정 보 보 호 학 회 지
제23권 제6호, 2013. 12

전자금융 보안위협 관련 대응기술 연구 추진 방안

조 강 유*, 민 상 식**, 성 재 모***

요 약

최근 정보 기술(IT)의 발전은 전자금융환경에 큰 영향을 주고 있으며, 전자금융 서비스 채널을 인터넷뱅킹, 스마트폰 뱅킹 등으로 다양하게 진화시켰다. 하지만 이러한 전자금융 서비스는 내부자로 인한 정보 유출뿐만 아니라 전문화된 악성코드의 대상이 되는 등 다양한 위협이 존재하고 있다. 본 논문에서는 전자금융 사고 분석을 통해서 다양한 전자금융 보안 위협에 대응할 수 있는 보안기술 연구 방향을 도출하고자 한다.

Ⅰ. 서 론

정보기술의 발전은 디바이스, 인프라, 통신 환경에 영향을 주고 있으며, 점차적으로 스마트화・융합화가 되고 있다[1]. 전 세계적으로 PC 및 모바일을 이용한 전자금융 이용자를 증가시켰으며 온라인 뱅킹 서비스뿐만 아니라 지급결제 영역에 영향을 줌으로써 금융 인프라의 성장을 도모시키고 있다[2].

특히 금융회사는 대면 위주의 서비스가 비대면 거래로 진화함에 따라[3] 표 1과 같이 인터넷뱅킹, 스마트폰 뱅킹 등 다양한 서비스를 제공하고 있다. 한국은행에 따르면 2013년 9월말 현재 전체 인터넷뱅킹 등록 고객수는 9,347만명으로 전분기말(9,163만명)대비 2.0%(+183만명) 증가하였으며, 모바일뱅킹 등록 고객수는 스마트폰기반 등록고객의 증가에 힘입어 전분기말(4,432만명) 대비 6.2%(+274만명) 증가한 4,706만명으로 집계되었다[4].

하지만 이러한 전자금융 서비스는 외부 해킹, 내부자로 인한 정보 유출뿐만 아니라 인터넷 뱅킹, 온라인 결제 등을 대상으로 하는 전문화된 악성코드가 지속적으로 발견되는 등 다양한 위협이 존재한다. 또한 백신 프로그램만으로 수많은 악성코드 및 취약점을 대응하기에는 많은 어려움이 존재하기 때문에 이를 대응하기 위한 다양한 연구가 필요하다.

이에 본 논문에서는 국내 전자금융 주요 사고 사례 분석을 통해 이를 대응하기 위한 보안기술 및 연구 방향을 도출하고자 한다.

〔표 1〕 국내 주요 전자금융 서비스 현황

권역	주요 전자금융 서비스(2013년 2월 기준)
은행	뱅킹서비스(오픈뱅킹, 인터넷뱅킹, 텔레뱅킹, 뱅킹전용프로그램서비스 등), 모바일뱅킹(VM뱅킹, IC칩 뱅킹, WAP뱅킹, PDA 뱅킹 등), CD/ATM서비스, 금융IC카드 서비스(현금카드결제서비스, 전자통장, 전자화폐, 폰 ATM 등), 기타(POS 뱅킹 에스크로, 전자지불시스템, TV-ATM뱅킹 등)
증권	폰트레이딩(ARS주식매매거래), 인터넷트레이딩(HTS, WTS), 모바일트레이딩(MTS), 전자금융 서비스, 기타 상품 서비스(펀드, CMA, 방카슈랑스, ELS/DLS 등)
카드	결제서비스(직불, 후불), 결제서비스(선불), 카드대출서비스, 로열티서비스, 부가서비스(결제 편의성/보안성/생활 편의성)
보험	인터넷마케팅(보험가입 및 신청, 조회, 대출, 증명서발급 등), 모바일마케팅, 텔레마케팅, 기타서비스(전자청약서비스 등)

* 금융보안연구원 보안기술팀 (kycho@fsa.or.kr)
** 금융보안연구원 보안기술팀 (ssmin@fsa.or.kr)
*** 금융보안연구원 정보보안본부 (sitcom@fsa.or.kr)

Ⅱ. 국내 주요 전자금융 사고 사례 및 위협 분석

시만텍社에 따르면 중요 인프라에 대한 공격, 클라이언트 S/W에 대한 공격, 제어시스템 대상 공격 등 최근 사건에 사용된 공격 기술들이 점점 더 정교화 되고 있으며[5], 사회 공학적 기법이 이용되는 등 금융회사의 공격도 다양해지고 있다.

국내에서 발생한 2011년 N社 전산망 장애, 2013년 3.20사건 등을 보면 공격자는 장기간에 걸쳐 정보를 수집하고, 최신 익스플로잇 등의 다양한 기법을 이용하는 등 지속적으로 공격기법이 발전하고 있다. 최초 회사 내부의 PC나 서버에 침입하기 위해 이메일을 이용한 악성코드 전파, 클라이언트 소프트웨어 취약점 공격, 브라우저 취약점을 악용하기 위한 웹사이트 해킹공격 등 다양한 공격기법이 이용되고 있다[6].

2011년 美 C그룹 정보 유출은 해킹을 통해 네트워크에 직접 침투하였으며[7], 2011년 日 C카드社는 내부자에 의해 정보가 유출되는 등 보안사고가 발생하였다[8],

이러한 공격기술이 정교화 되고 전자금융 채널이 다양해짐에 따라 발생되는 전자금융 사고 및 피해 금액도 표2와 같이 증가되고 있다[9].

〔표 2〕 10년간 전자금융관련 사고 현황

년도	건수	금액	년도	건수	금액
2004년	20	192	2009년	24	384.2
2005년	11	411	2010년	16	591.6
2006년	2	15	2011년	10	130.3
2007년	23	331.5	2012년	82	2058.9
2008년	10	428	2013년 6월	224	2271.3

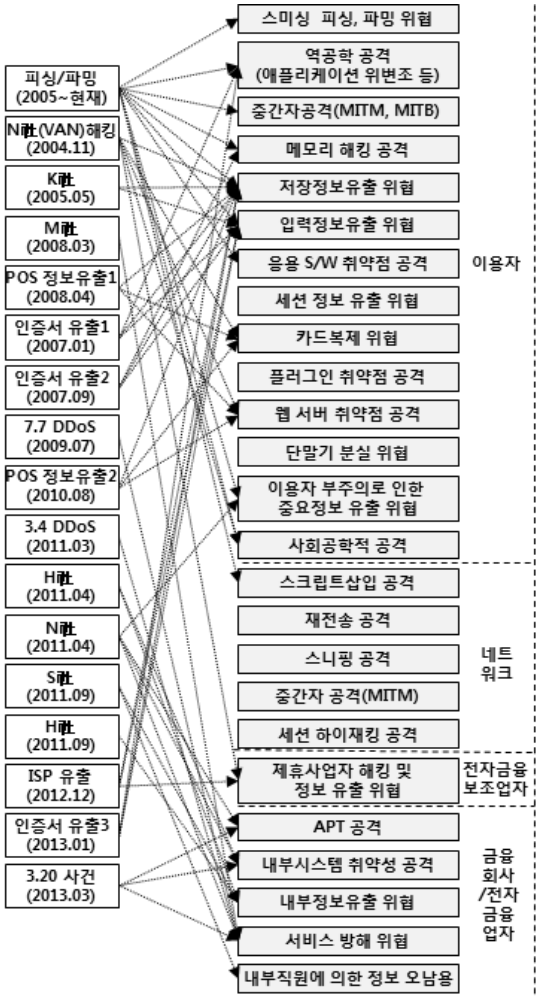
(단위:건, 백만원)

표 3은 2012년 12월 ISP 정보 유출, 2013년 3.20 전산망 장애 등 국내 전자금융관련 주요사고를 보여준다. 최근에는 내부 직원을 통한 금융정보를 포함한 개인정보 유출뿐만 아니라 악성코드를 이용하여 하드디스크 데이터를 파괴하는 등 사고 유형도 다양해짐을 알 수 있다.

국내에서 발생한 전자금융관련 사고는 주로 악성코드 감염(피싱 메일, 제로데이 취약점 등)과 내부자 유출, 해킹 등을 통하여 발생하였다. 이러한 전자금융 사고 분석을 기반으로 스미싱·파밍, 역공학 위협, 중간자 공격(MITM, MITB), APT 공격 등 최근 공격에 대한 위협을 그림 1과 같이 이용자, 네트워크, 전자금융보조업자, 금융회사 및 전자금융업자 측면으로 구분하고 이와 관련된 위협을 25개로 분류하였다.

〔표 3〕 최근 국내 금융기관의 주요 피해 사례 및 관련 보안위협

발생일	대상	피해사례	보안위협
2005년 ~	이용자	피싱 메일, 취약점 등을 이용하여 사용자 PC를 감염시켜 정보를 빼내거나, 개인정보를 입력하도록 유도	-스미싱 피싱, 파밍 위협 -역공학 공격 -메모리 해킹 공격 등
2010년 8월 ~ 9월	이용자	프랜차이즈 음식점에서 카드결제, 판매내역 등이 포스(POS) 시스템을 해킹해 다량으로 고객 정보가 유출되어, 해외에서 460여건이 부정사용	-저장정보유출 위협 -카드복제 위협 -웹 서버 취약점 공격
2011년 4월	N社	I社 직원 노트북에 악성코드를 심은 후, 감염된 노트북을 H社 서버에 연결하면 악성코드를 삽입하고, 서버 데이터가 삭제	-이용자 부주의로 인한 중요정보 유출 위협 -APT 등
2012년 1월	이용자	대형마트의 포스 단말기의 보안 문제로 인해 카드 정보가 유출되어 해외에서 복제카드가 무단으로 사용	-카드복제 위협 -저장정보 유출위협
2011년 9월	H社	내부 직원을 통해 S社 가입자 5만여명의 고객정보가 유출	-내부정보유출 위협
2012년 12월 (ISP 해킹)	A社 B社	사용자PC에서 ISP 정보를 유출시켜 30만원 미만의 소액결제를 통해 부정사용하여 190명이 피해	-입력정보유출 위협 -제휴사업자 해킹 등
2013년 1월	이용자	사용자 PC가 악성코드에 감염되어 공인인증서 700여개가 탈취되었으며, 만료된 약 300여개를 제외한 약 400여개의 공인인증서를 폐기	-역공학 공격 -입력정보유출 위협 -저장정보유출 위협
2013년 3월 (3.20 사건)	금융회사 다수	내부 컴퓨터가 악성코드에 감염된 후 사내 업데이트서버 취약점을 이용하여 악성코드를 내부에 유포. PC에 저장된 서버 정보를 수집하여 서버 데이터 및 사용자PC 데이터 삭제	-APT -내부통제 취약성 공격 -서비스 방해 위협 등



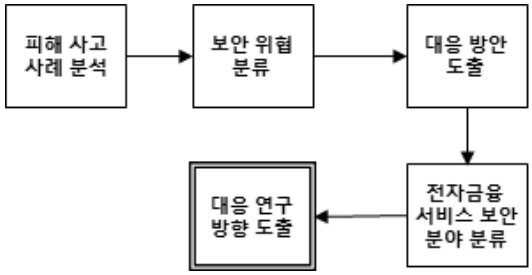
〔그림 1〕 사고 사례 분석을 통한 위협 분류안

상기 분류에 따르면 지난 2013년 3월에 발생한 3.20 사건의 경우 특정 대상을 목표로 설정하여 주요 정보 탈취 및 파괴 등을 목표로 한다. 이를 위해 신규 취약점을 이용하여 지능적인 공격을 지속적으로 시도하기 때문에 APT 공격, 내부 시스템 취약성 공격, 서비스 방해 위협으로 분류한다.

Ⅲ. 전자금융 위협 대응 및 보안기술 연구 방향

3.1. 전자금융 보안기술 연구 방향 도출 방법

전자금융 위협에 대응하기 위한 보안기술 연구 방향을 도출 방법은 그림 2와 같다.

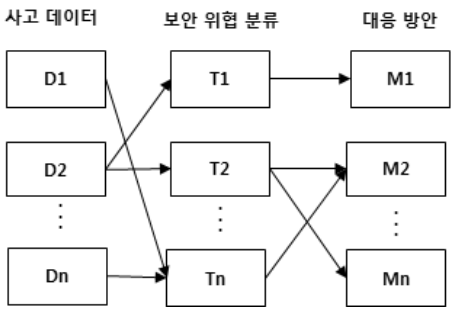


〔그림 2〕 전자금융 보안기술 연구 방향 도출 방법

첫 번째로 국내에서 발생한 피싱·파밍, ISP유출, 3.20 사건 등 전자금융 사고 데이터 분석을 통하여 2장에서 언급한 바와 같이 보안 위협을 분류한다. 두 번째로는 분석된 보안 위협별로 각각의 대응 방안 기술을 도출한다. 셋째로 전자금융 보안위협에 대응할 수 있는 보안기술 분류 체계를 도출하며 이는 3.2장에서 언급한다. 마지막으로 보안기술 분류에 따른 전자금융 서비스에 필요한 보안위협 대응 기술연구 방향을 도출한다.

3.2. 전자금융 보안 위협 대응 방안 분석 및 보안 분야 분류

전자금융 보안 위협별 대응 방안을 도출하는 방법은 그림 3과 같이 전자금융 사고별로 보안 위협을 분석한 후 대응 방안을 도출하는 절차로 진행된다.



〔그림 3〕 각 위협별 대응 방안 도출 방법 예시

보안위협 대응항목은 금융보안에 대한 기술, 정책, 시험, 교육 등 범위를 반영하였다. 예를 들어 APT 공격에 대한 대응 방안의 경우 악성코드 방어, 공격 위협 사전 대응 정보 수집, 금융회사간 통합 모니터링, 접근제어(매체 접근), 망분리 구축 등 다양한 대응 기술 및 정책 등의 대응방안이 필요하다.

〔표 4〕 보안 위협 대응 방안

구 분	보안위협 대응
인증기술	·카드결제 인증 강화 ·사용자 인증 강화 ·서버인증(EV SSL 인증서 등)
암호기술	·저장정보 암호 기술 강화 ·전송 암호 기술 강화
서비스 보안	·거래전문 무결성 강화 ·입력정보보호 ·악성코드 방어(ActiveX 등) ·소프트웨어 무결성 검증 및 난독화
응용 S/W 보안	·소프트웨어 개발보안 ·전자금융 보안S/W 시험강화
스마트 기기보안	·악성코드 방어(악성 앱) ·스마트기기보안 및 관리 강화
모니터링	·악성코드 방어(APT공격 대응) ·공격 위협 사전 대응 정보 수집 ·이상행위(거래, 세션 등) 모니터링 ·피싱사이트 탐지 및 차단 ·금융회사 간 통합 모니터링
보안관리	·운영자 계정관리 ·내부 통제 강화 ·접근제어(매체제어) ·제휴 사업자 안전성 점검
네트워크 보안관리	·망분리(가상화 등) ·무선 통신망 보안 강화
사고대응/ 복구	·운영로그 저장 및 분석(포렌식 등) ·사이버 공격대응 모의 훈련 ·서비스 연속성(이중화, 백업, 복구 등)
이용자 보안	·전자금융 이용자 환경 보안 강화 ·IC카드 적용 확대 ·전자금융 이용자 대상 교육
차세대 보안	-

전자금융 서비스의 보안 분야는 분석된 위협과 국내외 정보보안 관련 표준 로드맵[10,11,12,13]을 반영하여 인증기술, 암호기술, 서비스 보안, 응용 S/W보안, 스마트기기보안, 모니터링, 보안관리, 네트워크 보안, 사고대응/복구, 이용자보안, 차세대 보안의 11개 항목으로 구분하였다. 이는 보안 분야별로 각 전자금융 보안위협을 반영한 연구 주제를 분류하기 위한 데이터로 활용된다. 표 4는 전자금융 서비스 보안 분류와 보안위협별로 대응 방안 도출 결과를 보여준다,

3.3. 전자금융 보안기술 연구 방향 도출

전자금융 보안 위협 대응과 서비스 보안 분류에 따른 연구 방향은 표 5와 같다. 이는 현재까지 발생한 전자금융 사고 데이터와 최근 금융권의 위협요소를 적용한 연구 방향으로써, 우선적으로 선행되어야 할 것으로 판단된다.

서비스 부분에서는 스마트결제 서비스 보안기술 연구의 경우, 현재 PC 및 모바일 기반의 다양한 결제 서비스(USIM, 앱카드 등)가 등장하고 있기 때문에 이에 대한 보안 강화 방안 연구가 이루어져야 할 것이다.

〔표 5〕 전자금융 보안기술 연구 방향

구 분	전자금융 보안기술 연구 방향 도출
인증기술	·사용자 및 디바이스 인증 기술 연구 ·전자금융 新 인증기술 연구
암호기술	·금융부문 암호기술 보안성 연구 ·암호키 관리 및 적용방안 연구 ·전자서명 기술 연구
서비스 보안	·입력정보보호 강화방안 ·스마트 결제 서비스 보안기술 연구 ·위변조 대응 기술 연구 ·이용자 단말의 악성코드 대응 기술 연구 ·금융S/W 배포 검증 기술 연구 ·금융부문 보안적합성시험 , 품질 평가
응용 S/W 보안	·금융 S/W 시큐어코딩 방안 연구 ·전자금융S/W 취약점 분석
스마트 기기보안	·모바일 악성 앱 위협 대응 방안 연구 ·스마트 단말 관리 방안 연구 ·스마트 단말 보안 강화 기술 연구
모니터링	·금융사 대상 악성코드(APT) 위협 대응 방안 연구 ·이상거래 탐지 시스템 기술 연구 ·금융 위협정보 공유체계 연구 ·유사 및 피싱 도메인 탐지 강화
보안관리	·내부 통제 강화 기술 및 정책 연구 ·업무용 PC 보안 관리 강화 연구 ·금융IT 보안 컴플라이언스 연구 ·개인정보보호 기술 및 정책 연구
네트워크 보안관리	·금융회사 망분리 방안 연구
사고대응 / 복구	·금융 디지털 포렌식 연구 ·홈페이지/서버/네트워크 등 취약점분석 ·DDoS 등 공격대응 모의 훈련
이용자 보안	·이용자단 S/W 보안강화 연구 ·금융 보안 교육 강화
차세대 보안	·금융부문 빅데이터 분석 기술 응용방안 연구 ·차세대 웹 기술 금융권 적용 방안 연구 ·차세대 통신망에서의 전자금융 안전성 연구 ·금융부문 클라우드 컴퓨팅 보안연구 ·보안강화를 위한 표준화 연구

모니터링 부분에서는 이상거래 탐지 및 대응 기술 연구의 경우 이용자 구간(거래 단말, 거래 채널 등)의 정보와 연계하여 제공될 수 있는 탐지 방안이나 현재 도입된 이상금융거래시스템의 기능을 향상 시킬 수 있는 기술 및 표준이 도입될 수 있도록 지속적인 연구가 이루어져야 할 것으로 판단된다.

금융회사 망분리 방안 연구의 경우에는 망분리 적용 기술뿐만 아니라 망분리시 적용되는 망연계 등 다양한 기술에 대한 보안 위협 및 안전하고 효율적으로 적용할 수 있는 방안에 대해 연구가 필요하다.

Ⅳ. 결 론

전자금융 서비스 채널은 온라인 뱅킹, 스마트폰 뱅킹 등으로 다양화 되고 있지만 전자금융 사고도 해킹, 악성코드, 내부자 등으로 인해 금융정보 유출뿐만 아니라 직접적인 금전적 피해가 지속적으로 발생하고 있다. 특히 최근에는 금융 전산망 내부의 데이터를 직접적으로 파괴(삭제)함으로써 업무중단으로 인한 사회적 혼란까지 야기시키고 있다.

이처럼 전자금융 보안 위협도 지속적으로 증가되고 위협 요소도 다양해짐에 따라 이를 대응하기 위한 전자금융 보안기술 연구의 필요성이 증가되고 있다.

본 논문에서는 약 10년 동안의 전자금융 사고에 대한 위협 분석을 기반으로 보안 위협에 대한 연구 방향을 도출하였다. 이를 기반으로 전자금융서비스 분야에서 잠재적으로 존재하는 보안 위협이나 향후 발생 가능한 다양한 보안 위협에 대해 피해를 최소화하고 선제적으로 대응할 수 있는 체계에 활용 가능할 것으로 기대된다.

참고문헌

[1] Brett king, “bank 2.0”, Marchall Cavendish Business, 2010

[2] Capgemini, “World Payments REPORT 2011”, 2011.08

[3] Deloitte Consulting, “The Future Of Bank Branch”, 2009. 2

[4] 한국은행, “2013 3/4분기 국내 인터넷뱅킹 서비스 이용현황”, 2013.11

[5] Symantec, Internet Security Threat Report 2013,

[6] 성재모, “국내외 전자금융 보안정책 분석을 통한 효과적인 전자금융 보안 대응 체계”, 전남대학교, 2011

[7] “씨티그룹 해킹당해...20만명 계좌정보 유출”, 뉴스핌, 2011. 6

[8] “씨티카드, 일본 고객 9만명 정보 유출”, 조선일보, 2011. 9

[9] 금융감독원, “10년간 전자금융사고 발생현황”, 2013.9

[10] 한국정보통신기술협회, “2013 ICT 표준화 전략맵”, 2013

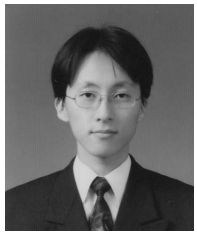
[11] 지식경제부, “정보통신 산업융합원천 R&D 전략(2012~2016), 2011.11

[12] 한국인터넷진흥원, “2013 국가정보보호백서”, 2013

[13] ACM Digital Library, “http://dl.acm.org”, 2012

〈저자소개〉

조 강 유 (Kangyu Cho)
2012년 8월 : 전남대학교 정보보안협동과정 석사
2012년 5월~현재 : 금융보안연구원 보안기술팀 연구원
<관심분야> 악성코드, 모바일 보안, 카드결제 보안



민 상 식 (Sangshik Min)
2009년 8월~현재 : 금융보안연구원 보안기술팀 팀장
<관심분야> 가상화 및 클라우드 컴퓨팅, 대용량 데이터 분석, 모바일 보안, HTML5, 소셜 네트워크 보안, 오픈뱅킹 보안

성 재 모 (Jaemo Seung)
정회원
1993년 2월 : 스티븐스공과 대학교 전산학 석사
2011년 2월 : 전남대학교 정보보호 박사
1993년 8월~2003년 8월 : LG 데이콤 정보보호기술팀 팀장
2003년 8월~2006년 10월 : KISA 인터넷침해사고대응지원센터 해킹대응팀 팀장
2006년 10월~현재 : 금융보안연구원 정보보안본부 본부장
<관심분야> 컴플라이언스, 정보보호 관리체계, 포렌식, 컴퓨터와 네트워크, 모바일 보안, 금융보안 분야