중소기업융합학회 논문지 제4권 제3호 pp. 27-31, 2014 ISSN 2234-4438

중소기업형 바이오정보와 OTP를 이용한 사용자 인증

이상호[1*]
[1]충북대학교 정보보호경영학과

User Authentication Using Biometrics and OTP in Mobile Device

Sang Ho Lee[1*]
[1]Department of Information Security Management, Chungbuk National University

요 약 스마트기기에서 스마트뱅킹, 인터넷쇼핑, 비접촉거래 등의 지급결제 거래가 급증함에 따라 모바일 OS의 취약점, 인증서 오남용 문제 등의 보안상의 문제가 대두되며, 이에 대처할 수 있는 강력한 개인 인증 수단이 요구된다. 이와 같은 상황에 대처하기 위한 인증 수단으로 바이오인식정보와 더불어 PKI를 이용한 OTP를 적용하고자 한다. 바이오인식정보는 분실이나 도용의 위험이 적으며 OTP를 이용한다면 바이오인식정보만을 이용할 때 보다 보안성이 강화될 수 있다. 이에 본 논문에서는 모바일 기기에서 바이오인식정보와 OTP를 이용한 개인 인증 기법을 제안한다.

Abstract According to increasing of payment and settlements like smart banking, internet shopping and contactless transaction in smart device, the security issues are on the rise, such as the vulnerability of the mobile OS and certificates abuse problem, we need a secure user authentication. We apply the OTP using biometrics and PKI as user authentication way for dealing with this situation. Biometrics is less risk of loss and steal than other authentication that, in addition, the security can be enhanced more when using the biometric with OTP. In this paper, we propose a user authentication using biometrics and OTP in the mobile device.

Key Words : One Time Password, PKI, Biometrics, User Authentication

1. 서론

최근 스마트폰의 확산으로 인하여 PC에서 사용하던 인터넷 뱅킹, 인터넷 쇼핑 등의 지급결제 서비스를 스마트폰에서도 이용할 수 있게 되었다. 따라서 스마트기기의 취약점을 노린 피싱, 파밍 등의 보안사고가 급증하고 있으며 이에 대처하기 위한 강력한 인증 기법이 요구되고 있는 상황이다.

OTP(One Time Password, 일회용 패스워드)는 로그인 세션 또는 통신 시마다 매번 변경되며 단 한번만 사용가능한 패스워드이다. 일반적인 고정 패스워드가 수집에 의한 재사용 공격에 취약한 반면, OTP는 매번 패스워드가 변경되어 이전에 수집한 패스워드를 사용할 수 없게 되므로 보안성이 높다[1].

바이오인식정보는 지문이나 홍채 등 개인의 고유한 생체 정보를 추출한 정보로 도용, 변경, 분실 등의 위험이 낮기 때문에 기존의 패스워드나 PIN을 이용한 인증의 대체수단으로 각광받고 있다. 하지만 바이오인식정보는 수정이 불가능하기 때문에 공개키 기반에서 바이오인식정보에 OTP를 적용시켜 기존의 ID/패스워드 또는 바이오인식정보만을 이용한 인증보다 보안성을 향상시키고자 한다.

Received 2014-08-06 Revised 2014-08-24 Accepted 2014-08-30
*교신저자 : Sang Ho Lee(shlee@chungbuk.ac.kr)

OTP는 매우 안전한 인증 수단이지만 기존 사용자들의 OTP 전환으로 인한 불편함, 비용 문제 등으로 인해 현재 활발하게 이용되고 있지 않다. 또한 모바일뱅킹에서의 공인인증서 이용시 비밀번호 유출 가능성이 밝혀짐에 따라 안전하고 편리한 본인인증을 위하여 모바일기기를 이용한 OTP 인증, 모바일기기에서의 바이오인식정보를 이용한 인증과 모바일 OTP와 PKI의 연계방안 등에 대해 다양한 연구가 진행되고 있다[2][3]. 이에, 본 논문에서는 모바일기기에서 바이오인식정보와 더불어 시간동기화 OTP를 적용하여 안전한 본인확인을 위한 인증기법을 제안하고자 한다.

2. 관련연구

2.1 OTP 생성방식

OTP(One-Time Password) 기기는 한 세션에서 사용가능한 1회용 암호를 생성하는 보안 매체로서, 전통적인 정적 암호들이 내재하고 있는 기본적인 보안위협에 대처하기 위해 개발되었다. 현재 사용하는 비밀번호로부터 다음에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성을 가져서 기존의 여러 공격들로부터 안전하기 때문에, 금융권 전자금융거래, 기업체 사내시스템 접근통제, 인터넷포털 사이트의 사용자 인증 등 여러 분야에서 활발하게 사용되고 있다.

일반적으로, OTP 토큰은 고유 OTP 생성키 뿐만 아니라 동기화 데이터에 기초하여 상기 OTP 생성 기능을 통해 패스워드를 생성하기 때문에 OTP 생성키와 동기화 데이터 등의 입력 데이터를 필요로 한다. 또한, 특정 토큰은 OTP를 생성하기 위해 활성화의 데이터를 필요로 할 수 있다.(그림1 참조)

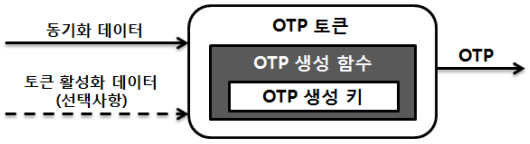

Fig. 1. 일반적인 OTP 생성기

입력 데이터의 조합이 OTP 생성 함수의 출력으로 나오기 때문에 입력 데이터에 따라 다른 특성을 갖는 OTP 타입을 생성 할 수 있다. 입력 데이터의 특징에 따라 네 가지 유형으로 나눌 수 있는데 비동기화 방식의 경우 질의응답 방식이 있고, 동기화 방식의 경우 시간 동기화 생성방식, 이벤트 동기화 생성방식 및 이 두 방법을 조합한 조합생성방식이 있다. 입력데이터의 조합을 살펴보면 OTP 입력 값으로 질의응답 방식은 사용자가 OTP 인증요청 시 인증서버로부터 받은 질의 값을 받고, 시간 동기화 방식은 현재시간 값을 입력받으며, 이벤트 동기화 방식의 경우 이벤트 카운터 값을 입력받는다. 그리고 마지막으로 조합방식의 경우, 시간 표현 값과 이벤트 카운트 값을 모두 입력받는다[4].

특히 시간동기화 방식과 이벤트 동기화 방식을 보안 및 사용성 측면에서 매우 유사하며 기본 암호화가 두 가지 방법에 본질적으로 동일하다는 점을 감안할 때 우리는 작동 방법상에서의 몇 가지 문제점을 발견할 수 있다. 이벤트 동기화 방식의 경우 OTP값이 자동으로 지정된 시간 후에 만료되지 않는다는 특징이 있는데 이로 인해 OTP값이 악의적 공격자에게 넘어갔을 때 이 OTP가 나중에 사용자 계정 해킹에 이용될 수 있다는 단점이 있다. 시간동기화 방식의 경우, 각각의 OTP는 짧은 시간에서만 유효하다. 따라서 이벤트 동기화 방식에서 적용될 수 있는 공격방법이 시간동기화 방식에서는 적용될 수 없다. 하지만 시간동기화 방식의 경우 OTP값이 OTP토큰에 지속적으로 나타나기 때문에 OTP의 노출이 잦고 때문에 기기의 관리가 중요하다[5].

2.2 공개키 기반 구조(PKI)

공개키 암호화란 송신자는 수신자의 공개키로 자신의 정보를 암호화하여 전송하고, 수신자는 자신의 개인키로만 복호화 할 수 있는 기법으로 오늘날 공개키 기반구조(Public Key Infrastructure, PKI)는 전자서명을 통한 인증, 부인방지 서비스의 제공과 함께 대칭키와 비대칭키의 결합을 통한 기밀성 보장 및 키 관리 서비스의 사용을 위한 기반구조로써 널리 이용되고 있다[6].

Fig. 2. 공개키 기반 암호화 원리

PKI(공개키 기반 구조)는 X.509 인증서에 기반하여 인증기관 이라 불리는 신뢰할 수 있는 기관에서 부여된

공개키와 개인키를 사용함으로써, 안전하게 정보를 교환할 수 있기 때문에 인터넷 표준으로 자리잡고 있다. PKI는 암호화를 통한 기밀성유지, 선택된 수신자만이 정보에 접근할 수 있는 접근제어, 정보가 전송 중에 변경되지 않음을 보장하는 무결성, 정보의 원천지 인증, 정보가 송신자에 의해 전송되었음을 보장하는 부인봉쇄 등 5가지 보안기능 요소를 제공한다.

공개키는 사용자가 연관된 개인 키를 암호화 또는 디지털 서명 메커니즘에 사용할 때 정확한 사람 또는 시스템이 소유하고 있어야 한다. 공개키는 인증서 사용을 통해 얻어지는데 이때의 인증서는 신뢰할 수 있는 제 3자, 즉 CA의 서명을 통해 얻을 수 있다. CA는 본인의 개인키를 이용하여 인증서를 얻고자 하는 사람 또는 시스템에게 인증서를 발급하며, 이 인증서를 사용하여 사용자는 신뢰할 수 없는 통신 및 서버 시스템을 배제할 수 있다[7].

공개키 암호화는 두 개의 키(공개키-개인키)를 이용하므로 무결성 뿐만 아니라 기밀성, 키분배 및 인증분야에서 성능이 뛰어나다[8]. 따라서 공개키 기반 암호화를 통해 민감한 프라이버시 정보인 바이오인식정보의 강력한 보호가 가능하다.

2.3 바이오인식정보

바이오인식 시스템에서의 바이오인식 정보를 설명하기 위하여 먼저 설명되어야 할 것이 바이오인식 템플릿이다. 국제 표준(ISO)에 따르면 바이오인식정보는 다음과 같이 정의된다.

- 바이오인식 정보(biometric reference): 비교를 위해 개인식별 대상자에 대해서 추출한 속성으로 하나 또는 다수의 저장된 바이오인식 샘플, 바이오인식 템플릿, 바이오인식 모델 등을 의미한다.

위의 정의에 따르자면, 얼굴이나 지문 영상과 같은 바이오인식 샘플뿐만 아니라, 이들로부터 추출된 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값과 같은 특징값이 저장된 형태의 바이오인식 템플릿을 포함한다. 뿐만 아니라 음성인식시스템에 있어서 화자의 발음으로부터 추출된 가우시언 혼합모델 (Gaussian Mixture Model)도 여기에 포함된다.

한편, 한 개인의 신원을 나타내는 식별자(identity)는 그 사람이 신원 확인하기를 바라는 상황에서 대상자와 관련된 모든 속성이라고 할 수 있으며, 따라서 한 사람에 대해서 다수의 식별자가 제시될 수도 있다[9]. 본 논문에서는 바이오인식정보의 유출을 방지하기 위해 2.2절에서 언급한 공개키 암호화를 사용한다.

3. 모바일기기에서 바이오인식정보와 OTP를 이용한 본인인증기법

3.1 약어 및 용어

- MD (Mobile Device) : 사용자의 모바일기기
- AS (Authentication Server) : 인증서버
- BIO (Biometric Reference) : 사용자가 모바일기기에 인식한 바이오인식정보
- BIO_S (Server Biometric Reference) : 인증서버에 등록된 바이오인식 템플릿
- BIO_M (Mobile Biometric Reference) : 모바일기기에 저장된 바이오인식 템플릿
- OTP_S (Server One Time Password) : 인증서버에서 생성한 OTP
- OTP_M (Mobile One Time Password) : 모바일기기에서 생성한 OTP
- RN (Random Number) : OTP 알고리즘으로 생성한 난수
- Input(A) : A를 입력
- OTP(A) : A를 OTP 알고리즘에 적용
- Sign_U(A) (User Sign Algorithm) : A를 사용자의 개인키로 서명
- Veri_S(A) (Server Verification Algorithm) : A를 인증서버의 공개키로 검증
- Enc_S(A) (Server Encryption Algorithm) : A를 인증서버의 공개키로 암호화
- Dec_S(A) (Server Decryption Algorithm) : A를 인증서버의 개인키로 복호화

3.2 수행환경

본 논문에서 제안한 본인인증이 수행되기 위해 다음을 가정한다.

- 사용자는 사전에 인증서버에 바이오인식정보를 등

록했고, 모바일기기에 바이오인식정보를 저장했다.
- PKI 암호화 알고리즘에 이용되는 공개키와 개인키는 사전에 분배되었다.
- 난수(RN)는 각각 시간동기화, 질의응답 방식을 사용하여 생성한다.
- 시간동기화 방식의 경우, 모바일기기와 인증서버는 동기화를 통해 항상 동일한 시간을 유지한다.

3.3 시간동기화 OTP를 이용한 각 단계별 인증 절차

제안 모델 중 시간동기화 OTP를 이용한 기법의 인증 절차를 단계별로 구체화하였다. 다음의 ①~⑦의 단계를 거쳐서 최종적으로 본인인증을 수행한다.

3.3.1 공인인증서 로그인

사용자는 모바일기기에서 공인인증서 로그인을 하고, 로그인이 완료되면 다음 단계를 진행한다.

① MD → AS : 공인인증서 로그인

3.3.2 인증 서버 OTP 생성

사용자 기기 인증이 완료되면 인증 서버는 생성한 난수(RN)와 등록된 바이오인식 템플릿을 OTP 알고리즘의 입력 값으로 하여 다음과 같이 OTP 값을 생성한다.

② AS : 서버에 등록된 바이오인식정보(BIO_S)와 난수(RN)를 XOR한 값(BIO_S ⊕ RN)을 OTP 알고리즘에 입력하여 OTP_S 생성

3.3.3 모바일 OTP 생성 및 전송

모바일기기에서는 바이오인식정보를 입력 받아 저장된 바이오인식 템플릿과 비교하여 동일인의 정보인지 확인한다. 동일인으로 확인되면 난수(RN)와 저장된 바이오인식 템플릿을 OTP 알고리즘의 입력값으로 하여 OTP 값을 생성하고 이를 암호화하여 서버로 전송한다.

③ MD : 바이오인식정보 입력
④ MD : 저장된 바이오인식 템플릿과 난수(RN)를 XOR한 값(BIO_M ⊕ RN)을 OTP 알고리즘에 입력하여 OTP_M생성
⑤ MD → AS : 생성한 OTP_M을 사용자의 개인키로 서명하고 서버의 공개키로 암호화하여 인증서버로 전송

3.3.4 OTP 인증

인증서버는 모바일기기로부터 전송 받은 OTP 값과 인증서버에서 생성한 OTP 값이 일치하는지 비교하고, 두 값이 동일한 값이라면 인증을 완료한다.

⑥ AS : 전송 받은 값을 서버의 개인키로 복호화한 후 사용자의 공개키로 검증한다.
⑦ AS : OTP_M과 OTP_S가 일치하면 사용자 인증 완료

3.4 제안 모델과 기존 모델 비교

기존에 연구되었던 모델(그림 3)과 제안 모델(그림 4)은 사용자가 입력한 정보를 PKI 기반에서 OTP 기법을 적용시켜 암호화한다는 점에서 유사하다. 하지만 기존 모델은 패스워드 기반이기 때문에 패스워드가 유출되면 타인이 인증 받을 수 있는 위험이 존재하며, 기존 모델의 OTP 생성방식은 질의응답 방식을 사용하여 난수를 전송하기 위한 추가적인 암호화/복호화 과정이 요구된다.

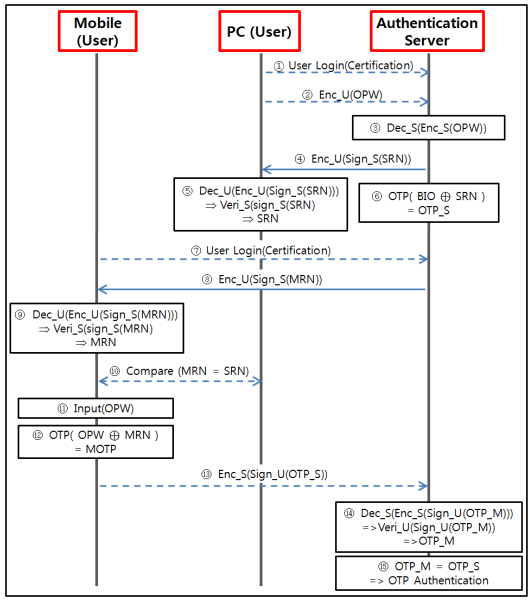

Fig. 3. PKI기반의 모바일 OTP 메커니즘[2]

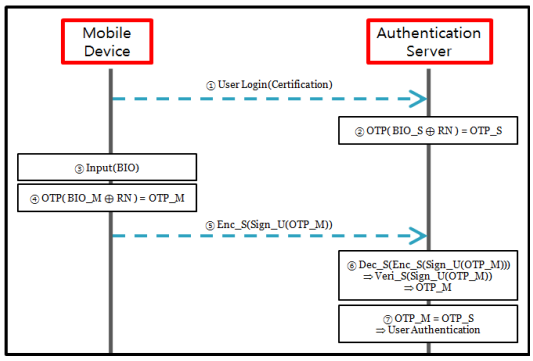

Fig. 4. 제안된 모바일 본인인증 기법 – 시간동기화 OTP

반면 시간동기화 OTP를 사용한 방식의 경우, 난수 전송을 위한 별도의 암호화/복호화 과정이 필요하지 않다. 또한 제안모델의 경우 사용자가 입력하는 패스워드 대신 바이오인식정보를 입력하여 본인인증을 진행하기 때문에 패스워드를 이용할 때에 비해 도난, 분실 위험이 없으며 유일성을 보장한다.

제안 모델에서는 공인인증서 로그인 후 바이오정보를 입력하면 사용자 인증이 수행되는 관계로 안전한 본인인증이 이루어진다.

4. 결론

최근 각종 개인정보 유출 사고가 발생하면서 기존의 문자로 이루어진 패스워드에 대한 불신이 커짐에 따라 바이오인식정보를 이용하여 본인 인증을 하고자 하는 연구가 활발히 진행되고 있다.

본 논문에서는 모바일기기에서 바이오인식정보와 OTP 및 PKI를 이용한 본인인증 기법을 제안하였다. 제안 기법에서 이용되는 PKI는 국내 금융 거래에서도 이용하고 있는 안전성이 매우 뛰어난 기술로, 사용자 인증을 받기 위한 값을 안전하게 전송하기 위해 사용된다. 그러나 OTP와 PKI만을 이용한 기존 기법에서는 OTP 생성 비밀번호를 탈취당한다면 얼마든지 타인이 본인인증을 받을 수 있다. 그러나 제안 기법에서는 바이오인식정보를 입력받기 때문에 본인이 아닌 경우에는 절대로 인증을 받을 수 없다.

아이폰6, 갤럭시S5 등 지문인식기능을 갖춘 스마트폰이 출시되고, 스마트폰용 홍채인식 솔루션이 개발되는 등 특히 모바일기기에서 바이오인식정보를 이용한 본인인증 기술이 활발히 개발 되고 있는 상황을 감안할 때, 본 연구 결과를 금융결제 등의 응용에 널리 사용 될 수 있으리라 생각된다.

참 고 문 헌

[1] 금융보안연구원. (2010), 일회용 패스워드(OTP) 키 컨테이너, 한국정보통신기술협회.(http://committee.tta.or.kr/data/standard_view.jsp?rn1=Y&standard_no=TTAK.KO-12.0129&pk_num=TTAK.KO-12.0129&nowSu=1&rn=1)

[2] 김태형, (2011), “피싱방지 및 가용성개선을 위한 PKI기반의 모바일OTP 메커니즘 연구”, 고려대학교 금융보안학과 석사학위 논문.

[3] 김홍기, 이임영, (2011), “모바일 환경에서 안전한 One-Time Password 인증 기법에 관한 연구”, 멀티미디어학회논문지, Vol.14 No. 16, pp. 785-793.

[4] ITU-T X.1153 Management framework of a one time password-based authentication service. (2011)

[5] Andrew Y. Lindell. (2007). “Time versus Event Based One-Time Passwords”, SafeNet.

[6] 양종필, 신원, 이경현, (2006), “효율적인 공개키 프레임워크에 대한 실용적 개선과 응용”, 한국통신학회논문지, Vol.31, pp.472-481

[7] R.Housley, W. Ford, W. Polk and D. Solo. (1999). “Internet X.509 public key infrastructure certificate and CRL profile”, RFC 2459. (http://www.ietf.org/rfc/ rfc2459.txt)

[8] 서상원, (2007), “메시지 인증과 공개키 암호화”, 월간 마이크로소프트웨어, pp.306-313.

[9] 신용녀, 권만준, 이용준, 박진일, 전명근, (2009), “개인식별정보와 바이오인식정보의 보호기법”, 한국지능시스템학회 논문지, Vol. 19, No. 2, pp.160-167.

저 자 소 개

이 상 호(Sang Ho Lee) [정회원]

▪ 1981년 3월 ~ 현재 : 충북대학교 전자정보대학 소프트웨어학과 교수

<관심분야> : 네트워크 보안, 개인정보보호, 데이터베이스 보안