http://dx.doi.org/10.5392/JKCA.2014.14.12.565

OTP를 이용한 PKI 기반의 개인키 파일의 안전한 관리 방안

Management Method to Secure Private Key of PKI using One Time Password

김선주*, 조인준**
한국정보통신기술협회*, 배재대학교 사이버보안학과**

Seon-Joo Kim(sunjoo@tta.or.kr)*, In-June Joe(injune@pcu.ac.kr)**

요약

인터넷이 활성화되면서 우리는 PC나 스마트폰에서 온라인 뱅킹, 주식 거래, 쇼핑 등의 다양한 전자상거래를 한다. 인터넷 상에서 거래 당사자 간의 신원확인 및 부인방지를 위한 주요 수단으로 공인인증서를 주로 활용한다. 하지만, 2005년 이후로 공인인증서 사용자에 대한 공격이 증가하고 있다. 즉, 공격자는 사용자 PC로부터 탈취한 공인인증서와 개인키 파일을 가지고, 은행 계좌 조회/이체나 전자상거래에 정당한 사용자로 위장하여 사용하게 된다. 이때, 개인키 파일은 사용자의 비밀번호로 암호화되어 저장되고, 필요할 때마다 복호화 되어 사용한다. 만약, 사용자의 비밀번호가 공격자에게 노출된다면 암호화된 개인키 파일을 쉽게 복호화 할 수 있다. 이러한 이유로 공격자는 사용자 PC에 트로이목마, 바이러스 등의 악성코드를 설치하여 사용자 인증서, 개인키 파일, 비밀번호를 탈취하려고 한다. 본 논문에서는 개인키 파일을 OTP 인증 기술을 이용하여 암호화함으로써 안전하게 관리할 수 있는 방안을 제안한다. 그 결과, 암호화된 개인키 파일이 외부에 노출되더라도 일회용 패스워드와 사용자 비밀번호가 노출되지 않으므로 암호화된 개인키 파일은 안전하게 보관된다.

■ 중심어 : | 공개키 기반 구조 | 공인인증서 | 개인키 파일 | 패스워드 | 일회용 패스워드 |

Abstract

We have various e-commerce like on-line banking, stock trading, shopping using a PC or SmartPhone. In e-commerce, two parties use the certificate for identification and non-repudiation but, the attack on the certificate user steadily has been increasing since 2005. The most of hacking is stealing the public certificate and private key files. After hacking, the stolen public certificate and private key file is used on e-commerce to fraud. Generally, the private key file is encrypted and saved only with the user's password, and an encrypted private key file can be used after decrypted with user password. If a password is exposed to hackers, hacker decrypt the encrypted private key file, and uses it. For this reason, the hacker attacks user equipment in a various way like installing Trojan's horse to take over the user's certificate and private key file. In this paper, I propose the management method to secure private key of PKI using One Time Password certification technique. As a result, even if the encrypted private key file is exposed outside, the user's private key is kept safely.

■ keyword : | PKI | Certificate | Private Key File | Password | OTP |

접수일자 : 2014년 10월 08일
수정일자 : 2014년 10월 30일
심사완료일 : 2014년 10월 30일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

우리는 인터넷을 통해 PC나 스마트폰에서 온라인 뱅킹, 주식 거래, 쇼핑 등의 다양한 전자상거래를 한다. 이때 안전한 전자상거래를 위해 신원확인 및 부인방지의 수단으로 공인인증서를 활용한다. 이처럼 전자상거래 활성화를 위해 필수적인 공인인증서의 안전한 발급 및 관리의 체계를 마련코자 전자서명법이 제정되었다[1].

하지만, 사용자 PC의 키보드 해킹(Key Stroke)을 통해 계좌번호, 비밀번호, 공인인증서의 비밀번호 등을 빼내가는 사고[2]를 시작으로, 최근에는 KBS와 디지털뉴스에서 공동으로 악성코드를 이용해 사용자 PC에 저장된 공인인증서와 비밀번호를 빼내는 공격을 시연하기도 하였다[3]. 사용자 PC의 키보드나 메모리 해킹, 스마트폰에 저장된 공인인증서와 비밀번호 탈취 시도 등의 해킹 기술이 급속하게 발전하고 있으며, 최근 온라인 뱅킹 관련 해킹 피해액이 40억 원을 육박하고 있다[4]. 이러한 해킹 사고에 대응하기 위해 공인인증서 뿐만 아니라, 일회용 패스워드(One Time Password, 이하 'OTP'라 함) 인증 방식, 소프트보안카드 기반 다중 인증 방식 등 다양한 인증방법을 도입하려는 시도가 늘고 있다[5-7].

특히, 은행/증권 등의 금융기관에서는 다양한 해킹사고를 방지하기 위해 SMS, 공인인증서, OTP, 가상 키패드 등을 함께 사용하도록 강제하고 있으며, 추가적으로 키보드 보안 솔루션, 백신 등 다양한 보안 프로그램을 사용자 PC에 반드시 설치하도록 요구한다. 또한 사용자의 비밀번호를 영문/대소문자/숫자/특수문자 3가지 조합으로 9자리 이상을 요구함으로 인해 사용자는 비밀번호 관리에 부담을 갖게 된다. 하지만, 여러 가지 보안 대책에도 불구하고 사용자의 비밀번호와 개인키 파일이 외부에 노출되면 금융기관의 보안대책은 어떠한 보호막 역할을 수행하지 못한다. 따라서 여러 가지 보안대책이 있더라도 사용자의 비밀번호에 대한 안전한 관리 방안이 필요하다.

따라서 본 논문에서는 OTP 기술을 활용하여 사용자 비밀번호와 개인키 파일이 노출되더라도 안전하게 유지할 수 있는 방안을 제안하고자 한다.

본 논문의 구성은 2장에 본 논문과 관련된 공개키 기반 구조(Public Key Infrastructure, 이하 'PKI'라 함) 와 OTP 개념을 정리하고, 3장에 제안시스템을 설명하였다. 4장에서는 제안시스템의 타당성을 객관적으로 증명하기 위해 타 사용자 인증방법과 비교 분석하였고, 5장에 결론을 맺었다.

II. 관련 연구

2.1 ID/PW 인증 개요

대부분의 웹이나 응용프로그램에서 사용자 인증은 ID와 패스워드를 사용한다. 이러한 인증 방식은 네트워크상에서 해커에 의해 쉽게 ID와 패스워드가 노출될 수 있다. 이러한 위험에 대응하기 위해 대부분 SSH, SSL 등의 보안프로토콜과 함께 사용자 패스워드 조합규칙(예. 최소 9자 이상 12자 이내, 영대소문자/숫자/특수문자조합 등)을 강제로 요구한다. 또한 사용자 패스워드를 3개월이나 6개월 단위로 주기적으로 갱신하도록 요구하여 사용자의 불편함을 초래한다.

2.2 PKI 개요

PKI는 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보보호 표준 방식으로 인터넷상의 전자상거래와 같이 지역적으로 떨어져 있는 이용자 간의 전자서명과 암호화에 의한 보안기술이다[9]. 즉, 통신을 하고자 하는 쌍방이 모두 신뢰할 수 있는 기관(공인인증기관)에서 생성한 공개키와 개인키를 사용하여 안전한 전자상거래를 할 수 있도록 지원한다.

PKI 인증시스템은 사용자 정보에 따라 랜덤하게 생성된 공개키 정보를 저장한 인증서를 발급하고 관리하는 인증기관(CA), 사용자의 인증서 발급 요청에 따라 사용자 정보를 등록하는 등록대행기관(RA), 인증서와 폐지된 인증서 목록을 사용자에게 제공하는 디렉터리 시스템(DS) 등으로 구성되며, 각 구성요소 간 관계는 다음 [그림 1]과 같다.

이러한 PKI 인증시스템의 동작절차는 다음과 같다. 먼저, 사용자가 등록대행기관에서 자신의 신원정보를

확인받고 인증서 발급 요청한다. 요청을 받은 등록대행 기관은 사용자 신원정보를 전송하면서 인증기관에 인증서 발급 요청을 한다. 사용자 인증서 발급요청을 수신한 인증기관은 사용자에게 인증서를 발급해주면서 발급된 인증서와 인증서 폐지목록을 디렉터리 시스템에 게시한다. 사용자가 인터넷 상점(Market)에 접속하여 전자상거래 시, 상점에서는 디렉터리 시스템에 접속하여 사용자 인증서와 인증서 폐지목록을 다운받아 사용자의 인증서의 유효성을 검사 후 인증서가 유효한 사용자에게만 해당 서비스를 제공한다.

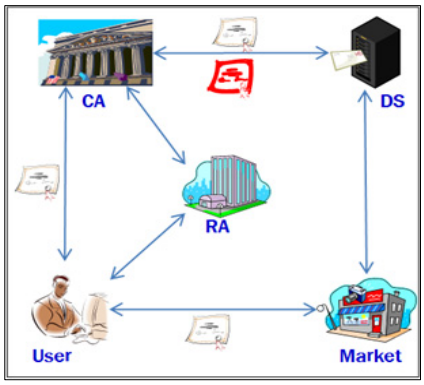

그림 1. PKI 개요

이처럼 PKI 인증시스템은 암·복호화 및 전자서명 기술을 이용하여 전송데이터의 위·변조 확인 메커니즘을 제공하여 다양한 인터넷 서비스나 전자상거래를 안전하게 할 수 있도록 지원한다. 전자상거래 시 ID/PW방식이나 보안토큰 등의 방식에 비해 PKI 기반의 기술이 암호학적으로 더 안전하여, 우리나라에서 공인인증기관을 운영하고 있다. 이때 사용하는 X.509 공인인증서는 signCert.der, signPri.key, CaPubs라는 파일들로 구성되며, 각 파일의 용도는 [표 1]과 같다.

표 1. X.509 공인인증서 구성파일

파일명	용도
signCert.der	인증서의 버전, 인증서 소유자 정보, 유효기간, 인증서 발급자 정보 등이 X.509 형식에 맞춰서 저장된 공개키 파일
signPri.key	PKCS#8 구조에 따라 저장한 개인키 파일
CaPubs	인증서의 유효성 검증을 위한 인증서 체인(발급기관 정보) 파일

[그림 2]와 같이 X.509 공인인증서 상세정보는 인증서 소유자 정보, 유효기간, 서명알고리즘, 서명해시 알고리즘, 발급자, 공개키 등의 정보를 X.509 인증서 구조체 형식에 따라 ASN.1 인코딩하여 저장하고, 개인키 상세정보는 개인키 암호 알고리즘, 서명 알고리즘 등의 정보를 PKCS#8 구조체 형식에 따라 사용자가 입력한 암호로 암호화하여 저장한다[10]. 이때 개인키 파일의 암호화 메커니즘은 패스워드 기반의 암호화 방식(Password Based Encryption Scheme, PBES)을 사용한다[11]. 즉, 사용자로부터 입력 받은 암호로 개인키 파일을 암호화하여 저장하고, 개인키가 필요할 때마다 사용자로 부터 암호를 입력 받아 암호화된 개인키 파일을 복호화 후 전자서명 생성·검증, 암·복호화에 사용하게 된다.

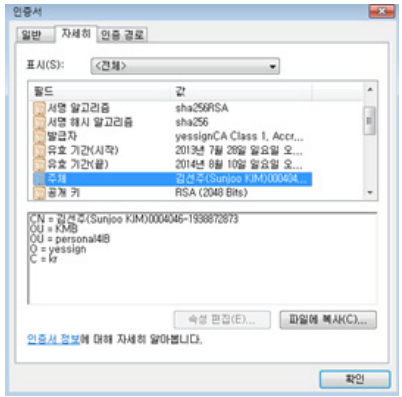

그림 2. 공인인증서 상세 정보

이와 같은 공인인증서는 공개키 및 개인키 파일, 인증서 체인파일이 그룹으로 사용되지만, 암호화된 개인키 파일이외의 다른 파일은 모두 공개되므로 암호화된 개인키 파일이 해커들로 부터 주요 공격대상이 된다.

2.3 OTP 개요

OTP는 사용자가 로그인할 때마다 해당 세션에서만 사용할 수 있는 일회용 패스워드를 생성하는 보안시스템[9]으로, ID/PW 방식에서 사용자 패스워드가 외부 노출 시 재사용될 수 있는 문제를 예방하기 위해 매 인

증시마다 달라지는 일회용 패스워드를 생성하여 사용자를 인증한다.

사용자와 OTP 인증센터는 OTP 생성·검증 알고리즘을 공유하고, 사용자가 자신의 ID와 타임스탬프 값을 OTP 생성알고리즘에 입력하여 생성한 OTP값을 OTP 인증 센터에 전송하면 OTP 인증센터는 사용자로부터 수신한 OTP값과 사용자 ID값을 OTP 생성·검증 알고리즘에 입력하여 사용자ID에 따른 OTP값을 생성 후 이를 비교하여 검증하게 한다.

이때, OTP 생성 알고리즘은 암호학적으로 안전한 방법으로 타임스탬프 값과 비밀번호를 일방향 해시 알고리즘으로 OTP 값을 생성하고, OTP값을 요청할 때 마다 매번 다른 OTP값이 생성되어 공격자가 중간에서 OTP값을 획득했다 하더라도 추후 인증에 재사용할 수 없다. 하지만 이러한 OTP 방식은 OTP 인증센터와 동기화 과정의 필요여부에 따라 동기화 방식과 비동기화 방식으로 나눌 수 있다.

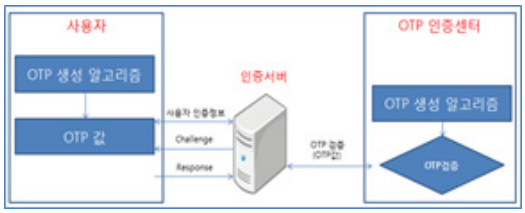

그림 3. 비동기화 방식

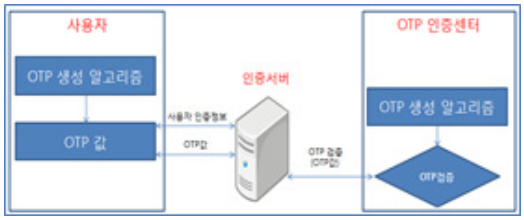

그림 4. 동기화 방식

비동기화 방식은 [그림 3]와 같이 사용자가 자신의 인증정보를 요청하면 인증 서버가 Challenge 값을 사용자에게 요청하여 사용자로부터 Response값을 다시 수신하여 사용자 인증정보와 Response값을 가지고 사용자를 인증하는 방식이고, 동기화 방식은 [그림 4]과 같이 사용자가 자신의 인증정보가 포함된 OTP값을 인증서버에 전송하면 인증서버는 이를 인증센터에 OTP 검증을 요청하여 그 결과로 사용자를 인증하는 방식이다.

[그림 3]에서 보는 바와 같이 비동기화 방식은 인증서버와 OTP 인증센터 간에는 동기화 과정이 필요 없지만, 사용자가 OTP 인증센터로부터 수신한 Challenge 값을 매번 입력해야 하고, 동기화 방식에 비해 네트워크 부하가 발생하며, 기존의 ID/PW기반의 어플리케이션과 호환성이 떨어진다. 반면, 동기화 방식은 OTP 인증센터의 Challenge값에 대한 Response값을 받을 필요가 없고, 비동기화 방식에 비해 네트워크 부하가 상대적으로 적고, 기존 ID/PW기반의 어플리케이션과 호환성이 높다. 그러나 사용자와 인증서버 OTP 인증센터 간에 시간 동기화 및 동기화 횟수 등의 기준값이 동기화가 반드시 이뤄져야 한다.

III. 제안 방안

지금까지 PKI 인증시스템과 OTP 기술의 특성을 정리하였다. 본 장에서는 제안 방안의 설계 내용 및 동작 절차를 설명한다.

본 논문에서는 기존에 사용하던 PKI 인증시스템에 OTP 기술을 접목하여 사용자의 암호화된 개인키 파일을 효율적으로 사용할 수 있도록 개선하는데 초점을 맞추었다. PKI 인증시스템에서 사용하는 개인키 파일은 사용자로부터 암호를 입력받아 암호화하여 저장한다. 이때, 공격자(해커)는 사용자가 입력하는 암호를 몰래 빼내기 위해 키보드 해킹, 메모리 해킹 등의 다양한 해킹을 시도한다. 이러한 해킹에 대응하기 위해 사용자에게 암호를 수시로 변경하도록 권고하고 있다.

본 논문에서는 사용자 비밀번호와 OTP 서버로부터 수신한 값을 이용해 개인키 파일의 암호화 방안을 제안함으로써 암호화된 개인키 파일을 안전하게 보호할 수 있는 방안을 제안하였다.

3.1 사용자 등록 절차

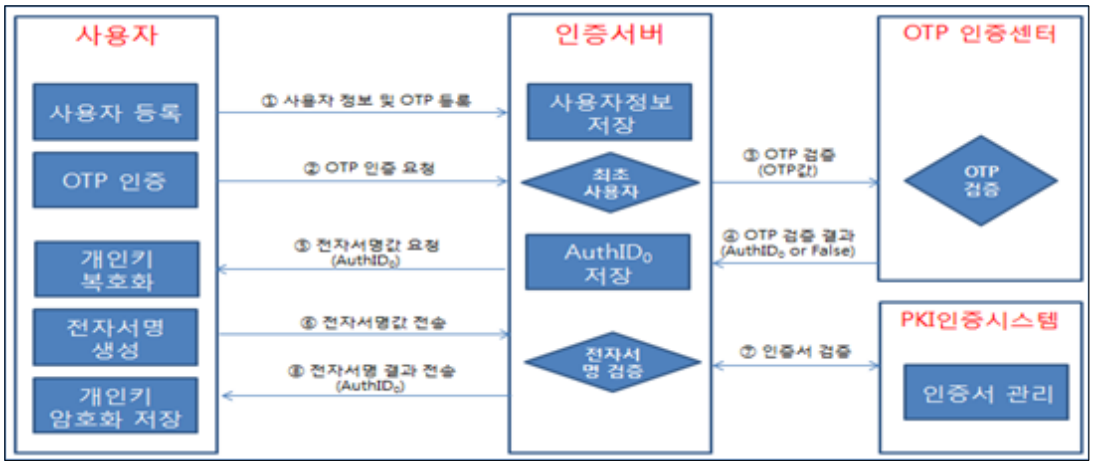

그림 5. 사용자 등록 절차

본 절에서는 PKI인증시스템으로 부터 사용자의 인증서와 개인키 파일을 발급받은 상태에서 추가적으로 OTP 인증센터와 인증서버에 사용자 등록 및 개인키 파일의 암호화 절차를 설명한다.

사용자 등록 및 개인키 파일 암호화 절차는 [그림 5]와 같다.

① 사용자 등록 단계에서는 사용자의 정보(예. ID, PW, 이름, 연락처 등)와 OTP 인증센터로부터 발급받은 OTP 기기정보(예. 시리얼 번호)를 인증서버에 등록한다. 이 단계에서는 사용자의 개인키 파일(signPri.key)이 사용자가 입력한 패스워드로만 암호화된 상태이며, 개인키 파일을 암호화에 필요한 $AuthID_0$가 인증서버에 저장되지 않은 초기 상태이다.

② OTP 인증 단계에서는 사용자와 OTP 기기정보가 인증서버에 저장되어 있는 상태에서 사용자의 ID(UserID)와 OTP 기기에 표시된 OTP 값(OTP_No)을 인증서버에 전달하여 사용자에 대한 OTP 인증을 인증서버에 요청한다.

③ 최초 사용자 검증 단계에서는 사용자로부터 수신한 OTP 인증 요청을 OTP 인증센터에 요청하기 전에 자신의 DB에 등록되어 있는 사용자 인지여부와 OTP를 처음 인증 요청하는지를 확인 후 최초 사용자인 경우에만 사용자로부터 수신한 OTP 값(OTP_No)을 OTP 인증센터에 전송하여 OTP 검증 요청한다. 만약 최초 사용자가 아닌 경우 OTP 검증 요청을 거절한다.

④ OTP 검증 단계에서는 OTP 인증센터가 인증서버로부터 수신한 사용자의 OTP값(OTP_No)의 유효성을 검사 후 유효한 경우에만 $AuthID_0$값을 생성하여 전송한다. 만약 사용자 OTP값이 유효하지 않으면 오류코드(False)를 인증서버에 전송한다.

$$AuthID_0 = H(\ OTP\_DeviceNo \mid OTP\_No \mid Timestamp\ )$$

⑤ $AuthID_0$저장 단계에서는 OTP 인증센터로부터 수신한 사용자별 $AuthID_0$값을 인증서버에 저장 후, 사용자에게 $AuthID_0$값을 전송하고, 전송된 $AuthID_0$에 대한 전자서명된 결과값을 요청한다.

⑥ 개인키 복호화 단계에서는 사용자로부터 패스워드를 입력 받아서 일방향 해시하여 해시값을 복호화 키로 사용하여 암호화된 개인키 파일의 복호화를 시도한다.

$$Es\_key = H(\ 패스워드\ )$$
$$User\_Pri\_key = D_{Es\_key}(signPri.key)$$

⑦ 전자서명 생성 단계에서는 ⑥단계에서 복호화된 개인키로 인증서버로부터 수신한 $AuthID_0$값에 대해 전자서명 후 인증서버로 다시 전송한다.

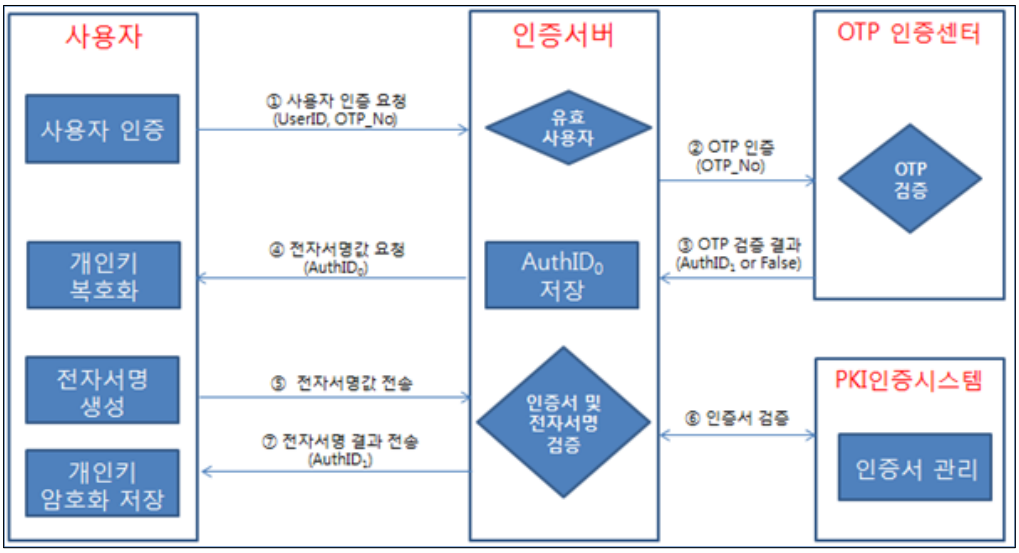

그림 6. 사용자 인증 절차

$Sig_{User\_Pri\_key}(AuthID_0)$

⑧ 전자서명 검증 단계에서는 인증서버가 사용자로부터 수신한 전자서명 값을 검증하기 위하여, 사용자의 인증서를 검증 후, 유효한 경우 사용자로 부터 수신한 전자서명을 검증한다. 이때 사용자의 인증서에 대한 유효성 검증을 위해 PKI 인증시스템의 디렉터리 서버에 접속하여 인증서와 인증서 폐지목록을 다운 받아 인증서의 유효성을 검증하고 사용자 인증서가 유효한 경우에만 $AuthID_0$값을 인증서버의 DB에 저장하고, 사용자에게 $AuthID_0$값을 재전송한다.

$D_{User\_Pub\_Key}[Sig_{User\_Pri\_key}(AuthID_0)]$

⑨ 개인키 암호화 저장 단계에서는 인증서버로부터 수신한 $AuthID_0$을 수신한 사용자는 [패스워드 | $AuthID_0$]로 조합하여 일방향 해시하여 생성된 문자열을 암호키로 사용자의 복호화된 개인키 파일(signPri.key)을 암호화하여 파일로 저장한다.

⑩ 개인키 암호화 단계에서는 사용자로부터 입력받은 패스워드와 ⑨단계에서 수신한 $AuthID_0$값의 문자열을 조합하여 평문인 개인키 파일(signPri.key)을 암호화용 비밀키를 생성한다. 생성된 비밀키를 이용하여 평문인 개인키 파일을 암호화 후 인증서버에 등록함으로써 사용자 등록이 완료된다.

Es_key_1=H(패스워드 | $AuthID_0$)

E_{Es_key1}(signPri.key)

3.2 사용자 인증 절차

본 절에서는 인증서버에 등록된 사용자의 인증 절차를 설명한다.

사용자에 대한 인증 절차는 [그림 6]과 같다.

① 사용자 인증단계에서는 사용자가 자신의 ID(UserID), OTP 값(OTP_No) 을 입력하여 인증서버에 사용자 인증 요청한다.

② 유효 사용자 검증 단계에서 사용자로 부터 수신한 ID(UserID)가 유효한 사용자인지 확인 후, 유효한 사용자인 경우 OTP 인증센터에 OTP기기번호(OTP_DeviceNo)와 OTP 값(OTP_No)을 전송하면서 OTP 인증을 요청한다.

③ OTP 검증 단계에서는 OTP 인증센터는 인증서버로부터 수신한 OTP 인증요청이 유효하면 $AuthID_1$값을 전송하고, 유효하지 않으면 인증 실패(False)값을 전송한다.

$AuthID_1$= H(OTP_DeviceNo | OTP_No | Timestamp)

④ $AuthID_0$ 저장 단계에서 인증서버는 $AuthID_1$을 DB에 저장 후 $AuthID_0$값을 User에게 전송하고, $AuthID_0$값에 대한 전자서명 값을 요구한다. 그러나 OTP 인증센터로부터 인증 실패값을 수신하면 사용자에게 인증실패 메시지를 전송한다.

⑤ 전자서명 생성 단계에서는 사용자로 부터 입력받은 패스워드를 해시한 값과 $AuthID_0$를 조합하여 암호화된 개인키 파일에 대해 복호화를 시도한다. 복호화된 개인키(User_Pri_key)로 $AuthID_0$값을 전자서명 하여 인증서버로 전송한다.

Es_key = H(비밀번호 | $AuthID_0$)
User_Pri_key = D_{Es_key}(signPri.key)
$Sig_{User\_Pri\_key}(AuthID_0)$

⑥ 인증서 관리 단계에서는 인증서버는 사용자의 인증서의 유효성을 점검하여 유효한 인증서 사용자인 경우 수신한 전자서명값($Sig_{User\_Pri\_key}(AuthID_0)$)을 검증한다. 검증에 성공 시, 인증서버는 해당 사용자의 $AuthID_0$값을 $AuthID_1$로 변경하고, 사용자에게 $AuthID_1$값을 사용자의 공개키(User_Pub_Key)로 암호화하여 재전송한다. 그러나 검증에 실패 시 사용자에게 오류메시지를 전송한다.

$Enc\_AuthID_1=E_{User\_Pub\_Key}(AuthID_1)$

⑦ 개인키 암호화 후 저장단계에서는 전자서명 Enc_AuthID_1을 수신한 사용자가 자신의 개인키(User_Pri_key)로 복호화 후, 복호화된 $AuthID_1$와 사용자가 입력한 비밀번호를 이용하여 사용자의 개인키 파일(signPri.key)을 암호화하여 파일로 다시 저장한다.

Es_key1=H(비밀번호 | $AuthID_1$)
E_{Es_key1}(signPri.key)

지금까지 제안시스템의 사용자 등록 절차, 사용자 인증 절차 및 사용자 인증 완료 후 개인키 파일에 대한 재암호화 절차를 설명하였다.

IV. 평가

본 장에서는 제안시스템의 객관적인 안전성을 기존의 사용자 인증 방식과 비교 평가하였다. 기존의 보안 시스템에서 사용하는 사용자 인증 방식으로 가장 대표적인 ID/PW방식과 공인/사설인증서를 이용한 인증서 방식, OTP 방식과 비교 평가하였다. 그 결과는 다음 [표 2]와 같다.

표 2. 인증방식 비교 평가

	ID/PW방식	인증서 방식	OTP 방식	제안시스템
특성	정적	정적	동적	동적
PW 변경 필요	필요	필요	불필요	불필요
재사용	가능	가능	불가 (1회사용)	불가 (1회사용)
추측 가능성	있음	있음	없음	없음
인증요소	사용자 소유 정보	사용자 소유 정보	사용자매체를 통한 정보	사용자 소유정보와 사용자매체를 통한 정보
위변조 가능성	높음	낮음 (개인키 파일 노출위험증가)	낮음	낮음 (개인키 파일 노출위험감소)
보안강도	하	상	상	상

제안 시스템은 개인키 암호화를 위해 사용하는 비밀키 생성은 해시 알고리즘의 종류에 따라 160/256/384/512bit를 생성한다. 위의 [표 2]에서 보는 바와 같이, ID/PW 방식과 인증서 방식과 달리 비밀번호가 동적으로 바뀌어 비밀번호를 주기적으로 변경할 필요성이 없어진다. 또한 네트워크상에서 해커가 패킷을 수집

하여 재전송하더라도 재사용이 어려우며, 개인키 파일을 외부에 노출되더라도 위변조 가능성이 낮아 기존의 인증서 방식에 비해 암호화된 개인키 파일의 노출 위험성이 줄어들어 보안강도가 아주 높다.

V. 결론

최근 사용자 PC의 키보드나 메모리 해킹, 스마트폰에 저장된 공인인증서와 비밀번호 탈취 시도 등의 해킹 기술이 급속하게 발전하고 있으며, 이에 대응하는 사용자 인증기술도 ID/PW 방식뿐만 아니라, 인증서, OTP 방식, SMS, 바이오인식 등 다양한 인증 방법이 제안되어 개발되고 있다.

본 논문에서는 인증서 방식에서 사용하는 암호화된 개인키 파일이 해커에게 노출된다면, 보안성이 탁월한 인증서 방식이라고 해도 인증 방법이 무력화 될 수 있다. 이에 본 논문에서는 이러한 위험성을 해결하기 위한 방안으로 PKI 기술과 OTP 기술을 접목시켜 개인키의 안전한 관리 방안을 제안하였다. 즉, 기존의 인증서 방식에서 사용하는 사용자 인증 방법은 그대로 유지하고, 개인키 파일을 OTP에서 제공되는 일회용 비밀키를 사용하여 암·복호화 하여 사용할 수 있다.

4장에서 살펴본 바와 같이, 제안시스템은 기존의 ID/PW 방식에 비해 패스워드가 160/256/384/512bit 길이를 사용하며, 인증서 방식과 OTP 방식을 접목하였으므로 보안성이 훨씬 강화되었다. 특히, OTP 방식을 사용함에 따라 사용자가 패스워드를 매번 변경하지 않아도 되고, 사용자 패스워드 조합규칙(예. 최소 9자 이상 12자 이내, 영대소문자/숫자/특수문자조합 등)을 준수하지 않아도 되어 사용자의 편의성이 크게 향상되었다. 따라서 인터넷뱅킹, 홈트레이딩 시스템 등의 사용자 인증이 필요한 시스템에서 제안된 방식을 적용이 가능할 것으로 예상한다.

향후 본 제안시스템에서 사용하는 암호화된 개인키 파일을 저장하는 저장매체 관리 방안과 OTP 인증 센터와 인증서버 및 사용자간의 효과적인 시간 동기화 방안에 대한 연구가 지속적으로 필요하다.

참 고 문 헌

[1] 전자서명법, 법률 제11690호, 2013.03.23 시행

[2] http://news.naver.com/main/read.nhn?mode=LSD &mid=sec&sid1=101&oid=014&aid=0000177855

[3] http://news.kbs.co.kr/news/NewsView.do?SEAR CH_NEWS_CODE=2819893&ref=&

[4] http://www.zdnet.co.kr/news/newsview.asp?article _id=20131016174155

[5] http://www.ddaily.co.kr/news/article.html?no=116994

[6] 이형우, “안전한 로그인을 위한 소프트 보안카드 기반 다중 인증시스템”, 한국콘텐츠학회논문지, 제9권, 제3호, pp.28-38, 2009.

[7] 김대진, 최홍섭, “OTP를 이용한 IPTV 콘텐츠 보호 및 인증 시스템 설계”, 한국콘텐츠학회논문지, 제9권, 제8호, pp.129-137, 2009.

[8] 고윤미, 권경희, “SIP에서의 강화된 사용자 인증 방식”, 한국콘텐츠학회논문지, 제11권, 제12호, pp.88-93, 2011.

[9] http://word.tta.or.kr

[10] B. Kaliski, *PKCS #8: Private-Key Information Syntax Standard V1.2,* RSA Laboratories, 2008.

[11] B. Kaliski, *PKCS #5, Password Based Cryptography Standard V2.1*, RSA Laboratories, 2000.

저 자 소 개

김 선 주(Sun-Joo Kim) 정회원

- 1998년 2월 : 배재대학교 컴퓨터공학과 졸업
- 2001년 2월 : 배재대학교 컴퓨터공학과 석사
- 2013년 2월 : 배재대학교 컴퓨터공학과 박사
- 2001년 1월 ~ 2003년 9월 : ㈜케이사인 선임연구원

▪ 2013년 9월 ~ 현재 : 한국정보통신기술협회 책임연구원

<관심분야> : 클라우드 컴퓨팅, SW 테스팅, 정보보호 제품 평가

조 인 준(In-June Jo) **정회원**

▪ 1982년 2월 : 전남대학교 계산통계학과 졸업

▪ 1985년 2월 : 전남대학교 전자계산학과 석사

▪ 1999년 2월 : 아주대학교 컴퓨터공학과 박사

▪ 1983년 ~ 1994년 : 한국전자통신연구원 선임연구원

▪ 1994년 1월 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : 정보보호, 컴퓨터네트워크보안, 전산조직응용