피싱 방지를 위한 OTP 이용 서버 인증 기법 제안

이준섭 ○ 이민수 조상현

KAIST KAIST NHN

{jslee, mslee}@depnedable.kaist.ac.kr, bungae@nhncorp.com

Anti-Phishing Solution Using Server-Side OTP Authentication

Junsup Lee ○ Min Soo Lee Sanghyun Cho

KAIST KAIST NHN

요 약

피싱의 위험이 증대되는 현재의 온라인 서비스 환경에서 사용자를 기본적인 피싱 시도로부터 보호하기 위해 OTP를 사용하여 서버와 사용자를 상호 인증하는 기법을 제안한다. 제안 하는 기법에서 사용자는 사이트를 신뢰 할 수 없는 환경에서 서버와 공유하고 있는 비밀 키인 OTP를 사용하여 서버의 진위 여부를 확인하고, 서버 또한 사용자를 인증하도록 함으로서 일반적인 피싱 시도로부터 사용자 보호가 가능하다. 이러한 기법은 클라이언트 단에 어떠한 부가적인 프로그램을 설치할 필요 없으며 사용자 직관적이어서 활용도가 매우 높다.

1. 서 론

최근 OTP를 이용하여 온라인 금융 거래의 보안수준을 향상 하고자 하는 노력이 두드러지고 있으며 많은 금융기관과 정부는 전자금융거래의 안전성 강화 수단으로 일회용비밀번호(OTP) 기술을 도입하는 서두르고 있다[1]. OTP는 기존의 전자인증서 + 보안카드 시스템의 취약성을 보완하여 온라인 금융 거래뿐만 아니라 다양한 온라인 상거래에 적용될 것으로 기대되고 있다. 이에 따라 금융보안연구원은 OTP 통합인증센터를 운영함과 동시에 OTP 기술 표준화 작업을 통하여 금융기관을 포함한 다양한 온라인 비즈니스 업체가 높은 수준의 보안 인증 시스템을 원활하게 적용 할 수 있도록 하고 있다[3].

OTP를 활용한 접근은 사용자 인증 수준을 높일 수 있으나 피싱에는 아직 취약한 면을 보이고 있다[4]. OTP 기술 자체가 근본적으로 피싱 방지 솔루션이 아니며, 금융거래상의 해킹 등의 공격에 대비하기 위한 대응책으로 제안된 것이다. 전 세계적으로 가장 큰 온라인 결제 대행 사이트중 하나인 PayPal이 OTP를 사용자 인증 시스템으로 적용하였으나 아직 피싱 공격에 취약한 것으로 평가 되고 있다[5,6]. 국제피싱대응협의체 안티피싱워킹그룹(Anti-Phishing Working Group (APWG)) 에 따르면 전 세계적으로 피싱 공격은 매달 50%씩 증가 하고 있으며, 피싱 타겟 중 5%의 사용자는 피싱의 피해자가 되고 있다[7]. 국내의 환경은 현재 다른 나라와 비교하여 피싱의 발생 빈도가 낮으나 지속적으로 피싱의 위험이 증대 대고 있다. 관련 업계에서는 이러한 피싱 위험의 증대를 고려하여 새로이 도입되는 통합 온라인 보안 방안인 OTP에서 피싱에 대한 대응책을 고려해야 한다고 말하고 있다[4].

이 논문에서는 OTP를 활용하여 클라이언트 단에서 피싱을 방지를 위해 서버를 사용자가 인증 할 수 있는 기법을 제안 한다. 현재 OTP는 서버측에서 사용자 측을 인증 하는 과정에만 활용되고 있다. 하지만, 서버측과 사용자측이 동등한 입장에서 비밀키를 공유하고 있는 OTP의 특성을 이용하면 사용자가 서버측을 인증 하는 용도로 사용가능하다. 본 논문에서는 웹 사이트가 제공하는 온라인 서비스 유형에 따라 로그인 과정이나, 카드 결제, 현금 이체 등의 중요 서비스 제공시에 현재의 웹 사이트 및 웹 페이지의 진위 여부를 사용자가 판단 할 수 있는 방안을 제안한다. 이를 통하여 사용자는 대부분의 피싱 시도로부터 보호 받을 수 있다.

우리의 접근 방식은 과거의 접근과는 다르게 OTP를 활용하여 서버를 인증함으로서 사용자가 별도의 피싱 방지 프로그램 설치 없이 피싱 시도로부터 보호 받을 수 있다. 현재까지의 피싱 대응 방식은 알려진 피싱 사이트에 대한 블랙리스트를 유지하여 그것을 차단하거나, 그와 반대로 화이트 리스트를 유지하여

합법적인 사이트의 정보를 유지하는 방법을 사용했다[11]. 두 방안의 경우 별도의 데이터를 유지 관리 업데이트하기 위한 비용이 크게 필요 하다는데 큰 제약이 있었다. 그러한 유지 관리의 부가 비용을 없애기 위하여 사용자의 웹 브라우저 등의 플러그인 형식으로 설치되어 페이지의 내용과 URL 의 이상성을 계산하여 피싱 위험 정도를 계산 하는 연구가 있었으나 그 정확도가 아직 만족할 만한 수준이 못되어 적용에 한계가 있다[8,9,10]. 기존의 접근은 모두 피싱 대응을 하기 위하여 별도의 프로그램을 설치하거나 장비를 설치해야 하는 등 부가적인 사용자 액션을 요구 하여 그 적용에 큰 제약이 있었다[12]. 하지만 여기서 제안하는 방법은 사용자가 어떠한 부가적인 프로그램이나 장비를 설치를 할 필요가 없으며, 서버 인증을 위하여 자신의 OTP 값과 서버가 보내온 일부분의 OTP 값을 비교함으로서 사이트 진위 여부를 확인 가능하다는 장점이 있다.

2장에서는 기존 피싱 방지 솔루션과 과 OTP와 관련된 연구를 살펴보고, 3장에서는 본 논문에서 제안하는 기법에 대한 설명과 그 사례에 대해 기술 한다. 또한 그 사례를 들어 시스템의 활용을 설명한다. 4장에서는 제안한 시스템과 이전의 시스템의 보안 수준을 표로 비교하겠다. 마지막으로 5장을 통해 이 논문의 결론에 대해 기술한다.

2. 관련 연구

2.1 기존 피싱 방지 연구

연구 커뮤니티에 의해 가장 활발하게 연구되고 있고, 현실적인 접근 방법은 알려진 피싱 사이트에 대한 블랙리스트(Web-site Black Lists : WBLs)를 생성 하는 것이다. 현재의 많은 피싱 대응 솔루션 들은 블랙리스트(Web-site Black Lists : WBLs)를 이용하여 클라이언트에 설치된 별도의 프로그램이나 네트워크의 게이트웨이 DNS서버에서 필터링을 하는 방법을 사용한다. 이러한 블랙리스트는 보안 솔루션 업체나 비영리 커뮤니티 단체의 의하여 업데이트 되고 유지 된다. 현재 가장 많은 활동을 벌이고 있는 피쉬탱크(PhishTank)의 경우 28만 건의 신고에 의하여 현재 8,142개의 피싱 사이트 리스트를 보유하고 있다. 하지만 안티피싱워킹그룹에 따르면 블랙리스트를 이용하여 피싱 사이트를 차단하는데 걸리는 업계평균 시간이 110 시간이다. 결국 사용자는 이 시간 동안 해당 피싱 사이트에 사용자는 아무 보호 장치 없이 노출 되어 있는 것이다[7]. 또한 평균 피싱 사이트의 생명 주기가 3일 인 것을 생각했을 때 블랙리스트는 실효성이 떨어지는 접근이라 평가 되고 있다[7,11].

피싱 사이트 블랙리스트의 단점을 보안 하고자 제안된 것이 화이트 리스트(Web-site White Lists : WWLs)이다. 알려진 적합 사이트에 대한 리스트를 유지함과 동시에 각 사이트의 특성을 기록하여 사용자가 사이트에 접근 하였을 때 해당 사이트의 진위 여부를 확인하도록 한다[12]. 마이크로소프트의 인터넷 익스플로러 7에는 자체적으로 현재 페이지의 위험도를 평가하는 방법과 동시에 WWLs 를 사용하는 피싱 필터를 제공하고 있다. 이 방법 또한 위의 블랙리스트의 문제와 마찬 가지로 리스트를 지속적으로 유지 관리를 해야 한다는 문제뿐만 아니라, 합법적인 사이트가 리스트에 등록 되지 않아 피싱으로 오인 받는 경우가 있다는 것과, 공격자가 IP 변조를 통하여 쉽게 우회 가능 하다는 문제가 있다.

앞서 기술한 두 가지의 접근 이외에도, 두 가지를 혼용하고 자체 알고리즘을 이용하여 클라이언트 단에서 피싱을 차단하는 솔루션들이 몇몇 메이저 업체에 의하여 서비스되고 있다. 대표적인 예로 구글(Google)과 시만텍(Symantec)사가 웹 브라우저 툴바 형태로 피싱 필터링 솔루션을 제공 하고 있다[13]. 이 뿐만 아니라 사이트의 특유 정보를 기록하여 비교하는 방법이나 페이지 정적 분석을 통하여 피싱 위험도를 계산 하는 등의 연구가 다각도로 진행 되고 있다[8,9,10].

이러한 기존 접근 방식은 피싱에 대한 대응책으로서 개별적인 솔루션 상으로는 부족하다는 문제뿐만이 아니라, 부가적인 프로그램이나 장비의 설치, 관련 데이터를 지속적으로 유지하고 업데이트해야 한다는 단점이 있다. 대부분의 인터넷 사용자는 피싱 위험에 대한 자세한 사항을 잘 모르거나 무지한 상태라는 점을 생각 했을 때 사용자에게 부가적인 보안 장치와 프로그램의 설치는 불편함을 가중 시킬 뿐이다.

본 논문에서 제안하는 OTP를 이용하는 서버 인증은 사용자가 피싱을 피하기 위하여 사이트의 진위 여부를 매우 손쉽게 확인 할 수 있으며, 별도의 부가적인 프로그램이나 장비의 설치가 전혀 필요 없다는 장점을 가지고 있다. 또한 방지 할 수 있는 피싱 공격의 범위도 위의 기존 접근 방법과 동일하거나 더 넓어 매우 효과적인 피싱 방지 대응책이라 할 수 있다.

2.2 국내외 OTP 관련 연구 및 활용

해외의 주요 금융 결재 사이트들은 주로 OTP를 사용자 인증 시스템으로서 도입하고 있다. 해외 최대의 결재 대행 사이트중 하나인 PayPal 은 사용자의 인증을 위하여 ID, 비밀번호 이외에 OPT를 사용하는 이중 인증 시스템을 사용하고 있다. 하지만 아직 피싱 위험에는 여전히 취약한 것으로 평가 되고 있다. PayPal 은 현재 전 세계적으로 가장 활발히 피싱 시도가 이루어지고 있는 사이트 이며, OTP 인증 시스템 도입 이후에도 피싱공격 성공의 사례가 보고되어 보안 업계의 큰 관심을 끌었다[5].

국내에서는 6월에 OTP 통합 인증 센터를 도입함과 함께 전자 금융 거래 안전성 강화를 위한 차별화된 노력을 진행하고 있다[3]. 금융권에서는 2007~2008년

이내에 전체 온라인 금융 사용자 천만 명 중 30%에서 많게는 50%에 해당하는 300~500만의 사용자가 금융 결재 보안 솔루션으로 OTP를 사용 할 것으로 예상하고 있다. 또한 OTP 통합 인증 센터의 도입으로 금융권의 사이트뿐만 아니라 다양한 온라인 상거래, 비즈니스 사이트에서도 폭 넓게 적용되리라 보고 있다.

현재의 국내외 OTP의 활용은 매우 제한된 금융권에서 사용자의 인증을 위해서만 사용되고 있으며 이전 솔루션과 마찬가지로 피싱에 대해 노출되어 있다. 매달 전 세계 평균 1만 5천 건의 피싱 웹 사이트가 출현하고 있으며, 국내에서도 2005년 7월 이후 피싱 웹 사이트가 지속적으로 증가하고 있는 추세이다. 또한 피싱을 이용한 인증서 대량 유출 및 현금 인출 사고가 증가하고 있으며, 최근에는 공격 대상이 금융권에서 비금융권으로 확대되어 가고 있다[2]. 이러한 심각성을 고려해 볼 때 본 논문에서 제안하는 OTP를 활용한 피싱 방지 방법은, 전자금융거래 안전성 강화에 크게 기여 할 것이다.

3. 본론

3.1 OTP를 이용한 사용자 인증

기존의 인증서에서 발생했던 인증서 유출과 복제의 문제를 해결하기 위해 도입 되었던 보안 카드 또한 공격 성공 사례가 발생함에 따라 안전성의 문제가 대두되었다. 이를 극복하기 위해 OTP를 이용한 사용자 인증 방안이 도입되어 사용되고 있다.

그림 1 OTP를 활용한 사용자 인증 예:계좌 이체 서비스

그림 2 OTP 이용 사용자 인증

OTP는 사용자와 서버가 공유하는 고유의 비밀 키를 제공하는 장비로서, 이를 이용해 서버는 사용자를 인증할 수 있고, 대부분의 암호 키 노출 문제와 그 공격에 안전한 특징을 가지고 있다. 이를 위해서 사전에 사용자 OTP기기는 서버 쪽과 동기화를 이루고 있어야 한다. 사용자는 로그인시나 중요 서비스 이용 시에 자신의 OTP코드 값을 입력함으로서 서버가 자신을 인증 할 수 있도록 한다.

국내에서는 신한 은행을 포함한 몇 개의 은행이 계좌 이체 등의 중요 서비스에 OTP를 사용 하도록 하고 있다<그림 1>. 해외에서도 국내와 같이 금융 거래 시의 사용자 인증을 위해 사용하는 것뿐만 아니라 로그인 시에도 OTP를 활용하는 시스템을 적용하고 있다. PayPal의 경우 OTP를 도입하여 사용자의 ID, 패스워드 이외에 OTP에서 생성하는 값을 함께 입력해서 로그인 하는 이중 인증(2-factor authentication) 시스템을 도입하였다<그림 2>.

OTP이용한 사용자 인증을 통해 웹 사이트는 합법한 사용자와 트랜젝션의 인증을 이룰 수 는 있으나, 사용자는 이러한 사이트가 피싱 사이트가 아니라는 가정 하에 서비스를 이용하게 된다. 하지만 악의적 사용자가 DNS 하이잭킹이나 IP 스푸핑을 통하여 가상의 피싱 사이트를 만들어 사용자의 중요 정보를 훔침으로서 적합한 사이트가 OTP로 사용자 인증을 하여도 사용자는 <그림 3>과 같이 피싱에 공격을 당할 수 가 있다.

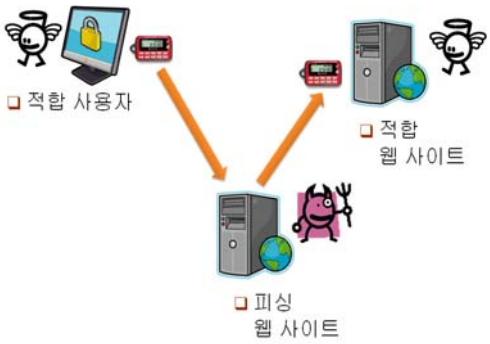

그림 3 피싱 공격에 의한 OTP 취약성

이러한 문제로 사용자는 피싱을 방지하기 위한 별도의 보안 솔루션을 설치해야 하거나 서비스에 가입해야 한다. 문제는 대다수의 사용자가 웹 사이트 이용 시에 어떠한 위험이 있고 어떠한 솔루션을 설치 사용해야 하고 어느 서비스에 가입해야 하는지 잘 모른다는 것에 있다. 이러한 점을 고려했을 때 사용자가 별도의 부가적인 프로그램의 도움 없이 자신이 사용하려는 사이트와 서비스의 진위 여부를 확인 할 수 있는 방법이 필요하다. 즉 자신의 중요한 정보가 피싱 웹사이트에 들어가지 않도록 현재 자신이 보고 있는 웹사이트를 별도의 프로그램과 솔루션의 도움 없이 간단히 진위 여부를 확인 할 수 있는 방안이 필요하다.

3.2 OTP를 이용한 서버 인증 방법

본 논문에서 제안하는 OTP를 활용한 서버 인증 방안을 통하여 사용자는 자신이 받으려고 하는 서비스의 진위 여부를 손쉽게 확인 가능하다. 지금까지의 OTP코드는 서버측에서 사용자 확인을 위하여 주로 사용되었다. 하지만 앞서 기술한 바와 같이 이러한 과정에서 피싱에 의하여 손쉽게 사용자의 개인 정보가 공격자에게 노출 될 수 있는 취약성을 가지고 있다. 하지만 OTP의 코드가 서버와 개인 사용자간 동기화 되는 고유의 비밀 키라는 것을 생각해 보면, 서버가 사용자 확인 과정에서 OTP코드를 사용하는 것뿐만 아니라, 개인 사용자가 서버의 진위 여부를 확인하기 위하여 공유된 OTP를 사용하게 된다면 대부분의 일반적인 피싱 공격을 방어 할 수 있다.

본 논문에서 제안한 OTP를 활용한 사용자 서버 인증방안은 크게 두 개의 방법으로 사용 될 수 있다. 첫째는 사용자가 사이트 로그인 전에 사이트를 인증하는 방법이고, 두 번째는 사용자가 중요 서비스 이용 시 해당 페이지를 인증하는 방법이다.

첫 번째 방법은 사용자가 사이트 로그인시에 해당 사이트가 적합 사이트인지를 확인 하기위해 서버가 보내온 OTP코드의 일부를 사용자 자신의 것과 비교 확인 후 로그인을 하는 것이다. 이러한 과정을 통하여 사용자의 패스워드 정보 등을 피싱으로부터 보호함과 동시에 사용자의 피싱 사이트로의 접근을 막을 수 있다.

두 번째는, 사용자가 카드 결제나 계좌 이체 등의 중요 서비스를 이용하는 데 있어서 사용자가 그 서비스의 진위 여부를 확인 할 수 있도록 서버가 해당 서비스 페이지에 현재의 OTP 코드의 일부를 사용자에게 표시하여 사용자가 자신의 OTP 코드와 비교 하도록 하는 것이다. 이를 통하여 사용자는 해당 페이지가 적합한 사이트에서 보내온 올바른 서비스 페이지라는 것을 확인 할 수 있다.

위의 두 방법을 통하여 사용자는 웹 사이트를 방문하거나, 금융거래와 같은 중요한 서비스를 이용하는 경우에 피싱으로부터 이중으로 보호를 받을 수 있게 된다. OTP를 활용한 사이트와 서비스의 진위 여부를 확인/인증 방안은 별도의 프로그램이나 장치등과 같은 추가적인 비용에 대한 부담과 불편함 없이 피싱 방지를 높일 수 있다는 장점을 가진다.

다음 3.2.1 과 3.2.2 에서는 두 가지 방법에 대한 자세한 설명을 하겠다.

3.2.1 서버 클라이언트 상호 인증 이중 OTP 활용 로그인

사용자 로그인 시 ID 확인과 동시에 서버가 OTP값의 일부를 화면에 표시 해줌으로서 사용자가 패스워드를 입력 전에 사이트의 진위 여부를 확인 하도록 하는 방법이다. 기존의 이중 인증(Two-factor Authentication) 인증 방법과는 다르게 사용자와 서버를 동시에 인증 가능하다.

사용자가 보안이 요구되는 웹 사이트에 방문하여 로그인을 하고자 할 때 사용자가 ID를 입력하고 해당 ID 입력 컨트롤을 벗어나면 ID 값을 AJAX 방식이나 다른 비동기적 방법을 통하여 사용자의 ID정보를 서버로 전송한다. ID정보를 받은 해당 서버는 그 사용자의 OTP 값에 대한 특정 부분만을 전송하게 로그인 창에 바로 표시한다. 사용자는 서버가 보내온 OTP값의 일부와 현재 자신의 OTP 값이 동일하다면, 사용자의 고유 비밀번호나 현재의 OTP 값 또는 두 개를 동시에 입력하여 로그인을 한다<그림 4>. 이러한 과정은 기존의 금융권의 ID를 입력하지 않고 인증서와 인증서 비밀번호만을 넣어서 로그인 하는 경우에도 약간의 프로그램의 수정을 거치어 적용 가능하다.

이러한 절차를 통하여 사용자는 부가 프로그램이나 기타 피싱 방지 솔루션의 설치 없이 해당 웹 사이트의 진위 여부를 확인 할 수 있다. 또한 이 방법은 국내 OTP 통합 센터의 구축과 맞물려, 통합적인 사용자/서버 인증 환경을 구축이 가능 하도록 할 수 있다. 제안된 방안으로 사용자 로그인 과정에서 부터 피싱으로부터 사용자를 보호하여 사용자의 id/pass 노출과 개인 정보 노출을 막을 수 있다.

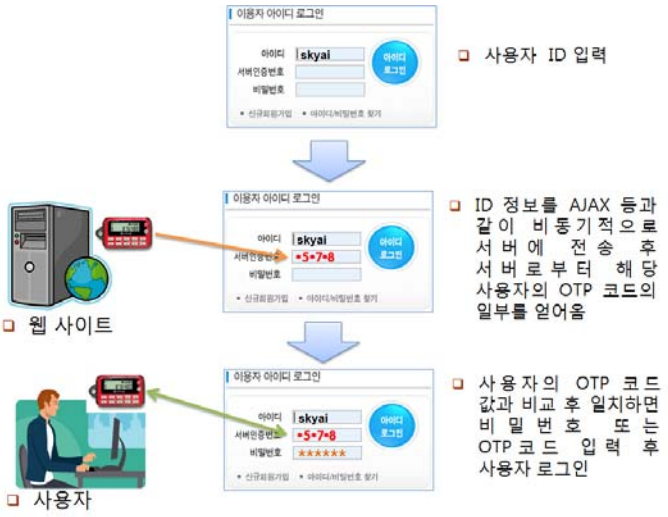

그림 4 OTP 사용 서버 인증 후 사용자 로그인

3.2.2 중요 서비스 OTP 활용 서버 인증

기존에는 금융 결재 및 거래 과정에서 사용자 확인을 위해 OTP를 사용하였으나 피싱 위험에 노출위험이 증가함에 따라, 사용자가 이용하는 중요 서비스에 대한 피싱 방지를 위한 방안이 필요하다.

로그인과정에서 OTP를 활용하여 서버를 인증하는 것과 유사하게 사용자가 금융 결재 등의 중요 서비스를 이용할 때 해당 서비스 페이지의 진위 여부를 확인 할 필요가 있다. 사용자가 중요 서비스 사용 시, 해당 서비스 트랜잭션마다 서버가 OTP 값의 무작위로 특정

부분을 선택하여 화면에 표시해 주고 사용자는 자신의 OTP 값과 비교함으로서 해당 서비스의 진위 여부 확인이 가능하다.<그림 5>

그림 5 중요 서비스 페이지에서 OTP 활용 서버/사용자 상호 인증

<그림 6>에서 보는바와 같이 웹 사이트는 사용자에게 현재 OTP 코드 값의 특정 부분을 랜덤하게 선택하여 화면에 보여 주게 된다. 사용자는 현재의 자신의 OTP 기기로부터 OTP코드 값을 확인하여 서버가 보내온 값과 자신의 값을 비교하여 페이지의 진위 여부를 확인하게 된다. 그 이후에 사용자는 서버가 비워서 보내온 OTP 코드의 나머지 부분을 채우거나 새로운 현재의 OTP 번호를 서버에게 보냄으로서 서버가 사용자 인증을 할 수 있도록 한다. 이러한 과정을 통해 서버와 사용자 모두 상호 인증을 이룰 수 있다.

3.2.1.1 OTP 서버 인증 : 사례 1 – 카드 결제 서비스 형

카드 결제 서비스 형은 사용자가 입력하는 정보의 보안성이 유지 되어야 하고 그 값에 대한 별도의 인증 절차가 있는 경우에 해당 된다. 이러한 경우, OTP를 사용자 인증 보다는 서버 인증에만 사용 하도록 할 수 있다. 온라인 쇼핑몰에서 카드결재를 하는 것이 매우 보편화됨에 따라 개인 사용자가 해당 서비스를 믿고 안심 결재를 할 수 있도록 하는 솔루션의 필요성이 대두 되었다. 현재는 해당 서비스 페이지에 대한 의심 없이 사용자는 카드번호와 안심카드 비밀번호 등의 중요한 정보를 입력하고 있어 피싱의 위험이 높다. 국내 사례와는 그 결재 방법에 따라 차이가 있지 만 미국에서 가장 많은 피싱 대상이 되는 것이 카드 결제 대행 사이트인 Pay-Pal 이다.

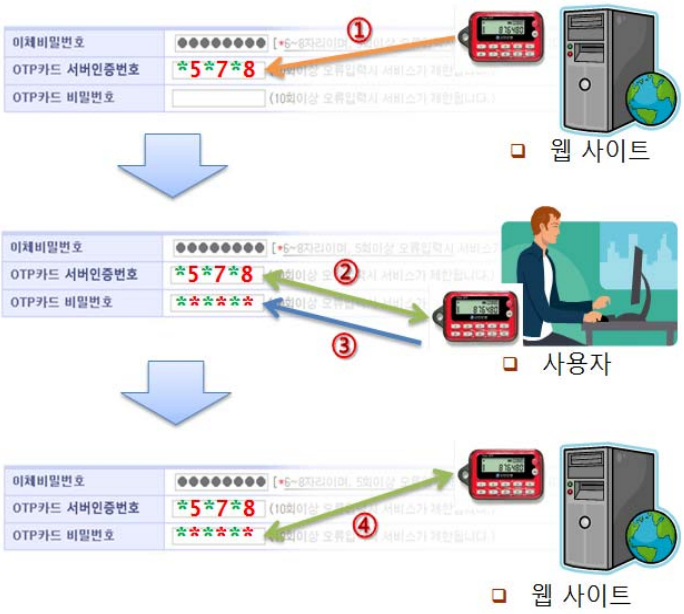

그림 6 OTP 활용 서버 및 사용자 상호 인증 절차

이러한 카드 결제 서비스와 같은 유형의 페이지에서 사용자가 요구 하는 것은 자신이 현재 보고 있는 페이지와 그 서비스가 피싱이 아니어야 한다는 것이다. 현재는 이를 만족하기 위한 어떠한 통합 솔루션이 없으며 개인 사용자가 로컬에 설치한 안티 피싱 솔루션에 의존할 수밖에 없는 실정이다. 이러한 현재의 취약한 환경은 언제라도 악의적인 피싱 공격에 의해 대형의 피싱 사고의 위험성을 안고 있다.

사용자는 카드 결제 페이지 이전에 해당 사이트에서 로그인 과정 혹은 유사한 개인 확인 과정을 거쳤을 것이다. 서버는 사용자에게 카드 결제 페이지 폼을 보여줌에 있어 해당 사용자가 사용하고 있는 OTP 코드의 일부를 보여 주게 된다. 이를 통해 사용자는 자신의 OTP 코드와 비교를 통해 해당 결제 페이지가 적합한 사이트로부터 왔다는 것을 확인 할 수 있다. 그리고 결제와 사용자 인증은 이전 방식과 동일하게 사용자 입력 암호, CVS 코드와 개인인증서를 이용하여 이루어질 수 있다.

3.2.1.2 OTP 서버 인증 : 사례 2 – 온라인 뱅킹 서비스 형

온라인 뱅킹 서비스 형은 OTP 자체가 사용자 인증으로 사용 되는 경우 이다. 만약 사용자가 서버 인증을 위하여 OTP 코드를 요청 하였을 때, OTP 값의 전부가 넘어 오게 되면, 서버측에서 보내온 OTP 값을 공격자가 가로채어 응답 공격(replay-attack) 에 악용될 소지가 있다. 이러한 문제를 피하기 위해서는 서버 측 인증에 사용되는 OTP와 사용자 인증에 사용 하는 OTP의 값이 다르도록 해야 한다.

다른 방법으로는 위에서 예시로 보인 것처럼

서버측에서 OTP의 특정 자리 값만을 보내어 이를 통해 사용자가 서버 인증을 하도록 하고, 별도의 OTP 값 갱신을 할 필요가 없도록 하는 방법이 있다.

4. 제안시스템 보안 수준 비교

우리가 제안하는 시스템은 기존의 시스템과 비교하여 다음[표 1]과 같은 공격 유형에 대응 가능하다.

표 1 제안 시스템과 기존 인증 시스템 보안 수준 비교

	Brute Force Attack, Password Guessing	인증서 복제	키보드후킹, 메모리 해킹, Mal-ware 해킹	DNS 하이잭킹 피싱, IP 스푸핑 피싱, 유사 URL 피싱, 일반적 피싱	Man-in-the-Middle 피싱, 사용자 로컬 시스템 관리자 권한 획득
ID+Password	X	X	X	X	X
인증서	O	X	X	X	X
인증서 + 보안카드	O	O	X	X	X
OTP - 사용자 인증	O	O	O	X	X
OTP - 사용자+서버 인증 (제안 시스템)	O	O	O	O	X

5. 결론

본 논문에서는 사용자를 피싱 환경으로부터 보호하기 위하여 OTP를 활용하여 사용자 인증뿐만이 아니라 서버 인증까지 하는 방법을 제안하였다. 이러한 방법은 클라이언트에서 피싱 방지를 위해 어떠한 부가적인 프로그램을 설치할 필요가 없으며, 매우 간단한 절차로서 사용자의 보호가 가능하다. 본 논문에서 제안한 방법은 OTP 도입 할 수 있는 어떠한 사이트 및 서비스에서 거의 시스템의 변경 없이 도입이 가능하다는 장점이 있다. 하지만 금융권 메모리 해킹 사례에서도 확인 할 수 있듯이, 고도의 악의적인 사용자가 PC의 권한을 획득 후 악성 프로세스를 통하여 메모리 접근 감시 및 조작을 수행하면 대응하기 어렵다는 단점이 있다. 하지만 이러한 문제는 사용자의 시스템 환경자체가 최소한의 보안 요구 수준을 이루고 있지 못하고 말할 수 있다.

향후 연구에서는 사용자의 환경이 최소 보안 수준 요구에 못 미치어 해당 시스템이 침해당했을 때에도 OTP 코드 값의 서버측 사용과 클라이언트측 사용을 모니터링 하여 이중으로 사용되거나 변조 되어 사용되지 않도록 하는 방안에 대한 연구가 필요하다.

6. 참고문헌

[1] 코리아 헤럴드, 1회용 비번생성 OTP카드 7월 서비스… 해킹 봉쇄, http://www.heraldbiz.com/SITE/data/html_dir/2007/04/24/200704240152.asp, 2007

[2] 아니뉴스 , 안티 피싱 주력할것..마크 게펜 EMC RSA 정보보안사업부 이사, http://www.inews24.com/php/news_view.php?g_serial=288965&g_menu=020200, 2007

[3] 디지털 데일리, 일회용비밀번호(OTP) 기술 표준화 추진된다, http://www.ddaily.co.kr/news/news_view.php?uid=28985, 2007

[4] e컴퓨터월드, 위험천만한 OTP 통합인증 서비스, http://www.com-world.co.kr/news/articleView.html?idxno=8876, 2007

[5] Tamebay, HSBC says “No” to PayPal style security keys, http://www.tamebay.com /2007/01/5-paypal-security-key-gives-false-hope.html, 2007

[6] Tamebay, $5 PayPal security key gives false hope to stop phishers, http://www.tamebay.com/2007/01/5-paypal-security-key-gives-false-hope.html, 2007

[7] The Anti-Phishing Working Group, http://www.antiphishing.org, 2007.

[8] W. Liu et al., "Phishing Webpage Detection," Proc. 8th Int'l Conf. Document Analysis and Recognition, pp. 560–564, IEEE Press, 2005,

[9] A.Y. Fu, W. Liu, and X. Deng, "EMD-based Visual Similarity for Detection of Phishing Webpages," presented at the Int'l Workshop on Web Document Analysis, 2005.

[10] W. Liu et al., "Detection of Phishing Webpages based on Visual Similarity," Proc. 14th Int'l World Wide Web Conf., pp. 1060–1061, ACM Press, 2005,.

[11] PhishTank, http://www.phishtank.com, 2007.

[12] Gregg Tally, Roshan Thomas and Tom. Van Vleck, McAfee Research, Anti-Phishing: Best Practices for Institutions and Consumers, January 01, 2005.

[13] Symantec Phish Report, www.phishreport.net, 2007