韓國 컴퓨터情報學會 論文誌
第12卷 第2號, 2007. 5.

2007-12-2-2-2

Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구

박 대 우*, 서 정 만**

A Study of Information Leakage Prevention through Certified Authentication in Phishing, Vishing, SMiShing Attacks

Dea-Woo Park*, Jeong-Man Seo**

요 약

최근의 사이버 범죄 중 사기성 피싱, 파밍, 비싱, 스미싱 등을 이용한 금융범죄가 늘어가고 있다. 본 논문에서는 사회공학 기법과 VoIP를 이용하는 피싱, 비싱, 스미싱으로 정보의 유출과 침해가 얼마나 손쉽게 발생할 수 있는지 실험을 통해 체계적으로 연구한다. 해커가 피싱과 비싱 사이트를 제작하고 서버를 구축하여 피싱 메일 및 바이러스, 악성코드, 비싱, 스미싱 문자, 키로거 방지 S/W의 무력화 등을 통한 사용자의 정보침해 과정을 실험한다. 실험 결과에서 피싱과 비싱, 스미싱으로 인한 정보가 유출 및 침해됨을 확인하고, 방지 대책으로 공인인증서와 White List 및 공인인증마크, 플러그 인 프로그램 설치 등을 실험하여 보안이 됨을 증명한다. 본 논문의 피싱과 비싱 공격에 대한 기술적인 실험 및 방지대책은 정보침해의 피해를 줄이고, 유비쿼터스 정보보안을 위한 학문 ·기술적 발전에 기여할 것이다.

Abstract

The financial crime that used morale anger Phishing, Pharming, Vishing, SMiSing etc. will gain during recent cyber crimes. We are study systematically whether or not leakage of information and infringement can how easily occur to Phishing, Vishing, SMiSing using a social engineering technique and VoIP at these papers through experiment. A hacker makes Phishing, Vishing site, and test an information infringement process of a user through PiSing mail and a virus, a nasty code, Vishing, a SMiSing character, disarmament of Keylogger prevention S/W etc. as establish server. Information by Phishing, Vishing, SMiSing is infringed with leakage in the experiment results, and confirm, and test certified certificate and White List and a certified authentication mark, plug-in program installation etc. to prevention, and security becomes, and demonstrate. Technical experiment and prevention regarding Phishing of this paper and Vishing attack reduce the damage of information infringement, and be education for Ubiquitous information security will contribute in technical development.

▸ Keyword : Certificate, Phishing, SMiShing, Ubiquitous Security, Vishing

• 제1저자 : 박대우
• 접수일 : 2006.12.7, 심사일 : 2007.4.7, 심사완료일 : 2007. 5.10.
* 호서대학교 벤처전문대학원 교수, ** 한국재활복지대학 컴퓨터게임개발과 교수

Ⅰ. 서 론

유비쿼터스 네트워크(Ubiquitous Network) 기반으로 인터넷으로 연결된 업무와 생활방식이 변화하고 있다. 사이버 공간의 활성화는 시간과 공간의 제한을 극복한 정보 통신의 업무와 유비쿼터스 생활환경을 제공하고 있다.

이러한 작용에 수반되어 불건전 정보의 유통, 허위 정보 유포, 정보시스템 불법 침입과 가용자원의 파괴, 사생활 침해, 사이버 폭력, 지적 재산권 침해, 언어폭력, 사이버 중독 등 다양한 역기능이 나타나 사회적 불안감도 증대되고 있다. 특히 경제적 측면에서 전자상거래, 인터넷 뱅킹 등 개인과 사회의 경제에 직접적인 피해를 끼치는 침해 사고를 예방하고, 실시간으로 방지하기 위해서는 기술과 제도적인 보안 대응책이 연구되어 져야 한다.

유비쿼터스 사회의 조기 실현을 위한 준비로 국내에서는 u-IT839전략[1]을 국가정책으로 추진하고 있지만, 유비쿼터스 컴퓨팅을 통한 업무 및 생활환경에 미치는 부정적 측면의 증가세가 뚜렷하다. 한국정보보호진흥원(KISA)의 보고서에[2] 따르면 그림 1과 같이 국내 백신업체(안철수 연구소, 하우리)와 KISA에 신고된 웜·바이러스 신고건수는 2006년 9월 865건으로 전월 683건에 비하여 26.6%, 전년 동월 798건에 비해서는 8.4% 증가하였다. 또한 변종 웜·바이러스는 전월 대비 19.8%의 증가율을 보였다.

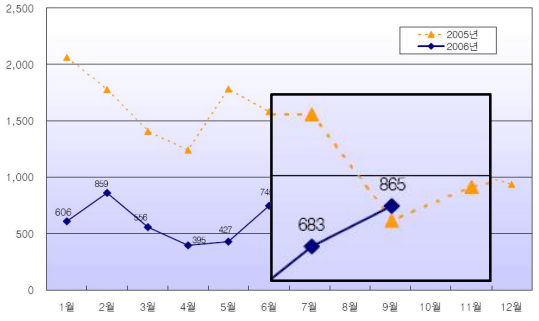

그림 1. 2005년~2006년 국내 웜·바이러스 신고건수
Fig. 1. Domestic 2005~2006, Worm and Virus Report Number of Cases

이러한 현실을 반영하듯 개인, 네트워크 시스템 관리자들은 컴퓨터 바이러스 백신 프로그램(Vaccine Program) 방화벽(Firewall), IDS(Intrusion Detection System), IPS(Intrusion Prevention System)등[3] 보안 시스템과 네트워크 보안 장비를 설치하여 사용자 및 네트워크 시스템의 중요 자원에 대한 피해를 예방하기 위해 보안을 강화하고 있다.

최근의 사이버 범죄 중 가장 큰 폭의 상승세를 보이고 있는 것이 사회공학(社會工學) 기법을 이용한 금융범죄이다. 이 기법은 인간의 깊은 신뢰를 바탕으로 하는 사람들의 상호작용을 속임으로써 정상적 정보보안 절차를 깨트리기 위한 비기술적 침입 수단의 하나로써 이용된다.

이러한 사회공학적 기법을 사용하는 금융범죄자들은 사기성 피싱(Phishing)과 파밍(Pharming) 메일, VoIP로 불특정 다수에게 전화를 걸어 개인정보를 빼내는 비싱(Vishing), 문자메시지를 이용한 스미싱(SMiShing) 등을 이용하여 자신들의 금전적 이득을 위해 많은 사용자에게 피해를 주고 있어 사회적 이슈화 되고 있는 실정이다.

VoIP 서비스[4]를 이용하는 비싱과 바이러스를 심어서 이용하는 스미싱이 있다[5]. 보안회사인 시만텍은 2006년 10대 보안 위협의 하나로 'VoIP 위협 증가'를 꼽았다[6].

이렇게 피싱과 비싱, 스미싱 등을 통한 금융범죄는 특별히 전문적 기술이 필요치 않으면서도 시중에 유포되어 손쉽게 구할 수 있는 컴퓨터 바이러스나 악성코드, 툴킷을 이용해 정보를 유출시켜 악용[7]할 수 있으며 그로 인하여 개인·사회적으로 경제적 손실을 야기시킬 수 있다는 데 문제가 있다.

본 논문에서는 해커가 피싱 사이트를 제작하고 서버를 구축하여 바이러스와 키로거 방지 S/W의 무력화를 통하여 사용자의 정보침해를 실험한다. 실험에서 피싱과 바이러스로 인한 정보가 유출되고 피싱과 VoIP 서비스를 이용하는 비싱과 스미싱 공격[8]에 이용됨을 확인한다.

피싱과 비싱 및 스미싱 공격에 대한 방어 대책으로 공인인증서를 이용하여 실시간으로 정보침해가 방지되는 대책을 수립할 것이다. 즉, 사용자가 피싱과 비싱 사이트에서 입력한 정보를 피싱 서버에 저장된 파일과 비교하여 정보가 유출되더라도, 화이트 리스트와 신뢰성있는 공인 인증서를 이용한 방지 대책이 작동하면서 피싱과 비싱 및 스미싱 공격이 무력화됨을 네트워크 실험을 통해 체계적으로 연구한다.

본 논문의 피싱과 비싱 및 스미싱 공격 실험을 통하여 최근 사회적으로 심각한 금융적인 피해를 일으키고 있는 피싱과 비싱, 스미싱에 대한 기술적인 대비 방안으로 정보침해의 피해를 줄이고, 금융감독원, 한국정보보호진흥원, 경찰청, 대검찰청 등의 기관에서 수행하는 유비쿼터스 정보보안을 위한 학문·기술적 발전에 기여하고자 한다.

II. 관련 연구

세계적으로 많은 피해를 끼쳤던 최근의 바이러스 및 악성코드를 이용한 피해 사례를 통해 금융사기 기법에 관하여 연구한다.

2.1. 세계적인 바이러스의 피해 사례

1) CIH

1998년 6월 대만에서 나타난 CIH는 전 세계 PC의 데이터를 파괴하여 약2천만~8천만 달러의 피해를 입혔다. 윈도우 95와 98, ME 실행 파일을 감염시켰으며 PC의 메모리에 잠복했다가 다른 실행 파일도 감염시켰다.

2) 멜리사(Melissa)

1999년 3월 26일 발생하였다. 모든 기업용 PC의 워드 매크로 스크립트 중 15~20%가 감염되었고 수 억 달러의 피해를 입었다. 멜리사는 전염 속도가 빨라서 마이크로소프트 아웃룩을 사용하던 인텔과 마이크로소프트 및 수많은 기업들이 피해를 입었다.

3) ILOVEYOU

2000년 5월3일에 처음 유포된 ILOVEYOU 바이러스는 레브레터나 러브 버그(Love Bug)로도 알려져 있으며 비주얼 베이직 스크립트 바이러스로, 연애편지로 위장해 메일로 발송된다. 'ILOVEYOU'라는 제목과 함께 Love-Lettet-For-You.TXT.vbs라는 첨부 파일이 포함되어 이메일로 전송되면 멜리사처럼 마이크로소프트 아웃룩 주소록을 타고 전파된다.

4) 코드 레드(Code Red)

2001년 7월 13일에 처음으로 네트워크 서버에서 발견된 코드 레드는 네트워크 서버나 인터넷을 통해 전파되는 바이러스다. 특히, 마이크로소프트의 인터넷 인포메이션 서버(IIS) 웹 서버에 구동하는 컴퓨터를 타깃으로 했기 때문에 치명적인 버그였다. 이 웜은 IIS 운영체제의 특정 취약점을 공략할 수 있었다.

바이러스 공격은 약 20일 동안, 미국 백악관의 웹 서버를 포함해 특정 IP 주소에 대한 DoS공격(Denial of Service attack)[9]을 실행했다. 일주일 만에 40만 대의 서버를 감염시켜 26억 달러 규모의 피해를 입혔으며, 백만 대의 컴퓨터를 감염시키는 전염성을 갖고 있다.

5) SQL 슬래머(Slammer)

2003년 1월 25일에 출현으로 알려진 SQL 슬래머는 과도한 인터넷 트래픽을 유발한다. 서버를 타깃으로 삼았으며 376바이트의 작은 패킷 하나로 임의의 IP 주소들을 생성하고 다시 전송함으로써 SQL 서버를 감염시켰다. SQL 슬래머는 단 10분만에 75,000대의 컴퓨터를 감염시켰으며 전세계 라우터에 임계치를 초과하는 과도한 트래픽[10]을 발생시켜 인터넷을 마비시켰으며 한국의 인터넷 접속이 12시간 동안 불통되는 사태를 초래했다.

6) 블래스터(Blaster)

2003년 8월 11일에 탐지된 블래스터는 네트워크와 인터넷 트래픽을 통해 윈도우 2000과 윈도우 XP의 취약점을 공격했으며, 활성화 될 경우, 시스템을 재 시동한다는 메시지가 뜨며 시스템을 종료하는 경우가 발생한다. 이 웜 바이러스는 수십만대의 PC를 감염시켜 20~100억 달러의 피해를 입힌 것으로 추산된다.

7) Sobig.F

소빅 웜 중에서 빠른 속도의 전파 능력이 특징이다. 8월 19일 출현한 지 24시간 동안 1백만 개의 복제판을 만들어 냈다. application.pif와 thank_you.pif 등의 이름이 붙은 이메일 첨부파일을 통해 호스트 컴퓨터를 감염시켰고, 이메일 주소록을 통해 전송되었고 백만 대 이상의 PC를 감염시킨 다음 자체적으로 비활성화 되었다.

8) 베이글(Bagle)

2004년 1월 18일에 등장 이메일 첨부파일을 통해 사용자의 시스템을 감염시킨 다음, 복제로 사용되는 이메일 주소를 위해 윈도우 파일을 검색한다. 감염된 시스템에서의 데이터 접근을 위해 원격지 사용자들과 애플리케이션에 의해 사용되는 TCP 포트에 대한 백 도어를 제공한다는 점에서 위험성이 크다. 이 웜은 자신의 이름을 알리고자 하는 해커에서 금전적인 이득을 취하려는 '범죄자'로 이동하는 멀웨어(Malware)의 활동을 알리는 '신호탄'이 되었다.

9) 마이둠(MyDoom)

2004년 1월 26일, "메일 송수신 오류(Mail Transaction Failed)"라는 제목으로 이메일 에러 메시지처럼 보이게 위장하면서 첨부파일을 통해 전송된다. 첨부파일을 클릭하면서 주소록의 이메일 주소로 웜이 전파되고 사용자의 카자(Kazza) P2P 네트워킹 계정의 공유 폴더를 통해 전파될 수도 있다.

10) 사세르(Sasser)

2004년 4월 30일 활동을 시작하여 일부 프랑스의 뉴스 방송국의 위성 통신을 중단시키고 델타 항공의 일부 운항을 취소시켰으며, 전 세계 기업들의 시스템을 중단시키는 파괴력을 지녔다. 사세르는 윈도우 2000과 윈도우 XP 시스템이 갖고 있는 보안의 취약점을 공략하여 보안이 취약한 다른 시스템을 찾아낸 후 자가 복제를 계속한다.

2.2. 최근의 금융사기 기법

1) 피싱

피싱이란 개인정보(Private Data)와 낚시(Fishing)의 합성어로 유명업체인 은행, 증권사, 포털 등의 위장 홈페이지인 복사본을 만든 뒤, 불특정 다수의 이메일 사용자에게 메일을 발송하여 위장된 홈페이지로 접속하도록 현혹하여 개인정보를 빼내는 행위를 의미한다. 주요 특징은 1.한 화면에서 공인인증서 비밀번호, 계좌비밀번호, 보안카드 비밀번호 등 개인정보를 동시에 입력하도록 요구한다. 2. 이체 거래 시 자신의 출금계좌번호를 이용자가 직접 입력하도록 요구하고 있다. 3. 로그인 절차 (ID/Password 또는 공인인증서 입력) 없이 바로 은행주소만 치면 화면이 나타난다. 4. 인터넷뱅킹에서는 보안카드 비밀번호 2자리를 2회 입력하도록 요구하지만, 피싱사이트는 그 이상의 자릿수와 횟수를 입력하도록 요구한다. 5.공인인증서 비밀번호를 화면에서 직접 입력하도록 한다. 6.평소 본인이 거래하는 은행의 인터넷뱅킹 사이트와 화면 구성이 약간 다르다.

결과적으로 피싱의 발생은 피싱 메일을 발송하고 수신자가 이메일 내용에 현혹되어 링크되어 있는 사이트를 클릭하여 위장사이트에서 개인정보나 금융정보를 입력함으로써 정보침해가 발생하며, 입력된 정보를 이용해 금융사기 등의 행위를 함으로써 2차적 범죄행위가 성립된다[11].

2) 파밍

파밍이란 그림 2처럼 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 DNS(Domain Name System) 이름을 속여서 IP주소를 변경하여 위장사이트를 생성하고, 사용자에게 스팸메일을 발송함으로써 의심 없이 개인 ID, 패스워드, 계좌정보 등을 노출하게 되는 피싱의 변형된 인터넷 사기 기법이다. DNS주소 자체를 변경하기 때문에 피싱보다 이용자가 속아 넘어갈 확률이 더 높다.

피해사례를 보면 2007년 이메일로 대학의 추가합격 소식을 전달하고, 이메일을 열면 해당 학교 사이트로 자동 연결하면서 사용자는 합격 사실을 확인했습니다. 그리고

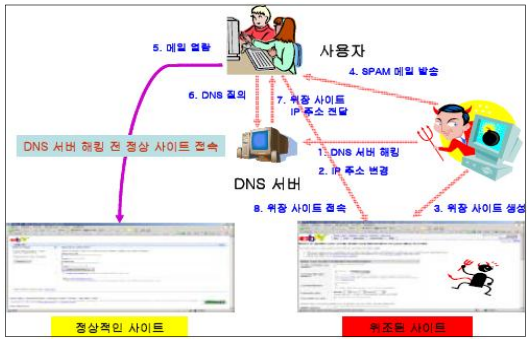

그림 2. 파밍 공격 절차
Fig. 2. PaMing Attack Procedures

정해진 날까지 등록금 4백 9십만원을 입금하라는 휴대전화 문자를 세 차례 받았습니다. 합격 소식을 기다리는 학생과 학부모의 절박한 심정을 이용한 사기입니다[12].

3) 비싱

비싱이란 VoIP기능을 이용하여 개인정보를 빼내는 신종 사기수법이다. 종래의 피싱 범죄자들이 E-Mail을 이용한 것과 달리 비싱은 VoIP망을 통한 불특정 다수에게 자동 녹음된 음성메시지를 보내 은행계좌에 문제가 있다고 경고하는 방식으로 이용자들을 유인한다. 계좌 문제를 해결하라면서 전화번호를 알려주고 개인이 전화를 걸면 계좌번호나 신용카드 번호, 비밀번호를 입력하게 하여 정보를 빼내어 금융범죄에 악용한다.

4) 스미싱

스미싱이란 불특정 다수에게 핸드폰 문자메시지를 이용, 핸드폰에서 트로이목마를 주입하는 새 해킹 기법[13]이다. 맥아피가 스미싱(SMiShing: SMS + Phishing)이라고 이름을 정한 이 기법을 사용하는 해커는 핸드폰 사용자에게 웹사이트 링크를 포함한 문자메시지를 보낸다. 해커는 휴대폰 사용자가 웹사이트에 접속하면 트로이목마를 주입해 인터넷 사용이 가능한 휴대폰을 통제할 수 있게 된다.

실례로 아이스랜드와 호주에 사는 많은 휴대폰 사용자들에게 SMS가 도착했다. '당신은 우리 데이트 사이트에 회원가입을 했습니다. 등록을 취소하지 않으면 하루에 2달러가 부과 됩니다'라는 내용으로 여기에서 핸드폰 사용자들은 가입 취소를 위해 부득이하게 그 사이트에 접속하게 되며, 접속하는 순간 바로 트로이목마에 감염된다.

VBS/Eliles.A.라는 웜의 분석결과는 아주 단순했으며 핸드폰이 실제로 사용된 통화내역 안에서만 전화번호를 생성했다.

III. 피싱, 비싱, 스미싱에 의한 정보의 침해 실험

사회공학 기법을 이용한 피싱과 비싱, 스미싱은 컴퓨터 바이러스 및 악성코드를 사용자에게 감염시키는데 탁월한 효과를 보인다. 본 논문은 피싱과 비싱 및 스미싱에 의해 정보가 얼마나 손쉽게 유출될 수 있는지 실험을 통하여 해커가 어떠한 과정으로 정보침해를 가능케 하는지 정보침해 과정을 설계한다.

3.1. 실험 환경 구축

본 논문에서 실험할 피싱과 비싱 및 스미싱을 이용한 정보침해 및 키로거에 의한 특정 서버로의 정보침해[14] 과정을 실험하기 위해 실험실의 네트워크에 일반적 PC의 사용환경을 구축한다.

1) 시스템 사양

❖ **Attacker 시스템 사양**

Microsoft Windows XP Professional(SP2) (OS), Intel Pentium(R) 4 3.00GHz(CPU), 512M RAM(Memory), 320GB(HDD)

❖ **Target(Victim) 시스템 사양**

Microsoft Windows XP Home Edition(SP2) (OS), Intel Pentium(R) 4 3.00GHz(CPU), 512M RAM(Memory), 250GB(HDD)

2) Network 구성

실험을 위해 간단한 네트워크를 구성한다. 피싱과 비싱 및 스미싱에 의한 정보침해는 일반적 상황에서 발생함으로 공인IP를 사용하는 네트워크로 구성한다. 따라서 본 논문에서 피싱과 비싱 및 스미싱을 위한 네트워크는 피싱과 비싱에 사용할 서버와 모든 사용자의 PC 및 단말기로 구성된다.

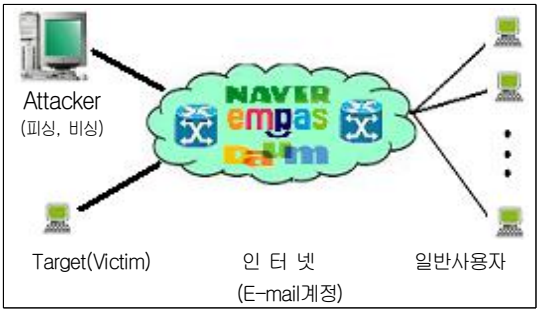

그림 3. 실험을 위한 네트워크 구성
Fig. 3. Network Configuration for Experiment

3) 피싱, 비싱, 스미싱 서버구축

본 논문에서는 실험의 특성상 사회 경제적 파급효과가 크므로 실제로 특정 도메인 네임을 사용하지 않고, 실험실 IP Address를 사용 할 것이다. 사용자가 ID와 비밀번호를 입력하고 Enter를 누르거나 확인버튼을 클릭하는 순간 사용자가 입력한 내용이 피싱 서버의 'c:\tomcat\webapps\ROOT\ajax\log\login.txt'에 저장된다.

피싱 서버의 시스템 사양과 서버기능을 하기위한 설치프로그램은 아래와 같다.

- OS : Microsoft Windows XP Professional(SP2)
- CPU : Intel Pentium(R) 4 3.00GHz(CPU)
- Memory : 512M RAM
- HDD : 250GB
- 개발환경 : J2SE Development Kit 5.0
- 웹서버 : Apache_Tomcat_5.5.17

4) 위장사이트 제작

실험에 사용할 위장사이트는 국내 최대 은행인 국민은행을 모델로 하였으며 실제 그림 4처럼 국민은행 홈페이지 http://www.kbstar.com에서 제공되는 로그인 페이지를 유사 웹페이지로 변조하여 홈페이지의 정상적 초기화면에 접속되기 전에 위장사이트를 경유하도록 제작한다.

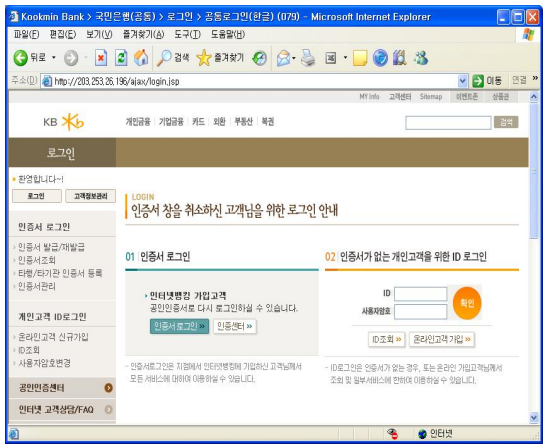

그림 4. 국민은행 위장사이트
Fig. 4. Kookmin Bank Camouflage Site

3.2. 피싱, 비싱, 스미싱에 의한 정보침해 과정

해커는 사용자에게 정상을 가장한 피싱 메일을 발송하고 위장사이트로 접속을 유도하여 사용자가 입력한 정보가 피싱 서버에 log파일로 저장되는 과정을 설계한다.

1) 피싱 메일과 VoIP 비싱, 스미싱에 의한 정보침해

가. 해커는 사용자에게 사회공학적 기법을 이용하여 위장사이트로 링크될 수 있도록 '안녕하세요 고객님, 국민은행입니다. 시스템 업그레이드 과정에서 고객님의 공인인증서에 문제가 발생하여 금융거래시에 인증서 사용이 제한적일 수 있습니다. 이 문제를 해결하려면 국민은행 홈페이지(http://위장사이트 주소)를 방문하여 주시기 바랍니다. 불편을 드려 죄송합니다.'의 내용으로 정상적 E-mail과 VoIP 및 SMS를 발송한다.

나. 사용자는 자신의 E-Mail과 VoIP 및 SMS를 보고, 해커가 발송한 사회공학적 사기 내용에 현혹되어 국민은행 홈페이지(http://위장사이트 주소) 링크를 클릭하여 변조된 국민은행 위장사이트에 접속한다.

다. 사용자는 국민은행 위장사이트의 로그인 페이지에서 우측에 위치한 ID와 사용자암호에 자신의 정보를 입력한 후 확인버튼을 클릭한다.

라. 사용자가 입력한 ID와 사용자암호는 해커가 설치한 피싱 서버의 'c:\tomcat\webapps\ROOT\ajax\log' 폴더에 'login.txt' 파일로 저장된다.

마. 해커는 저장된 'login.txt'를 윈도우의 메모장으로 열기하여 사용자가 입력한 국민은행의 ID와 사용자암호를 습득한다.

2) 피싱 메일 및 스미싱 바이러스에 의한 정보침해

가. 해커는 사용자에게 정상적인 E-mail을 가장한 피싱 메일에 키로거 기능이 있는 바이러스 또는 악성코드를 첨부파일로 발송한다.

나. 사용자는 자신의 E-Mail 계정에 접속하여 해커가 발송한 피싱 메일을 확인하고 첨부 파일을 다운받아 실행한다.

다. 사용자가 실행한 바이러스 파일은 사용자 PC에서 백그라운드로 실행되어 사용자의 키보드 타이핑을 *.txt파일로 저장하고 주기적으로 해커의 시스템에 전송한다.

라. 해커는 사용자 시스템에서 전송된 *.txt 파일을 열어 사용자 정보를 유용한다.

3) 키로거 방지 S/W의 무력화를 통한 정보침해

2)의 실험에서 키로거 방지 S/W[15]가 설치되어 있는 컴퓨터의 경우 정보침해가 차단되므로 툴을 이용하여 키로거 방지 S/W를 무력화시킨 후 사용자 정보를 해커의 시스템으로 전송하여 해커가 사용자 정보를 취득하는 과정을 설계한다. 덧붙여 실험에 사용한 바이러스, 악성코드, 키로거 방지 S/W 등은 일반사용자의 모방 가능성이 높아 밝히지 않기로 한다.

가. 해커는 사용자에게 정상적인 E-mail로 가장한 피싱 메일에 바이러스 또는 악성코드와 키로거 방지 S/W 무력화 툴을 첨부하여 발송한다.

나. 사용자는 자신의 E-Mail 계정에 접속하여 해커가 발송한 피싱 메일을 확인하고 첨부된 정상을 가장한 파일을 다운받아 실행한다.

다. 실행된 바이러스, 악성코드는 백그라운드로 실행되어 키로거 기능을 수행하며 nProtect와 같은 키로거 방지 S/W가 실행되고 있음이 감지되면 무력화 시킨 후 해커의 시스템으로 사용자가 입력한 정보를 전송한다.

라. 해커는 사용자 시스템으로부터 전송된 파일을 열어 사용자가 입력한 개인정보를 확인 후 유용한다.

3.3. 피싱, 비싱, 스미싱 정보침해 과정 검증

본 논문에서 실험의 검증은 위 3.2. 피싱에 의한 정보침해 과정 중 1) 피싱 메일에 의한 정보침해 부분을 보일 것이다. 2)와 3)의 검증은 개인정보보안에 있어 영향을 끼칠 수 있고 일반 사용자들에 의한 모방이 우려되어 사회적 물의를 야기할 수 있는바, 본 논문에서는 사용된 바이러스, 악성코드 등과 검증과정은 생략하기로 한다.

1) 피싱 메일과 VoIP 비싱에 의한 정보침해

해커는 국민은행에서 보낸 것처럼 사용자에게 피싱 메일을 발송하고 사용자는 자신의 E-Mail 계정에 접속하여 해커가 발송한 피싱 메일을 확인한 후 국민은행 위장사이트인 http://위장사이트 주소로 접속하여 자신의 ID와 사용자암호를 그림 5와 같이 입력한다.

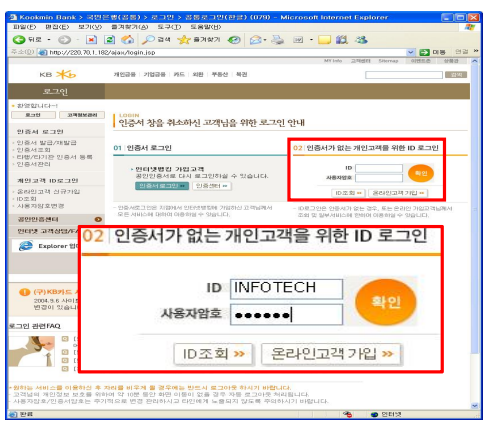

그림 5. 사용자의 개인정보 입력화면
Fig. 5. Personal Information Input Screen of a User

사용자가 입력한 국민은행의 ID와 사용자암호는 피싱 서버의 'c:\tomcat\webapps\ROOT\ajax\log 폴더에 'login.txt'파일로 생성되므로 윈도우 탐색기를 사용하여 폴더에 저장된 'login.txt'를 열어 사용자가 입력한 ID와 사용자암호가 'login.txt'에 저장된 ID와 사용자암호가 동일한지 확인하여 정보침해를 증명한다.

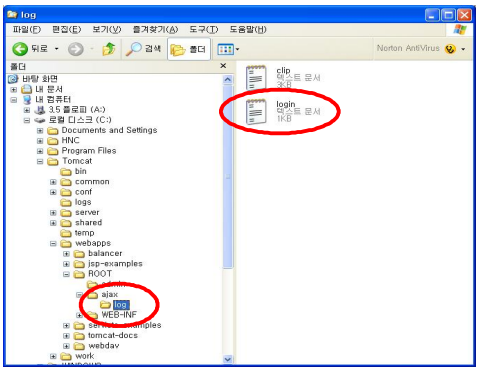

그림 6. 피싱 서버의 login.txt 생성
Fig. 6. Login.txt of PiSing Server generation

그림 5와 그림 6에서 보듯이 사용자가 피싱 사이트인 국민은행 위장사이트에서 입력한 ID와 사용자암호는 INFOTECH, 123456이었으며, 이 내용은 피싱 서버 'c:\tomcat\webapps\ROOT\ajax\log 폴더의 'login.txt' 파일에 저장되었음을 확인할 수 있다. 또한 저장된 정보가 사용자가 입력한 정보와 동일한지 확인하기 위해 그림 7과 같이 'login.txt' 파일을 열어 비교하니 입력된 ID와 사용자암호의 내용이 동일함에 따라서 사용자 정보가 유출되었음을 증명하였다.

그림 7. login.txt 파일의 내용
Fig. 7. Login.txt Contents of a File

2) 피싱 메일 및 스미싱 바이러스를 이용한 정보침해

해커는 사용자에게 정상적 E-Mail로 가장한 피싱 메일을 발송한다. 첨부파일은 키로거 기능을 가진 바이러스를 사용한다. 사용자는 자신의 E-Mail 계정에 접속하여 내용을 확인한 후 첨부된 바이러스를 다운로드하여 실행한다. 실행된 바이러스는 키로거 기능으로 작동하며 해커의 시스템에 사용자가 입력하는 개인정보를 전송한다. 해커의 시스템으로 전송된 파일을 열어 사용자가 입력한 내용과 비교하여 동일함을 확인함으로써 정보침해가 되었음을 증명한다.

3) 키로거 방지 S/W 무력화를 통한 정보침해 검증

피싱 메일 및 바이러스를 이용한 정보 침해와 동일한 과정으로 해커는 사용자에게 키로거 방지 S/W 무력화 기능을 탑재한 바이러스나 악성코드를 피싱 메일에 첨부하여 발송한다. 사용자는 메일 확인 후 첨부파일을 다운로드하여 실행하고 파일은 백그라운드로 동작한다. 사용자의 시스템에 nProtect처럼 키로거 방지 S/W가 작동하는 상태일 경우 실행중인 바이러스와 악성코드는 키로거 방지 S/W를 무력화 시키고 해커의 시스템으로 사용자의 개인정보를 전송한다. 개인정보의 유출을 확인하기 위해 해커의 시스템에 저장된 파일을 열고 사용자가 입력한 내용과 비교하여 동일한 내용임을 확인하는 것으로 키로거 방지 S/W 무력화를 통한 정보침해를 증명한다.

실제로 키로거 기능을 가진 Bot 바이러스의 변종인 rBot을 이용하여 nProtect가 동작중인 시스템에서 실험해 본 결과 nProtect가 동작중임에도 불구하고 사용자가 입력한 정보를 본인 모르게 공격자의 시스템에 전송되었고 내용의 동일성을 확인할 수 있었다.

Ⅳ. 피싱, 비싱, 스미싱 공격에 대한 정보침해 방지 방안

3.2.에서 제시한 피싱에 의한 정보침해 과정을 증명하기 위하여 3.3.의 실험을 통해 정보침해가 손쉽게 이루어 질 수 있음을 증명하였다. 따라서 이에 대한 일반적 피싱에 의한 정보침해 예방 및 방지 방안을 4.1.과 4.2.에서 제시한다.

4.1. 정보침해 예방 방안

3.의 실험결과 정보침해는 전문적 지식 및 기술보다 사회공학적 방법에 의해 이루어지므로 사용자의 각별한 주의가 선행되어야 한다.

이용자들이 인터넷뱅킹 사고를 예방하기 위해서는 다음과 같은 안전수칙을 준수해야 한다.

- 윈도 보안 패치 및 바이러스 백신 프로그램의 정기 업데이트를 통한 최신 버전 유지.

- 의심스러운 이메일 열람 금지.
- PC방 등 공공장소에서 금융거래 자제.
- P2P 등 공개 소프트웨어 설치 자제.
- 공인인증서 별도 저장 매체에 저장 사용.
- 개인 이용자 스스로가 사기성 이벤트 등에 현혹되어 개인정보를 제공하는 일이 없도록 주의.
- 메일, 게시판에 링크된 사이트에 개인정보 입력에 주의
- 무분별한 인터넷 참여 및 회원가입은 지양.
- 비밀번호를 서로 다르게 설정하여 주기적으로 변경.
- 파일을 다운 시 공인된 사이트에서만 다운로드.
- 인터넷 공개자료실이나 파일공유(P2P)등을 통해 다운로드 받은 파일은 백신프로그램으로 항상 검사하고 치료.
- 공인인증마크를 확인한 후 사이트를 이용.
- 피싱이 의심된다면 관련 기관으로 신고.

4.2. 공인인증을 통한 실시간 정보침해 방지방안

현재 우리나라는 KISA가 지정한 6개(SignGATE, SignKorea, Yessign NCAsign, CrossCert, Tradesign)의 공인인증기관에서 개인 및 사이트에 대한 공인인증서를 발급하고 발급받은 개인과 사이트는 전자상거래, 공공기관, 금융기관 등에서 활용하고 있다.

그러나 사용자는 자신이 접속한 사이트가 공인된 사이트인지 확인하기 위해 별도의 시간과 노력으로 찾아서 확인해야 하는 번거로움이 있다.

따라서 본 논문에서 제안하는 첫 번째 대책은 아래 그림 9와 같이 공인 인증기관으로부터 공인인증서를 받은 사이트 목록을 사용자가 발급받는 공인인증서에 White List를 포함하여 사용자가 접속한 사이트로부터 인증을 받는 것과 동시에 사이트도 사용자에게 인증을 받는 것이다.

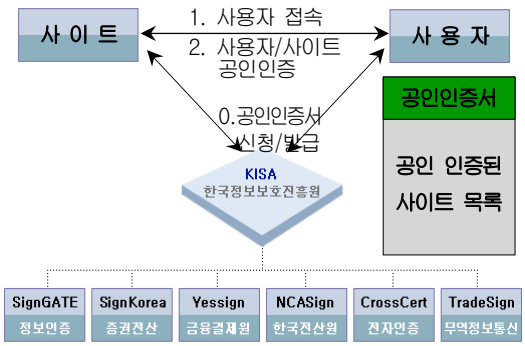

그림 9. 공인인증 사이트 확인을 위한 데이터 흐름도(1)
Fig. 9. Data Flow Chart for Certified Authentication Site Confirmation (1).

단지, 공인인증 사이트가 증가 할 경우 사용자의 공인 인증서 용량 크기가 증가하여 용량에 제한이 따를 수는 있으나 현재의 저장매체 즉, 하드디스크나 USB 메모리 등의 용량을 감안하더라도 충분히 가능하다.

그림 10. 개인 공인인증서
Fig. 10. Personal Certified Certificate

현재 사용하고 있는 일반적인 개인 공인인증서의 크기는 그림 10에서 보듯 2KB 정도임을 알 수 있다.

둘째 대책은, 그림 11에서 보듯 공인인증 최상위 기관인 KISA와 6개의 공인인증 지정기관이 공동의 데이터베이스를 운용함으로서 공인된 인증 사이트의 목록을 공유한다. 사용자가 사이트에 접속하여 사용자인증 과정을 수행하는 동안 사용자는 공인인증 기관으로 접속한 사이트의 공인인증 확인을 요청하고 공인 인증기관은 사용자에게 사이트의 인증 확인사항을 통보하여 사용자로 하여금 사이트

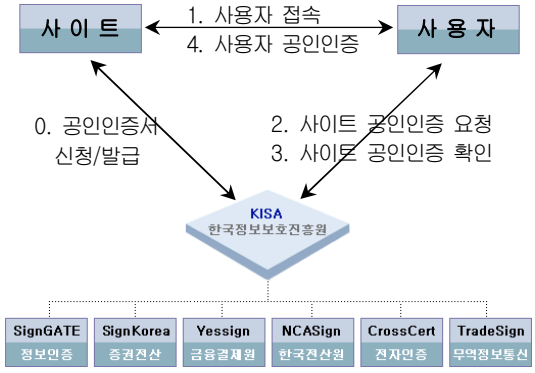

그림 11. 공인인증 사이트 확인을 위한 데이터 흐름도(2)
Fig. 11. Data Flow Chart for Certified Authentication Site Confirmation (2).

접속 가·부에 대한 기준을 제시한다.

셋째, 위와 유사한 방법으로 공인인증 최상위 기관인 KISA와 6개의 공인인증 지정기관이 공인된 인증 사이트의 목록을 공유한다. 그림 12처럼 사용자가 Internet Explorer 실행 후 주소창에 도메인 네임을 입력할 때와 링크를 통한 접속 시 링크의 도메인 네임 부분에 대한 공인인증을 확인할 수 있는 Internet Explorer 자체에 코드를 내장시키거나 플러그인 프로그램을 추가 설치함으로서 정보침해를 방지한다.

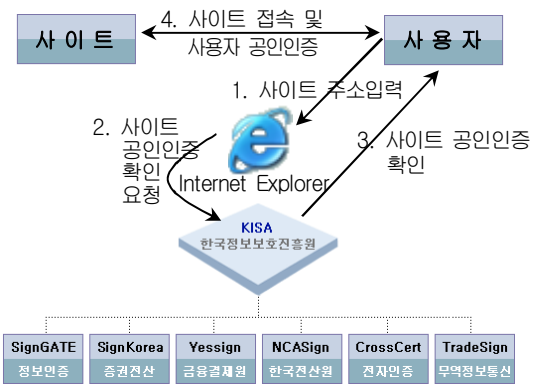

그림 12. 공인인증 사이트 확인을 위한 데이터 흐름도(3)
Fig. 12. Data Flow Fhart for Certified Authentication Site Confirmation (3).

V. 결론

본 논문은 피싱과 비싱 및 스미싱으로 인한 사회적 문제가 증가함에 따라 인터넷을 통한 피싱과 비싱 및 스미싱에 의한 정보침해 연구를 통해 전문적 지식보다 사회공학적 기법을 이용해 손쉽게 발생함을 실험하였다.

실험에서 해커는 단순히 사회공학 기법을 이용하여 국민은행에서 발송한 정상적인 E-Mail로 가장한 후 사용자가 메일 확인 후 문제의 해결을 위해 링크를 클릭하면 국민은행으로 위장한 피싱 사이트로 연결된다. 또한 VoIP 서비스를 이용하여 비싱 사이트로 연결되도록 하였다. 사용자가 입력한 정보는 해커의 시스템에 'login.txt' 파일로 저장되고 저장된 파일을 확인하여 사용자가 입력한 내용과 일치함을 보였다.

정보보안의 방안으로 본 논문은 피싱과 비싱 및 스미싱에 의한 사이버 범죄의 예방법을 제시하였다. 첫째, 개인 이용자 스스로가 피싱 메일이나 사기성 이벤트 등에 현혹되어 개인정보를 제공하는 일이 없도록 주의한다. 둘째, 윈도우즈 업데이트와 백신프로그램은 필수적으로 설치하여 혹시 모를 정보침해를 예방한다. 셋째, 파일을 다운받을 때에는 신뢰할 수 있는 공인된 사이트에서만 다운로드한다. 넷째, 공인인증 사이트의 경우 공인인증마크가 있으므로 접속자는 공인인증마크를 클릭하여 반드시 해당 정보를 확인한 후 사이트를 이용한다. 다섯째, 피싱이나 비싱 및 스미싱이 의심되면 관련 기관으로 신고한다.

정보보안 대책으로 공인인증을 통한 세 가지의 정보침해 방지방안을 제시하였다. 첫째는 공인인증 사이트의 확인을 위해 개인의 공인인증서에 공인인증 사이트 목록인 White List를 포함하는 것이고, 둘째는 사용자가 사이트 접속시 개인 공인인증을 받는 동시에 공인인증기관으로 사이트에 대한 인증을 요청하여 확인 후 접속하는 것이며, 마지막으로 Internet Explorer 자체에 코드를 내장하거나 플러그인 프로그램을 추가 설치함으로써 사용자가 주소창에 사이트의 주소를 입력 또는 링크를 클릭했을 때 KISA로 사이트의 공인인증 유무를 자동으로 확인 후 사용자에게 인지시키는 방법이다.

유비쿼터스 시대의 비대면 금융거래는 공인인증을 통해 업무를 처리하는 것이 바람직하다. 즉, 자신이 어디에 있든지, 무엇을 하든지 공인인증기관에 의한 공인 인증을 통할 경우 자기 자신의 존재를 신뢰 할 수 있다. 이런 의미에서 본 논문은 현재의 유비쿼터스 초기사회에서 일어나는 피싱과 비싱에 의한 정보침해 공격에 대한 실험과 공인 인증을 이용한 보안이 얼마나 중요한지 알아보는데 큰 의미가 있겠다.

향후 연구로는 앞에서 제시된 피싱, 비싱, 스미싱에 의한 정보침해 예방법과 제안한 3가지 방지대책을 실생활에서 활용할 수 있도록 개인의 프라이버시를 침해하지 않으면서도 좀 더 편리하고 익명성이 보장된 유비쿼터스 시스템을 활용하는 방안을 제안하고 강구해야 할 것이다.

참고문헌

[1] 정보통신부, 2006년 연두업무보고 및 IT839 전략 http://www.mic.go.kr/html/ebook/report_2006/it839/it839/default1.html. 2006. 7.

[2] 한국정보보호진흥원, 2006년 9월 해킹바이러스 통계 -KrCERT. 2006. 10.

[3] 박대우, 임승린. "해커의 공격에 대한 지능적 연계 침입 방지시스템의 연구." 한국컴퓨터정보학회논문지, 제11권 제2호, pp44-50, 2006. 5. 31.

[4] 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, pp155-164, 2006. 9. 30.

[5] NIST Draft. "Security Consideration for Voice

over IP systems." April 2004.
〔6〕 SYMANTEC. http://www.symantec.com. 2006.
〔7〕 SBS 뉴스, 2007.2.26 22:03
〔8〕 Deawoo Park. "A study about dynamic intelligent network security systems to decrease by malicious traffic". International Journal of Computer Science and Network Security, V.6, N.9B. pp 193-199. Sep 2006.
〔9〕 Thomas Poter 외 7인. "Practical VoIP Security," SYNGRESS. 2006.
〔10〕 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.
〔11〕 Deawoo Park. "Formal Network Designs for Critical Network Security Systems." International Journal of Computer Science and Network Security, Vol. 6 No. 4, pp 172-178. 2006.04.30.
〔12〕 Kanellis, P., Kiountouzis, E., Kolokotronis, N.,& Martakos, D. (Eds.). "Digital crime and forensic science in cyberspace". Journal of digital forensic practice. Hershey: Idea Group. 2006.
〔13〕 Peter Szor. "COMPUTER VIRUS RESEARCH AND DEFENSE." Addison-Wesley, May 2005.
〔14〕 Luoma, V. "Forensics and electronic discovery: The new management challenge". Computers & Security, 25(2), 91-96. 2006.
〔15〕 보안위협 DB 검색, 최신 보안위협 정보. http://info.ahnlab.com/securityinfo/virus_search.jsp?svccode=aa1001&contentscode=ad001. 2006.11.

저 자 소 개

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

서 정 만

2003년 충북대학교 컴퓨터공학과 (공학박사)
2002년~현재 한국재활복지 대학 컴퓨터게임개발과 교수
〈관심분야〉 데이터베이스, 게임프로그래밍, 실시간처리