ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

인터넷 뱅킹 서비스 보안기술의 현황과 미래☆

Status and Future of Security Techniques in the Internet Banking Service

이 경 률[1] 임 강 빈[2] 서 정 택[2]*
Kyungroul Lee Kangbin Yim Jungtaek Seo

요 약

인터넷 뱅킹 서비스가 보편화되면서 많은 사용자들이 온라인을 통한 재화의 교환이 가능하였다. 하지만 이러한 이점에도 불구하고 인터넷 뱅킹 서비스에서 존재하는 보안위협에 의하여 사고사례가 지속적으로 발생하는 실정이다. 이러한 문제점을 보완하기 위하여 인터넷 뱅킹 서비스의 전 구간에 걸쳐 다양한 보안기술이 적용되었으며, 본 논문에서는 금융기관 구간과 네트워크 구간에 적용된 보안기술에 대한 조사 결과를 서술한다. 본 논문의 결과를 통하여 내부자에 의하여 발생하는 피해사례와 구현과정에서의 취약점으로 인하여 발생하는 위협에 대응하기 위한 참고 자료로써 활용 가치가 있을 것으로 사료된다.

☞ 주제어 : 인터넷 뱅킹 서비스, 보안 기술, 기술 분류, 금융기관 구간, 네트워크 구간

ABSTRACT

As Internet banking service became popular, many users can exchange goods by online. Even though this advantage, there are incident cases in the Internet banking service due to security threats. In order to counteract this problem, various security techniques have been applied over whole area in the Internet banking service. Therefore, we described that analyzed results of security techniques applied in the financial institutions area and network communication area in this paper. We consider that this paper will be useful as a reference to protect security threats occurred by insiders and vulnerabilities in implementation.

☞ keyword : Internet Banking Service, Security Techniques, Technical classification, Financial institution area, Network communication area

1. 서 론

인터넷 뱅킹 서비스에서의 다양한 보안위협에 의하여 다수의 사고사례가 발생하였다. 이를 규제하기 위하여 전자서명법 등 인터넷 뱅킹 서비스와 관련된 법률을 제정하였지만, 법률은 사고 후의 조치를 취하기 위한 수단일 뿐 사고 자체를 예방하지는 못한다. 이에 인터넷 뱅킹 서비스에서 활용하는 온라인 본인확인수단의 안전성을 제공하기 위하여 다양한 보안기술이 연구되었다. 따라서 본 논문에서는 인터넷 뱅킹 서비스의 안전성을 확보하고자 연구된 보안기술을 네트워크 영역, 금융기관 영역으로 분류하고 각 기술에 대하여 조사한 결과를 상세히 서술하고자 한다.

2. 보안기술 분류

2005년 5월, 국내 최초로 인터넷 뱅킹 사고가 발생하였으며, 이와 같은 위협에 대응하고자 키보드 보안 프로그램과 PKI 응용 프로그램 등의 보안기술을 도입하였다. 이러한 기술들은 주요한 해킹사고가 발생할 때마다 발전하였으며, 이를 (그림 1)에 나타내었다[1].

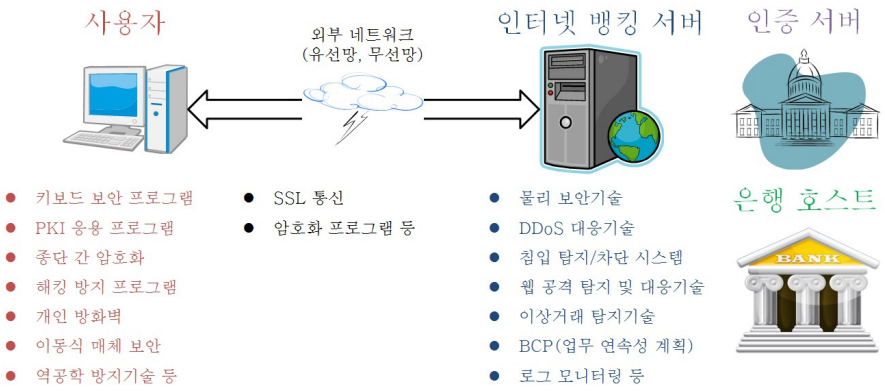
현재는 사용자 PC와 같은 전자적 장치와 유/무선기반의 네트워크, 인터넷 뱅킹 서버, 인증서버, 은행 호스트를 포함한 금융기관에서 다양한 위협에 대응하기 위하여 (그림 2)와 같은 구간별 보안기술이 연구되었다.

1 R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University, Asan, 31538, South Korea.
2 Dept. of Information Security Engineering, Soonchunhyang University, Asan, 31538, South Korea.
* Corresponding author (seojt@sch.ac.kr)
[Received 1 February 2017, Reviewed 3 February 2017, Accepted 2 March 2017]
☆ 본 연구는 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01057300). 본 연구는 순천향대학교 학술연구비 지원으로 수행하였음.

https://doi.org/10.7472/jksii.2017.18.2.31

	1999년	2000년 9월	2002년~2005년	2005년 12월	2007년~현재
컴플라이언스	인터넷 뱅킹 서비스 출시	전자서명법 개정		전자금융거래 보안강화조치	전자금융거래법 강화
보안조치 전자적 장치	아이디/비밀번호 → 공인인증서 (사용자 인증)		보안카드	키보드 보안 프로그램 해킹 방지 프로그램 보안카드의 조합 번호 OTP	안티 피싱/파밍 종단 간 암호화 가상 브라우저 HSM
보안조치 별도 장치					
주요 해킹사고	아이디/비밀번호 유출	악성코드에 의한 공인인증서 유출	악성코드에 의한 보안카드 유출	악성코드, 피싱, 중간자 공격에 의한 고객정보 유출	DDoS 공격, 사회공학에 의한 고객정보 유출

(그림 1) 국내 인터넷 뱅킹 서비스 보안기술의 발전과정
(Figure 1) Development process of security technologies for the Internet banking service



(그림 2) 인터넷 뱅킹 서비스에서의 보안기술 분류
(Figure 2) Classification of security techniques for the Internet banking service

3. 금융기관 구간에서의 보안기술

금융기관 구간에서의 보안기술은 물리 보안기술, DDoS 공격 대응기술, 침입 탐지/차단 시스템, 웹 공격 탐지 및 대응기술, 데이터베이스 보안기술, 이상거래 탐지기술, 업무 연속성 계획(BCP, Business Continuity Planning), 로그 모니터링 기술로 분류된다. 금융기관 구간은 보안이 매우 강화된 구조를 이루고 있어 공격자에게는 주요한 공격대상은 아니지만, 내부자에 의한 피해 사례가 존재한다. 따라서 본 논문에서는 이러한 기술에 대한 분석 결과를 서술하며 그 분류를 (표 1)에 나타내었다.

3.1 물리 보안기술

물리 보안기술[18, 19]은 이익이 창출되지 않는 분야라는 이유로 대부분 적극적으로 도입하지 않는 실정이다. 심지어 인터넷 데이터 센터(IDC, Internet Data Center)와 같이 높은 수준의 보안이 유지되어야 하는 시설에서도 관리가 미흡하며, 보여주기 식의 시스템을 도입하는 것이 현실이다. 하지만 내부 직원에 의한 유출사고가 발생함으로써 물리 보안기술에 대한 중요성이 대두된다.

금융기관이나 인증기관의 경우, 개인정보와 같이 매우 중요한 정보를 저장하므로 인력이나 자산 등과 같은 모든 자원을 관리하고 통제하여야 한다. 이를 통하여 발생

(표 1) 금융기관 구간에서의 보안기술
(Table 1) Security techniques for the financial institutions

대분류	소분류	보안기술
물리 보안 기술	물리 보안과 관련된 법적 제도 및 지침	• 건축법의 지능형 건축물인증제도 • 집적정보 통신시설 보호지침에 관한 고시 • 국가 보호시설 관리지침
	CCTV를 통한 물리 보안기술	• 특정 장소 촬영 • 경고 및 추적기능 • 영상보안 및 키 관리
	출입통제를 통한 물리 보안기술	• 잠금장치 • 제한구역 및 통제구역의 통제 정책
	보안 인프라 시스템 운영 및 관리	• 통합적인 보안 인프라 시스템 운영 및 관리(경보장치, CCTV 등) • 보안상황실 운영
	저장매체 폐기 정책	• 전면 덮어쓰기와 같은 소프트 소거 • 파쇄 및 소각과 같은 물리적 파괴
DDoS 공격 대응 기술	장비 설정 적용 및 다양한 연구 진행	• SYN ICMP, UDP flooding 공격 대응 • MAC, DHCP spoofing 공격 대응
침입 탐지/ 차단 시스템	호스트 기반 방식	• 시스템 콜이나 API의 호출 • 자원에 대한 불법 접근 탐지 및 차단
	네트워크 기반 방식	• 비정상적인 패킷 탐지 및 차단
웹 공격 탐지 및 대응 기술	검색 사이트를 통한 개인정보 유출 대응기술	• 웹 필터링 솔루션 활용 • 문자열의 이미지 변환
	홈페이지 취약점을 이용한 정보유출 대응기술	• 웹 서비스 보안 설정 • 웹 방화벽 도입
데이터베이스 보안 기술	컬럼 암호화 방식	• 플러그인, API, 하이브리드 방식
	블록 암호화 방식	• TDE, 파일 암호화 방식
이상 거래 탐지 기술	패턴기반 탐지	• 사용자의 환경이나 행위에 대한 패턴 탐지
업무 연속성 계획 (BCP)	국제표준	• ISO 22301, BC Practitioners • BC 25999, BCM Guidelines
로그 모니터링	로그 기록 및 모니터링	• 증거 확보 및 차단목록 후보 생성

가능한 물리적 사고를 예방하고, 사고 발생 시 피해를 최소화할 수 있으며, 사고 원인을 신속히 파악함으로써 해결이 가능하다. 자원의 관리 및 통제를 위해서는 적절한 기준이 필요하며, 국내의 법적 제도 및 지침에는 건축법의 지능형건축물인증제도, 한국인터넷진흥원의 집적정보 통신시설 보호지침에 관한 고시와 국가보호시설 관리지침 등이 있다. 이에 대한 일례로 집적정보 통신시설 보호지침의의 세부기준 일례를 (표 2)에 나타내었다[2, 3].

(표 2) 집적정보 통신시설 보호지침 세부기준 일례
(Table 2) An example of detailed guidelines for the protection of ICT facilities

항목	설명
출입통제 장치	• 주요시설중 중앙감시실, 전산실, 전력감시실, 통신장비실, 방재센터의 출입구에는 출입자의 신원확인을 통해 개폐되는 잠금장치를 설치한다.
출입기록	• 주요시설에 대한 출입기록(모든 출입자의 신원과 방문목적 및 방문일시에 대한 기록, CCTV녹화, 출입통제장치의 로그기록)을 출입일로부터 2개월 이상 유지되도록 보관한다. • 주요시설이외의 시설에 대한 출입기록(외부 방문자의 신원과 방문목적 및 방문일시에 대한 기록)을 출입일로부터 1개월 이상 유지되도록 보관한다.
고객정보 시스템 장비 보호	• 전산실내에 보관하여 관리하는 고객의 컴퓨터장비 등 정보시스템 장비는 잠금장치가 있는 구조물에 설치한다.
중앙 감시실	• 주요시설중 전산실 및 통신장비실에 대하여 각 시설의 기능별 작동상황 및 사고발생여부를 확인한다. • CCTV가 촬영한 영상을 24시간 감시할 수 있는 모니터를 설치한다.
CCTV	• 주요시설의 출입구와 주요시설중 전산실 및 통신장비실 내부에 CCTV를 설치한다.

CCTV는 고정된 장소에 설치되어 촬영하는 카메라로써 직접적으로 통제에 관여하지는 않지만, 사고를 예방하거나 증거를 확보하여 신속히 대처하는데 기여한다. 과거에는 특정 장소를 촬영하는 기능만을 제공하였지만, 현재는 지능화된 기술과 융합되어 통제된 구역에 침입할 경우 경고를 발생하거나 선택된 사람에 대한 추적기능 등을 제공함으로써 더욱 신속한 대처가 가능하다. 이러한 CCTV는 사각지역이 없도록 설치되어야 하고, 알람시스템과 연동시켜 알람이 작동할 경우 특정 장소를 집중적으로 녹화하거나 영상의 화질을 높이는 등의 기능을 제공할 수 있도록 한다[2].

출입통제를 통한 물리 보안기술은 출입문에 잠금장치를 설치함으로써 인가되지 않은 제3자의 출입을 제한하는 것으로, 생체인증, 스마트카드, 비밀번호와 같은 간접적인 방법을 활용하거나, 대면확인과 같은 직접적인 방법을 활용함으로써 출입을 인가한다. 또한, 건물 내 제한구역과 통제구역을 나누어 내부인과 외부인의 출입을 관리하는 정책이 있으며, 이에 대한 일례를 (표 3)에 나타내었다[2].

경보장치, 출입통제시스템, CCTV와 같은 보안장비를 활용하여 통합적인 보안 인프라 시스템을 운영하고 관리하여야 하며, 이를 위한 보안상황실을 운영하도록 한다. 보안상황실에는 모니터링 시스템을 구축하여 24시간 감시하고 조치하여야 하며, 위험상황에 대처하는 교육과 훈련이 이루어져야 한다[2].

(표 3) 제한구역 및 통제구역의 통제정책 일례
(Table 3) An example of control policies of restricted areas and controlled area

항목	설명
출입통제 장치	• 주요시설중 중앙감시실, 전산실, 전력감시실, 통신장비실, 방재센터의 출입구에는 출입자의 신원확인을 통해 개폐되는 잠금장치를 설치한다.
출입기록	• 주요시설에 대한 출입기록(모든 출입자의 신원과 방문목적 및 방문일시에 대한 기록, CCTV녹화, 출입통제장치의 로그기록)을 출입일로부터 2개월 이상 유지되도록 보관한다. • 주요시설이외의 시설에 대한 출입기록(외부 방문자의 신원과 방문목적 및 방문일시에 대한 기록)을 출입일로부터 1개월 이상 유지되도록 보관한다.
고객정보 시스템 장비 보호	• 전산실내에 보관하여 관리하는 고객의 컴퓨터장비 등 정보시스템 장비는 잠금장치가 있는 구조물에 설치한다.
중앙 감시실	• 주요시설중 전산실 및 통신장비실에 대하여 각 시설의 기능별 작동상황 및 사고발생여부를 확인한다. • CCTV가 촬영한 영상을 24시간 감시할 수 있는 모니터를 설치한다.
CCTV	• 주요시설의 출입구와 주요시설중 전산실 및 통신장비실 내부에 CCTV를 설치한다.

(표 4) 저장매체 삭제 방식 및 특징
(Table 4) Deletion methods and characteristic of storage medium

분류	방식	특징
윈도 우즈	FDISK	• 파티션 정보의 단순 재설정 • 데이터가 남아있어 복구 가능
	High level format	• FAT 정보 초기화 • 데이터 복구 가능
	Low level format	• 복구 가능성 존재
소프트 소거	전면 덮어쓰기	• 장시간 소요(수시간~10시간 이상, 수회 실시) • 낮은 보안성, 불량 시 삭제불가
소자 (디가우저)	강한 자기장 이용	• 기록된 데이터 완전 삭제 가능 • 단시간 소요(10초~1분 이내) • 대량의 데이터 삭제 가능
물리적 파괴	파쇄	• 대형장치 및 원격지 이동 필요, 소음 발생 • 조각 크기를 0.25mm 이하로 파쇄
	소각	• 소각 시 유해물질 방출 • 소각로, 용광로 등으로 한정 • 이동에 따른 정보유출 가능
	산성 물질로 용해	• 현실적으로 어려움

저장매체 내에는 각종 기밀정보가 저장되며, 삭제하거나 포맷을 하여도 이를 복구하는 다양한 방법이 존재한다. 따라서 기밀정보와 같은 데이터를 완전히 제거하기 위한 저장매체 폐기 정책이 요구되며, 이에 대한 일례를 (표 4)에 나타내었다[2].

3.2 DDoS 공격 대응기술

DDoS 공격은 금융기관과 같은 기관이나 업체가 제공하는 서비스를 이용할 수 없도록 패킷을 대량으로 발생시키거나 서버의 자원을 소모하는 패킷을 전송함으로써 네트워크 장비나 서버의 자원을 고갈시키는 공격이다. 이와 같은 공격에는 SYN, ICMP, UDP, DHCP, TCP Syn flooding 공격, IP 주소 변조 공격, MAC, DHCP spoofing, ARP 또는 ICMP를 이용한 공격 등이 있으며, 네트워크 장비의 설정을 변경함으로써 일부 대응이 가능하고 다양한 연구가 진행되고 있으므로 자세한 내용은 생략한다[4].

3.3 침입 탐지/차단 시스템

침입 탐지/차단 시스템은 DDoS 공격을 포함한 다양한 침입을 탐지하고 차단하는 시스템으로, 설치 위치에 따라 호스트 기반 방식과 네트워크 기반 방식으로 분류된다. 호스트 기반 시스템은 특정 서버나 호스트에 설치되며, 운영체제나 응용 프로그램과 같은 자원을 보호하는 형태로 시스템 콜이나 API의 호출, 자원에 대한 불법 접근을 커널과 유저모드 사이에서 탐지하고 차단하는 방식이다. 네트워크 기반 시스템은 네트워크상에서 인라인 형태로 직접 연결되어 비정상적인 패킷을 탐지하고 차단하는 방식이다[4]. 또한, 탐지 및 차단방식도 그 특성에 따라 차단 목록 기반의 필터링, 허용 목록 기반의 필터링, 부여 등급 기반의 필터링 방식으로 분류된다. 차단 목록 기반의 필터링 방식은 위협적인 패킷에 대한 차단 목록을 작성하고 해당 패킷이 유입되는 경우에는 이를 차단하는 방식이고, 허용 목록 기반의 필터링 방식은 위협적이지 않은 패킷에 대한 허용 목록을 작성하고 해당 패킷이 유입되는 경우에는 이를 허용하는 방식이며, 부여 등급 기반의 필터링 방식은 접근 가능한 정보에 대하여 등급을 부여하고 부여된 등급보다 높은 등급의 정보에 접근할 경우 이를 차단하는 방식이다[5].

3.4 웹 공격 탐지 및 대응기술

금융 대출 사이트나 쇼핑몰 등에서 운영하는 웹 사이트를 해킹하여 개인정보가 유출되는 사고가 발생함에 따라 웹 공격을 탐지하고 대응하는 기술에 대한 관심이 높아지고 있다. 이와 같은 공격은 웹 어플리케이션이 가지는 취약점에 의하여 발생하는 경우가 대부분이며, 검색 사이트를 통하여 개인정보가 유출되거나 홈페이지 취약

점(OWASP, Open Web Application Security Project)을 이용한 정보유출이 있다[2].

검색 사이트를 통한 개인정보 유출에 대한 대응기술로는 웹 필터링 솔루션을 활용하거나 이미지를 활용한 방안이 있다. 웹 필터링 솔루션을 활용한 방안은 웹 페이지에 작성되는 내용에 개인정보가 포함될 경우, 이를 차단하는 방안으로 개인정보뿐만 아니라 음란물이나 불법적인 광고를 차단하도록 확장할 수 있다. 이와 같은 방안은 외부에서 내부로 들어오는 패킷을 차단하는 인바운드 웹 필터링/차단 기술과 내부에서 외부로 나가는 패킷을 차단하는 아웃바운드 웹 필터링/차단 기술로 분류된다[2]. 이미지를 활용한 방안은 게시물이 검색 엔진에 노출되지 않도록 이미지로 변환하는 방안이다[6].

홈페이지 취약점(OWASP)을 이용한 정보유출에 대한 대응기술로는 웹 서비스 보안 설정과 웹 방화벽 도입을 통한 보안성 향상이 있다. 웹 서비스 보안 설정은 웹 어플리케이션의 작성단계부터 취약점을 고려하여 설계하여야 하지만, 이미 완성된 경우에는 이를 수정하는 것이 쉽지 않으므로 모든 사용자 입력 값이 안전하지 않은 것으로 간주하여 입력 값 검증과 인증, 세션을 안전하게 관리하도록 개발하여야 한다. 웹 방화벽 도입을 통한 보안성 향상은 이미 개발된 웹 어플리케이션을 수정할 필요가 없이 웹 방화벽을 설치함으로써 취약점에 대응하는 방법으로 설치가 간편하다는 장점이 존재한다[2].

그 밖에 웹 기반 공격을 탐지하는 방안으로는 호스트 기반 탐지기술, 네트워크 기반 탐지기술, 오용 탐지기술, 비정상행위 탐지기술, 오용 탐지와 비정상행위 탐지를 혼합한 탐지기술이 있다[7]. 호스트 기반 탐지기술은 시스템의 운용 기록을 이용한 방법이고[8], 네트워크 기반 탐지기술은 IP 주소와 포트를 이용한 방법이며[9, 10], 오용 탐지기술은 알려진 취약점을 패턴으로 정의한 후, 패턴과 일치하는 경우를 침입으로 탐지하는 방법이다. 비정상행위 탐지기술은 정상적인 모델을 학습시킨 후, 학습된 모델에 벗어나는 경우를 침입으로 탐지하는 방법이며, 오용 탐지와 비정상행위 탐지를 혼합한 탐지기술은 정상적인 행위와 비정상행위에 대한 패턴을 생성한 후, 생성된 두 패턴을 기반으로 탐지하는 방법이다[7].

3.5 데이터베이스 보안기술

데이터베이스는 서비스에 필요한 각종 정보를 저장하고 관리하기 위한 데이터 집합이다. 다양한 정보가 저장되고 공유되는 특성으로 인하여 외부로 노출될 경우에는 심각한 피해가 발생하므로 이를 보호하기 위한 보안기술이 요구된다. 이를 위한 기술로 암호화를 통한 보안기술이 일반적이며, 관련 법률로는 개인정보보호법 제24조 3항, 정보통신망법 제28조 2항, 전자금융감독규정 제17조 1항, 제32조, 제33조 1항이 있다. 데이터베이스를 암호화하는 방식은 컬럼 암호화 방식과 블록 암호화 방식으로 분류되며, 각 방식별 내용을 (표 5)에 나타내었다[11].

3.6 이상거래 탐지기술

이상거래 탐지기술은 본인확인수단으로도 활용되지만, 보통 보안기술로 활용된다. 사용자의 거래에 이용되는 정보는 특정한 환경이나 행위와 같이 패턴을 정의할 수 있으므로 정상적인 거래에 활용된 정보를 토대로 패턴을 생성하고, 생성된 패턴을 기반으로 패턴에 벗어나는 거래를 악의적인 이상거래로 탐지하는 기술이다. 패턴을 생성하기 위하여 활용되는 정보는 접속정보, 거래정보,

(표 5) 데이터베이스 암호화 제품 유형별 특징
(Table 5) Data encryption features by product type

방식	제품 유형	운영 형태	설명
컬럼 암호화 방식	플러그인	데이터베이스 서버	암/복호화 모듈을 데이터베이스 서버 내에 설치하여 암/복호화 수행
	API	데이터베이스 & 어플리케이션 서버	암/복호화 모듈을 어플리케이션 서버에 설치하여 암/복호화 수행
	하이브리드 (플러그인+API)	데이터베이스 & 어플리케이션 서버	암/복호화 모듈을 데이터베이스 서버와 어플리케이션 서버에 설치하고 필요에 따라 일부를 API 방식을 이용하거나 플러그인 방식을 이용하여 암/복호 수행
블록 암호화 방식	TDE 방식	데이터베이스 서버	데이터베이스에 내장되거나 옵션으로 제공되는 암/복호화 기능 이용
	파일 암호화	데이터베이스 & 어플리케이션 서버	OS상의 개체인 파일을 전체 암/복호하는 방식
기타		데이터베이스 or 어플리케이션 서버	토큰 방식, secure proxy 방식, 필터 방식, appliance 방식

행동정보로 분류되며, 접속정보는 IP 주소, MAC 주소, 하드디스크 시리얼넘버, 브라우저 정보, 운영체제 정보 등이 있고, 거래정보는 송금자, 거래시간, 거래금액 등이 있으며, 행동정보는 사용자가 거래를 하는 과정, 예를 들어 계좌이체일 경우 잔액조회 후 계좌이체를 하는 순서와 같은 사용자의 습관 등이 있다. 이러한 정보를 토대로 패턴을 생성할 수 있으며, 패턴에 벗어나는 거래가 탐지될 경우, 예를 들어 한 번의 거래 후 짧은 시간 내에 이동할 수 없는 거리에서 거래를 시도하는 경우가 탐지될 때, 이에 대한 경고를 발생하거나 OTP 생성기와 같은 추가적인 본인확인을 요구하는 방법으로 대응한다[12].

3.7 업무 연속성 계획(BCP)

BCP는 업무 연속성 계획으로 2010년 겨울 온도조절장치 동파로 인하여 전산망이 마비되는 사고와 2013년 초 사이버 공격에 의한 전산망 마비로 전자금융거래가 지연되는 사고가 발생되면서 물리적이나 전자적 공격 또는 천재지변 등으로 인하여 업무를 제공할 수 없을 때, 손실을 최소화하고 신속히 복구할 수 있는 일련의 계획을 의미한다. 2001년 미국에서 발생한 9.11 테러와 2004년 인도양 쓰나미 사건을 계기로 BCP에 대한 중요성이 부각되었고 표준화 활동도 활발히 진행되었으며, 표준 현황을 (표 6)에 나타내었다[13]. 국내에서는 LIG 손해보험이 2012년 6월에 ISO 22301을 취득하였다[14].

3.8 로그 모니터링

로그 모니터링은 사용자가 인터넷 뱅킹 서비스를 이용하였던 내역에 대한 로그를 기록하고 기록된 로그를 모니터링 함으로써 불법적인 접속이나 이용의 단서, 혹은 증거를 확보할 수 있으며, 이를 기반으로 차단 목록에 대한 후보를 작성하는 기능으로 확장할 수 있다. 로그를 기록하기 위한 정보로는 로그인 날짜 및 시간, 로그인 유형, 접속국가, 이체금액 등이 있으며, 사용자가 접속하지 않은 날짜에 로그인이 되었거나, 이체금액이 실제와 다를 경우, 사용자의 계정정보와 같은 본인확인수단에 문제점이 발생하였을 가능성이 높을 것이라는 판단이 가능하다[1].

4. 네트워크 및 사용자 구간에서의 보안기술

네트워크 및 사용자 구간에서의 보안기술은 SSL 통신과 암호화 응용 프로그램을 포함한 암호 통신기술로 분류된다. 네트워크 구간도 금융기관 구간과 마찬가지로 암호학적으로 매우 강인한 구조를 이루고 있어 공격자에게는 주요한 공격대상에서 제외되지만, 구현과정에서의 취약점으로 인한 피해사례가 존재한다. 따라서 본 논문에서는 이러한 기술에 대한 분석 결과를 서술하며 그 분류를 (표 7)에 나타내었다.

(표 6) 주요국의 BCP 표준 현황
(Table 6) BCP standards of major countries

구분	표준	개발 기관	제정 연도	주요 특징
국제 표준	ISO 22301	국제 표준화기구 (ISO)	2012	해외 여러 국가의 공공기관 및 기업에서 사용하는 표준 미국, 영국, 싱가포르 등 해외 여러 나라의 BCP 표준으로부터 모범 실무만을 엄선하여 개발
미국	BC Practitioners	미국재해복구협회 (DRII)	2007	정부, 민간, 공공기관 전문가로 소위원회를 구성하여 작성 영국 BCI와 공동으로 작성한 10가지 BCP 실무분야에 대한 세부지침 제공
영국	BC 25999	영국 표준협회(BSI), 영국업무연속성 협회(BCI)	2006	2002년 PAS(Publicly Available Specification) 56을 근간으로 작성 BS 25999 part.2는 2012년 11월부터 ISO 22301로 대체
일본	BCM Guidelines	내무성 (Cabinet Office), 경제산업성(METI)	2006	영국 BCM 표준을 기반으로 상세한 가이드라인을 제공 회사규모 등을 고려하여 세분화된 BCM 구현 지침 제시
싱가포르	Technical Reference for BCM	중소기업 육성개발기관 (SPRING Singapore)	2005	미국 DRII와 영국 BCI 감수를 통하여 표준, 지침을 준수 금융, 보건 분야를 중심으로 인증심사에 대한 관심 지속

(표 7) 네트워크 구간에서의 보안기술
(Table 7) Security technologies for the network communication

대분류	소분류	보안기술
SSL 통신	SSL/TLS	• Full handshake 프로토콜 • Abbreviated handshake 프로토콜
암호화 프로그램	웹 구간 통신을 위한 암호화 모듈	• HTTP 프로토콜 활용 • SDK 방식 • 미들웨어 방식 • 터널링 방식
	클라이언트-서버 형태의 암호화 모듈	• 직접 설계한 프로토콜 활용

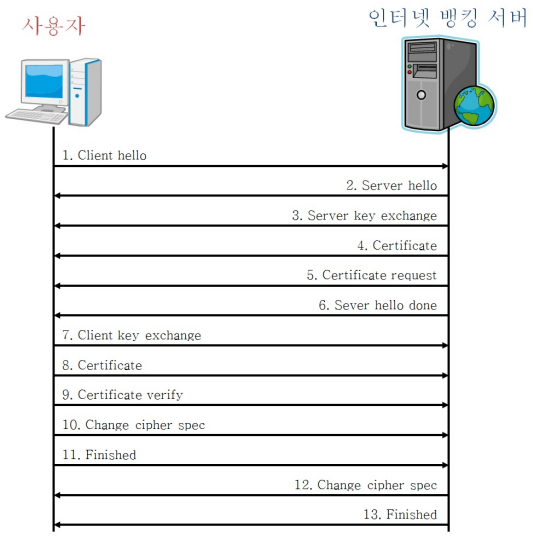
4.1 SSL 통신

SSL은 1994년 Netscape사에서 웹 브라우저를 통하여 안전하게 데이터를 전송하기 위한 목적으로 제안되었으며, 1996년 IETF(Internet Engineering Task Force)에서 SSL v3.0을 제안하였다. 이후 지속적으로 수정 및 보완되었으며, 1999년에는 TLS(Transport Layer Security)로 명칭이 변경되어 RFC 2240(TLS v1.0)으로 표준화되었다. SSL/TLS는 전송계층과 응용계층 사이에 위치하여 응용계층 프로그램의 보안설정을 지원하며, 이를 위하여 내부적으로 레코드 레이어와 handshake, change cipher spec, alert, application data 프로토콜로 이루어진다.

SSL/TLS는 세션상태와 커넥션상태로 이루어지며, 하나의 세션 내에 여러 개의 커넥션이 포함되는 형태이다. 또한, 클라이언트와 서버가 통신을 수행하면서 설정하는 알고리즘과 키를 저장할 때는 예비상태, 레코드 레이어에서 데이터를 처리할 때는 현재상태로 변경하여 통신을 하며, 데이터 송/수신을 위하여 읽기상태와 쓰기상태를 준비하고 있다.

Handshake 프로토콜에서는 알고리즘과 같은 보안 파라미터를 설정하며, 설정된 파라미터는 레코드 레이어로 전달되어 키 블록을 생성한 후, 예비상태로 전환한다. 이후 change cipher spec 프로토콜에 의하여 현재상태로 전환되며, 기존의 예비상태는 초기화되고, 이 과정에서 change cipher spec 메시지가 전송되면 읽기상태와 쓰기상태를 통하여 데이터를 송/수신한다. Full handshake에 의하여 세션이 생성되면, 이후 통신은 abbreviated handshake 프로토콜에 의하여 세션상태는 공유하면서 커넥션상태만 재생성하여 통신이 이루어진다.

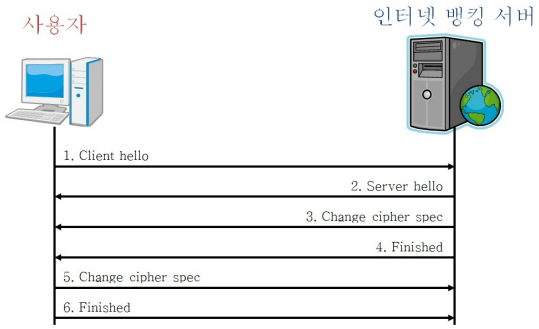
Handshake 프로토콜에서는 클라이언트가 서버에게 보안 파라미터를 요청하면, 서버는 필요한 파라미터를 설정하여 change cipher spec 프로토콜을 활성화하고, application data 프로토콜을 통하여 데이터를 안전하게 전송한다. 그리고 통신 과정에서 발생한 오류들은 alert 프로토콜을 통하여 처리된다. 이 프로토콜에서는 클라이언트와 서버가 상호인증을 수행하고, 암호 알고리즘과 암호키, MAC 알고리즘 등의 파라미터를 설정한다. Handshake 프로토콜은 full handshake 프로토콜과 abbreviated handshake 프로토콜로 구성되며, full handshake에 대한 동작과정을 (그림 3)에 나타내었다[15].



(그림 3) SSL의 full handshake 프로토콜
(Figure 3) Full handshake protocol of SSL

클라이언트는 client hello 메시지를 서버로 전송한 후, 서버의 응답을 기다리며, 서버가 server hello 메시지를 전송함으로써 프로토콜이 시작된다. 클라이언트와 서버는 hello 메시지에 프로토콜 버전과 세션 아이디, cipher suite, 압축방법 등을 포함하여 생성한 난수를 교환한다. 이후, certificate와 key exchange 메시지를 통하여 키 생성에 필요한 pre-master secret과 master secret을 서로 공유하며, 인증을 위하여 인증서를 교환할 수 있다. 이와 같은 과정이 완료되면 설정된 파라미터들을 change cipher spec 메시지를 통하여 공유한 후 finished 메시지를 전송함으로써 세션이 연결된다.

클라이언트가 새로운 세션을 요구할 때는 empty 세션 아이디를 전송하며, 연결된 세션을 통하여 새로운 커넥션을 생성할 경우에는 client hello 메시지에 재사용을 위한



(그림 4) SSL의 abbreviated handshake 프로토콜
(Figure 4) Abbreviated handshake protocol of SSL

세션 아이디를 서버로 전송한다. 서버는 일치하는 세션 아이디를 확인하여 abbreviated handshake 프로토콜을 통하여 change cipher spec을 교환하며, 이에 대한 과정을 (그림 4)에 나타내었다[15].

Change cipher spec 메시지는 handshake 프로토콜 과정에서 설정된 예비상태를 현재상태로 전환하는 메시지이며, alert 프로토콜은 모든 통신과정에서 발생하는 에러메시지를 전달한다. 에러메시지는 warning level과 fatal level로 구분되며, fatal level일 경우에는 세션이 종료된다.

4.2 암호화 프로그램

인터넷 뱅킹 서비스에서 사용자가 입력하는 거래정보를 인터넷 뱅킹 서버로 전송하기 위하여 HTML 문서를 암호화하여 전송한다. 따라서 전송되는 HTML 문서에는 거래와 관련된 정보가 포함되므로 기밀성이 보장되어야 한다. 이를 위하여 HTML 문서를 암호화함으로써 평문으로 전송할 때 발생하는 도청과 같은 공격에 의한 거래정보의 위/변조에 대응한다[16].

암호화 프로그램의 종류는 인터넷 뱅킹 서버의 시스템과 통신 프로토콜의 특성에 따라 인터넷 뱅킹과 같은 웹 구간 통신을 위한 암호화 모듈과 증권 HTS와 같은 클라이언트-서버 형태의 암호화 모듈로 나누어진다. 웹 구간 통신을 위한 암호화 모듈은 HTTP(HyperText Transfer Protocol)를 활용하고, 클라이언트-서버 암호화 모듈은 직접 설계한 프로토콜을 활용하며, 암호화 방식에 따라 키 교환 정보와 암호화된 메시지가 하나의 암호문에 포함된 전자봉투 방식과 키를 교환한 후 암호화를 수행하는 세션키 교환 방식으로 나누어진다[16]. 이러한 암호화 모듈의 공통 기능을 (표 8)에 나타내었다[17].

(표 8) 암호화 프로그램의 공통 기능
(Table 8) Common functions of cryptography programs

항목	지원 내용	설명
키 교환 알고리즘	RSA, DH, ECDH	• RSA: 1024비트 이상 • DH: 512비트 이상 • ECDH: 160비트 이상
암호화 알고리즘 (기밀성)	SEED, AES, ARIA	• 128비트 이상
인증 및 확인 알고리즘 (무결성, 인증)	HMAC, 전자서명	• 전자서명 적용 시 선택적 평문 공격 차단에 대한 대책 필요
키 교환 시 PKI 메커니즘	X.509 인증서 지원 인증서 경로 검증 (RFC 3280)	• 세션키에 대한 중간자 공격 방지
개인키 관리방법	파일시스템, HSM	• Encrypted PKCS #8 • PKCS #11(HSM) • PKCS #12

웹 구간 통신을 위한 암호화 모듈은 보통 HTTP를 활용하며, 보안을 위한 HTTPS(HyperText Transfer Protocol Secure)를 활용할 수 있지만, SEED 128비트를 지원하지 않으므로 SDK(Software Development Kit) 방식과 미들웨어 방식, 터널링 방식을 주로 활용한다. SDK 방식은 어플리케이션 내부에 암/복호 함수를 삽입하는 형태로 가장 많이 사용되고, 미들웨어 방식은 웹 브라우저 프로토콜 계층에서 암/복호 및 공인인증서 등의 기능을 수행하는 방식이며, 터널링 방식은 클라이언트와 서버 사이에 터널링 클라이언트와 터널링 서버를 설치하고 이를 통하여 암/복호를 수행하는 방식이다[17].

4.3. 사용자 구간에서의 보안기술

사용자 구간에서의 보안기술은 키보드 보안 프로그램, PKI 응용 프로그램, 종단 간 암호화, 해킹 방지 프로그램, 개인 방화벽, 이동식 매체 보안, 역공학 방지기술로 분류된다. 금융기관과 네트워크 구간에서는 공개되지 않은 환경과 암호학적으로 안전하게 구성되어 공격자가 공격을 시도하기 위해서는 많은 시간과 노력이 필요하여 의욕을 상실하거나 공격 자체가 불가능하므로 공격대상을 보통 사용자 구간으로 선택하는 경우가 많아 이를 대응하기 위한 많은 기술이 연구되었다. 사용자 구간에서의 보안기술 분류를 (표 9)에 나타내었다.

(표 9) 사용자 구간에서의 보안기술
(Table 9) Security techniques for the user terminal area

대분류	소분류	보안기술
키보드 보안 프로그램	PS/2 키보드	• 메시지 후킹 • 필터 드라이버 삽입 • 인터럽트 객체 대체 • IDT 대체 • 0xD2 명령을 이용한 임의의 스캔코드 발생 • 키보드 내부 메모리를 이용한 임의의 스캔코드 발생 • 디버그 예외처리 이용
	USB 키보드	• 필터 드라이버 삽입 • 인라인 후킹
PKI 응용 프로그램	통신구간 암호기술	• 직접 설계 • 라이브러리 활용
종단 간 암호화	초기 종단 간 암호화	• 키보드 보안 프로그램과 PKI 응용 프로그램 연동(암/복호 모듈 존재)
	확장 종단 간 암호화	• 이중 암호화(암호 모듈만 존재)
해킹 방지 프로그램	패턴기반	• 안티 바이러스 제품
개인 방화벽	행위기반	• 프로그램 접근관리 • IP 주소 접근관리 • 네트워크 연결관리
이동식 매체 보안	보안 USB	• 소프트웨어 방식 • 하드웨어 기반 파티션 분할 방식 • 하드웨어 방식
역공학 방지기술	배치 난독화	• 형식 변환, 주석 제거, 식별자 변환
	자료 난독화	• 저장장소 변환, 인코딩 변환, 집합 변환, 순서 변환
	제어 난독화	• 계산 변환, 집합 변환, 순서 변환
	방지 난독화	• 고유의 변환방법, 대상이 있는 변환방법

4.4. 보안기술의 발전방향

2005년 5월, 인터넷 뱅킹 서비스에서의 해킹사건이 발생됨으로 인하여 기밀성, 무결성, 가용성, 부인방지와 같이 외부로부터의 침입에 대응하기 위하여 본 논문에서 분석한 다양한 보안기술을 적용하였다. 이러한 보안기술은 암호화 기반의 기술을 토대로 검증된 수학적 도구를 활용함으로써 사용자 인증 및 전달되는 데이터의 안전성을 제공하며, 그 효용성이 충분히 입증되었다. 하지만 암호화 기반의 기술이 아닌 이를 활용하는 과정 및 환경에서 발생하는 문제점이 드러나고 있어, 이를 대응하기 위한 추가적인 기술이 도입되는 추세이다. 대표적으로 투채널 인증과 캡챠가 있다. 투채널 인증은 현재 사용하는 채널이 아닌 별도의 채널을 통하여 사용자를 인증하며, 공격자는 두 개의 채널 모두를 공격하여야 하므로 보다 안전한 환경을 제공한다[20]. 캡챠는 문자열을 왜곡하고 노이즈 삽입, 배경 그라데이션 등을 적용함으로써 자동화된 프로그램이 문자열을 인식하지 못하도록 방지하여 트랜잭션을 변조하는 공격에 대응함으로써 보다 안전한 승인 과정을 제공한다[21].

상기와 같이 인터넷 뱅킹 서비스의 금융기관 구간, 네트워크 구간, 사용자 구간에서 다양한 보안기술이 적용되었음에도 불구하고, 일부 심각한 공격기술에 의한 피해가 발생하며, 이를 대응하기 위한 기술이 필요하다. 대표적으로 내부자에 의하여 발생하는 위협이 있다. 국외에서는 내부자 공격에 대응하기 위한 정책 및 기술들에 대한 연구가 지속적으로 진행되고 있으나, 국내에서는 외부로부터의 공격에 주로 초점을 맞추고 있어 내부자의 공모에 의하여 공격이 발생하는 경우에 대한 대응이 미흡하다. 따라서 내부자의 권한 및 접근 등의 정책적인 부분부터 실제 데이터에 접근하거나 유출하는 등의 행위를 방지하고 데이터를 보호하기 위한 보안기술 등이 충분히 고려되어 적용하여야 할 것으로 사료된다. 또한 많은 다양한 기술이 지나치게 복합적으로 구성됨으로써 이로 인하여 발생하는 문제점 및 취약점, 그리고 성능 저하 등으로 이어지며, 사용자가 사용하기 어렵거나 불편하도록 구성됨으로써 비효율적인 측면이 존재한다. 따라서 현재의 다양한 기술적인 요소들을 제공하면서도 보다 단순화된 구조를 가지는 통합 프레임워크 및 응용 등을 지원하기 위한 설계가 필요할 것으로 사료된다.

5. 결 론

본 논문에서는 인터넷 뱅킹 서비스에서 발생하는 보안 위협에 대응하기 위하여 인터넷 뱅킹 전 구간에 적용된 보안기술 중 금융기관 구간과 네트워크 구간에 적용된 보안기술을 조사하고 분류한 결과를 서술하였다. 금융기관 구간과 네트워크 구간은 보안이 매우 강화된 구조를 이루고 있어 공격자에게는 주요한 공격대상은 아니지만, 내부자에 의하여 발생하는 피해사례와 구현과정에서의 취약점으로 인하여 발생하는 피해사례가 존재하므로 이러한 위협에 대응하기 위한 참고 자료로써 활용 가치가 있을 것으로 기대된다.

향후 연구로는 본 논문에서 분류한 보안기술이 적용되어 있음에도 불구하고 발생이 가능한 추가적인 보안위협, 그리고 내부자에 의하여 발생하는 위협에 대응하기 위한 연구가 필요할 것으로 사료된다.

참고문헌(Reference)

[1] Jaemo Seung, “Effective Electronic Financial Security Response System by Analyzing Domestic and International Electronic Financial Security Policies”, Interdisciplinary Program of Information Security Graduate School of Chonnam National University, PH.D. thesis, Feb. 2011. http://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=4cf156faf6a619d7ffe0bdc3ef48d419#redirect

[2] Financial Security Agency(FSA), “Technical report of information leakage threats and countermeasures”, research report, 2010(13), Dec. 2010.

[3] National law information center, “Guidelines for the protection of integrated information and communication facilities”, Retrieved Feb., 15, 2017, from http://www.law.go.kr/LSW/admRulInfoP.do?admRulSeq=2000000070960

[4] Financial Security Agency(FSA), “DoS/DDoS attack countermeasure guidelines”, research report, 2007(01), Oct. 2007.

[5] Hyung-Ik Lee, “A Study on Real-time IP Blocking System about prevent of Internet Banking Fraud”, Master’s Thesis, Graduate School of Engineering & Technology, Korea University, Aug. 2010. http://www.riss.kr/link?id=T12167198

[6] K. Lee, J. Byun, M. Park, and K. Yim, “A Search-Mask Technique on Privacy-Severe Web Contents”, Proceedings of the 2nd International Conference on Internet(ICONI), pp.809-810, Dec. 2010.

[7] Jae-Chul Park, “Detection and classification of web-based attack for security of internet banking”, Review of the Korea Institute of Information Security and Cryptology(KIISC), 18(5), pp.62-72, Oct. 2008. http://www.dbpia.co.kr/Journal/ArticleDetail/NODE01075878

[8] D. E. Denning, “An Intrusion-Detection Model”, Journal of the IEEE Transactions on Software Engineering, SE-13(2), pp.222-232, Feb. 1987. https://doi.org/10.1109/TSE.1987.232894

[9] C. Kruegel and G. Vigna, “Anomaly detection of web-based attacks”, Proceedings of the 10th ACM Conference on Computer and Communications Security(ACM CCS), pp.251-261, Oct. 2003. https://doi.org/10.1145/948109.948144

[10] M. Roesch, “Snort: Lightweight Intrusion Detection for Networks”, Proceedings of the 13th USENIX Conference on System Administration, pp.229-238, Nov. 1999. http://static.usenix.org/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf

[11] Financial Security Agency(FSA), “DB encryption trend and security technology”, research report, 2012(3), Sep. 2012.

[12] Financial Security Agency(FSA), “E-finance new authentication technology”, research report, Mar. 2011.

[13] Financial Security Agency(FSA), “Comparison and analysis of BCP(Business Continuity Planning) of financial sector in major countries”, research report, 2013(2), Jul. 2013.

[14] Kyungroul Lee, Kangbin Yim, et al., “Implementation of large-capacity secure storage system for backing up confidential information based on USB 3.0”, Small and Medium Business Administration, research report, May. 2012.

[15] Jinwoo Lee, Junghyun Nam, Seungjoo Kim, and Dongho Won, “Present and Future of SSL/TLS, and

WTLS", Review of Korea Institute of Information Security and Cryptology(KIISC), 14(4), pp.27-36, Aug. 2004.
http://www.dbpia.co.kr/Journal/ArticleDetail/NODE00897965

[16] Telecommunications Technology Association(TTA), "Security Threats Analysis and Management Methods in Electronic Financial Services", Technical report TTAR-12.0008, Dec. 2011.
http://www.tta.or.kr/data/ttas_view.jsp?rn=1&pk_num=TTAR-12.0008

[17] Financial Security Agency(FSA), "Application guide for end-to-end encryption", Security guide, 2007(2), Oct. 2007.

[18] Jeong-Hoon Jeo, "A study on the classification systems of domestic security fields", Journal of the Korea Society of Computer and Information, 20(3), pp.81-88, Mar. 2015. https://doi.org/10.9708/jksci.2015.20.3.081

[19] Jeong-hoon Jeon, Chnag Hoon Ahn, and Sang-Choon Kim, "Study on the physical vulnerability factors in the convergence IT environment", Journal of the Korea Convergence Security Association, 16(1), pp.59-68, Feb. 2016.
https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002087087

[20] Han-na You, Jae-Sik Lee, Jung-Jae Kim, Jae-Pio Park, Moon-Seog Jun, "A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment", Journal of the Korean Institute of Communications and Information Sciences (KICS), 36(8), pp.939-946, Aug. 2011.
https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001585271

[21] Sang-ho Lee, Sung-ho Kim, Jeon-il Kang, Je-sung Byun, Dea-hun Nyang, Kyung-hee Lee, "A Method of Enhancing Security of Internet Banking Service using Contents-Based CAPTCHA", Journal of the Korea Institute of Information Security & Cryptology (KIISC), 23(4), pp.571-583, Aug. 2013.
https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001795943

◐ 저 자 소 개 ◑

이 경 룰 (Kyungroul Lee)

2008년 8월 순천향대학교 정보보호학과(공학사)
2010년 8월 순천향대학교 정보보호학과(공학석사)
2015년 2월 순천향대학교 정보보호학과(공학박사)
2011년 5월~2011년 12월 (미)퍼듀대학교 방문연구원
2015년 6월~2016년 2월 순천향대학교 박사후연구원
2016년 3월~현재 순천향대학교 연구조교수
관심분야 : 취약점 분석, 시스템 보안, 하드웨어 보안, 인터넷 뱅킹, 사용자 인증, 디바이스 인증
E-mail : carpedm@sch.ac.kr

임 강 빈 (Kangbin Yim)

1992년 2월 아주대학교 전자공학과(공학사)
1994년 2월 아주대학교 전자공학과(공학석사)
2001년 2월 아주대학교 전자공학과(공학박사)
1999년 3월~2000년 2월 (미)아리조나주립대학교 연구원
2003년 3월~현재 순천향대학교 정보보호학과 교수
2005년 3월~현재 한국정보보호학회 이사
2009년 3월~현재 한국인터넷정보학회 이사
2010년 12월~2012년 2월 (미)퍼듀대학교 객원교수
관심분야 : 취약점 분석, 내부자 공격, 보안 하드웨어 구조, 인증 프로토콜, 홈랜드 시큐리티
E-mail : yim@sch.ac.kr

서 정 택(Jungtaek Seo)

1999년 2월 한국교통대학교 컴퓨터공학과(공학사)
2001년 2월 아주대학교 컴퓨터공학과(공학석사)
2006년 2월 고려대학교 정보보호대학원 정보보호공학과(공학박사)
2000년 11월~2016년 2월 국가보안기술연구소 책임연구원/부장
2014년 6월~2015년 6월 University of Florida 초빙연구원
2012년 3월~2014년 6월 고려대학교 정보보호대학원 겸임교수
2010년 1월~현재 한국정보보호학회 이사
2012년 2월~현재 한국스마트그리드협회 보안위원회 위원장
2017년 1월~현재 한국정보보호학회 CPS보안연구회 회장
2016년 3월~현재 순천향대학교 정보보호학과 교수
관심분야 : 네트워크 보안, 시스템 보안, SCADA 보안, CPS 보안
E-mail : seojt@sch.ac.kr