ETRI

2013
Electronics and
Telecommunications
Trends

사이버 보안 기술 특집

액티브 피싱 공격 및 대응방안 고찰

Active Phishing Attack and its Countermeasures

Ⅰ. 서론
Ⅱ. 액티브 피싱
Ⅲ. 기존 대응방안 고찰
Ⅳ. 대응방안의 요구사항
Ⅴ. 결론

김승현 (S.H. Kim) 인증기술연구실 선임연구원
이성훈 (S.H. Lee) 인증기술연구실 UST 연구생
진승헌 (S.H. Jin) 인증기술연구실 실장

인터넷을 기반으로 하는 서비스가 활성화됨에 따라, 불순한 목적으로 악용하는 사례 또한 증가하고 있다. 특히 피싱 공격은 사회적인 문제로까지 확대되고 있으며, 대응방안 또한 대국민 교육 차원에서 전달되고 있다. 하지만, 새롭게 등장하는 액티브 피싱 공격은 기존의 대응방안으로는 해결할 수 없으며, 여러 보안 기술을 사용하더라도 해결할 수 없다는 점에서 심각하다. 본고는 액티브 피싱에 대한 소개와 함께, 기존의 대응방안과 여러 보안 기술들의 한계점을 제시한다. 그리고 액티브 피싱을 해결하기 위해 필요한 기술의 요구사항을 고찰한다.

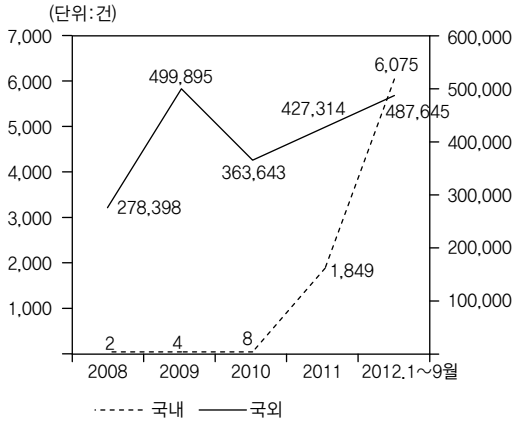
Ⅰ. 서론

인터넷 환경은 우리의 삶에 많은 변화를 주었다. 오프라인 매장에 가서 쇼핑을 하는 대신에 온라인 쇼핑몰을 이용하고, 오프라인 은행 지점에 가는 대신에 인터넷 뱅킹을 이용하여 컴퓨터와 인터넷이 있는 곳이라면 언제 어디서라도 편하게 생활할 수 있게 됐다. 인터넷을 통한 금융 거래의 경우, 2012년 기준으로 인터넷 뱅킹 등록 고객 수는 8,643만 명 정도이고, 하루 평균 인터넷 뱅킹 금액은 33.2조 원 수준으로 전체 금융 거래의 33.9%를 차지할 정도로 활성화되었다[1].

그러나 인터넷 환경이 활성화됨에 따라, 불순한 목적으로 악용하는 사례 또한 증가하고 있다. 대표적인 사례로 피싱(phishing) 공격이 있는데, 이는 개인의 중요한 정보를 부정하게 얻으려는 공격시도를 총칭한다. 피싱 공격은 1996년에 미국의 AOL사의 신용도가 높은 사용자의 계정을 도용한 해커에서 그 유래를 찾을 수 있다[2]. 현재는 사회공학적 방법과 기술적 은닉기법을 이용해서 민감한 개인정보, 금융계정 정보를 절도하는 신종 금융사기 수법을 피싱이라고 지칭하고 있다.

국내의 경우에는 〈표 1〉과 같이 2008년에 첫 피해가 발생한 이후에 2011년부터 본격적으로 피싱 사이트 피해가 발생하기 시작하였다[2]. 특히 국내의 피싱 공격은 게임머니를 탈취하기 위한 공격에서 최근에는 금융권을 대상으로 개인정보 및 금융거래정보 입력을 유도하는 공격으로 급격히 이동하고 있다.

〈표 1〉 국내 피싱 사이트 피해 현황



〈자료〉: 인터넷진흥원(국내)[2], APWG 2012 3분기 보고서(국외)[3]

국외의 경우, 〈표 1〉과 같이[3] 2009년 이후에 피싱 공격이 주춤한 것을 볼 수 있는데, 일부 해커들이 사용자를 피싱 사이트로 유도하는 방법에서 벗어나 직접적으로 사용자에게 영향을 미치는 악성코드를 제작했기 때문이다. 하지만 2010년 이후 다시 피싱 사이트가 증가하면서, 전통적인 피싱 공격은 계속 지속될 것으로 예상된다. 국외의 피싱 공격 또한 2/3는 금융/지불 서비스를 목표로 하고 있다(34%: 금융 서비스, 32%: 지불 서비스).

전통적인 피싱 공격 이외에도 파밍(pharming), 스미싱(smishing) 등 교묘한 신종 피싱 공격도 발생하고 있다. 파밍은 DNS(Domain Name System)를 조작하거나 악성코드를 이용하여 접속 주소를 변조하는 공격으로, 정상 홈페이지 주소를 입력하여도 피싱 사이트로 유도되어 금융거래정보 등이 탈취된다. 스미싱은 문자 메시지를 이용한 새로운 휴대폰 해킹 기법으로, 웹 사이트 링크가 포함된 문자 메시지를 보내 휴대폰 사용자가 결제 서비스 링크를 클릭하거나 악성코드가 내장된 애플리케이션을 설치하게 만들어 개인금융정보를 빼내거나 소액결제를 하게 하는 공격이다.

기존의 피싱/파밍 공격에 대응하는 방안으로 어떤 경우라도 보안카드 번호 전체를 입력하지 말고, 휴대폰 같은 2채널(two-channel) 솔루션이나 OTP(One Time Password)를 사용하라는 식의 지침이 제시된다[4]. 하지만 새로운 피싱 공격 기법인 '액티브 피싱(active phishing)'은 기존의 대응방안으로는 대응하기 어려우며, 사용자가 정상 사이트와 피싱 사이트를 전혀 구분할 수 없어 심각한 문제가 우려된다. 본고에서는 액티브 피싱 공격 기술을 소개하고, 기존의 피싱 대응방안들이 액티브 피싱에 취약함을 보인다. 액티브 피싱 공격을 막기

위해서 어떤 요구사항을 만족해야 하는지 제시하고 이를 고찰한다.

II. 액티브 피싱

1. 액티브 피싱이란?

액티브 피싱은 MITM(Man In The Middle) 공격을 피싱 공격에 응용한 것으로, MITM 피싱 또는 실시간(real-time) 피싱으로도 불린다. (그림 1)에서 보듯이, 액티브 피싱은 사용자가 입력한 정보를 중간에서 가로채서 사용자에게는 공격자가 실제 웹 사이트인 것처럼 속이고, 웹 사이트에게는 공격자가 정상 사용자인 것처럼 속인다. 웹 사이트에 적용된 키로깅(key-logging), 안티 바이러스(anti-virus), 피싱 차단 솔루션 등과 같은 기존의 피싱 공격 대응방안들은 액티브 피싱 공격을 수행하는 공격자의 PC에 설치되나, 공격자는 정상 사용자처럼 동작하기 때문에 이들 방안은 무용지물이 된다. 정상 사용자의 경우, 일단 액티브 피싱 사이트에 접속하면 공격자가 조작한 웹 사이트 콘텐츠와 보안 솔루션이 적용된다. 따라서 정상 사용자는 공격자에게 모든 개인정보/인증정보를 평문으로 제공하게 되고, 2채널/투팩터(two-factor) 인증 또한 공격자를 대행하여 수행하는 셈이므로 액티브 피싱에는 효과가 없다.

다음과 같은 액티브 피싱 가상 시나리오가 있을 수 있다. ① 공격자가 사용자와 실제 금융 사이트 사이에 위치하고, 사용자에게는 웹 사이트로부터 수신한 화면을 보여주어 실제 웹 사이트에 접속한 것처럼 속인다. ② 사용자가 계좌이체를 시도할 때, 공격자는 사용자가 입력한 계좌이체 정보를 변조하여 사용자에게는 원래 계좌이체 정보를 보여주지만 실제 웹 사이트에는 공격자의 계좌이체 정보를 입력하고 대기한다. ③ 사용자는 실제 웹 사이트에 사용하는 인증 기술(가령, OTP와 2채널 인증)을 수행한다. ④ 실제 웹 사이트는 사용자로부터 2채널 인증을 확인받고, 공격자가 전달한 OTP를 검증하여 계좌이체를 완료한다.

〈자료〉: the phishing guide; underatnding&preventing phishing attacks[5]

(그림 1) 액티브 피싱 구조도

2. 액티브 피싱 히스토리

가. 뉴스

액티브 피싱의 피해 사례는 2010년부터 등장하기 시작했다. 한 기사에 따르면, 투팩터 인증을 사용하는 웹 사이트들에 대한 공격의 30%는 실시간 중간자 공격이었다[6]. 실시간 피싱 공격에서 공격자가 사용자로부터 가로채는 정보들은 OTP/보안 토큰/SMS 인증 등을 포함하며, 기존의 피싱 공격의 대응수단이었던 OTP 또한 실시간 피싱 공격에는 무용지물이라고 언급했다.

다른 기사에서도 액티브 피싱 공격에는 투팩터 인증과 OTP가 대책이 될 수 없다고 경고했다[7]. Trusteer의 CEO인 Mickey Boodaei에 따르면 액티브 피싱 공격은 보안 분야에서는 이미 널리 알려진 공격 방법 중에 하나인데, 지금까지는 공격 사례가 거의 없었지만 점차 확대되고 있다고 말했다.

이어 2012년 BBC에서 해커들은 온라인 뱅킹의 보안 시스템보다 한발 앞선다고 말하며 액티브 피싱의 위험성에 대해서 언급했다[8].

나. 관련 논문 소개

액티브 피싱의 가능성은 2005년도에 Bruce Schneier

가 처음 제기했다[9]. 그는 논문에서 투팩터 인증의 취약성을 제시하면서 MITM 공격의 위험성에 대해서 경고했다. 투팩터 인증은 매번 변경되는 비밀번호를 사용함으로써 과거 비밀번호 시스템의 약점을 극복했지만, 비밀번호의 제한시간 전에 해커가 이를 실제 웹 사이트에 전달하는 식의 적극적인 공격에는 취약하다. 그러므로 투팩터 인증은 내부 네트워크나 일부 회사 네트워크 망에서만 사용하는 것이 적합하며, 투채널 인증도 MITM 공격에 대한 대응방안이 될 수 없다고 언급하였다.

이 후, 2007년도에 Gunter Ollmann은 MITM 피싱 공격 방법을 제시하면서 그 위험성을 경고했다[5]. 그는 논문에서 MITM 피싱 공격의 예시를 보여주면서 HTTP(Hypertext Transfer Protocol)와 HTTPS (Hypertext Transfer Protocol Secure) 통신 모두 공격이 가능함을 보였다. 이 공격을 위해서는 마치 공격자의 서버가 진짜 은행 웹 사이트인 것처럼 속여 사용자가 공격자의 서버에 접속하게 만들어야 하는데, 4가지 방법(프록시 서버 사용, DNS 캐시 변조, 유사한 URL 사용, 브라우저의 프록시 설정 변경)을 제시하였다.

다. 기존 피싱 공격과의 차별성

기존의 피싱 공격은 사용자가 피싱 사이트에 접속하여 입력한 인증/개인 정보를 공격자가 탈취하고, 향후 범죄 행위에 이 정보를 악용하는 방식이었다. 하지만 액티브 피싱 공격은 사용자에게 실제 웹 사이트에 접속한 것과 같은 착각을 하게 만들면서, 실시간으로 사용자의 정보를 탈취하여 악성 행위를 수행한다.

여러 언론 매체에서 보도되었고 금융 사이트에서도 주기적으로 공지하는 것처럼, 기존의 피싱 공격은 고정된 피싱 사이트에 사용자의 개인정보와 보안카드 번호 등 민감한 정보의 입력을 요구한다. 이에 대한 대응방안으로, 보안카드 번호를 모두 입력하라는 요청을 하는 경우 피싱으로 간주하거나 보안카드 대신 OTP를 사용하라는 제안이 해결책으로 제시되고 있다.

그러나 이 해결책은 액티브 피싱 공격에는 무용지물이다. 공격자는 사용자가 입력하는 정보에 따라 실시간으로 사용자에게 개인화된 화면을 제공하고, 기존과 동일한 사용자 경험을 제공한다. 또한 사용자의 인증/개인정보를 은밀하게 탈취하고, 계좌번호 등을 실시간으로 변조한다. 액티브 피싱에서 공격자는 보안카드 번호를 모두 요구할 필요가 없고, OTP를 사용하더라도 실제 웹 사이트에 실시간으로 전달할 수 있다.

Ⅲ. 기존 대응방안 고찰

본 장에서는 기존의 피싱 공격 대응방안들인 ID/Password, OTP, PKI(Public Key Infrastructure)와 플러그인, SSL(Secure Sockets Layer), 개인화 이미지, 피싱 차단 솔루션, 2채널 인증, OOB(Out Of Band) 인증, 서버 확인, 툴바 기술에 대해서 살펴보고 이러한 대응방안들이 액티브 피싱 공격에 대응책이 될 수 없는 이유에 대해서 알아본다.

1. ID/Password

ID와 비밀번호를 이용한 인증은 가장 많이 사용되는 방식이다. 하지만 비밀번호는 비교적 오랫동안 변경되지 않고 사용되고, 여러 사이트나 애플리케이션에 같은 ID와 비밀번호가 재사용되기도 한다. 그렇기 때문에 이 인증 방식은 액티브 피싱뿐만 아니라 기존의 피싱 공격에도 상당히 취약하다[10].

최근에는 단순히 평문의 ID와 비밀번호를 웹 사이트에 전달하는 대신에, 사용자가 비밀번호를 가공하여 전달하도록 웹 사이트가 특정한 작업을 요청하기도 한다. 한 포털 사이트는 보안 로그인이라는 서비스를 제공하여, 사용자 단에서 자바스크립트나 플래시를 통해 비대칭키를 생성하고 사용자 패스워드를 암호화하여 전달한

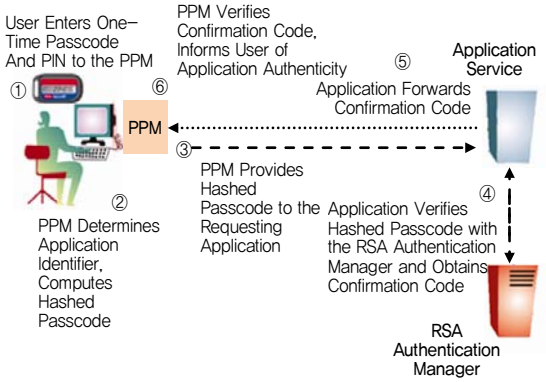
다. 기존의 MITM 공격일 경우, 공격자가 중간에서 패스워드를 복호화할 수 없기 때문에 안전하다.

하지만 액티브 피싱의 경우, 웹 사이트에서 보안 로그인 기술을 제공하더라도 웹 사이트와 공격자 사이에만 적용되고, 사용자와 공격자 간에는 평문으로 비밀번호를 전달하게 된다. 따라서 공격자는 웹 사이트의 보안 로그인을 공격하지 않으면서, 정상 사용자처럼 로그인할 수 있다.

2. OTP

OTP는 사용자 측에서 별도의 하드웨어/소프트웨어를 통해 제한된 시간(대부분 1분)에만 유효한 비밀번호를 생성하고, 웹 사이트는 검증 서버를 통해 해당 비밀번호의 유효성을 인증하는 방식이다. ID/Password 방식의 경우 한번 노출된 패스워드는 더 이상 유효하지 않지만, OTP는 매번 다른 비밀번호로 인증하기 때문에 노출되어도 상대적으로 안전하다. 현재는 대부분의 금융권에서 피싱 방지 대책으로 많이 채택하여 사용하고 있다.

하지만 OTP 또한 액티브 피싱 공격에 안전할 수 없다. 공격자가 중간에서 서버인 척 사용자의 OTP를 전송받고, 이 OTP를 실시간으로 실제 서버에 전송하면, 공격자는 쉽게 실제 서버에 사용자인 척 인증할 수 있다. OTP의 유효시간이 수십 초에 불과하더라도, 공격자가



〈자료〉: RSA SECURITY, 2006.

(그림 2) PPM을 이용한 OTP 보호[11]

사용자로부터 수신하여 실제 웹 사이트에 전송하는 시간이 OTP의 유효시간보다 짧기 때문이다.

OTP의 이러한 단점을 보완하여 RSA에서 제시한 OTP 개선안은 사용자 측에 PPM(Password-Protection Module)이라는 별도 모듈/단말을 설치하는 것으로, 세부 흐름은 (그림 2)와 같다[11]. PPM은 사용자로부터 OTP를 입력받고, 서버 식별자(URL, 도메인 이름 등)와 결합하여 해시(hash)된 OTP를 사용한다.

그러나 TPM(Trusted Platform Module)에 해당하는 PPM이 PC/OS에 기본 탑재되어 있어야 하며, PPM이 사용하는 애플리케이션 서버 식별자를 조작할 수 있으면 액티브 피싱에 여전히 취약하다. 만약 PPM이 플러그인 형태로 설치될 경우, 기존 OTP와 동일한 방식으로 액티브 피싱 공격이 가능하다. 즉, 공격자는 사용자의 OTP를 입력받은 뒤, 공격자의 PC에 설치된 PPM에 전달하여 해시 OTP를 생성하고 서버에 전송할 수 있다.

3. PKI와 보안 플러그인

한국의 금융 사이트들은 대부분 PKI 기반의 서비스를 제공하고 있다. 공인인증서는 사용자의 컴퓨터나 이동식 디스크 등에 저장되는데, PKI 시스템을 이용하기 위해서 사용자들은 안티 바이러스, 안티 키로깅, 방화벽 등과 같은 보안 모듈을 웹브라우저 플러그인을 통해서 설치해야 한다[12].

사용자의 컴퓨터를 안전한 상태로 만들기 위한 보안 플러그인들은 액티브 피싱에서는 전혀 도움이 되지 않는다. 이들 플러그인이 공격자의 PC에 설치되는데, 공격자는 정상적인 사용자처럼 행동하기 때문에 피싱 솔루션에 탐지되지 않는다.

사용자는 기존에 정상 웹 사이트를 사용하기 위해 다수의 플러그인을 설치했던 경험에 익숙하기 때문에, 피싱 사이트를 정상 웹 사이트로 오인하고 공격자에 의해 조작된 플러그인에 쉽게 노출 당하게 된다. 이 때 공격

자에 의해 조작된 공인인증서 플러그인을 설치하면, 사용자의 컴퓨터에서 공인인증서를 검색/복제하고 사용자가 입력한 비밀번호와 함께 공격자에게 전송된다.

플러그인을 논할 때, 마이크로소프트의 ActiveX 방식이 보안상 취약하다는 문제를 지적하는 경향이 있다. 하지만 액티브 피싱 공격은 플러그인 개념 자체의 문제에 기인하기 때문에 PKI나 다른 보안 솔루션이 플러그인에 의존해서는 안 된다. 또한 자바나 플래시/브라우저별로 특화된 플러그인 등 구현 방식에도 무관하며, 적용되는 보안 기술에 무관하게 액티브 피싱에 취약하다.

4. SSL

SSL는 서버의 공개키 인증서를 활용하여 매번 다른 보안채널을 형성하는 기술로, 사용자의 브라우저와 서버 사이에 안전한 통신을 제공한다. SSL 통신이 제대로 설정됐는지 확인하기 위해서는 사용자의 노력이 필요한데, 웹 사이트 URL을 확인하고 SSL 아이콘 이미지가 브라우저 상단에 제대로 표시됐는지 확인해야 한다. (그림 3)처럼 최근의 EV SSL인 경우, 주소창의 색이 녹색으로 변하여 사용자가 좀 더 직관적으로 보안 통신 여부를 인지할 수 있다.

하지만, 대부분의 사용자들은 SSL 여부를 제대로 확인하지 않는다. MIT/Harvard의 조사 결과, 정교하게 제작된 피싱 사이트에 참가자들의 90%가 SSL 여부를 인지하지 못하였다[13]. 현재의 보안 표기(예를 들면, SSL 아이콘 이미지, 상태 바, 주소 창)도 비효율적이었다. 참가자의 23%는 보안 표기를 확인하지 않았고, 심지어 보안 표기가 무엇을 의미하는지 알지 못했다.

국내의 경우, 최근에야 금융 사이트들이 SSL 통신을 지원하기 시작했다. 기존에는 SSL 통신을 수행할 경우

(그림 3) SSL을 사용하는 사이트에 접속한 모습

통신뿐만 아니라 메시지 처리 과정에서 부하를 우려하여 최대한 기피하는 성향을 보였다. SSL 통신은 사용자의 인식 여부가 중요한데, 일부 금융 사이트는 로그인 단계에만 SSL 통신을 제공하는 등 소극적으로 활용하고 있다. 이 때문에 사용자들이 SSL 통신을 학습하고, SSL 유무를 인식하는데 여전히 어려운 상황이다.

5. 개인화 이미지

개인화 이미지는 사용자가 미리 설정한 특정 이미지의 유무에 따라 실제 사이트와 피싱 사이트를 구분하는 방법이다. 대표적인 사례로 Bank of America의 피싱 방지 기술인 Sitekey가 있다[14]. Sitekey는 secure cookie에 사용자의 개인화 이미지 정보를 설정해 두었다가, 웹 사이트에 접속할 때 쿠키(cookie) 정보를 확인하여 사용자의 개인화 이미지를 보여준다. 이 기술 또한 SSL 아이콘처럼 사용자의 명시적인 확인을 요구한다.

그러나 MIT와 Harvard의 연구에 따르면, 피싱 사이트에 접속한 사용자의 3%만이 Sitekey를 활용하여 피싱 사이트임을 확인하고 개인정보를 제공하지 않았다. eBay 사용자들을 대상으로 수행한 연구에서도 사용자들은 안전하지 않은 세션(예를 들면, 자물쇠 아이콘이 툴 바에 표기되지 않더라도)이더라도, 100%가 비밀번호를 입력하였다[14]. 이것은 대부분의 사람들이 Sitekey의 개인화 이미지를 제대로 확인하지 않으며, 피싱 차단에는 효과가 없음을 보여준다.

또한 Sitekey는 쿠키 정보를 활용하기 때문에 다른 PC에서는 사용할 수 없다는 문제가 존재하였다. 이를 해결하기 위해, Sitekey는 쿠키가 없는 경우, 웹 사이트가 사용자로부터 ID를 입력 받은 뒤 개인화 이미지를 출력하는 방식을 제안하였다. 하지만, 액티브 피싱의 경우, 사용자로부터 ID를 입력받아 실시간으로 정상 웹 사이트에 포워딩하고, 개인화 이미지를 수신받아 다시 사용자에게 전달하는 식으로 Sitekey를 무력화 시킬 수

있다.

6. 피싱 차단 솔루션

대다수의 피싱 차단 솔루션은 블랙리스트(black list)에 기반하는데, 알려진 피싱 사이트의 주소를 블랙 리스트 서버에 등록하여 접속하지 못하도록 한다. 블랙리스트는 APWG 또는 PhishTank, 금융기관에서 탐지한 피싱 사이트들을 관련 전문가가 직접 분석하여 등록한다[15]. 블랙리스트는 사용자의 컴퓨터에 다운로드되어 적용되는데, 파이어폭스 브라우저의 경우에는 매 30분마다 피싱 사이트 블랙리스트를 다운로드 한다[16].

그러나 APWG의 기술 논문에 따르면, 2011년 하반기 피싱 사이트의 평균 사이트 오픈부터 폐쇄까지의 시간은 46시간에 불과하였다[17]. 피싱사이트가 활동하는 시간이 매우 짧기 때문에, 보안 단체와 금융기관이 완벽하게 피싱사이트를 확보하여 적용하는 것은 어려운 실정이다. 더구나 액티브 피싱은 사용자가 피싱 여부를 인지하기 어려운 구조이기 때문에, 블랙리스트에 추가되는데 걸리는 시간 또한 상대적으로 길 수 밖에 없다.

7. 2채널 인증

2채널 인증은 금융 거래 시 1채널(pc)에서 이루어지는 본인 인증 과정을 다른 채널(스마트폰, 유선전화 등)로 확대하는 것을 말한다. 거래 인증에서의 투채널 시스템은 TAN(Transaction Authentication Numbers)을 포함하고 있다. TAN 코드는 사용자가 정말로 거래를 시작한 것이 맞는지 확인하는데 요구되는 일회용 비밀번호로서 제공되며, 신뢰된 채널(SMS 등)을 통해 사용자에게 발급된다. 사용자는 은행 웹 사이트에 PC 채널(1채널)을 이용하여 ID/패스워드 등으로 로그인한 후에, 휴대폰(2채널)으로 TAN 코드를 입력한다[11].

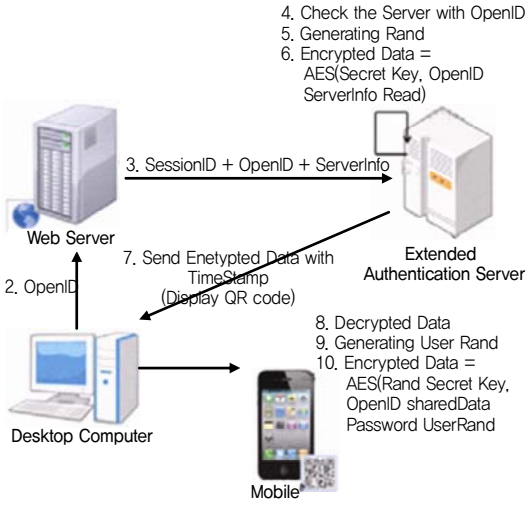
TAN 코드를 이용한 투채널 인증의 주요 이슈는 TAN 코드의 유효 기간이다. TAN 코드는 보통 1년 이상 유효하기 때문에 ID/패스워드와 같이 해커에게 노출될 가능성이 높다[11].

TAN 코드의 유효기간이 매우 짧더라도, 액티브 피싱 공격에 취약하다. 사용자가 공격자의 서버를 통해서 은행에 접속한 경우, 사용자가 PC가 아닌 다른 채널로 인증을 하다고 해도 결국 중간에서 공격자가 은행 서버로부터 거래 확인이나 인증을 받기 때문이다. 즉, 공격자를 위해 은행과 사용자가 신뢰된 채널로 인증하는 셈이 된다.

8. OOB 인증

OOB 인증은 신뢰된 채널을 통해 비신뢰 채널에 대한 인증 절차를 대행하는 기술을 의미한다. 즉, 사용자가 피싱 사이트에 접근하더라도 본인의 인증정보를 피싱 사이트에 직접 제공하지 않고, 신뢰 채널을 통해 실제 웹 사이트에 제공하기 때문에 인증정보가 안전하게 유지된다는 장점을 가진다. OOB 인증과 관련하여 스마트폰 QR코드를 활용한 방안이 다수 제시되었다.

(그림 4)는 OpenID 솔루션에서 QR코드를 이용하는 모바일 기반 피싱 방지 인증 기법을 보인다. 이 기법은



〈자료〉: An Anti-Phishing mechanism for Single Sign-On based on QR-Code, 2011.

(그림 4) 모바일 기반 QR코드 인증[18]

QR코드와 미리 공유된 비밀키(shared secret key)를 이용해서 사용자와 인증서버 사이를 인증하는 방식이다. 사용자가 접속한 서버의 피싱 사이트 여부를 확인하기 위해서, 인증서버는 사용자가 접속한 서버 정보를 공유 비밀키로 암호화하고 QR코드로 변환하여 사용자에게 전송한다. 사용자는 해당 QR코드를 스마트폰으로 인식하여 서버와 직접 로그인 절차를 수행한다[18].

QR코드에 타임스탬프(time stamp)를 추가하여 QR코드의 안정성을 향상시킨 기법도 있다[19]. 서버는 사용자에게 암호화된 QR코드와 함께 타임스탬프T1을 전송한다. 사용자는 QR코드를 복호화한 후에 타임스탬프T2와 함께 서버에 전송한다. 서버는 QR코드의 유효성과 T2의 시간 유효성(acceptability)을 검사한다. 서버와 사용자 간의 타임 스탬프의(T1−T2) 차이는 최소(수 초~1분 이내)라고 가정한다면, 중간에서 공격자가 암호화된 QR코드를 가로챈 후 나중에 사용자인 척 인증을 시도하여도, T2가 이미 만료됐기 때문에, 서버에서 인증이 실패하게 됨으로써 중간자 공격에서 안전하다고 한다.

OOB 인증은 기존의 피싱공격에 대한 대응방안으로는 유효하지만, 액티브 피싱 공격에서는 공격자가 자신의 QR코드를 사용자에게 전달하여 대신 인증을 받게 할 수 있다. 이 경우, 사용자와 실제 웹 사이트가 아무리 강력한 인증 메커니즘을 적용하더라도 사용자는 공격자를 위해 대신 인증을 수행해 주기 때문에 액티브 피싱에 취약하게 된다.

9. 서버 확인

서버 측에서의 피싱 방지 솔루션으로는 이상 거래 탐지(transaction anomaly detection), 로그 파일 분석(log file analysis) 등이 있다[11].

이상 거래 탐지는 오래 전부터 자금 세탁과 신용카드 범죄를 탐지하기 위해서 많은 금융기관에서 사용했던 기술이다. 사용자의 프로파일링과 정상적인 거래 규칙에 어긋나는 악의적인 거래가 발생하면, 서버 측의 담당자에게 알림이 전달되어 적절한 대응을 할 수 있다.

피싱 공격을 탐지하기 위해서 로그 기록에 대한 자동화 분석을 이용하는데, 대표적으로 HTTP referrer 로그 분석과 로그인 로그 분석이 있다. 웹 브라우저가 은행 사이트의 콘텐트를 요청할 때, 출처 URL을 표시하는 referrer-header를 전송한다. 만일 출처 URL이 은행 사이트가 아니라면, 해당 사이트가 피싱 공격을 수행한다고 확인할 수 있다.

로그인 로그 분석은 동일한 IP에서 여러 로그인 요청 기록이 있으면 피싱으로 간주하는 방법이다. 예를 들어, 서로 다른 ID의 로그인 요청이 하나의 IP주소로부터 오거나, 특정 ID가 기존과 다른 장소에서 로그인을 시도한다면 피싱 공격이라고 여기는 것이다. 그리고 지도상의 위치와 IP 주소를 매핑하여 피싱 공격의 근원지가 어디인지 탐지할 수도 있다.

서버에서 피싱사이트 여부를 확인하기 위해서는 모든 로그들이 실시간으로 감시되어야 하고, 매우 빠른 응답이 시간이 요구된다. 또한 사용자가 서버를 대상으로 수행하는 행동 패턴만으로 피싱 여부를 분석해야 하기 때문에, 액티브 피싱과 같이 정상 사용자와 동일하게 동작하는 공격은 막기 어렵다. 또한 은행 사이트의 콘텐츠를 그대로 활용하지 않고 복제하여 이용하거나, 여러 IP 대역을 활용하여 기존 로그 분석을 회피할 수 있다.

10. 툴바

웹 브라우저에 있는 보안 툴바는 사용자들이 피싱 공격을 인지하도록 사용자가 접속한 웹 사이트의 보안 관련 정보를 보여준다. 보안 툴바는 3가지 종류로 나뉜다[20].

1) 중립정보 툴바: 도메인 이름, 호스트 네임, 사이트 등록 날짜, 호스팅 국가 등과 같은 웹 사이트 정보를 보여주는 툴바이다. 사용자들이 웹 사이트 정보를 보고 스스로 피싱 사이트인지 파악해야 한다.

2) SSL 인증 툴바: SSL을 사용하는 사이트와 그렇지

않은 사이트를 구분하는 툴바이다. 중립 정보 툴바와 마찬가지로 사용자의 인지가 필요하다.

3) 시스템 결정 툴바: 해당 웹 사이트가 잠재적인 위험이 있다고 경고 메시지를 보여주거나, 접속을 차단하는 툴바이다. 사용자가 툴바를 신뢰해야 한다는 단점이 있다.

하지만 보안 툴바의 경우에도, MIT 조사결과, 중립정보 툴바를 사용하는 참가자들의 33%, SSL 툴바를 사용하는 참가자들의 38%, 시스템 결정 툴바를 사용하는 참가자들의 45%는 툴바를 어떻게 해석해야 하는지 몰랐으며 피싱 사이트에 속았다.

대부분의 사용자들은 툴바를 어떻게 해석해야 하는지 모르고, 툴바의 정보를 제대로 확인하지 않는다. 이 때문에 기존의 피싱 공격 사이트뿐만 아니라, 액티브 피싱 공격 사이트에 대한 정보를 툴바에서 표시한다고 하더라도 대부분의 사용자들은 지나칠 것이다.

Ⅳ. 대응방안의 요구사항

이전 장에서 기존 대응방안을 고찰하였고, 모두 액티브 피싱에 취약하다는 것을 확인할 수 있었다. 본 장에서는 액티브 피싱에 대응하기 위한 방안이 만족해야 하는 요구사항을 고찰하기로 한다. 대응방안은 크게 편의성, 성능, 보안성의 세 항목으로 구분할 수 있으며, 〈표 2〉는 대응방안의 요구사항 목록을 보인다.

〈표 2〉 액티브 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
	액티브 피싱 공격 대응
	새로운 피싱 공격에 유연하게 대처 가능

'편의성'은 피싱 사이트 탐지 과정이 사용자에게 불편함을 초래하거나 별도의 추가적인 작업 또는 하드웨어를 요구하지 않는 방향으로 이루어져야 함을 요구한다.

'성능'은 피싱 사이트 여부를 빠르게 확인할 수 있어야 되며, 올바른 사이트를 피싱 사이트로 잘못 탐지하거나(오탐) 피싱 사이트를 제대로 탐지하지 못하는 경우(미탐)를 최소화해야 됨을 요구한다.

'보안성'은 대응방안 자체가 안전해야 하며 외부의 공격에 대해 대응할 수 있어야 함을 요구한다. 또한 기존의 피싱/파밍 공격에 대응해야 하며, 액티브 피싱을 비롯하여 새로운 피싱 공격에 유연하게 대처 가능할 수 있어야 한다.

Ⅴ. 결론

본고는 기존의 피싱 공격과는 달리 사용자와 실제 웹 사이트 사이에서 실시간으로 사용자의 정보를 탈취하고 변조하는 액티브 피싱 공격을 소개하였다. 또한 기존 방안인 ID/Password, OTP, PKI와 플러그인, SSL, 개인화 이미지, 피싱 차단 솔루션, 2채널 인증, OOB 인증, 서버 확인, 툴바 기술이 액티브 피싱에 무력함을 보였다.

그리고 편의성, 성능, 보안성 관점에서 기본적인 요구사항을 정의하여 액티브 피싱을 비롯한 피싱 공격에 대응하는 방안을 마련하기 위한 지침을 제시하였다. 향후에도 고도의 피싱 공격들이 등장하여 사용자와 인터넷 서비스를 위협할 것으로 예상되므로, 본고의 지침을 통해 근본적이고 꾸준한 대응방안이 수립되어야만 한다.

약어 정리

DNS Domain Name System
HTTP Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
MITM	Man In The Middle
OOB	Out Of Band
OTP	One Time Password
PKI	Public Key Infrastructure
PPM	Password-Protection Module
SSL	Secure Sockets Layer
TAN	Transaction Authentication Numbers
TPM	Trusted Platform Module

용어해설

키로깅(key-logging) 사용자가 키보드로 PC에 입력하는 내용을몰래 낚아채어 기록하는 행위

Anti-Virus 컴퓨터 바이러스를 탐지하여 사용자의 컴퓨터를 바이러스로부터 안전하게 보호하는 프로그램

Two-Factor Authentication 두 가지 인증 방식을 동시에 사용해 기존 패스워드의 취약점을 보완한 것으로, 현재 국내에서는 ID/패스워드와 함께 공인인증서(PKI)/일회용비밀번호(OTP) 방식을 많이 사용

QR코드 흑백 격자무늬 패턴으로 정보를 나타내는 2차원 형식의 바코드

OS 컴퓨터의 하드웨어와 소프트웨어를 제어하여, 사용자가 컴퓨터를 사용할 수 있게 만들어주는 프로그램

참고문헌

[1] 한국은행, "2012년중 국내 인터넷뱅킹서비스 이용현황," 2013. 2. 22.

[2] 김진홍, 김헌기, 조성래, "보이스피싱(파밍) 합동 경보 발령!" 금융위원회, 2013. 3. 3.

[3] APWG, "Phishing Activity Trends Report 3rd Quarter 2012," APWG, Feb. 1st, 2013.

[4] 금융위원회, "금융소비자 보호를 위한 보이스피싱 피해방지 종합대책", 2012. 1. 31.

[5] G. Ollmann, "The Phishing Guide: Understanding & Preventing Phishing Attacks," IBM Internet Security Systems, 2007.

[6] HELP NET SECURITY, "Real Time Phishing Attacks Increase," Sept. 10th, 2010.

[7] DARK READING, "Researchers See Real-Time Phishing Jump," Sept. 9th, 2010.

[8] BBC NEWS, "Hackers Outwit Online Banking Identity Security Systems," Feb. 10th, 2012.

[9] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," Commun ACM, vol. 48, no. 4, Apr. 2005, pp. 135-136.

[10] Stan Hegt, "Analysis of Current and Future Phishing Attacks on Internet Banking Services," Master Thesis, Technische Universiteit Eindhoven, May 2008.

[11] RSA Security, "Enhancing One-Time Passwords for Protection against Real-Time Phishing Attacks," 2006.

[12] H. Kim, J.H. Huh and R. Anderson, "On the Security of Internet Banking in South Korea," University of OXFORD, Mar. 2010.

[13] R. Dhamija, J.D. Tygar and M. Hearst, "Why Phishing Works," Proc. Conf. Human Factors Comput. Syst. (CHI2006), Apr. 2006.

[14] slight paranoia, "A Deceit-Augmented Man In The Middle Attack Against Bank of America's SiteKey," Apr. 10th, 2007.

[15] S. Sheng et al., "An Empirical Analysis of Phishing Blacklists," 6th Conf. Email Anti-Spam, July 2009.

[16] F. Schneider et al., "Phishing Protection: Design Documentation," Mozila Wiki, Jan. 2009.

[17] APWG, "Global Phishing Survey: Trends and Domain Name Use in 2H2011," Apr. 2012

[18] K. Choi et al., "A Mobile Based Anti-Phishing Authentication Scheme Using QR Code," Int. Conf. Mobile IT Convergence, 2011, pp. 109-113.

[19] S. Mukhopadhyay and D. Argles, "An Anti-Phishing mechanism for Single Sign-On based on QR-Code," IEEE Int. Conf. Inf. Society, 2011, pp. 505-508.

[20] M. Wu, R.C. Miller, S.L. Garfinkel, "Do Security Toolbars Actually Prevent Phishing Attacks?" Proc. Conf. Human Factors Comput. Syst. (CHI2006), Apr. 2006.