情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

MITM 공격과 리버스 엔지니어링을 이용한 OTP 적용환경의 취약점 연구*

강 병 탁,† 김 휘 강‡
고려대학교 정보보호대학원

A study on the vulnerability of OTP implementation by using MITM attack and reverse engineering*

Byung-Tak Kang,† Huy Kang Kim‡
Graduate School of Information Security, Korea University

요 약

OTP (One Time Password) 인증방식은 국내 금융거래나 포털 및 온라인게임과 같은 인터넷 서비스에서 계정 보안을 위한 수단으로 널리 이용되고 있다. OTP 는 국내 금융 거래 시 1등급 보안수단으로 지정될 만큼 보안성을 인정받고 있으나, OTP 인증을 구현한 서비스를 대상으로 한 다양한 해킹 방법들 역시 존재한다. 이러한 해킹 방법들은 대부분 OTP 알고리즘 자체의 결함을 찾아내어 공격하기보다는 OTP 인증방식을 구현한 방식이나 환경에 따라 발생 가능한 취약점을 이용하는 것이 일반적인데, 이 논문에서는 MITM (Man-in-the-Middle) 공격과 같이 기존에 알려져 있던 OTP 기반 인증방식을 대상으로 한 해킹기법 및 리버스 엔지니어링(Reverse Engineering)을 이용한 해킹 방법들에 대해 논의하고, 이에 대한 해결방안을 제시하도록 한다.

ABSTRACT

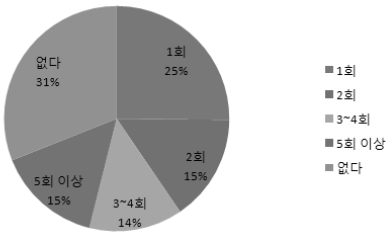
OTP (One Time Password) is widely used for protecting accounts on Internet banking, portal services and online game services in Korea. OTP is very strong method for enforcing account security but there ar*e several ways for exploiting vulnerabilities caused by implementation errors. These attacks can work because of the weakness from OTP enabled system's vulnerabilities, not for OTP's algorithm itself. In this paper, we present the known attack scenarios such as MITM (Man-in-the-Middle) attack and various reverse engineering techniques; also, we show the test result of the attacks and countermeasures for these attacks.

Keywords: OTP, Malware, Reverse Engineering, MITM attack, Internet Banking

I. 서 론

최근 인터넷뱅킹, 포털 서비스, 온라인게임서비스 등 다양한 인터넷 서비스 제공자들이 고객들의 계정 정보를 보호하기 위해 많은 보안 메커니즘을 적용하며 계정도용방지에 노력을 기울이고 있지만, 사용자 PC 에 설치되는 신종 키로거(keylogger)나 지속적으로 발전하는 해킹 방법에 의하여 계정정보가 유출되는 위

접수일(2011년 3월 12일), 수정일(2011년 6월 4일), 게재확정일(2011년 8월 1일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1001-0004)
† 주저자, window31@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr



〔그림 1〕 온라인 게임 이용자의 69%가 해킹 피해를 경험 (신뢰도 95%)

험은 여전히 계속되고 있다. 실제로 아래는 M온라인 게임 보안서비스 설문조사 결과이며 (설문기간: 2010/06/10 ~ 2010/08/01, 총 19732 명 설문응답), 계정 도용의 피해 경험이 있느냐는 질문에 설문 유저의 69% 가 1회 이상 해킹을 당했다는 결과를 보여주고 있다〔1〕. 또한, 이 설문조사를 통해 알 수 있었던 점 중 주목할 만한 사항으로는, 여러 계정보안을 위한 메커니즘 중 가장 견고하며 안전한 보안 장치로 알려진 온라인게임사에서 제공해주고 있는 OTP (One Time Password) 서비스를 사용해도 해킹을 막을 수 없다고 응답한 경우가 10% 나 되었다는 점이다.

본 논문에서는 현재 인터넷 서비스 상에서 심각한 위험이 되고 있는 계정 도용의 현황을 분석하여, 어떠한 위협요소가 존재하고 있는지를 살펴보고 이에 대한 대응방법을 기술하였다. 특히, OTP가 구현된 서비스 상에서 발생 가능한 해킹방법에 대하여 초점을 맞추어, 관련 해킹 시나리오를 도출하고 실험을 통하여 계정도용이 충분히 발생할 수 있음을 증명해 보았다. 2장에서는 국내 서비스를 중심으로 현재 각 기업들에서 제공하고 있는 고객 보안수단들의 핵심 요소와 취약점들에 대해 정리하여 OTP 해킹에 대한 문헌연구와 함께 현재 보안장치의 취약점을 지적하였다. 3장에서는 현재까지 가장 안전한 계정보안 수단으로 여겨지는 OTP 의 동작 원리와 더불어 OTP 내에 내재된 취약점을 제시하였다. 4장에서는 OTP 데이터의 탈취 시나리오를 작성하여 실제 OTP 값을 변조/공격한 결과를 기술했으며, 5장에서는 4장에서 기술된 시나리오를 토대로 국내에서 현재 OTP가 적용되어 서비스 되고 있는 20여개 주요 웹사이트에 실제 해킹 테스트를 수행하였다. 그리고 6장에서는 본 논문에서 제기한 문제점에 대한 해결방법과 개선책에 대한 내용 그리고 기존 대안과의 비교 과정을 기술하였다.

II. 관련 연구 및 동향

본 장에서는 온라인 서비스에서 고객들의 계정보안을 향상시키기 위해 제공되는 주요 보안수단에 대해, 특히 사용자 인증 기법을 위주로 살펴보며 각각 어떤 취약점이나 제약성이 있는지 조사하였다. OTP가 타 보안수단에 비해 어떤 점에서 보다 안전한 보안수단인지를 정리해 보았고, OTP 해킹 방법에 대하여 기존에 알려져 있던 여러 방법들과 함께, 이 논문에서 다뤄질 OTP 해킹은 지금까지의 사례들과 어떠한 차이점이 있는지 정리하였다.

2.1 타 보안수단과의 비교

사용자 인증 기법에는 크게 세 가지의 분류로 나눌 수 있다. 첫 번째로 패스워드 입력 방식을 변형하거나

〔표 1〕 사용자 인증 기법 별 비교 (O: 대응 가능, X: 대응 불가, △: 부분 대응)

		사용자 편의성			보안위협		
		사용자 불편	설치비용	사용자부주의	스니핑	키보드로깅 /화면캡쳐	피싱
범주 1	ID패스워드 방식	낮음	낮음	낮음	X	X	X
	가상키보드	보통	낮음	낮음	O	△	X
	사전질의응답 방식	보통	보통	보통	X	O	X
	보안카드	보통	높음	보통	O	O	△
	이미지검증 방식	보통	보통	보통	O	X	△
범주 2	비대칭키방식	보통	높음	낮음	O	O	X
	대칭키 방식	보통	높음	낮음	O	O	X
범주 3	단방향 방식	낮음	높음	보통	O	O	X
	양방향 방식	보통	높음	보통	O	O	X
범주기타	키보드보안	보통	낮음	낮음	O	O	X

부가 정보를 입력받는 단순패스워드 기법, 두 번째로는 소프트웨어, 하드웨어 토큰기법, 세 번째로는 별도 채널 사용 기법이다. 이런 범주를 1,2,3 으로 나누어 봤을 때, 〔표 1〕 에서는 범주에 따른 인증 기법들을 비교하고 있다(단, 키보드보안의 경우는 인증 기법으로 분류하기 모호하므로 "기타 범주"로 정의) 〔2〕 〔3〕 〔4〕 〔5〕 〔6〕 〔7〕.

〔표 1〕의 세로축은 분류 범주에 따른 인증 기법들을 나타내며, 가로축은 사용자 편의성이 영향을 받는 부분과 대표적인 보안 위협을 보여주고 있다. 사용자 불편은 사용자 인증 방식을 사용하며 조작이나 동작, 운영 등에 있어 복잡성을 의미하며, 설치비용의 경우는 소프트웨어나 하드웨어의 설치 및 유지에 대한 복잡성을 의미한다. 사용자 부주의의 경우는 해당 인증 방식을 사용자가 관리할 때 부주의나 관리 소홀 등으로 발생할 수 있는 문제들을 의미한다.

범주1의 ID패스워드 방식은 가장 일차적인 인증수단인 ID와 패스워드를 이용한 인증방법이며, 미리 정의된 ID와 패스워드를 비교하여 인증하는 방식을 말한다. 같은 범주에 있는 가상키보드는 역시 입력 수단이 물리적인 키보드에서 화면에 만들어진 비주얼 키보드로 옮겨진 것으로, 사전에 정의된 패스워드를 입력하는 인증 방식이라는 점에서는 ID패스워드 방식과 동일하다. 사전질의응답 방식은 역시 사전에 등록된 질의/응답에 대하여 로그인시 질의 내용이 요구되면 응답하는 방식이다. 보안카드나 이미지검증 방식도 유사한 원리로 모두 고정된 챌린지(challenge)/리스폰스(response)를 기본으로 하거나 그것을 응용한 기능에 해당된다. 대표적인 것으로 캡챠(CAPTCHA)가 있다 〔8〕.

범주2의 대칭키 방식은, 통신하는 양자 간에 동일한 키를 분비하여 키로 암호화 또는 메시지 인증 코드(MAC) 연산을 수행하여 인증하는 방식이며, 이 논문에서 다루고 있는 OTP가 여기에 해당한다. 비대칭키 방식은 통신하는 양측이 개인키와 공개키를 쌍으로 분배하고 자신의 개인키로 서명하여 보내면 공개키로 그 내용을 확인하는 형태가 되며, 대표적인 것으로 공인인증서 방식이 있다. 국내 게임포털들에서는 PC 등록제라는 물리적인 하드웨어 정보를 이용한 기기인증방식도 존재한다. 해커가 물리적으로 원래의 소유주의 PC에 접근할 수 있지 않는 한, 원격의 다른 PC에서 도용된 계정으로 로그인한다는 점에 착안하여 사용자가 지정한 PC, 자신의 집 PC 또는 노트북 등을 등록해 놓고 그 PC 가 아닌 다른 곳에서 로그인을 할 수 있게 처리하는 시스템이다 〔9〕.

범주 3은 별도채널을 사용하는 방식으로 두 가지를 제공한다. 단방향 방식은 이동 통신 단말기나 다른 응용 프로그램을 통하여 일회용 패스워드를 수신한 뒤, 브라우저를 이용하는 방식이며, 양방향 방식은 단방향 방식을 좀 더 응용한 것으로, 별도의 채널로 비밀값을 수신한 뒤, 그것의 요청에 대한 내용을 확인 및 응답한 후에 거래가 완료되는 방식이다. 대표적인 것으로 전화승인서비스 같은 장치가 있다 〔10〕. 거래내역을 출력하고 이 장치를 통해 승인하도록 하는 방법이다. 계좌이체 승인단계에서 ARS 시스템을 통해 사용자에게 전화를 걸어 거래내역을 확인시켜주고, 거래를 승인하거나 취소할 수 있게 되어 있다. 게임 포털 쪽에서도 유사한 서비스로 mControl 이라는 알림서비스가 있다 〔11〕. 게임 로그인을 하였을 때, 휴대폰으로 접속시간, 계정, 서버명을 알려주며 휴대폰으로 강제 종료시킬 수 있는 서비스까지 제공한다. 마지막으로 범주 기타는 인증 분류에 넣기는 모호하지만 계정도용 방지 솔루션 중 하나로 취급되고 있어 추가한 범주로, 키입력 스니핑 등을 방지하는 기능을 제공한다. 또한, 키보드 보안 솔루션의 결함을 보완한 대안으로 E2E (End to End) 라는 기능이 최근 구축사례가 늘고 있다 〔12〕. 입력값을 보호하는 것을 넘어서서, 입력값을 암호화 시켜서 서버로 전송시킬 때까지 보호하는 방식이다. 네트워크 구간 스니핑을 방지하기 위한 방법 중 하나로 제시되고 있다 〔13〕.

범주1의 지정된 ID패스워드 방식은 스니핑 공격(sniffing attack) 〔14〕 등에 취약하며, 가상키보드는 화면캡쳐를 하여 전송하는 기능이 있는 악성코드에 의해 공격을 받을 수 있다. 사전질의응답 방식은 "당신의 애완동물 이름은?" 등의 질문과 답변을 미리 등록시켜두고, 적절히 답변할 수 있는가를 확인하는 방식이나, 어느 웹사이트에 접속해도 질문들이 유사하고, 일부 질문들은 답변이 쉽게 예측할 수 있어서 사회공학적 공격이나 브루스포스에 의하여 예상답변들을 무차별적으로 대입하는 방식에 의해 공격될 수 있다. 보안카드나 이미지검증 방식의 경우 MITM 으로 공격하는 것이 가능하며, 공인인증서의 경우는 인증서 복사나 사용자의 이동성에 제약을 준다. 그리고 이 방식들 중 클라이언트 단에 적용되는 보안 솔루션들은 각종 메모리 해킹 공격이나 스니핑 공격, 리버스 엔지니어링(Reverse Engineering)에 노출되어 있기 때문에 해커가 보안솔루션들의 코드를 분석하여 사용자 계정이 입력되는 메모리 주소나 처리하는 함수를

찾아낼 수 있고, 계정을 탈취할 수 있는 취약점이 존재한다 [15] . 그러나, OTP 는 생성된 OTP값을 입력 시 키보드보안으로 입력단계부터 보호되고 있고, 별도 채널을 사용하는 등 투팩터 인증으로 보호되고 있어 리버스 엔지니어링의 영향을 크게 받지 않기 때문에 계정보안에 가장 강한 인증방식을 제공하는 것으로 알려져 있다.

2.2 OTP의 장점과 단점

[표 1] 에서 볼 수 있듯이, 계정도용방지를 위해 쓰이는 각 보안메커니즘 중에서 보안성이 가장 높은 수단은 OTP 다. OTP 는 로그인 할 때마다 해당 세션에서만 사용할 수 있는 1회성 패스워드를 생성하는 보안 시스템이다. 1회성 패스워드를 생성하고 정합성을 유지하기 위해서는 OTP서버와 OTP생성단말 사이에 동기화가 필요한데, 방식에 따라 이벤트동기화 방식(Event-based Synchronization), 시간동기화 방식(Time-based Synchronization), 그리고 이 두 방식을 혼용하는 하이브리드(Hybrid) 방식이 있으며 시간동기화 방식이 가장 보편적으로 쓰이고 있다 [16] . 보통의 패스워드는 같은 값이 오랜 기간 동안 반복적으로 사용되기 때문에, 사용자가 관리를 소홀히 할 경우 언제든 유출될 수 있으며, 또 사용자가 아무리 주기적으로 패스워드를 변경한다 하더라도 해커가 계정을 탈취해간 그 직후에 변경 작업이 이뤄지지 않는다면 역시 위험에 빠지는 문제를 내포하고 있다. 하지만 OTP 값은 한번 사용한 세션이 끝나면 즉시 폐기되기 때문에 재사용이 불가능하여 사실상 해킹이 발생하기 어려운 솔루션이다. 또한 생성된 OTP 값을 투펙터인증(Two-Factor Authentication)의 효과가 유지될 수 있도록 SMS발송, 휴대폰OTP, 하드웨어방식토큰과 같은 다양한 방식을 이용하여 전송한다 [17] [18] [19] [20] [21] [22] .그리고, OTP 에서도, 키보드보안솔루션에서 아직 탐지할 수 없는 키로거를 이용하여 키 스니핑을 할 경우, 입력된 값이 유출될 수 있다는 문제는 제기되고 있지만, 실제로 OTP 를 인증할 수 있는 유효시간은 보통 60초 정도로 매우 짧기 때문에 유출되었다 하더라도 공격이 성공할 확률은 낮다는 연구 결과가 나와 있다 [23] .

하지만 OTP 를 대규모 고객들에게 보안서비스화 하여 제공할 경우에는 보안성을 떨어뜨릴 수 있는 제약사항에 부딪히게 되는데, 예를 들어, 생성된 OTP의 유효시간을 최대한 짧게 유지하는 정책을 유지하기 어렵다. 유효시간의 범위를 60초 정도로 해도, 컴퓨터 사용에 익숙하지 않은 고연령층에서는 OTP 에 대한 이해의 부족이나 타이핑속도의 문제로 제한된 시간 내에 입력을 하지 못하여 인증에 실패하는 경우가 발생할 수 있다. 즉, 기밀성을 높이기 위해 엄격한 기준을 적용할 경우 정상적인 이용자라 하더라도 인증에 실패하는 비율이 증가하게 되는데, 전체 고객수가 10만 명 이상인 대규모서비스라고 할 경우, 사용자 입력 에러율이 0.1%만 되어도 무시할 수 없는 규모가 되어, 고객문의응대의 증가를 유발하게 되어 이는 결국 비용상승으로 이어지게 된다. 이런 현실적인 문제들로 인해 입력시간이 약간 초과해도 인정될 수 있도록 유효시간을 충분한 길이로 설정하는 경우가 발생하게 되므로, OTP를 구현하고 서비스를 하는 과정에서 보안성이 취약해지는 문제를 유발하게 된다. Citibank OTP 해킹 사건의 경우는 유효시간이 3분 이상이었으나 이같이 여유 있는 시간 간격에 대한 취약점이 지적되면서 국내에서는 30초까지 시간을 단축한 사례가 있었다 [24] . 하지만 결국 현실적인 시간 간격을 고려하여 60초라는 시간이 보편적으로 쓰이고 있다.

2.3 알려진 OTP 해킹 방법

OTP의 높은 보안성에도 불구하고, 다양한 취약점이 제기되어 왔으며 해킹을 할 수 있는 시나리오들이 다수 알려져 있다. 이 절에서는 알려진 OTP 해킹 방법에 주로 거론되는 MIT-X (Man-in-the-X) 부류의 공격방법을 모델링하고, 과거에 논의되던 OTP 해킹방법에는 어떤 것들이 있는지 비교하였다. 그리고 해당 분류를 통해, 이 논문에서 제시하려는 해킹 기술에 대해 정의하였다.

MITM (Man-in-the-Middle) 공격은 데이터가 오가는 접속 경로 중간에서 정보를 탈취하여 이용하는 것을 말하며 [25] . MITB (Man-in-the-Browser) 공격은 웹브라우저에 악의적인 프로그램을 설치하여 해킹을 하는 것을 의미한다. 주요 원리는 사용자의 문서를 변조하는 방법으로, 계좌번호나 패스워드 등 사용자가 주요 정보를 입력하는 페이지를 같은 사이트에 가짜 폼으로 만들어 두고 사용자의 입력을 기다리는 방식이다. MITPC (Man-in-the-PC) 공격은 운영 체제의 취약점 또는 하드웨어 환경을 악용한 것으로 키입력 및 마우스 로깅, 화면캡쳐에서부터 메모리 변조까지 운영체제 기반에서 사용자가 액세스하는 모든 경로가 공격 대상이 되는 방식이다 [26]

〔표 2〕 공격 방법 비교

공격 방법	공격 위치	예제
MITM (Man-in-the -Middle)	접속 경로, 접속 통로	네트워크 구간 공격, 중간자 공격
MITB (Man-in-the -Browser)	웹 브라우저	인터넷 익스플로러, BHO, 자바스크립트
MITPC (Man-in-the-PC)	PC 환경	키보드, 마우스 로깅, 화면캡쳐, API 모니터링, 코드 변조

〔27〕. OTP 적용환경을 해킹하는 방법에는 이러한 개념을 여러 가지로 혼용하여 공격하는 방식으로 이루어진다.

2.3.1 피싱과 결합된 MITM 공격

MITM 공격은 OTP 해킹에 가장 많이 거론되는 내용으로, 공격자가 사용자의 PC 해킹 등을 통하여 공인인증서를 탈취하고, 피싱 사이트 개설 후 사용자의 각종 금융 비밀정보를 알아내어 OTP 로그인을 할 때마다 MITM 공격을 수행하면 OTP 를 사용하더라도 해킹이 가능하다는 이론이다. 실제로, 2005년 11월에 Swedish Internet Bank에 OTP 시스템을 노린 피싱 공격이 등장하여 인터넷뱅킹 웹사이트를 한시적으로 폐쇄한 사건이 있으며, 2006년 7월에는 Citibank의 Citibusiness 서비스와 흡사하게 제작한 피싱사이트를 통해 사용자 계정, 패스워드, OTP 값을 훔쳐 실시간 MITM 공격을 한 사례가 있다〔28〕〔29〕. 또한, 안티바이러스 개발사에서도 유사한 부분을 지목하여, 시만텍 연구소에서 보고한 BankSlient 와 같은 악성코드의 출현에서도 이런 MITM 공격에 대한 취약점이 존재한다는 연구결과를 가지고 있다 〔30〕.

2.3.2 MITB 공격

OTP 해킹으로 또 하나 거론되는 것은 MITB (Man-in-the-Browser) 공격이다. MITB 공격은 피싱 사이트가 존재해야만 하는 MITM 공격과는 달리 별도의 가짜 사이트 없이 사용자의 웹브라우저에 악의적인 프로그램을 설치하는 작업이 필요하다. 계좌번호나 패스워드 등 사용자가 주요 정보를 입력하는 페이지를 같은 사이트에 가짜 폼으로 만들어 두고 사용자의 입력을 기다리며. 사용자는 피싱 사이트가 아니므로 의심 없이 공격자가 원하는 내용으로 거래를 진행한다는 점이 핵심이다 〔31〕. 이와 같은 방법은 인터넷 익스플로러(Internet Explorer) 의 BHO (Browser Helper Object)를 악성코드로 만들어 설치하는 방법이나, 자바스크립트(Javascript)를 이용하여 가짜 페이지를 진짜 인터넷뱅킹 사이트나 게임 사이트에 덧씌우는 방법으로 구현할 수 있다. 더구나 사용자들에게 제공되고 있는 보안 솔루션은 주로 프로세스 단위의 악성 코드를 검사하며, 실제 거래내용이 담긴 HTML 문서 자원은 보호하거나 검사하지 않는 경우가 많기 때문에 MITB 공격이 더욱더 논란이 되고 있다〔32〕. 이처럼 웹브라우저에 악성코드가 상주하여 공격할 수 있다는 방안은 Augusto 에 의하여 처음 발표되었으며 2007년부터 Guhring 에 의하여 MITB 공격으로 불리기 시작하였다 〔33〕.

2.3.3 MITPC + MITM 공격

본 논문에서 제안하는 공격 형태는 MITPC (Man-in-the-PC) 공격방식과 MITM 공격방식을 혼용한 형태라고 정의할 수 있다. 즉, MITPC 공격을 통해 PC 에 입력되는 ID, 패스워드 등의 각종 개인정보를 가로챈 뒤, 실시간으로 MITM 공격을 통해 해킹을 시도하는 방식이다. 특히 인터넷뱅킹이나 게임 포털 등은 키보드 보안 솔루션 등으로 보호되고 있기 때문에 일반적인 방법으로는 키입력 스니핑이 불가능하지만, 리버스 엔지니어링을 이용하여 코드 변조나 API 후킹을 시도하고(MITPC 공격) 계정을 탈취할 수 있다. 그리고 입력시간 제한이 있는 OTP 값을 즉시 사용하기 위해 MITM 공격을 결합하여 탈취한 정보를 즉시 해커에게 전송하는 공격 방법이다. 이렇게 MITPC 공격과 MITM 공격을 결합한 방법으로 OTP 적용환경을 대상으로 한 새로운 해킹 시나리오를 작성할 수 있다.

III. OTP 동작원리와 해킹을 위한 기반지식

2장에서 살펴본 것처럼, OTP 의 보안성은 높지만 실제 서비스에 구현하는 과정에서 파생될 수 있는 보안상 취약점이나, MITM, MITB, MITPC 공격과 피싱을 연계한 공격에 취약할 수 있음을 알 수 있다. 또, 이러한 피싱과 연계된 실시간 MITM 공격에 대응하기 위해 CAPTCHA 와 OTP를 동시에 사용하

여 문제를 해결하려 한 연구도 제안되었다 [34].

이 장에서는 기존에 알려진 방식 외에도 OTP를 해킹할 수 있는 시나리오를 제시하고, 어떤 기법들을 이용하여 OTP 값을 탈취할 수 있는지 기술하였다. 피싱을 이용한 공격방법이나 기존 CAPTCHA 등의 대응방법과는 달리 OTP 를 해킹할 수 있는 쿼리 스니핑(Query sniffing)이라는 새로운 방법과, 리버스 엔지니어링을 통하여 OTP 값을 탈취, 조작할 수 있는 공격방식을 소개한다.

3.1 OTP 의 기본 구조

OTP 생성절차는 다음과 같다. 먼저 사용자가 인증요청을 하면 OTP 토큰에는 자동으로 새로운 값이 생성된다. 사용자는 이 입력정보를 서비스 서버(게임, 뱅킹 등)를 통해 OTP 인증서버로 전달해 주고, OTP 인증서버에서 사용자가 입력한 OTP 값과 인증서버에서 계산한 OTP 값이 동일한지 확인한다. 그리고 사용자가 입력한 값이 정상이라면, 인증에 성공한 것이며 사용자에게 이후 서비스를 진행할 수 있도록 처리해 준다.

3.2 wininet.dll

wininet.dll 은 Win32 가 제공하는 고수준의 네트워크 라이브러리다. HTTP, FTP 는 물론 HTTPS까지 지원하며, Win32 API 형태로 마이크로소프트에서 제공되므로, 인터넷 프로그래밍을 위한 인터페이스를 가지고 있다. InternetOpen(), InternetConnect(), HttpOpenRequest(), HttpSendRequest() 등의 API 를 사용하면 HTTP 쿼리를 만드는 프로토콜을 제작할 수 있다.

3.3 입력값은 웹 쿼리로 사용

사용자는 HTTP을 이용하여 URI-요청을 통해 원하는 웹 서비스 자원(예를 들면 /bbs/board.asp)에 입력값(name=notice&no=337)을 전송하게 된다. 그리고 웹 브라우저에서는 URL 에서 웹 어플리케이션의 위치와 해당 웹 어플리케이션의 입력값이 POST 또는 GET 방식으로 전달된다. 이 때 OTP 에서 입력되는 값도 마찬가지로 HTTP POST/GET 방식으로 전달되며 name=notice&no=337&otp=123456 등으로 입력값이 생성된다. 그리고 이 쿼리는 wininet.dll 의 HttpSendRequestA/W 를 통해서 네트워크로 전달되는 형태를 가진다.

3.4 HttpSendRequestA/W 후킹

따라서 wininet.dll 의 HttpSendRequestA/W 를 후킹(hooking)하여 모니터링 한다면, HTTP 로 통신하는 모든 쿼리를 감청할 수 있다. 아래 제시되는 쿼리를 보면 id= pwd= otp= 등의 값이 모두 노출되어 있기 때문에 아이디나 패스워드는 물론 OTP 내용까지도 스니핑이 가능하다. 그리고 wininet.dll 에서 만들어지는 이 쿼리는 유저 클라이언트 내부에서 발생하는 일이기 때문에, SSL(Secure Socket Layer)를 적용하여 HTTPS로 통신하거나, 별도의 플러그인을 이용하여 네트워크 단에서의 패킷 암호화 처리를 하는 것과는 무관하게 취약해 질 수 있게 된다. 즉, 이 영역은 암호화 직전의 평문 쿼리 상태이므로 통신 채널 암호화 작업으로는 해결이 불가능하다. 또한 키보드 보안 솔루션은 입력값을 보호하는 솔루션이므로, 쿼리 단에서 전달되는 값을 스니핑 하는 것은 방지하지 못한다. 따라서 키보드 보안 솔루션이 적용되어 있어도 아이디, 패스워드, OTP값을 쿼리에서 가로채는 것을 보호할 수 없다[표 3].

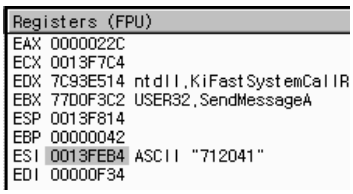
http%3A%2F%2Fxxxxxx.com&fail_url=&loginsite=&site_id=31&adult_yn=N&encoding_type=utf-8&ukey=1BB7E5F2937203480D408B5196E9AC3B9DDF487E636EA15426FAEABDAFB00A6908F2069ECB5FA6C7B618E4C68C5F37C2900DB07DE9A0CACEC7300A6DBD342A83&game_id=13&**id=window31&pwd=xxxxx&otp=12345678**

3.5 코드 후킹 (code hooking)

wininet.dll을 변조하여 쿼리를 스니핑 하더라도, 만약 쿼리 암호화가 되어있는 상태라면 쿼리를 후킹할 수 없다. 국내 게임포털과 인터넷뱅킹 사이트들을 대상으로 조사해본 결과, 대부분의 게임포털사이트들의 경우에는 쿼리가 노출되어 있지만, 인터넷뱅킹 같은 경우는 그보단 한 단계 더 암호화 되어 있어서 쿼리 단에서는 OTP 값이나 ID,패스워드를 추출해낼 수 없다. 따라서 wininet.dll 같은 시스템 DLL을 변조하는 것이 아닌, 인터넷뱅킹 모듈이나 키보드보안 모

〔표 3〕 스니핑 방법에 따른 보안 가능 영역

	키보드 보안	SSL
차단원리	IDT 후킹 등의 입력값 보호	통신채널 암호화
키 스니핑	차단	차단하지 못함
패킷 스니핑	차단하지 못함	차단
쿼리 스니핑	차단하지 못함	차단하지 못함



〔그림 2〕 리버스 엔지니어링으로 추출 가능한 OTP 값

듈을 직접 변조하는 코드 후킹 방식을 사용할 수 있다. 키보드보안 솔루션 등이 아무리 보호하고 있어도, 보호를 하기 위해서는 키보드보안 모듈이나 DLL 등으로 입력된 값을 전달해야 한다. 키입력 단에서는 메시지 후킹 등의 스니핑으로 그 값을 가져갈 순 없지만 일단 메모리 들어온 이후에는 eax, ebx, ecx, edx 등의 메모리, 레지스터 안에서 OTP 값이 전달되고 있으므로 리버스 엔지니어링을 통하여 입력값 탈취를 진행할 수 있다. 클라이언트 단에서 입력되는 값은 아무리 높은 보안성으로 보호하고 있어도 결국 리버스 엔지니어링이 가능하기 때문에 어떠한 형태로든 입력값 추출은 가능하다〔15〕.

IV. OTP 탈취 시나리오

OTP 가 높은 보안성을 갖는 이유는, 첫번째로 사용자가 생성한 OTP 값은 일회용이기 때문에 한번 쓰고서는 버릴 수 있다는 점이며, 두번째로는 유효시간이 60초 정도로 짧기 때문에, 유출이 되어도 60초라는 제한된 시간 내에 해커가 원래 사용자보다 먼저 로그인을 해야 한다는 제약조건이 있어서 성공확률이 무척 낮기 때문이다. 하지만 이번 장에서는 이러한 기존의 전제사항들을 벗어나, OTP 값을 탈취하여 실제로 사용할 수 있는 해킹 시나리오를 작성하였다. OTP는 크게 분류하여 인터넷뱅킹이나 게임포털에서 주로 사용하는데 두 플랫폼이 다르기 때문에 각 사이트에 맞는 시나리오를 별도로 구성하였다. 먼저 게임포털 기반 하에서 앞 3장에서 다룬 HTTP 를 통한 네트워크 단 전송과 이를 위해 클라이언트 단의 wininet.dll 를 통한 함수 호출 시 OTP 값을 탈취하고 게임아이템 탈취 등 실제로 해킹을 할 수 있는 시나리오를 작성하였다. 그리고 인터넷뱅킹 기반 하에서는 먼저 공인인증서를 탈취하고, 인터넷뱅킹 모듈의 코드 후킹을 통하여 OTP 값을 탈취, 변조할 수 있는 시나리오를 구성해 보았다.

4.1 게임포털 사이트 환경

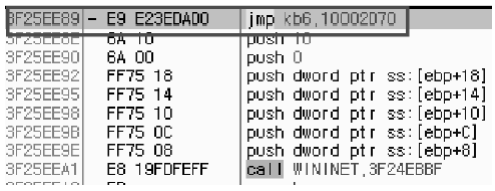
사용자 PC 에서 입력되는 OTP 값을 탈취하기 위해서는 우선 해당 PC가 웹브라우저 상에 입력되는 값을 탈취해 내는 악성코드에 감염되어 있음을 전제조건으로 한다. 이 악성코드는 웹브라우저인 인터넷 익스플로러 후킹, 문자열 파싱(parsing), 탈취한 정보 전송, 정상사용자의 입력방해의 기능을 가지고 있으며 각 기능들이 순차적으로 동작한다.

4.1.1 웹브라우저 후킹

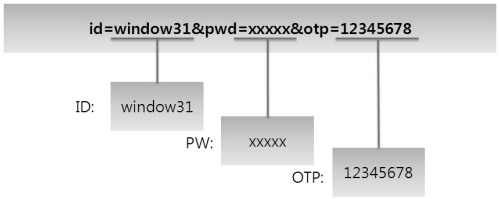
HTTP 쿼리가 평문 상태로 전달되는 시점인 HttpSendRequestA/W 를 후킹하여 쿼리를 스니핑하는 HookHttpSendRequestA/W 함수를 작성한다. kb6.dll 등으로 DLL 을 제작하여 후킹 프로시저(hooking procedure)를 담고, iexplore.exe 에 인젝션(injection)하여 인터넷 익스플로러에서 HTTP 쿼리를 모니터링 하였다.

4.1.2 문자열 파싱

HttpSendRequestA/W 이 호출될 때 불러오는 kb6.dll 의 HookHttpSendRequestA/W 에서는 받은 쿼리의 문자열 파싱 기능을 추가하였다. id= pw= password= otp= 등의 문자열이 발견되면 로그인 쿼리라고 간주하고 해당 위치에서의 아이디, 패스워드, OTP 값만 추출하였다.



〔그림 3〕 HttpSendRequest 가 후킹된 모습



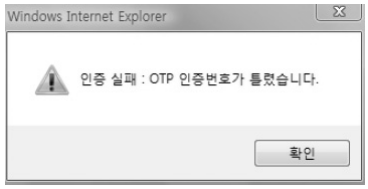
〔그림 4〕 문자열 파싱

4.1.3 탈취한 정보 전송

위 과정을 통해 획득한 아이디, 패스워드, OTP 값을 해커에게 전송하는 기능을 추가하였다 (실시간 MITM 공격방식). OTP 가 생성된 60초 안에 사용해야 하므로 해커의 모니터링 PC 에서는 탈취한 계정이 전송되면 해커에게 실시간으로 알려줄 알람 기능도 필요하다.

4.1.4 60초 시간 확보

OTP 는 사용자가 해커보다 먼저 생성된 OTP값을 전송하여 인증을 하게 되면 해당 패스워드가 무효화 되어버린다. 그리고 인증을 하지 않더라도 대기 시간은 통상 60초로, 그 유효시간이 지나면 역시 패스워드는 폐기된다. 따라서 OTP 값을 탈취한 직후, 사용자가 제한시간 내에 인증을 하지 못하도록 입력 방해 장치가 필요하다. 이 방법 역시 HttpSendRequestA/W 후킹으로 제작할 수 있다. 사용자가 입력한 뒤, HTTP 쿼리가 전송될 때, "id=window31&pwd=xxxxx&otp=12345678" 등의 문자열이 발견되면, otp=12345678 이라는 사용자가 입력한 정상 OTP 값을 변조하는 방법을 이용한다. 후킹 프로시저(hooking procedure)인 HookHttpSendRequestA/W 안에서 otp=87654321 같은 식으로, 비정상 패스워드로 바꿔서 외부 네트워크로 전달되도록 한다〔표 4〕. 그렇다면 사용자는 아무리 정상 OTP 값을 입력해도 후킹 코드에 의하여 가짜 값으로 바뀌게 되고, 인증 서버에서는 잘못된 패스워드를 전달받게 되므로 60초 동안 계속 패스워드가 잘못되었다는 메시지가 출력되게 된다. 정상 사용자는 계속 OTP 값을 맞게 입력해도 실제로 네트워크로 전송되는 쿼리에는 해커가 변조한 잘못된 값이 입력되어 있으므로 서버에서는 인증을 처리해 주지 않는다. 그렇게 정상 사용자는 OTP 인증을 할 수 없는 상태가 되며 60초가 흘러가는 동안 해커는 실시간으로 전송받은 진짜



〔그림 5〕 해커에 의한 인증 실패 메시지 (게임 사이트 군)

OTP 값을 이용해 로그인을 할 수 있다.

본 논문에서 제시하고 있는 방법은 사용자들에게 계속 인증이 되지 않는 메시지가 발생하며 뭔가 의심할 수 있지만 실제로 해킹에 사용되는 시간은 60초에 불과하며 사용자가 의심하고 패스워드를 변경하거나 고객센터에 연락을 하는 등 어떠한 조치를 취하려 해도 이미 계좌의 금액, 아이템 탈취 등이 발생한 이후가 될 수 있다. 따라서 MITM 과 MITPC를 혼용한 공격을 할 때, 일부 민감한 사용자들이 의심을 한다 하더라도 충분히 해킹이 가능하다.

4.1.5 취득한 OTP 값 전달을 통한 MITM 공격

탈취한 OTP 값을 해커가 미리 준비해둔 웹사이트의 게시판에 POST 방식으로 전송하여 지속적으로 기록하게 하거나, 이메일로 전달하게 할 경우, 해커는 거의 실시간에 가깝게 탈취된 OTP 값을 확인할 수 있다. 그리고 지속적으로 들어오는 계정 값 중 60초가 지나지 않은 것을 선택하여 해커의 PC 에서 로그인을 하면, OTP 시간이 만료되지 않은 상태에서 사용이 가능하다. 이러한 방식으로, 해커는 HTTP 쿼리 파싱으로 전달받은 아이디, 패스워드, OTP 을 이용하여 로그인을 할 수 있게 된다.

4.2 인터넷뱅킹 사이트 환경

인터넷뱅킹 사이트 이용환경 역시 앞 절에서 살펴본 게임포털 사이트 이용환경과 기본적인 구조는 비슷하지만, 공인인증서가 필요한 점과 뱅킹 쪽 모듈은 쿼

〔표 4〕 해커가 변조할 쿼리 비교

상태	쿼리
원래 만들어져야 할 쿼리	id=window31&pwd=xxxxx&otp=12345678
실제로 전달되는 쿼리 (해커가 변조한 쿼리)	id=window31&pwd=xxxxx&otp=87654321

리 스니핑이 차단되어 있다는 것이 게임포털 사이트 이용환경과 다른 점들이다. 따라서 먼저 공인인증서를 탈취하는 과정과, 쿼리 스니핑 대신 뱅킹 모듈의 코드 후킹을 통한 OTP 값의 탈취 부분만을 추가적으로 기술하였다.

4.2.1 공인인증서 해킹

역시 악성코드에 감염되었다는 것을 전제로 하며, 악성코드는 공인인증서를 해킹하기 위해 두 가지 행동을 한다. 첫 번째는 키보드보안 솔루션으로 보호되고 있는 공인인증서의 패스워드 탈취, 두 번째로는 공인인증서 파일 자체를 탈취하는 행위다. 먼저 공인인증서의 패스워드는 키보드보안 솔루션이 보호하고 있기 때문에 키입력 스니핑은 불가능하지만, 3장에서 소개한 코드 후킹 기법으로 패스워드를 탈취할 수 있다. 뱅킹 DLL을 리버스 엔지니어링 하면 GetXxxXxxxxxxx() 라는 Export 함수를 찾아낼 수 있는데, 그 위치에 코드 후킹을 걸어 놓으면 공인인증서의 패스워드가 첫 번째 인자로 넘어가는 것을 확인할 수 있고, 인증서 패스워드를 얻어낼 수 있다. 그리고 두 번째 인증서 파일 탈취 방법으로, 공인인증서는 주로 USB 에 담아 보관하므로 악성코드는 USB 장치의 삽입 유무를 주기적으로 검사한다. 그리고 이동식 디스크 감지가 될 경우, 디스크의 루트 폴더에 NPKI 폴더를 통째로 복사하여 방금 탈취한 패스워드와 함께 해커에게 실시간으로 전송한다. 공인인증서의 위치는 항상 루트의 NPKI 위치로 고정되어 있기 때문에 악성코드 입장에서 찾기는 매우 간단하며, 또 파일 크기도 4KB 에 불과하기 때문에 단시간에 전송이 가능하다. 그리고 본래 공인인증센터에서 인증서 파일을 USB 에 담을 때, 별도의 USB 하드웨어 시리얼 (Hardware serial) 값을 키 값으로 포함시키지 않기 때문에, 이렇게 임의로 복사하여 다른 USB 에 넣어도 인증이 되는 문제를 가지고 있다.

```
.text:100015BF
.text:100015BF loc_100015BF:                          ; CODE XREF:
.text:100015BF                call    IsSecKeyAvailable
.text:100015C4                test    eax, eax
.text:100015C6                jz      short loc_10001613
.text:100015C8                call    IsSFNullKey
.text:100015CD                test    eax, eax
.text:100015CF                jnz     short loc_10001613
.text:100015D1                mov     esi, [esp+60Ch+hDlg]
.text:100015D8                mov     edi, ds:GetDlgItem
.text:100015DE                lea     edx, [esp+60Ch+String]
.text:100015E2                push    7Fh
.text:100015E4                push    edx
.text:100015E5                push    0FFDh           ; nIDDlgItem
.text:100015EA                push    esi             ; hDlg
.text:100015EB                call    edi ; GetDlgItem
.text:100015ED                push    eax
.text:100015EE                call    Get[redacted]
.text:100015F3                add     esp, 0Ch
.text:100015F6                lea     eax, [esp+60Ch+var_580]
```

〔그림 6〕 리버스 엔지니어링을 통해 공인인증서 패스워드 탈취

4.2.2 OTP 값, 계좌비밀번호 탈취

앞 절 공인인증서 해킹 방법과 유사하게, 인터넷뱅킹 모듈의 코드 후킹을 통하면, OTP 값과 계좌비밀번호가 메모리에 남거나 eax 등의 레지스터를 거쳐서 키보드보안 DLL 또는 인터넷뱅킹 DLL 로 전달된다는 것을 알 수 있다. 따라서 게임포털처럼 쿼리 스니핑을 거치지 않아도, 메모리 단에서 리버스 엔지니어링을 거쳐서 입력된 OTP 값과 계좌번호를 탈취할 수 있다.

4.2.3 문자열 파싱, 탈취한 정보 전송

앞 절 게임포털 사이트의 환경에서의 동작원리와 동일하다.

4.2.4 60초 시간 확보

앞 절 게임포털에서는 쿼리 단에서 OTP 값을 변조하여 악성코드에 감염된 사용자가 60초간 인증을 하지 못하게 처리하였지만, 인터넷뱅킹 단에서는 2.2.절의 코드 단에서 eax 등의 레지스터에 OTP 값이 보이는 순간, 레지스터에 "mov eax, x"를 넣는 형태로

〔표 5〕 보안위협에 따른 대응방법

보안위협	공격방법	대응방법
통신경로 상 정보 노출 및 변조	패킷 스니핑	암호통신, 전자서명
키보드 입력 노출	키로거	키보드보안, PC보안, 가상키보드
메모리 정보 노출, 변조	악성코드, 키로거	E2E, 안티바이러스, 보안 브라우저, 공인인증서
전자서명 생성정보 유출	악성코드	PC 보안
화면 노출	원격제어프로그램, 악성코드	PC 보안, 가상키보드, 화면캡쳐방지
피싱	사회공학, 악성코드	피싱방지, PC보안

직접 값을 변조할 수 있다. 잘못된 값을 뱅킹 서버에 전달하게 하여 사용자에게는 인증을 시켜주지 않고 해커는 60초 시간을 확보한다.

4.2.5 취득한 OTP 값 전달을 통한 MITM 공격

공인인증서의 패스워드와 인증서 파일까지 해커에게 전달된 상태이므로, 실시간 MITM 공격을 이용하여 해커가 공인인증서로 직접 로그인하여 동시에 탈취된 OTP 값과 계좌비밀번호를 이용하여 해커의 계좌로 계좌이체를 한다.

4.3 기존 해킹 방법과의 차이점

이 기법은 MITM 과 MITPC 공격을 응용한 방법으로, OTP 해킹과 관련하여 수많은 논문에서 다뤄지던 MITM 공격기법보다 진보된 형태라 할 수 있다. 먼저, 인터넷뱅킹 서비스에 대한 대표적인 해킹 방법들을 〔표 5〕에 조사하여 비교, 분석하였다. 〔3〕

본 논문에서 제시한 공격방법은 '메모리 정보 노출, 변조' 와 '전자서명 생성정보 유출' 에 해당한다. 하지만 OTP 의 60초 시간을 유지시킨다는 관점에서는 현재 알려져 있는 대표적인 해킹 분류에 추가적인 범주가 필요할 것으로 보인다. 또한 메모리 정보 노출 변조와 전자서명 생성정보 유출에 공통적으로 제시되고 있는 PC 보안이라는 대응방법은, 결국 악성코드가 사전에 입수되어야만 안티바이러스의 시그너쳐나 패턴에 추가되고, 알려져 있지 않은 악성코드의 행위는 차단할 수 없다는 제약성이 있다.

4.3.1 MITM 과 피싱을 조합한 공격과의 비교

일단 기존 MITM 공격에서는 피싱 사이트가 필요하였다. 실제 사이트에서는 가져간 OTP를 사용자가 바로 사용해 버리기 때문에 OTP 값은 해커가 사용하기 전에 무효화 되어버리고, 결국 OTP 값을 유효하게 유지시킬만한 수단으로 아예 가짜 사이트를 사용하는 방법을 기존 MITM 공격에서는 택하고 있다. 하지만 이 논문에서는 실제 사이트에서 바로 MITM 공격이 이뤄지고 있으며, 사용자가 60초 동안 로그인을 하지 못하도록 시간을 확보하는 장치까지 사용하고 있다. 피싱 사이트가 존재해야만 MITM 공격이 가능했던 기존 방법과는 다른 방식의 공격이며 별도의 피싱 사이트를 운영하지 않고도 가능하다는 점에서 공격의 성공 가능성 및 위험도가 보다 높다고 할 수 있다.

4.3.2 MITB 공격과의 비교

본 논문에서 제안한 공격방식은 MITB 공격유형과도 차이점이 크다. MITB 공격방식은 MITM 공격방식과는 달리 피싱 사이트 없이 실제 사이트에서 OTP 값을 가져가긴 하지만 BHO 등의 가짜 웹페이지를 위에 덧씌우는 방법을 사용하고 있기 때문에, 예민한 사용자들의 경우에는, 실제 사이트의 화면 인터페이스의

〔표 6〕 OTP 현황

분류	포털명	OTP 개발사	홈페이지
게임포털	넥슨	AT솔루션	http://www.atsolution.co.kr
	플레이엔씨 (엔씨소프트)	이니텍	http://www.initech.com
	한게임 (NHN)	AT솔루션	http://www.atsolution.co.kr
	피망 (네오위즈게임즈)	모빌리언스	http://www.mobilians.co.kr
	넷마블 (CJ E&M)	모빌리언스	http://www.mobilians.co.kr
	엠게임	AT솔루션	http://www.atsolution.co.kr
	올스타 파란	이니텍	http://www.initech.com
인터넷뱅킹	우리은행	미래테크놀로지	http://www.mirae-tech.co.kr
	국민은행	vasco	http://www.vasco.com
	신한은행	미래테크놀로지	http://www.mirae-tech.co.kr
	외환은행	미래테크놀로지	http://www.mirae-tech.co.kr
	Citibank	미래테크놀로지	http://www.mirae-tech.co.kr
	기업은행	RSA	http://www.rsa.com
	산업은행	미래테크놀로지	http://www.mirae-tech.co.kr
	대구은행	미래테크놀로지	http://www.mirae-tech.co.kr
	전북은행	미래테크놀로지	http://www.mirae-tech.co.kr

변화를 감지하고, 원래의 은행 또는 포털 사이트와 디자인이 다르다는 것을 인지하여 해킹을 일으킬 수 있는 페이지라는 것을 시각적으로 탐지할 수 있다. 또 요즈음은 안티-피싱(Anti-Phishing) 솔루션 등에서 악의적인 BHO 나, 웹 페이지 위에 불필요하게 얹혀 있는 HTML 페이지를 검출해 주고 있으므로, 이와 같은 공격방식은 점차 성공확률이 낮아지고 있다. [35] 그러나 이 논문에서 다루는 OTP 해킹은 BHO 등으로 가짜 문서를 만드는 방법과 다르며, 문서를 전혀 건드리지 않고 네트워크 관련 모듈인 wininet.dll 에서 API 후킹과 인터넷뱅킹의 DLL 변조방법으로 실제 사이트의 페이지에서 정보를 입력받으며 그 내용을 탈취해가고 있다.

V. 실험 및 결과

실험을 시작하기 전에 현재 게임포털과 인터넷뱅킹에서 사용하고 있는 OTP 적용현황을 [표 6]에 정리해 보았다. 게임포털은 주요 대형 사이트에서만 사용하는 것과 달리, 은행 쪽은 인터넷뱅킹 사이트에선 대부분 사용하고 있다.

다음으로는 주요 국내 7개 게임포털 사이트와 10개 인터넷뱅킹 사이트에서 IV장의 OTP 탈취 시나리오를 토대로 실험해 보았다. 7개 사이트의 선정 기준은 검색 엔진 결과로 상위 첫 페이지에 검색되는 대표성 사이트로, 테스트한 결과를 [표 7] 에 기재하였다. 실험 방법으로는 트레이 아이콘을 살펴보아 키보드 보안이 설치되는지 확인하고, HttpSendRequest()를 후킹하는 DLL을 개발하여 각 사이트에서 쿼리를 모니터링 하였으며, 쿼리가 모니터링 되지 않는 경우는 인터넷뱅킹 DLL을 직접 코드 후킹하여 패스워드와 OTP 값을 탈취하였다. 그리고 서로 외부 IP 가 다른 두 대의 PC를 이용하여 한 대에서는 OTP 발급과 동시에 OTP 값을 변조하여 인증을 막았고, 그와 동시에 60초 안에 다른 PC에서 로그인이나 계좌이체를 시도해 보았다. 그 결과 모든 사이트에서 쿼리 스니핑 또는 코드 후킹을 통해 MITM 과 MITPC를 혼용한 OTP 탈취 공격이 사용 가능하였다 (A사의 경우는 쿼리가 암호화 되어 쿼리 스니핑은 되지 않았지만, 역시 그 앞단에서 코드 후킹을 통해 패스워드와 OTP 값을 가져갈 수 있었다).

VI. 해결책 및 기존 대안과의 비교

OTP 가 피싱과 MITM 을 조합한 공격에 취약하다는 것은 여러 논문들을 통해 알려져 있고, 다른 많은 대안들도 제시되고 있다. 예를 들어 OTP 해킹으로 기존에 가장 많이 알려져 있는 것이 피싱과 MITM 을 조합한 방법이고 대안으로 제시되는 것 역시 피싱방지를 위한 CAPTCHA가 가장 많은 대응방법으로 논의되고 있다. [34] 하지만 이 논문에서 제시한 쿼리 스니핑을 통한 OTP 해킹은 네트워크 쿼리

[표 7] 국내 20여개 사이트 테스트 결과

분류	포털명	키보드보안	쿼리 스니핑 or 코드후킹	공인인증서 탈취 후 타 USB에서 인증	타 PC에서 OTP 인증
게임포털	A사	적용	쿼리 스니핑은 불가 코드후킹은 가능	인증서 미사용	가능
	B사	적용	가능	인증서 미사용	가능
	C사	적용	가능	인증서 미사용	가능
	D사	적용	가능	인증서 미사용	가능
	E사	적용	가능	인증서 미사용	가능
	F사	적용	가능	인증서 미사용	가능
	G사	적용	가능	인증서 미사용	가능
인터넷뱅킹	a사	적용	가능	가능	가능
	b사	적용	가능	가능	가능
	c사	적용	가능	가능	가능
	d사	적용	가능	가능	가능
	e사	적용	가능	가능	가능
	f사	적용	가능	가능	가능
	h사	적용	가능	가능	가능
	g사	적용	가능	가능	가능
	h사	적용	가능	가능	가능
	i사	적용	가능	가능	가능

를 가져가는 것이기 때문에 CAPTCHA 와 관련이 적으며, 오히려 CAPTCHA를 통해 입력한 값을 스니핑 할 수도 있는 취약점까지 예상할 수 있다. 따라서 주된 대응방법으로 제시하기는 어렵다. 이번 장에서는 기존 대안과 이 논문에서 제시한 쿼리 스니핑 원리의 OTP 해킹과의 비교 과정을 통해 어떤 차이점이 있는지 기술한다. 또한, 본 논문에서 제시하는 공격기법은 정확히 표현하여 OTP 의 알고리즘 자체의 취약점이 아니라 구현상의 편의 때문에 오는 오류 또는 웹 브라우저나 클라이언트 단에서 데이터 유출을 차단하지 못하는 오류 등에서 생기는 취약점이다. 따라서 구현단계 또는 운영단계에서 많은 보완이 필요하며, 본 논문에서 제시하는 해결책도, 여러 가지를 솔루션을 복수로 적용하여 상호 보완하자는 데 있다. 게임포털과 인터넷뱅킹에 적용된 OTP 환경이 다르기 때문에, 먼저 공통으로 적용할 수 있는 대안을 소개하고 다음으로는 각 사이트에 적합한 방법을 제안한다.

6.1 공통 대안

이 논문에서 제시한 방법은 여러 가지 공격기법이 종합된 방식이다. 따라서 취약점을 제거하기 위해서는 각 기법에 대응가능한 여러 가지 제안을 각각 제시할 수 있다. 하나의 대안이 OTP 해킹 시스템 전체를 보완할 수는 없기 때문에 이 장에서 소개하는 여러 가지 대안을 종합적으로는 적용하는 작업이 필요하다.

6.1.1 서버에서의 상호 인증

OTP 인증 서버와 연결된 서비스 서버(게임, 뱅킹 등)에서 사용자가 입력한 OTP 값을 받아서 처리해주고 있으며, ID와 패스워드는 물론 공인인증서까지 탈취해간 입장이기 때문에 해커의 침입 행위 자체가 서버에서 인식하기에는 정상적인 로그인 상태라고 볼 수 밖에 없다. 따라서 서버에서의 인증 구분보다는 물리적인 위치의 선별이 필요하다. 해커는 60 초 안에 해킹당한 사용자의 OTP 값을 받아서 사용하게 되므로, 60초 동안 감염자의 PC IP 그리고 해커의 PC IP 가 물리적으로 다른 상태이다. 따라서 60초라는 짧은 시간 안에 서로 다른 IP에서 로그인 요청이 온다면 서버에서 해당 사용자는 해킹 상태라고 간주하여 로그인이나 계좌이체를 처리해주지 않는 방법이 있다. OTP 시스템의 구현 방식에 따라 IP를 우회할 수 있는 취약점이 존재할 수도 있다. 가장 기본적인 대안이다.

전화승인서비스

2장에서 설명한, 범주3의 양방향 방식 인증에 해당하는 전화승인서비스가 있다. 거래내역을 전화로 승인한 뒤, 사용자가 취소하면 이체를 해 주지 않는 방법으로 MITM 과 MITPC 공격에 좋은 대응방안이 될 수 있다. 그러나 이와 같은 부가장치를 이용한 승인방법도 해커가 접근할 수 없는 별도의 서버에서 사용자에게 휴대폰으로 알려주지 않고, 현재 사용자의 PC에서 SMS 요청 패킷을 전송하게 된다면, 역시 이 논문에서 지적한 쿼리 스니핑 또는 코드 후킹의 위험에 노출될 수밖에 없다. 승인을 받을 휴대폰 번호를 쿼리 스니핑을 통하여 해커의 것을 바꾸어 전송시킨 후 해커가 대신 승인을 할 가능성도 존재하기 때문에, 구현 시스템의 구조상 취약점을 반드시 검토하여야 한다. 물론 별도의 서버나 시스템에서 승인 처리를 따로 해주면 좋겠지만, 사용자의 수만큼 요청 패킷이 전송될 것이기 때문에 서버의 비용 리소스나 퍼포먼스 부분에서도 많은 고려가 필요하다. 그래서 제한적으로 현재 사용자의 클라이언트 PC를 이용할 수밖에 없으며 여기서는 해커가 접근할 수 있기 때문에 여러 가지 취약점이 발생할 수 있다.

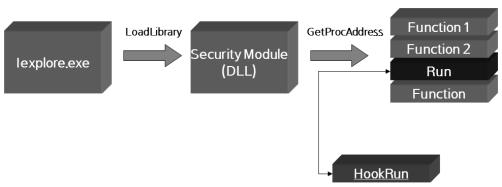
〔표 8〕 대안제시 비교

분류	대안	효과	제약성
공통	60초 IP체크	MITM 로그인 차단	IP 우회 가능성 존재
	전화승인서비스	해커의 계좌이체 방지	서비스 편의성 저해, 운영적 요소, 사후 대책
	E2E	쿼리 스니핑 방지, 구간암호화	리버스 엔지니어링에 의한 코드 후킹에는 효과 없음
게임포털	쿼리 암호화	쿼리 스니핑 방지	리버스 엔지니어링에 의한 코드 후킹에는 효과 없음
	API 후킹 복원	쿼리 스니핑 방지	리버스 엔지니어링에 의한 코드 후킹에는 효과 없음
	PC 등록제	해커의 로그인 차단	리버스 엔지니어링에 의한 코드 후킹에는 효과 없음
인터넷뱅킹	코드 무결성 검사	코드 후킹 차단	리버스 엔지니어링에 의한 우회 가능성
	공인인증서 보호	공인인증서 탈취 차단	리버스 엔지니어링에 의한 우회 가능성

그리고 SMS 전송량이 많은 시기인 명절이나 연말연시에는 SMS 의 전송이 몇 분 길게는 몇 시간 이후에 지연 도착하는 경우도 발생하는데, 이 같은 때에 부가장치 인증으로 강제화를 시켜 놓았다면 긴급하게 이체를 할 때에 처리가 되지 않거나, 로그인을 할 수 없는 상태가 될 수 있다. 이러한 경우, mControl 같은 경우는 여기서 문제가 발생한다. 해커가 로그인해서 아이템을 탈취하려 할 때 부가장치에서 SMS 를 보낸다 하더라도, 사용자가 SMS 를 받지 못하거나 즉시 확인하지 못하는 경우에 휴대폰으로 강제 종료를 시키지 못하여 아이템 해킹을 막을 수 없고, 또한 심야나 새벽 시간 잠들어 있는 시간에 SMS 가 오는 것은 발견하지 못할 수 있기 때문에, 역시 이 시간에 해커가 접속하여 악의적인 행동을 하는 것은 확인이 불가능하다. 결국 휴대폰을 이용한 승인방법 역시 제약성이 존재하는데, 해커가 사용자 PC를 감염시킨 이후에 사후 처리적인 면이 강하기 때문에 일단 사용자가 악성코드로 감염을 시키고 나면 해커는 모든 악의적인 행위를 할 수 있다는 점과 관련하여 제약성이 일부 존재한다.

6.1.3 E2E

키보드 보안 솔루션의 결함을 보완할 수 있고, 네트워크 구간 암호화를 통해 쿼리 스니핑을 차단할 수 있다. 따라서 MITM 을 방어하기 위해서는 E2E 기술 적용이 기본적으로 필요하다. 하지만 E2E 를 적용해도 키보드 보안 솔루션을 우회하는 기법을 이용하면 키보드 보안 기능을 제거할 수도 있고, 여전히 OTP 값을 포함한 키 값을 탈취해 갈 수 있는 방법은 아주 많이 제기되고 있다. [그림 7] 을 보면, 키보드 보안 솔루션은 DLL 로 제공되며, GetProcAddress()를 통하여 함수 포인터를 얻어간 뒤 Run() 을 통하여 보안 기능이 가동되게 되어 있으나, 해커들은 이 함수를 보안 기능을 가동시키지 않는 HookRun() 같은 다른 함수로 후킹하여 키보드 보안을 무력화 시킬 수 있다. E2E 를 이용하더라도 클라이언트에서 입력값의 완전한 보완은 쉽지 않으며 리버스 엔지니어링을 통하여 많은 공격이 가능하다는 취약점이 있다 [15] .



[그림 7] 키보드보안 솔루션 우회 방법

6.2 게임포털에서의 대안

6.2.1 HTTP 쿼리 암호화

로컬 단에서 쿼리를 wininet.dll 에서 작성할 때 변조가 일어나고 있고, 그 쿼리가 평문 상태라는 것이 첫번째 취약점이다. 또, 이 쿼리는 HTTPS 를 거치기 전에 만들어지고 있으므로, 로컬 단에서 HttpSendRequestA/W 가 호출되기 전에 HTTP 쿼리를 암호화 하는 작업을 진행해야 한다. 코드프로젝트 (Code Project) 사이트에서 Blackinkbottle 은 RSACryptoServiceProvider 라는 오픈소스를 제공하며 이러한 HTTP 쿼리에 대한 보호를 주장하고 있다 [36] . 하지만 쿼리를 암호화 하더라도 앞 단에서 코드를 후킹하여 스니핑 하는 것에 대해서는 보완이 되지 않는다는 제약성이 있다.

6.2.2 API 후킹 감지, 복원

해커가 클라이언트에서 행하는 내용의 핵심은 HttpSendRequestA/W 를 후킹하여 HTTP 쿼리를 엿볼 수 있다는 점이다. 이 작업이 선행되어야 입력 쿼리의 id, pw, otp 를 가져갈 수 있고, 60초를 확보하기 위해 사용자 PC 에서 나가는 정상 OTP 값도 변조할 수 있다. 따라서 iexplore.exe 의 HttpSendRequestA/W 후킹 탐지 작업이 필요하다. 단순히 탐지만으로는 사용자에게 불편한 메시지 박스를 계속 출력하며 인증이 되지 않는 문제가 발생할 수 있으므로 오리지널 코드로 복원하는 작업이나, 시큐어 브라우저(secure browser) 같은 장치에서 코드 변조 없는 안전한 환경에서 로그인 하는 작업이 필요하다 [37] .

6.2.3 PC 등록제

또 하나의 대안으로 게임업계에서는 지정 PC 등록제라는 서비스도 제공하는데, 본인이 자주 사용하는 집 PC 나 주로 방문하는 PC 방의 컴퓨터를 등록하여 그 PC 가 아닌 다른 곳에서는 로그인을 하지 못하게 할 수 있다. 그러나 이런 방법도 사용자의 PC 인 클라이언트 단에서 해당 PC 임을 증명할 수 있는 해시

(hash) 값, 맥어드레스(mac-address)나 하드웨어 시리얼(hardware serial) 등을 구해야 하는데, 결국 이것도 이 논문에서 제시한 리버스 엔지니어링에 취약할 수 있는 문제를 내포하고 있으며, 해커는 악성코드를 통하여 맥어드레스나 하드웨어 시리얼을 언제든지 변조할 수 있다. 따라서 4장에서 제시한 대로 클라이언트 보안의 제약성을 지목할 수 있다.

6.3 인터넷뱅킹에서의 대안

6.3.1 코드 무결성 검사

현재 공인인증서 모듈은 DLL 파일에 대해 별도의 무결성 검사가 이뤄지지 않고 있다. DLL 의 코드 변조를 통하여 ID,패스워드는 물론, OTP 값이 유출되고 있는데 만일 인터넷뱅킹 DLL 에 대해 무결성 검사가 시행된다면 코드 변조 시에는 이체를 시켜주지 않는 등의 보완이 가능하다. 다만, 무결성 검사 기능도 리버스 엔지니어링으로 다시 우회가 가능하다는 문제는 여전히 존재한다.

6.3.2 공인인증서 보호

공인인증센터에서 USB 에 인증서를 발급해 줄 때, 별도의 USB 인증 절차 없이 단순 복사만 이뤄지고 있다. 만약 USB 의 하드웨어 시리얼을 인증 키나 암호화키의 한 값으로 연동한다면 다른 USB 에 단순 복사하는 작업으로는 공인인증서를 사용할 수 없게 된다. 따라서 인터넷뱅킹 시에 사용되는 공인인증서에 하드웨어 인증 기능을 포함해야 한다.

6.3.3 거래연동 서명(transaction signing), 거래연동 OTP인인증서 보호 [38]

사용자가 PC 에 입력한 계좌번호 등의 거래정보와 연동된 인증 값을 생성하는 방식이다. 금융 서버에서는 이를 확인하고 계좌번호 등이 변경된 경우 거부할 수 있기 때문에 중간에서 거래정보를 변경하는 경우에 서버에서 탐지 가능하기 때문에 안전하다. 2004년 영국 지불결제 연삽(APACS)에서 최초로 제안한 기술이며, 현재 영국 Barclay, 호주 Bank of Queenisland, 네덜란드 ABN-AMRO 등의 은행에서 VIP 를 대상으로 적용되고 있다 [39] . 또한, 유럽을 중심으로 800만 이상이 사용하는 CAP(Chip Authentication Program)이라는 거래연동 인증 기술이 범용으로 쓰이고 있다. 다만 이 방식은 거래를 위한 별도의 전용 리더기가 함께 제공되어야 하며, 계좌번호까지 입력해야 하기 때문에 단말기의 크기가 커서 휴대가 불편한 문제가 있다. 또한 이벤트 방식의 인증 코드를 생성하여 ATM 이 해킹된 경우, 인증 코드가 노출될 수 있다는 취약점도 발표되었다 [40] .

따라서 그런 단점을 보완한 거래연동 OTP 라는 장치가 도입되었다. 별도의 리더기 없이 은행에서 발급한 OTP 와 동일한 크기의 전용장치를 사용하기 때문에 편이성 부분에서 용이하며, 시간 동기화 방식을 이용하기 때문에 취약점이 발생하지 않는다. 다만 거래시 계좌번호를 입력해야 하기 때문에 OTP 생성기에 숫자패드가 부착되어야 하여 크기가 커지는 문제점은 기존과 동일한 단점으로 거론되고 있다.

6.4 종합

우선순위로 보았을 때, 인터넷뱅킹에서는 1)서버에서의 상호 인증, 2) 공인인증서 보호, 3) E2E, 4) 코드 무결성 검사 등의 작업이 필요하고, 게임포털에서는 1) 서버에서의 상호 인증, 2) E2E, 3) HTTP 쿼리 암호화, 4)API 후킹 복원 등의 순으로 진행하는 것이 보다 효과적으로 취약점을 제거할 수 있다. 전화승인서비스나 PC 등록제는 추가 장치 도입이 필요하고, 사용자가 직접 이 서비스를 사용하지 않는다면 보완할 수 없다는 단점이 제기된다. 따라서 사용자에게 불편을 야기할 수 있는 이러한 별도 보안장치 도입보다는, MITM 공격을 결과를 차단할 수 있는 서버에서의 상호 인증 방식과, MITM 공격 과정을 차단할 수 있는 E2E, 쿼리 암호화 등의 작업을 처리해야 한다.

VII. 결론

본 논문에서는 계정보안을 위해 어떤 보안수단이 있는지 확인하고, 각 장치의 취약점 정리와 더불어 현재 가장 근본적인 대안이라는 OTP 의 우회 방법에 대해 논하였다. 해커가 만들 수 있는 시나리오를 작성하고 실제 게임포털, 인터넷뱅킹 사이트 등 국내 20여 개 OTP 사이트에 직접 모의 테스트를 수행함으로써 대부분의 사이트가 취약점을 가지고 있다는 점, 그리고 그에 대한 대응방안을 설계함으로써 OTP 의 취약점을 보완하기 위한 대책을 제시하였다는 데에 의의가

있다. 본 논문에서 설계한 OTP 해킹에 대한 해결책은 현재까지 많은 OTP 개발사가 간과하고 있는 부분인 서버에서의 인증 비교 시스템, 그리고 OTP 뿐만 아니라 아이디와 패스워드까지 쉽게 웹 입력 쿼리 또는 코드 후킹으로 스니핑이 가능한 부분과 키보드 보안 솔루션이나 HTTPS 로 그것을 해결할 수 없다는 것에 대한 환기, 마지막으로 리버스 엔지니어링과 DLL 인젝션을 이용한 후킹으로 보안 프로그램 해킹은 물론, OTP 의 입력값까지 제어할 수 있다는 점을 주지하였다. 기존에 알려진 OTP 해킹이 피싱, MITM, MITB 에 포커스가 맞추어져 있지만, 쿼리 스니핑과 리버스 엔지니어링을 통한 OTP 해킹도 존재하고 있다는 점을 이 논문을 통하여 입증하였다. OTP 서비스 제공사 혹은 포털, 은행, 게임사 등에서는 사내 모의 해킹을 통해 이러한 내용들을 점검해 보고, 추후에 유사한 공격을 방지하고 계정정보 시스템을 안전하게 운영할 수 있도록 해야 한다.

참고문헌

〔1〕 "온라인게임 보안서비스 설문조사," 인소야닷컴, http://www.insoya.com/bbs/zboard.php?id=poll&no=39

〔2〕 임형진, 심희원, 서승현, 강우진, "전자 금융 거래 환경의 인증 기술 동향 분석," 한국정보보호학회 학회지, 제18권 제5호, pp.84-98, 2008년 10월.

〔3〕 유정각, 송주민, "인터넷뱅킹 호환성을 고려한 보안 기술 적용방안," 지급결제와 정보기술, pp.84-98, Jul. 2010.

〔4〕 김소이, "전자금융사고 발생유형 및 대응현황," 지급결제와 정보기술, pp.35-61, 2010년 10월.

〔5〕 Petr Hanacek, Kamil Malinka, and Jiri Schafer, "E-Banking Security - Comparative Study," 10th ACIS, pp.263-26 Jun.2009

〔6〕 Alain Hiltgen, Thorsten Kramp, and Thomas Weigold, "Secure Internet Banking Authentication," IEEE Security & Privacy, 2006

〔7〕 Oppliger, R. Rytz, and R. Holderegger, T.eSecurity Technol, "Internet Banking: Client-Side Attacks and Protection Mechanisms," IEEE Computer, pp.27-33, Aug 2009

〔8〕 Steeves, D.J., & Snyder, M.W. "Secure online transaction using a CAPTCHA image as a watermark," U.S.Patent, 11/157,336, Jun, 2005

〔9〕 지정PC등록제, Nexon, http://security.nexon.com/ pcr/index.aspx

〔10〕 전화승인서비스, http://bank1.kbstar.com/quics?asfilecode=5023&_nextPage=page=B002346

〔11〕 mControl, NCSoft, https://security.plaync.co.kr/privateservice/mcontrol/intro.aspx

〔12〕 Hangbae Chang, "The study on end-to-end security for ubiquitous commerce," The Journal of Supercomputing Volume 55 Issue 2, pp.228-245, Feb 2011

〔13〕 배광진, 임강빈, "키보드 보안의 근본적인 취약점 분석," 한국정보보호학회지, 제18권 제3호, pp.89-95, 2008년 4월.

〔14〕 Linda D. Paulson, "Key snooping technology causes controversy," IEEE Computer, pp.27, Mar. 2002

〔15〕 강병탁, "Bypass AntiVirus - 키보드 보안 솔루션 취약점," 마이크로소프트웨어 pp.204-211, 2009년 6월.

〔16〕 서승현, 강우진, "OTP기술현황 및 국내 금융권 OTP 도입사례," 한국정보보호학회지, 제17권 제3호, pp. 18-25, 2007년 6월.

〔17〕 Wikipedia.: One-Time Password, http://en.wikipedia.org/wiki/One-time_password

〔18〕 S. Mizuno, K. Yamada, and K. Takahashi, "Authentication using multiple communication channels," in DIM 2005: Proceedings of the 2005 workshop on Digital identity management. New York, NY, USA: ACM, pp.54 - 62. Nov. 2005

〔19〕 Wikipedia.: Two-factor Authentication, http://en.wikipidia.org/wiki/two-factor_authentication

〔20〕 Fadi Aloul, Syed Zahidi, Wassim and El-Hajj, "Two factor authentication using mobile phones," IEEE/ACS International Conference on Computer Systems and Applications, pp.641-644, Apr. 2009

〔21〕 Hallsteinsen, S., Jorstad, I., and Thanh,

D. "Using the Mobile Phone as s Security Token for Unified Authentication. In," ICSNC 2007. IEEE Computer Society, Los Alamitos pp.68, Aug. 2007

〔22〕 Thanh, D., Jonvik, T., Feng, B., Thuan, and D., Jorstad, I., "Simple Strong Authentication for Internet Applications Using Mobile Phones,". IEEE GLOBECOM pp.1-5, Nov, 2008

〔23〕 Wei-Chi KU, Hao-Chuan TSAI, and Maw-Jinn TSUAR, "Stolen - verifier attack on an efficient smartcard-based one-time password authentication scheme," IEICE Transactions on Communication, vol.E87-B, no8, pp.2374-2376, Jan, 2005

〔24〕 UOTP, http://www.u-otp.co.kr/blog/

〔25〕 Wikipedia.: Man-in-the-middle Attack , http://en.wikipedia.org/wiki/Man_in_the_middle_attack

〔26〕 Security aspects of the SuisseID, http://postsuisseid.ch/en/suisseid/security/security-aspects

〔27〕 Heutige Situation, Angriffsvarianten und mögliche Schutzmassnahmen, "Cyber-Kriminalität ist heute zur Normalität geworden," Robert Weiss Consulting "The WEISSBUCH-Company" 2009

〔28〕 Phishing attack targets one-time passwords - scratch it and weep, http://www.theregister.co.uk/2005/10/12/outlaw_phishing/

〔29〕 Citibank Phish Spoofs 2-Factor Authentication, http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

〔30〕 NetworkWorld, "New Trojan intercepts online banking information," Jan. 14. 2008

〔31〕 Guhring, P. "Concepts against man-in-the-browser attacks," Jan, 24. 2007

〔32〕 맹영재, 신동오, 김성호, 양대헌, 이문규, "국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석," Internet and Information Security, 제 1권 제 2호, pp.101-118, 2010년 11월.

〔33〕 Augusto, P. B. "O futuro dos backdoors - O pior dosmundos", Retrieved August 10, 2010, http://www.paesdebarros.com.br/backdoors.pdf Sep. 15. 2005

〔34〕 Chun-Ming Leung, "Depress phishing by CAPTCHA with OTP," 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, pp.187-192 Aug, 2009

〔35〕 Wikipedia.: No Phishing, http://ko.wikipedia.org/wiki/%EB%85%B8%ED%94%BC%EC%8B%B1

〔36〕 Blackinkbottle, "RSA Interoperability between JavaScript and RSACryptoServiceProvider - Form Login Example," Codeproject, http://www.codeproject.com/KB/aspnet/rasinterop.aspx Aug, 2005

〔37〕 시큐어브라우저 http://www.ahnlab.com/kr/site/product/productView.do?prodSeq=48

〔38〕 금융보안연구원, "거래연동 인증기술의 이해," 이슈리포트 2010-001, 2010년 1월

〔39〕 Gartner, "Transaction Verification Complements Fraud Detection and Stronger Authentication," http://www.gartner.com/id=496217 Nov, 2006

〔40〕 S.Driner "Otimised to Fall: Card Readers for Online Banking," Springer, Light Blue Touchpaper http://www.lightbluetouchpaper.org/2009/02/ Feb 2009

〈著者紹介〉

강 병 탁 (Byung Tak Kang) 정회원
2004년 4월 ~ 2007년 3월 : 잉카인터넷 엔진개발팀
2008년 1월 ~ 2010년 7월 : 월간 마이크로소프트웨어 칼럼 작가
2009년 7월 : Microsoft MVP - Developer Security
2007년 4월 ~ 현재: 넥슨 게임보안팀 팀장
2010년 8월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 온라인게임 보안, 리버스 엔지니어링, 안티바이러스, 네트워크 보안

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직