융 거래 시스템의 보안사건 중 59% 역시 웹 어플리케이션 상의 문제로 인해 발생한다.

다음은 인터넷 뱅킹의 주요 공격방법을 <표 4>와 같이 나타낸다.

〈표 4〉 인터넷 뱅킹의 주요 공격방법

분 류	내 용
공인인증서	- 공인인증서 관리를 위한 ActiveX 컨트롤의 개발시 설계상 오류 - 저장된 공인인증서 유출
OTP[14]	- OTP(One Time Password)의 암호키 관리 부주위로 OTP 키유출 - Man-In-The-Middle 공격
Kye Logger	- 키보드 입력 정보를 일정 위치에 저장시키는 프로그램으로 기록된 정보를 통해 개인정보 유출
보안카드	- 인터넷 뱅킹 이용시 보안카드의 정보 입력을 키로거를 통하여 수집 후 보안카드의 조합을 알아냄
입금 계좌번호 변경	- 이체과정에서 입금 계좌번호를 해커가 위.변조함
DDoS공격	- DDoS 공격을 통해 인터넷 서비스 장애 발생
인젝션[6]	- SQl 인잭션 공격, 스크립트 인잭션 공격, 악의적인 명령어 수정
악성코드[5]	- 웜, 바이러스, 키로깅이나 백도어 프로그램 등의 악성코드 침입으로 사용자 입력 정보(ID, 주민번호, 비밀번호, 카드 유효기간 등)나 저장 정보를 사용자 모르게 가로채 유출
전송정보 스니핑[15]	- 네트워크상에서 스니핑 툴을 이용하여 사용자가 서버에 전송하는 정보를 도청 및 변조
크로스 사이트 스크립팅(XSS)[6]	- Scripting attacks, Cross-Site Scripting attacks
취약한 인증 및 세션관리[6]	- 인증 및 권한 우회, 세션 가로채기
안전하지 않은 직접 객체 참조[6]	- 노출된 객체 조작으로 허가되지 않은 데이터 접속
크로스 사이트 요청 위조[6]	- 사용자의 세션 정보 등을 이용하여 취약한 어플리케이션 공격
보안 설정상의 오류[6]	- 보안설정 부재로 인한 공격
URL 접속 제한 실패[6]	- URL 접속 권한 및 제한 미 체크로 인한 공격
검증되지 않은 Redirect와 forward[6]	- 피싱 싸이트 또는 멜웨어 사이트로 Redirect하거나 Forward해 허가받지 않은 싸이트로 접속
데이터 암호화하지 않고 저장[6]	- 신용카드, SSN, 인증 식별 정보 등의 암호화되지 않음으로 인한 공격
전송 계층에 대한 불충분한 보호[6]	- 암호화 하지 않은 네트워크 트래픽 또는 약한 알고리즘 사용 등을 통한 공격

3. 인터넷 뱅킹 시스템을 위한 보호프로파일

인터넷과 정보보안기술의 발달로 온라인을 통한 온라인 뱅킹 사용자는 급격히 증가하고 있다. 하지만 정보보안기술의 발달과 함께 시스템을 공격하는 기술도 발전하여 현재 인터넷 뱅킹 시스템의 보안기능은 제 기능을 하지 못하는 경우가 종종 발생한다. 2장에서 살펴봤듯이, 인터넷 뱅킹에 대한 키보드 해킹, DDoS 공격, 악성코드 삽입 등으로 인한 취약성이 보고되고 있다. 또한 사용자에게 제공되는 정보보호 기능 역시 인터넷 뱅킹 시스템과 완전한 연동이 이루어지지 않아 보안 기능을 제대로 수행하지 못하는 경우도 발생하고 있다.

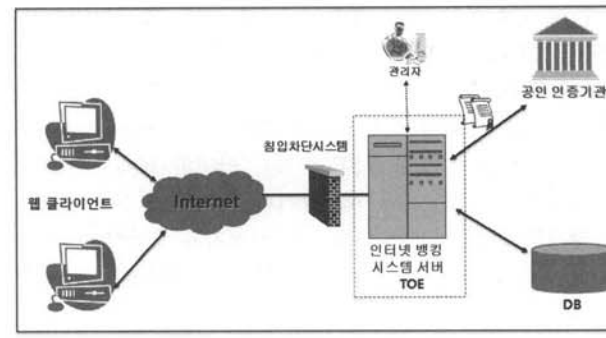
이와 같이 인터넷 뱅킹 시스템이 취약한 원인 중 시스템의 개발 및 구현이 대부분 아웃소싱으로 이루어지고 있는 점을 지적할 수 있다. 개발 업체는 금융 거래 시스템과 정보보호에 대한 충분한 이해와 기술력 없이 시스템을 설계하고 개발하기 때문에 이러한 취약점이 발생되고 있다.

인터넷 뱅킹 시스템의 문제점을 해결하기 위해서는 위협분석을 통해 보안요구사항을 도출하여 설계과정부터 시스템에 대한 검증이 필요하다. 2.1절에서 언급한 인터넷 뱅킹 시스템에 적용 가능한 표준들은 실제로 적용하기에는 적절하지 않다. 인터넷 뱅킹 시스템에 대한 위협들을 충분히 반영하고 있지 않을 뿐만 아니라, 설계과정부터 보안 기능 및 검증을 제공하지 않는다. 따라서 인터넷 뱅킹 시스템에 특화 된, 정보보호제품의 연동에 대한 보증과 모듈단위의 설계 과정에서부터 시스템에 대한 검증 및 보증까지 할 수 있는 기준이 필요하다.

본 논문에서는 이러한 기준을 제시하기 위해 공통평가기준(CC, Common Criteria[8-11])을 통하여 인터넷 뱅킹 시스템의 보안기능에 대한 보안요구사항을 도출한다. 3장은 TOE 설명 및 구성, 보안문제 정의, 보안목적 및 보안목적의 이론적 근거, 보안기능요구사항 및 보안기능요구사항의 이론적 근거로 구성된다.

3.1 TOE(Target Of Evaluation) 설명 및 구성

(그림 1)은 TOE의 운영환경을 보여준다. 인터넷 뱅킹 시스템의 운영환경은 사용자 PC의 웹 클라이언트와 인터넷 뱅킹 시스템 서버가 공용망을 통해서 통신이 이루어지고 인터넷 뱅킹 시스템 서버는 사용자 인증을 위한 공인증기관, 온라인 뱅킹과 관련한 사용자의 요청을 처리하는 DB와 연결되어 있다. TOE는 인터넷 뱅킹 시스템 서버이며 사용자에게 서비스를 제공하는 식별 및 인증 모듈, 보안관리 모듈, TSF(TOE Security Function) 데이터 보호 모듈, 사용자 데이터 보호 모듈, 보안감사 모듈로 구성 된다. 운영을 위해 부가적인 비-TOE로서 하드웨어, 소프트웨어 또는 펌웨어를 필요로 한다. 사용자는 인터넷 뱅킹 서비스를 제공 받기 위하여 웹 어플리케이션이나 웹 클라이언트 프로그램 등을 다운받아 사용한다. 사용자는 TOE 접근 시 사용자의 안전을 위하여 사용자에게 키보드 보안 솔루션인 키로깅 방지와 악



(그림 1) TOE 운영환경

성 코드 및 해킹을 방지하기 위한 프로그램을 TOE로부터 다운받아 안전한 접속이 유지되게 한다.

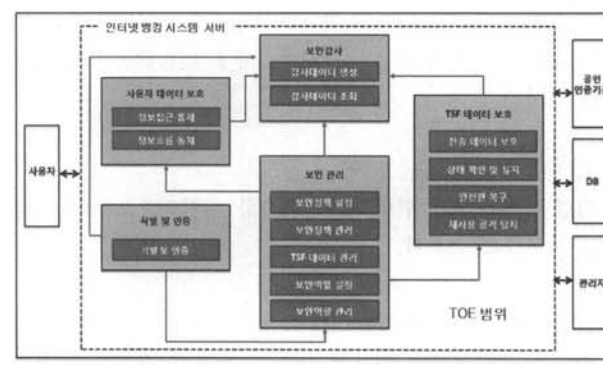
침입차단 시스템은 침입 차단기능을 포함한 정보보호 제품을 의미하며, TOE와 인터넷 사이에 위치하여 TOE를 운영하는데 필요한 모든 서비스를 허용한다. 관리자는 지역 또는 원격으로 TOE에 접근하여 TOE의 보안관리를 수행할 수 있다. 공인 인증기관과 TOE는 사용자 인증을 위하여 사용자가 TOE로 제출한 인증서 검정을 안전한 경로를 통하여 통신한다. 이때 공인 인증기관과 TOE 사이에 전송되는 시그너처는 기밀성과 무결성이 보장되어야 한다.

TOE의 주요 보안기능은 식별 및 인증, 보안관리, TSF 데이터 보호, 사용자 데이터 보호, 보안감사로 (그림 2)와 같이 구성된다.

TOE는 다음과 같은 보안기능을 제공한다.

식별 및 인증 : 식별 및 인증 기능은 관리자와 사용자의 식별 및 인증을 수행한다. TOE에 대한 접근은 정책에 따라 인가된 관리자만이 허용된다. 사용자의 경우 TOE에 접근하기 전에 공인 인증서 등을 통하여 사용자의 신원을 식별하고 인증한다.

보안 관리 : 보안관리 기능은 보안기능, TSF(TOE Security Functionality) 데이터, 보안 역할 등 관련 사항을 관리한다. 전체적인 TOE 보안 관리는 관리자만 담당한다. 그러나 조직의 정보보안 정책에 따라 관리자는 구분될 수 있다. 예를 들어 보안정책 설정 관리, 등록 관리, 세션 관리 등으로 구분할 수 있다.



(그림 2) TOE 범위

TSF 데이터 보호 : TSF 데이터 보호 기능은 TOE의 TSF를 보호하기 위하여 데이터의 가용성, 무결성, 비밀성 보호와 TOE 자체 상태 확인을 수행한다. TOE 운영중 관리자에게 TSF 데이터의 무결성과 TSF의 오동작을 판단하는 기능을 수행한다. 또한 TSF 손상시 안전한 상태로 복구할 수 있음을 보장하고, 재사용 공격이 탐지되는 경우 재사용을 방지를 위한 기능을 수행한다. 사용자와 온라인 뱅킹 서버 사이에 송수신되는 TSF 데이터들의 암호화는 SSL 등의 안전한 경로를 통해 지원받는다.

사용자 데이터 보호 : 사용자 데이터 보호 기능은 접근 통제 및 정보흐름 통제를 수행한다. 사용자 데이터 보호는 정책의 통제 범위에 대한 접근을 제어하고 정보의 흐름을 통제한다. 이를 통해 침입을 탐지하고 차단하며 대응할 수 있는 기능이 수행된다.

보안감사 : 보안관련 행동에 관한 정보의 인식, 기록, 저장, 분석 등 보안 레코드는 기록된다. 필요시 기록된 내용을 통해 어떤 보안 관련 행동이 발생 하였나 알 수 있고 그 발생에 대한 책임을 물을 수 있는 자료로도 활용될 수 있다.

3.2 보안문제 정의

보안문제 정의는 TOE 및 운영환경에 의해 대응되어야 하는 위협과 수행되어야 하는 조직의 보안정책 및 지원되어야 하는 가정사항으로 나누어 설명한다. 인터넷 뱅킹 시스템 서버의 위협원은 TOE에 불법적인 접근을 시도하거나 비정상적인 방법으로 TOE에 공격적인 행동을 하는 실체의 공격자와 인가된 사용자, 관리자, 시스템 소유자와 개발자 등이 있다. 위협원은 기본 수준의 전문지식, 자원, 동기를 가진다.

3.2.1 자산

IT 시스템에서 자산은 정보, 프로세스, 물리적 자산으로 나뉜다. 인터넷 뱅킹 시스템에서 정보 자산은 사용자 데이터, 시스템 데이터로 분류 한다. 사용자 데이터는 인터넷 뱅킹 시스템의 사용자를 식별하는 개인 정보와 사용자의 금융 관련 정보이다. 시스템 데이터는 시스템의 보안기능에서 사용되는 데이터로 보안기능 구성 데이터와 인증 데이터, 감사 정보가 있다. 정보 자산은 위치에 따라 저장 데이터와 전송 데이터로 분류 될 수 있다. 프로세스 자산은 관리, 감사, 통신, 인증 등의 프로세스를 포함한다. 물리적 자산은 정보와 프로세스 자산을 지지하기 위해 사용된 실제 정보 처리 장비로서 네트워크 기반 시설, 사용자의 PC, DB 서버 등이 있다.

3.2.1.1 위협(Threats)

위협을 도출하기 위해 앞서 서술한 취약점으로부터 기본적인 위협을 도출한다.

3.2.1.2 조직의 보안정책

조직의 보안정책은 위협에 대응하는 보안 기능을 적절하게 수행하기 위해 필요한 정책을 서술한다.

〈표 5〉 위협

위 협	설 명
T.가로채기	공격자는 인가된 사용자의 세션을 가로채어 인증 권한을 얻을 수 있다.
T.도청	공격자는 스니핑이나 키로깅을 통해 사용자와 시스템 간의 보안 정보를 도청 할 수 있다.
T.위조 데이터 전송	공격자는 알려진 메시지 형식에 따라 데이터를 위조하여 웹 어플리케이션으로부터 인증을 받거나, 원하는 정보에 대한 접근 권한을 가질 수 있다.
T.서비스 거부 공격	공격자는 시스템의 자원을 소모 시켜 적법한 사용자의 시스템 접근을 방해 할 수 있다.
T.암호기능 관리 오류	관리자의 부적절한 관리나 개발자의 잘못된 구현으로 인해 공격성공 가능성이 높은 암호 알고리즘을 사용하거나 암호 기능을 잘못 구성하거나 암호키를 평문으로 저장하여 정보를 노출 시킬 수 있다.
T.연속 인증 시도	공격자는 인터넷 뱅킹 시스템에 연속적으로 인증을 시도하여 입력 정보 및 인가된 사용자의 권한을 획득할 수 있다.
T.위장	공격자는 도청이나 우회접근, 위조 데이터를 통해 얻은 사용자 개인정보를 이용하여 정당한 사용자로 위장할 수 있다.
T.잔여정보	공격자 또는 인가된 사용자는 재할당된 자원으로부터 이전에 사용된 데이터를 취득하여 악용 할 수 있다.
T.재사용공격	공격자는 인가된 사용자의 인증 데이터를 재사용하여 인터넷 뱅킹 시스템의 보안기능에 접근할 수 있다.
T.저장 데이터 훼손	공격자 또는 인가된 사용자는 시스템에 저장된 데이터를 노출 또는 변경, 삭제 할 수 있다.
T.전송 데이터 훼손	공격자는 클라이언트와 서버의 통신에서 전송 정보를 변경하여 사용자의 금융 관련 정보를 훼손할 수 있다.
T.주소위장	공격자는 자신의 주소를 바꿔 인가된 사용자로 위장하여 보안기능에 접근 할 수 있다.

〈표 6〉 조직의 보안정책

보안정책	설 명
P.감사	서버-클라이언트 프로그램과 사용자 보안 솔루션의 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 적절하게 검토할 수 있어야 한다.
P.안전한 관리	인가된 관리자는 정기적인 교육을 통해 시스템을 안전하게 관리하고, 운영환경에 적절한 보안 관리 정책을 세우고 그에 따라 시스템을 운영해야 한다.
P.전송데이터보호	TOE는 클라이언트 키보드와 서버 사이에 전송되는 사용자 데이터를 인가되지 않은 노출, 변경으로부터 보호해야 한다.

3.2.1.3 가정사항

기술적인 기능 및 보증에서 해결 할 수 없는 위협에 대해서는 가정사항을 제시하여 위협을 해결 할 수 있도록 한다.

3.3 보안목적

본 논문에서는 제안하는 인터넷 뱅킹 시스템 서버가 만족해야 할 보안목적을 TOE에 대한 보안목적 및 운영환경에 대한 보안목적으로 분류하여 정의한다. TOE 보안목적은 TOE에서 직접 다루어지는 보안목적이고, 환경에 대한 보안목적은 IT 영역이나 비기술적/절차적 수단에 의해 이루어지는 보안 목적이다. TOE 보안목적은 'O' 인덱스로, 환경에 대한 보안목적은 'OE로 표기한다. <표 8>은 TOE에 대한 보안목적과 운영환경에 대한 보안목적을 서술한 것이다.

〈표 7〉 가정사항

가정사항	설 명
A. 물리적 보안	TOE는 물리적으로 안전한 환경에 위치하며 인가되지 않은 물리적 접근으로 부터 보호된다.
A.신뢰된 관리자	시스템의 인가된 관리자는 악의가 없으며, 시스템 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행한다.
A.운영체제보강	운영체제상의 취약점에 대한 보강작업이 수행되며, 운영체제에 대한 신뢰성과 안전성이 보장된다.
A.유일한연결점	시스템의 서버와 클라이언트간의 통신은 반드시 보안기능을 통과한다.
A.침입차단시스템	침입차단시스템은 시스템과 인터넷 사이에 위치하며, 시스템을 운영하는데 필요한 모든 서비스를 허용한다.

〈표 8〉 보안목적

보안목적	설 명
O.감사	인터넷 뱅킹 시스템은 보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야한다.
O.관리	인터넷 뱅킹 시스템은 안전한 방법으로 배포, 설치되어야 하며, 인가된 관리자가 인터넷 뱅킹 시스템을 효율적으로 관리할 수 있는 관리 수단을 제공하며 TSF 데이터를 최신상태로 유지하는 수단을 제공하여야한다.
O.식별 및 인증	인터넷 뱅킹 시스템 내 기능은 사용자를 유일하게 식별 및 인증해야 하고, 연속인증 실패에 대해 대응해야 한다.
O.안전한 암호 기능	개인 정보 및 사용자의 금융 관련 정보를 보호하기 위한 암호화/복호화 키는 안전하게 보호되어야 한다.
O.잔여정보제거	인터넷 뱅킹 시스템은 운영 시에 재할당된 자원으로 부터 접근권한에 사용가능한 잔여정보를 취득할 수 없어야한다.
O.TSF 데이터보호	인터넷 뱅킹 시스템은 TOE에 저장된 TSF 데이터 혹은 신뢰할 수 있는 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야한다.
O.정보흐름통제	인터넷 뱅킹 시스템은 클라이언트와 서버 간 통신의 전송 정보 즉 사용자 데이터 및 TSF 데이터를 인가되지 않은 정보의 유·출입을 통제 해야 한다.
O.침해사고식별/대응	인터넷 뱅킹 시스템에서 발생하는 침해사고 등에 관한 이벤트 관리, 분석 및 대응을 위해 보안 관리를 제공해야 한다.
O.해킹툴 차단	TOE는 서버 및 클라이언트에게 인터넷에서 유입되는 해킹툴을 방지하고 이에 대한 대응 수단을 제공해야 한다.
OE. 물리적 보안	TOE는 물리적으로 안전한 환경에 위치해야 하며, 인가되지 않은 물리적 접근으로부터 보호되어야 한다.
OE.신뢰된 관리자	인터넷 뱅킹 시스템은 신뢰된 관리자에 의해서 운영 및 관리 되어야 한다.
OE.운영체제보강	운영체제상의 취약점에 대한 보강 작업을 수행하여야 하며, TOE와 다른 응용프로그램간에 간섭이 없음을 보장해야 한다.
OE.유일한 연결점	사용자가 서버에 접속 시 TOE를 반드시 통과해야 한다.
OE.타임스탬프	TOE 운영환경에서 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안관련 사건을 정확하게 기록해야 한다.
OE.침입차단시스템	침입차단시스템은 시스템과 인터넷 사이에 위치하며, TOE를 운영하는데 필요한 모든 서비스를 허용해야 한다.

3.4 보안목적의 이론적 근거

보안목적의 이론적 근거는 앞서 제시한 보안 목적이 보안 문제를 다루기 충분하며, 과도하지 않고 반드시 필요한 것임을 입증하는 것이다.

- o 각 위협, 조직의 보안정책 및 가정사항이 최소한 하나의 보안목적에 의해서 다루어진다.
- o 각 보안목적은 최소한 하나의 위협, 조직의 보안정책, 가정사항을 다룬다.

3.5 보안기능요구사항

보안요구사항은 TOE에서 만족되는 기능 및 보증요구사항으로 나누어지는데 본 논문에서는 보안기능 요구사항만을 기술한다. 보증요구사항을 위한 평가보증등급(EAL)은 EAL4이고 공통평가기준 3부의 부록 패키지 형태로 구성될 수 있다. 본 보안기능요구사항은 앞에서 식별한 보안목적을 만족시키기 위하여 공통평가기준 2부의 컴포넌트를 선정하여 사용한다. TOE에서 요구되는 보안기능요구사항 컴포넌트는 <표 10>과 같다.

3.6 보안기능요구사항의 이론적 근거

보안기능요구사항의 이론적 근거는 서술된 보안요구사항이 보안목적을 만족시키기에 적합하고, 그 결과 보안문제를 다루기에 적합함을 입증한다. 그러므로 각 TOE의 보안목적은 적어도 하나의 TOE 보안기능요구사항에 의해서 다루어지고 각 보안기능요구사항은 적어도 하나의 TOE 보안목적을 다룬다. 다음의 <표 11>은 보안목적과 보안기능요구사항의 사이의 대응관계를 나타낸다.

4. 결 론

인터넷 뱅킹 시스템은 인터넷과 보안 기술의 발달로 소비자에게 다양한 서비스를 제공하고 있으며 점점 그 사용량이 증가하고 있다. 하지만 금융기관의 보안에 대한 인식 부족과 기술력의 부족으로 인해 보안 기술이 제대로 시스템에 적용되지 못하고 있다. 이로 인하여 인터넷 뱅킹 시스템에 여러 보안 취약점이 발생하였고, 악의적인 공격 목표가 되고 있다.

〈표 9〉 보안목적의 이론적 근거

보안목적 / 보안문제 정의	O. 감사	O. 관리	O. 식별 및 인증	O. 안전한 암호기능	O. 잔여정보 제거	O. TSF 데이터보호	O. 정보흐름 통제	O. 침해사고 식별/대응	O. 해킹툴 차단	OE. 물리적 보안	OE .신뢰된 관리자	OE. 운영체제 보강	OE. 유일한연 결점	OE. 타임스탬 프	OE. 침입차단 시스템
T.가로채기							X								
T.도청							X								
T.위조 데이터 전송							X								
T.서비스 거부 공격	X							X							
T.암호기능 관리 오류				X											
T.연속 인증 시도			X												
T.위장	X		X					X							
T.잔여정보					X										
T.재사용공격			X					X							
T.저장 데이터 훼손			X			X									
T.전송 데이터 훼손							X								
T.주소위장	X		X					X							
P.감사	X													X	
P.안전한 관리		X									X				
P.전송데이터보호									X						
A. 물리적 보안										X					
A.신뢰된 관리자											X				
A.운영체제보강												X			
A.유일한연결점													X	X	
A.침입차단시스템															X

〈표 10〉 보안기능 요구사항

보안기능클래스	보안기능 컴포넌트		보안기능클래스	보안기능 컴포넌트	
보안 감사	FAU_ARP.1	보안경보	식별 및 인증	FIA_UAU.7	인증 피드백 보호
	FAU_GEN.1	감사 데이터 생성		FIA_UID.2	모든 행동 이전에 사용자 식별
	FAU_SAR.3	선택 가능한 감사검토	보안 관리	FMT_MOF.1	보안기능 관리
	FAU_STG.1	감사 증적 저장소 보호		FMT_MSA.1	보안속성 관리
	FAU_STG.3	감사 데이터 손실 예측 시 대응 행동		FMT_MSA.3	정적 속성 초기화
	FAU_STG.4	감사 데이터의 손실 방지		FMT_MTD.1	TSF 데이터 관리
암호 지원	FCS_CKM.1	암호키 생성		FMT_MTD.2	TSF 데이터 한계치의 관리
	FCS_CKM.2	암호키 분배		FMT_SMF.1	관리기능 명세
	FCS_CKM.4	암호키 파기		FMT_SMR.1	보안 역할
사용자 데이터 보호	FDP_DAU.2	증거 생성자의 신원을 포함한 데이터 인증	TSF 보호	FPT_ITC.1	외부전송 TSF 데이터의 비밀성
	FDP_IFC.1	부분적인 정보흐름통제		FPT_ITI.1	외부전송 TSF 데이터의 변경 탐지
	FDP_IFF.1	단일 계층 보안속성		FPT_TST.1	TSF 자체 시험
	FDP_RIP.2	전체적인 잔여정보 보호		FPT_RPL.1	재사용 공격 탐지 및 대응행동
	FPT_ITT.1	내부전송 TSF 데이터의 기본적인 보호	TOE 접근	FTA_MCS.1	기본적인 동시 세션 수의 제한
식별 및 인증	FIA_AFL.1	인증 실패 처리		FTA_SSL.1	TSF에 의한 세션 잠금
	FIA_UAU.1	인증		FTA_SSL.3	TSF에 의한 세션 종료
	FIA_ATD.1	사용자 속성 정의			

〈표 11〉 보안목적과 보안기능요구사항 대응

보안목적 / 보안문제 정의	O. 감사	O. 관리	O. 식별 및 인증	O. 안전한 암호 기능	O. 잔여 정보 제거	O. TSF 데이터 보호	O. 정보 흐름 통제	O. 침해 사고 식별/대응	O. 해킹 툴 차단	보안목적 / 보안문제 정의	O. 감사	O. 관리	O. 식별 및 인증	O. 안전한 암호 기능	O. 잔여 정보 제거	O. TSF 데이터 보호	O. 정보 흐름 통제	O. 침해 사고 식별/대응	O. 해킹 툴 차단
FAU_ARP.1	X							X	X	FIA_UAU.7			X						
FAU_GEN.1	X									FIA_UID.2		X	X			X			
FAU_SAR.3	X									FMT_MOF.1		X							
FAU_STG.1	X									FMT_MSA.1		X							
FAU_STG.3	X									FMT_MSA.3		X							
FAU_STG.4	X									FMT_MTD.1		X							
FCS_CKM.1				X						FMT_MTD.2		X							
FCS_CKM.2				X						FMT_SMF.1		X							
FCS_CKM.4				X	X					FMT_SMR.1		X							
FDP_DAU.2			X							FPT_ITC.1		X							
FDP_IFC.1							X			FPT_ITI.1							X		
FDP_IFF.1							X			FPT_TST.1						X			
FDP_RIP.2					X					FPT_RPL.1								X	X
FPT_ITT.1						X				FTA_MCS.1			X					X	
FIA_AFL.1			X							FTA_SSL.1		X				X			
FIA_UAU.1		X	X			X				FTA_SSL.3		X				X			
FIA_ATD.1			X																

본 논문에서는 인터넷 뱅킹 시스템의 보안을 강화하기 위해 제도적인 측면에서 대안을 제시한다. 기존의 표준 및 제도를 분석하고 인터넷 뱅킹 시스템에 단일 표준을 적용함으로써 현재의 시스템이 보안을 보증하지 못하는 이유를 분석하였다. 그리고 이러한 문제점을 보강하기 위해 인터넷 뱅킹 시스템에 특화된 보호프로파일은 제안하였다. 본 논문에서 제안한 보호프로파일은 인터넷 뱅킹 시스템의 취약성으로부터 도출한 보안기능요구사항을 포함하기 때문에 효과적으로 인터넷 뱅킹 시스템의 취약성을 방지 할 수 있다. 또한 본 보호프로파일은 공통평가기준에 의해 작성되어 정보보호시스템 평가를 전문으로 하는 평가기관에 의해 참고 될 수 있고 인터넷 뱅킹 시스템을 관리하는 입장에서 보안목표명세서 작성 시 활용 될 수 있다.

참 고 문 헌

[1] 김성천, 장희만, 신용녀, "범금융 산업 메시지 체계 표준화 동향", TTA Journal No.126, 2009.

[2] ISO, International Standards ISO/IEC 27001, "Information technology Security Techniques-Information security management Systems-Requirements," 2005.

[3] 정보시스템의 구축·운영 기술 지침, 정보통신부 고시 제 2006-37호, 2006. 9. 11.

[4] ISO/IEC 2nd WD 15446, Guide for the production of protection profiles and security targets, 2007. 01. 22.

[5] James C. Foster, Vitaly Osipov and Nish Bhalla, "Buffer Overflow Attacks," 2005.

[6] The Open Web Application Security Project, "OWASP TOP 10" www.owasp.org., 2010.

[7] 조혜숙 외5, "상이한 DRM 시스템의 호환성을 위한 보호프로파일 개발에 관한 연구", 정보처리학회논문지C, 제16-C권, 제1호, 2009.2.

[8] International Standard ISO/IEC 18045, "Common Methodology for Information Technology Security Evaluation," Version 3.1, Revision 3, 2009.07.

[9] International Standard ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation, Part1," Version 3.1, Revision 3, 2009.07.

[10] International Standard ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation, Part2," Version 3.1, Revision 3, 2009.07.

[11] International Standard ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation, Part3," Version 3.1, Revision 3, 2009.07.

[12] 정보통신부, "전자거래 안전성 강화 종합대책", 2005.09.

[13] 전자금융거래법, 법률 제9325호, 2008.12.

[14] 한국정보통신기술협회, "OTP 암호키관리 보안 요구사항", 2009.12.

[15] 송성현, 남형준, 권태경, "MITM 공격에 강인한 OTP시스템 설계", 한국정보보호학회, 2009.6.

[16] 한국정보통신기술협회, "웹 환경 구축 및 운영을 위한 보안 관리 지침", TTAS.KO-10.0090, 2006.12.

[17] 조혜숙, 이성진, 조성규, 김승주, 원동호, "온라인 금융거래 시스템을 위한 관련 표준 분석에 관한 연구", COMSW2009, 2009.7.

[18] 유진호, 지상호, 임종인, "개인정보 유.노출 사고로 인한 기업의 손실비용 추정", 정보보호학회논문지, 2009.08

조 혜 숙

e-mail : hsjo@security.re.kr

2003년 한성대학교 멀티미디어정보처리과 (학사)

2005년 성균관대학교 전자전기컴퓨터공학과 (공학석사)

2006년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정

관심분야 : 암호이론, 정보보호, 보안성평가, 무선네트워크

김 승 주

e-mail : skim@security.re.kr

1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)

1998년~2004년 한국정보보호진흥원(KISA) 팀장

2004년~현 재 성균관대학교 정보통신공학부 교수

2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원

2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가

2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장

2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원

관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호

e-mail : dhwon@security.re.kr

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공업대 객원연구원

1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원

2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장

관심분야 : 암호이론, 정보이론, 정보보호