Journal of The Korea Society of Computer and Information
Vol. 21 No. 10, pp. 63-68, October 2016

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.10.063

A Robust Mutual Authentication between User Devices and Relaying Server(FIDO Server) using Certificate Authority in FIDO Environments

Seungjin Han *

Abstract

Recently, Biometrics is being magnified than ID or password about user authentication. However, unlike a PIN, password, and personal information there is no way to modify the exposure if it is exposed and used illegally. As FIDO(Fast IDentity Online) than existing server storing method, It stores a user's biometric information to the user device. And the user device authentication using the user's biometric information, the user equipment has been used a method to notify only the authentication result to the server FIDO. However, FIDO has no mutual authentication between the user device and the FIDO server. We use a Certificate Authority in order to mutually authenticate the user and the FIDO server. Thereby, we propose a more reliable method and compared this paper with existed methods about security analysis.

▸ Keyword : FIDO(Fast IDentity Online), Mutual Authentication, User Device, Relaying Server, Certificate Authority

I. Introduction

1993년 금융실명제를 도입하면서 금융회사는 고객과 계좌의 주인이 일치하는 대면(face-to-face) 인증을 거쳐야만 금융 거래가 가능하였다. 그러나 IT 인프라와 핀테크의 발달, 인터넷 전문은행 출범 등으로 비대면 인증의 필요성이 대두되면서, 소비자의 비대면 채널(CD/ATM, 인터넷뱅킹, 텔레뱅킹, 간편 결제, 인터넷 결제)을 통한 금융 서비스 이용 비중이 90%에 육박하고 있다. 비대면 인증 방법은 크게 4가지로 나뉜다. 지식기반 인증, 소지기반 토큰 인증, 생체정보기반 인증, 특징기반 인증 등이다[1].

생체정보기반 인증은 최근 가장 주목받고 있는 방식이다. 지문, 홍채, 망막, 정맥, 얼굴, 뇌전도(EEG, Electroencephalogram), 심전도(ECG, Electrocardiogram) 등 신체 일부 고유 정보를 파악해 본인 여부를 확인한다. 넓게는 목소리, 필체, 체형, 걸음걸이, 특정 행동까지 생체인식 기술에 포함된다.

모바일 디바이스에 생체정보를 이용하여 사용자를 인증하는 사실표준(De-facto)인 FIDO(Fast IDentity Online)[2]의 멀티팩터 인증이 국제적 추세이다. 기존 패스워드를 사용하는 온라인 서비스에서 두 번째 인증요소로 생체인식을 사용하고 있다. NIST(National Institute of Standards and Technology)의 보안 등급별 적용인증 수단에서도 높은 등급의 레벨(Level) 3 이상의 인증을 위해서는 싱글팩터 사용 보다는 멀티팩터 소프트웨어 암호 토큰, 멀티팩터 OTP 장치, 멀티팩터 암호장치를 권장하고 있다[3].

그러나 사용자의 과실없이 사용자의 생체정보를 저장한 기관, 회사 혹은 서버로부터 사용자의 생체정보가 유출된다면 그 파급효과는 상당히 크다. 예를 들어 지문 생체정보를 이용하여 서비스를 받던 사용자가 자신이 이용하던 기관에서 지문정보가 유출되었다면 사용자는 자신의 지문정보를 이용하여 다른 기관이 서비스를 받을 수 없을 것이다. 따라서, 최근에는 사용자의 생체정보를 서버에 저장하지 않고 사용자의 장치에만 저장하는 FIDO 방식을 여러 기관들이 도입하고 있다. 그러나 FIDO 방식은 사용자 장치와 서비스 업체간의 상호인증이 없기 때문에 이에 대한 연구가 필요하다.

본 논문은 II장에서는 관련연구 및 표준을 기술하고, III장에서는 공인인증기관을 이용한 사용자 장치와 RP(Relying-Party Server)서버(FIDO 서버)간 상호인증을 정의한다. IV장에서는 본

• First Author: Seungjin Han, Corresponding Author: Seungjin Han
*Seungjin Han(softman@kiwu.ac.kr), Dept. of Business Administration, Kyung-In Women's University
• Received: 2016. 08. 17, Revised: 2016. 09. 14, Accepted: 2016. 09. 28.

논문에서 제안하는 방법에 대해 보안성 평가를 하고, V장에서는 결론 및 추후 연구과제에 대해서 기술한다.

II. Preliminaries

1. Related works

관련연구에서는 생체인식을 적용한 표준 및 관련 연구를 살펴보고, 문제점을 기술한다.

1.1 ITU-T X.tam

모바일 장치를 이용하여 생체인식 정보를 획득하고, 비교하고, 저장하기 위한 기술 및 관리적 보안 지침인 ITU-T SG17 Q9 X.tam은 인증 모델을 생체인식 정보 획득, 저장 및 비교의 주체 방식에 따라 12가지 모델을 제시하였다[4].

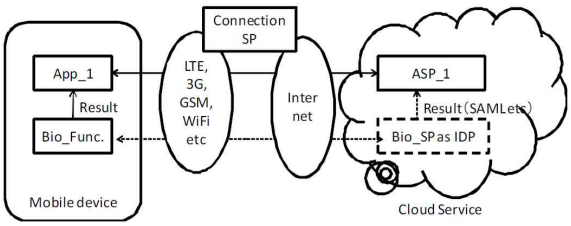

Fig. 1. ITU-T X.tam Standard Environments

본 논문에서 제안하는 방법은 표 1의 12가지 모델 중 FIDO 개념과 가장 유사한 인증모델 1과 비교한다.

Table 1. Authentication Model of Mobile Biometrics

	BioHSM	Mobile Device	Server
Model 1	Acquire	Compare, Store*	
Model 2	Acquire	Compare	Store
Model 3	Acquire		Compare, Store
Model 4	Acquire, Compare		Store
Model 5	Acquire, Compare	Store	
Model 6	Acquire, Compare, Store		
Model 7	Acquire, Store	Compare	
Model 8	Acquire, Store		Compare
Model 9	Acquire	Store	Compare
Model 10		Acquire, Compare, Store	
Model 11		Acquire	Compare, Store
Model 12		Acquire, Compare	Store

* 생체인식 참조 템플릿이 저장되는 장소

인증 모델 1은 센서에서 생체인식 정보를 획득하고 모바일 장치에서 저장된 사용자의 생체 정보와 비교 및 저장을 하는 모델이다. 그러나 인증모델 1은 사용자 장치가 도난 되었거나 변형된 데이터와 같은 적법하지 않게 획득된 데이터로의 교체가 가능하고, 적법하지 않은 생체인식 참조 템플릿 데이터의 사용이 가능하다. 또한 적법하지 않은 비교 프로그램의 사용이 가능하고, 모바일 장치의 분실 및 도난 등을 통한 생체 참조 템플릿의 유출이 가능하다.

1.2 FIDO

FIDO 기술 표준을 제정한 FIDO Alliance(www.fidoalliance.org)는 2016년 4월 현재 250여 업체가 참여하고 있고, 참여업체 수가 꾸준히 늘어나고 있는 거대한 기업 연합체이다. 참여하는 기업들은 생체인식 기업뿐 아니라, 칩 제조사(퀄컴, NXP 등), 단말 제조사(삼성, 레노버 등), OS 플랫폼 기업(구글, MS), 금융 서비스 기업(페이팔, 알리바바, VISA, 마스터카드 등)들로 구성되어 있으며, 패스워드를 대체하여 다양한 인증 수단을 수용할 수 있는 사용자 인증 공통 플랫폼 기술 개발을 목표로 참여하고 있다.

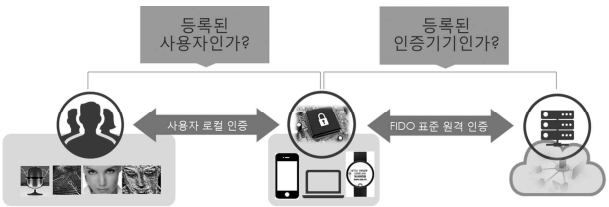

Fig. 2. A Core concept of FIDO Authentication Scheme

그림 2는 FIDO 인증 기술의 핵심 개념을 설명하고 있다[5]. 사용자는 사용자가 소지하고 있는 기기가 제공하는 인증 수단을 통해 사용자 로컬 인증을 수행하고 사용자 기기는 인증된 사용자를 대신하여 FIDO 표준 기반의 원격 인증을 수행한다. FIDO 표준의 원격 인증은 이미 많이 사용되어 안전이 입증된 공개키 암호 기술을 사용한다. 공개키 암호에 사용되는 개인키는 사용자의 기기에만 저장되고 외부에 노출되지 않으며, 사용자가 기기에 인증한 경우에만 저장되어 있던 개인키를 이용해 암호문을 생성하고 해당 암호문을 서버에 전송할 수 있다. 서버는 사용자 등록 과정에서 전달받은 저장된 공개키를 이용하여 전송된 암호문을 검증하고 사용자 인증을 완료한다.

서비스 웹 서버는 사용자에게 서비스를 제공하기 위한 응용 서버(Relying-Party Server)와 FIDO 서버로 구성된다. FIDO 서버는 FIDO 클라이언트와 FIDO 프로토콜을 수행하여 사용자 등록, 인증, 탈퇴 관련 서비스를 제공하며, 이를 위한 서버정책 및 메타데이타 관리 서비스를 제공하도록 구성된다. 서버 정책은 응용 서버에서 수용 하고자 하는 인증 수단 및 장치를 세밀하게 조정할 수 있다. 따라서 서비스 제공자 측에서는 서버에 대한 수정 변경 없이도, 서버정책만을 조정하여 새로운 인증 수

단을 수용하거나 제어할 수 있게 된다. 또한 서버정책을 설정하는 것만으로 멀티 팩터를 이용한 인증도 가능해진다.

FIDO 기술은 크게 사용자 기기와 사용자에게 서비스를 제공하는 웹 서버로 구성된다. 사용자 기기는 웹 서버의 서비스를 사용자에게 제공하기 위한 응용 앱(Relying-Party APP)과 사용자 인증을 수행하기 위한 FIDO 클라이언트로 구성된다. 그리고 FIDO 클라이언트는 더 세밀하게는 FIDO 클라이언트, FIDO ASM(Authenticator Specific Module), FIDO 인증장치(Authenticator)로 구성되는데, 실제적인 사용자 인증과 FIDO 키 관리 및 서명은 FIDO 인증장치에서 대부분 수행된다. 따라서 FIDO 인증장치는 사용자 인증을 위한 모듈과 키 관리 및 서명을 위한 모듈이 기본적으로 탑재된다[2].

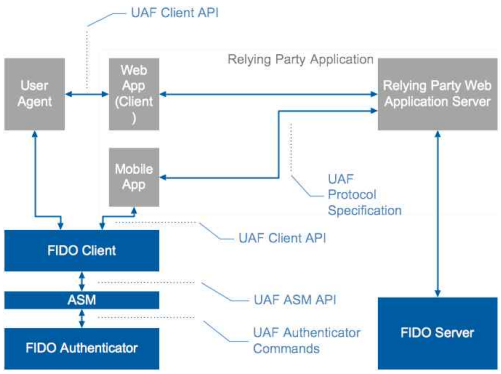

Fig. 3 FIDO Architecture

FIDO 시스템의 장점은 사용자의 개인식별정보와 무관한 공개키 정보만 FIDO 서버에 저장되기 때문에, 서버의 정보가 해킹 등으로 모두 유출되더라도 사용자 개인의 정보는 유출되지 않는다. 그러나 신뢰성이 있는 제 3기관을 이용하지 않는 기술이기에 공인인증서와 같은 신뢰성을 구축하기 어렵다. 사용자 입장에서는 RP 서버가 적법한 서버인지에 대한 의문점이 있을 수 있고, RP 서버 입장에서는 사용자가 적법한 사용자인지에 대해 공인된 기관에서의 인증이 필요하다.

1.3 Distributed Management of Biometrics(KFTC)

금융결제원의 생체정보 분산관리는 인간의 생체정보를 나누어 각기 다른 서버에 저장하고 필요한 경우 각 서버로부터 생체정보를 전송받아 합친 후 대상자를 검증하는 방식이다[6]. 이는 생체정보 DB를 하나에 저장하느냐 아니면 2개의 서버에 저장하느냐의 차이일 뿐 근본적인 해결책이 되지 못한다.

1.4 Etc

[7]은 FIDO를 이용한 공인인증시스템을 제안하였다. 사용자는 공인인증기관(CA : Certificated Authority)으로부터 공인증서를 발급받아 RP 서버(FIDO 서버)에 저장을 한다. 사용자 기기는 이후 RP 서버(FIDO 서버)에 저장된 공인인증서를 통해 자신의 적법성을 입증한다. 그러나 RP 서버(FIDO 서버)가 해킹 등으로 정보가 유출되면 공인인증서와 같은 민감한 정보가 유출되어 타 시스템에도 영향을 미친다.

Fig 4. Standard for distributed management of biometrics(KFTC)

III. The Proposed Scheme

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

Table 2. Notations

기호	설명
$\{X \rightarrow Y: M\}$	X sends the message M to Y
$X_H(Y)$	X hashes Y using a strong one-way hash function(H).
$A \| B$	concatenate A and B
$A \stackrel{?}{\equiv} B$	compare A with B
$CA_H(RN_1)$	CA sends the sufficiently long random number from a hash function results to User Device.
$CA_H(RN_2)$	CA sends the sufficiently long random number from a hash function results to RP Server(FIDO Server)
$CA_H(RN_1)'$	User device receives the sufficiently long random number from a hash function results from CA.
$CA_H(RN_2)'$	RP Server(FIDO Server) receives the sufficiently long random number from a hash function results from CA.
FU_{PK}	Public Key of FIDO User Device
FU_{RK}	Private Key of FIDO User Device
CA_{PK}	Public Key of CA
CA_{RK}	Private Key of CA
FS_{PK}	Public Key of RP Server(FIDO Server)
FS_{RK}	Private Key of RP Server(FIDO Server)

1.1 Mutual Authentication Steps between User Devices and RP Server(FIDO Server)

FIDO방식은 사용자의 생체정보가 서버에 저장되지 않고, 사용자의 장치에 저장되고 단지 사용자의 생체정보를 이용하여 본인 확인만을 하고 이에 대한 결과를 RP서버(FIDO 서버)에 전송하기 때문에 서버저장 방식에 비해 상대적으로 집단적인 개인정보 유출로부터 자유로울 수 있다. 그러나 FIDO방식의 가장 큰 문제점은 신뢰성이 있는 제 3기관을 사용하지 않는 기술이기에 공인인증서와 같은 신뢰 체인(Chain of Trust)을 구축하기 어렵다는 것이다. 이는 사용자의 장치에 대한 신뢰성 뿐 아니라 RP서버(FIDO 서버)에서 사용자 장치로 보내온 챌린지(Challenge)의 유효성 문제이다. 즉, 서로가 전송한 인증서에 대한 신뢰성 문제이다. 이는 FIDO 사용자 장치에서 전송한 전자서명과 RP서버(FIDO 서버)에서 전송한 챌린지에 대한 신뢰를 보장해 줄 공인인증기관(CA) 혹은 TTP(Trusted Third Party)에 기반하지 않는 기술이기 때문이다. 따라서, FIDO 사용자 장치와 RP서버(FIDO 서버)간의 상호 인증 단계가 필요하다.

$$\{FU \rightarrow CA : FU_{PK}, Request\} \quad (1)$$

사용자 장치는 공인인증기관에 자신의 공개키와 함께 등록 요청을 한다.

$$\{FS \rightarrow CA : FS_{PK}, Request\} \quad (2)$$

RP서버(FIDO 서버)는 공인인증기관에 자신의 공개키와 함께 등록 요청을 한다.

$$\{CA \rightarrow FU : FU_{PK}(CA_H(RN_1)), CA_{PK}\} \quad (3)$$

공인인증기관은 충분히 긴 난수(RN_1)를 생성하여 해쉬함수로 해쉬화한 후 (1)에서 전송받은 사용자 장치의 공개키(FU_{PK})로 암호화하고 공인인증기관의 공개키(CA_{PK})를 사용자 장치에 전송한다. 사용자 장치는 수신한 $\{FU_{PK}(CA_H(RN_1))\}$를 사용자 장치의 개인키(FU_{RK})로 복호화하고, $CA_H(RN_1)$을 저장한다.

$$\{CA \rightarrow FS : FS_{PK}(CA_H(RN_2)), CA_{PK}\} \quad (4)$$

공인인증기관은 충분히 긴 난수(RN_2)를 생성하여 해쉬함수를 이용하여 해쉬화한 후 (2)에서 전송받은 RP서버(FIDO 서버)의 공개키(FS_{PK})로 암호화하고 공인인증기관의 공개키(CA_{PK})를 RP서버(FIDO 서버)에 전송한다. RP서버(FIDO 서버)는 수신한 $\{FS_{PK}(CA_H(RN_2))\}$를 RP서버(FIDO 서버)의 개인키(FS_{RK})로 복호화하고, $CA_H(RN_2)$를 저장한다.

$$\{FU \rightarrow FS : FU_{PK}\} \quad (5)$$

사용자 장치는 RP서버(FIDO 서버)에게 자신의 공개키(FU_{PK})를 전송한다.

$$\{FS \rightarrow FU : FS_{PK}\} \quad (6)$$

RP서버(FIDO 서버)는 사용자 장치에게 자신의 공개키(FS_{PK})를 전송한다.

$$\{FU \rightarrow FS : FS_{PK}(CA_H(RN_1)')\} \quad (7)$$

사용자 장치는 RP서버(FIDO 서버)로 공인인증기관에게서 전송받은 $CA_H(RN_1)$을 (5)에서 전송받은 RP서버(FIDO 서버)의 공개키(FS_{PK})로 암호화하여 RP서버(FIDO 서버)에 전송한다. 이후 (8)에서 전송받은 $FU_{PK}(CA_H(RN_2)')$를 사용자 장치의 개인키(FU_{RK})로 복호화한 후 $CA_H(RN_2)'$를 저장한다.

$$\{FS \rightarrow FU : FU_{PK}(CA_H(RN_2)')\} \quad (8)$$

RP서버(FIDO 서버)는 사용자 장치로 공인인증기관에게서 전송받은 $CA_H(RN_2)$를 (6)에서 전송받은 사용자 장치의 공개키(FU_{PK})로 암호화하여 사용자 장치로 전송한다. (7)에서 전송받은 $FS_{PK}(CA_H(RN_1)')$을 RP서버(FIDO 서버)의 개인키(FS_{RK})로 복호화한 후 $CA_H(RN_1)'$을 저장한다.

$$\{FU \rightarrow CA : CA_{PK}(FU_{RK}(FU_H(CA_H(RN_1)' \| CA_H(RN_2)')))\} \quad (9)$$

사용자 장치는 $CA_H(RN_1)'$과 RP서버(FIDO 서버)에게서 전송받은 $CA_H(RN_2)'$를 연결하고, 사용자 장치가 해쉬화한다. 그 후 사용자 장치의 개인키(FU_{RK})로 암호화하고, 공인인증기관의 공개키(CA_{PK})로 암호화를 한번 더 한 후 공인인증기관에 전송한다.

$$\{FS \rightarrow CA : CA_{PK}(FS_{RK}(FS_H(CA_H(RN_1)' \| CA_H(RN_2)')))\} \quad (10)$$

RP서버(FIDO 서버)는 $CA_H(RN_2)'$와 사용자 장치에게서 전송받은 $CA_H(RN_1)'$을 연결하고, 사용자 장치가 해쉬화한다. 그 후 RP서버(FIDO 서버)의 개인키(FS_{RK})로 암호화한다. 공인인증기관의 공개키(CA_{PK})로 암호화를 한번 더 한 후 공인인증기관에 전송한다.

$$CA_{RK}(CA_{PK}(FU_{RK}(CA_H(RN_1)' \| CA_H(RN_2)'))) \quad (11)$$

공인인증기관은 (9)와 (10)에서 수신한 메시지를 각각 자신의 개인키(CA_{RK})로 복호화한다.

$$FU_{PK}(FU_{RK}(CA_H(RN_1)' \| CA_H(RN_2)')) \quad (12)$$

공인인증기관은 사용자 장치의 공개키(FU_{PK})를 이용하여 한번 더 복호화한다.

$$FS_{PK}(FS_{RK}(CA_H(RN_1)' \| CA_H(RN_2)')) \quad (13)$$

공인인증기관은 RP서버(FIDO 서버)의 공개키(FS_{PK})를 이용하여 한번 더 복호화한다.

$$CA_H(CA_H(RN_1)\|CA_H(RN_2)) \stackrel{?}{=} CA_H(CA_H(RN_1)'\|CA_H(RN_2)') \quad (14)$$

공인인증기관이 사용자 장치와 RP서버(FIDO 서버)에게 전송한 후 보관중인 해쉬화된 충분히 긴 난수($CA_H(RN_1)\|CA_H(RN_2)$)를 공인인증기관은 한번 더 해쉬화($CA_H(CA_H(RN_1)\|CA_H(RN_2))$)하고, 공인인증기관은 사용자 장치와 RP서버(FIDO 서버)에게서 수신한 해쉬화된 충분히 긴 난수($CA_H(RN_1)'\|CA_H(RN_2)'$)를 한번 더 해쉬화($CA_H(CA_H(RN_1)'\|CA_H(RN_2)')$)한 후 비교한다.

$$\{CA \rightarrow FU : OK \text{ or } NOK\} \quad (15)$$

공인인증기관은 (14)에서 비교한 결과를 토대로 사용자 장치에게 RP서버(FIDO 서버)의 적법성을 알린다.

$$\{CA \rightarrow FS : OK \text{ or } NOK\} \quad (16)$$

(15)와 마찬가지로 공인인증기관은 (14)에서 비교한 결과를 토대로 RP서버(FIDO 서버)에게 사용자 장치의 적법성을 알린다.

(15)와 (16)의 결과를 이용하여 사용자 장치와 RP서버(FIDO 서버)는 작업 절차를 계속 진행할지 여부를 결정한다.

사용자 장치와 RP 서버(FIDO 서버)간의 등록 및 인증 과정은 기존의 FIDO 사실 표준을 사용한다.

IV. Security Analysis

보안 분석에서는 본 논문에서 제안하는 방법에 대해 상호 인증의 경우에 대해 안전하다는 것을 입증한다.

Table 3. Security property comparison

Security Property	KFTC [6]	J.J Kim [7]	FIDO [2]	ITU-T X.Tam [4]	This Paper
Mutual Authentic-ation	*No*	*Yes*	*No*	*No*	*Yes*
User Protection in Mobile Device	*partial*	*Yes*	*Yes*	*Yes*	*Yes*
Prevention of Replay Attack	*partial*	*Yes*	*Yes*	*partial*	*Yes*
use a Certificate	*Yes*	*Yes*	*No*	*No*	*No*
Message Integrity	*Yes*	*Yes*	*partial*	*partial*	*Yes*
Prevention of MITM	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

표 3에서는 [2], [4], [6], [7]에서 제안하는 방법과 본 논문의 보안 특성과 비교한다. 본 논문에서 제안하는 방법은 비교하는 모든 분야에서 보안 요건을 충족함을 알 수 있다.

1.1 Mutual Authentication

사용자 장치와 RP서버(FIDO 서버)는 공인인증기관으로부터 전달받은 $CA_H(RN_1)$와 $CA_H(RN_2)$를 이용하여 식(9)~(14)까지를 이용하여 상호인증한다. 사용자장치는 공인인증기관이 RP서버(FIDO 서버)에게 전송한 $CA_H(RN_2)$를 알지 못하고, RP서버(FIDO 서버)는 공인인증기관이 사용자 장치에게 전송한 $CA_H(RN_1)$를 알지 못한다. 두 개의 값을 모두 알고 있는 것은 공인인증기관 뿐이므로 공인인증기관은 사용자 장치와 RP서버(FIDO 서버)가 각각 전송한 식(9)와 (10)을 자신이 보관하고 있는 값($CA_H(RN_1)$, $CA_H(RN_2)$)과 비교(식14)하여 수신한 값($CA_H(RN_1)'$, $CA_H(RN_2)'$)의 위조 여부를 알 수 있다.

1.2 Privacy Protection

개인정보는 기존의 단일 모달리티에 단일 생체인식 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 FIDO 방식처럼 RP서버(FIDO 서버)에는 어떠한 사용자의 생체정보가 저장되지 않고, [7]과 같이 RP서버(FIDO 서버)에 공인인증서가 저장되지 않기 때문에 서버가 해킹을 당해도 유출되는 개인정보는 없다.

또한 식(1)~(16)까지 어디에도 사용자의 개인키 혹은 생체정보를 전송하지 않기 때문에 전송도중 메시지가 유출되어도 파급효과는 극히 미비하다.

1.3 Replay Attack

공격자가 사용자 장치 ↔ RP서버(FIDO 서버), RP서버(FIDO 서버) ↔ 공인인증기관, 사용자 장치 ↔ 공인인증기관 사이에서 전송되는 $CA_H(RN_1)$, $CA_H(RN_2)$, $CA_H(RN_1)'$, $CA_H(RN_2)'$를 가로채더라도 사용자 장치, RP서버(FIDO 서버)의 개인키를 알지 못하므로 재생공격이 불가능하다.

1.4 Man-in-the-Middle Attack

본 논문에서 제안하는 방식은 공격자가 사용자 장치와 RP서버(FIDO 서버)사이에서 정보를 가로채더라도 4.2의 상호인증 단계에서 서로 인증을 하고, 모든 메시지는 암호화와 해쉬화되어 전송되기 때문에 중간자 공격으로부터 안전하다.

V. Conclusions

본 논문에서는 FIDO에서 제안하는 기술 중에서 사용자 장치와 RP 서버(FIDO 서버)간의 상호 인증 문제를 공인인증기관(CA)을 두어 해결하였다. 기존의 방법에 비해 RP 서버(FIDO 서버)가 해킹을 당해서 기존의 FIDO 방법과 마찬가지로 유출되는 개인 정보는 없다. 본 논문에서 제시하는 방법은 보안 분석을 통해 기존의 방법에 비해 보안 특성이 우수하고, 여러 가지 공격에 대해 안전함을 보였다. 본 논문에서 제안하는 방법은 서비스 보안 등급 중에서 상위 레벨 적용 시 유용하다. 서비스 보안 등급이 낮은 서비스에서는 기존의 FIDO 방법을 사용하는 것이 사용자 장치, RP 서버(FIDO 서버) 및 공인인증기관(CA)의 부하를 감소시킨다.

추후 연구과제로는 다중 생체 정보와 다중 모달리티를 효과적으로 사용 및 관리할 수 있는 방법에 대해서 연구할 계획이다.

REFERENCES

[1] Tae Bong Kim, “SmartSIGN,” Fintechforum June Annual Presentation, KTB Solution, 23rd, June, 2015.

[2] Fido Alliance, https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.pdf

[3] NIST(National Institute of Standards and Technology), DRAFT NIST Special Publication 800-63-3 Digital Authentication Guideline, https://pages.nist.gov/800-63-3/sp800-63-3.html

[4] ITU-T SG17 WG5 Q9, http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=9429

[5] SooHyung Kim, YeongSub Cho, and DaeSeon Choi, “FinTech Era: Needs for the innovation of user authentication technologies,” Communications of the Korean Institute of Information Scientists and Engineers, KIISE, vol. 33, no. 5, pp17-22, May, 2015.

[6] Korea Financial Telecommunications & Clearings Institute, “Standard for distributed management of biometrics,” Korea Financial Telecommunications & Clearings Institute, Jun., 2015.

[7] Jaejung Kim, "Study on the password-free certification system using the FIDO (Fast IDentity Online)," Communications of the Korea Information Science Society, KIISE, vol. 33, no. 5, May., 2015.

Authors

Seungjin Han received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Inha University, Korea, in 1989, 1992 and 2004, respectively.

Dr. Han joined the faculty of the Department of e-Business at Kyung-In Women’s University, Incheon, Korea, in 2004. He is currently a Associate Professor in the Department of Business Administration, Kyung-In Women’s University. He worked for Research Center of Daewoo Telecommunication as a TDX software developer from Jan. 1992 to Jun. 1996, and National Information Society Agency(NIA) as project manager from Jun. 1996 to Jul. and SKTelecom as project manager from Jul. 1996 to Jan. 1998. He was a lecturer of Inha University from Mar. 2002 to Feb. 2004. He is interested in parallel computing, internet and mobile computing, and cloud computing.

His research has always been in the area of MANET and Sensor Networks or technologies which relate to it, such as Security, Protocol and Routing in MANET and USN, Middleware in USN and Security using Biometric Systems.