JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 10, pp. 93-101, October 2023
https://doi.org/10.9708/jksci.2023.28.10.093

User Authentication Protocol preserving Enhanced Anonymity and Untraceability for TMIS

Mi-Og Park*

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

[Abstract]

In this paper, as a result of analyzing the TMIS authentication protocol using ECC and biometric information proposed by Chen-Chen in 2023, there were security problems such as user impersonation attack, man-in-the-middle attack, and user anonymity. Therefore, this paper proposes an improved authentication protocol that provides user anonymity to solve these problems. As a result of analyzing the security of the protocol proposed in this paper, it was analyzed to be secure for various attacks such as offline password guessing attack, user impersonation attack, smart-card loss attack, insider attack, perfect forward attack. It has also been shown to provided user privacy by guaranteeing user anonymity and untraceability, which must be guaranteed in TMIS. In addition, there was no significant increase in computational complexity, so the efficiency of execution time was achieved. Therefore, the proposed protocol in this paper is a suitable user authentication protocol for TMIS.

▸ **Key words**: Authentication protocol, User anonymity, Untraceability, ECC, TMIS

[요 약]

본 논문에서는 2023년에 Chen-Chen이 제안한 ECC와 생체정보를 사용한 TMIS 인증 프로토콜을 분석한 결과, 사용자 가장 공격, 중간자 공격, 사용자 익명성 등의 안전성 문제가 있었다. 그러므로 본 논문에서는 이러한 문제를 해결하기 위하여 사용자 익명성을 제공하는 개선된 인증 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜의 안전성 문제를 분석한 결과, 제안한 프로토콜은 오프라인 패스워드 추측 공격, 사용자 가장 공격, 스마트카드 분실 공격, 내부자 공격, 전방향 안전성, 재생 공격 등 여러 공격에 안전한 것으로 분석되었다. 또한 TMIS에서 반드시 보장해야 하는 사용자 익명성과 추적 불가능성도 함께 보장하여 사용자의 프라이버시를 보장하는 것으로 나타났다. 게다가 계산 복잡도에서도 크게 증가하지 않아 실행시간의 효율성도 달성하였다. 그러므로 본 논문에서 제안한 프로토콜은 TMIS에 적합한 사용자 인증 프로토콜이다.

▸ **주제어**: 인증 프로토콜, 사용자 익명성, 추적불가능성, 타원곡선 암호, 원격의료정보시스템

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@daum.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2023. 09. 05, Revised: 2023. 09. 19, Accepted: 2023. 09. 26.

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

I. Introduction

TMIS는 원격의료 정보 시스템(telecare medicine information system)의 간략화 된 명칭으로 그 명칭에서 보듯이 의료 서비스를 원격으로 지원하는 시스템으로, 환자(사용자)의 개인 정보와 의료정보들이 오픈 채널을 통하여 전송된다. TMIS는 환자가 병원에 직접 가지 않고 의료 서비스를 받을 수 있는 편리성은 제공하나, 오픈 채널 상에 전송되는 데이터가 모두 드러나기 때문에 전송 데이터의 비밀성(secrecy)과 무결성(confidentiality) 등을 보장해야 한다. 또한 개인의 민감한 의료정보가 전송되기 때문에, 익명성(anonymity)을 제공하여 사용자의 프라이버시도 보장해야한다. 이러한 TMIS의 안전성을 위하여 2015년 Chaudhry et al[1]은 타원곡선 암호(ECC, elliptic curve cryptosystem)와 바이오 해싱함수(biohashing)를 이용한 사용자 인증 프로토콜을 제안하면서, Lu et al.[2]의 인증 프로토콜에 대한 안전성 문제를 지적하였다. Lu et al.은 Arshad et al[3]의 인증 프로토콜이 오프라인 패스워드 추측 공격으로 사용자의 ID와 패스워드 추측 공격, 사용자 가장 공격에 대한 저항성이 없다고 지적하고 이러한 문제를 해결하기 위하여 ECC을 사용한 인증 프로토콜을 제안하였다. 그러나 Chaudhry et al.은 그들의 인증 프로토콜이 사용자 가장 공격, 서버 가장 공격, 그리고 사용자 익명성을 제공하지 못한다고 지적하였다. 또한 이로 인하여 사용자에 대한 추적 불가능성도 제공하지 못한다고 지적하였다.

2016년 Chaudhry et al.[4]는 ECC와 바이오 해싱함수를 사용한 인증 프로토콜을 제안하였고, Amin et al.[5]의 프로토콜이 스마트카드 분실 공격과 패스워드를 변경할 때 CMS(control management system)라는 최상위 서버와 상호연동을 해야 하고, 검증(verifier) 테이블을 유지하는 오래된 인증 방식을 사용하여 도난된 검증자 공격(stolen verifier attack)에 안전하지 않다고 지적하였다. 여기서 Amin et al.의 인증 프로토콜은 인증과 키 교환(Authentication and Key Agreement, AKA)의 제안 외에 TMIS의 전체 구조(architecture)를 제안하였고, 이 구조의 최상위 서버를 CMS라고 지칭하였다.

2017년 Han et al.[6]의 인증 프로토콜은 Lu et al.의 인증 프로토콜이 사용자 익명성과 사용자 및 서버 가장 공격에 안전하지 않고, 동적 ID의 잘못된 설계로 인하여 연결 익명성(unlinkability)을 제공하지 못한다고 지적하였다. 그리하여 이러한 동적 ID의 문제를 해결하기 위하여 ECC와 바이오 해싱함수를 사용한 프로토콜을 제안하였다.

2018년 Sahoo-Mohanty[7]은 ECC와 퍼지 추출함수(fuzzy extractor)를 사용한 가벼운(lightweight) 프로토콜을 제안하였고, 계산 복잡도와 전송비용이 다른 인증 프로토콜들보다 더 효율적이라고 주장하였다. 그러나 본 논문에서 Sahoo-Mohanty의 프로토콜을 검토한 결과 전송비용은 관련된 다른 프로토콜들보다 더 효율적이지만, 계산 복잡도에서는 Arshad et al.[8]을 제외한 나머지 프로토콜들과 비슷하고, 내부 공격자가 스마트카드의 정보를 획득하였다고 가정할 경우, 등록단계에서 사용자가 서버에 제출한 정보들을 가지고 사용자가 생성한 난수를 계산해 낼 수 있고, 이로 인하여 사용자의 동적 ID와 세션키를 계산해 낼 수 있다. 그러므로 Sahoo-Mohanty의 인증 프로토콜도 안전성 문제들이 존재하기 때문에 다른 인증 프로토콜들보다 더 효율적인 프로토콜이라고 할 수 없다.

2019년 Sarif et al.[9]의 인증 프로토콜은 Ravanbakhsh-Nazari[10]의 인증 프로토콜에 대한 전방향 안전성(perfect forward secrecy) 문제를 지적하고, 이 문제를 해결하기 위하여 익명성을 제공하는 ECC 기반의 2-factor TMIS 프로토콜을 제안하였다. 그러나 2023년 Chen-Chen[11]의 인증 프로토콜은 Sarif et al.의 인증 프로토콜이 사용자의 ID와 패스워드 입력 시 이 값들의 정확성(correctness)을 확인하지 않고 그 다음 과정을 곧바로 진행하는 로그인 단계의 문제가 있다고 지적하였다. 또한 오프라인 패스워드 추측 공격의 문제도 함께 지적하였다. Chen-Chen의 인증 프로토콜은 이러한 문제를 해결하기 위하여 퍼지 추출함수를 사용한 ECC 기반의 TMIS 프로토콜을 제안하였다.

그러나 본 논문에서 Chen-Chen의 인증 프로토콜을 분석한 결과, 사용자 익명성을 위하여 동적 ID을 사용하였으나 현재 세션에서 서버가 생성한 새로운 동적 ID을 공개적으로 전송하고, 사용자는 이 값을 다음 세션의 동적 ID로 그대로 사용하기 때문에 사용자에게 안전한 익명성을 제공하지 못한다. 또한 이러한 문제로 인하여 사용자에 대한 추적 불가능성도 제공하지 못한다. 그러므로 본 논문에서는 이러한 문제점을 해결하기 위하여 ECC와 생체정보를 사용한 개선된 TMIS 인증 프로토콜을 제안한다.

본 논문의 구성은 2장에서 Chen-Chen의 인증 프로토콜에 대하여 살펴보고, 3장에서 Chen-Chen의 인증 프로토콜에 대한 문제점을 분석한다. 4장에서는 문제를 개선한 새로운 인증 프로토콜을 제안하고 그에 대한 안전성을 5장에서 분석한다. 6장에서는 전체 논문의 결론을 요약하고 본 논문을 마무리한다.

II. Chen and Chen's Protocol

Chen-Chen의 TMIS 인증 프로토콜은 다음과 같다.

ID_i, PW_i: i번째 사용자의 ID와 패스워드

B_i: i번째 사용자의 생체정보

x: 서버 s의 개인키(private key)

$h()$: 안전한 단방향 해시함수(hash function)

$\oplus$: XOR 연산, $||$: 연접(concatenation) 연산

1. System initialization phase

ECC 알고리즘을 사용하는 Chen-Chen 인증 프로토콜은 다음과 같은 초기화 작업을 진행한다.

1.서버는 타원 곡선 $E(F_p)$와 $E(F_p)$상의 큰 난수 q을 가지는 기본 점 G을 선택한다.

2.서버는 안전한 단방향 해시 함수 $h()$을 선택한다.

3.서버는 개인키로 사용할 난수 $x \in Z_q^*$을 선택하고, 공개키 $Pub_s = x \cdot G$을 계산하여 $\{E(F_p), G, Pub_s, q, h()\}$을 공개한다.

2. Registration phase

Chen-Chen이 제안한 등록 단계는 다음과 같다.

1.환자 U_i은 자신의 ID_i와 패스워드 PW_i, 그리고 자신의 생체정보 B_i을 입력하고, 난수 r을 생성하여, $(\sigma_i, \theta_i) = Gen(B_i)$과 $OPW_i = h(ID_i||r_i||PW_i)$을 계산한 후, 안전한 채널을 통해 $\{ID_i, OPW_i\}$을 서버에 전달한다.

2.메시지를 받은 서버는 $h(ID_i)$가 데이터베이스에 존재하는지 확인하고, 존재하면 다른 ID_i을 선택하도록 요구한다. 만약 ID_i가 존재하지 않으면 서버는 $A_i = h(ID_i||x)$, $D_i = OPW_i \oplus A_i$을 계산한 후 난수 r_s을 생성하여 $EIDi = E_x(ID_i||r_s)$, $C_i = h(ID_i||A_i||OPW_i)$을 계산한다. 서버는 스마트카드에 $\{EID_i, D_i, C_i, h()\}$을 저장하여 안전한 채널을 통해 사용자에게 전달한다.

3.환자는 $y_i = r_i \oplus h(\sigma_i)$을 계산하여 스마트카드에 θ_i, y_i을 추가적으로 저장한다.

3. Login and authentication phase

Chen-Chen의 로그인 단계와 인증 단계의 간략화는 Fig. 1과 같고, 자세한 과정은 다음과 같다.

1.환자 U_i가 자신의 ID_i, PW_i, 생체정보 B_i을 입력하면 모바일 장치는 메모리의 y_i와 D_i을 검색하여 $\sigma_i = Ren(B_i, \theta_i)$, $r_i = y_i \oplus h(\sigma_i)$, $OPW_i = h(ID_i||r_i||PW_i)$, $A_i = OPW_i \oplus D_i$을 계산한다. 그런 다음 모바일 장치는 $h(ID_i||A_i||OPW_i)?= C_i$ 의 여부를 확인하여, 동일하지 않으면 세션을 종료하고 그렇지 않으면 난수 α와 타임스탬프 T_i을 생성하여 $X_i = \alpha \cdot G$, $V_i = h(ID_i||A_i||X_i||T_i)$을 계산한다. 그런 다음 모바일 장치는 $\{EID_i, X_i, V_i, T_i\}$를 서버에 전송한다.

2.서버는 T_i의 최신성을 검증하여, 타당하지 않으면 세션을 종료하고, 타당하면 $(ID_i||r_s) = D_x(EID_i)$, $A_i = h(ID_i||x)$을 계산한다. 그런 다음 $h(ID_i||A_i||X_i||T_i)?= V_i$의 동일성 여부를 확인하여, 동일하지 않으면 세션을 여기서 종료하고, 동일하면 난수 β을 생성하여 $X_s = \beta \cdot G$, $SK = h(ID_i'||T_1||A_i||\beta \cdot X_i)$을 계산한다. 서버는 새로운 난수 r_i^{new}을 선택하여, $EID_i^{new} = E_x(ID_i||r_s^{new})$, $V_s = h(A_i||T_2||EID_i^{new}||SK)$을 계산하여 $\{EID_i^{new}, X_s, V_s, T_2\}$을 모바일 장치로 전송한다.

3.모바일 장치는 $SK = h(ID_i||T_1||A_i||\alpha \cdot X_i)$을 계산하여 $h(A_i||T_2||EID_i^{new}||SK)?= V_s$이 동일한지 확인하고, 동일하면 EID_i을 새로운 EID_i^{new}로 대체한다. 동일하지 않을 경우에는 세션을 종료한다.

4. Password biometrics update phase

Chen-Chen 프로토콜의 패스워드 변경 단계는 다음과 같이 진행한다.

1.환자 U_i은 자신의 스마트카드를 카드리더기에 장착하고, 자신의 ID_i와 PW_i, 그리고 생체정보 B_i을 입력한다. 스마트카드는 $\sigma_i = Rep(B_i, \theta_i)$, $r_i = y_i \oplus h(\sigma_i)$, $OPW_i = h(ID_i||r_i||PW_i)$, $A_i = OPW_i \oplus D_i$을 계산한다.

2.스마트카드는 $h(ID_i||A_i||OPW_i)?= C_i$의 여부를 확인하여 두 값이 동일하지 않으면 세션을 종료하고, 그렇지 않으면 환자에게 새로운 패스워드 PW_i^{new}와 B_i^{new}을 입력하도록 요청한다.

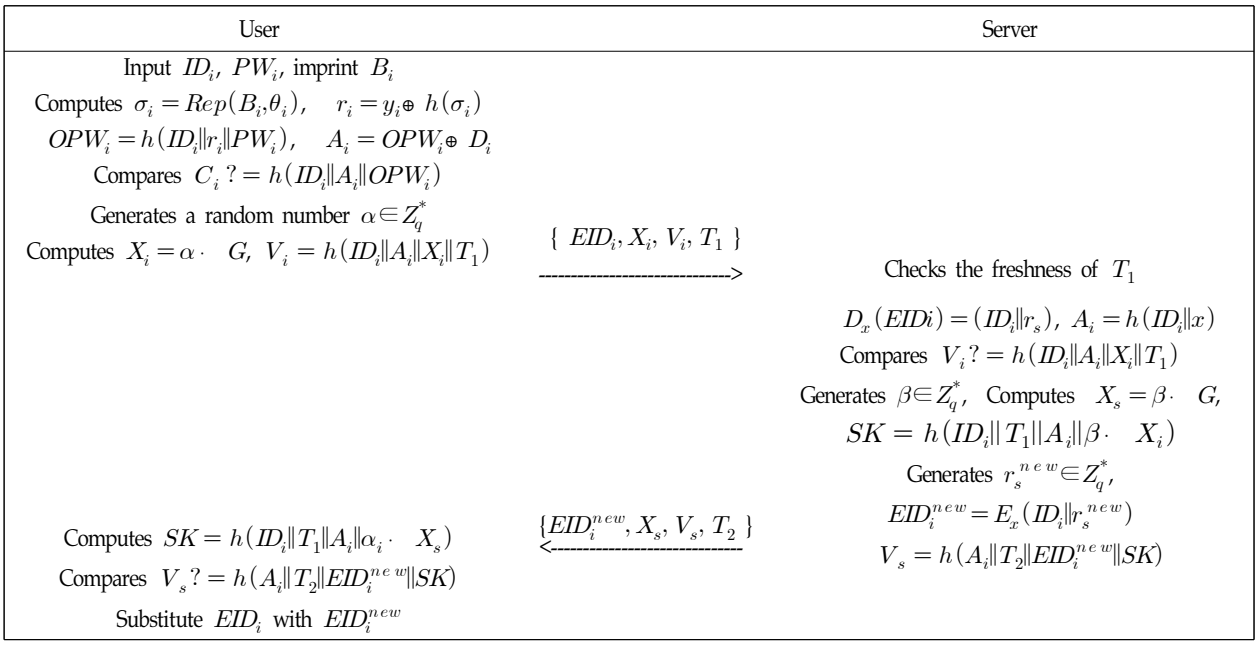

Fig. 1. Chen and Chen's Login and Authentication

3.환자는 새로운 패스워드 PW_i^{new}와 생체정보 B_i^{new}을 입력한다.

4.스마트카드는 새로운 난수 r_i^{new}을 생성하고, $(\sigma_i^{new}, \theta_i^{new}) = Gen(B_i^{new})$, $OPW_i^{new} = h(ID_i \| r_i^{new} \| PW_i^{new})$, $D_i^{new} = A_i \oplus OPW_i^{new}$, $C_i^{new} = h(ID_i \| A_i \| OPW_i^{new})$, $y_i^{new} = r_i^{new} \oplus h(\sigma_i^{new})$을 계산한다. 마지막으로 스마트카드는 $\{D_i, C_i, \theta_i, y_i\}$을 $\{D_i^{new}, C_i^{new}, \theta_i^{new}, y_i^{new}\}$로 업데이트한다.

III. Weakness of Chen and Chen's Protocol

본 장에서는 Chen-Chen의 인증 프로토콜에 대한 안전성과 설계 측면에서의 문제를 제시한다.

1. Security Analysis

3.1.1 User impersonation attack

공격자는 등록단계의 환자가 서버에 제출하는 정보 $\{OPW_i, ID_i\}$와 스마트카드의 $\{EID_i, D_i, C_i, y_i, h()\}$의 정보 획득에 성공하였다고 가정할 경우, 공격자는 다음과 같은 과정을 통하여 사용자 가장 공격을 할 수 있다. 공격자는 A_i을 계산하기 위하여, 앞에서 획득한 OPW_i'와 D_i'을 사용하여 $A_i' = OPW_i \oplus D_i$와 같이 A_i'을 계산한다. V_i은 앞에서 획득한 ID_i와 A_i', 공개 데이터 X_i, V_i, T_1을 사용하여, 획득한 값들의 정확성을 확인할 수 있다.

$$V_i ? = h(ID_i \| A_i' \| X_i \| T_1)$$

공격자는 사용자의 생체정보를 획득하기 어려워 난수 r_i을 계산해 낼 수 없다고 하더라도, 앞에서 계산해 낸 값들과 로그인 요청 메시지 V_i을 사용하여 사용자를 가장한 공격에 성공할 수 있다.

3.1.2 Man-in-the-middle attack

앞의 사용자 가장 공격에서 획득한 정보들 중 A_i', ID_i', T_1, 그리고 메시지 X_s을 그대로 사용하고 공격자 자신이 생성한 난수 α'을 사용하여 $X_i^a = \alpha' \cdot G$을 계산하여 서버에 전송하면 공격자는 Fig. 2의 과정에 의하여 서버의 인증과정을 통과할 수 있다. 또한 공격자는 난수 α'을 자신이 생성하였기 때문에 서버로부터 로그인 응답 메시지를 받을 경우, 다음 계산 과정을 진행하여 세션키 SK을 계산할 수 있다. 그러므로 Chen-Chen의 프로토콜은 중간자 공격과 세션키 노출 공격에 안전하지 않다.

3.1.3 Unsecure untraceability

Chen-Chen의 프로토콜은 사용자가 EID_i을 사용하

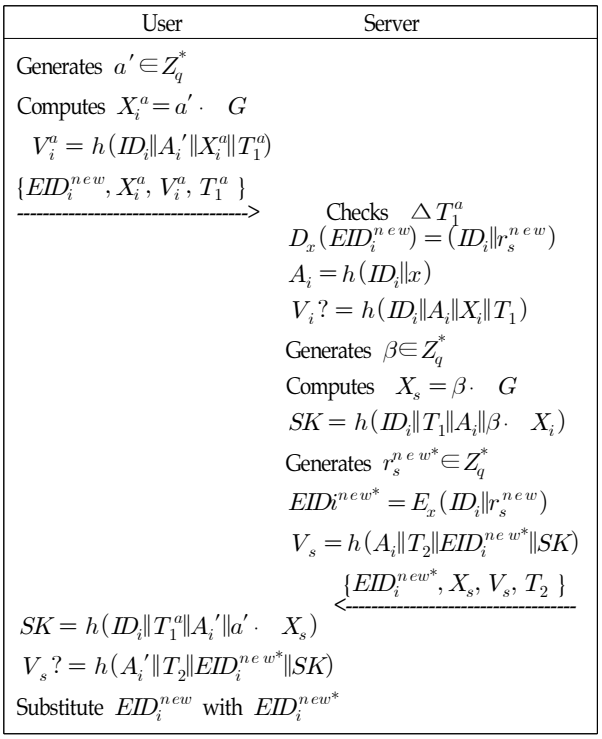

Fig. 2. Man-in-the-middle attack

여 로그인 요청 메시지를 보내면, 서버는 응답 메시지로 EID_i^{new}을 공개적으로 사용자에게 보낸다. EID_i^{new}은 다음에 사용할 동적 ID이기 때문에 공격자가 이 두 개의 공개 데이터만으로는 사용자의 ID_i을 직접 계산해 낼 수 없어 어떤 사용자인지는 정확히 알 수 없다 하더라도, EID_i^{new}을 계속 추적할 경우 임의의 동일한 사용자가 서버에 접속한다는 것을 알 수 있다. 그러므로 Chen-Chen 프로토콜은 안전한 추적 불가능성을 제공하지 못한다.

2. Analysis of Design Defects

Chen-Chen의 등록단계는 사용자의 ID 중복을 확인하기 위하여 $h(ID_i)$가 데이터베이스에 존재하는지의 여부를 확인한다. $h(ID_i)$로 확인하는 것은 데이터베이스의 정보가 노출될 경우를 대비하여 해시함수를 사용한 것으로 보인다. 그러나 해시함수를 사용하여 저장하였다 하더라도 이 값들이 노출될 경우 높은 엔트로피의 ID가 아닌 이상 ID 추측 공격에 안전하다고 할 수 없다.

IV. The Proposed Protocol

본 장에서는 Chen-Chen 프로토콜의 문제를 해결하고자 개선된 안전성과 사용자 익명성을 제공하는 향상된 프로토콜을 제안한다. 시스템 초기화 단계는 Chen-Chen 프로토콜의 과정과 동일하다.

1. Registration phase

서버에 등록을 원하는 새로운 사용자는 다음 과정을 진행한다.

1.환자 U_i은 자신의 ID_i, 패스워드 PW_i, 그리고 자신의 생체정보 B_i을 입력하고, 난수 r_i을 생성하여, $Gen(B_i) = (\sigma_i, \theta_i)$, $RPW_i = h(PW_i \oplus r_i)$, $OPW_i = h(ID_i \| r_i \| PW_i)$을 계산하여, $\{ID_i, RPW_i\}$을 보호된 채널을 통하여 서버로 보낸다.

2.서버는 환자의 ID_i에 대한 타당성을 확인하여, 사용가능한 ID_i이면 $A_i = h(ID_i \| x)$, $D_i = RPW_i \oplus A_i$을 계산한 후 난수 r_s을 생성하여 $EID_i = E_x(ID_i \| r_s \| A_i)$을 계산한다. 서버는 $\{EID_i, D_i, h()\}$을 스마트카드에 저장하여 보호된 채널을 통하여 환자에게 안전하게 보낸다.

3.환자는 $y_i = r_i \oplus h(\sigma_i)$, $A_i = D_i \oplus RPW_i$, $C_i = h(ID_i \| A_i \| OPW_i)$, $C_i' = C_i \oplus r_i$, 그리고 $D_i' = A_i \oplus OPW_i$을 계산하여 스마트카드에 최종적으로 $\{EID_i, D_i', C_i', y_i, \theta_i, h()\}$을 저장한다.

2. Login and authentication phase

서버의 로그인 요청을 원하는 사용자는 다음과 같은 과정을 진행하며 간략화 된 과정은 Fig. 3과 같다.

1.환자 U_i가 자신의 ID_i와 패스워드 PW_i, 생체정보 B_i을 입력하면 모바일 장치는 y_i와 D_i'을 검색하여 $\sigma_i = Re n(B_i, \theta_i)$, $r_i = y_i \oplus h(\sigma_i)$, $OPW_i = h(ID_i \| r_i \| PW_i)$, $A_i = OPW_i \oplus D_i'$, $C_i = C_i' \oplus r_i$을 계산한다. 그런 다음 모바일 장치는 $h(ID_i \| A_i \| OPW_i) ? = C_i$의 여부를 확인하여, 동일하지 않으면 세션을 종료하고 그렇지 않으면 난수 α와 타임스탬프 T_i을 생성하여 $X_i = (\alpha \oplus PW_i) \cdot G$, $V_i = h(ID_i \| A_i \| X_i \| EID_i \| T_1)$을 계산한다. 모바일 장치는 $\{EID_i, X_i, V_i, T_1\}$를 서버에 전송한다.

2.서버는 T_1의 타임스탬프 임계조건을 확인하여 타당하지 않으면 세션을 종료하고, 타당할 경우, 자신의 개인키 x로 복호화 $D_x(EID_i) = (ID_i \| r_s)$을

계산한 후 $A_i' = h(ID_i \| x)$을 계산한다. 그런 다음 $V_i ? = h(ID_i \| A_i' \| X_i \| EID_i \| T_1)$의 동일성 여부를 확인하여, 동일하지 않으면 세션을 종료하고 동일할 경우 난수 β을 생성하여 $X_s = \beta \cdot G$, $SK = h(ID_i' \| T_1 \| A_i' \| \beta \cdot X_i)$을 계산한다. 서버는 새로운 난수 r_i^{new}와 타임스탬프 T_2을 생성하여, $EID_i^{new} = E_x(ID_i \| r_s^{new} \| A_i')$, $NEID_i^{new} = EID_i^{new} \oplus h(A_i' \| T_2)$, $V_s = h(A_i' \| T_2 \| EID_i^{new} \| SK \| X_s)$을 계산하여 $\{NEID_i^{new}, X_s, V_s, T_2\}$을 환자에게 전송한다.

3.환자는 T_2의 타임스탬프 임계조건을 확인하여, 타당하지 않으면 세션을 종료하고, 타당할 경우 세션키 $SK = h(ID_i \| T_1 \| A_i \| (\alpha \oplus PW_i) \cdot X_s)$와 $EID_i^{new'} = NEID_i^{new} \oplus h(A_i \| T_2)$을 계산하여 $h(A_i \| T_2 \| EID_i^{new'} \| SK \| X_s) ? = V_s$이 동일한지 확인한다. 동일하면 $EID_i^{new'}$을 EID_i 대신에 저장하고, 동일하지 않을 경우에는 세션을 종료한다.

환자는 다음과 같은 과정을 진행하여 자신의 패스워드를 새롭게 업데이트한다.

1.환자 U_i은 자신의 스마트카드를 카드리더기에 장착하고, 자신의 ID_i와 PW_i, 그리고 생체정보 B_i을 입력한다. 스마트카드는 $\sigma_i = Rep(B_i, \theta_i)$, $r_i = y_i \oplus h(\sigma_i)$, $OPW_i = h(ID_i \| r_i \| PW_i)$, $A_i = OPW_i \oplus D_i'$을 계산한다.

2.스마트카드는 $h(ID_i \| A_i \| OPW_i) ? = C_i$의 여부를 확인하여 두 값이 동일하지 않으면 세션을 종료하고, 그렇지 않으면 환자에게 새로운 패스워드 PW_i^{new}와 생체정보 B_i^{new}을 입력하도록 요청한다.

3.환자는 새로운 패스워드 PW_i^{new}와 생체정보 B_i^{new}을 입력한다.

4.스마트카드는 $(\sigma_i^{new}, \theta_i^{new}) = Gen(B_i^{new})$을 계산한 후, 새로운 난수 r_i^{new}을 생성하여 $y_i^{new} = r_i^{new} \oplus h(\sigma_i^{new})$, $OPW_i^{new} = h(ID_i \| r_i^{new} \| PW_i^{new})$, $C_i^{new} = h(ID_i \| A_i \| OPW_i^{new})$, $C_i'^{new} = C_i^{new}$

3. Password biometrics update phase

User		Server
Inputs ID_i, PW_i, imprint B_i Computes $\sigma_i = Rep(B_i, \theta_i)$, $r_i = y_i \oplus h(\sigma_i)$ $OPW_i = h(ID_i \| r_i \| PW_i)$, $A_i = OPW_i \oplus D_i'$, $C_i = C_i' \oplus r_i$, $h(ID_i \| A_i \| OPW_i) ? = C_i$ Generates a random number $\alpha \in Z_q^*$ Computes $X_i = (\alpha \oplus PW_i) \cdot G$, $V_i = h(ID_i \| A_i \| X_i \| EID_i \| T_1)$	EID_i, X_i, V_i, T_1 ---------->	Checks time delay of T_1 Computes $D_x(EID_i) = (ID_i \| r_s)$, $A_i' = h(ID_i \| x)$ Compares $V_i ? = h(ID_i \| A_i' \| X_i \| EID_i \| T_1)$ Generates a random number $\beta \in Z_q^*$ Computes $X_s = \beta \cdot G$ $SK = h(ID_i \| T_1 \| A_i' \| \beta \cdot X_i)$ Generates a random number $r_s^{new} \in Z_q^*$ $EID_i^{new} = E_x(ID_i \| r_s^{new} \| A_i')$ $NEID_i^{new} = EID_i^{new} \oplus h(A_i' \| T_2)$ $V_s = h(A_i' \| T_2 \| EID_i^{new} \| SK \| X_s)$
Checks time delay of T_2 $SK = h(ID_i \| T_1 \| A_i \| (\alpha \oplus PW_i) \cdot X_s)$ $EID_i^{new'} = NEID_i^{new} \oplus h(A_i \| T_2)$ $V_s ? = h(A_i \| T_2 \| EID_i^{new'} \| SK \| X_s)$ Substitute EID_i with EID_i^{new}	<---------- $NEID_i^{new}, X_s, V_s, T_2$	

Fig. 3. The Proposed Login and Authentication

$\oplus\ r_i^{new}$, $D_i'^{new} = A_i \oplus OPW_i^{new}$을 계산한다. 마지막으로 스마트카드는 새롭게 계산한 $\{D_i'^{new}, C_i'^{new}, \theta_i^{new}, y_i^{new}\}$로 업데이트한다.

V. Analysis of The Proposed Protocol

1. Security analysis

Table. 1은 제안 프로토콜과 관련 프로토콜들에서 제공하는 기능과 안전성을 비교한 것이다.

Smart-card/mobile device lost attack

공격자는 스마트카드 SC_i을 손에 넣을 경우, SC_i에 저장된 $EID_i, D_i', C_i', y_i, \theta_i$들과 식 $D_i' = A_i \oplus OPW_i$나 $C_i' = C_i \oplus r_i$을 사용하여 사용자의 ID_i와 패스워드 PW_i에 대한 추측 공격을 시도할 것이다. 그러나 $D_i' = A_i \oplus OPW_i$에서 D_i'을 제외한 A_i와 OPW_i은 SC_i에 저장된 값이 아니고, $C_i' = C_i \oplus r_i$에서는 C_i'은 저장하나 C_i와 r_i은 높은 엔트로피의 저장하지 않은 정보들이다.

전송 메시지들 중 EID_i은 $E_x(ID_i \| r_s \| RPW_i)$와 같이 서버의 비밀키 x로 암호화되어 있어, 이 비밀키가 노출되지 않는 한 이 식으로부터 사용자의 PW_i을 계산해 내기 어렵고, 전송 메시지 $X_i = (\alpha \oplus PW_i) \cdot G$은 ECDLP의 어려움에 근거하여 X_i와 G을 안다고 하더라도 $\alpha \oplus PW_i$을 계산해내기 어렵다.

Offline password guessing attack

제안 프로토콜에서 사용자의 패스워드 PW_i은 난수 r_i와 함께 RPW_i나 OPW_i와 같이 해시함수로 연산 처리하였고, r_i, RPW_i, 그리고 OPW_i은 저장되지 않는 값이다. 공격자가 난수 r_i을 계산해내려면 식 $r_i = y_i \oplus h(\sigma_i)$을 사용할 수 있는데, 이 식에서 σ_i은 높은 엔트로피의 사용자 생체정보이므로 이 값을 알아내기 힘들다.

Perfect forward secrecy

공격자가 서버의 개인키 x을 안다고 가정할 경우, 공격자는 EID_i을 복호화($D_x(EID_i) = (ID_i \| r_s \| RPW_i)$)할 수 있고, 사용자의 ID_i을 얻게 된 공격자는 $A_i = h(ID_i \| x)$을 계산할 수 있다. 그러나 공격자가 세션키 $SK = h(ID_i \| T_1 \| A_i \| \beta \cdot X_i)$을 계산하려면 공격자가 서버가 생성한 난수 β을 알아야 하는데, 이 난수는 매 세션마다 새롭게 생성하여 사용하므로 서버의 개인키가 노출되더라도 이전의 세션키를 공격자는 계산할 수 없다.

Insider attack

내부 공격자가 등록단계의 ID_i와 RPW_i을 손에 넣었을 경우, RPW_i로부터 패스워드 추측공격에 성공하려면 난수 r_i을 알아야한다. 그러나 높은 엔트로피의 난수와 함께 해시 처리한 RPW_i로부터 PW_i을 계산해내기 어렵다. 또한 제안 프로토콜은 내부 공격자가 사용자의 PW_i을 모른다하더라도 등록단계에서 획득한 RPW_i을 재사용할 수 있는데 이러한 재사용을 막기 위해서 서버가 전송한 D_i의 값을 사용자는 D_i'으로 계산하여 스마트카드에 저장한다. 그러므로 RPW_i 값 자체로는 사용자의 PW_i을 알아내기 어렵다.

User anonymity

제안 프로토콜은 다음 세션의 동적 ID을 $NEID_i^{new}$

Table 1. Comparison of Security Functions and Design Defects

	[1]	[4]	[6]	[7]	[9]	[11]	Ours
User anonymity	X	O	O	X	O	X	O
User impersonation attack	O	X	X	X	X	X	O
Server spoofing attack	O	O	O	O	O	O	O
Stolen smart card attack	O	O	X	O	X	O	O
Insider attack	O	X	O	X	O	X	O
Password guessing attack	O	O	O	O	X	O	O
Replay attack	O	O	O	O	O	O	O
Man-in-the-middle attack	O	X	X	X	X	X	O
User untraceability	X	O	X	X	O	X	O
Perfect forward attack	O	O	O	X	O	O	O
Design defects	X	X	X	X	X	X	O

Table 2. Performance Comparison of Related Protocols

	User	Server	Total
Chaudhry et al.[1]	$3T_h$+$3T_{EM}$+$1T_{BH}$	$3T_h$+$2T_{EM}$+$1T_{IN}$	$6T_h$+$5T_{EM}$+$1T_{BH}$+$1T_{IN}$ ≈ 0.12601
Chaudhry et al.[2]	$7T_h$+$4T_{EM}$+$2T_{SY}$+$1T_{BH}$	$6T_h$+$3T_{EM}$+$3T_{SY}$	$13T_h$+$7T_{EM}$+$6T_{SY}$ ≈ 0.2516
Han et al.[6]	$5T_h$+$2T_{EM}$+$1T_{BH}$	$4T_h$+ $2T_{EM}$+$2T_{SY}$	$9T_h$+$4T_{EM}$+$2T_{SY}$+$1T_{BH}$ ≈ 0.13921
Sahoo et al.[7]	$7T_h$+$3T_{EM}$+$1T_{FE}$	$4T_h$+$4T_{EM}$	$11T_h$+$7T_{EM}$+$1T_{FE}$ ≈ 0.191389
Sarif et al.[9]	$7T_h$ + $2T_{EM}$	$6T_h$+ $2T_{EM}$+$2T_{SY}$	$13T_h$+$4T_{EM}$+$2T_{SY}$ ≈ 0.1007
Chen-chen[11]	$5T_h$+$2T_{EM}$+$1T_{FE}$	$4T_h$+ $2T_{EM}$+$2T_{SY}$	$9T_h$+$4T_{EM}$+$2T_{SY}$+$1T_{FE}$ ≈ 0.141189
The Proposed protocol	$7T_h$+$2T_{EM}$+$1T_{FE}$	$5T_h$+$2T_{EM}$+$2T_{SY}$	$12T_h$+$4T_{EM}$+$2T_{SY}$+$1T_{FE}$≈ 0.156189

$= EID_i^{new} \oplus h(A_i' \| T_2)$와 같이 계산하여 전송하기 때문에 공격자는 A_i'을 알아야 만이 $NEID_i^{new}$로부터 EID_i^{new}을 계산해낼 수 있다. A_i'은 OPW_i와 D_i'을 알아야 계산해 낼 수 있으나, OPW_i와 A_i'은 저장하지 않는 값이기 때문에 $A_i = OPW_i \oplus D_i'$로부터 A_i'을 계산해내기 어렵다.

Man-in-the-middle attack

제안 프로토콜에서 공격자가 중간자 공격에 성공하려면 전송 메시지 $\{EID_i, X_i, V_i, T_1\}$을 생성할 수 있어야 한다. 제안 프로토콜은 V_i 연산 시 전송 메시지의 EID_i, X_i, T_1을 모두 포함하여 계산하므로 이 메시지들에 대한 무결성을 제공한다. 그러므로 이 3개의 메시지에 대한 재사용이나 변경은 불가하고, 공격자는 A_i의 값을 알아야 만이 공격에 성공할 수 있다. 그러나 Smart-card lost attack 절에서 분석한 바와 같이 공격자는 스마트카드의 정보들을 획득하였다 할지라도 A_i을 계산해내기 힘들다.

2. Performance Analysis

본 논문에서 비교한 계산 복잡도는 Table 2와 같고, 각 프로토콜의 계산 복잡도는 로그인 단계와 인증 단계에서 사용자와 서버의 계산 복잡도로 각각 구별하여 표기하였다. 계산 복잡도에 사용한 기호들의 의미와 실행시간은 다음과 같이, T_h은 해시함수로, 0.0005s의 실행 시간, T_{BH}는 바이오 해시함수로 0.00001s, T_{EM}은 ECC point 곱셈으로 0.0192s, T_{SY}은 대칭키 암·복호화로 0.0087s, T_{FE}은 퍼지 추출함수로 0.001989s이다[3][12][13].

각 프로토콜의 계산 복잡도를 살펴보면, Sharif et al. 프로토콜만 생체정보를 사용하지 않아 0.1007s로 가장 빠르다. 반면에 Chaudhry et al.[2]의 프로토콜은 0.2516s로 가장 긴 실행시간을 나타내는데 이것은 그들의 인증 프로토콜에서 TMIS의 전체 구조를 제어하는 최상위 CMS 서버가 더 추가되었기 때문이다. Sahoo et al.의 프로토콜은 T_{ECM} 연산 횟수가 총 7번으로 다른 프로토콜들에 비하여 곱셈연산 횟수가 많아서 실행시간이 두 번째로 크게 나온 것을 볼 수 있다.

Han et al.의 프로토콜은 실행시간이 대략 0.13921s인데, 이 프로토콜에서 사용한 바이오 해시함수를 퍼지 추출함수로 변경하여 실행시간을 계산하면 대략 0.141s로 퍼지 추출함수를 사용한 다른 프로토콜들과 비슷한 실행시간을 보인다. Chen-Chen의 프로토콜도 퍼지 추출함수를 사용한 프로토콜로 실행시간이 대략 0.141189s가 되고, Chen-Chen 프로토콜의 문제점을 개선한 제안한 프로토콜은 0.156189s가 걸린다.

IV. Conclusions

본 논문에서는 Chen-Chen이 제안한 ECC와 생체정보를 사용한 인증 프로토콜을 분석하였고, 사용자 가장 공격, 중간자 공격, 사용자 익명성, 그리고 추적 불가능성 등의 문제가 있었다. 그리하여 본 논문에서는 이러한 문제를 해결하고 사용자 익명성을 제공하는 안전한 인증 프로토콜을 제안하였다.

제안한 프로토콜의 안전성 문제를 분석한 결과, 오프라인 패스워드 추측 공격, 사용자 가장 공격, 스마트카드 분실 공격, 내부자 공격, 전방향 안전성, 재생 공격 등 여러 공격에 안전한 것으로 분석되었다. 또한 제안 프로토콜은 TMIS에서 반드시 보장해야 하는 사용자 익명성을 제공함으로써, 추적 불가능성과 사용자에 대한 프라이버시를 안전하게 보장하였다.

게다가 제안 프로토콜은 Chen-Chen 프로토콜에 비하여 실행시간도 크게 증가하지 않아 계산 복잡도에서도 좋은 결과를 나타내었다. 그러므로 본 논문에서 제안한 프로토콜은 TMIS의 사용자들에게 안전한 익명성과 안전성을 제공하여 민감한 정보를 다루는 TMIS에 적합한 인증 프로

토콜이라고 할 수 있다.

REFERENCES

[1] S. A. Chaudhry, K. Mahmood, H. Naqvi, H., M. K. Khan, "An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography," Journal of Medical Systems, Vol. 39, pp.1-12, Sept. 2015. DOI: 10.1007/s10916-015-0335-y

[2] 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, pp.1-8, Feb. 2015. DOI: 10.1007/s10916-015-0221-7

[3] H. Arshad, and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," Journal of Medical Systems, Vol. 38, pp.1-12, Oct. 2014. DOI: 10.1007/s10916-014-0136-8

[4] S. A. Chaudhry, M. T. Khan, M. K. Khan, and T. Shon, "A multiserver biometric authentication scheme for TMIS using elliptic curve cryptography," Journal of Medical Systems, Vol. 40, pp.1-13, Sept. 2016. DOI: 10.1007/s10916-016-0592-4

[5] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "An efficient and practical smart card based anonymity preserving user authentication scheme for tmis using elliptic curve cryptography," Journal of Medical Systems, Vol. 39, pp.1-18, Oct. 2015. DOI: 10.1007/s10916-015-0351-y

[6] L. Han, Q. Xie, and W. Liu, "An Improved Biometric Based Authentication Scheme with User Anonymity Using Elliptic Curve Cryptosystem," International Journal of Network Security, Vol. 19, No. 3, pp.469-478, May 2017. DOI: 10.6633/IJNS.201703.19(3).16

[7] S. S. Sahoo and S. Mohanty, "A Lightweight Biometric-based Authentication Scheme for Telecare Medicine Information Systems Using ECC," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, pp.1-6, July 2018. DOI: 10.1109/ICCCNT.2018.8494092.

[8] H. Arshad, and A. Rasoolzadegan, "Design of a secure authentication and key agreement scheme preserving user privacy usable in telecare midicine information systems," Journal Medical Systems, Vol. 40, pp.1-19, Sept. 2016. DOI: 10.1007/s10916-016-0585-3

[9] A. O. Sharif, D. A. Mood, and M. Nikooghadam, "An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC," International Journal of Communication Systems, Vol. 32, Issue. 5, pp.1-23, Feb. 2019. DOI: 10.1002/dac.3913

[10] N. Ravanbakhsh, and M. Nazari, "An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems," Multimedia Tools and Applications, Vol. 77, No. 1, pp.55-88, 2018. DOI: 10.1007/s11042-016-4208-2

[11] Y. Chen and J. Chen, "A biometrics-based mutual authentication and key agreement protocol for TMIS using elliptic curve cryptography," Multimedia Tools and Applications, Vol. 82, pp.16009-16032, 2023. DOI: 10.1007/s11042-022-14007-3

[12] Hathaliyaa, J. J., Tanwar, S. and Evans, R., "Securing electronic healthcare records: A mobile-based biometric authentication approach," Journal of Information Security and Applications, Vol. 53, pp.1-14, May 2020. DOI: 10.1109/ACCESS.2022.3208347.

[13] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF," IEEE Access, Vol. 10, pp.101330-101346, Sept. 2022. DOI: 10.1109/ACCESS.2022.3208347

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.