금융기관을 타켓으로 하는 피싱/파밍 공격 기술 동향


김 승 현
ETRI


이 성 훈
과학기술연합대학원대학교 (UST)


진 승 헌
ETRI

Ⅰ. 동향 소개

한국은행은 'The Banker' 2013년 7월호에 수록된 내용을 기초로 작성된 '세계 1000대 은행과 우리나라 은행' 보고서를 통해 10개 국내 은행이 세계 1000대 은행에 포함됐으며, 〈표 1〉과 같이 이 중에서 6개 은행이 세계 100대 은행에 포함됐다는 내용을 밝혔다[1].

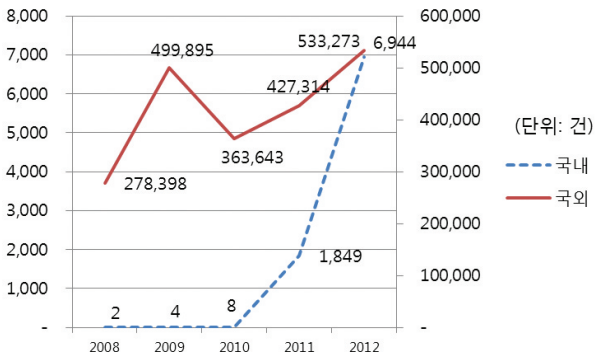
이처럼 국내 은행의 자본이 성장한 큰 이유 중의 하나로, 인터넷을 통한 온라인 뱅킹의 활성화를 꼽을 수 있을 것이다. 국내 인터넷뱅킹서비스 현황을 살펴보면, 2013년 3월까지 인터넷뱅킹 등록고객수는 8,940만명이며, 하루 평균 인터넷뱅킹의 이용금액은 33.8조원으로 전체 금융 거래의 31.4%를 차지하고 있다[2]. 또한 국내 스

〈표 1〉 국내 은행의 세계 순위 (억 달러)

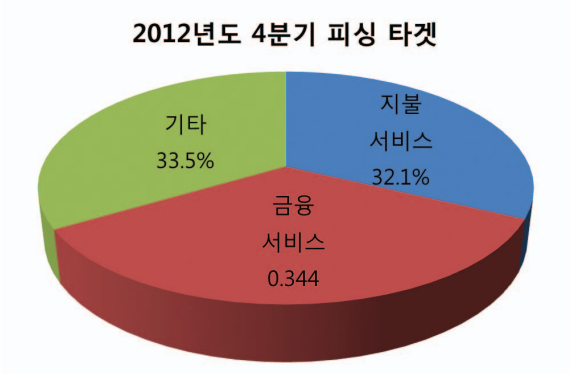
2012년 말				
순위		은행명	기본자본	총자산
기본자본	총자산			
68	88	KB지주	192.4	2,634.1
69	111	산은지주	188.3	1,792.1
72	79	우리지주	181.1	3,042.3
73	86	신한지주	178.6	2,810.1
81	87	하나지주	156.7	2,650.1
83	95	농협지주	154.6	2,297.2
111	105	기업	105.0	1,847.0
290	328	BS지주	29.1	400.6
322	362	DGB지주	24.6	319.6
744	660	전북	6.7	106.4

출처 : 한국은행, "세계1000대 은행과 우리나라 은행", 2013년 7월

〈표 2〉 국내외 피싱 사이트 피해 현황



출처 : 인터넷진흥원(국내), APWG 2012 4분기 보고서(국외)



출처 : APWG 2012 4분기 보고서

〈그림 1〉 2012년도 4분기 피싱 타겟

마트폰 가입자 수가 3,300만 명에 육박할 만큼 스마트폰이 보급되면서[3], 모바일뱅킹 등록고객수도 4,113만명을 기록했다[2]. 2013년도 1/4분기 중 하루 평균 모바일 뱅킹 이용 금액은 1조 2,640억원으로 전체 인터넷 뱅킹 이용 금액의 3.8% 수준이지만 지속적으로 상승하고 있다.

금융기관의 인터넷 뱅킹 발달과 함께 피싱/파밍 공격의 피해가 심각해지고 있다. 금융감독원에 따르면 2006년부터 올해 5월까지 경찰청에 신고된 피싱 사기 피해 규모는 약 4,380억원에 달한다[4]. 〈표 2〉와 같이, 국내의 경우에는 2011년부터 본격적으로 온라인 피싱 피해가 발생하기 시작하였으며, 공격 수법이 갈수록 고도화되어 피해가 증가하고 있는 추세이다[5]. 국외의 경우에는 2010년에 잠시 말웨어(Malware)에 집중된 공격으로 인해서 잠시 주춤하였지만, 그 이후에는 꾸준히 피싱 공격이 증가하고 있다[6].

카스퍼스키 랩(Kaspersky Lab)의 '2011-2013 피싱 공격의 진화' 리포트에 따르면, 최근 1년 사이에 5천만명 중에 3,730만명이 피싱 공격을 경험할 정도로 피싱 공격이 일상화되었다. 이중에 12%만이 전통적인 방식인 스팸 메일을 통해 피싱 공격을 시도하였고, 나머지 88%는 웹 사이트의 배너, 블로그나 포럼의 메시지, 메신저의 메시지 등과 같은 다양한 채널을 통해 시도됐다[7]. APWG (Anti Phishing Working Group)의 2012년도 4분기 피싱 액티비티 트렌드 보고서에 따르면, 〈그림 1〉 처럼 피싱 공격의 2/3에 해당하는 지불 서비스(32.1%)와 금융 서비스(34.4%)같이 환금성이 뛰어난 업종이 주요 타겟이었다[6].

본 논문에서는 금융기관을 타켓으로 하는 피싱/파밍 공격과 이에 대응하는 현재의 보안 솔루션의 특징 및 한계점을 살펴본다. 그리고 결론 및 향후 연구로 마무리한다.

Ⅱ. 피싱/파밍 공격

1. 온라인 피싱/파밍

온라인 피싱/파밍은 사용자 PC에서 인터넷을 사용하는 과정에서 발생하는 공격을 가리킨다. 스팸메일이나 원본 사이트와 유사한 웹주소를 가진 피싱사이트 같은 전통적인 방식에서부터 신원을 사칭하는 APT 공격 또는 악성코드와 같은 고도화된 피싱/파밍 공격까지 다양한 온라인 피싱/파밍 공격 유형이 존재한다.

스팸메일이나 원본 사이트와 유사한 웹주소를 가진 피싱사이트 같은 전통적인 방식에서부터 신원을 사칭하는 APT 공격 또는 악성코드와 같은 고도화된 피싱/파밍 공격까지 다양한 온라인 피싱/파밍 공격 유형이 존재한다.

최근에는 악성코드로 인한 공격이 많이 발견되고 있는데, 주로 불법 다운로드 컨텐츠에 악성코드를 심어 파밍 공격을 수행한다. 사용자가 컨텐츠를 다운받아 실

행하면 사용자의 컴퓨터는 악성코드에 감염된다. 악성코드는 사용자가 원본 은행 홈페이지에 접속하려 할 때, 가짜 은행 홈페이지로 접속하도록 조작한다. 그리고 사용자에게 보안 승급 명목으로 보안카드 번호 등 개인 금융정보를 입력을 요청한 뒤, 공인인증서를 재발급 받아 해커의 통장으로 돈을 이체한다[8-9].

한국의 금융서비스를 타켓으로 하여, 보안 솔루션처럼 보이면서 금융 개인정보를 탈취하는 악성코드도 발견되고 있다. 인터넷 뱅킹 보안 솔루션을 변조한 악성코드인 KRBanker가 가장 유명한데, 이 악성코드는 2012년 9월에 처음 등장했으며 2013년 6월까지 약 550개의 변종이 확인됐다. 특히 최근에는 보안 인증 및 암호화 등을 수행하는 보안 솔루션의 특정 모듈을 악성행위를 수행하도록 변조하는 기법을 사용한다. 이렇게 변조된 보안 모듈은 정상 보안 수단 확인 창 대신에 가짜 보안 수단 확인 창을 띄워 사용자의 금융 관련 개인정보를 탈취한다[10].

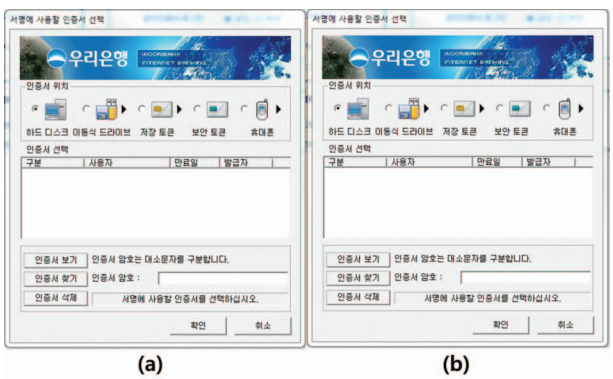
계좌정보와 암호는 물론이고 공인인증서까지 탈취하는 '카스토브' 트로이목마도 존재한다. 이 악성코드는 공격용 툴킷 '공다'를 통해 배포되고 있는데, 보안업체인 시만텍의 분석결과 공격의 98%가 한국에 집중된 것으로 나타났다. 이 악성코드의 공격은 크게 2단계로 이뤄진다. 사용자의 컴퓨터가 1차 악성코드에 감염되면, 안티바이러스 소프트웨어의 작동을 멈추게 하고, 2단계에서 명령제어(C&C) 서버로부터 암호화된 파일을 사용자의 컴퓨터에 다운로드 시킨다. 이 파일은 암호, 계좌정보, 거래 내역은 물론 NPKI 폴더에 저장된 디지털 인증서도 수집한다[11].

악성코드 감염을 목적으로 사칭 이메일을 보내는 방법도 여전히 사용되고 있다. 2013년 4월, 한국인터넷진흥원(KISA)를 사칭하여 3.20 전산망 대란 관련 악성코드 치료용 전용백신 첨부 이메일을 보내는 사례가 보고되었다. 해당 파일을 다운로드하여 실행하면 실제 백신과 똑같이 전용 백신 도움말 화면이 실행되기 때문에, 사용자는 악성코드 여부를 알 수 없다. 하지만 실제로는 악성코드가 설치되어 피싱/파밍 공격을 수행한다[12].

이메일 피싱이 진화한 것이 스피어 피싱(Spear phishing)이다. 스피어 피싱은 이미 유출된 정보를 이용하여 특정 개인 또는 조직으로 대상을 한정하여 공격하는 피싱 수법이다. 불특정 다수가 아닌 소수를 대상으로 피싱 공격을 시도하기 때문에 대응하기가 매우 어렵다[13]. 중국 해커들의 뉴욕 타임스 공격 사건이 대표적이며, 기업 네트워크에 가해지는 공격의 95%는 스피어 피싱이다[14].

사용자가 알지 못하는 사이에 악성 콘텐츠를 사용자 몰래 사용자의 컴퓨터에 다운로드하는 '드라이브 바이 다운로드' 방식으로 악성코드가 감염되기도 한다[15]. 웹브라우저, 플러그인, 또는 브라우저에서 동작하는 컴포넌트의 취약점을 이용한 공격으로, 최근에는 자바 취약점이 악용되는 사례가 다수 등장하였다. 최근 안랩에서 보고한 악성코드의 경우, 드라이브 바이 다운로드 방식을 사용하였다. 이 악성코드는 〈그림 3〉과 같이 실제 공인인증서 사용화면과 똑같은 사용화면을 사용자에게 보여주기 때문에, 사용자는 실제 공인인증서 화면으로 착각하게 된다. 이 화면에서 사용자가 입력한 공인인증서와 비밀번호는 그대로 해커에 전달된다.

최근에는 보안카드의 두 자리 숫자 입력만으로도 피싱 공격에 성공하는 사례도 있다[16]. 사용자가 은행 사이트에 로그인 한 뒤 보안카드 번호 두 자리를 입력하고 이체를 실행하면, 보안카드 입력 에러 메시지를 사용자에게 보여준다. 전자금융감독 규정상 입력 오류나 거래 중지 후 재시도할 때 이전과 동일한 보안카드 번



〈그림 2〉 실제 공인인증서(a)와 똑같은 악성 코드 공인인증서(b)

호 입력을 요구하기 때문에, 해당 보안카드 번호를 재사용하여 해커의 PC에서 다른 사용자의 계좌로 자금을 이체하는 방식이다.

2. 스미싱

SMS와 피싱(Phishing)의 합성어인 스미싱(Smishing)은 휴대폰 문자메시지를 이용한 신종 사기 수법으로, 웹 사이트 링크가 포함된 문자 메시지를 전송하여 휴대폰 사용자가 링크를 클릭하거나 악성코드가 내장된 어플리케이션을 설치하게 유도한다. 악성코드는 사용자 몰래 개인정보를 탈취하거나 소액결제를 일으켜 금전적 피해를 발생시키고 스마트폰에 저장된 공인인증서를 탈취하여 2차 피해를 입히기도 한다.

스미싱을 이용한 공격 절차는 〈그림 4〉와 같다. 우선 해커가 스미싱 문자메시지를 사용자에게 전송한다. 사용자가 문자메시지를 확인 후 악성 어플리케이션을 설치하게 되면, 사용자의 스마트폰은 악성코드에 감염되고 해커는 사용자의 스마트폰 정보를 취득한다. 이렇게 취득한 정보로 스마트폰 소액결제를 시도하고, 인증번호를 가로채어 가로챈 인증번호로 결제를 완료한다[17].

스미싱에 사용되는 문자메시지의 형태는 휴대폰 소액결제 확인형, 프렌차이즈 업체 쿠폰 발송형, 금융기관 사칭 개인정보 확인형, 국가재난 전달형 등이 존재한다[18]. 사용자의 호기심을 유도하기 위해, 사회 이슈에 따라 문자메시지의 형태는 끊임없이 진화한다. 또한 문자메시지에 포함된 링크 주소를 단축URL(ex. bit.ly, goo.gl, durl.me 등)로 변형했기 때문에 사용자가 피싱사이트 여부를 확인하기 어렵다.

출처 : 보안닷컴

〈그림 3〉 스마트폰 스미싱 개요도

악성코드는 사용자 몰래 개인정보를 탈취하거나 소액결제를 일으켜 금전적 피해를 발생시키고 스마트폰에 저장된 공인인증서를 탈취하여 2차 피해를 입히기도 한다.

Ⅲ. 안티 피싱/파밍 기술 및 한계

1. 각 은행의 보안솔루션 소개(표)

온라인 피싱/파밍 공격으로부터 안전한 인터넷 뱅킹을 위하여, 국내 은행은 여러 보안 프로그램을 사용자의 컴퓨터에 설치하도록 요청한다. 1장에서 소개했던 세계 100대 은행에 선정된 국내 은행을 대상으로, 각 은행이 제공하는 보안솔루션(인터넷 익스플로러 버전)은 아래 〈표 3〉과 같다.

공인인증서, 개인 PC 방화벽, 키보드 보안, 안티 바이러스, 2채널 인증 솔루션, OTP는 6개 은행 모두가 적용하고 있다. 보안 로그 기록은 우리은행과 산업은행, 데이터 암호화는 농협과 산업은행, EV-SSL 인증서는 국민/우리/

〈표 3〉 국내 주요 은행 보안 솔루션 비교

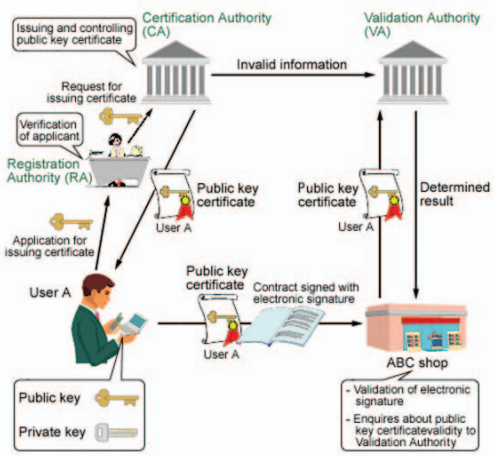
	국민	우리	하나	신한	농협	산업
공인인증서 보안(PKI)	o	o	o	o	o	o
개인 방화벽	o	o	o	o	o	o
키보드 보안	o	o	o	o	o	o
안티 바이러스(백신)	o	o	o	o	o	o
데이터 암호화	x	x	x	x	o	o
2채널 인증	o	o	o	o	o	o
보안 로그	x	o	x	x	x	o
EV-SSL 인증서	o	o	x	x	x	o
OTP	o	o	o	o	o	o
HSM	x	x	x	x	o	x
안티 파밍 솔루션	o	o	x	x	o	x
지정 PC제	o	o	o	o	o	x
그래픽 인증	x	o	x	o	x	x

산업은행이 적용하고 있다. 은행별로 최소한 4개 이상의 보안 솔루션을 적용하고 있으며, 인터넷 뱅킹을 시작하기 전에 모든 보안 프로그램을 제대로 설치한 사용자만이 인터넷 뱅킹을 시작할 수 있다.

2. 각 기술 설명

각 은행별로 적용하고 있는 보안 솔루션들에 대해서 알아보겠다. 우선 국내 은행은 PKI기반 서비스를 적용한 공인인증서로 사용자 인증을 수행한다. PKI(Public Key Infrastructure)는 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 보안 시스템 환경이다. 〈그림 4〉와 같이 사용자는 CA(Certificate Authority)로부터 공인인증서를 발급받고 PKI 서비스를 이용한다[19]. 공인인증서는 사용자의 컴퓨터나 이동식 디스크 등에 저장되는데, PKI 시스템을 안전하게 이용하기 위해서 사용자들은 ActiveX 기반의 웹브라우저 플러그인을 설치하도록 되어있다.

개인방화벽 프로그램은 비인가된 접근을 차단하고 악성프로그램을 자동으로 진단 및 치료해주는 프로그램으로 TCP/IP나 다른 프로토콜을 통하여 사용자 몰래 외부로 전송하거나 외부로부터의 접속이 있을 경우 이를 모니터링하고 차단/경고하는 기능을 제공한다. 주로 방화벽, 개인 정보 유출 차단, 클라이언트 접속 제한 등의 기능이 있다. 백신 기능이 포함되어 있는 프로그램을 사용하는 은행도 있고, 방화벽 기능만 있는 프로그램을 사용하는 은행도 있다.



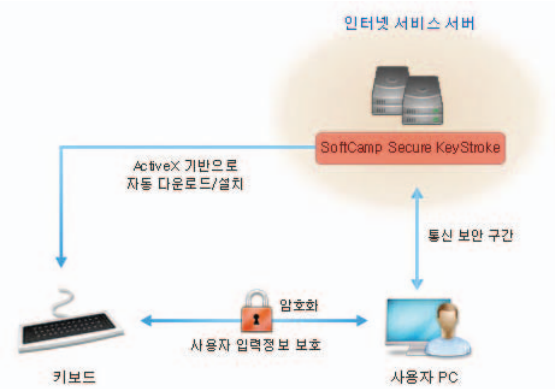
출처 : On the security of internet banking in South Korea

〈그림 4〉 PKI 구조

키보드 보안 솔루션은 사용자가 키보드를 통해서 입력하는 정보를 안전하게 관리하여, 기존에 알려져 있거나 혹은 알려지지 않은 키로깅(Key-logging) 프로그램들이 가로채지 못하도록 방어하는 프로그램이다. 〈그림 5〉와 같이 키보드를 통해 입력되는 사용자의 정보를 암호화함으로써 악의적인 해킹이나 공격에 의한 중요정보 유출을 방지한다.

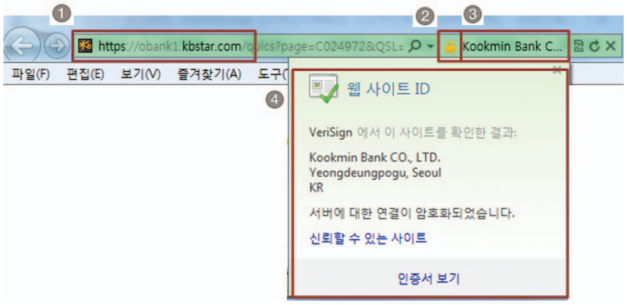
백신 프로그램은 사용자의 컴퓨터를 악의적인 악성코드로부터 보호하여 안전하게 인터넷 뱅킹을 할 수 있도록 도와준다. ActiveX 플러그인을 이용하여 은행 사이트에 접속하면 설치되고, 매번 사이트에 접속할 때마다 자동으로 실행된다.

2채널 인증 솔루션은 금융 거래 시 1채널(PC)에서 이루어지는 본인 인증 과정을 다른 채널(스마트폰, 유선 전화)로 확대하여 추가 인증을 하는 것을 말한다. 하나은행의 2채널 인증의 경우, 스마트폰 앱을 이용하여 인터넷뱅킹 이체 거래시에 임의로 생성된 1회용 비밀번호를 사용자의 스마트폰 앱에 입력해야 최종 거래가 가능하다. 국민은행은 ARS 채널을 이용하여 사용자의 전화번호로 전화를 걸어서 본인 확인을 수행한다. 우리은행은 ARS 혹은 휴대폰 SMS 인증을 추가 인증 수단으로 활용하고 있는데, 등록된 휴대폰번호로 전송된 인증번호를 입력하여 추가 인증을 한다. 추가 인증



출처 : 소프트캠프

〈그림 5〉 키보드 보안 솔루션



〈그림 6〉 EV SSL 화면

출처 : 국민은행

〈그림 7〉 국민은행의 파밍 차단 프로그램

수단인 ARS나 SMS, 스마트폰 앱 등으로 2채널 인증을 하지 않으면, 사용자의 컴퓨터에서 공인인증서나 개인정보가 유출되더라도 계좌이체가 불가능하게 된다.

OTP(One Time Password)는 사용자 측에서 별도의 하드웨어/소프트웨어를 통해서 전자금융 거래에서 사용되는 일회용 비밀번호를 생성하고, 웹 사이트는 검증 서버를 통해서 해당 비밀번호의 유효성을 인증하는 방식이다[20]. 1분마다 새로운 비밀번호가 생성되어 해킹이나 외부노출의 위험이 적고, 한번 사용된 비밀번호는 제한된 시간이 넘지 않았더라도 다시 사용할 수 없다. 사용자는 금융기관으로부터 OTP발생기를 발급받아서 사용할 수 있다.

OTP(One Time Password)는 사용자 측에서 별도의 하드웨어/소프트웨어를 통해서 전자금융 거래에서 사용되는 일회용 비밀번호를 생성하고, 웹 사이트는 검증 서버를 통해서 해당 비밀번호의 유효성을 인증하는 방식

EV SSL(Extended Validation SSL)은 웹브라우저와 웹서버 간의 암호화 통신 시, 사용자에게 서버의 안전성과 신뢰성을 전달하기 위하여 브라우저 주소 창을 녹색으로 변화시킨다. 발급 심사과정이 SSL 보다 더욱 강화되어 웹사이트 신원을 보증한다. 〈그림 6〉에서 첫 번째 표시는 녹색 주소창을 통하여 진짜 사이트임을 확인할 수 있고, 두 번째 노란색 자물쇠는 SSL 암호화통신임을 나타낸다. 세 번째는 접속한 사이트를 운영하고 있는 회사를 나타내고, 네 번째는 접속한 사이트를 운영하는 회사의 회사명, 주소 등을 나타내어 사용자가 웹 사이트 진위여부를 쉽게 확인할 수 있다.

HSM(Hardware Security Module)은 보안토큰으로 인증서 해킹방지를 위해 사용하는 보안성이 강화된 인증서 저장장치이다. HSM에 저장된 인증서는 해킹이 불가능하고 PIN번호가 일치해야만 이용가능하다. 현재 농협에서만 제공하는 서비스이다.

국민은행의 안티 파밍 솔루션은 실시간으로 사용자 PC의 Hosts 파일을 감시하여 위·변조 내역을 사용자에게 알려주고, 기존의 상태로 복원할 수 있어 파밍을 사전에 예방할 수 있는 프로그램이다. 〈그림 7〉과 같이 악성코드 및 기타 이유로 인해서 Hosts 파일 변경 시에 사용자에게 알려주고, 기존의 Hosts 파일로 복원할 수 있다.

농협의 '나만의 은행주소'는 사용자가 인터넷뱅킹 주소를 직접 만들어서 사용할 수 있는 개인별 인터넷뱅킹 주소를 제공하는 서비스이다. 피싱/파밍 악성코드에 감염되더라도 PC 입력된 은행 주소를 찾을 수 없기 때문에 피싱/파밍 공격 대응이 가능하다.

지정PC제는 등록된 PC에서만 이체 등 인터넷뱅킹 거래가 가능하도록 하는 서비스이다. 은행 서버는 사용자 PC의 고유한 맥 주소(MAC address)를 이용하여 기 등록된 PC를 인증한다.

그래픽인증 서비스는 실제 사용자가 사전에 본인이 선택한 그림(Hole)에 키로 설정한 그림들을 넣는 방식으

로, 2차 인증을 통해서 피싱 사이트 구별이 가능하다.

보안로그는 인터넷뱅킹 거래 IP정보를 확인하여 해킹(불량)IP 접속 차단 등 인터넷 뱅킹 거래 로그를 관리하는 프로그램이고, 데이터 암호화 프로그램은 송수신 데이터 암호화/복호화를 수행하는 프로그램이다.

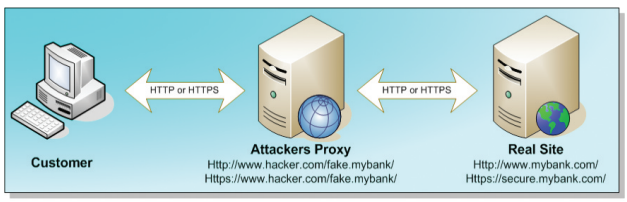
3. 한계

피싱/파밍 공격에 대응하기 위해 많은 보안 솔루션들이 제시되었고, 국내 금융 기관에서도 여러 보안 솔루션들을 적용하여 안전한 인터넷 뱅킹을 이용하도록 하고 있다. 하지만 이러한 보안 솔루션들이 있음에도 불구하고, 피싱/파밍 피해는 여전히 발생하고 있다. 본 절에서는 각 보안 솔루션들의 한계점에 대해서 알아본다.

PKI 기반 공인인증서는 사용자의 컴퓨터에 디지털 파일로 저장되기 때문에 복제가 용이하고 해커에 의해서 불법 복제가 됐더라도, 사용자는 해킹 여부를 인지할 수 없다. 또한 공인인증서 사용 및 관리를 위해서는 보안 플러인을 설치해야 하는데, 사용자의 컴퓨터에 설치되는 보안 플러그인이 진짜인지 악성코드가 숨겨진 플러그인이 사용자가 구분하기 어렵다.

> OTP의 유효 시간보다 더 짧은 시간에 해커가 사용자인 것처럼 실제 은행 사이트에 인증 받을 수 있다.

방화벽 프로그램, 키보드 보안 프로그램, 백신 프로그램 등은 사용자의 컴퓨터를 악성코드로부터 보호하기 위한 목적으로, 인터넷 뱅킹을 시작하기 전에 웹브라우저의 보안 플러그인 형태로 사용자의 컴퓨터에 설치된다. 이들 보안 솔루션은 끊임없이 더욱 고도화된 방식의 악성코드에 취약하다. 또한, 만일 사용자가 피싱 사이트에 접속한 뒤 정상 플러그인으로 착각하여 악성코드가 숨겨진 플러그인을 설치하게 되면, 사용자의 컴퓨터는 악성코드에 감염된다.



〈그림 8〉 MITM 피싱 공격

2채널 인증은 기존의 피싱 공격에는 효과적으로 대응할 수 있지만, Bruce Schneier에 의해 제기된 MITM (Man-In-The-Middle) 피싱 공격에는 대응하기 어렵다[21]. MITM 공격은 〈그림 8〉과 같이 해커가 사용자와 은행 서버 사이에 위치하면서 사용자에게는 은행 서버인척, 은행 서버에게는 사용자인척 속이며 동작한다. 피싱 사이트는 실제 사이트와 똑같은 UI로 구성되어 사용자가 피싱 사이트 여부를 구분하기 어렵고, 해커는 사용자가 입력한 정보를 실시간으로 포워딩하기 때문에 실제 은행사이트도 정상 사용자와 해커를 구분하기 어렵다. 사용자가 2채널 인증을 사용할 경우, 거래 완료 직전에 사용자가 별도 채널로 확인 메시지를 받는다. 하지만 사용자가 피싱 사이트 여부를 구분하지 못했다면, 해당 2채널에서 거래를 승인하기 때문에 피싱 방지에 도움이 되지 못한다.

EV SSL 인증서의 경우, 가장 직접적으로 피싱/파밍 사이트 유무를 확인할 수 있는 방법이다. 사용자가 웹브라우저의 주소창을 확인하고 실제 은행 사이트인지 아닌지를 결정할 수 있다. 하지만 MIT/HARVARD의 조사 결과에 따르면, 대부분의 사용자들은 SSL 여부를 제대로 확인하지 않았고, SSL 아이콘 이미지, 주소창, 상태 바와 같은 다양한 보안 표기의 변화에도 제대로 반응하지 못했다[19].

OTP는 제한된 시간(대략 1분) 내에서만 사용가능한 임의의 비밀번호를 생성하기 때문에, 해커에게 노출되어도 비교적 안전하다고 알려져 있다. 하지만, 본 절에서 언급한 MITM 피싱 공격에서는 사용자가 입력한 OTP가 실시간으로 해커에 의해 은행 서버로 포워딩될 수 있다. 이 때문에 OTP의 유효 시간보다 더 짧은 시간에 해커가 사용자인 것처럼 실제 은행 사이트에 인증 받을 수 있다.

지정PC제의 경우에는 사용자 컴퓨터의 고유한 맥 주소를 이용하여 지정된 컴퓨터에서만 이체 서비스가 가

능하도록 서비스 하고 있다. 하지만 맥 주소는 악성코드로 쉽게 탈취 가능하고, 해커 컴퓨터가 사용자 컴퓨터와 동일한 맥 주소로 변경하기도 쉽다.

국내 주요 은행에서는 사용하고 있지 않지만, 해외에서 사용하는 블랙리스트 기반 피싱 공격을 탐지하는 방법도 있다. 알려진 피싱 사이트 주소를 블랙리스트 서버에 저장하여 피싱 사이트 주소에 접속하면, 서버에 등록된 피싱 사이트 주소와 비교하여 피싱 사이트 여부를 사용자에게 알려준다. 하지만 APWG의 보고서에 따르면 피싱 사이트는 개설된 지 평균 26시간 만에 폐쇄되기 때문에 블랙리스트 기반의 솔루션으로 피싱 공격을 탐지하기는 어렵다[6].

Ⅴ. 향후 연구 및 결론

본 논문에서는 온라인 피싱/파밍의 최근 동향에 대해서 알아봤고, 국내 금융기관들이 적용하고 있는 보안 솔루션들을 비교하고 각 솔루션들에 대해서 기술하였다. 그리고 각 보안 솔루션들의 한계점에 대해서 알아봤다. 이러한 보안 솔루션들의 한계를 극복하고 고도화된 피싱 기술에 대응하기 위한 솔루션은 아래 표4의 요구사항을 만족시켜야 한다[22].

'편의성' 항목은 사용자 컴퓨터에 설치하도록 강요하는 개인 방화벽, 키보드 보안, 백신 프로그램처럼 별도의 추가적인 작업 또는 하드웨어를 요구하지 않아야 한다는 것을 의미한다. 그리고 낮은 오/미탐률과 함께 피싱 사이트 여부를 빠르게 확인할 수 있는 '성능', 기존의 피싱/파밍 공격에 대응하고 MITM 피싱 공격과 같은 새로운 피싱 공격에도 유연하게 대처 가능한 '보안성'을 갖춘 피싱/파밍 대응 보안 솔루션이 국내 금융기관에 필요하다.

〈표 4〉 피싱 대응방안 요구사항

분류	요구사항
편의성	낮은 사용자 입력 횟수
	사용자에게 인지 작업 요청하지 않음(자동화)
	새로운 하드웨어 요구하지 않음
성능	빠른 탐지 시간
	낮은 오탐률
	낮은 미탐률
보안성	자체 프로토콜 안전성
	자체 보안
	기존 피싱/파밍 공격 대응
	새로운 피싱 공격에 유연하게 대처 가능

참 고 문 헌

[1] 한국은행, "세계1000대 은행과 우리나라 은행 보고서", http://news.mt.co.kr/mtview.php?no=2013070711394468885, 2013. 7.

[2] 한국은행, "2013년 1/4분기 국내 인터넷뱅킹서비스 이용현황", 2013. 5.

[3] 동아일보, "국내 스마트폰 사용자 수", http://it.donga.com/14733/, 2013. 6.

[4] 이데일리, "금융기관 피싱 피해 현황", http://www.edaily.co.kr/news/NewsRead.edy?SCD=JA21&DCD=A00102&newsid=02007366602870584, 2013. 7.

[5] 인터넷진흥원, "인터넷 침해사고 대응통계", 2013. 5.

[6] APWG, "Phishing Activity Trends Report 4th Quarter 2012", 2013. 4.

[7] 카스퍼스키 랩, "2011-2013 피싱 공격의 진화", 2013. 7.

[8] KBS, "'파밍' 수법으로 수십억 가로챈 금융사기단", http://news.kbs.co.kr/news/NewsView.do?SEARCH_NEWS_CODE=2689768&ref=D, 2013. 7.

[9] YTN, "가짜 은행 사이트, 사기 일당 검거", http://www.ytn.co.kr/_ln/0115_201307120024588324, 2013. 7.

[10] 미디어잇, "인터넷 뱅킹 '안심클릭', 결코 안심하면 안돼", http://www.it.co.kr/news/mediaitNewsView.php?nSeq=2381740, 2013. 6

[11] 전자신문, "계좌 · 암호 · 인증서 훔치는 악성코드 기승", http://www.etnews.com/news/computing/security/2775401_1477.html, 2013. 5.

[12] 머니투데이, "이번엔 KISA 사칭 이메일 '속지마세요'", http://news.mt.co.kr/mtview.php?no=2013040915413798159, 2013. 4.

[13] KISA 인터넷 침해대응 센터, “새로운 피싱 사기 방법, Spear phishing”, http://www.krcert.or.kr/kor/data/TrendView.jsp?p_bulletin_writing_sequence=1708, 2012. 12.
[14] ITWorld, “기업 사이버공격의 95%를 차지하는 스피어 피싱, 어ᄄᅠᇂ게 예방할 것인가”, http://www.itworld.co.kr/news/80682, 2013. 3.
[15] 보안닷컴, “공인인증서 탈취하는 악성코드 주의보”, http://www.boan.com/news/articleView.html?idxno=8092, 2013. 4.
[16] ZDNET, “금융 사기 대책 투팩터 보다 투채널 인증”, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130709081807, 2013. 7.
[17] 보안닷컴, “내 돈 빼간 신종 스미싱 사기단 검거”, http://www.boan.com/news/articleView.html?idxno=8069, 2013. 03.
[18] 동아일보, “더욱 교묘해진 스마트폰 사기 메시지(스미싱)”, http://it.donga.com/15376/?page=2, 2013. 7.
[19] 김형식, 허준호, 로스 안데르센, “On the Security of Internet Banking in South Korea”, University of OXFORD, 2010. 3.
[20] Haller, N., Metz, C., Nesser, P. and Straw, M. “A One-Time Password System”, IETF, RFC 2289, 1998.
[21] Bruce Schneier, “Two-Factor Authentication: Too Little, Too Late”, Communications of the ACM, 48권 4호, 135-136쪽. 2005.
[22] R. Dhamija, J. D. Tygar, M. Hearst, “Why Phishing Works”, in the proceeding of the Conference on Human Factors in Computing Systems(CHI 2006), 2006. 4.
[23] 김승현, 이성훈, 진승헌, “액티브 피싱 공격 및 대응방안 고찰”, ETRI 전자통신동향분석, 2013. 6.

김 승 현

2002년 2월 금오공과대학교 컴퓨터공학과 (학사)
2004년 2월 포항공과대학교 컴퓨터공학과 (석사)
2004년 1월~현재 한국전자통신 선임연구원

〈관심분야〉
ID 관리, 모바일 지불 결제, 정보보호

이 성 훈

2011년 8월 충주대학교 컴퓨터공학과 (학사)
2011년 9월~현재 과학기술연합대학원대학교 정보보호공학과 (석사)

〈관심분야〉
ID 관리, 온라인 피싱, 정보보호

진 승 헌

1993년 2월 숭실대학교 전자계산학과 (학사)
1995년 2월 숭실대학교 전자계산학과 (석사)
2004년 2월 충남대학교 전산학(정보보호) (박사)
1996년 4월 ㈜대우통신 종합연구소 연구원
1999년 5월 ㈜삼성전자 통신연구소 전임연구원
1999년 6월~현재 한국전자통신연구원 인증기술 연구실장

〈관심분야〉
정보보호(PKI, 인증/인가기술, 프라이버시 보호기술), 모바일 지불결제, 컴퓨터/네트워크 보안