JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 29 No. 6, pp. 53-60, June 2024
https://doi.org/10.9708/jksci.2024.29.06.053

Problem Analysis and Enhancement of 'An Improved of Enhancements of a User Authentication Scheme'

Mi-Og Park*

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

[Abstract]

In this paper, we analyze the authentication scheme of Hwang et al. proposed in 2023 and propose a new authentication scheme that improves its problems. Hwang et al. claimed that their authentication scheme was practical and secure, but as a result of analysis in this paper, it is possible to attack the password/ID guessing attack and session key disclosure attack due to insider attack and stolen smart card attack. In addition, Hwang et al.'s authentication scheme, which provides user anonymity, does not provide user untraceability due to its unstable design. The proposed authentication scheme, which improves these problems, not only provides user untraceability, but also is secure for stolen smart card attack, insider attack, session key disclosure attack, and replay attack. In addition, except for one fuzzy extraction operation, it shows the same complexity or very similar one as related authentication schemes. Therefore, the proposed authentication scheme can be said to be an authentication scheme with safety and practicality.

▸ **Key words**: User Authentication, TMIS, Insider attack, Smart-card attack, Session Key

[요 약]

본 논문에서는 2023년에 제안된 Hwang et al.의 인증 스킴에 대하여 분석하고, 그에 대한 문제점을 개선한 새로운 인증 스킴을 제안한다. Hwang et al.은 자신들의 인증 스킴이 실용적이고 안전하다고 주장하였으나 본 논문에서 분석한 결과, 내부자 공격과 스마트카드 분실 공격으로 인하여 사용자의 패스워드/ID 추측 공격과 세션키 노출 공격 등이 가능하다. 또한, 사용자 익명성을 제공하는 Hwang et al.의 인증 스킴은 불안전한 설계로 인하여 사용자 추적 불가능성을 제공하지 못한다. 이러한 문제를 개선한 제안 인증 스킴은 사용자 추적 불가능성을 제공할 뿐만 아니라 스마트카드 분실 공격, 내부자 공격, 세션키 노출 공격, 재생 공격 등에 안전한 것으로 분석되었다. 또한, 한 번의 퍼지 추출 연산을 제외하면 관련된 인증 스킴들과 동일한 복잡도나 매우 비슷한 복잡도를 보인다. 그러므로 제안 인증 스킴은 안전성과 실용성을 갖춘 스킴이라고 할 수 있다.

▸ **주제어**: 사용자 인증, TMIS, 내부자 공격, 스마트카드 공격, 세션키

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@daum.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2024. 04. 24, Revised: 2024. 05. 29, Accepted: 2024. 05. 29.

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

I. Introduction

2017년 Aslam et al. 등은 인증 스킴[[1]에서 40개의 사용자 인증 스킴들을 분석하였고, 그 중에서 인증 스킴[2]가 가장 좋은 인증 방식이라고 주장하였다. ECC(Ellipse Curve Cryptography)를 이용한 인증 스킴[2]는 2015년에 제안된 3-factor 인증 방식으로, 원격의료 정보시스템(Telecare Medicine Information Systems, TMIS)의 사용자를 위하여 사용자 익명성(user anonymity)을 제공하고, 생체정보 처리에는 바이오 해시함수(bio hash function)를 사용하였다. TMIS을 위한 인증 스킴들에는 사용자 익명성을 제공하지 않는 다수의 인증 스킴들도 있으나, TMIS는 환자들의 개인 정보와 건강 정보 등을 인터넷으로 전송하기 때문에, TMIS에서의 사용자 익명성은 필수적인 기능이다[3-5]. TMIS에서의 사용자 익명성을 제공하는 인증 스킴[2]는 인증 스킴[3]과 인증 스킴[6]을 개선한 것으로, 인증 스킴[3], [6]에서도 TMIS의 사용자 익명성을 제공한다.

Amin et al.은 RSA을 이용한 다른 TMIS 인증 스킴[7]도 2015년에 제안하였으며, 이 인증 스킴은 인증 스킴[8]이 오프라인 패스워드 추측 공격(offline password guessing attack)과 내부자 공격(privileged insider attack)에 안전하지 않고, 사용자 익명성을 제공하지 않는다고 분석하면서 사용자 익명성을 제공하는 방식을 제안하였다. 2020년에 Kim이 제안한 인증 스킴[9]에서도 인증 스킴[8]이 스마트카드 분실 공격(stolen smart-card attack)과 재생 공격(replay attack)에 안전하지 않다고 지적하였다. 그러나 인증 스킴[9]는 TMIS에서의 사용자 익명성 문제는 개선하지 않았다.

2021년에 Liu et al. 등이 제안한 인증 스킴[10]은 인증 스킴[2]를 개선한 것으로, 인증 스킴[2]가 내부자 공격, 재생 공격, 스마트카드 분실 공격, 그리고 사용자 가장 공격(user impersonation attack)에 안전하지 않다고 분석하였다. 인증 스킴[10]은 이러한 문제들을 해결하기 위하여, ECC와 바이오 해시함수를 이용한 3-factor 인증 스킴을 제안하였고 자신들의 인증 스킴은 관련 인증 스킴들보다 더 빠르고 안전하다고 주장하였다. 그러나 2023년 Hwang et al.이 제안한 인증 스킴[11]은 인증 스킴[10]이 위조된 스마트카드 공격(fake smart card attack)과 암기하기 어려운 난수의 문제가 있다고 지적하였다. 여기서 암기하기 어려운 난수 문제란 인증 스킴[10]에서 난수처럼 긴 패스워드를 사용하였고, 패스워드 길이가 난수처럼 길기 때문에 공격자가 패스워드 추측 공격에 성공할 수 없으므로, 자신들의 인증 스킴이 안전하다고 주장하였다. 그러나 일반적인 사용자들은 난수처럼 긴 패스워드를 암기하기 어렵기 때문에, 인증 스킴[10]이 비실용적이라고 인증 스킴[11]에서 지적한 것이다. 이러한 문제를 개선한 3-factor 인증 스킴[11]은 자신들의 인증 스킴이 실용성과 안전성을 모두 제공한다고 주장하였다.

본 논문에서 인증 스킴[11]을 분석한 결과, 사용자 익명성을 강조한 인증 스킴[10]은 서버에서 받은 응답 메시지의 일부를 다음 세션에서 그대로 사용하여 추적 불가능성을 제공하지 못하며, 인증 스킴[11]에서도 동일한 문제가 발생하였다. 또한 인증 스킴[11]에서 분석하지 못한 문제 중, 인증 스킴[10]은 스마트카드 분실 공격과 내부자 공격 등의 문제도 존재한다. 또한 TMIS는 사용자의 민감한 건강 정보를 처리하므로 사용자의 구별이 매우 중요하다. 그러나 본 논문에서 분석한 인증 스킴[3], [10], [11]은 모두 등록 단계에서 사용자 식별자를 검증하지 않는다. 본 논문에서는 이러한 문제들과 인증 스킴[11]에 대한 문제점을 개선한 새로운 인증 스킴을 제안한다.

본 논문의 구성은 2장에서 Hwang et al.이 제안한 인증 스킴에 대해 살펴보고, 3장에서는 본 논문에서 분석한 문제점들을 제시한다. 4장과 5장에서는 본 논문에서 제안하는 인증 스킴의 제시와 그에 대한 안전성과 설계상의 문제 여부를 분석하고, 마지막으로 6장에서 제안 인증 스킴의 결론을 제시한다.

II. Review of Related Scheme

본 장에서는 Hwang et al.이 제안한 등록 단계, 로그인과 인증 단계, 그리고 패스워드 변경 단계를 살펴본다. 본 논문에서 사용하는 기호들의 의미는 다음과 같다.

ID_i, PW_i: i번째 사용자의 식별자와 패스워드
T_i : i번째 사용자의 지문(fingerprint)
x : 서버 s의 비밀키(secret key)
$E_x(), D_x()$: 비밀키 x를 이용한 대칭키 암·복호화
P : 타원곡선상의 점(point)
$h()$: 단방향 해시함수(one-way hash function)
$\oplus$, $||$: XOR 연산과 연결(concatenation) 연산

1. Registration phase

1.사용자 U_i는 자신의 ID_i와 패스워드 PW_i을 선택한다.
2.사용자는 자신의 지문 T_i을 입력한다.

User		Server
Inputs ID_i, PW_i, T_i $F_i' = h(T_i) ?= F_i$, $A_i' = h(PW_i \| h(F_i')) ?= A_i$ $RID_i' = h(ID_i \| h(F_i')) ?= RID_i$ Selects a random number r_i $W' = B_i \oplus h(RID_i \| A_i)$, $C_1 = r_i P$ $C_2 = r_i \oplus W$, $C_4 = h(RID_i \| r_i \| W \| T_1)$	$\{C_2, CID_i, C_4, T_1\}$ ----->	Checks $\triangle T_1$ Computes $RID_i \| r_s = D_x(CID_i)$ $W = h(ID_s \| x \| RID_i)$, $r_i' = C_2 \oplus W$ $C_1' = r_i' P$, $C_4' = h(RID_i \| r_i' \| W \| T_1)$ Compares $C_4' ?= C_4$ Selects a random number r_j Computes $SK = r_j C_1'$, $D_1 = r_j P$, $G_1 = D_1 + C_1'$, $L_i = h(RID_i' \| h(D_1) \| W \| T_2)$ $CID_i' = E_x(RID_i \| r_s')$
Checks $\triangle T_2$	<----- $\{CID_i', G_1, L_i, T_2\}$	
Computes $D_i' = G_1 - C_1'$ $L_i' = h(RID_i \| h(D_1') \| W \| T_2)$, $SK = r_i D_1' = r_i r_j P$ Compares $L_i' ?= L_i$ Computes $Z_i = h(RID_i \| SK)$	$\{Z_i\}$ ----->	Computes $Z_i' = h(RID_i \| SK)$, $Z_i' ?= Z_i$

Fig. 1. Hwang et al.'s Authentication Scheme

3.사용자는 $F_i = h(T_i)$, $A_i = h(PW_i \| h(F_i))$, 그리고 익명성을 위한 $RID_i = h(ID_i \| h(F_i))$을 계산한다.

4.사용자는 안전한 채널을 통하여 $\{RID_i, A_i, F_i\}$을 서버 S에게 보낸다.

5.서버는 $W = h(ID_s \| x \| RID_i)$, $B_i = h(RID_i \| A_i) \oplus W$을 계산한 후 난수 r_s을 선택하여 자신의 비밀키 x로 $CID_i = E_x(RID_i \| r_s)$을 계산한다. 그런 다음 $A_i, B_i, CID_i, h(W), h(F_i), h()$을 스마트카드에 저장한다.

6.서버 S는 안전한 채널을 통하여 사용자에게 스마트카드를 보낸다.

7.사용자는 A_i, B_i, $W' = h(RID_i \| A_i) \oplus B_i$을 계산한 후 W'과 W가 동일한지 확인하여 동일하면 스마트카드가 서버에서 발행된 것이라고 믿는다. 동일하지 않으면 세션을 종료한다.

2. Login and authentication phase

1.사용자는 ID_i, PW_i, T_i을 입력하여 다음 값들을 검증한다.

$$F_i' = h(T_i), \; A_i' = h(PW_i \| h(F_i'))$$
$$RID_i' = h(ID_i \| h(F_i'))$$

입력한 파라미터들이 일치하면, 사용자는 난수 r_i을 생성하여 다음 값들을 계산한 후, $\{C_2, CID_i, C_4, T_1\}$을 서버에서 보내고, 만약 파라미터들이 일치하지 않으면 세션을 종료한다. 여기서 T_1은 타임스탬프이다.

$$W' = B_i \oplus h(RID_i \| A_i), \; C_1 = r_i P$$
$$C_2 = r_i \oplus W, \quad C_4 = h(RID_i \| r_i \| W \| T_1).$$

2.서버는 T_1의 타당성을 검증하여 타당하면 자신의 비밀키 x로 CID_i을 복호화하여 RID_i을 추출해 낸 $((RID_i \| R = D_x(CID_i))$ 후 다음을 계산한다.

$$W = h(ID_s \| x \| RID_i), \; r_i' = C_2 \oplus W$$
$$C_1' = r_i'.P, \; C_4' = h(RID_i \| r_i' \| W \| T_1)$$

서버는 C_4'과 C_4가 동일한지 비교하여 동일하면 난수 r_j을 생성하여 다음을 계산한 후, 타임스탬프 T_2와 함께 $\{CID_i, G_1, L_i, T_2\}$을 사용자에게 보낸다.

$$SK = r_j C_1', \; D_1 = r_j P$$
$$L_i = h(RID_i' \| h(D_1) \| W \| T_2)$$
$$G_1 = D_1 + C_1', \; CID_i' = E_x(RID_i \| r_s')$$

3.사용자는 타임스탬프 T_2의 타당성을 검증하여 타당하면 다음 값들을 계산한 후 L_i'과 L_i가 동일한지 비교한다. 동일하면 $Z_i = h(RID_i \| SK)$을 계산하여 서버에 전송하고, 그렇지 않으면 세션을 종료한다.

$$D_i' = G_1 - C_1'$$
$$L_i' = h(RID_i \| h(D_1') \| W \| T_2)$$

$$SK = r_i D_1' = r_i r_j P$$

4.서버 S는 $Z_i' = h(RID_i \| SK)$을 계산하여 Z_i와 동일한지 비교하여 사용자를 인증한다.

2.3 Password change phase

1.사용자는 ID_i, PW_i, T_i을 입력하여 다음의 $F_i' = h(T_i) ? = F_i$, $A_i' = h(PW_i \| h(F_i')) ? = A_i$, $RID_i' = h(ID_i \| h(F_i')) ? = RID_i$을 검증한다. 만약 입력한 파라미터들이 일치하면, 사용자는 새로운 패스워드 PW_i^{new}을 선택하여 $A_i^{new} = h(PW_i^{new} \| h(F_i^*))$, $B_i^{new} = h(RID_i \| A_i^{new}) \oplus W$를 계산한다. 그런 다음 A_i와 B_i를 새로운 값들로 업데이트한다.

III. Problem of Related Scheme

본 장에서는 본 논문에서 분석한 인증 스킴[11]에 대한 문제들을 제시한다. 분석 결과 이 인증 스킴은 내부자 공격과 스마트카드 분실 공격에 안전하지 않고, 이로 인한 패스워드/ID 추측 공격과 세션키 노출 공격 등 다양한 공격에 안전하지 않다.

1. Security analysis

3.1 Privileged insider attack

인증 스킴[11]에서 A_i 값은 $h(PW_i \| h(F_i))$로 계산하기 때문에 내부 공격자가 $\{RID_i, A_i, F_i\}$를 획득할 경우, A_i와 F_i을 이용하여 $A_i ? = h(PW_i \| h(F_i))$의 값이 동일해질 때까지 반복하면 낮은 엔트로피의 패스워드를 계산해낼 수 있다. 또한 F_i와 RID_i를 이용하여 $RID_i ? = h(ID_i' \| h(F_i))$의 값이 동일해질 때까지 반복하면 사용자의 ID 추측 공격에 성공할 수 있다. 그러므로 Hwang et al.의 인증 스킴은 내부자 공격에 안전하지 않다.

3.2 Stolen smart-card attack

공격자가 스마트카드를 손에 넣었다고 가정할 경우, 스마트카드의 A_i와 $h(F_i)$는 카드에 저장된 값이므로 공격자는 식 $A_i ? = h(PW_i' \| h(F_i))$이 동일해질 때까지 반복하여 패스워드 추측 공격에 성공할 수 있다. 사용자의 ID 추측 공격은 RID_i을 $h(ID_i \| h(F_i))$로 대체하고, 카드의 값들 중 A_i, B_i, $h(F_i)$을 이용하여 $W' ? = h(h(ID_i' \| h(F_i)) \| A_i) \oplus B_i$을 계산한다. 계산해 낸 ID_i' 값의 정확성은 카드의 $h(W)$을 사용하여 앞에서 계산한 식을 해시함수로 연산한 후 $h(W') = h(h(ID_i' \| h(F_i) \| A_i) \oplus B_i)$을 비교하면 된다. W'와 W은 동일한 값이고, 공격자는 W의 값을 모르기 때문에 W'을 사용하여 계산 가능하다.

3.3 Session key disclosure attack

스마트카드 분실 공격에 성공한 공격자는 W'과 전송 메시지 C_2을 $r_i' = C_2 \oplus W$ 와 같이 계산하여 난수 r_i'을 계산해 낼 수 있고, 이 값과 G_1, T_2를 이용하여 세션키 SK'을 다음과 같이 계산해 낼 수 있다.

$$C_1' = r_i' P, \quad D_i' = G_1 - C_1'$$

$$SK' = r_i' D_1' = r_i' r_j P$$

공격자는 RID_i와 SK'을 알고 있으므로 서버에 대한 응답 메시지 $Z_i' = h(RID_i \| SK')$을 계산할 수 있다. 그러므로 인증 스킴[11]은 세션키 공격에 안전하지 않다.

3.4 User untraceability attack

본 논문에서 인증 스킴[3], [10], [11]을 분석한 결과, 이 인증 스킴들은 모두 로그인 요청에서 CID_i를 서버에 전송하고, 서버로부터 CID_i'을 응답으로 받아서 기존의 CID_i를 CID_i'로 대체하여 스마트카드에 저장한다. 그러므로 이전 세션에서 받은 CID_i'은 내용 변경 없이 다음 세션의 CID_i를 그대로 사용함으로, 공격자가 연속된 임의 세션들을 도청할 경우, 사용자의 정확한 ID_i을 모른다 할지라도 임의의 동일한 사용자라는 것을 알 수 있다. 그러므로 인증 스킴[11]은 안전한 추적 불가능성을 제공하지 않는다.

IV. The Enhanced Authentication Scheme

본 논문에서는 내부자 공격과 스마트카드 분실 공격으로 인하여 패스워드 추측 공격, ID 추측 공격, 세션키 노출 공격, 그리고 사용자 추적불가능성 등의 문제가 있는 인증 스킴[11]을 개선한 새로운 인증 스킴을 제안한다.

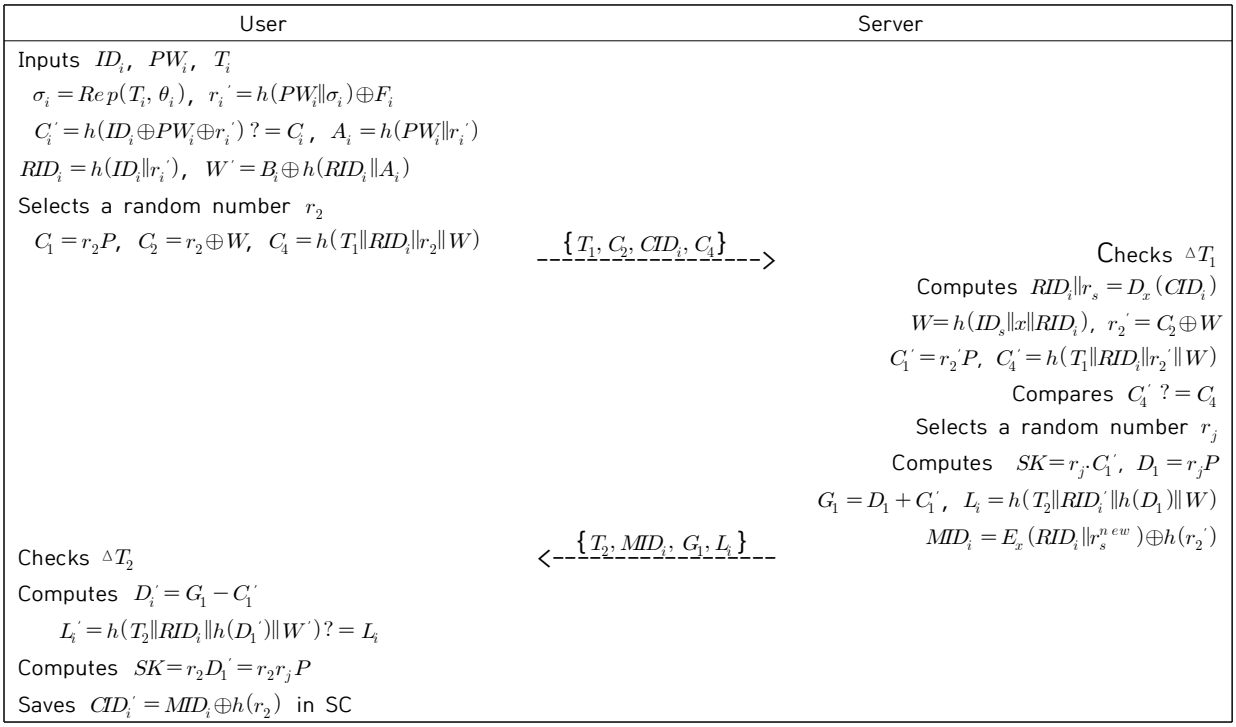

Fig. 2. The Proposed Authentication Scheme

4.1 Registration phase

1.사용자는 자신의 ID_i와 패스워드 PW_i을 선택한 후, 자신의 지문정보 T_i를 입력한다.

2.사용자는 $Gen(T_i) = (\sigma_i, \theta_i)$를 계산한 후 난수 r_i를 생성하여 $RID_i = h(ID_i \| r_i)$와 $A_i = h(PW_i \| r_i)$을 계산하여 안전한 채널을 통해 서버에게 보낸다.

3.서버 S는 RID_i의 타당성을 검증하여, 그 값이 타당할 경우 $W = h(ID_s \| x \| RID_i)$, $B_i = h(RID_i \| A_i) \oplus W$를 계산하고, 난수 r_s를 선택하여 자신의 비밀키 x로 $CID_i = E_x(RID_i \| r_s)$을 계산한다.

4.서버 S는 스마트카드에 $B_i, CID_i, h()$을 저장하여 안전한 채널을 통하여 사용자에게 보낸다.

5.사용자는 $F_i = h(PW_i \| \sigma_i) \oplus r_i$, $C_i = h(ID_i \oplus PW_i \oplus r_i)$을 계산하여 스마트카드에 저장한다. 스마트카드에는 최종적으로 $\{B_i, C_i, F_i, CID_i, h()\}$가 저장된다.

4.2 Login and authentication phase

1.사용자 ID_i, PW_i, T_i을 입력하여, 카드에 저장된 F_i로부터 난수 r_i'을 계산해 낸 후, 카드의 소유자 검증 과정을 진행한다.

$$\sigma_i = Rep(T_i, \theta_i),\ r_i' = h(PW_i \| \sigma_i) \oplus F_i$$

$$C_i' = h(ID_i \oplus PW_i \oplus r_i) ? = C_i$$

C_i'과 C_i가 동일하면 사용자는 $A_i' = h(PW_i \| r_i')$, $RID_i' = h(ID_i \| r_i')$을 계산하고, 난수 r_2와 타임스탬프 T_1을 생성하여 다음 값들을 계산한 후, $\{T_1, C_2, CID_i, C_4\}$를 서버에 전송한다.

$$W' = B_i \oplus h(RID_i \| A_i),\ C_1 = r_i P,$$

$$C_2 = r_i \oplus W,\ C_4 = h(T_1 \| RID_i \| r_i \| W)$$

2.서버는 타임스탬프 T_1의 타당성을 검증하여 타당하면 자신의 비밀키 x로 CID_i을 복호화하여 RID_i를 알아낸 후 다음을 계산한다.

$$W = h(ID_s \| x \| RID_i),\ r_2' = C_2 \oplus W$$

$$C_1' = r_2' P,\ C_4' = h(T_1 \| RID_i \| r_2' \| W)$$

서버는 C_4'과 C_4가 동일한지 비교하여 동일하면 난수 r_j, r_s^{new}와 타임스탬프 T_2을 생성하여, 다음 값들을 계산한 후 사용자에게 $\{T_2, MID_i, G_1, L_i\}$를 전송한다.

$$SK = r_j C_1',\ D_1 = r_j P,\ G_1 = D_1 + C_1'$$

$$L_i = h(T_2 \| RID_i' \| h(D_1) \| W)$$

$$MID_i = E_x(RID_i \| r_s^{new}) \oplus h(r_2')$$

3.사용자는 타임스탬프 T_2의 타당성을 검증하여 타당하면 L_i'과 L_i가 동일한지 비교하고, 동일할 경우 세

션키 SK와 $CID_i^{'}$을 계산하여, $CID_i^{'}$은 카드에 저장한다.

$$D_i^{'} = G_1 - C_1^{'}, L_i^{'} = h(RID_i \| h(D_1^{'}) \| W \| T_2)$$

$$SK = r_i D_1^{'}, \ CID_i^{'} = MID_i \oplus h(r_2)$$

4.2 Password change phase

1.사용자는 ID_i, PW_i, T_i를 입력하여, 다음 계산을 진행한다. 만약 $C_i^{'}$과 C_i가 동일하면 $A_i^{'} = h(PW_i \| r_i^{'})$, $RID_i^{'} = h(ID_i \| r_i^{'})$, $W^{'} = B_i \oplus h(RID_i \| A_i)$을 계산하고, 그렇지 않으면 세션을 종료한다.

$$\sigma_i = Rep(T_i, \theta_i), \ r_i^{'} = h(PW_i \| \sigma_i) \oplus F_i$$

$$C_i^{'} = h(ID_i \oplus PW_i \oplus r_i) \, ? = C_i$$

2.사용자는 새로운 패스워드 PW_i^{new}를 선택하여 다음 값들을 계산한 후 기존 값들을 F_i^{new}, B_i^{new}, C_i^{new}로 업데이트한다.

$$F_i^{new} = h(PW_i^{new} \| \sigma_i) \oplus r_i^{'}$$

$$C_i^{new} = h(ID_i \oplus PW_i^{new} \oplus r_i^{'})$$

$$A_i^{new} = h(PW_i^{new} \| r_i^{'})$$

$$B_i^{new} = h(RID_i \| A_i^{new}) \oplus W$$

V. Analysis of The Proposed Scheme

1. Security and Design Analysis

본 장에서는 제안한 인증 스킴의 안전성과 설계상의 문제를 분석한다. Table 1은 제안 인증 스킴과 관련된 주요 인증 스킴들에 대한 분석 결과로, 공격에 대한 저항성이 있는 것은 √ 기호로 표기하고, 그렇지 않은 것은 - 기호로 표기한다.

Privileged insider attack

서버의 내부 공격자가 A_i와 RID_i의 획득에 성공할 경우, 이 값들로부터 사용자의 패스워드와 ID_i를 계산해내려면 난수 r_i을 알아야 한다. 그러나 공격자는 높은 엔트로피의 난수와 단방향 해시함수의 안전성 때문에 r_i을 알아내기 힘들어, 제안 인증 스킴은 내부자공격에 안전하다.

Stolen smart-card attack

제안 인증 스킴의 스마트카드에는 B_i, C_i, F_i, $CID_i^{'}$, $h()$가 저장되어 있고, C_i로부터 패스워드를 알아내려면 난수 r_i을 알아야 하고, F_i로부터 난수 r_i을 알려면 사용자의 생체정보를 알아야 한다. 그러나 해시연산한 높은 엔트로피의 생체정보는 알아내기 어렵다. 또한 B_i로부터 필요한 값을 알아내려면 RID_i, W, A_i가 필요하나 이 값들은 스마트카드에 저장하지 않는다. 그러므로 제안 인증 스킴은 패스워드 추측 공격과 ID 추측 공격에 안전하다.

User untraceability attack

제안 인증 스킴은 로그인 요청 시, $CID_i^{'} = E_x(RID_i \| r_s)$을 전송하고, 서버는 $MID_i = CID_i^{'} \oplus h(r_2)$을 사용자에게 전송한다. CID_i와 $CID_i^{'}$은 서로 다른 난수를 사용한 값이고, MID_i로부터 $CID_i^{'}$을 알기 위해서는 사용자가 생성한 난수 r_2을 알아야 한다. 그러나 제안 인증 스킴은 내부자 공격이나 스마트카드 분실 공격 등을 통해서 난수 r_2을 계산해 낼 수 없다.

Replay attack

제안 인증 스킴은 전송 메시지에 타임스탬프 T_1, T_2을 사용하여 타임스탬프의 임계 차이를 먼저 검증한 후에 다음 과정을 진행한다. 그러므로 제안 인증 스킴은 재전송 공격에 안전하다.

Table 1. Comparison of Security Functions and Design Defects

	Mishra[6]	Xu[3]	Amin[2]	Liu[10]	Hwang[11]	Proposed
User anonymity	-	√	√	√	√	√
User impersonation attack	-	-	-	-	-	√
Server spoofing attack	-	√	√	√	√	√
Stolen smart-card attack	-	-	-	-	-	√
Privileged insider attack	√	√	-	-	-	√
Offline password guessing attack	√	-	-	-	-	√
Replay attack	√	√	-	√	√	√
Known-key attack	-	√	√	√	√	√
Session key attack	-	√	-	-	-	√
User untraceability attack	√	√	-	-	-	√
Design defects	-	-	-	-	-	√

Known-key attack

제안 인증 스킴의 세션키는 매 세션마다 다른 난수를 사용하여 계산하기 때문에, 공격자가 임의의 세션키 값을 안다고 할지라도 이 값을 사용하여 이전의 다른 세션키를 계산해내기 어렵다. 또한, 안전한 해시함수로 연산하였고, 정당한 사용자와 서버 외에는 이 값을 모르기 때문에 세션키 노출 공격에도 안전하다.

Improved design defect

제안 인증 스킴은 등록 단계에서 사용자의 RID_i 형식을 검토하여 동일한 사용자의 여부를 먼저 검토한다. 그러므로 제안 인증 스킴은 사용자의 중복성 문제를 해결하고, 이로 인하여 발생할 수 있는 의료과실 문제를 개선하였다.

2. Performance Comparison

Table 2는 제안 인증 스킴과 관련된 ECC 인증 스킴들에 대한 계산복잡도를 비교 분석한 것으로, 로그인 단계와 인증 단계에서의 사용자와 서버 측의 계산복잡도를 분석한 것이다. T_h, T_{emul}, T_{sym}, 그리고 T_m은 각각 단방향 해시함수, ECC 곱셈 연산, 대칭키의 암·복호화 연산, 그리고 모듈러 지수 연산을 나타낸다. 각 연산의 실행시간은 0.00032s, 0.0171s, 0.0056s, 0.0192s이고, 퍼지 추출 연산인 T_f는 $T_f \approx T_{emul}$로 0.0171s이다[12][13].

Fig. 3은 로그인과 인증 단계의 사용자 측과 서버 측에서의 각각의 실행시간, 그리고 각 측에서의 전체 실행시간을 나타낸 것으로 제안 인증 스킴은 사용자 인증을 위한 퍼지 연산을 제외하면 Liu et al.의 인증 스킴과 동일한 실행시간을 나타낸다. Hwang et al.의 인증 스킴에 비해서는 단 한 번의 해시연산의 증가로 제안 인증 스킴이 매우 양호한 복잡도인 것을 알 수 있다. Fig. 5를 보면 ECC을 이용한 관련 인증 스킴들이 주로 0.1초 대의 실행시간이 소요됨을 볼 수 있으며, 퍼지 추출 연산을 포함한 제안 인증 스킴도 0.1초 대의 실행시간인 것을 볼 수 있다.

Table 2. Computation Complexity Analysis

	User	Server
Mishra[6]	$8T_h$	$5T_h+2T_{sym}$
Xu[3]	$6T_h+3T_{emul}$	$6T_h+3T_{emul}$
Amin[2]	$7T_h+2T_{emul}$	$5T_h+3T_{emul}+2T_{sym}$
Liu[10]	$8T_h+2T_{emul}$	$5T_h+3T_{emul}+2T_{sym}$
Hwang[11]	$9T_h+2T_{emul}$	$4T_h+3T_{emul}+2T_{sym}$
The Proposed	$9T_h+2T_{emul}+1T_f$	$5T_h+3T_{emul}+2T_{sym}$

Fig. 3. Comparison of Rum Times

VI. Conclusions

본 논문에서 인증 스킴[11]을 분석한 결과, 내부자 공격, 스마트카드 분실 공격으로 인한 패스워드/ID 추측 공격, 세션 키 노출 공격, 사용자 추적불가능성 등의 문제가 있었다. 또한, 인증 스킴[11]은 등록 단계에서 사용자의 식별자를 검증하지 않아, 제안 인증 스킴에서는 식별자 구별 문제를 개선하였고, 안전성 문제에서도 내부자 공격이나 스마트카드 분실 공격, 오프라인 패스워드 추측 공격, 세션 키 노출 공격, 사용자 추적불가능성, 재생 공격 등에 안전한 것으로 분석되었다. 또한, 계산복잡도에서도 퍼지 추출 연산을 제외하면 기존의 인증 스킴[10]과 동일한 복잡도를 나타내었고, 인증 스킴[11]과 비교해서는 단 한 번의 해시 연산이 증가하였다. 그러므로 본 논문에서 제안한 인증 스킴은 안전성과 실용성을 함께 갖춘 TMIS 인증 스킴이라고 할 수 있다.

REFERENCES

[1] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in telecare medicine information systems," Journal of Network and Computer Applications, Vol. 87, pp. 1-19, June 2017. DOI: 10.1016/j.jnca.2017.03.003

[2] R. Amin and G. P. Biswas, "A secure three-factor user authentication and key agreement protocol for tmis with user anonymity," Journal of Medical Systems, Vol. 39, No. 78, pp. 1-19, June 2015. DOI: 10.1007/s10916-015-0258-7

[3] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ecc for telecare medicine information systems," Journal of Medical Systems, Vol. 38, pp. 1-7, 2014. DOI: 10.1007/s10916-013-9994-8

[4] T. Y. Wu, L. Yang, Z. Lee, C. M. Chen, J. S. Pan, and S. H. Islam, "Improved ECC-based three-factor multiserver

authentication scheme," Security and Communication Networks, Vol. 2021, pp. 1-14, Jan. 2021, DOI: 10.1155/2021/6627956

[5] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, "Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System," in IEEE Access, Vol. 10, pp. 11511-11526, 2022, DOI: 10.1109/ACCESS.2022.3145959

[6] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. Khan, "Cryptanalysis and improvement of Yan et al.'s biometric-based authentication scheme for telecare medicine information systems," Journal of Medical Systems, Vol. 38, pp. 1-12, 2014. DOI: 10.1007/s10916-014-0024-2

[7] R. Amin and G. P. Biswas, "An improved RSA based user authentication and session key agreement protocol usable in TMIS," Journal of Medical Systems, Vol. 39, No. 8, pp. 1-14, 2015. DOI: 10.1007/s10916-015-0262-y

[8] D. Giri, T. Maitra, R. Amin, and P. D. Srivastava, "An Efficient and Robust RSA-Based Remote User Authentication for Telecare Medical Information Systems," Journal of Medical Systems, Vol. 39, Issue. 145, pp. 1-9, Jan. 2015. DOI: 10.1007/s10916-014-0145-7

[9] Kwonkim, "Cryptanalysis and Improvement of RSA-based Authentication Scheme for Telecare Medical Information Systems," Journal of Korean Society of Computer Information, Vol. 25, No. 2, pp. 93-103, Feb. 2020. DOI: 10.9708/jksci.2020.25.02.093

[10] W. R. Liu, X. He, Z. Y. Ji, "Security analysis and enhancements of a user authentication scheme," International Journal of Network Security, Vol. 23, No. 5, pp. 895-903, Sept. 2021. DOI: 10.6633/IJNS.202109 23(5).17

[11] M. S. Hwang, H. W. Li, and C. Y. Yang, "An Improved of Enhancements of a User Authentication Scheme," International Journal of Network Security, Vol. 25, No. 3, pp. 508-514, May 2023. DOI: 10.6633/IJNS.202305 25(3).15)

[12] D. He, N. Kumar, J. H., Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, pp. 30–37. Feb. 2014. DOI: 10.1109/TCE.2014.6780922.

[13] F. Wang, G. Xu, and G. Xu., "A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map," IEEE Access, Vol. 7, pp. 101596-101608, 2019. DOI: 10.1109/ACCESS.2019.2930542

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.