공인인증서와 OTP를 이용한 트렌젝션 보호에 관한 연구

김낙현* ·이훈재**

*동서대학교 유비쿼터스 IT학과

**동서대학교 컴퓨터 정보공학부

Sutdy of transaction protection by certificate and OTP

Nack Hyun Kim* ·Hoon Jae Lee**

*Dept. of Ubiquitous IT, DongSeo University

**Div. of Computer & Information, DongSeo University

E-mail : redroopang@hotmail.com

요 약

금융거래나 전자상거래 등 전자거래에서 공인인증서를 중심으로 OTP(One Time Password), 보안카드등이 사용되고 있다. 그러나 이러한 인증 기법을 단일적으로 사용하면, 기밀성, 무결성, 사용자 인증, 부인방지 효과를 모두 완벽하게 이룰 수는 없다. 본 논문에서는 공인인증서와 OTP의 단점을 보완하기 위해 공인인증서와 OTP 인증 방식을 병합하여 사용한 인증 방안을 제안한다.

ABSTRACT

We are using a certificate, OTP(One Time Password), Security Card etc. for safety on E-commerce. However, These are not perfectly protect Confidentiality, integrity, user authentication, and nonrepudiation. In this paper, we are proposed authentication scheme by certificate and OTP.

키워드

공인인증서, OTP, 사용자 인증

Ⅰ. 서 론

정보통신을 위한 기술이 발달함에 따라 인터넷을 통한 전자상거래와 금융거래 등과 같은 인터넷 서비스가 보편화 되어 있다. 아이디/패스워드 단일 방식만으로 사용자 인증을 할 경우 브루트 포스 공격(Brute-Force Attack), 패스워드 추측(Password Guessing), 키보드 후킹(Keyboard hooking), 피싱(Phishing), 스푸핑(spoofing)등과 같이 상당히 많은 보안 위협을 가진다. 이에 따른 피해를 막고자 금융기관을 중심으로 전자금융거래의 보안 강화를 위한 방안으로 보안토큰에 대한 중요성이 대두되고 있다. 그 예로 공인인증서, 보안카드, OTP(One Time Password)토큰, HSM(Hardware Security Module) 등을 사용하여 보안성 강화에 사용 하고 있다.

공인인증서는 무결성, 서버인증및 부인 방지 효과등을 제공 한다. 그러나 전자 서명시 원문을 포함하여 전송하기 때문에 기밀성 측면에서 취약하다고 볼 수 있다. 그리고 SSL(Secure Socket Layer)+OTP의 경우 기밀성, 무결성과 서버 인ㅇ증은 제공하지만 부인 방지 효과는 제공하지 않는다.

본 논문에서는 공인인증서와 OTP를 혼합 사용하여, 기밀성과 부인 방지 효과를 동시에 충족 할 수 있는 인증 방안을 제안한다.

Ⅱ. 관 련 연 구

2.1 공인인증서

공인인증서는 공인인증기관에서 발행하는 전자적 정보로서, 전자서명의 검증 및 암호화에 필요한 공개키에 소유자 정보를 추가하여 만든 일종의 전자 신분증이다.

공인인증서에는 사용자가 공개키가 저장되며 개인키 저장 파일에는 사용자 개인키가 저장된다. 사용자의 개인키는 다른 사용자에게 노출되면 보안상의 위험이 있으므로 SEED블록 암호 알고리즘을 이용하여 암호화한다. SEED블록 암호 알고리즘에 사용되는 비밀키는 사용자의 개인키 암호화 패스워드를 이용하여 생성된다. 전자서명시스템에서 사용되는 공인인증서와 개인키 저장파일은 현재 X.509 v3의 기준에 따라 작성되며 "TTA, TTAS.KO-12.0012, 전자서명 인증서 프로파일 표준, 2002"와 "TTA, TTAS.KO-12.0013, 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준, 2001"에 국내 표준 및 규격이 명시되어 있다.[1]

2.2 OTP(One Time Password)

OTP(One Time Password)는 사용자가 인증요구를 할 때 마다 새로운 비밀번호를 생성하여 사용하는 방식이다. 사용자와 인증기관과의 동기화 여부에 따라 동기화 방식과 비동기화 방식으로 나누어 진다.

OTP는 금융감독원의 전자거래 안전성 강화 종합대책에 의하여 거래금액이 일정액 이상일 경우 OTP사용을 의무화와 OTP 통합인증센터의 설립으로 인하여 인증 방법으로써 각광을 받고 있다.

그러나 OTP도 단일 매체로 사용하여 인증 할 경우 여러 종류의 보안적 문제점을 나타낸다. 그 예로 피싱(Phishing) 공격[2]의 경우 공격자가 가상의 피싱 사이트를 만들어 인증에 사용되는 OTP값을 획득하여 인증을 받을 수 있다. 그리고 시간 동기화 방식의 경우 공격자가 사용자와 인증 서버 중간에서 MITM(Main-IN-The Middle) 공격으로 OTP값을 획득하게 되었을 때 일정 시간동안 사용할 수 있는 위험성을 가지고 있다.[3]

Ⅲ. 제안하는 방법

본 논문에서 제안하는 인증 방식은 공인인증서에서 추출한 데이터를 OTP생성에 사용한다. 그리고 생성된 OTP값을 암호화 키로 사용하여, 전자서명과 함께 전송하는 방식이다.

사용자가 공인인증서를 발급 방법은 그림 1과 같이 기존의 방법과 동일하다. 그리고 추가적으로 추후 OTP생성에 사용될 키 값 OTPkey을 인증기관이 보유 하게 된다.

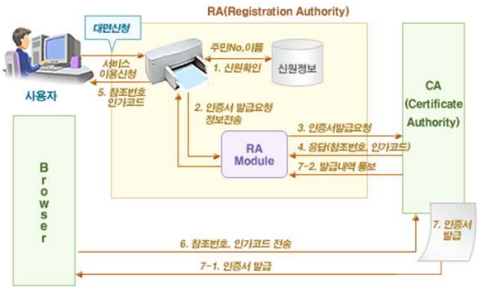

그림 1. 공인인증서 발급 과정

공인인증서는 signCert.der 파일과 signPri.key 파일로 구성되어 있다. 개인키 키는 signPri.key파일에 암호화 되어 저장되어 있다. 사용자가 공인인증서 비밀번호를 입력하면 개인키를 추출 한다. 이과정에서 OTPkey를 추출한다. 이 내용은 그림 2에서 확인 할 수 있다.

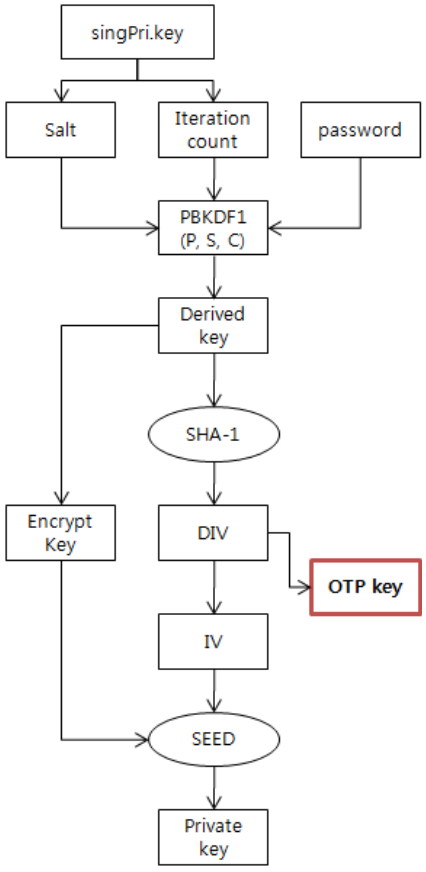

그림 2. OTPkey 추출 과정

암호화된 개인키에서 Salt 와 iteration count를 추출하게 된다. Salt는 공인인증서를 발급할 때 마다 난수 형태로 생성 되는 것으로, 불특정 다수의 사전 공격을 방지 한다. 그리고 iteration count는 비밀키 생성을 위해 사용한 해쉬 함수를 포함 하고 있다.

사용자가 입력한 Password를 Salt와 iteration count를 이용하여 추출키인 Derived key를 추출하게 된다[4]. 그리고 추출키에서 개인키 복호화에 사용될 Encrypt key 와 초기화 백터 IV를 추출하게 된다. 이 과정에서 IV를 추출 하고난 후 나머지 값을 OTPkey로 사용한다.

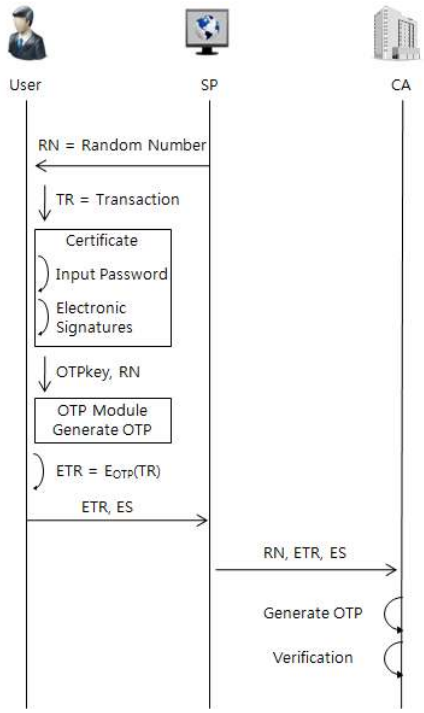

그림 3. 인증 과정

본 논문에서 제안하는 사용자가 실제적으로 임하는 행동은 기존의 방식과 동일하다. 그리고 실제 데이터의 흐름은 그림 3으로 표시 한다. 사용자는 서비스 제공자로부터 난수 RN을 전달 받는다. 그리고 사용자가 입력한 Password 와 Transaction을 공인인증서로 전자 서명을 실시한다. 이때, 추출한 OTPkey 와 RN을 이용하여 OTP를 생성한다. 생성된 OTP를 이용하여 평문을 암호화 하여, 전자서명된 파일과 함께 서비스 제공자에게 전송한다. 그리고 서비스 제공자는 자신이 생성한 RN을 추가하여 인증 기관에게 전송한다. 인증기관은 초기 등록에 저장된 OTPkey 바탕으로 OTP를 생성하게 되고, 전자 서명을 검증 하게 된다.

Ⅳ. 결 론

본 논문에서는, 공인인증서의 부인 방지 효과와 OTP의 일회성을 바탕으로 기밀성, 무결성, 사용자 인증, 서버 인증과 부인방지 효과를 가지는 인증 방안을 제안 하였다.

참고문헌

[1] 한국정보보호진흥원, "공인인증서 표시를 위한 기술규격", Vol. 1.10, 2008.10

[2] T Moore, R Clayton, "An empirical analysis of the current state of phishing attack and defence", Workshop on the Economics of information, 2007

[3] 이장춘, 이훈재, 김태용, “스트림 알고리즘을 이용한 OTP 생성 및 동기화 인증 프로토콜”, 한국해양정보통신학회 추계종합학술대회, 2007

[4] http://www.ietf.org/rfc/rfc2898.txt