모바일 장치에서 바이오인식을 이용한 개인정보 등록

A Registration of Personal Information using Biometrics in Mobile Devices

한 승 진, 김 낙 현*, 김 재 성*
경인여자대학교,
한국인터넷진흥원*

Han seung-jin, Kim nak-hyun*, Kim jae-sung*
Kyungin wemen's Univ.,
Korea Internet & Security Agency*

요약

바이오인식 기술은 기존의 패스워드나 PIN을 대체할 수 있는 새로운 수단이지만 바이오인식 기술은 한번 도용이 되면 기존의 수단과 달리 수정할 방법이 없으므로 바이오인식 정보를 안전하게 신뢰하는 제3의 장치에 등록하는 방법을 제안한다.

I. 서론

대부분의 스마트폰 사용자들은 장치의 휴대성으로 인해 스마트폰을 이용하여 금융결제 서비스를 이용하고 있다.

▶▶ 그림 1. 모바일 장치에서 이용가능한 바이오인식 정보

그러나 무선 환경은 유선 환경에 비해 보안이 취약하다. 또한 외국의 쇼핑몰 및 앱스토어에서는 공인인증서 없이 결제가 가능하다. LG CNS[1], 애플, 알리바바 등 국내외 업체들은 IT 기술을 기반으로 이러한 문제점들을 극복하려고 한다[2]. 그러나 패스워드나 PIN 또는 바이오인식 정보만을 사용하는 1FA(Factor Authentication)는 많은 문제점을 내포하고 있다. 따라서, 본 논문에서는 모바일 환경에서 바이오인식 정보를 이용하여 안전하게 금융결제에서 본인의 정보를 등록할 수 있는 방법을 제안한다.

II. 관련 연구

모바일 장치에 적용된 바이오인식 표준 사례를 살펴본다.

1. 모바일 장치에서 바이오인식을 이용한 보안 모델

모바일 장치를 이용하여 바이오인식 정보를 획득하고, 비교하고, 저장하기 위한 기술 및 관리적 보안 지침[3]에서는 인증 모델을 바이오인식 정보 획득, 저장 및 비교의 주체 방식에 따라 12가지 모델을 제시하였다.

Ⅲ. 모바일 장치에서 바이오인식을 이용한 개인정보 등록

본 논문에서 제안하는 수식을 간단하고 명료하게 하기 위해 다음과 같은 기호를 정의한다.

표 1. 기호

기호	설명
$\{X \rightarrow Y : M\}$	X가 Y에게 메시지 M을 전송
$h(\bullet)$	보안성이 강한 단방향 해쉬함수
ID_i	i 번째 사용자의 ID
PW_i	i 번째 사용자의 패스워드
PIN_i	i 번째 사용자의 PIN(Personal Identity Number)
B_{i,x,y_j}	i 번째 사용자에게 획득한 x 종류의 바이오인식 정보 중 j 번째 바이오인식 정보
b_{i,x,y_j}	i 번째 사용자에게 획득한 x 종류의 바이오인식 정보 중 j 번째 바이오인식 정보를 해쉬 함수로 해쉬한 결과
U_{PK}	사용자의 공개키
U_{SK}	사용자의 개인키
S_{PK}	TTP 서버의 공개키

* 본 연구는 미래창조과학부 '2014-PM10-14: 모바일 바이오인식 신융합기술 표준개발' 연구과제의 일환으로 수행하였음

$S_{PK_{tmp}}$	TTP 서버의 임시 공개키
S_{SK}	TTP 서버서버의 개인키
EK_{US}	사용자와 서버간의 비밀 대칭키
ts_U	사용자의 타임스탬프
ts_S	서버의 타임스탬프
R_1	임의의 난수 1
R_2	임의의 난수 2

1. 등록단계

최초에 모바일 장치 사용자는 서버에 ID와 PW 혹은 PIN을 이용하여 TTP(Trusted Third Party)에 TTP의 공개키을 요청한다. 이 공개키는 TTP가 임시로 발급한 키로서 이후 단계에서 사용자의 바이오인식 정보를 이용하여 생성한 키로 변경된다.

TTP의 서버는 사용자로부터 받은 바이오인식 정보를 [4]를 이용하여 서버의 공개키를 만들어 전송한다. 이때 서버의 공개키는 각 사용자의 바이오인식 정보를 사용하기 때문에 모두 다르다. TTP의 서버는 사용자와 세션이 연결되는 동안 이 공개키를 사용한다.

사용자는 TTP 서버에 서버의 임시 공개키를 요청한다.

$r_1 = h(R_1)$

$$\{U \rightarrow TTP : ID_i, h(PW_i|PIN_i), r_1\} \quad (1)$$

TTP 서버는 서버의 임시 공개키를 사용자에게 발급한다.

$$\{TTP \rightarrow U : r_1, S_{PK_{tmp}}\} \quad (2)$$

사용자는 r_1를 통해 자신이 요청한 TTP 서버로부터 전송된 메시지임을 안다.

$$b_{i,x,y_n} = h(B_{i,x,y_n}) \quad (3)$$

$$ts1_U = U_{SK}(TS1_U) \oplus R_1 \quad (4)$$

$$\{U \rightarrow TTP : E_{S_{PK_{tmp}}}((ID_i, h((PW_i|PIN_i) \| B_{i,x,y_1}), b_{i,x,y_1}), h((PW_i|PIN_i) \| B_{i,x,y_2}), b_{i,x,y_2}), \ldots, h((PW_i|PIN_i) \| B_{i,x,y_n}), b_{i,x,y_n}), U_{PK}, ts1_U)\} \quad (5)$$

i번째 사용자는 x형태의 바이오인식 모달리티를 y번째 템플릿을 해쉬화하고, 메시지를 전송할 때의 타임스탬프를 사용자의 개인키로 전자서명하고 임의의 난수와 XOR하여 서버에게 전송한다. 식 (7)에서 서버로부터 $ts1_U$를 재전송 받아 저장된 타임스탬프와 비교한다.

사용자의 단말기는 서버로 바이오인식 정보를 전송한 후 원본은 삭제하고, 해쉬화된 바이오인식 정보만 저장한다. 서버는 전송받은 바이오인식 정보를 사용자의 암호화하여 저장한다.

$$ts1_S = S_{SK}(TS1_S) \oplus R_2 \quad (6)$$

$$\{TTP \rightarrow U : E_{U_{PK}}(h(ID_i \| EK_{US}) \oplus h((PW_i|PIN_i) \| (b_{i,x,y_1}) \| (b_{i,x,y_2}) \| \ldots \| (b_{i,x,y_n})), ts1_U, ts1_S)\} \quad (7)$$

서버는 사용자와 서버 사이에 사용할 비밀 대칭키를 사용자에게 전송한다. (7)의 메시지를 수신한 사용자는 $ts1_U$를 검증하여 자신이 보낸 것인지 검증한다.

$$\{TTP \rightarrow U : E_{U_{PK}}(h(ID_i \| S_{PK}) \oplus h((PW_i|PIN_i) \| (b_{i,x,y_1}) \| (b_{i,x,y_2}) \| \ldots \| (b_{i,x,y_n})), ts1_U, ts1_S)\} \quad (8)$$

사용자에게 서버의 공개키 전송받는다. 사용자는 서버로부터 받은 두 개의 메시지를 이용하여 EK_{US}와 S_{PK}를 얻는다.

$$\{U \rightarrow TTP : S_{PK}(ID_i, ts1_S)\} \quad (9)$$

사용자는 서버의 공개키를 이용하여 자신의 아이디와 서버로부터 전송받은 $ts1_S$를 재전송하고, 이를 수신한 서버는 자신이 ID_i에게 보냈던 메시지임을 확인한다.

Ⅳ. 결론 및 추후연구

본 논문에서는 다중 바이오인식 정보를 안전하게 TTP 서버에 등록하는 프레임워크를 제안하였다. 기존의 방식과 달리 다중 바이오인식 정보와 다중 모달리티를 사용할 수 있는 방법을 제안하였다. 추후 연구과제로는 본 논문을 확장하여 인증 및 거래(Transaction) 단계 및 삭제 단계에 대해서 사용자, TTP, 금융기관간의 서비스 프레임워크에 적용할 예정이다.

■ 참 고 문 헌 ■

[1] 정운호, "모바일결제 및 공인인증서 대체인증수단 동향," http://www.t-town.co.kr:8080/images/Event/2014tech/5_tmonet_mobilepay.pdf, LG CNS, 14th, May, 2014.

[2] Seungjin Han, A Financial Security using Mobile Biometrics Application and Technology, Technical Report, KISA, March, 2014.

[3] ITU-T, "A Guideline to Technical and Operational Countermeasures for Telebiometric Applications using Mobile Devices," Comm. 3rd Draft Recommendation ITU-T X.1087(X.tam)

[4] Lin You, et. al., "Signature Systems on Smart Card with Keys Generated by Fingerprint," pp. 675-679, ICACT2006, Feb. 20-22, 2006.