인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식

정회원 유 한 나*, 이 재 식*, 김 정 재*, 박 재 표*, 전 문 석*

A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment

Han-na You*, Jae-Sik Lee*, Jung-Jae Kim*, Jae-Pio Park*, Moon-Seog Jun* ***Regular Members***

요 약

인터넷 뱅킹 서비스는 기존의 오프라인 서비스에 비해 편리성을 제공하지만, 해킹 등에 보안에 대한 많은 문제점을 가지고 있다. 이에 대해 금융기관은 보안을 강화하기 위해서 공인인증서, 보안토큰, 보안카드, OTP와 같은 인증 방법들을 제공하여 취약점을 보완토록 하였지만, 해킹 사건이 끊이지 않고 발생하고 있다. 특히 기존 인증방법들은 메모리해킹이나 중간자 공격과 같은 해킹에 대해서 취약점이 제기되고 있어, 새로운 인증방법이 필요하게 되었다. 본 논문에서는 인터넷 뱅킹에서 전자금융거래를 할 때 사용자의 PC와 Mobile 기기에서 이중으로 인증을 받는 Two Channel 인증 방식을 제안하고, 기존의 방식들과 비교분석을 통하여 안전성 및 신뢰성 측면이 강화되는 것은 확인할 수 있다.

Key Words : OTP, Internet Banking Security, Two-channel Authentication

ABSTRACT

The Internet banking service provides convenience than the traditional offline services. However, it still causes a number of security problems including hacking. In order to strengthen security, the financial institutions have provided such authentication methods as the official authentication certificate, the security token, the security card and OTP. However, the incidents related to hacking have continuously occurred. Especially, various weak points have been suggested for the authentication methods in regard to such types of hacking as the memory hacking or the MITM attack. So I needed was a new authentication method. In this study, the two-channel authentication method which provide two-way authentication on the user's PC and mobile device when executing the electronic financial transactions in the Internet banking environment is suggested. Also, by analyzing it in comparison with other existing methods, it is possible to check that the prospects of safety and credibility are strengthened.

Ⅰ. 서 론

정보통신 기술의 급격한 발전은 정치, 경제, 사회 등 다양한 분야에서 영향력을 발휘하였고, 그 결과 기업은 과거의 경영 방식에서 벗어난 디지털 경쟁 체제로 대변혁이 일어났다. 금융 업무도 기존의 창구 대면 거래를 벗어나, 인터넷 뱅킹 서비스 시행되었으며, 이후, 전 세계적으로 빠르게 확산되었다.

* 숭실대학교 컴퓨터학과 (belover@naver.com)
논문번호 : KICS2011-03-150, 접수일자 : 2011년 3월 18일, 최종논문접수일자 : 2011년 8월 4일

인터넷 뱅킹은 은행 측면에서는 비용 절감과 같은 수익성을 제고하고, 사용자 측면에서는 시간과 공간 등의 제약을 벗어나 비대면 거래의 편리성을 제공한다. 하지만, 거래 사실 부인, 전송되는 정보의 무결성과 기밀성 보장의 어려움, 해킹 등 여러 문제점을 가지고 있다. 이에 따라 금융기관에서는 보안 강화를 위하여 공인인증서, 보안토큰, 보안카드, OTP 등 다양한 인증방법과 방화벽, 키보드 보안 프로그램, 백신 프로그램과 같은 많은 보안 메커니즘을 제공하고 있다. 그러나, 금융기관에 비해 상대적으로 보안이 취약한 개인 PC를 대상으로 하는 해킹 사건들이 증가하고 있으며, 중간자 공격(MITM : Man-In-The-Middle)과 메모리 해킹은 현재의 인증 방식들에 대해서 취약점이 알려진 상태이다.

따라서, 본 논문에서는 현재 금융기관의 인증 방식보다 효과적인 보안을 제공하는 방식으로 PC와 Mobile에서 이중으로 인증하는 Two-Channel 인증 방식을 제안 한다. Ⅱ장에서는 인터넷 뱅킹 서비스에서 사용하는 인증 방식들과 그에 대한 문제점을 살펴보고, Ⅲ장에서는 기존 인터넷 뱅킹 서비스에 대한 흐름을 알아본다. 제안하는 Two-Channel 인증 방식에 대해서는 Ⅳ장에서 상세히 설명하고, Ⅴ장에서 기존의 인증방식들과 제안하는 인증방식을 비교 분석하고, 마지막으로 Ⅵ장에서 본 논문의 결론에 대해서 정리하였다.

Ⅱ. 금융기관의 인증 매체와 문제점

2.1 인증서

인증서는 사용자의 신원을 확인하고, 거래 정보의 위조와 변조, 거래 사실의 부인 방지 등의 기능을 제공하는 일종의 사이버 인감증명서이다. 국내에서는 2002년부터 공인인증서를 사용하여 현재 경제 활동 인구의 90% 이상이 사용하고 있으며[1], 2007년에는 전자금융감독규정 및 시행규칙'이 개정되어 소액거래나 기술적으로 공인인증서 적용이 곤란한 경우를 제외한 모든 전자금융 거래 시 공인인증서를 의무적으로 사용토록 하도록 하였다[2].

이러한 인증서는 다음과 같은 문제점을 가지고 있다.

2.1.1 재발급 문제

사용자가 전자 서명 키를 분실하거나 노출되었을 경우 해당 인증서를 폐지하고 새로운 인증서를 재발급 받아야 한다. 재발급 할 때는 해당 금융기관 등을 직접 방문하여 본인 여부를 확인 받아야 하지만 사용자에게 상당한 불편을 초래하여 온라인상에서 간단한 본인 확인을 통해 인증서 재발급을 허용하고 있다[3]. 이러한 방법은 해커가 대상의 간단한 기본 정보만을 가지고 재발급을 받을 수 있으며, 재발급을 받으면서 개인키를 새로 입력하여 대상의 인증서를 사용할 수 있다[4].

2.1.2 개인키 유출 문제

인증서의 개인키는 해킹된 웹사이트 등을 이용하여 사용자의 개인정보를 알아내는 피싱(Phishing)이나, 키보드나 입력 매체를 통해 입력되는 키(Key)값을 가져오는 키로그(Keylog) 프로그램 등 간단한 해킹으로 유출할 수 있고, 사용자들은 자신의 개인키가 유출된 사실을 모르기 때문에 2차 피해가 우려된다.

2.2 보안토큰

보안토큰(HSM : Hardware Security Module)은 개인키 유출문제를 원천적으로 봉쇄하기 위한 암호 장비 중 하나이다. 이 장치는 CA(Certificate Authority) 키, SSL(Secure Sockets Layer) 키 등 중요한 정보를 안전하게 관리하기 위해 장치 내부에 프로세스 및 암호 연산 장치가 있어 전자 서명 키 생성, 전자서명 생성 및 검증, 난수 생성 등 여러 기능을 제공한다[4]. 보안토큰의 내부에 있는 암호화 키는 키가 기기 바깥으로 가져갈 수 없도록 물리적 보안을 제공하고 있다. 보안토큰의 문제점은 다음과 같다.

2.2.1 고가의 비용문제

현재 사용되고 있는 지문인식용 보안토큰의 경우, 한국정보인증, 한국전자인증, 조달청을 통해 최소 6만원 이상으로 구입가능하다. 이는 OTP기기 발급 비용에 비해 매우 고가에 해당한다.

2.2.2 유연성 부족

기기의 암호 알고리즘에 대한 취약성이 발견되었을 경우 새로운 알고리즘으로 업그레이드해야 하는데, 보안토큰은 하드웨어 기반이기 때문에 기능의 추가 및 삭제가 어렵다.

2.2.3 도난 또는 훼손 문제

보안토큰 내부에 있는 키에 대한 안전성은 기기에 기인하기 때문이 장치가 도난당하거나 훼손되는 경우 키에 대한 안전성을 유지 할 수 없다.

2.3 보안카드

보안카드(Security Card)는 단일 인증의 보안 취약

성을 보강하기 위한 Two-Factor 인증의 요소 중 “what you have (스마트카드, 토큰, 키 등)”에 해당하는 매체이다. 2005년 6월 보안카드에서 1개의 번호를 비밀번호로 입력하는 방법에서 2개의 번호를 제시하여 조합하여 새로운 비밀번호를 생성하는 방식이 제안되어 현재까지 사용하고 있다[5].

보안카드는 다음과 같은 문제점을 가지고 있다.

2.3.1 보안카드 관리의 문제

금융기관마다 각각 다른 보안카드는 사용자들에게 관리에 불편함을 준다. 이러한 문제점은 사용자들이 보안카드를 스캔 하거나 전자 문서화하여 PC나 메일 등에 보관하거나, 복사기로 복사하여 지갑, 집, 직장 등 여러 곳에 두고 다니는 상황이 생기게 되어, 보안카드 번호 노출이나 해킹 위험으로 다가온다. 또한 보안카드는 자체적으로 갖는 보안 장치가 없고, 노출이나 분실되었을 때 즉시 조치할 방법이 국한되어 있다[6].

2.3.2 키로거(Keylogger)에 의한 해킹

현재 보안카드의 패스워드 생성방식은 키보드를 이용하여 입력하여 키로그 프로그램을 통하여 유출이 가능하다. 또한, 현재 입력하는 방식은 1,190개의 비밀번호 생성 경우를 가지는데 약 1,500번의 해킹 시도 또는 20번의 해킹 시도 후 패턴을 분석하여 보안카드의 모든 조합을 알 수 있다.

2.4 일회용 패스워드

일회용 패스워드(OTP : One Time Password)는 현재 사용하는 비밀번호로부터 다음에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능하며, 동적인 특성을 가지고 있기 때문에 현재 사용하는 비밀번호를 재사용할 가능성이 희박하다[7].

OTP는 다음과 같은 문제점을 가지고 있다.

2.4.1 비용 및 기기 분실, 훼손 문제

별도의 기기를 사용하기 때문에 발급 받는데 비용이 들며, 장치가 도난당하거나 훼손되는 물리적 피해에 대해서는 안전성을 유지 할 수 없다.

2.4.2 실시간 피싱 및 중간자 공격의 취약점

OTP의 기술적 취약점이 아닌 OTP 사용 프로세스의 취약한 연결 고리에 대한 공격방식이다. 해커는 사용자의 PC에 키로거(Keylogger) 등의 악성 프로그램을 감염시켜 사용자 정보와 OPT값을 취득할 수를 있고, 현재 사용자가 거래 하고 있는 금융기관을 제외한 다른 금융기관에 접속하여 인증 받을 수 있다. 금융기관과 동일한 피싱사이트를 개설하여 사용자가 접근하도록 하고, 사용자가 입력한 정보와 OTP값을 이용하여 해당 금융기관에 인증 받을 수 있다.

2.5 Two-Channel 인증

인터넷과 전화회선과 같이 서로 다른 경로를 통해서 인증하는 방식으로, 사용자의 정보가 노출되어도 최후의 방어로 가장 좋은 방법 이다. 현재 “전화인증서비스”가 실행 중이며, 문제점은 다음과 같다.

2.5.1 거래 취소에 대한 문제점

사용자가 통화 중이거나 통신장애 등으로 무응답 시 거래가 성립되지 않는다.

2.5.2 도청 및 피싱에 대한 위험

현재 서비스는 ARS(Automatic Response Service)를 이용하기 때문에 도청으로 금융정보가 노출 될 수 있으며, 금융기관임을 확인 할 수 없어 금융기관을 사칭하는 피싱에도 위험이 있다.

Ⅲ. 기존 인터넷 뱅킹 인증 프로세스

현재 금융기관에서 사용되는 인터넷 뱅킹은 웹 기반으로 이 서비스들의 안전한 거래를 위해 인증서를 이용한 전자서명, 단대단 키 공유과정 및 암호화 기법 등 각종 보안기술이 적용된다.

그림 1은 기존 인터넷 뱅킹 인증 프로세스를 나타내는 것으로 사용자가 자신의 아이디(W_ID)와 패스워드(W_PW)를 이용하여 웹 기반의 인터넷 뱅킹 서버(IBS)에 로그인 하면 인터넷 뱅킹은 인증, 무결성, 부인방지를 위한 암호채널을 형성한다. 이때, 금융기관은 사용자의 인증서를 이용하여 신원을 확인하고, 사용자는 세션키(SeK)를 생성하여 금융기관의 인증서에서 추출한 공개키(Bank_PuK)를 이용하여 암호화

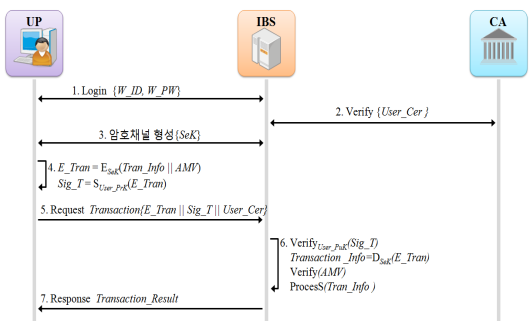


그림 1. 기존 인터넷 뱅킹 인증 프로세스

하여 전송한다. 사용자가 거래 정보를 세션키를 통하여 암호화하고 자신의 개인키를 이용하여 전자 서명하여 금융기관에게 전송한다. 금융기관은 서명값을 검증하고, 암호화된 거래정보(E_Tran)을 복호화하여 거래정보를 확인하고 처리한다.

이러한 인터넷 뱅킹 시스템은 일방향 인증을 제공하여 Cross Site Scripting 공격과 같은 중간자 공격에 취약점이 있으며, 사용자의 PC를 통해 전송되는 거래정보와 인증정보들은 메모리에 상주한 데이터를 조작하여 받는 계좌와 금액을 변경하는 메모리 해킹에 매우 취약하다.

Ⅳ. 모바일 인증서를 이용한 Two-Channel 인증방식

본 논문에서는 PC에서 이루어지는 해킹을 근본적으로 방지하기 위하여 기존의 다중요소 인증 방법이 아닌 서로 다른 채널에서 이중으로 인증 받는 Two-Channel 인증 방식이다.

제안하는 시스템은 그림 2와 같이 사용자의 PC에서 거래정보를 금융기관에 전송하면, 금융기관은 이를 사용자의 Mobile Device에 재전송하여, 사용자는 자신의 Mobile Device에서 거래정보를 다시 확인하고 인증하는 전송한다. 그러면 금융기관은 사용자의 PC에서 받은 정보와 Mobile에서 받은 정보를 비교하여 위·변조가 있는지 확인한 후에 처리하는 방식으로 거래정보를 이중으로 인증을 받아 처리함으로써 안전한 금융거래를 할 수 있도록 한다.

제안하는 시스템에 다음과 같은 조건을 만족하고 있다고 가정한다.

- 시스템 구성원은 크게 사용자와 금융기관, 인증기관(CA)으로 구분된다. 그리고 사용자는 개인 PC(UP)와 Mobile Device(UM)가 있고, 금융기관은 인터넷 뱅킹 서버(IBM)과 모바일 서버(MS)가 있다.
- 사용자의 PC와 Mobile Device에는 각각 인증기관에서 발행한 유효한 인증서(User_Cer)가 존재하고 있다.
- 금융기관에는 인증을 받은 사용자의 Mobile Device 정보가 등록되어 있고, 사용자의 Mobile Device에는 금융기관의 VM(Virtual Machine) Program이 설치되어 있다.

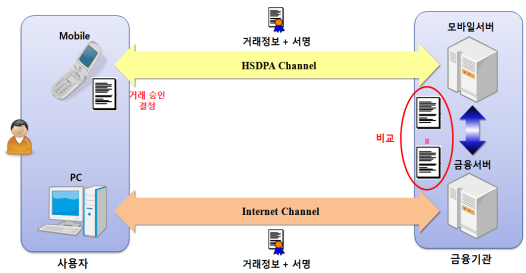


그림 2. 제안시스템 개념도

본 논문에서는 사용자의 PC에서 웹 기반의 인터넷 뱅킹 서비스에 접속하는 방식을 인터넷 채널 통신이라고 한다. 그리고 인터넷 채널과는 다른 채널로써 사용자의 Mobile Device를 이용하여 금융기관의 모바일 서버와 통신하는 것을 HSDPA(High Speed Downlink Packet Access) 채널 통신이라고 한다.

4.1 인터넷 채널 통신의 데이터 전송 프로토콜

인터넷 채널 통신은 그림 3과 같이 기존 인터넷 뱅킹 서비스와 대부분 유사하다. 사용자가 로그인하여 거래 정보(Tran_Info)와 인증 값(AMV)을 암호화하고, 거래정보(Tran_Info')에 대해 Hash값 H1을 구한다. 이후, 암호화된 거래정보 E_Tran, Hash값 H1 그리고 전자서명 값 Sig_T를 금융기관에 전송한다. 금융기관에서는 전자서명을 확인하고 암호화된 데이터를 복호화하여 거래정보를 확인한다.

$$Tran\_Info = \{W\_ID \,||\, 출금계좌 \,||\, 계좌비밀번호 \,||\, 출금액 \,||\, 입금은행 \,||\, 입금계좌\} \quad (1)$$

$$Tran\_Info' = \{출금계좌 \,||\, 출금액 \,||\, 입금은행 \,||\, 입금계좌\} \quad (2)$$

이후, 인터넷 뱅킹 서버는 거래 정보를 바로 처리하

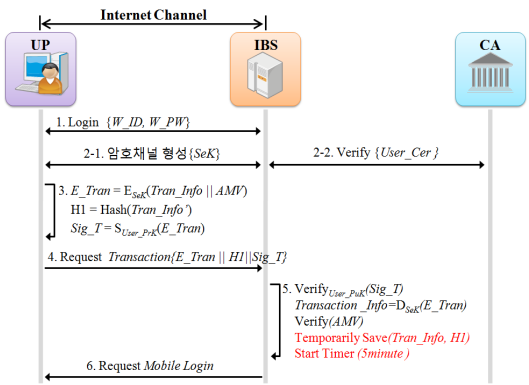


그림 3. 인터넷 채널 통신의 데이터 전송 프로토콜

지 않고, 거래 정보와 해시 값을 저장하여, 거래 번호(Tran_No)를 생성하고, 타이머를 시작한다. 일정 시간이 지나도록 사용자의 Mobile Device에서 인증된 거래 정보가 오지 않으면, 인터넷 뱅킹 서버는 저장해 놓은 거래 정보를 삭제하고, 거래가 처리 되지 않았음을 사용자에게 알려준다.

4.2 HSDPA 채널 통신의 데이터 전송 프로토콜

사용자가 PC에서 거래 정보를 전송한 후, 금융기관에서 사용자 Mobile을 이용하여 로그인 요청이 오면 사용자는 자신의 Mobile Device를 이용하여 그림 4와 같이 HSDPA 채널 통신을 한다.

4.2.1 VM Program 실행, VM_PW입력

모바일 서버와 통신하기 위해서 설치한 VM Program을 실행한다.

4.2.2 request UM_Login{P_Num || SID || VM_PW}

사용자의 전화번호(P_Num)과 USIM의 고유번호(SID), VM Program에 로그인하면서 입력한 패스워스(VM_PW)를 모바일 서버에 전송하여 로그인 요청을 한다.

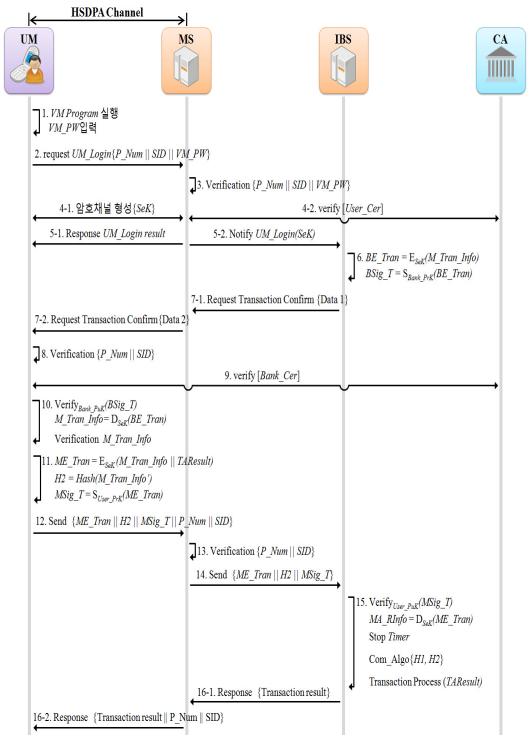


그림 4. HSDPA 채널 통신의 데이터 전송 프로토콜

4.2.3 Verification {P_Num || SID || VM_PW}

모바일서버는 사전에 등록되어있는 사용자의 Mobile 정보를 확인한다.

4.2.4-1 암호채널 형성{SeK}

사용자의 신원확인을 위해여 인증서와 데이터 암호화를 위한 세션키를 전송한다.

4.2.4-2 verify {User_Cer}

사용자의 인증서를 검증한다.

4.2.5-1 Response UM_Login result

사용자의 로그인 결과를 전송한다.

4.2.5-2 Notify UM_Login(SeK)

사용자의 Mobile에서 로그인이 정상적으로 이루어지면 모바일 서버는 인터넷 뱅킹 서버에서 로그인 사실을 알려주고, 데이터 암호화를 위해서 세션키를 전송한다.

4.2.6 BE_Tran = E_{SeK}(M_Tran_Info)

BSig_T = S_{Bank_PrK}(BE_Tran)

인터넷 뱅킹 서버는 세션키를 이용하여 사용자의 Mobile에게 전송할 데이터(M_Tran_Info)를 암호화하고, 자신의 개인키를 이용하여 서명한다.

M_Tran_Info = {Tran_No, W_ID, 출금계좌번호, 입금은행명, 입금자명, 입금계좌번호, 금액} (3)

4.2.7-1 Request Transaction Confirm {Data 1}

인터넷 뱅킹 서버는 암호화된 거래정보(BE_Tran)와 전자서명(BSig_T), 금융기관의 인증서를 전송한다.

$$Data\ 1 = \{BE\_Tran \parallel BSig\_T \parallel Bank\_Cer\} \quad (4)$$

4.2.7-2 Request Transaction Confirm{Data 2}

(3)의 데이터를 받은 모바일 서버는 사용자의 전화번호와 고유번호를 붙여 Mobile로 전송한다.

$$Data\ 2 = \{Data\ 1 \parallel P\_Num \parallel SID\} \quad (5)$$

4.2.8 Verification {P_Num || SID}

자신의 전화번호와 고유번호를 확인한다.

4.2.9 verify {Bank_Cer}

인증서버를 통해 금융기관의 인증서를 검증받는다. 이 과정을 통하여 사용자는 양방향 인증을 제공받을 수 있다.

4.2.10 Verify $_{Bank\_PuK}$(BSig_T)
M_Tran_Info= D_{SeK}(BE_Tran)
Verification M_Tran_Info

인증서가 유효하면, 사용자는 인증서를 통해 금융기관의 공개키를 추출하여, 서명값을 검증하고, 세션키를 이용하여 데이터를 복호화하여 M_Tran_Info를 확인한다.

4.2.11 ME_Tran = E_{SeK}(M_Tran_Info || TAResult)
H2 = Hash(M_Tran_Info')
MSig_T = S_{User_PrK}(ME_Tran)

거래정보를 확인한 사용자는 거래에 대해서 처리를 할 것인지 취소를 할 것인지 결정한 정보(TAResult)와 함께 암호화하고 전자서명 한다. 그리고 거래정보 M_Tran_Info 중 일부분(M_Tran_Info')을 이용하여 Hash값을 계산한다.

$$M\_Tran\_Info' = \{출금계좌번호,\ 출금액,\ 입금은행,\ 입금계좌번호\} \quad (6)$$

4.2.12) Send {ME_Tran || H2 || MSig_T || P_Num || SID}

사용자는 Mobile Dedive에서 암호화된 거래 정보와, Hash값, 전자서명, 자신의 전화번호와 기기의 고유번호를 함께 전송한다.

4.2.13 Verification {P_Num || SID}

모바일 서버는 전송받은 데이터에서 사용자를 확인한다.

4.1.14 Send {ME_Tran || H2 || MSig_T}

사용자가 확인되면, 암호화된 거래정보 ME_Tran과 Hash값, 서명값을 인터넷뱅킹 서버에 전송한다.

4.1.15 Verify$_{User_PuK}$(MSig_T)
MA_RInfo = D_{SeK}(ME_Tran)
Stop Timer
Com_Algo {H1, H2}
Transaction Process(TAResult)

인터넷 뱅킹 서버는 서명 값을 확인하고, 데이터를 복호화 한 후 작동한 Timer를 멈춰서 시간 안에 데이터가 전송되었는지 확인한다. 이후 인터넷 뱅킹 서버는 사용자의 PC에서 보낸 Hash값 H1과 모바일에서 보내온 Hash값 H2를 비교한 후 거래를 처리한다.

4.2.16-1 Response {Transaction result}

인터넷 뱅킹 서버는 처리 결과를 모바일 서버로 전송한다.

4.2.16-2 Response {Transaction result || P_Num || SID}

모바일 서버는 사용자가 받을 수 있게 사용자 정보를 붙여서 처리 결과를 전송한다.

Ⅴ. 비교분석

현재 금융기관에서 사용하는 인증 방식은 기본적으로 비밀번호인 "알고 있는 것"과 자신만이 가지고 있는 인증서, OTP, 보안카드 등인 "가지고 있는 것"을 두 가지 모두 사용하여 본인 확인을 하는 Two-Factor 인증을 제공하고 있지만, 최종적으로 PC의 웹 브라우저를 통해 입력된다. 이러한 방법들은 근본적으로 PC 해킹으로부터 자유롭지 못하기 때문에, 메모리 해킹이나, 웹 사이트 해킹, 스파이웨어, 키보드 해킹, 중간자 공격 등과 같은 방법으로 중요한 금융 정보와 인증 정보들에 대해 해킹 가능하다. 또한 기존의 PC와 전화 인증을 병행하는 Two-Channel 인증 방식도 암호화되지 않은 음성으로 거래내용을 전송하여 도청과 피싱, VoIP를 이용하는 경우에는 VoIP 해킹 등을 통하여 공격이 일어날 수 있다.

표 1은 제안하는 인증 방식과 기존 인터넷 뱅킹 인증 방식을 비교 분석한 자료로서, 제안하는 시스템은 PC와 다른 매체인 Mobile Device를 이용하여 근본적인 PC 해킹으로부터 안전하며, Mobile Device와 통신할 때 암호화된 데이터 전송과 고유 정보, 인증서를 사용하여 보다 안전한 데이터 전송을 지원한다. 또한, 기존의 사용자만 인증하는 일방향 인증 방식이 아닌 은행과 사용자 모두를 인증하는 양방향 인증을 제공한다.

표 2는 공격 유형에 따른 보안성 분석표이다.

무차별 공격에 대해서 인증서와 보안카드를 사용하는 경우는 보안카드의 입력자리가 4자리 수 이므로 $1/10^4$ 확률로 공격에 성공 가능하며, 인증서와 OTP 발행기를 사용하는 경우는 OTP 발행 번호의 수가 6자리이므로 $1/10^6$ 확률로 성공 가능하다. HSM 방식은 인증서의 생성에 필요한 값이 $1/2^{2048}$에 보안카드나

표 1. 제안하는 인증방식과 기존 인터넷 뱅킹 인증 방식 비교 분석

인증 / 요소	기존 인증방식			제안하는 인증방식
	인증서 + 보안카드	인증서 + OTP	인증서 + 전화인증	
보관 수단	PC, 매체	PC, 매체	PC, 매체	PC, Mobile
입력 방식	키보드	키보드	키보드 + 음성	키보드, Mobile 키패드
유출 경로	PC 해킹, 도난, 분실	PC 해킹, 도난, 분실	PC 해킹, 도난, 분실	PC 해킹, 도난, 분실
공격 방법	키보드해킹, 백도어, 원격제어, 등	중간자공격, 메모리해킹, 실시간피싱	중간자공격, 메모리해킹, 피싱, 도청, VoIP해킹, 등	-
보안 요소	인증	인증	인증, 부인방지	인증, 부인방지
인증 방향	일방향 (사용자 → 금융기관)	일방향 (사용자 → 금융기관)	일방향 (사용자 → 금융기관)	일방향 (사용자 ↔ 금융기관)

표 2. 공격 유형에 따른 보안성 분석

인증 / 요소	기존 인증방식			제안하는 인증방식
	인증서 + 보안카드[8]	인증서 + OTP[8]	HSM+ 보안카드 or OTP[8]	
무차별 공격	$1/10^4$	$1/10^6$	$1/(2^{2048}\times N)$	$1/(10^{15}\times 2^{128})$
암호문 단독 공격	$1/10^4\times$ (1-번호 매칭율(%))	$1/10^6\times$ (1-시간당)	$1/(2^{2048}\times N)$	$1/(10^{15}\times 2^{128})$
메모리 해킹	100%	100%	100%	$1/(10^{15}\times 2^{128})$

OTP발행기 등 다른 인증 방법들의 공격 성공 확률이 더해진 값이 공격 성공확률이 된다. 제안하는 방식은 USIM카드의 15자리로 이루어진 식별 번호와 Mobile에서 사용하는 128비트의 암호화키를 사용하기 때문에 $1/(10^{15}\times 2^{128})$의 공격 성공 확률을 가진다.

암호문 단독 공격은 화면 및 키보드 입력을 통해 수집된 암호문들을 이용하여 공격하는 방법으로, 인증서와 보안카드를 사용하는 방식은 보안카드의 번호와 수집한 값들의 매칭률에 따라 공격성공 확률이 다르다. 보안카드의 모든 값을 수집한 경우, 100% 확률로 공격에 성공한다. OTP발행기를 사용하는 경우는 OTP 번호의 갱신 시간에 따라, 갱신 시간 이내에 공격이 이루어지는 경우 100% 공격 성공 가능하만, 갱신 시간이 지나면 기존 확률을 유지한다. HSM 방식과 제안하는 방식은 PC를 통해 비밀 값을 추출할 하여 수집할 수 없기 때문에 무차별 공격과 동일한 확률을 가진다.

메모리 해킹의 경우, 공격자는 사용자에게 보이는 데이터와 다르게 사용자 PC의 메모리 영역을 조작하여, 데이터 정보를 변경할 수 있다. 따라서 인증방법에 상관없이 사용자 PC에서 발생하는 모든 방식은 100% 해킹 성공 확률을 보인다. 제안하는 방식은 PC와 다른 채널을 이용하기 때문에 이전 공격 유형과 동일한 확률을 가지다.

Ⅵ. 결 론

본 논문에서는 근본적인 PC해킹으로부터 위협을 막고 금융거래의 안전성 및 신뢰성을 높이기 위하여 Mobile Device를 이용하여 현재의 보안 인증방식이나 개인정보가 유출되어도 최후로 방어로 가장 좋은 Two-Channel 인증 방식을 제안하였다. 제안한 방식은 사용자의 PC에서 인증한 거래정보를 금융기관에 전송하면, 금융기관은 사용자의 Mobile Device에 다시 전송한다. 사용자는 Mobile Device에서 거래 정보를 2차 인증하여 다시 금융기관으로 전송하도록 함으로써 안전한 금융거래를 할 수 있다.

기존의 인터넷 뱅킹 환경에서 사용하는 인증 방식들과 비교분석을 통하여 제안하는 방식은 중간자공격, 메모리해킹, 피싱, 도청 등에 안전하며, 기존 일방향 인증이 아닌 양방향 인증을 제공하는 것을 확인하였다. 그리고 현재 알려진 공격에 대해서도 $1/(10^{15}\times 2^{128})$의 매우 낮은 공격 확률을 가지는 것을 확인하였다.

향후 제안한 시스템은 인터넷 뱅킹 시스템에 국한되지 않고 모든 전자상거래에서 사용할 수 있는 효과를 기대할 수 있다. 그러기 위해서 아직까지 알려지지 않은 공격 유형에 대한 연구 및 분석이 필요할 것이다.

참 고 문 헌

〔1〕 전자인증센터, “전자금융거래시 공인인증서 의무사용 규제완화 관련 주요이슈 및 현황,” 2010. 07.

〔2〕 금융감독위원회, ‘전자금융감독규정,’ 2007. 01.

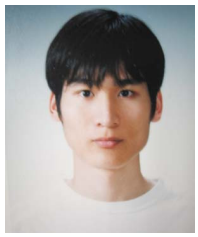
〔3〕 장우석, 이광우, 최동현, 정학, 이병희, 최윤성, 김승주, 원동호, “인터넷 뱅킹 보안,” *대한전자공학*

회 전자공학회지 제32권 제11호, pp.37-50, 2005. 11.
〔4〕 한국과학기술정보연구원, "HSM 제품 동향 및 안전성 분석," *한국정보보호학회* 제14권 제1호, pp.76-90, 2004. 02.
〔5〕 금융보안연구원, "금융부문 암호 기술 관리 가이드," 2010. 01.
〔6〕 한국개발연구원, "2009년중 국내 인터넷뱅킹서비스 이용현황," 2010. 01.
〔7〕 N. Haller, C. Metz, P. Nessser, M. Straw, "A One-Time Password System," RFC 2289, IFTF 1998.
〔8〕 조창현, "보안성이 강화된 인터넷 뱅킹 환경을 위한 이동통신 이중채널 인증 기법에 관한 연구," *숭실대학교 대학원*, 2010. 06.
〔9〕 금융보안연구원, "OTP 이용자 가이드라인," 2009. 12.
〔10〕 금융감독원, "전자금융 보안 종합대책," 2005. 07.
〔11〕 금융보안연구원, "종단간(End-to-End) 암호화 적용 가이드," 2007. 10.
〔12〕 정용훈, "모바일 환경에서 스크램블링 기법을 이용한 새로운 전자화폐 부분 암호화," *숭실대학교 박사학위논문*, 2009. 12.
〔13〕 Forouzan, "Cryptography and Network Security," McGraw-Hill, 2007.
〔14〕 T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol.IT-31, No.4, pp.469-472, 1985.
〔15〕 한국은행 은행국, "우리나라 은행의 인터넷뱅킹 도입현황과 대응방안," 한국은행, 2000. 04.

유 한 나 (Han-na You) 정회원

2008년 8월 평생교육원 정보보안전공 공학사
2010년 8월 숭실대학교 컴퓨터학과 공학석사
2010년 9월~현재 숭실대학교 컴퓨터학과 박사과정
<관심분야> 금융보안, 인증, 네트워크보안

이 재 식 (Jae-sik Lee) 정회원



2005년 8월 경원대학교 컴퓨터공학과 졸업
2007년 8월 숭실대학교 컴퓨터학과 공학석사
2007년 9월~현재 숭실대학교 컴퓨터학과 박사과정
<관심분야> RFID/USN, 인증이론 및 시스템, 암호프로토콜

김 정 재 (Jung-jae Kim) 정회원

1999년 2월 영동대학교 컴퓨터공학과 공학사
2001년 2월 숭실대학교 컴퓨터학과 공학석사
2005년 8월 숭실대학교 컴퓨터학과 공학박사
<관심분야> RFID, DRM, Network security, 멀티미디어보안

박 재 표 (Jae-pyo Park) 정회원

1996년 2월 숭실대학교 컴퓨터학부 공학사
1998년 8월 숭실대학교 컴퓨터학과 공학석사
2004년 8월 숭실대학교 컴퓨터학과 공학박사
2008년 9월~2009년 8월 숭실대학교 정보미디어기술연구소 전임연구원
2010년 3월~현재 숭실대학교 정보과학대학원 교수
<관심분야> 컴퓨터통신, 보안

전 문 석 (Moon-seog Jun) 정회원

1981년 2월 숭실대학교 전자계산학과 졸업
1986년 2월 University of Maryland Computer Science 석사
1989년 2월 University of Maryland Computer Science 박사
1991년 3월~현재 숭실대학교 정교수
<관심분야> 정보보호, 네트워크 보안, 전자여권, 암호학