Journal of The Korea Society of Computer and Information
Vol. 20, No. 1, January 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.1.143

모바일 환경에서 다중 바이오인식 기반의 금융 거래를 위한 사용자 인증 프레임워크

한 승 진*

A Framework of User Authentication for Financial Transaction based Multi-Biometrics in Mobile Environments

Seung-Jin Han*

요 약

바이오인식 기술은 기존의 PIN이나 패스워드와 달리 분실하거나 도용될 가능성이 적기 때문에 새로운 인증 수단으로 대체되고 있다. 그러나 바이오인식 정보는 PIN이나 패스워드 혹은 개인정보와 달리 노출되어 도용이 된다면 수정할 방법이 없다. 따라서, 기존의 단일 모달리티에 단일 바이오인식 정보처럼 노출이 되면 치명적인 방법이 아닌 다중 모달리티와 다중 바이오인식 정보를 사용하여 사용자와 TTP 혹은 금융기관 간 인증하도록 함으로써 본 논문은 보다 신뢰성있는 방법을 제안하고 기존의 방법과 보안 및 성능을 비교한다.

▸ Keywords : 바이오인식, 다중 모달리티, 다중 바이오인식, 패스워드, 모바일 장치, 제3의 신뢰기관, 금융기관, 금융거래

Abstract

Biometric technology has been proposed as a new means to replace conventional PIN or password because it is hard to be lost and has the low possibility of illegal use. However, unlike a PIN, password, and personal information there is no way to modify the exposure if it is exposed and used illegally. Therefore, the existing single modality with single biometrics is critical when it expose. However in this paper, we use a multi-modality and multi-biometrics to authenticate between users and TTP or between users and financial institutions. Thereby, we propose a more reliable method and compared this paper with existed methods about security and performance in this paper.

•제1저자 : 한승진
•투고일 : 2014. 11. 15, 심사일 : 2014. 11. 24, 게재확정일 : 2014. 12. 1.
* 경인여자대학교 e-비즈니스과(Dept. of e-Business, KyungIn Women's College)

▸ Keywords : Biometrics, Multi-Modality, Multi-Biometrics, Password, Mobile Device, TTP, Financial Institution, Financial Transaction

I. 서 론

국내 대다수의 스마트 모바일 장치 이용자들은 모바일 결제 서비스를 사용하고 있다. 외국의 대부분 쇼핑몰 및 앱스토어에서는 공인인증서 없이 결제가 가능하지만 국내에서는 공인인증서 사용에 의해서 모바일 결제 시장이 활성화되지 못하고 있다. 모바일 결제 방식에는 PG(Payment Gateway) 사를 통해 금융정보와 공인증서를 연동하여 결제처리하는 모바일 신용카드, 금융정보 대신 전화번호와 주민등록번호 입력만으로 결제 처리하는 휴대폰 결제, NFC 방식으로 충전 후 결제하는 모바일 교통카드, 은행, 카드사 스마트폰 앱을 이용하여 송금 서비스하는 모바일 뱅킹, 스마트폰 앱에 카드 정보를 사전에 입력하여 온라인 결제 수단으로 활용하는 전자지갑, 스마트폰 운영체제 및 결제 앱을 활용하여 결제하는 모바일 간편 결제 등이 있다. 그러나 대부분이 일정 금액 이상 결제 시 모바일 신용카드처럼 공인인증서를 요구하고 있다. 이를 대체하고자 여러 방법이 제안되고 있고, 최근에는 LG CNS가 MPay[1]라는 모델을 이용하여 금융감독원으로부터 보안 가군을 획득하였다.

그림 1은 휴대전화(모바일 장치)에서 사용가능한 바이오인식 정보들이다. 이를 이용하여 기존의 PIN(Personal Identity Number)이나 패스워드를 대체하고자 하는 연구들이 있다[2-8]. 기존의 바이오인식 기반의 시스템은 단일 장치내에서 바이오인식 정보의 획득, 처리, 인식 등을 모두 처리하는 장치에 적용되지만, 최근에는 단일 시스템에서 클라우드 방식의 서버와 클라이언트 방식으로 변경되는 추세이다. 이러한 추세는 바이오인식 데이터를 금융거래[4], 의료정보[5,6]에 적용하고자 하는 많은 노력들이 있다.

바이오인식 기술은 기존의 PIN이나 패스워드와 달리 분실하거나 도용될 가능성이 적기 때문에 PIN이나 패스워드를 대체할 새로운 수단으로 대두되고 있다. 그러나 바이오인식은 PIN이나 패스워드와 달리 유출되어 도용이 된다면 수정할 방법이 없다.

그림 1. 모바일 장치에서 이용 가능한 바이오인식 정보
Fig. 1. Mobile Device using Biometrics

본 논문에서는 모바일 장치에서 바이오인식 정보를 이용하여 난수를 발생시키고, 이를 타임스탬프와 함께 악의의 공격으로부터 안전하게 메시지를 전송하는 방법을 제시한다. 또한 사용자의 바이오인식 정보를 단일이 아닌 다중 모달리티와 다중 바이오인식 정보를 이용하여 바이오인식 정보가 노출이 되더라도 다른 바이오인식 정보를 사용할 수 있는 방법을 제안한다. 이를 통해 기존의 PIN이나 패스워드 혹은 바이오인식 정보만을 이용한 인증의 문제점을 해결하고 금융거래에 사용할 수 있는 프레임워크를 제안하고자 한다.

본 논문은 III장에서 TTP, 금융기관, 사용자간의 바이오인식 정보 등록, 비밀 대칭키 교환을 비롯하여 인증, 갱신, 삭제 단계를 정의하고, IV장에서는 본 논문에서 제안하는 방법에 대해 보안성 평가를 하고, V장에서는 결론 및 추후 연구과제에 대해서 기술한다.

II. 관련 연구

관련연구에서는 모바일 장치에 바이오인식을 적용한 보안 서비스 사례를 살펴보고, 문제점을 기술한다.

2.1 모바일 장치에서 바이오인식을 이용한 보안 모델

모바일 장치를 이용하여 바이오인식 정보를 획득하고, 비교하고, 저장하기 위한 기술 및 관리적 보안 지침[9]에서는 인증 모델을 바이오인식 정보 획득, 저장 및 비교의 주체 방식에 따라 12가지 모델을 제시하였다.

표. 1. 모바일 바이오인식 인증 모델
Table. 1. Authentication Model of Mobile Biometrics

	BioHSM	모바일 장치	서버
인증모델 1	획득	비교, 저장*	
인증모델 2	획득	비교	저장
인증모델 3	획득		비교, 저장
인증모델 4	획득, 비교		저장
인증모델 5	획득, 비교	저장	
인증모델 6	획득, 비교, 저장		
인증모델 7	획득, 저장	비교	
인증모델 8	획득, 저장		비교
인증모델 9	획득	저장	비교
인증모델 10		획득, 비교, 저장	
인증모델 11		획득	비교, 저장
인증모델 12		획득, 비교	저장

* 바이오인식 참조 템플릿이 저장되는 장소

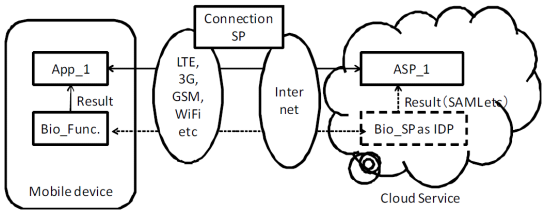

그림 2. ITU-T X.tam 표준 환경
Fig. 2. ITU-T X.tam Standard Environments

본 논문은 ITU-T X.tam의 12가지 모델 중 인증모델 3을 이용하지만, 바이오인식 정보의 원본을 저장하는 것이 아니라 사용자의 단말기에서 바이오인식 정보를 획득한 후 이를 해쉬화하여 TTP(Trusted Third Party)로 전송하고, TTP 역시 원본은 알지 못한다. 사용자의 단말기에서는 바이오인식 정보를 해쉬화하고, TTP로 전송한 후에는 바로 삭제한다.

2.2 모바일 장치에서 바이오인식 정보를 이용한 보안

[10]은 음성의 바이오인식 정보를 이용하여 모바일용 일회용 암호키를 생성해 내는 기법을 제안하였고, 이를 이용하여 모바일 뱅킹 프로토타입 시스템에서 음성 OTP(One Time Password) 생성 및 인증과정을 제안하였다. [11]은 지문을 이용하여 스마트 카드에 개인키를 저장하고 오로지 등록된 사용자의 지문과 비교하고자 하는 사용자의 템플릿과 동일할 경우만 사용이 가능하고, 획득한 지문을 이용하여 이를 숫자로 변환하고 개인키로 변환하는 방법을 제안하였다. 본 논문에서는 [11]의 방법을 이용하여 사용자의 바이오인식 정보로부터 키를 생성한다고 가정한다.

[12]는 사용자가 지문인식 센서가 부착된 모바일 리더를 이용하여 각 상품에 부착된 태그에 대한 정보를 읽고, 상품을 구매하고자 할 때 캐쉬 레지스터를 통해 서버와 통신한다. 그러나 획득한 바이오인식 정보에 대한 유출문제 등 관리에 대한 언급이 없다.

애플에서 서비스하고 있는 애플페이는 iPhone에 자신의 지문을 이용하여 본인임을 인증하고, NFC를 통해 결제를 하는 방법이다. 그러나 단말기 분실, NFC를 위한 동글이의 보급문제 등에 따른 해결책은 제시되지 못하고 있다.

바이오인식 정보를 USIM(Universal Subscriber Identity Module)에 저장하는 것은 부채널 공격(Side Channel Attack)에 매우 취약하다[13]. 따라서 본 논문에서 제시하는 방법은 사용자의 단말기에는 어떠한 정보도 저장하지 않고, TTP에서 조차 바이오인식 정보 원본을 저장하는 것이 아니라 해쉬화하고 암호화하여 저장되기 때문에 부채널 공격과 같은 해킹으로부터 안전하다.

III. 모바일 환경에서 다중 바이오인식 기반 금융 결제를 위한 사용자 인증

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

표 2. 기호
Table 2. Notations

기호	설명
$\{X \rightarrow Y : M\}$	X가 Y에게 메시지 M을 전송
$h(\bullet)$	보안성이 강한 단방향 해쉬함수
ID_i	i번째 사용자의 ID
PW_i	i번째 사용자의 패스워드
PIN_i	i번째 사용자의 PIN
B_{i,x,y_j}	i번째 사용자에게 획득한 x종류의 바이오인식 정보 중 y번째 바이오인식 정보
b_{i,x,y_j}	i번째 사용자에게 획득한 x종류의 바이오인식 정보 중 y번째 바이오인식 정보를 해쉬 함수로 해쉬한 결과
U_{PK}	사용자의 공개키
U_{SK}	사용자의 개인키
S_{PK}	TTP의 공개키
$S_{PK_{tmp}}$	TTP의 임시 공개키
S_{SK}	TTP의 개인키
S_{EK}	TTP가 생성한 비밀 대칭키

U_{EK}	사용자가 생성한 비밀 대칭키
F_{PK}	금융기관의 공개키
F_{SK}	금융기관의 개인키
TS_U	사용자의 타임스탬프
TS_S	TTP의 타임스탬프
TS_F	금융기관의 타임스탬프
R_1	사용자가 생성한 임의의 난수 1
R_2	TTP가 생성한 임의의 난수 2
R_3	금융기관이 생성한 임의의 난수 3
$A \stackrel{?}{\equiv} B$	A와 B가 같은지 비교
FT_i	i번째 사용자의 금융거래 내역

본 논문에서 제안하는 방법을 설명하기 전에 다음을 가정한다. TTP와 금융기관은 상호 신뢰 상태이고, 서로 상대방의 공개키(S_{PK}, F_{PK})는 알고 있다고 가정한다. 또한 금융기관이 생성한 난수의 해쉬값($r_3 = h(R_3)$)도 TTP는 알고 있다고 가정한다. 그림 3은 본 논문의 모델인 시스템 형상이다.

3.1 등록

최초에 모바일 장치 사용자는 TTP에 ID와 PW 혹은 PIN을 이용하여 TTP에 TTP의 공개키을 요청한다. 이 공개키는 TTP가 임시로 발급한 키로서 이후 단계에서 사용자의 바이오인식 정보를 이용하여 생성한 키로 변경된다.

TTP는 사용자로부터 받은 바이오인식 정보를 이용하여 TTP의 공개키를 만들어 전송한다[11]. 이때 TTP의 공개키는 각 사용자의 바이오인식 정보를 사용하기 때문에 모두 다르다. TTP는 사용자와 세션이 연결되는 동안 이 공개키를 사용한다.

사용자는 TTP에 DH 알고리즘[14]을 이용하여 TTP의 임시 공개키를 요청한다.

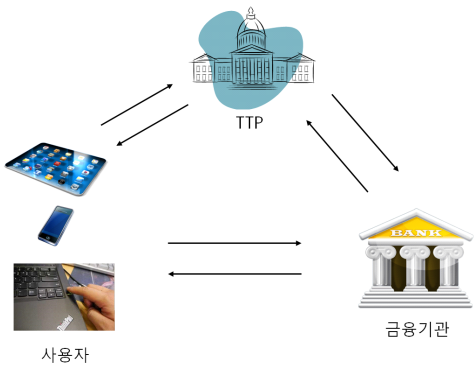

그림 3. 시스템 형상
Figure 3. System Configuration

$$r_1 = h(R_1)$$
$$\{U \rightarrow TTP : ID_i, h(PW_i | PIN_i), r_1\} \quad (1)$$

TTP는 TTP의 임시 공개키를 사용자에게 발급한다.

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

사용자는 r_1를 통해 자신이 요청한 TTP로부터 전송된 메시지임을 안다.

$$b_{i,x,y_n} = h(B_{i,x,y_n}) \quad (3)$$
$$ts1_U = U_{SK}(TS1_U) \oplus r_1 \quad (4)$$
$$\{U \rightarrow TTP : E_{S_{PK_{tmp}}}(1, (ID_i, h((PW_i|PIN_i) \| B_{i,x,y_1}), b_{i,x,y_1}, h((PW_i|PIN_i) \| B_{i,x,y_2}), b_{i,x,y_2}, \ldots, h((PW_i|PIN_i) \| B_{i,x,y_n}), b_{i,x,y_n}, U_{PK}, ts1_U))\} \quad (5)$$

식 (5)에서 1은 등록을 의미한다. i번째 사용자는 x형태의 바이오인식 모달리티를 y번째 템플릿을 해쉬화하고, 메시지를 전송할 때의 타임스탬프를 사용자의 개인키로 전자서명하고 임의의 난수와 XOR하여 TTP에게 전송한다. 식 (5)에서 TTP로부터 $ts1_U$를 재전송 받아 저장된 타임스탬프와 비교한다.

사용자의 단말기는 TTP로 바이오인식 정보를 전송한 후 원본은 삭제하고, 해쉬화하고 TTP의 공개키로 암호화된 바이오인식 정보만 저장한다. TTP는 전송받은 바이오인식 정보를 사용자의 암호화하여 저장한다.

$$ts1_S = S_{SK}(TS1_S) \oplus r_2 \quad (6)$$
$$\{TTP \rightarrow U : E_{U_{PK}}(h(ID_i \| EK_{US}) \oplus h((PW_i | PIN_i) \| (b_{i,x,y_1}) \| (b_{i,x,y_2}) \| \ldots \| (b_{i,x,y_n})), ts1_U \oplus S_{PK}, ts1_S)\} \quad (7)$$

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

TTP는 사용자에게 TTP의 공개키를 전송한다. 사용자는 TTP로부터 받은 메시지 (7)을 이용하여 EK_{US}와 S_{PK}를 얻는다.

$$\{U \rightarrow TTP : S_{PK}(ID_i, ts1_S)\} \quad (8)$$

사용자는 TTP의 공개키를 이용하여 자신의 아이디와 TTP로부터 전송받은 $ts1_S$를 재전송하고, 이를 수신한 TTP는 자신이 ID_i에게 보냈던 메시지임을 확인한다.

표 3~7까지는 사용자의 해쉬화된 바이오인식 정보를 사용자의 개인키와 TTP의 암호키를 이용하여 암호화하고 TTP에 등록한 것이다.

$$\theta(x_i,y_i) = E_{S_{EK}}(E_{U_{SK}}(h(x_i,y_i))) \quad (9)$$

TTP는 사용자의 바이오인식 정보를 표 3~7과 같이 테이블 형태로 해쉬화하고, 암호화하여 안전하게 저장한다.

표 3. 지문표
Table 3. Fingerprint table

x_1(지문)	오른손	왼손
엄지	$\theta(x_1, y_{11})$	$\theta(x_1, y_{21})$
검지	$\theta(x_1, y_{12})$	$\theta(x_1, y_{22})$
중지	$\theta(x_1, y_{13})$	$\theta(x_1, y_{23})$
약지	$\theta(x_1, y_{14})$	$\theta(x_1, y_{24})$
소지	$\theta(x_1, y_{15})$	$\theta(x_1, y_{25})$

표 4. 음성표
Table 4. Voice table

숫자	x_2(음성)
1	$\theta(x_2, y_1)$
2	$\theta(x_2, y_2)$
3	$\theta(x_2, y_3)$
4	$\theta(x_2, y_4)$
5	$\theta(x_2, y_5)$
6	$\theta(x_2, y_6)$
7	$\theta(x_2, y_7)$
8	$\theta(x_2, y_8)$
9	$\theta(x_2, y_9)$
0	$\theta(x_2, y_0)$

표 5. 얼굴표
Table 5. Face table

얼굴	x_5(얼굴)
	$\theta(x_5, NULL)$

표 6. 지정맥표
Table 6. Vein table

손	x_4(지정맥)
오른쪽	$\theta(x_4, y_1)$
왼쪽	$\theta(x_4, y_2)$

표 7. 홍채표
Table 7. Iris table

눈	x_3(홍채)
오른쪽	$\theta(x_3, y_1)$
왼쪽	$\theta(x_3, y_2)$

3.2 인증

인증 단계는 TTP와 사용자, 사용자와 금융기관 간에 인증하는 단계에 대해서 기술한다. 단, TTP와 금융기관 간에는 서로 신뢰하고, TTP는 금융기관에서 생성한 $r_3 = h(R_3)$를 알고 있다고 가정한다.

사용자는 금융기관으로 자신의 정보와 금융정보(FI_i)를 전송한다.

$$\{U \rightarrow F : E_{F_{PK}}(E_{U_{SK}}(ID_i, b_{i,x,y_n}, FI_i, r_1, TS1_U))\} \quad (10)$$

(10)을 수신한 금융기관은 메시지를 복호화 후 정보를 저장하고, 금융기관정보(F_i)를 포함한 (11)을 사용자에게 전송한다.

$$\{F \rightarrow U : E_{U_{PK}}(E_{F_{SK}}(F_i, r_3, \triangle))\} \quad (11)$$

여기서 $\triangle = TS1_F - TS1_U, 0 < \triangle \leq Threshold$이다.

Threshold는 사용자의 모바일 장치에서 임의로 정의한 임계치이다.

사용자는 금융기관으로부터 받은 메시지를 이용하여 금융기관이 적법한지 TTP에게 질의를 한다.

$$\{U \rightarrow TTP : E_{S_{PK}}(E_{U_{SK}}(F_i, h(r_1|r_3)))\} \quad (12)$$

금융기관 역시 사용자가 적법한지 여부를 TTP에게 질의를 한다.

$$\{F \rightarrow TTP : E_{S_{PK}}(E_{F_{SK}}(ID_i, b_{i,x,y_n}, h'(r_1|r_3)))\} \quad (13)$$

(12)와 (13)을 수신한 TTP는 각각의 메시지를 복호화한 후 r_1, r_3를 알고 있기 때문에 다음을 비교한다.

$$h(r_1|r_3) \stackrel{?}{=} h'(r_1|r_3) \quad (14)$$

식 (14)에서 우변에 있는 h'은 좌변에 있는 h와 구분하기 위해 표기한 것으로 같은 해쉬 함수이다.

만약에 (14)의 결과가 같지 않다면, 사용자 혹은 금융기관이 적법하지 않은 것이고, 같다면 모두 적법한 것이다. TTP는 사용자와 금융기관에게 각각 현재 접속하고 있는 대상이 적법한지 아닌지에 대한 메시지를 전송한다.

3.3 거래

거래 단계는 사용자와 금융기관 간에 거래하는 단계에 대해서 기술한다.

사용자는 바이오인식 정보를 비밀키로 암호화하고, TTP의 공개키를 비밀키를 암호화한다.

$$EK_U(b_i), S_{PK}(EK_U) \quad (15)$$

사용자는 식 (16)을 금융기관에 전송한다.

$$\{U \rightarrow F : EK_U(b_{i,x,y_n}), S_{PK}(EK_U), FT_i, (h(FT_i)|h(b_{i,x,y_n})) \\ U_{SK}(h(h(FT_i)|h(b_{i,x,y_n})))\} \quad (16)$$

이를 수신한 금융기관은 사용자가 보내온 메시지를 금융정보가 변조되었는지 식 (17)처럼 확인한다.

금융기관은 식 (16)으로부터 수신한 금융정보(FT_i)를 이용하여 새롭게 해쉬화하여 $h(FT_i)|h(b_{i,x,y_n})$에서 해쉬화된 금융정보(FT_i)를 대체한다.

사용자의 공개키를 이용하여 사용자의 개인키를 암호화된 내용을 복호화한다. 이후 새롭게 이중 해쉬화된 내용과 비교한다.

$$U_{PK}(U_{SK}(h(h(FT_i)|h(b_{i,x,y_n})))) \\ \stackrel{?}{=} h(h'(FT_i)|h(b_{i,x,y_n})) \quad (17)$$

금융기관은 TTP로 식 (18)을 전송한다.

$$\{F \rightarrow TTP : EK_U(b_i), S_{PK}(EK_U), (h(FT_i)|h(b_i)), \\ U_{SK}(h(h(FT_i)|h(b_i)))\} \quad (18)$$

TTP는 S_{PK}를 이용하여 b_{i,x,y_n}를 구하고, 금융기관에서 수행한 방법과 유사하게 식 (16)에서 (17) 사이의 과정을 수행하여 사용자의 바이오인식 정보가 변조되었는지 확인한다. 또한 표 3~7 사이의 바이오인식 정보와 비교하여 변조되었는지 확인한다.

3.4 갱신

갱신 단계는 사용자의 정보를 갱신하는 단계로서 TTP와 사용자 간에 갱신하는 단계에 대해서 기술한다.

사용자는 자신의 바이오인식 정보를 다른 것으로 대체하고자 할 때 갱신 단계를 수행한다. 갱신은 등록의 식 (5)에서 1 대신 갱신을 의미하는 2를 사용한다.

$$\{U \rightarrow TTP : E_{S_{PK_{TTP}}}(2, ID_i, (h((PW_i|PIN_i) \| B_{i,x,y_1}), \\ b_{i,x,y_1}), (h((PW_i|PIN_i) \| B_{i,x,y_2}), b_{i,x,y_2}), \ldots, \\ (h((PW_i|PIN_i) \| B_{i,x,y_n}), b_{i,x,y_n}), U_{PK}, ts1_U)\} \quad (19)$$

그 외 나머지는 등록과 동일하다.

3.5 삭제

삭제 단계는 사용자가 TTP와 사용자 간에 개인정보를 삭제하는 단계에 대해서 기술한다.

삭제는 등록 단계와 유사하지만, 식 (7)만 (20)으로 변형된다.

$$\{TTP \rightarrow U : E_{U_{PK}}(3, ID_i, h((PW_i|PIN_i) \| \\ (b_{i,x,y_1}) \| (b_{i,x,y_2}) \| \ldots \| (b_{i,x,y_n})), ts1_U, ts1_S)\} \quad (20)$$

이후 TTP는 사용자가 적법한 사용자임이 판명이 나면 바이오인식 정보 테이블에서 사용자의 정보를 삭제한다.

IV. 보안 분석

보안 분석에서는 본 논문에서 제안하는 방법에 대해 다양

한 경우에 대해 안전하다는 것을 입증한다.

표 8에서는 SAA[17]에서 제안하는 방법과 본 논문의 보안 특성과 비교한다. 본 논문에서 제안하는 방법은 비교하는 모든 분야에서 보안 요건을 충족함을 알 수 있다.

표 8. 보안 특성 비교
Table 8. Security property comparison

보안 특성		Zeng [15]	3G scheme [16]	SAA [17]	This Paper
상호 인증	ME ↔ USIM	*Yes*	*No*	*Yes*	*Yes*
	사용자 ↔ USIM	*Yes*	*Yes*	*Yes*	*Yes*
	사용자 ↔ ME	*Yes*	*Yes*	*Yes*	*Yes*
모바일 장치에서 사용자보호		*Yes*	*No*	*Yes*	*Yes*
재생 공격 방지		*Yes*	*No*	*Yes*	*Yes*
메시지 암호화		*partial*	*No*	*Yes*	*Yes*
메시지 무결성		*partial*	*partial*	*Yes*	*Yes*
바이오인식 식별		*Yes*	*No*	*Yes*	*Yes*
BCS의 전송 필요성		*Yes*	*N/A*	*No*	*No*
다중 요소 인식		*Yes*	*No*	*Yes*	*Yes*
다중 모달리티 수용		*No*	*No*	*No*	*Yes*
다중 바이오인식 정보 수용		*No*	*No*	*No*	*Yes*
다중 사용자와 다중 모바일 장치를 위한 유연한 인증 메카니즘 제공		*No*	*No*	*Yes*	*Yes*
부채널 공격 방지		*No*	*No*	*No*	*Yes*
중간자 공격 방지		*No*	*No*	*No*	*Yes*

4.1 위조된 TTP 및 금융기관

사용자는 DH 알고리즘을 이용하여 TTP로부터 TTP의 임시 공개키($S_{PK_{tmp}}$)를 발급받고, 이후에는 [11]의 알고리즘을 이용하여 사용자의 바이오인식 정보를 이용하여 TTP가 TTP의 공개키를 만들어 보내기 때문에 모든 사용자들은 각각 다른 TTP의 공개키를 사용하게 된다.

또한 금융기관의 위조 여부는 인증 단계에서 식 (14)의 $h(r_1|r_3) \stackrel{?}{=} h'(r_1|r_3)$를 이용하여 TTP가 알 수 있다.

4.2 개인정보 보호

개인정보는 기존의 단일 모달리티에 단일 바이오인식 정보를 이용하여 본인 인증을 하였고, 이 정보가 노출이 되면 상당히 치명적인 문제점이 된다. 예를 들어 회사의 식당에서 지문을 등록하여 사용하는 경우 이러한 지문이 유출이 된다면 지문만을 사용하는 금융기관 및 공공기관에서 도용이 될 수 있다. 그러나 본 논문에서는 다중 모달리티 및 다중 바이오인식 정보를 사용하기 때문에 기존의 바이오인식 정보가 아닌 다른 바이오인식 정보를 사용하여 인증이 가능하다.

식 (5)

$\{U \rightarrow TTP : E_{S_{PK_{tmp}}}(1, (ID_i, h((PW_i|PIN_i)\|B_{i,x,y_1}), b_{i,x,y_1}), h((PW_i|PIN_i)\|B_{i,x,y_2}), b_{i,x,y_2}), \ldots, h((PW_i|PIN_i)\|B_{i,x,y_n}), b_{i,x,y_n}), U_{PK}, ts1_U)\}$와 식 (7)

$\{TTP \rightarrow U : E_{U_{PK}}(h(ID_i\|EK_{US}) \oplus h((PW_i|PIN_i)\| (b_{i,x,y_1})\|(b_{i,x,y_2})\|\ldots\|(b_{i,x,y_n})), ts1_U, ts1_S)\}$을 통해 사용자의 단말기와 TTP에는 바이오인식 정보 원본이 저장되지 않는다. 다만, TTP에는 해쉬화된 사용자의 바이오인식 정보가 암호화 되어 표 3~7처럼 저장된다.

4.3 단말기 분실

사용자가 단말기를 분실하고, 악의의 사용자가 이를 습득하여 이용하고자 하려해도 사용자의 금융기관 정보를 알지 못하고, 사용자의 바이오인식 정보 역시 알지 못한다. 또한 식 (10)의 $\{U \rightarrow F : E_{F_{PK}}(E_{U_{SK}}(ID_i, b_{i,x,y_n}, FI_i, r_1, ts1_U))\}$와 같이 악의의 사용자는 b_{i,x,y_n}에서 어떤 모달리티인지 알 수 없고, 설사 모달리티가 지문인 것을 안다 할지라도 몇 번째 손가락인지, 몇 개를 사용하는지, 오른손인지 왼손인지 알 수 없다. 그리고 금융기관으로부터 전송받은 r_3와 함께 같이 해쉬화하여 TTP로 전송하는 r_1이 틀리기 때문에 위변조가 불가능하다.

4.4 상호 인증

4.1 위조된 TTP 및 금융기관에서 기술한 것처럼 사용자와 금융기관은 서로 전송한 r_1과 r_3를 해쉬화하여 TTP로 전송하고 TTP는 자신이 알고 있는 r_1과 r_3를 해쉬화하여 $h(r_1|r_3) \stackrel{?}{=} h'(r_1|r_3)$ 비교하기 때문에 상호 인증이 가능하다.

4.5 재생 공격

사용자는 금융기관에

$\{ U \rightarrow F : E_{F_{PK}}(E_{U_{SK}}(ID_i, b_{i,x,y_n}, FI_i, r_1, TS1_U))\}$ 와 같은 메시지를 전송한다. 이때 사용자가 생성한 난수 r_1이 있지만 악의의 사용자의 재생공격에 대비해 사용자의 타임스탬

프인 $TS1_U$를 생성하여 금융기관으로 전송한다. 이를 수신한 금융기관은 자신이 생성한 타임스탬프 $TS1_F$를 생성하여 사용자의 타임스탬프를 뺀다. 이때 △만큼의 차이가 발생할 것이고, 이를 다시 사용자에게 전송한다.

$F \rightarrow U : E_{U_{PK}}(E_{F_{SK}}(F_i, r_3, \triangle))$

사용자는 △가 임계치이내에 있다면 이를 수용한다.

$\triangle = TS1_F - TS1_U, 0 < \triangle \leq Threshold$

공격자는 △를 알 수 없기 때문에 재생공격으로부터 안전하다.

4.6 중간자 공격

본 논문에서 제안하는 방식은 공격자가 사용자와 금융기관 사이에서 정보를 가로채더라도 4.4의 상호인증 단계에서 서로 인증을 하고, 모든 메시지는 암호화와 해쉬화되어 전송되기 때문에 중간자 공격으로부터 안전하다.

V. 결 론

본 논문에서는 다중 바이오인식 정보를 안전하게 TTP에 등록하는 프레임워크를 제안하였다. 기존의 방식과 달리 다중 바이오인식 정보와 다중 모달리티를 사용할 수 있는 방법을 제안하였다. 따라서 본 논문을 통해 기존의 방법에 비해 보안 특성이 우수하고, 여러 가지 공격에 대해 안전함을 보였다. 추후 연구과제로는 사용자와 금융기관 사이의 인증, 등록, 갱신, 삭제만을 다루었으나, 이후에는 상점에서 다중 바이오인식 정보를 이용하여 안전하게 물건을 구매하는 프레임워크에 대해서 연구할 계획이다. 또한 다중 바이오인식 정보와 다중 모달리티를 효과적으로 관리할 수 있는 방법에 대해서도 연구할 계획이다.

참고문헌

〔1〕 Woonho Jung, "A Trends of Mobile payments and alternative authentication certificate," 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〕 Seungjin Han, "A Framework for Biometric Security based on OTP in Mobile Devices," Journal of The Korea Society of Computer and Information, Vol. 17, No. 4, pp. 121-127, Apr. 2012.

〔4〕 M. Gordon and S. Sankaeanaeayanan, "Biometric Security Mechanism in Mobile Payments", Proc., of the 5th National Conference; INDIACom-2011, Computing For Nation Development, March 10-11, 2011.

〔5〕 Bao, X, Wang, J. and Hu, J, "Method of Individual Identification based on Electroencephalogram Analysis", Proc., of 2009 International Conference on New Trends in Information and Service Science, pp. 390-393, Beijing, P.R.China, June 9-July 2, 2009.

〔6〕 Nakanishi, I, Baba, S and Miyamoto, C, "EEG Based Biometric Authentication Using New Spectral Features", Proc., of 2009 International Symposium on Intelligent Signal Processing and Communication Systems, pp. 651-654, Kanazawa, Ishikawa, Japan, December 7-9, 2009.

〔7〕 http://www.huffingtonpost.com/2011/10/19/face-unlock-ice-cream-sandwich_n_1020207.html

〔8〕 Daugman, J, "How Iris Recognition Works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan., 2004.

〔9〕 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)

〔10〕 Namho, Kim, *A Study on the Mobile OTP Key Creation Method using Biometrics Information*, Doctoral dissertation, Computer science and Statistics of Chonnam Univ., Feb., 2013.

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

〔12〕 Chin-Ling Chen, Jinn-Ke Jan, and Chih-Feng

Chien, "Using Mobile Device to Design A Secure Transaction," 2010 International Conference on Complex, Intelligent and Software Intensive Systems, IEEE, Krakow, 15-18 Feb. 2010.

[13] Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer and Stephane Tinguely, "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards", Proceedings of the 2002 IEEE Symposium on Security and Privacy, 2002.

[14] W. Diffie and M. Hellman, "New Directions on Cryptography," IEEE Transactions on Information Theory, IT-22(6): pp. 644~654, Nov., 1976.

[15] Y. Zheng, D. K. He, X. H. Tang and, H. X. Wang, "AKA and Authtentication Scheme for 4G Mobile Networks Based on Trusted Mobile Platform", ICICS 2005, pp. 976~980, 2005.

[16] 3GPP TS 24.002, Release 4. *GSM-UMTS public land mobile network access reference configuration*, June, 2003.

[17] Jian Wang, Nan Jiang, "Secure Authentication and Authorization Scheme for Mobile Devices," Proceedings of ICCTA2009, 2009.

저 자 소 개

한 승 진

1985~1990: 인하대학교 이과대학 전자계산학과 학사
1990~1992: 인하대학교 일반대학원 전자계산공학과 석사
1999~2002: 인하대학교 전자계산공학과 박사
1992~1996: 대우통신 종합연구소
1996~1996: 한국전산원 초고속사업단
1996~1998: SKTelecom 디지틀사업본부
2002~2004: 인하대학교 컴퓨터공학부 강의조교수
2004~현재: 경인여자대학교 e-비즈니스과 부교수
2007~현재: TTA PG505 표준화위원
2012~현재: TTA PG505 간사
관심분야 : USN, MANET, Mobile Computing, Security, Biometric, Computer Network,
Email : softman@kiwu.ac.kr