情 報 保 護 學 會 誌
第21卷 第7號, 2011. 11

국내 전자금융 현황 및 보안위협 분류

이 수 미*, 성 재 모**

요 약

최근 들어 초고속 인터넷서비스의 보편화, 무선통신망의 고속화 및 스마트폰 등 새로운 정보통신매체 등이 보급 활성화 됨에 따라 인터넷 뱅킹, 사이버 트레이딩 등 전자금융서비스가 보편화되고 이용률이 해마다 급증하고 있다. 이처럼 전자금융의 대중화 및 활성화로 인해 전자금융사고에 의한 이용자의 금전적인 손실은 해당 금융기관의 신뢰도 하락과 경영상 피해 등 과거보다 더 심각한 영향을 줄 수 있다. 따라서 본 논문에서는 다변화하는 전자금융 환경에 대해 살펴보고 인터넷, 모바일 및 자동화기기 등 전자금융에서 발생한 또는 발생 가능한 보안위협을 분류함으로써 향후 이를 기반으로 전자금융 서비스 안전성 강화를 위한 대응 방안 연구에 기반이 되고자 한다.

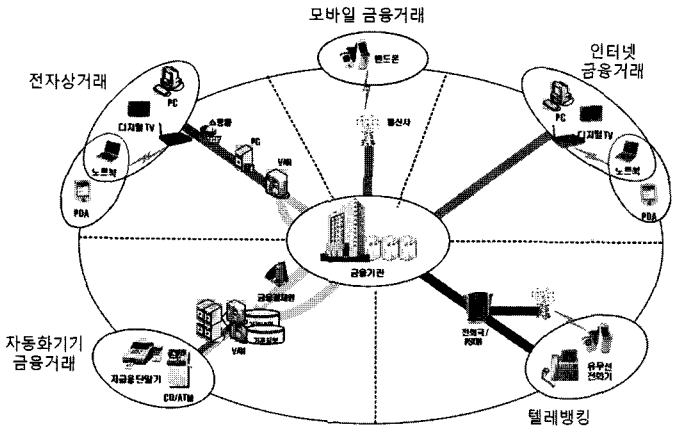
Ⅰ. 서 론

금융 환경의 변화에 따라 금융기관은 고객의 다양한 정보를 다루고 있고 고객 정보유출에 대한 사고에 대처하기 위해 IT조직의 전문화, 관리체계 구축을 추진하면서 IT를 주요한 요소로 확대하고 있다. 특히 대면방식의 전자상거래에 비해 인터넷을 이용한 비대면 방식의 전자상거래가 활발해지면서 보안에 관심이 증대되고 있다.

전자금융 서비스에서는 비대면 거래의 경우 양방향을 확인할 수 없고 거래 내역에 대한 외부 유출이나 변경의 가능성이 높아져 거래 사실에 대한 증빙이 어렵기 때문에 기밀성, 무결성, 가용성에 인증/부인방지까지 보안 요소로 고려되어야 할 것이다 [10]. 전자금융 서비스에서 보안 요소를 위협하는 공격의 유형은 크게 수동적인 공격과 능동적인 공격으로 구분할 수 있다. 수동적인 공격은 전송되는 메시지를 도중에 가로채거나 도청하여 그 내용을 외부로 유출시키는 유형과 메시지의 특성을 분석하여 특정 정보를 알아내기 위한 트래픽 분석 유형에 해당된다. 능동적인 공격은 의도적으로 메시지를 조작하는 공격 유형이며 메시지 변조, 삽입, 재생 등의 공격이 해당된다. 전자금융 거래에서의 기밀성은 공격으로부터 거래 정보를 보호하는 것으로 금융기관과 이용자만이 거래정보의 내용을 파악할 수 있는 것을 의미한다. 현재 전자금융 거래에서는 기밀성을 유지하기 위해 다양한 암호화 기술이 적용되어 있다. 무결성은 송수신되는 데이터가 불법적으로 재생 및 변조되었는지에 대한 확인을 보장해야한다. 이를 위해 해쉬 알고리즘을 적용하고 있다. 가용성은 인가된 전자금융 거래 이용자가 정보 시스템의 데이터를 필요로 할 때 부당한 지체 없이 원하는 자원에 접근하고 사용할 수 있는 것을 보장하는 것이다. 즉, 인터넷으로 연결된 정보 시스템의 성능을 안정적으로 유지하며 이용 효율을 극대화하는 방법으로 정보 시스템에 정당한 이용자가 원하는 시점에 적절한 정보를 이용할 수 있도록 해야 한다. 따라서 전자금융 거래 서비스의 응답시간이 가용성과 관련이 있다. 마지막으로 거래 내역에 대한 외부 유출이나 변경의 가능성이 높아지면서 거래 사실에 대한 증빙을 보장하기 위해 부인방지와 이용자와 서버 간의 양방향 신뢰를 비대면 거래에서도 보장하기 위해 인증을 만족해야 한다.

이용자PC, 모바일 장치, CD/ATM 등 이용자가 이용하는 전자적 장치에서 키보드 보안을 위해 다양한 보안 제품이 적용되어 있다 [4]. 예를 들어 인터넷 전자금융 거래를 위해 이용자 PC에서는 키보드 보안을 위해 키보드해킹 방지 프로그램이 설치되며 키보드해킹 방지

* 금융보안연구원 u-금융연구팀(smlee@fsa.or.kr)
** 금융보안연구원 정보보안본부(sitcom@fsa.or.kr)



〔그림 1〕 국내 전자금융 서비스 유형

프로그램은 이용자가 입력하는 키입력을 가로채어 정보를 알아내는 공격을 방어할 수 있다. 따라서 보안 요소 중 기밀성을 보장하기 위한 적용기술에 해당된다. 이외에도 무결성 및 인증/부인방지를 위해 이용자 인증, 전자서명 등이 있다. 전자적 장치에서 보안패치, 백신, 개인방화벽 등의 기술은 외부로부터의 침해를 대응하며 가용성을 보장하기 위해 적용된 기술이다. 네트워크에서는 기밀성을 보장하기 위해 가상사설망(VPN)이 있으며 네트워크로 전송되는 데이터를 암호화하여 기밀성을 보장하게 된다. 또한, 유해트래픽 통제 등이 적용되어 있으며 무결성을 위해 침입차단, 가용성을 위해 DDoS 공격 대응 기술 등이 적용되어 있다. 금융기관은 이용자의 금융정보 등 주요 정보에 대해 접근통제를 강화하며 내부정보 유출을 막기 위해 가장 중요한 암호화 키를 하드웨어 전용 보안 장비에서 별도로 보호하고 있다. 그 외에도 전자문서에 저작권 보호기술(DRM)이 경우에 따라 적용되어 있으며 무결성을 보장하기 위해 서버 접근 로그 모니터링, 가용성을 위한 로드 밸런싱(Load Balancing), 백업 등이 적용되어 있다. 하지만 국내 전자금융서비스는 다양한 환경에서 진행되고 있고 이에 수반되는 보안위협들도 증가하고 있는 추세이다. 따라서 본 논문에서는 다변화하는 전자금융 환경에 대해 살펴보고 이와 같은 전자금융 환경에서 발생한 또는 발생 가능한 보안위협에 대해 분류한다. 기존 논문 [8]에서 보안위협을 분류하였으나 최근에 이슈가 되고 있는 금융기관 내부 시스템에서의 보안위협을 세분화하고 PG사, VAN사와 같은 제휴 사업자에서 발생한 위협 등을 반영하여 보안위협을 재분류하여 기술하였다.

Ⅱ. 국내 전자금융 환경

국내 전자금융 거래 유형과 전자금융 서비스에 접근할 수 있는 전자적 장치와 국내에서 제공 중인 다양한 전자금융 환경을 소개한다. 전자금융 서비스는 이용자에 의해 조작되는 PC, TV, 전화기, 자동화기기 등 전자적 장치를 통해 금융기관이 제공하는 서비스를 의미하며, 전자금융 서비스 유형으로는 계좌 조회, 자금 이체, 주식 매매, 현금 출금, 현금 서비스 등 다양하다. 전화기는 일반 전화기, 모바일폰, 스마트폰 등을 포함하며, 자동화기기는 현금자동인출기(CD, Cash Dispenser), 현금자동입출금기(ATM, Automatic Teller Machine) 등을 포함한다 [3]. 자동화기기는 금융기관에 의해 직·간접적으로 통제 및 관리되고 있지만, 본 논문에서는 전자금융 서비스의 범주에 포함시켰다.

온라인 형태의 전자금융 거래는 모든 거래 과정이 사람의 대면 없이 전자적인 방식에 의하여 이루어지는 거래를 의미하며, 자동화기기를 이용하여 현금의 입·출금, 자금이체 또한 온라인 거래로 분류된다. 반면에 오프라인 형태의 금융거래는 금융기관 직원이 개입하여 거래를 완성시키는 거래이며, 영업점에서 통장을 이용하여 이루어지는 거래 또는 가맹점에서 신용카드를 이용하여 결제하는 형태를 포함한다. 전자금융 거래는 장표, 통장 등 종이문서가 아닌 전자문서, 휴대폰 등으로 의사표시를 전달 및 확인하는 비서면성과 점포창구의 직원과 거래가 아닌 이용자 PC, 전화기, 자동화기기 등의 전자적 장치를 통해 이루어지므로 금융기관 직원과 의사소통 없어 비대면성이라는 특징을 지니고 있다 [1,2].

전자금융 환경은 그림 1과 같이 전자적 장치에 따라 인터넷 금융거래, 모바일 금융거래, 자동화기기 금융거래 등으로 분류된다. 인터넷 금융거래는 고객이 인터넷을 통해 각종 은행, 증권, 카드 서비스를 원격지에서 처리할 수 있는 금융거래이다. 특히, 인터넷 트레이딩은 전용 프로그램을 이용하여 증권거래를 할 수 있는 홈트레이딩(HTS, Home Trading Service) 방식과 웹 브라우저를 이용하여 거래를 할 수 있는 웹 트레이딩(WTS, Web Trading Service) 방식으로 나뉜다. 모바일 금융거래는 고객이 휴대전화, PDA 등 이동 통신 기기를 이용하여 무선 인터넷을 기반으로 각종 은행, 증권 등의 업무를 처리하며, 자동화기기 금융거래는 현금자동인출기 또는 현금자동입출금기를 통해 은행, 증권, 카드 서비스를 처리한다. 텔레뱅킹 금융거래는 가정, 사무실 등에서 전화기를 통해 자동 응답 서비스 등에 접근하여 자금이체, 조회, 분실 신고 및 FAX 통지 등을 할 수 있다. PC, 전화기 등의 전자적 장치를 통해 이용 가능한 전자금융 서비스는 은행, 증권, 카드, 보험에서 거래 수단별로 모두 이용하고 있으나 보험사에서는 자동화기기를 사용하지 않고 있다. 이에 반해 증권 권역에서는 2009년 2월, 자본시장과 금융 투자업에 관한 법률의 시행으로 금융투자업자의 업무 범위에 자금이체 업무 등이 추가되어 자동화기기를 통해 투자 예탁금으로 송금, 공과금 납부를 할 수 있게 되었다.

본 논문에서는 중점적으로 다루지 않지만 최근 출시되어 제한적으로 운영되고 있는 클라우드 컴퓨팅, IPTV, VoIP 등 신기술 기반의 전자금융 환경에 대해서 살펴본다.

2.1 클라우드 컴퓨팅 기반 전자금융 환경

클라우드 컴퓨팅(Cloud Computing)은 인터넷 기술을 활용하여 다수의 고객에게 확장성을 가진 IT자원을 서비스로 제공하는 것으로서, 이용자들은 어플리케이션, 스토리지, OS 등 필요한 IT자원을 원하는 시점에 어디서나 사용할 수 있다. 클라우드 컴퓨팅의 중요기술인 "가상화(Virtualization)"와 "분산처리(Distributed Processing)" 기술을 이용하여 여러 곳에 분산되어 있는 데이터 센터를 통합하여 이용자에게 다양한 서비스를 제공한다. 가상화는 OS, 서버, 네트워크 등에 대하여 가상의 자원을 생성하는 것으로 제공하는 형태에 따라 서버 가상화, 데스크탑 가상화, 어플리케이션 가상화로 구분된다.

〔표 2〕 서버 가상화 기술 적용 현황

금융기관	일자	내용	비고
기업은행	2009 ~ 2013	서버통합 5개년 계획을 통해 가상화 프로젝트를 진행하고 있으며, 오는 2013년 까지 404대 서버를 69대로 줄이는 사업을 추진	서버 가상화
우리은행	2009 ~ 2012	2009~2012년 전 서버를 대상으로 가상화를 통한 대규모 서버통합 프로젝트(x86 서버 100대를 블레이드 서버 20여대로 통합, 향후 80대 유닉스·x86 서버를 6대로 통합)	서버 가상화
대구은행	2009	10대를 유닉스서버 2대로통합	서버 가상화
부산은행	2009	x86 서버 46대를 3대로 통합 1차 프로젝트 진행, 47대의 서버를 3대로 통합하는 2차 프로젝트를 완료	서버 가상화
산업은행	2010	100여대의 x86서버통합 작업을 실시할 예정	서버 가상화 (VM)

서버 가상화는 금융기관 서버에 적용할 경우, 이용자 측면에서는 기존과 동일하게 서비스가 제공되므로 추가적으로 고려할 사항이 없는 기술이다. 데스크탑 가상화는 데이터의 중앙 집중화, 서버운영 비용 절감, 보안 규제 준수에 대한 통합 지원을 위해 활용되고 있으며, 망분리 등의 장점으로 인해 기업 측면에서 데스크탑 가상화를 도입하고 있는 추세이다. T社의 엘클라우드(elcloud)서비스는 PC용 프로그램을 데스크탑(Windows, Mac 등), 스마트폰(아이폰, 윈모바일폰 등) 등에서 사용할 수 있는 서비스이며, 웹브라우저를 이용하여 인터넷뱅킹, 사이버트레이딩 등을 이용할 수 있다. 어플리케이션 가상화는 증권 권역에서 가상화 기술을 적용한 스마트폰(아이폰, 안드로이드폰)용 모바일 트레이딩을 이용할 수 있도록 하며, 주식·펀드·주가연계증권(ELS) 청약, 선물옵션거래, 해외 주식 거래 등에 대한 기능을 제공하고 있다.

2.2 IPTV 기반 전자금융 환경

서비스 품질(QoS, Quality of Service)이 제공되는 광대역 IP 네트워크와 IP-셋탑박스, 표준 TV 수상기를 통해 양방향 TV 서비스를 포함하는 디지털 방송·통신

〔표 3〕 IPTV기반 전자금융서비스 내용

기관	서비스 내용		
	서비스명	서비스 종류	인증방법
우리 은행	IPTV뱅킹	조회, 이체, 신용카드, 금융상품몰, 입금계좌관리	USB메모리
국민 은행	홈-ATM (가칭)	조회, 이체, 신용카드, 대출, 지로 등	필요없음 (ATM 방식) IC카드 이용
신한 은행	T-ATM (가칭)	조회, 이체, 신용카드, 대출, 지로 등	필요없음 (ATM 방식) IC카드 이용
기업 은행	IPTV뱅킹	조회, 신용카드조회 등	USB메모리
농협 중앙회	IPTV뱅킹 (포켓뱅킹)	조회, 이체, 신용카드, 대출, 지로 등	필요없음 (H/W 토큰방식)
우정사업 본부	IPTV뱅킹	계좌이체, 공과금납부	USB메모리
동양증권	동양 MyTV	주식매매, 계좌이체, 시세조회 등	USB메모리

의 융합 서비스가 활용되고 있으며, 최근에는 금융기관과 통신사업자가 IPTV 환경에서 홈-ATM, IPTV 뱅킹, 포켓 뱅킹 등의 다양한 전자금융서비스를 제공하고 있다. 표 3.3은 IPTV 뱅킹서비스의 참가자 역할을 설명한다. 기업은행과 우리은행에서 IPTV뱅킹 서비스를 제공하고 하고 있으며, 케이블TV 환경에서의 TV뱅킹서비스는 표 3.4와 같이 대부분 서비스가 중지된 상태이다. 2010년 6월부터 기업은행, 농협중앙회 등 8개 은행을 중심으로 '홈-ATM서비스'가 오픈 중이다.

2.3 VoIP 기반 전자금융 환경

최근 세션 초기화 프로토콜(Session Initiation Protocol) 기반의 VoIP(Voice over IP) 서비스가 활성화됨에 따라 금융기관에서는 일반 전화(PSTN) 기반 텔레뱅킹서비스와 인터넷 전화(VoIP) 텔레뱅킹 서비스를 동시에 제공하고 있다. 일반적으로 텔레뱅킹 서비스는 금융기관, 서비스 사업자, 이용자로 구성된다. 금융기관은 서비스사업자를 통해 이용자에게 텔레뱅킹 서비스를 제공하며, 서비스 사업자는 전기통신 회선 설비를 보유하고 이를 기반으로 일반 전화 서비스 및 VoIP 서비스 제공한다. 이용자는 개인, 중소기업, 대기업 및 이용자로 구분된다. 현재 텔레뱅킹 서비스는 이용자에 대한 본인 확인 절차와 서비스 종류(신규가입, 조회, 이체 등)에 따라 지정 전화 설정, 지정 계좌 설정, 거래내역 SMS 송부 등을 이용할 수 있다.

현재 대부분의 금융기관들이 인터넷 전화 기반 텔레뱅킹서비스를 제공하고 있다. 이처럼 PSTN 망과 VoIP 망이 혼재되어 있는 텔레뱅킹서비스 환경에서는 이용자가 속한 인터넷 전화 서비스 사업자와 금융기관과 연결된 서비스사업자(VoIP 및 PSTN 서비스사업자 모두 포함)가 서로 다를 수 있다. 그렇지만 기존 텔레뱅킹서비스 이용자는 VoIP를 이용한 서비스 가입 및 해지를 위한 별도의 추가 절차는 필요 없다.

Ⅲ. 국내 전자금융 보안위협 분석

다음 그림 2와 같이 전자금융 보안위협을 분류하고 전자적 장치, 네트워크, 금융기관, 이용자 구간 즉 전자금융 거래 구간별로 발생한 또는 발생 가능한 보안위협에 대해 살펴본다.

3.1 이용자

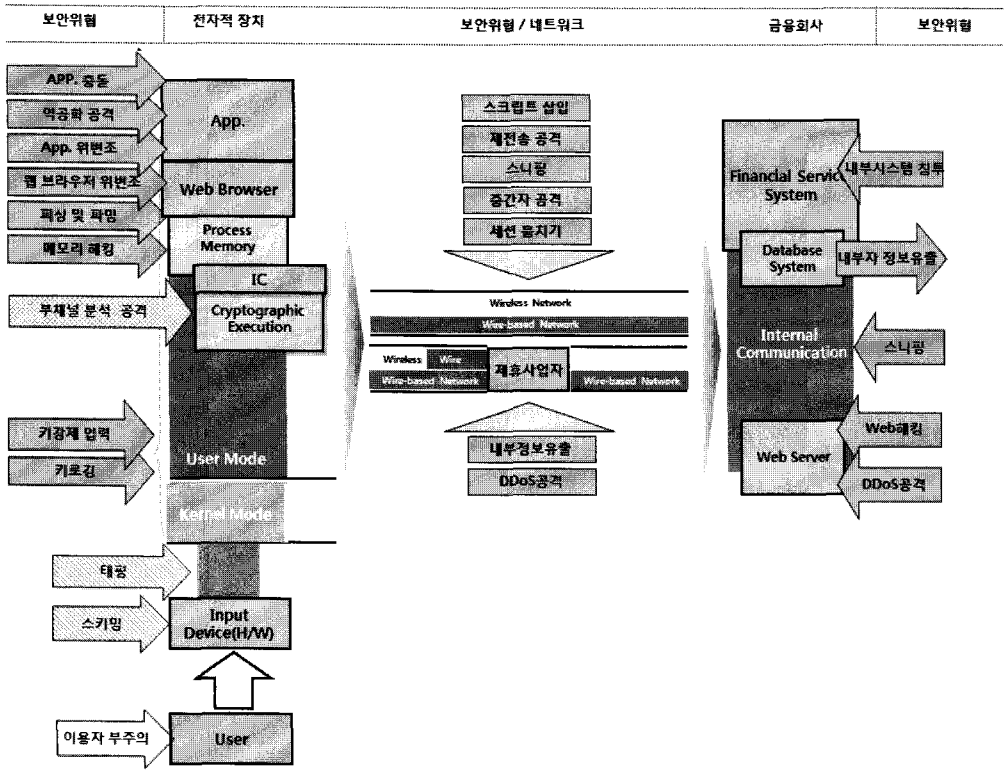
[분류1] 이용자 부주의 : 최근 방화벽과 같은 기술을 공격의 목표로 삼기보다 별 다른 비용, 리스크 없이 인간의 성향을 이용하여 공격이 행해지는 경향이 있다. 이를 잘 보여주는 예는 사회 공학적 위협이며 전자금융거래 이용자에게 온라인, 개인적, 폐기물 등의 접근방식으로 거래 정보를 빼내거나 활용하게 된다 [6].

3.2 전자적 장치

다음은 전자적 장치에서 발생할 수 있는 보안위협에 대해 조사 및 분류하고 각각의 보안위협에 대해 살펴본다.

3.2.1 애플리케이션 (App.)

[분류1] App.충돌 : 스마트디바이스, 이용자 PC, POS단말기 등에서 다수의 보안모듈이 설치되면서 모듈 간이 충돌이 발생할 수 있다. 예를 들어 복합형(PC형) POS단말기에서 인터넷 뱅킹과 POS지불결제가 이루어지는 경우 두 보안모듈이 각각 설치되어 실행될 때 모듈 간에 충돌이 발생할 수 있다. 충돌이 발생하는 경



〔그림 2〕 전자금융 보안위협 분류

우 보안기능이 작동하지 않아 계좌비밀번호 등이 유출될 수 있다.

[분류2] App.위·변조 : 스마트폰 뱅킹이 이슈화가 되면서 애플리케이션 위·변조 형태의 공격이 성행하고 있다. 2010년 2월에는 삼성, LG의 윈도 모바일이 탑재된 스마트폰 4종을 대상으로 위협이 발생됐고 이는 SMS 결제, SMS 훔쳐보기, 주소록 절취, 휴대폰 단말기 시스템 다운, SMS 공격에 대한 공격 시나리오를 통해 공격이 가능했다. 이는 스마트폰에 설치된 SMS 애플리케이션을 변조하여 결제 인증코드를 자신에게 보내도록 유도하는 방식이다.

[분류3] 역공학 공격 : 역공학이란 이미 만들어진 소프트웨어로부터 설계 사상이나 지식을 추출하는 과정이다. 공격자의 입장에서 역공학은 소프트웨어의 취약점을 분석할 수 있게 해준다. 특히 전자금융거래에 활용되는 소프트웨어의 경우 역공학을 통하여 암호키를 추출하거나 암호키를 유추할 수 있는 정보를 획득하는 등 소프트웨어 상의 취약점을 발견하여 이를 이용한 공격이 가능하다. 최근 아이폰 애플리케이션의 동작 루틴을 분석한 후 Jailbreak 탐지 기능을 우회하는 기술이 배포되어 역공학 공격에 대한 위협이 알려지고 있다.

3.2.2 웹 브라우저 (Web Browser)

[분류4] 웹 브라우저 위·변조 : 웹브라우저에 있는 입력 폼을 변조하여 공격을 수행하는 행위로서 웹 브라우저 중간자 공격이라고도 말한다. 이체페이지의 입력폼에 적용된 이벤트와 자바스크립트 함수들은 변조된 입력폼에서 작동되도록 한다. 이후 최근 입금계좌 목록 등과 관련된 스크립트를 변조하여 공격자가 원하는 입금계좌번호로 송금할 수 있는 공격이다.

[분류5] 피싱 및 파밍 : 피싱 (Phishing)은 금융기관에서 보낸 것처럼 메일을 위장하여 이용자의 금융 정보 및 관련 비밀번호, 인증번호나 신용카드번호, 계좌정보 등을 빼내는 사회 공학적인 사기 수법이다. 국내에는 2005년 이후 처음 발생하였고 그 이후 국내 금융권 사이트를 대상으로 한 10여 개의 피싱 공격이 발생했다. 파밍 (Pharming)은 이용자의 도메인을 탈취하거나 DNS, 프락시 서버의 주소, PC의 호스트 (hosts) 파일을 변조함으로써 이용자로 하여금 진짜 사이트에 접속

한 것으로 오인하도록 하여 이용자의 각종 개인 정보를 가로채는 수법이다. 2007년 호스트 파일을 변조한 파밍 공격은 인터넷 게시판 등을 이용해 호스트 파일을 변조하는 악성코드를 배포함으로써 특정 은행을 접속할 때 피싱 사이트로 자동 연결하게 한 공격이다. 대만에 위치한 서버를 통해 국내 은행을 대상으로 발생한 공격으로 5천 여명의 공인인증서가 누출됐으며 이 중 다수가 계좌비밀번호, 보안카드번호까지 피싱 사이트에 입력했다.

3.2.3 프로세스 메모리 (Process Memory)

[분류6] 메모리 해킹 : 공격자는 주요 금융거래정보인 입금계좌번호, 이체금액 등을 메모리상에서 변조하여 제3의 계좌로 자금을 이체시키거나 계좌비밀번호, OTP 등을 유출시키는 공격 기법이다 [11]. 이와 관련하여 2007년 8월에 악성코드에 감염된 이용자 PC에서 인터넷 뱅킹을 하는 동안 메모리에 보관된 데이터를 변조하는 방식으로 이용자가 원하는 입금계좌번호가 아닌 공격자가 원하는 계좌로 출금된 사실이 보도되었고, 2010년 3월에는 증권사 홈트레이딩 시스템 (HTS) 해킹이란 내용으로 HTS 메모리의 데이터를 위·변조하여 다른 계좌로의 이체, 보안카드 노출 등에 대한 보안위협에 대해 이슈가 제기되었다.

3.2.4 응용 및 커널 영역 (Application/Kernel Area)

[분류7] 키강제 입력 : 최근에 발생된 키 강제 입력은 웹페이지 위·변조 위협을 이용하여 키보드해킹방지프로그램의 보안 기능을 우회할 수 있는 웹 페이지 설정 후 공격이 가능하다. 변조된 입력폼의 입금계좌번호에 공격자는 원하는 키 이벤트를 발생시켜 제3자의 계좌로 자금을 이체시키는 이슈가 제기되었다.

[분류8] 키로깅 : 키로깅은 이용자가 키보드를 통해 입력하는 정보를 중간에서 가로채어 별도 저장한 후 해당 정보를 해커에게 전송하는 공격 기법으로서 이 공격은 최초로 국내에서는 2005년 5월에 발견되었으며 이후 지속적으로 발견되고 있다. 2007년에는 USB 키보드 보안 취약점이 발견되었고 원인으로는 상용 키보드 해킹 방지 프로그램의 경우 PS/2포트만을 통제하여 USB 키보드 보안에 대한 취약점이 발생했다. 그 후 2008년에는 키보드 컨트롤러의 근본적인 하드웨어 취약점을 제시하고 이를 이용한 스니핑 프로그램으로 키보드 해킹 방지 프로그램이 실행 중인 상태에서 이용자의 비밀번호를 검출해낼 수 있음을 보였고 키보드 입력값을 후킹한 후 사전공격 (Dictionary Attack)에 취약하여 이용자의 정보가 유출됨을 결과로 보였다 [5,6,10].

3.2.5 입력장치 (Input device(H/W))

[분류9] 태핑 (Tapping) : 금융자동화기기, POS단말기 등에서 발생 가능한 공격이며, CD/ATM 내에 카드리더기와 컴퓨터 사이의 케이블을 도청하여 현금·신용카드의 정보를 절취하여 복제하는데 사용되는 공격 기법이다. 그 사례로 2003년 5월에 VAN사업자로부터 자동화기기 구입하여 카드리더기와 본체 사이를 연결한 Cable을 절단하고 노트북과 연결하였다. 이러한 방법으로 14개 은행 495개 계좌번호를 절취하였고 동 계좌에서 예금을 인출하기 위해 필요한 비밀번호는 텔레뱅킹을 이용하여 확인하여 계좌번호와 비밀번호가 맞는 3개 은행 5개 계좌에서 56백만원을 인출하였다. 동 사고와 유사한 사고는 2007년 6월 부산 지역에서도 발생하였다 [2].

[분류10] 스키밍 (Skimming) : 금융자동화기기에서 발생하는 공격이며, 현금·신용카드 불법 복제 장비인 스키머(Skimmer)를 통해 현금·신용카드를 복사하고 몰래카메라를 통해 비밀번호를 탈취하고 현금·신용카드를 복제하는데 사용되는 공격 기법이다. 그 사례로 최근 2010년 11월에 미국 시애틀에서 자동화기기에 직불카드정보를 복사하고 복제 카드를 만드는 스키밍 장치가 설치된 사건이 발생했다.

3.3 네트워크

다음은 네트워크 구간에서 발생할 수 있는 보안위협에 대해 조사 및 분류하고 각각의 보안위협에 대해 살펴본다.

3.3.1 네트워크 구간

[분류1] 스크립트 삽입 : 암호화 제품은 웹브라우저에서 지원하는 자바스크립트를 기반으로 주요 금융 정보를 입력하는 필드만이 암호화를 수행하기 때문에 스크립트 코드를 추가할 수 있다. 공격자는 스크립트 코드

삽입으로 인해 이용자가 전송하는 데이터를 자신에게 전송하게 할 수 있다.

[분류2] 스니핑 (Sniffing) : 스니핑은 네트워크에서 송·수신되는 데이터 트래픽을 도청할 수 있는 스니퍼를 랜 포트나 액세스 포인트(AP, Access Point)에 설치하여 데이터를 가로채는 위협이다.

[분류3] 중간자 공격 (Man in the Middle Attack) : 중간자 공격은 통신 대상 사이에서 내용을 도청 및 변조하는 공격을 의미하며 이러한 공격을 수행하는 공격자는 능동형 공격자 (Active Attacker)에 해당된다. 중간자 공격은 통신 대상이 정상적으로 암호화를 통해 정당한 이용자와 통신하고 있다고 생각하지만 실제로는 공격자와 통신하거나 변조된 데이터를 정당한 이용자가 보낸 것으로 위조하는 것이다.

[분류4] 세션 훔치기 공격 (Session Hijacking) : 세션 훔치기 공격은 이용자와 서버 간에 연결된 세션에서 서버는 자신에게 접속되어 있는 이용자를 구분하기 위해 일반적으로 세션 아이디를 발급한다. 이때 공격자는 세션 아이디만 알면 해당 이용자의 로그인 세션을 사용할 수 있어 이용자 인증 정보(예 : 아이디, 비밀번호 등)를 모르고도 서버에 접속해 여러 정보를 조회하거나 거래를 수행할 수 있다. 일반적으로 세션 ID 추측 및 세션 ID 쿠키 도용을 통해 공격하는 기법이다.

[분류5] 재전송 공격 (Replay Attack) : 중간자 공격은 통신 대상 사이에서 내용을 도청 및 변조하는 공격을 의미하며 이러한 공격을 수행하는 공격자는 능동형 공격자 (Active Attacker)에 해당된다. 중간자 공격은 통신 대상이 정상적으로 암호화를 통해 정당한 이용자와 통신하고 있다고 생각하지만 실제로는 공격자와 통신하거나 변조된 데이터를 정당한 이용자가 보낸 것으로 위조하는 것이다.

3.3.2 제휴 사업자 구간

[분류1] 내부정보유출 : VAN사, PG사 등과 같이 신용카드 정보를 처리하는 기업체의 전산망을 해킹하여 대량의 카드정보를 유출되는 사고가 발생하고 있다. 2004년 국내 VAN사가 해킹을 당해 10억원 이상의 피해가 발생한 사례가 있다. 이처럼 보안인식이 부족하거나 규모가 영세하여 시스템에 대한 보안이 미약한 곳이 공격의 대상이 되고 있다.

[분류2] 분산 서비스 거부 공격 : VAN사, PG사 등에서 구성한 시스템을 대상으로 분산 서비스 거부 공격이 수행될 수 있다. 이를 통해 공격자는 서비스 장애를 발생시키고 위협하여 금전적 이익을 얻으려는 노력을 시도할 것이다. 최근 인터넷쇼핑, 경매, 매매게시판 등에 분산 서비스 거부 공격이 집중되고 있고 위협은 점점 확대되고 있다.

3.4 금융기관

다음은 금융기관 구간에서 발생할 수 있는 보안위협에 대해 조사 및 분류하고 각각의 보안위협에 대해 살펴본다.

3.4.1 웹 서버

[분류1] 웹 해킹 : 웹 해킹은 웹페이지의 취약성을 이용형태로 내부 시스템에 정상적으로 접속하여 정보유출을 목적으로 행해지는 공격이다. 2011년 웹 해킹의 사례로 다양한 금융서비스를 제공하는 사이트를 상대로 웹페이지의 취약성을 찾아 이용자 이름, 주민번호, 이메일 등 정보가 유출된 사례가 있었다. 웹 해킹은 국외에서도 미국 나스닥 서버가 공격받는 등 개인 정보 유출 이상의 피해가 속출하고 있다.

[분류2] 분산서비스 거부 공격 (Distributed Denial of Service, DDoS) : 기존 DDoS 공격 방식은 공격자 개인이 트로이 목마와 같은 악성코드를 유포시킨 후 좀비 PC를 생성시키거나 소수의 공격 툴을 사용하는 방법이 주를 이루었으나 2000년 이후 봇넷 컨트롤러에게 일정의 돈을 지불하고 일부 또는 모든 봇넷을 빌려 원하는 사이트를 공격하는 상업적인 서비스가 등장하였다. 최근 2008년 3월에 특정 증권사를 대상으로 발생한 DDoS 공격이 발생했으며 2009년 7월에 발생한 DDoS 공격은 한국과 미국의 주요 정부기관, 포털 사이트, 은행 사이트 등을 대상으로 수행되었다. 공격 방식은 공격 명령을 하달하는 명령 제어 서버 없이 미리 지정해둔 일정에 따라 공격하였다 [12]. 또한 2010년 3월에 상업적인 서비스를 목적으로 DDoS 공격을 수행하는 새로운 봇넷이 출현하였다.

3.4.2 내부 시스템

[분류1] 내부 시스템 침투공격 : 공격자가 취약한 시

스템을 악성코드로 감염시켜 네트워크 내부로 침투하는 공격을 의미한다. 그 공격 사례로 APT (Advanced Persistent Threat)에 의한 공격이 있으며 내부 시스템에 침투하기 위해 사전에 치밀하게 시스템 환경 등을 분석하여 악성코드를 제작하고 오랜 기간 동안 필요한 정보를 습득하여 기밀정보 유출을 달성하는 형태이다. 최근 금융권을 중심으로 이러한 공격이 계속 증가하는 추세이다.

[분류2] 내부자 정보유출 : 외부 해킹에 의한 것이 아닌 금전적 이익으로 인해 내부 직원이 개인정보를 판매하는 등 유출시키는 경우에 해당된다. 최근 카드사 개인정보 유출 사건이 내부 직원에 의한 것이며 현재 50,000건 정도 유출된 것으로 추정되고 있다.

3.4.3 내부 네트워크 구간

[분류1] 스니핑 : 금융기관의 내부 시스템 간에 연결된 네트워크에서 송·수신되는 데이터 트래픽을 도청할 수 있거나 가로채는 위협으로 아직 공식적인 사례는 발견되지 않았으나 충분히 외부에서 발생되는 스니핑 공격이 내부에서도 공격자에 의해 발생될 수 있는 가능성이 있다.

Ⅳ. 결론

지금까지 전자금융 환경과 전자적 장치, 네트워크, 금융기관, 이용자 구간에서 발생될 수 있는 보안위협에 대해 살펴보았다. 최근에 금융기관 내부 시스템을 대상으로 공격적인 위협이 발생하고 있고 이로 인해 이용자의 금융 정보가 유출되는 사고가 있었다. 이처럼 금융권에서 발생되는 공격적인 위협은 네트워크이나 이용자단에서만 발생하는 것이 아니라 금융기관을 상대로 공격이 행해지는 추세이다. 또한 제휴 사업자에서도 이용자의 금융정보를 취급하거나 전자금융서비스를 제공하고 있어 제휴사업자를 대상으로 발생 가능한 보안위협을 분석하는 것이 추가적으로 필요하다. 이처럼 전자금융서비스를 대상으로 한 보안위협은 지속적으로 발생하고 있으며 새로운 보안위협을 분석하고 이를 분류함으로서 전자금융서비스의 위협 포인트를 파악하는 것이 향후 대응 방안 연구에 대한 기반이 될 수 있을 것이다.

참고문헌

[1] 김기서, "전자금융거래법의 제정과 시행에 따른 과제", 전국은행연합회, 월간금융, 2006.

[2] 김인석, "전자금융 사고유형 분석을 통한 정보보호 정책에 관한 연구", 고려대학교, 2008.

[3] 김인석, 김태호, 강형우, 이정호, 홍기석, 전자금융 이러면 안전할까 - 금융 IT보호를 위한 최고의 길잡이, 2010.

[4] 금융감독원, 전자금융감독규정 해설, 2009.

[5] 금융보안연구원, 해외 주요국 인터넷 뱅킹 현황조사 보고서, 2010.

[6] 금융보안연구원 '휴먼팩터가 보안에 미치는 영향' 2011

[7] 배광진, 임강빈, "키보드 보안의 근본적인 취약점 분석", 한국정보보호학회논문지, v.18, no.3, pp. 89-95 , 2008년 6월.

[8] 성재모, "국내외 전자금융 보안정책 분석을 통한 효과적인 전자금융 보안 대응 체계", 전남대학교, 2011.

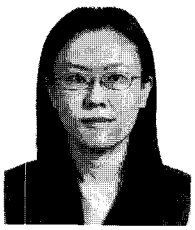
[9] 성재모, 이수미, 노봉남, 안승호, "이용자의 금융거래정보 보호를 위한 확장 종단간(End-to-End;E2E) 암호화 기술과 보안고려사항", 한국정보보호학회논문지, v.20, no.4, pp.145-154, 2010년 8월.

[10] ISO/IEC 27001 : Information technology -Security techniques - Information security management systems requirements.

[11] 이윤영, 최해랑, 한정훈, 홍수민, 이성진, 신동휘, 김승주, 원동호, "홈트레이딩 시스템 서비스의 보안 취약점 분석 및 평가기준 제안", 한국정보보호학회논문지, v.18, no.1, pp. 115-137 , 2008년 2월.

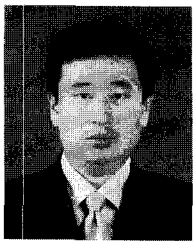
[12] 인터넷침해사고대응지원센터, "국내 주요 사이트 대상 분산서비스거부공격 분석보고서", 2009.

〈著者紹介〉



이 수 미 (Su-Mi Lee)
정회원

2003년 2월 : 고려대학교 정보보호대학원 석사
2004년 3월~2006년 8월 : 나사렛대학교 정보과학부 겸임교수
2007년 2월 : 고려대학교 정보보호대학원 박사
2006년 12월~현재: 금융보안연구원 u-금융연구팀 선임연구원
2010년 3월~현재 : 고려대학교 정보보호대학원 금융보안학과 초빙교수
<관심분야> 암호프로토콜, 포렌식 분야



성 재 모 (Jaemo Seung)
정회원

1993년 2월 : 스트븐스공과 대학원 전산학과 석사
2011년 2월 : 전남대학교 정보보호협동과정 박사
1993년 8월~2003년 8월 : 데이콤 정보보호기술팀 팀장
2003년 8월~2006년 10월 : KISA 인터넷침해사고대응지원센터 해킹대응팀 팀장
2006년 10월~현재 : 금융보안연구원 정보보안본부 본부장
<관심분야> 정보보호 관리체계, 포렌식, 컴퓨터와 네트워크, 모바일 보안, 금융보안 분야