JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 9, pp. 89-96, September 2021
https://doi.org/10.9708/jksci.2021.26.09.089

Analysis of Al-Saggaf et al's Three-factor User Authentication Scheme for TMIS

Mi-Og Park*

*Assistant Professor, Dept. of Computer Engineering, Sungkyul University, Anyang, Korea

[Abstract]

In this paper, we analyzed that the user authentication scheme for TMIS(Telecare Medicine Information System) proposed by Al-Saggaf et al. In 2019, Al-Saggaf et al. proposed authentication scheme using biometric information, Al-Saggaf et al. claimed that their authentication scheme provides high security against various attacks along with very low computational cost. However in this paper after analyzing Al-Saggaf et al's authentication scheme, the Al-Saggaf et al's one are missing random number s from the DB to calculate the identity of the user from the server, and there is a design error in the authentication scheme due to the lack of delivery method. Al-Saggaf et al also claimed that their authentication scheme were safe against a variety of attacks, but were vulnerable to password guessing attack using login request messages and smart cards, session key exposure and insider attack. An attacker could also use a password to decrypt the stored user's biometric information by encrypting the DB with a password. Exposure of biometric information is a very serious breach of the user's privacy, which could allow an attacker to succeed in the user impersonation. Furthermore, Al-Saggaf et al's authentication schemes are vulnerable to identity guessing attack, which, unlike what they claimed, do not provide significant user anonymity in TMIS.

▸ **Key words**: User authentication, TMIS, Smart-card, Password guessing attack, Biometrics

[요 약]

본 논문에서는 Al-Saggaf 등이 제안한 TMIS(Telecare Medicine Information System)를 위한 사용자 인증 기법을 분석하였다. 2019년에 Al-Saggaf 등이 제안한 인증 기법은 생체정보를 이용한 인증 기법으로, Al-Saggaf 등은 그들의 인증 스킴이 매우 적은 계산 비용으로 다양한 공격에 대한 높은 비도를 보장한다고 주장하였다. 그러나 본 논문에서 Al-Saggaf 등의 인증 기법을 분석한 결과, Al-Saggaf 등의 인증 기법은 서버에서 사용자의 ID를 계산해내기 위해서 필요한 난수 s가 DB에서 누락되었고, 서버의 ID SID를 사용자에게 전달하는 방식이 부재하여 인증 기법의 설계 오류가 존재하였다. 또한 Al-Saggaf 등은 그들의 인증 기법이 다양한 공격에 안전하다고 주장하였으나, 로그인 요청 메시지와 스마트카드를 사용한 패스워드 추측 공격, 세션키 노출, 내부자 공격 등에 취약하였다. 또한 공격자는 추측한 패스워드를 사용하여, DB에 패스워드로 암호화하여 저장된 사용자의 생체정보까지 복호화할 수 있었다. 생체정보의 노출은 사용자의 개인정보에 대한 아주 심각한 침해이고, 이로 인하여 공격자는 사용자 가장 공격에 성공할 수 있다. 게다가 Al-Saggaf 등의 인증 스킴은 ID 추측 공격에도 취약하여, 그들이 주장했던 것과 달리 TMIS에서 중요한 사용자 익명성을 보장하지 못한다.

▸ **주제어**: 사용자 인증, TMIS, 스마트카드, 패스워드 추측 공격, 생체 정보

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@hanmail.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2021. 08. 10, Revised: 2021. 08. 30, Accepted: 2021. 08. 31.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

2019년 Al-Saggaf 등은 생체 정보를 이용한 TMIS(Telecare Medicine Information System) 사용자 인증 스킴을 제안하였다[1]. TMIS는 원격의료정보시스템으로 환자가 병원에 직접 방문하지 않고도 의사의 진료와 환자 개인의 정보 등에 접근할 수 있다. 오픈 네트워크를 사용하는 TMIS에서 사용자의 신상 정보나 생체정보 유출은 사용자의 프라이버시(privacy)를 심각하게 침해할 수 있어, 의사와 사용자(환자)간의 안전한 상호 인증(mutual authentication)과 민감한 개인 정보의 익명성(anonymity)이 매우 중요하다[2][3]. 안전한 사용자 인증을 위한 스마트카드기반의 사용자 인증 스킴들[4][5]이 다수 제안되었고, 이러한 인증 스킴들은 TMIS 환경의 사용자 인증 스킴[6][7][8]으로 발전하였다.

2019년 Al-Saggaf 등은 사용자 익명성을 제공하는 thee-factor TMIS 사용자 인증 스킴을 제안하였다. Al-Saggaf 등은 보안과 기능적 특성, 그리고 계산 비용(computational cost) 등을 다른 인증 스킴들과 비교하면서, 자신들의 인증 스킴이 계산 비용 면에서 더 효율적이고 생체 정보를 사용하여 안전한 사용자 익명성과 재발급성(renewability)을 제공한다고 주장하였다. Al-Saggaf 등이 비교분석한 인증 스킴들 중 Das-Goswami 등의 인증 스킴[2]은 Chang 등[9]이 제안한 고유성과 익명성을 보장(uniqueness-and-anonymity-preserving)하는 사용자 인증 스킴이 해쉬 함수와 XOR 연산을 사용하여 효율적이나 로그인과 인증 단계, 그리고 패스워드 변경 단계에서 설계상의 오류가 있음을 보였다. 또한 Chang 등의 인증 스킴은 생체정보의 보안을 위하여 바이오해싱(bioHashing)을 사용하였으나, Das-Goswami 등은 Chang 등의 인증 스킴이 내부자 공격(insider attack)과 중간자 공격(man-in-the-middle-attack)에 취약하고, 적절한 인증을 보장하지 못한다는 것을 보이면서, Chang 등의 장점을 개선한 새로운 인증 스킴을 제안하였다. Das-Goswami 등은 자신들의 인증 스킴이 스마트카드 분실 공격(stolen/lost smart card attack), 가장 공격(impersonation attack), 재전송 공격(replay attack), 그리고 중간자 공격 등 다양한 공격에 안전하다고 주장하였고, 이에 대한 안전성은 AVISPA(Automated Validation of Internet Security Protocols and Applications)를 사용하여 증명하였다.

2010년 Awasthi-Srivastava 등[10]는 공개키 암호화 방식을 사용하는 패스워드기반의 TMIS 사용자 인증 스킴을 제안하였다. 인증 스킴의 높은 비도를 위하여 사용자의 패스워드를 난수와 함께 XOR 연산하여 서버의 공개키로 암호화하는 방식으로, Awasthi-Srivastava 등은 그들의 인증 스킴이 패스워드 추측 공격, 사용자 가장 공격, 스마트카드 분실 공격, 내부자 공격, 그리고 도난 검증자 공격(stolen verifier attack) 등에 안전하다고 주장하였다. Tan의 인증 스킴[11], Mishra 등의 인증 스킴 [3], 그리고 Awasthi-Goswami[12] 등의 인증 스킴은 Awasthi-Srivastava 등의 인증 스킴에 대한 취약점을 분석하였다. 2014년 Tan은 Awasthi-Srivastava의 인증 스킴이 패스워드 추측 공격과 반사 공격(reflection attack)에 취약하고, 사용자 익명성을 보장하지 못한다는 것을 보였고, 이들의 취약점을 개선하면서 사용자 익명성을 제공하기 위해 공개키를 사용하는 three-factor 인증 스킴을 제안하였다. Tan은 자신의 인증 스킴이 다른 인증 스킴들에 비하여, 사용자 익명성과 더 강력한 보안을 제공한다고 주장하였다. 그러나 Arshad 등[13]은 Tan 등의 인증 스킴이 재생 공격과 Dos(denial-of-service)에 취약하다고 분석하고 이를 개선하기 위하여, 타원곡선 알고리즘(ECC)을 사용한 효율적인 키 교환 인증 스킴을 제안하였다. 그러나 2015년 Lu 등[14]은 Arshad 등의 인증 스킴이 패스워드 추측 공격과 사용자 가장 공격에 취약하다고 분석하였다.

2014년 Mishra 등은 Tan이 분석한 것과 같이 Awasthi-Srivastava의 인증 스킴이 패스워드 추측공격에 취약하고, 패스워드 변경단계에서 사용자가 새로운 패스워드를 잘못 입력하였을 경우에, 잘못 입력된 패스워드를 체크할 수 있는 과정이 부재함을 보였다. 이러한 비효율적인 패스워드 변경 단계는 정당한 사용자가 자신의 스마트카드를 소유하고 있음에도 불구하고 잘못 입력한 패스워드를 모르기 때문에, 스마트카드를 사용할 수 없는 일이 발생하고, 이로 인하여 서버에 대한 DoS(denial of service) 공격까지 발생할 수 있다. Mishra 등은 이러한 취약점을 가진 Awasthi-Srivastava 등의 인증 스킴을 개선하기 위하여 난수를 사용한 three-factor TMIS 인증 스킴을 제안하였고, Awasthi-Srivastava의 패스워드 변경 단계와 달리 서버의 도움 없이 패스워드를 변경하기 때문에, 효율적인 패스워드 변경단계(User-friendly and efficient password changes phase)라고 주장하였다.

Al-Saggaf 등이 비교하는 인증 스킴들 중 Xu-Wu[15] 등의 인증 스킴은 서버의 도움을 받아 패스워드를 변경하고, 나머지 비교 스킴들은 사용자가 자유롭게 패스워드를 변경한다. 그러나 비교 인증 스킴들은 새로운 패스워드에 대한 체크 과정이 모두 부재하여, 패스워드 변경 단계에서

의 비효율적인 문제는 여전히 존재하는 것으로 분석되었다.

2014년 Das-Goswami 등[12]은 Awasthi-Srivastava 등의 인증 스킴이 매우 효율적이지만, 재전송 공격, 잘못된 패스워드 변경단계, 사용자 익명성과 안전한 세션키를 설정하지 못하여 엄격한 안전성 분석에는 부족하다고 분석하였고, Awasthi-Srivastava 등의 인증 스킴의 장점을 개선하면서, 난수에 기본을 둔 카오스 맵(chaotic map)을 사용한 생체정보 기반의 TMIS 인증 스킴을 제안하였다. 2017년 Zhang 등[16]은 Mishra 등의 인증 스킴이 재전송 공격, 중간자 공격, 그리고 전방향 안전성(forward secrecy)을 보장하지 못한다고 분석하였고, 이러한 취약점을 개선하기 위해서 chaotic map-based cryptography를 사용하는 TMIS three-factor 헬스케어 서비스를 제안하였다. Zhang 등은 그들의 인증 스킴이 TMIS에서 중요한 사용자의 프라이버시를 제공한다고 주장하였다.

Al-Saggaf 등이 비교분석한 인증 스킴들 중 Xu-Wu 등은 Xie 등의 인증 스킴[17]이 비동기화 공격(de-synchronization attack)에 취약하고, 서버의 메모리 부담이 크다고 분석하였다. Xu-Wu 등은 Xie 등의 인증 스킴을 개선하기 위하여, 비밀키 암호화 방식과 바이오해시(biohash) 함수를 사용하였고, 바이오해쉬 함수는 생체정보를 안전하게 처리하기 위해서 Al-Saggaf 등의 인증 스킴에서도 사용하였다. Al-Saggaf 등은 생체정보의 안전한 처리뿐만 아니라, 계산 비용면에서도 매우 효율적인 인증 스킴이라고 주장하였고, 7가지의 보안 기능을 비교하면서, 7가지 기능을 모두 만족하는 자신들의 인증 스킴이 TMIS에 적합한 사용자 인증 스킴이라고 주장하였다. 그러나 본 논문에서는 Al-Saggaf 등의 인증 스킴이 그들의 주장과 달리, 스마트카드와 로그인 요청 메시지를 사용하여 정보를 획득하려고 시도할 경우, 사용자의 ID와 패스워드 추측 공격이 가능함을 보인다. 또한 공격자가 사용자의 ID와 패스워드 추측 공격에 성공하였을 경우, 사용자 가장 공격, 사용자 익명성, 내부자 공격 등 다양한 공격에 취약함을 보일 것이다.

본 논문의 구성은 Al-Saggaf 등의 사용자 인증 스킴의 각 단계를 2장에서 살펴본다. 3장에서는 먼저 Al-Saggaf 등의 인증 스킴에 설계상의 오류가 존재함을 보이고, 후반부에서 안전성을 분석하여, 스마트카드와 로그인 요청 메시지만을 사용하여 사용자의 ID와 패스워드, 그리고 랜덤 넘버 codeword와 생체 템플릿까지 공격자가 쉽게 획득할 수 있음을 보인다. 마지막으로 4장에서 결론을 내리고 본 논문을 마친다.

II. Related Work

1. Review of Al-Saggaf et al's Authentication scheme

본 장에서는 Al-Saggaf 등이 제안한 TMIS 사용자 인증 스킴에 대한 각 단계를 살펴본다. Al-Saggaf 등이 제안한 각 단계는 등록 단계, 로그인 단계, 인증 단계, 그리고 패스워드 변경 단계로 구성되며, Table 1은 Al-Saggaf 등의 인증 스킴에서 사용한 기호와 의미를 나타낸 것이다.

2.1 Registration Phase

등록 단계는 Fig. 1과 같고, 다음과 같이 진행한다.

R1. 사용자 Ui는 패스워드 PWi와 난수 N을 선택하고, RPWi=h(PWi||N)를 계산한다.

R2. 사용자 Ui는 생체 템플릿 ti를 생성하는 장치에 자신의 생체정보 Bi를 제시하고, 에러정정코드(error correcting code) 집합 C에서 랜덤하게 codeword (부호어) ci를 선택한다. 그런 다음 퍼지 확약(fuzzy commitment) yi=Fi(ci, ti)=(h(ci), δi)를 계산한다.

R3. 등록 센터 RC는 ri=h(RPWi||h(ci))와 yi=h(IDi||Xs)⊕ri를 계산한다.

R4. RC는 시스템의 DB에 (h(ci), E_{PWi}(ci))를 저장한다.

R5. 스마트카드를 받은 사용자 Ui는 스마트카드에 난수 N을 저장한다.

2.2 Login Phase

로그인 단계와 인증 단계의 그림은 Fig. 2와 같다.

L1. 원격 서버에 접근하고자 하는 사용자 Ui는 자신의 스마트카드를 카드 리더기에 넣고, 생체정보 장치에 자신의 생체정보 Bi를 제공하여 생체정보 템플릿 t'i를 추출한다.

L2. 스마트카드는 codeword f(c'i)=f(t'i⊕δi)와 h(f(c'i)를 계산하여 h(f(c'i))?=h(c'i)이 동일한지 비교한다. 만약 두 값이 동일하지 않으면, 세션을 종료한다.

L3. 만약 앞 단계의 두 값이 동일할 경우, 사용자 Ui는 자신의 IDi와 패스워드 PWi를 입력한다.

L4. 스마트카드는 RPWi'=h(PWi'||N)와 r'i = h(RPWi'||h(f(c'i)))를 계산한 후 r'i?=ri가 동일한지 비교한다. 만약 두 값이 동일하지 않으면, 세션은 종료한다.

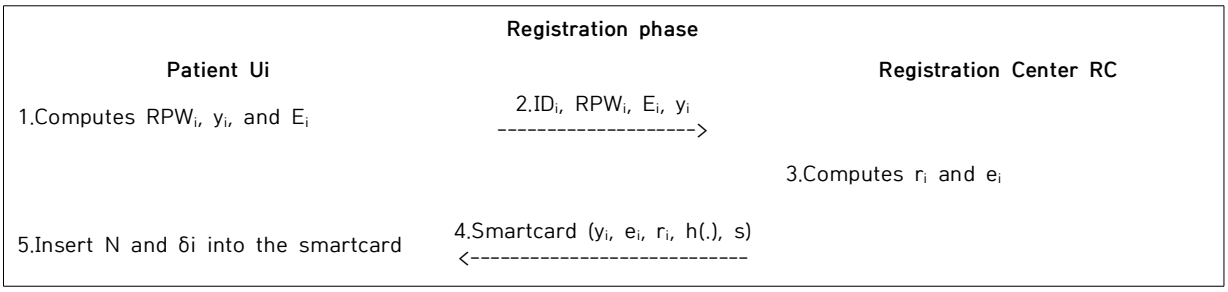

Fig. 1. Al-Saggaf et al's Registration Phase

Table 1. Notifications

Item	Description
RC	Trust Registration Center
MS	Medical Server in TMIS
Ui	Patient in TMIS
SID	Identity of MS
IDi	Identity of Ui
Bi	Biometric data of Ui
ti	Biometrics template of Ui extracted at registration phase
t'i	Biometrics template of Ui extracted at login phase
h(.)	One-way hash function
Xs	The master secret key shared between RC and MS, which is chosen by RC.
s	A secret number maintained by MS and stored in Ui's smart card
C	Error correction code set
F	Error correction decoded function
ci	codeword
Ru	A secret number chosen by Ui used for prevent replay attacks
Rs	A secret number chosen by MS used for prevent replay attacks
⊕	Exclusive-OR operation
||	Concatenation operation

L5. 만약 앞 단계의 두 값이 동일할 경우, 스마트카드는 다음 값들을 계산한다. 여기서 Ru는 사용자가 선택한 난수이다.

$ri=ei\oplus M_1$, $Ru=M_2\oplus M_1$, $M_3=h(s||Ru)$

$M_4=RPWi\oplus M_3$, $M_5=h(M_2||M_3||M_4)$, $M_6=M_3\oplus IDi$

L6. 사용자 Ui는 서버 MS에게 로그인 요청 메시지 (M_1, M_2, M_4, M_5, M_6)를 전송한다.

2.3 Authentication Phase

A1. 로그인 요청 메시지를 받은 서버 MS는 로그인 요청 메시지 M_1, M_2, M_6을 사용하여 $M_7=M_2\oplus M_1$과 $IDi=M_6\oplus h(s||M_1\oplus M_2)$를 계산한다.

A2. 서버 MS는 계산해 낸 IDi의 포맷을 비교하여, 타당한 IDi일 경우 $M_8=h(s||M_7)$를 계산하여 M_5가 식 M_5 ?= $h(M_2||M_8||M_4)$를 만족하는지 검증한다. 만약 조건을 만족하면, MS는 사용자 Ui의 로그인 요청을 받아들이고, 재전송 공격과 중간자 공격을 막기 위해서 (IDi, M_7)를 데이터베이스에 저장하고, 그렇지 않을 경우, MS는 로그인 요청을 거절하고 여기서 세션을 종료한다.

A3. 서버 MS는 $M_9=M_4\oplus M_8$, $M_{10}=h(M_9||SID||s)\oplus M_8\oplus Rs$, 그리고 $M_{11}=h(M_1||M_9||s||Rs)$를 계산하여 사용자 Ui에게 인증 메시지 ($M_{10}$, M_{11})를 전송한다.

A4. 사용자 Ui는 $M_{12}=h(RPWi||SID||s)\oplus M_3\oplus M_{10}$을 계산하고 M_{11}?=$h(M_1||RPWi||s||M_{12})$를 계산하여, 조건을 만족하면 비교한다. 조건을 만족할 경우, 사용자 Ui는 서버 MS를 정당한 서버로 인증하고, 사용자와 서버는 각자 자신의 세션키 $SK=h(RPWi||M_3||M_{12}||SID)$와 $h(M_9||M_8||Rs||SID)$를 생성한다. 만약 조건을 만족하지 않을 경우, 사용자 Ui는 세션을 종료한다.

2.4 Password Change Phase

C1. 사용자 Ui는 스마트카드를 입력하고 자신의 생체정보 Bi와 추출된 생체정보 템플릿 t'i를 제공한다. 검증을 통과할 경우, 사용자는 이전의 패스워드 PWi와 새로운 패스워드 PWi^{new}를 입력한다. 만약 검증을 통과하지 못할 경우, 세션을 종료된다.

C2. 스마트카드는 RPWi'=h(PWi'||N)와 r'i=h(RPWi'||h(f(c'i)))를 계산하여, r'i ?= ri가 동일한지 비교한다. 만약 두 값이 동일하지 않으면, 스마트카드는 세션을 종료하고, 그렇지 않을 경우 e'i=ei⊕r'i, $RPWi^{new}=h(PWi^{new}||N)$, $ri^{new}=h(RPWi^{new}||h(ci))$, 그리고 $ei^{new}=e'i\oplus ri^{new}$를 계산한다.

C3. 기존의 ei와 ri를 앞에서 계산한 ei^{new}와 ri^{new}로 각각 대체하여 저장한다.

III. Analysis of Al-Saggaf et al's Authentication Scheme

Al-Saggaf 등은 생체정보를 이용한 TMIS 사용자 인증 스킴을 제안하였고, 사용자의 개인 정보가 매우 중요한 TMIS 환경을 위하여 사용자 익명성을 보장한다고 주장하였다. 또한 Al-Saggaf 등은 자신들의 인증 스킴이 공격자가 스마트카드에 저장된 모든 정보를 안다고 할지라도, 안전하게 암호화되어있는 생체정보 관련 정보와 패스워드를 추측할 수 없기 때문에, 다른 여러 공격에 저항성을 가진 안전한 인증 스킴이라고 주장하였다. 그러나 본 논문에서는 Al-Saggaf 등의 인증 스킴을 분석하여, 정당한 사용자의 생체정보 없이도 분실된 스마트카드와 로그인 요청 메시지만을 사용하여 사용자의 ID 추측공격과 패스워드 추측공격이 가능함을 보일 것이다.

1. Design Flaw

먼저 3.1절에서는 Al-Saggaf 등의 인증 스킴에 존재하는 설계상의 오류를 분석한다.

Missing random number s

Al-Saggaf 등의 인증 단계 A1에서 서버가 사용자의 IDi를 계산해내려면 난수 s가 필요한데, 이 난수 s를 사용자가 전송한 정보들을 이용하여 계산해내던지 아니면 서버의 DB에 저장된 것을 사용해야 한다. 그러나 Al-Saggaf 등은 그러한 언급이 전무하나, 인증 단계의 서버는 $IDi=M_6 \oplus h(s||M_1 \oplus M_2)$에서 난수 s를 사용하고 있다. 식에서 필요한 M_1, M_2, M_6 등은 앞 과정의 연산을 통해 계산해낼 수 있으나, 난수 s는 그러한 계산 과정이 부재하다. 그러므로 Al-Saggaf 등의 인증 스킴에서는 난수 s가 서버의 DB에 저장되어 있어야하나, 실수로 누락한 것으로 보이며, 본 논문에서는 Al-Saggaf 등의 인증 스킴을 분석할 때 난수 s가 서버의 DB에 저장되어 있다는 가정 하에 그들의 인증 스킴을 분석할 것이다.

Server ID, SID

Al-Saggaf 등의 세션키 생성은 서버의 ID인 SID가 필요하다. 그러므로 서버는 모든 사용자들에게 자신의 SID를 전송하거나 다른 알릴 방법이 있어야하나, 이에 대한 아무런 언급 없이 세션키 생성에 SID를 사용하였다.

2. Security Analysis

본 논문에서는 Al-Saggaf 등의 인증 스킴이 스마트카드와 로그인 요청 메시지를 사용할 경우, 사용자의 ID와 패스워드 추측공격에 성공할 수 있고, 이로 인하여 서버의 DB에 사용자의 패스워드로 암호화되어 저장된 생체관련 정보들까지 복호화가 가능함을 보인다.

2.1 Resistance to various attacks

본 절에서는 본 논문에서 Al-Saggaf 등의 인증 기법을 분석한 결과로, Al-Saggaf 등의 인증 기법이 다양한 공격에 취약함을 보인다.

Lost smart-card attack

Al-Saggaf 등의 인증 스킴은 그들의 인증 스킴이 다음 두 가지 식 즉, $h(IDi||Xs)=ei \oplus ri$와 로그인 요청 메시지 $M_6=h(s||Ru) \oplus IDi$에서 사용자의 ID를 획득하기 어렵기 때문에, 스마트카드 분실 공격에 안전하다고 주장하였다. 그러나 본 절에서는 Al-Saggaf 등의 인증 스킴이 로그인 요청 메시지 (M_1, M_2, M_4, M_5, M_6)와 스마트카드의 정보를 함께 사용할 경우, 스마트카드 분실 공격에 매우 취약함을 보인다. 공격자의 시나리오는 다음과 같다.

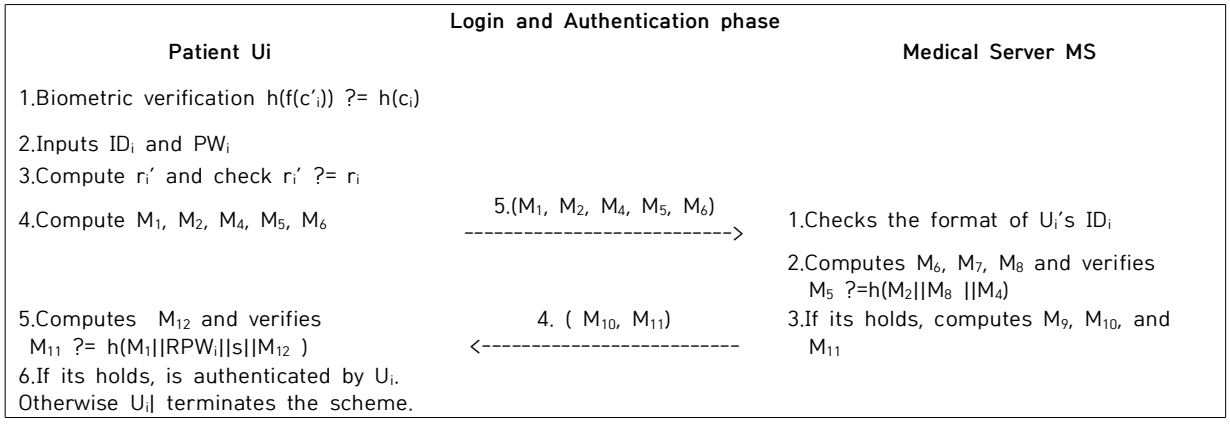

Fig. 2. Al-Saggaf et al's Login and Authentication Phase

1. 스마트카드에 저장된 (yi, ei, ri, s, N, δi) 중 ei와 ri를 연산하거나 ei와 M_1을 XOR 연산하면 ri를 계산할 수 있다. ei=h(IDi||Xs)⊕ri이기 때문에, XOR 계산 결과는 h(IDi||Xs)이고, 로그인 단계 L5에서 로그인 요청 메시지 M_1은 ei⊕ri로 계산된다.

   ei⊕ri=h(IDi||Xs)⊕ri⊕ri=h(IDi||Xs)=M_1

   이러한 계산 과정은 로그인 요청 메시지 M_1과 스마트카드의 ei를 XOR 연산하면 ri를 쉽게 계산할 수 있다.
2. 로그인 요청 메시지 M_2는 $M_2=M_1⊕Ru$와 같이 계산된다. 그러므로 이 식을 난수 Ru를 계산하기 위해 $Ru^*=M_2⊕M_1$과 같이 연산한다. M_1과 M_2는 둘 다 로그인 요청 메시지이기 때문에, 추측 공격할 필요 없이 간단히 XOR 연산에 의해 올바른 난수 Ru를 계산할 수 있다.
3. 스마트카드의 데이터 s와 앞에서 계산한 난수 Ru를 이용해 M_3을 $M_3^*=h(s||Ru^*)$와 같이 계산한다.
4. 로그인 요청 메시지 M_4의 계산식 $M_4=RPWi⊕M_3^*$을 이용해서 RPWi를 $RPWi?=M_4⊕M_3^*$와 같이 계산한다. 사용자의 패스워드 PWi를 추측하기 위해서, 스마트카드에 저장된 N을 사용하여 양쪽의 두 값이 동일할 때까지 PWi 값을 변경하면서 계속 반복한다. M_3^* 값은 로그인 요청 메시지와 스마트카드의 데이터를 사용하여 계산했기 때문에, 한 번의 계산에 의하여 올바른 값이 나오지만, 재확인을 위해서 M_5 $?=h(M_2||M_3^*||M_4)$를 사용할 수 있다.
5. 사용자의 IDi를 획득하기 위해서 로그인 요청 메시지 M_6의 식 $M_6=M_3^*⊕IDi$를 $IDi^*=M_3^*⊕M_6$처럼 계산한다.

본 논문에서 Al-Saggaf 등의 인증 스킴을 분석한 결과, Al-Saggaf 등의 인증 스킴은 스마트카드와 로그인 요청 메시지만으로 사용자의 ID를 간단히 계산해낼 수 있다. 또한 앞에서 제시한 시나리오에서 보는 것과 같이 Al-Saggaf 등의 인증 스킴은 패스워드 추측 공격에도 취약하여, 공격자는 사용자를 가장할 수 있는 두 가지 정보 획득에 성공할 수 있다.

Session Key

공격자는 스마트카드에 저장된 s와 Ru를 사용하여 $M_3=h(s||Ru)$를 생성할 수 있다. 인증 단계 A3에서 서버는 RPWi를 얻기 위해 로그인 요청 메시지 M_4와 A2 단계의 $M_8=h(s||M_7)$를 사용하여 $M_9=M_4⊕M_8=RPWi$ 계산한다. 그런 다음 서버가 생성한 난수 Rs를 획득하기 위해서 전송 메시지 M_{10}을 $Rs=M_{10}⊕h(M_9||SID||s)⊕M_8^*$처럼 계산한다. $M_9=RPWi$이고, $M_3=M_8^*$, $M_{12}=Rs$이다. 그래서 서버가 생성하는 난수 Rs를 획득할 수 있다. M_{11}을 계산하기 위해 필요한 값들을 보면, 로그인 요청 메시지 M_1, RPWi와 동일한 값인 M_9, 사용자의 난수 s와 서버의 난수 Rs는 앞에서 모두 획득할 수 있는 값들이다.

$$M_{11} = h(M_1||M_9||s||Rs)=h(M_1||RPWi||s||Rs)$$
$$= h(M_1||M_9^*||s||M12^*)$$

Al-Saggaf 등의 세션키는 $SK=h(RPWi||M_3||M_{12}||SID)$나 $h(M_9||M_8||Rs||SID)$처럼 계산된다. 이 식에 의하면 $M_{12}=Rs$, $M_3=M_8$, $M_9=RPWi$이 성립한다. 앞에서 분석한 것처럼 Rs, M_3^*, 그리고 $RPWi^*$를 획득할 수 있고, 그로인하여 이 값들과 동일한 M_{12}, M_8, M_9를 얻을 수 있다. 세션키 SK를 계산하기 위해, 서버의 SID를 뺀 나머지 모든 값을 획득할 수 있다. SID가 난수와 같이 긴 값이 아닐 경우, $SK ?= h(RPWi||M_3||M_{12}||SID)$ 또는 $SK ?= h(M_9||M_8||Rs||SID)$ 식을 사용하여 양쪽 값이 같아질 때까지 추측 공격을 통해 SID를 획득할 수 있다. 그러나 서버의 SID는 모든 사용자들이 공통으로 사용하는 값이기 때문에, 사용자는 누구나 알 수 있는 값으로 추측공격을 할 필요 없이, 공격자가 정당한 사용자를 가장하여 가입만하면 획득 가능한 값이다. 그러므로 Al-Saggaf 등의 인증 스킴은 공격자가 세션키 생성이 가능함으로, 매우 민감한 정보를 다루는 TMIS 상의 기밀성을 보장하지 못한다.

Stolen biometrics template attack

본 논문의 스마트카드 분석 절에서 분석한 결과, Al-Saggaf 등의 인증 스킴은 스마트카드 분실 공격에서 획득한 사용자의 PWi를 사용하여 DB에 저장된 $Ei=E_{PWi}(ci)$를 복호화하면 사용자의 랜덤넘버 codeword ci를 얻어낼 수 있다. 또한 복호화한 ci와 스마트카드의 δi를 ti=δi⊕Ci 연산하면 사용자의 생체 템플릿 ti도 간단히 계산해낼 수 있다. 그러므로 사용자의 프라이버시가 더욱 중요한 TMIS에서 Al-Saggaf 등의 인증 스킴은 안전한 인증 스킴이라고 할 수 없다.

Insider attack

앞에서 분석한 스마트카드 분실공격에 의한 패스워드 추측공격이 아니라할지라도, 패스워드로 암호화할 경우 용자의 패스워드는 추측공격에 취약하기 때문에, 공격자는 서버의 DB에 저장된 $E_{PWi}(ci)$를 복호화 할 수 있다. Al-Saggaf 등은 엔트로피가 높은 패스워드를 사용한다고 가정하였지만, 실제 모든 사용자들이 이 조건을 만족할 수 있는 패스워드를 사용하지 않을 것이고, 패스워드는 사용자가 스스로 생성해서 사용하기 때문에 높은 엔트로피의

Table 2. Comparison of security features

Security features	Chang [9]	Das-Goswami[2]	Xu-Wu[15]	Tan [11]	Lu [14]	Zhang [16]	Al-Saggafl[1]	Reanalysis result
F1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
F2	No	Yes	Yes	Yes	Yes	Yes	Yes	No
F3	No	No	No	Yes	Yes	Yes	Yes	No
F4	No	Yes	Yes	No	No	Yes	Yes	No
F5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
F6	Yes	Yes	Yes	Yes	No	Yes	Yes	No
F7	No	No	No	No	No	No	Yes	No

F1: Resists stolen stored biometric template attack, F2: Resists privileged insider attack, F3: Resists stolen smart-card attack, F4: Provide proper authentication, F5: Provide mutual authentication, F6: Provide user anonymity, F7: Provide biometric renewability

특성을 만족시키기가 어렵다. 그러므로 Al-Saggaf 등의 인증 스킴은 그들의 주장과 달리 내부자 공격에 안전하다고 할 수 없다.

Replay attack

Al-Saggaf 등의 인증 스킴은 사용자와 서버에서 각각 생성한 난수를 사용하고, 이 난수를 인증단계 A2에서 (IDi, M_7)를 DB에 저장함으로써, 재전송 공격과 중간자 공격을 막을 수 있다고 주장하였다. 그러나 이러한 공격을 막기 위해서는 공격자가 이전의 여러 난수 Ru 중의 어떤 것을 사용할지 모르기 때문에, 사용한 모든 난수 Ru를 저장해야 한다. 그러나 Al-Saggaf 등은 재전송 공격과 중간자 공격을 막기 위해서 난수를 DB에 저장한다고만 언급하였지 모든 난수인지 현재 세션의 난수인지에 대한 정확한 설명이 없다.

2.2 Security Features

본 절에서는 안전성 기능에 대한 측면에서 Al-Saggaf 등의 인증 기법을 분석·설명한다.

User anonymity

Al-Saggaf 등의 인증 스킴은 본 논문에서 분석한 결과, 로그인 요청 메시지 하나만으로는 사용자의 IDi를 획득할 수 없지만, 스마트카드의 정보를 같이 사용할 경우에는 사용자의 IDi를 쉽게 계산해낼 수 있었다. 또한 내부자 공격 측면을 볼 때, DB에 평문으로 IDi가 저장되기 때문에 내부 공격자가 DB 공격에 성공할 경우, 사용자 IDi를 그대로 획득할 수 있다. 그러므로 Al-Saggaf 등의 인증 스킴은 정당한 사용자에게 안전한 익명성을 보장한다고 할 수 없다.

Password change phase

Al-Saggaf 등의 인증 스킴은 패스워드 변경 단계는 사용자가 새로운 패스워드를 잘못 입력하였을 경우에, 잘못 입력한 패스워드를 올바로 수정할 수 있는 방법이 없다. 만약 사용자가 잘못 입력한 새로운 패스워드를 사용할 경우, 사용자는 다음 세션에서 자신이 올바로 입력했다고 생각한 패스워드를 입력할 것이기 때문에, 잘못 입력된 새로운 패스워드로 업데이트된 스마트카드를 사용할 수 없다.

앞에서 제시한 Table 2는 Al-Saggaf 등의 인증 스킴에서 그들이 자신들의 인증 스킴을 분석한 항목과 그에 대한 결과들, 그리고 본 논문에서 그들이 제시한 항목에 대해 재분석한 결과를 보인 것으로, Yes는 공격에 대한 저항성을 가지거나 해당하는 안전성을 제공한다는 의미이고, No는 공격에 대한 저항성이 없거나 해당하는 안전성을 제공하지 않는다는 것을 의미이다.

IV. Conclusions

본 논문에서 Al-Saggaf 등의 인증 스킴을 분석한 결과, Al-Saggaf 등의 인증 스킴은 스마트카드와 로그인 요청 메시지를 사용할 경우, 사용자의 ID와 패스워드 추측 공격에 취약하였고, 이로 인하여 DB에 사용자의 패스워드로 암호화되어있는 생체관련 정보의 복호화가 가능하였다. 암호화된 codeword ci와 생체 템플릿 ti의 복호화 및 계산이 가능함에 따라 Al-Saggaf 등이 주장한 것과 달리 사용자의 생체정보의 안전성을 보장할 수 없다. 또한 공격자가 세션키 생성까지 가능함에 따라 TMIS에서 중요한 기밀성과 사용자의 익명성 등도 안전하게 보장하지 못하여 Al-Saggaf 등의 인증 스킴은 TMIS에 적합한 사용자 인증 스킴이라고 할 수 없다. 향후 연구 계획은 Al-Saggaf 등의 인증 스킴의 취약점을 개선하고, 그들의 계산 효율성은 살릴 수 있는 안전한 three-factor 인증 스킴을 연구하는 것이다.

REFERENCES

[1] A. A. Al-Saggaf and T. R. Sheltami, "Renewable and Anonymous Biometrics-Based Remote User Authentication Scheme Using Smart Cards for Telecare Medicine Information System," 2019 Advances in Science and Engineering Technology International Conferences (ASET), pp. 1-6, 2019. DOI: 10.1109/ICASET.2019.8714479

[2] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," Journal of Medical Systems, Vol. 37, No. 3, May 2013.

[3] D. Mishra, S. Mukhopadhyay, S. Kumari, M. Khan, and A. Chaturvedi, "Security enhancement of a biometrics based authentication scheme for telecare medicine information systems with nonce," Journal of Medical Systems, Vol. 38, No. 5, Apr. 2014.

[4] Mi-Og, Park, "Design Flaws and Cryptanalysis of Cui et al's User Authentication Scheme," Journal of the Korea society of computer and information, Vol. 24, No. 10, pp. 41-48, Oct. 2019.

[5] Kwang-Cheul, Shin, "Structural vulnerability analysis and improvement of a biometrics-based remote user authentication scheme of Li and Hwang's," Journal of the Korea society of computer and information Vol. 17 No. 7, pp. 107-115, Jul. 2012.

[6] Q. Xie, B. Hu, N. Dong, and D. S. Wong, "Anonymous three party password-authenticated key exchange scheme for telecare medical information systems," PLoS One, Vol. 9, No. 7, e102,747, Jul. 2014.

[7] Younghwa An, "A Strong Biometric-based Remote User Authentication Scheme for Telecare Medicine Information Systems with Session Key Agreement," International Journal of Internet, Broadcasting and Communication, Vol. 8 No. 3, pp. 41-49, Aug. 2016.

[8] Keewon Kim, "Cryptanalysis and Improvement of RSA-based Authentication Scheme for Telecare Medical Information Systems," Journal of the Korea society of computer and information Vol. 25 No. 2, pp. 93-103, Feb. 2020.

[9] Chang, Y.F., Yu, S.H., and Shiao, D.R. , "A Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care," Journal of Medical Systems, Vol. 37, Issue. 2, Jan. 2013. DOI: 10.1007/s10916-012-9902-7

[10] A. K. Awasthi and K. Srivastava, "A biometric authentication scheme for telecare medicine information systems with nonce," Journal of Medical Systems, Vol. 37, Issue. 5, Aug. 2013.

[11] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," Journal of Medical Systems, Vol. 38, Issue. 3, Mar. 2014.

[12] A. K. Awasthi, , and A. Goswami, "An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function," Journal of Medical Systems, Vol. 38, Issue: 6, Jun. 2014.

[13] H. Arshad and M. Nikooghadam, "Three-Factor Anonymous Authentication and Key Agreement Scheme for Telecare Medicine Information Systems,"Journal of Medical Systems, Vol. 38, Issue. 12, Oct. 2014. DOI: 10.1007/s10916-014-0136-8

[14] Y. Lu, L. Li, H. Peng, and Y. Yang, "An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem," Journal of Medical Systems, Vol. 39, Issue. 3, Mar. 2015.

[15] L. Xu and F. Wu, "Cryptanalysis and Improvement of a User Authentication Scheme Preserving Uniqueness and Anonymity for Connected Health Care," Journal of Medical Systems, Vol. 39, Issue. 10, Jan. 2015.

[16] L. Zhang, S. Zhu, and S. Tang, "Privacy Protection for Telecare Medicine Information Systems using a Chaotic Map-Based Three Factor Authenticated Key Agreement Scheme," IEEE Journal of Biomedical and Health Informatics, Vol. 21, No. 2, pp. 465-475, Mar. 2017.

[17] Q. Xie, L. Wenhao, Wang. Shengbao, Han. Lidong, H. Bin, and W. Ting, "Improvement of a Uniqueness-and-Anonymity-Preser ving User Authentication Scheme for Connected Health Care," Journal of Medical Systems, Vol. 38, Issue. 9, Jul. 2014.

Authors

Mi-Og Park received the M.S. and Ph.D. degrees in Computer Science and Engineering from Soongsil University, Korea, in 1993 and 2004, respectively. Dr. Park joined the faculty of the Department of Computer Engineering at Sungkyul University, Korea, in 2005. She is interested in mobile security, security protocol and IoT security.