Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

# A Study on Design of Robust Remote User Authentication Scheme with Enhanced for Anonymity and Confidentiality

**Kwang-Cheul Shin***

*Division of Industrial Management Engineering, Sungkyul University*

## ABSTRACT

Until recently, a variety of biometric authentication schemes using smart cards have been proposed to enhance the security of remote authentication systems. Telecare medical information systems(TMIS) provides convenient health care services for user(patients) in order to save the patients' time and expense. Therefore, the system is important for secure mutual authentication between the user and the healthcare server, and sensitive medical information should not be exposed to third parties. In this paper, We analyzed the vulnerability of Lu et al.'s authentication protocol using elliptic curve encryption. And We propose a scheme to improve this paper. Lu et al.'s scheme has developed a biometric and smart card-based remote authentication scheme that complements the vulnerability to user spoofing attacks in the Arshad et al.'s scheme. However, result of analysis of their schemes reveals the confidentiality of the user's anonymity and login message by eavesdropping on the login message. Therefore, it is vulnerable to legitimate spoofing attacks of users and servers. In the proposed paper, we redesigned the security of server secret key and secret number. Therefore, we proposal suggests anonymity, confidentiality of messages, and a secure user authentication scheme for multiple attacks by legitimate users and servers. We will contribute to providing strong security and implementation efficiency when designing future authentication schemes.



**KEYWORDS:** Biometrics, Mutual authentication, Impersonation attack, Session key agreement, Smart card

**ARTICLE INFO:** Received 24 November 2018, Revised 2 January 2019, Accepted 8 February 2019.

*Corresponding author is with the Department of Industrial Management Engineering, Sungkyul University, 53 Sungkyul University-ro Manan-gu, Anyang-si, Gyeonggi-do, 14097, KOREA.

*E-mail address*: skcskc12@sungkyul.ac.kr

## 1. 서 론

원격 의료정보시스템(TMIS:Telecare Medical Information System)은 인터넷을 통해 의사가 환자에게 진단 및 치료를 효율적이고 편리하게 해주는 시스템으로 데이터 전송의 보안과 무결성을 보장하기 위해서는 서버와 사용자간 인증 메커니즘이 반드시 필요하다[1-5]. 그동안 민감한 의료정보는 데이터보안과 개인정보가 중요하기 때문에 다중서버 TMIS에 대한 새로운 생체인식기반의 인증 및 키 동의에 대한 연구가 꾸준히 진행되었다[6-11]. 2014년 Chuang et al.'s[12]는 다중서버구조에서 익명의 생체인식기반 인증스킴을 제시했지만 Mishra et al.'s[[13]에 의해 서버스푸핑과 스마트카드 도난 및 위장(impersonation)공격에 안전하지 못함이 증명되었다. 2015년 Baruah et al.'s[14]은 Mishra et al.'s 스킴이 위장공격과 스마트카드 도난공격에 취약하다고 분석하고 개선된 스킴을 제안했으나 완전한 해결방안을 제시하지 못하고 있음을 K.C. Shin은 분석하였다[17].

Arshad et al.'s[15]은 서비스 거부(denial of service)공격 및 재생공격에 안전한 타원형 곡선 암호화 시스템 (ECC)을 기반으로 한 스킴을 제시했다. 그러나 오프라인 패스워드 추측공격에 취약함으로 파생되는 합법적 제3자에 의해 식별자가 노출됨으로써 익명의 노출과 위장공격에 취약하였다.

본 논문에서 Lu et al.'s scheme[16]이 환자(user's)들의 익명성과 위장공격의 취약성, 그리고 합법적인 사용자가 시스템을 사용하는 모든 사용자들에 의해 안전하지 않음을 논리적으로 입증한다. 또한 제3자의 동시로그인 공격과 서버와 사용자간의 상호인증의 부적절함도 보이며 사용자를 기만하여 합법적인 서버로 위장 할 수 있음을 보여준다. 이어서 Lu et al.'s 스킴의 취약점을 해결하기 위해 향상된 생체인식 기반 인증체계를 제안한다.

2장에서 Lu et al.'s 스킴을 검토 및 분석하고 3장에서 익명성과 기밀성을 향상시킨 스킴을 제안하였으며 4장에서 제안스킴에 대한 분석과 토의를 하였다.

## 2. Review of Lu et al.'s Scheme

Arshad et al.'s 스킴은 익명성을 위한 3요소 인증과 키 동의 원격의료정보시스템을 제안하였으나 Lu et al.'s은 Arshad et al.'s의 스킴에서 위장공격과 전방향 보안공격에 취약성을 발견하고 타원곡선 암호시스템을 기반으로 한 생체정보 인증과 키 동의 스킴을 제안하였다. Lu et al.'s 스킴은 등록단계, 로그인단계, 인증단계, 패스워드변경 단계의 4단계로 구성되며 패스워드변경 단계를 제외한 각 단계별로 간략하게 리뷰한다. 본 논문에서 사용되는 기호는 <표 1>과 같다.

표 1. 약어표기 및 정의
Table 1. : Notations used in this paper

| 기호표기 | 정의 |
|---|---|
| U, S | 사용자(환자), 서버 |
| $ID_i$, $PW_i$, $B_i$ | 식별자, 패스워드, 생체정보 |
| H() | 생체기반 해시함수 |
| h1(), h2() | 해시함수 h1 :$\{0,1\}^*$->$\{0,1\}^n$, 해시함수 h2 :$\{0,1\}^*$->$Z_p^*$ |
| x | 서버의 비밀키 |
| y | 비밀의 수 |
| ⊕, ‖ | Exclusive-or 연산, 연접 |
| E[ ], D[ ] | 암호화함수, 복호화함수 |

### 2.1 등록 단계

등록단계에서는 새로운 사용자(환자) Ui는 개인용 스마트카드를 발급받기 위해 아래와 같은 절차로 서버 Sj에게 등록한다.

(1) 사용자 Ui는 자신의 식별자 IDi, 패스워드 PWi를 선택하고 생체인식정보 Bi를 입력한다.

(2) 사용자는 MPi= PWi⊕H(Bi)를 계산하고 [IDi, MPi]를 서버에 등록을 위해 안전한 채널을 통해 서버 Sj로 전송한다.

(3) 등록 요구를 수신한 Sj는 개인키 x를 사용하여 AIDi=IDi⊕h2(x)와 Vi=h1(IDi‖MPi)을 계산하고 [AIDi, Vi, h1(), h2(), H()]를 스마트카드(SCi)에 저장하여 Ui에게 안전한 채널로 전송한다.

## 2.2 로그인 단계

로그인 단계에서는 사용자 Ui와 서버 Sj간에 상호인증과 세션 키 동의를 위해 다음의 과정을 수행한다.

(1) Ui는 스마트카드 SCi를 리더기에 삽입하고 아이디 IDi, 패스워드 PWi 및 생체인식정보 Bi를 입력하면 SCi는 h1(IDi‖PWi⊕H(Bi))=Vi가 일치하는지 여부를 확인한다.

(2) 일치하지 않으면 거절되고 일치하면 SCi는 랜덤의 수 du를 선택하고 cyclic group의 duP를 생성한 다음 K=h1(IDi‖IDi⊕AIDi), M1=K⊕duP, M2=h1(IDi‖duP‖T1)를 계산하여 로그인 메시지 [M1, M2, AIDi, T1]를 Sj로 전송한다.

## 2.3 인증 단계

서버 Sj는 인증 및 세션키 동의를 위해 다음 절차를 수행한다.

(1) [M1, M2, AIDi, T1]을 수신 한 후 Sj에서 생성한 타임스탬프 Tc를 이용하여 |Tc-T1|<△T인지 여부를 검사한다. 델타 △T는 서버가 로그인 메시지를 수신했을 때의 타임스탬프이며 로그인 메시지 전송시간을 고려한 최소한의 인증시간이다. 조건이 만족하면 Sj는 IDi를 추출하기 위해 자신의 개인키 x를 사용하여 IDi를 추출(IDi=AIDi⊕h2(x))하고 duP=h1(IDi‖h2(x))⊕M1를 계산하여 M'2=(h1(IDi‖duP‖T1))과 M2의 일치여부를 비교한다.

(2) M2=M'2가 일치하지 않으면 거절되고 일치하면 Sj는 랜덤의 수 ds와 타임스탬프 T2를 생성하고 M3=K⊕dsP, SK=ds(duP), M4=h1(K‖duP‖SK‖T2)을 계산하여 [M3, M4, T2]를 Ui로 전송한다.

(3) [M3, M4, T2]를 수신하면 SCi는 T2의 유효성(|Tc-T2|<△T)을 검사하여 만족하면 dsP= M3⊕K, SK=du(dsP), M'4=h1(K‖duP‖SK‖T2)을 계산한 후 수신한 M4와 M'4를 비교한다.

(4) M4와 M'4가 일치하면 스마트카드 SCi는 T3을 생성하여 M5=h1(K‖dsP‖SK‖T3)을 계산하고 [M5, T3]을 Sj에 전송한다.

(5) Sj는 T3의 유효성(|Tc-T3|<△T)를 확인한 다음 만족하면 M'5=h1(K‖dsP‖SK‖T3)를 계산하여 수신한 M5와 일치여부를 검증한다. 일치하면 Sj는 Ui를 인증하고 SK를 세션 키로 승인한다.

## 2.4 Lu et al.'s 스킴분석

Lu et al'.s의 주장은 합법적 제3자가 전체 통신 채널을 완전히 제어하여 메시지를 도청, 수정, 삽입을 할 수 있다고 가정해도 익명성과 위장공격, 상호인증 등에 안전하다고 주장했다. 그러나 Lu et al'.s의 주장이 다름을 아래와 같이 증명한다.

### 2.4.1 등록과정에서의 오류

모든 사용자(IDn)들은 자신의 식별자(IDx)와 MPx을 서버 Sj에게 전송하면 서버는 Vx=h1(IDx‖MPx)과 AIDx=IDx⊕h2(x)을 계산하여 스마트카드에 저장 [Vx, AIDx]하고 Un에게 전송한다. 이 때 모든 합법적 사용자들은 해시값 h2(x)를 공통으로 보유

(h2(x)=AIDn⊕IDn)하게 되는 오류가 발생한다.

#### 2.4.2 식별자(ID)의 노출

모든 합법적 사용자들은 2.4.1에서 h2(x)를 보유하게 됨으로써 합법적 사용자 Ui가 로그인을 위해 AIDi를 비보호채널로 서버 Sj로 전송할 때 합법적인 제3자(Uj)는 로그인 메시지를 도청하여 Ui의 식별자(IDi)를 계산( IDi=AIDi⊕h2(x))할 수 있다.

#### 2.4.3 식별자(ID)의 검증부재

서버에서 식별자 검증부재로 로그인을 요청하는 사용자가 누구인지에 대한 식별자의 적법성 여부를 검증하지 않는다. 이러한 식별자의 검증부재는 합법적 제3자의 식별자가 로그인 요청을 했을 때 서버는 정해진 메커니즘을 수행하고 사용자 또한 합법적인지의 검증이 확인되지 않음으로써 위장공격과 동시로그인공격에 취약하다.

위 3가지의 오류 및 식별자의 노출, 검증부재를 가지고 어떤 취약점이 있는지 시나리오를 통해 3장에서 분석한다.

## 3. Lu et al.'s 스킴의 취약성

### 3.1 로그인 메시지 도청

합법적 사용자 Ui의 로긴 메시지[M1, M2, AIDi, T1]가 전송되는 과정에서 다른 합법적 사용자 Uj, Uk,....등에 의해 도청되었을 때 기밀성, 인증, 무결성을 위반하는 중대한 이유는 다음과 같다.

(1) 모든 합법적 사용자들은 AID=ID⊕h2(x)로부터 h2(x)를 알고 있다.

(2) 모든 사용자의 로그인 메시지 [M1, M2, AID, T1]를 합법적 제3자는 도청한다.

서버 S는 등록하는 사용자들에게 일괄적으로 부여하여 모든 합법적 사용자는 공통 파라미터 h2(x)로부터 사용자의 식별자(IDi=AIDi⊕h2(x))를 쉽게 구할 수 있어 익명성이 보호되지 않는다. 합법적 제3자 Uj는 사용자 Ui의 K를 쉽게 계산할 수 있으므로 기밀성에 취약하다. Uj는 도청한 AIDi와 2.4.2에서 알아낸 IDi로 다음과 같이 K'=h1(IDi ‖ IDi⊕AIDi)를 계산한다. 그 다음 Uj는 Ui의 M1을 이용하여 랜덤의 수 duP를 알아내고 duP와 K'를 이용하여 M'1을 계산할 수 있어서 세션키(SK)생성에 중요한 파라미터 duP가 노출되고 있다.

### 3.2 사용자 위장공격

3.1절에서와 같이 합법적 다른 사용자들은 사용자 Ui의 로긴 메시지를 도청하여 [IDi, K, M1, M2] 모두 알아냈다. 합법적 다른 사용자 Uj는 사용자 Ui로 위장 공격하는 시나리오는 다음과 같다.

(1) Ui는 로그인 메시지 [M1, M2, AIDi, T1]을 서버로 전송한다. Uj는 메시지를 가로챈다.

(2) Uj는 랜덤의 수 d'u, T1'을 생성하여 로긴메시지 [M'1, M'2, AIDi, T1']을 계산하고 서버 Sj로 전송한다.

[M'1, M'2, AIDi, T1']을 수신한 Sj는 타임스탬프 | Tc-T1' | < △T를 검증하여 유효하면 전송 주체인 사용자 아이디(IDi=AIDi⊕h2(x))를 알아낸다.

(3) Sj는 랜덤의 수 ds와 타임스탬프 T2를 생성하여 아래를 계산하고 Uj에게 [M3, M4, T2]를 전송한다.

- K'=h1(IDi ‖ h2(x))
- M'1=K'⊕d'uP)
- M'2=h1(IDi ‖ T1' ‖ d'up)
- M3=h1(IDi ‖ h2(x)⊕dsP)
- SK=ds(duP)
- M4=h1(K ‖ T2 ‖ SK ‖ duP)

(4) [M3, M4, T2]를 수신한 Uj는 아래를 계산하고 서버 Sj에게 [M5, T3]를 전송한다.

- dsP=K⊕M3
- SK=dsP(d'u)
- M4=h1(K ‖ T2 ‖ SK ‖ duP)=?M'4
- M5=h1(K ‖ T3 ‖ SK ‖ dsP)

(5) Sj는 T3의 유효성을 체크한 다음 만족하면 M'5를 계산하여 Uj를 Ui로 인증하고 세션 키 SK를 승인한다.

이와 같이 제3자인 Uj는 합법적 사용자 Ui로 위장할 수 있다.

### 3.3 서버 위장공격

Lu et al'.s 스킴은 합법적인 사용자가 합법적인 서버로 위장 할 수 있다. 합법적인 제3자 Uj가 TMIS 서버로 위장하는 시나리오는 다음과 같다.

(1) Ui가 로그인 및 인증 과정을 수행하기 위해 [M1, M2, AIDi, T1]을 Sj로 전송하면 Uj는 로그인 메시지를 가로 챈다.

(2) Uj는 h2(x)를 사용하여 3.2절의 (2)를 계산하여 Ui의 식별자 IDi를 알아내고 랜덤의 수 d's를 생성하여 아래 식을 계산하여 [M'3, M'4, T2]를 Ui로 전송한다.

- M'3 = h1(IDi ‖ h2(x))⊕d'sP,
- SK'=d's(duP),
- M'4 = h1 (K ‖ duP ‖ SK' ‖ T2)

(3) Ui는 타임스탬프 T2의 유효성을 확인하고 다음 식을 계산하여 메시지 M4를 검증한다.

- K ⊕ M'3 = d'sP,
- SK = du(d'sP),
- M'4 =? h1 (K ‖ duP ‖ SK ‖ T2)

Ui는 검증이 유효할 때 Uj를 합법적인 서버로 간주하여 세션키 SK를 승인한다.

### 3.4 상호인증

Lu et al'.s 스킴은 서버 Sj에서 타임스탬프 Tc를 이용하여 ∣Tc-T1∣<△T인지 여부와 M'2=(h1(IDi ‖ duP ‖ T1))=?M2를 검사함으로써 상호인증에 성공했다고 주장한다. 그러나 서버 Sj가 사용자 Ui의 식별은 AIDi와 자신의 개인키 x를 사용하여 메커니즘적으로 확인(IDi=AIDi⊕h2(x))할 뿐이지 사용자에 대한 적합성여부는 검사하지 않는다. 또한 서버 Sj의 인증결과 메시지 [M3, M4, T2]를 수신하였더라도 사용자는 합법적인 서버 Sj의 식별자를 확인할 수 없다.

## 4. 기밀성과 익명성을 위한 제안스킴

3절에서 Lu et al'.s 스킴의 문제는 서버의 개인키에 대한 정보가 누설되는 AIDi의 파라미터로 합법적인 제3의 사용자는 Lu et al'.s 스킴을 공격하는데 사용할 수 있는 h2(x)를 얻을 수 있다는 것이다. 이 절에서는 Lu et al'.s 스킴에 기반한 개선된 생체인식의 인증 및 키 동의 스킴을 제안한다.

### 4.1 등록 단계

<그림 1>과 같이 새로운 사용자 Ui는 서버 S에 등록하고 다음 단계를 통해 스마트카드(SCi)를 받는다.

(1) 사용자 Ui는 자신의 식별자 IDi, 패스워드 PWi를 선택하고 자신의 생체정보 Bi를 입력한다. SCi는 MPi=h(PWi⊕Bi)를 계산하고 [IDi, MPi]를 보안 채널을 통해 서버 Sj로 보낸다.

(2) 등록 요청을 수신한 Sj는 개인키 x, 비밀의 수 y를 이용하여 AIDi=h(IDi⊕h2(x)), Si=h(IDi⊕x)⊕MPi⊕h(y), Vi=MPi⊕h(AIDi), Ki=h(IDi⊕x)⊕h(x)를 계산하고 [Si, Vi, Ki, h()]를 SCi에 저장하여 Ui로 안전하게 보낸다.

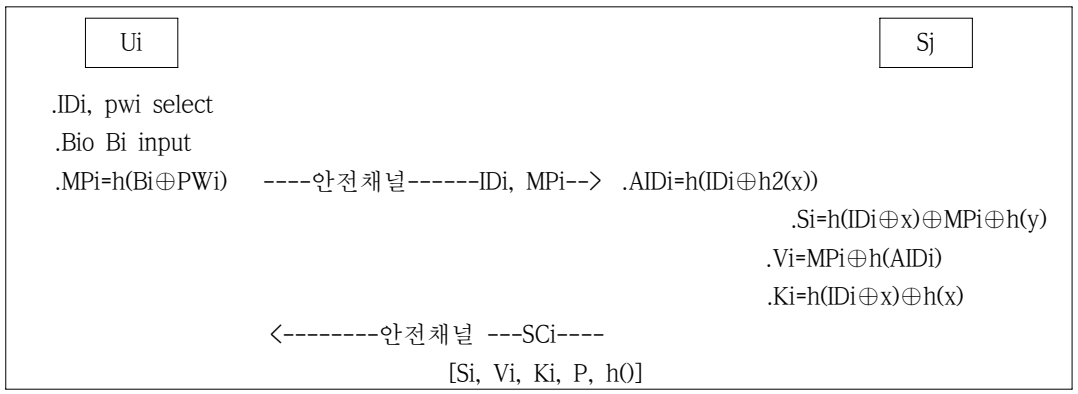


그림 1. 제안 등록단계
Figure 1. Registration phase of proposed scheme

### 4.2 로그인 단계

사용자 Ui와 서버 Sj는 인증과 세션 키 일치를 얻기 위해 <그림 2>의 단계를 실행한다.

(1) Ui는 스마트카드 SCi를 삽입하고, 자신의 식별자 IDi, 패스워드 PWi 및 생체정보 Bi를 입력한다.

(2) SCi는 Vi를 이용하여 h(AIDi)를 추출해 내고 SCi의 Vi와 비교하여 일치하면 스마트카드 소유자임을 검증하고 다음단계를 실행한다.

(3) SCi는 랜덤의 수 du와 타임스탬프 T1을 생성하여 로긴 메시지를 계산한다.

• M1=h(AIDi)⊕duP, M2=h(duP ‖ T1 ‖ IDi), M3=Si⊕MPi, R=M3⊕h(duP), K=Ki⊕h(duP),

L1=Ek[IDi, M1, M2]

(4) 사용자 Ui는 서버 Sj에게 로그 인 요청메시지 [R, T1, L1]을 전송한다.

### 4.3 인증 단계

인증 및 세션키 동의 단계에서는 수신한 로그인 요청 메시지를 이용하여 사용자 Ui에 대한 검증을 수행한다.

(1) 로그인 메시지 [R, T1, L1]를 수신한 서버 Sj는 타임스탬프 Ts를 생성하여 | Ts-T1 | < ΔT를 검증하고 유효하면 다음단계를 수행한다.

(2) 서버 Sj는 비밀키 x와 비밀넘버 y를 사용하여 K를 도출(K=R⊕h(x)⊕h(y))한다. 이어서 L을 디코드(Dk[Ek[L1]])하여 IDi, M1, M2을 추출해 낸다.

(3) 서버 Sj는 로긴 메시지 M1을 사용하여 duP(=h(AIDi⊕M1))를 추출해 내고 M'2를 계산(=h(IDi ‖ duP ‖ T1))하여 수신된 M2와 비교하여 일치하면 다음 단계를 수행한다.

(4) Sj는 위 (3)에서 M2와 계산한 M'2가 일치되면 검증자(verifier:IDi⊕duP⊕h(y))를 작성하고 한 세션 동안 만 사용되는 로그인 상태비트를 "1"로 변환한다.

디코드 된 값 L에서 전송한 사용자의 식별자 IDi를 확인할 수 있고 이 때 다중사용자의 로그인 공격(DoS)을 대비하여 임시저장소에 IDi, 검증값, 타임스탬프 T1, 상태비트를 일시 저장[표 2]한다. 세션이 끝나면 상태비트는 "0"으로 세팅한다. 즉 한 세션동안 동일한 ID 식별자로 동시에 다량의 메시지를 보낼 때 Sj는 세션을 거절한다.

(5) 서버 Sj는 비밀의 수 ds와 타임스탬프 T2를 생성하여 세션키 SKji=h(duP ‖ ds ‖ T1 ‖ T2)와 인증메시지 M4=dsP⊕h(duP), M5=h(SIDj ‖ dsP ‖ duP ‖ T2),

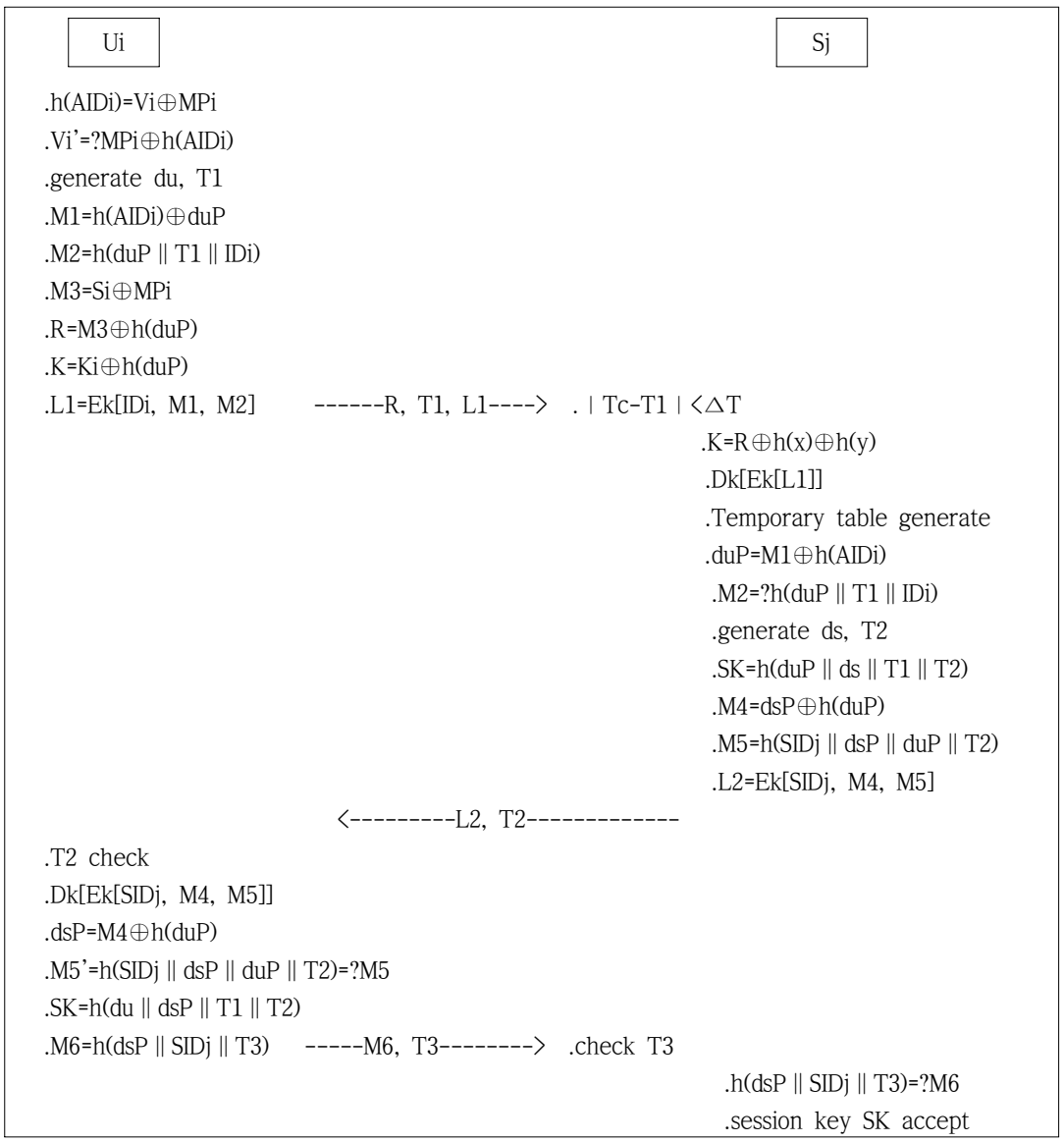


그림 2. 제안 로긴 및 인증단계
Figure 2. Login and authentication phase proposed scheme

L2=Ek[SIDj, M4, M5]를 계산한다.

(6) 서버 Sj는 사용자 Ui로 인증메시지 [L2, T2]를 전송한다.

(7) 사용자 Ui는 인증메시지를 수신하여 인증시간을 확인하고 L2를 디코드하여 다음을 계산한다.

- | Tc-T2 | ≤△T
- Dk[Ek[SIDj, M4, M5]]
- dsP=M4⊕h(duP)
- M' 5=h(SIDj || dsP || duP || T2)=?M5
- SKij=h(du || dsP || T1 || T2)

표 2. 임시테이블
Table 2. Temporary Table

| 사용자 아이디 | 타임 스탬프 | 검증값 | 상태 비트 |
|---|---|---|---|
| Ui | Ti | IDi⊕duPi⊕h(y) | 0/1 |
| Uj | Tj | IDj⊕duPj⊕h(y) | 0/1 |
| : | : | : | : |

(8) 사용자 Ui는 응답메시지 작성을 위해 타임스탬프 T3를 생성하여 M6=h(dsP ‖ SIDj ‖ T3)을 계산하고 M6를 서버 Sj로 전송한다.

(9) Sj는 T3의 신선성 ( | Tc-T3 | < △T)을 확인한 다음 조건이 만족하면 아래와 같이 M6을 계산하고 M'6와 비교하여 일치(M6=h(dsP ‖ SIDj ‖ T3)=?M6)하면 Sj는 Ui를 인증하고 SK를 세션 키로 승인한다.

## 5. 보안성 분석

본 절에서는 제안스킴에 대한 안전성과 효율성이 향상된 스킴을 논리적으로 증명한다. Lu et al's 스킴은 인증 파라미터들이 공개채널에서의 노출로 야기되는 사용자/서버의 위장공격, 익명성 노출, 비밀성 결여, 동시 로그인공격에 대해 3장에서 살펴보았다.

본 장에서는 이러한 취약점을 보완하여 4장에서 제안한 개선 스킴에 대해 익명성유지와 위장공격, 비밀키의 안전성과 동시 로그인공격에 안전함을 <표 3>의 토의내용에서 개선된 메커니즘을 중심으로 분석한다. 보안성분석을 위해 Arshad et al.'s[15], Lu et al.'s[16] 스킴을 인용하여 기능적인 측면과 성능적 측면에서 비교분석한다.

### 5.1 기능성 분석

Lu et al.'s 스킴의 가장 큰 취약점은 도청된 파라미터 값을 가지고 로그인정보를 합법적인 사용자인 것처럼 생성하여 위장할 수 있다는 것이 가장 큰 취약점이다. 이로 인해 익명의 노출, 사용자/서버 위장공격과 같은 연쇄적으로 취약점이 드러났다.

본 절에서는 로긴 메시지 노출의 문제해결방안으로 Lu et al's 스킴에서 취약한 파라미터 AIDi와 h2(x)를 노출되지 않도록 해시 값과 대칭키를 유도하는 파라미터(R, k)를 생성하여 메커니즘을 설계

표 3. Lu et al'.s 스킴의 주장에 대한 토의
Table 3. Discussion of Lu et al'.s scheme

| 주제 | Lu et al.'s 주장 | 오류 | 개선 |
|---|---|---|---|
| •위장공격 | •식별자와 비밀키는 제3자에 알려지지 않음으로 위장공격 불가 | •합법적 사용자는 인자 h2(x)를 공통인수로 보유 | •인자 h2(x)의 해시 값 |
| •익명성 | •서버의 비밀키, 사용자와 서버의 난수에 의해 보호 | •등록과정의 오류로 사용자 모두는 h2(x)를 보유 | •인자 h2(x)의 해시 값<br>•전송 메시지의 암호화 |
| •상호인증 | •M2=?M'2<br>•M4=?M'4<br>•cyclic group 난수 duP, duS 사용 | •사용자 및 서버의 식별자 검증부재 | •로긴메시지의 식별자검출<br>•인증메시지의 식별자검출<br>•cyclic group 난수 duP, duS 사용 |
| •동시 로그인공격 | •언급없슴 | •새로운 파라미터 점검기능 여부 | •임시테이블의 상태비트 |
| •도청공격 | •언급없슴 | •로그인메시지[M1, M2, $AID_i$, T1]분석 | •비밀키x, 비밀난수y 해시 값 |

한 것이 가장 큰 차이이다.

제안스킴에 대한 분석은 K, R의 안전성과 응용서버의 비밀키 x, 비밀의 수 y에 의존하며 응용서버에서는 사용자정보와 관련하여 로그인 세션동안만 유지되는 사용자 ID와 검증값, 타임스템프 Ti, 상태비트를 임시테이블에 일시 저장하여 서비스거부공격과 재생공격에 효율적으로 대처하였다.

#### 5.1.1 도청공격의 방어(익명성과 무결성, 기밀성 유지)

제안 논문에서 비밀 키 x와 비밀의 수 y는 서버 S만이 비밀리에 소유하고 있으며 처음 등록하는 모든 사용자들에게 적용하는 동일한 인자이다. 등록단계에서 서버 S는 다음과 같이 계산하여 사용자의 스마트카드에 Si, Vi, Ki를 제공한다. 어떤 합법적 사용자들이라도 비밀 키 x와 비밀의 수 y가 해시되어 있으므로 유추할 수 없음을 보여준다.

(1) 익명성

Lu et al.'s 스킴은 합법적 다른 사용자 Uj는 획득한(도청) 사용자 Ui의 로긴 메시지에서 AIDi로부터 사용자의 식별자 IDi를 알아낸다. 본 논문에서는 AIDi=h(IDi⊕h(x))와 같이 AIDi를 해시화 하여 제3자는 식별자 IDi를 알아내지 못한다.

로긴메시지 R, L1을 가로채었을 때 R=Si⊕MPi=h(IDi⊕x)⊕MPi⊕h(y), K=Ki⊕h(duP)=h(IDi⊕x)⊕h(x)⊕h(duP)와 같이 서버 S의 비밀키 x와 비밀의 수 y를 아는 서버만이 해독할 수 있다.

(2) 기밀성

Lu et al's 스킴은 합법적 다른 사용자 Uj는 합법적 사용자 Ui의 K를 계산할 수 있다. Uj는 도청한 AIDi와 2.4.2절에서 알아낸 IDi로 K'=h1(IDi‖IDi⊕AIDi)를 계산한다.

그 다음 합법적 다른 사용자 Uj는 합법적 사용자 Ui의 M1을 이용하여 duP(=K'⊕M1)를 계산해 내고 du와 K'를 이용하여 M'1(==duP⊕K')을 계산할 수 있다.

이와 같이 세션키(SK)생성에 중요한 파라미터 duP가 노출되고 있다.

본 논문에서는 S의 비밀키 x와 비밀의 수 y를 S만이 소유하므로 기밀성이 유지된다. 모든 사용자는 R=M3⊕h(duP), k=Ki⊕h(duP)를 계산할 수 있으나 k=R(duP)⊕h(x)⊕h(y)를 계산할 수 없다. 즉 인증 로긴메시지 Ek[IDi, M1, M2]를 디코드 할 수 있는 객체는 스마트카드를 발급한 정당한 서버 S만이 존재하므로 기밀성이 유지된다.

#### 5.1.2 사용자/서버 위장공격의 안전성

제안 논문에서 합법적인 제3의 사용자가 정당한 사용자로 위장하거나 정당한 서버로 위장할 수 없는 조건은 다음과 같다.

•AIDi=h(IDi⊕h(x))와 같이 모든 사용자는 서버의 비밀 키 x를 알 수 없다.

•정당한 사용자가 아니라면 생체정보(Bi)와 패스워드(PWi)를 알아내지 못한다.

•정당한 서버만이 x와 y를 알고 있다.

•그러므로 정당한 서버가 아니라면 duP를 계산할 수 없다.

(1) 서버 위장공격 시나리오

합법적 사용자 Uj는 Ui의 로긴 메시지 R, L1, T1을 가로채서 L1을 생성해 낼 수 없다.

•모든 사용자의 AIDx의 각각 고유값을 보유하나 h(x)를 모르고는 AIDx를 계산하지 못한다. 정확한 AIDx를 모르고는 MPi를 생성할 수 없다. 그러므로 R을 유추할 수 없으며 제3자가 임의 MPi를 생성할 경우 S의 MPi와 값이 다르므로 정상적인

h(IDi⊕x)⊕h(y)를 계산할 수 없다.

합법적 사용자 Uj는 Ui의 로긴 메시지 R, L1을 도청하여 L1(=Ek[IDi, M1, M2])을 복호할 수 없다.

이와 같이 h(x)와 h(y)는 서버 S의 소유로 비밀키와 비밀의 수로 노출되어 있지 않다. 오직 S만이 K를 알 수 있다.

(2) 사용자 위장공격 시나리오

합법적 제3자 Uj는 L'1, R'를 생성할 수 없다. M'3를 계산하기 위해서는 정확한 MPi를 생성하여야한다. 사용자의 AIDi는 정당한 사용자만이 알 수 있으므로 M1을 계산하지 못한다. M1을 계산하지 못한다면 duP를 알 수 없다. 그러므로 제3자는 R(=M3⊕h(duP))을 계산하지 못한다. 제3자는 duP를 알 수 없으므로 K를 계산할 수 없고 이로 인해 L'1을 생성할 수 없다.

#### 5.1.3 서비스거부 공격

서비스거부 공격은 응용서버의 다운, 서비스의 정지, 네트워크의 기능을 마비시키는 등 여러 형태로 나타나는데 Lu et al's 스킴에서는 로긴 정보를 대량으로 생산, 복제하여 ping of death와 같은 기법을 사용하여 동시에 많은 로그인 사용자들의 공격에 대하여 Sj는 동시에 다수의 사용자들의 접속에 대해 로그인을 승인하여야 한다.

Lu et al's 스킴에서는 로그인 요청메시지[M1, M2, AIDi, T1]를 S에 보내면 n번의 인증절차를 수행한다. 제안 스킴에서는 로그인 메시지 T1, R, L1=Ek[IDi, M1, M2]에서 정당한 응용서버 만이 L1을 디코드하여 IDi를 알아낸 후 임시 테이블에 한 세션(log out까지)동안 만 상태비트를 "1"로 저장하고 세션이 끝나면 "0"으로 세팅한다. 즉 한 세션동안 동일한 ID 식별자로 동시에 다량의 메시지를 보낼 때 응용서버는 세션을 거절한다.

#### 5.1.4 상호인증과 키 동의

사용자 Ui와 서버 Sj간의 상호인증은 각각 세션마다 L1과 L2에서 자신의 식별자를 포함시켜 유효한 개체인지 인증한다. 인증 파라미터를 위해 서버 Sj는 자신의 비밀 키 k와 비밀의 수 y를 사용한다. 사용자의 임의의 난수 duP는 h(x)를 보유한 서버만이 계산이 가능하며 로긴 메시지 M2의 유효성을 판단할 수 있다.

서버 S는 정당한 서버임을 증명하기 위해 ID(SIDj)를 encode하여 M5(=h(SIDj ‖ dsP ‖ duP ‖ T2))와 함께 L2(=Ek[SIDj, M4, M5])를 사용자에게 전송한다.

사용자 Ui는 메시지 M5를 생성 비교함으로써 정당한 서버임을 확인한다.

이와 같은 사용자와 서버 간의 상호인증 이후 사용자는 서버의 임의의 난수 ds를 연접한 메시지 M6를 서버에게 전송하여 마지막 비교가 이루어지면 세션 키 SK는 승인된다.

#### 5.1.5 스마트카드 도난

제안스킴에서 스마트카드 저장정보는 Si, Vi, Ki, h()로 제3자가 SPA(Simple Power Analysis)와 같은 공격으로 사용자의 스마트카드를 획득해도 사용자의 패스워드와 생체정보 Bi를 제3자는 계산할 수 없다. MPi는 Bi⊕pwi로 해시 값으로 되어 있어 당사자의 생체정보와 패스워드를 알고 있어야 한다. 또한 서버의 비밀 키 x와 비밀 수 y를 알 수 없으므로 AIDi를 찾아낼 수 없다.

### 5.2 효율성 분석

이 절에서는 TMIS에 대한 최근의 생체 인식 기반 인증 및 주요 계약 방식의 보안기능 및 계산성

능을 비교한다. <표 4>에서는 제안스킴과 Arshad et al.'s, Lu et al.'s 스킴을 비교하여 보안요소에 대한 공격을 저지하거나 속성을 만족시키는 체계로 √를 표시하고 공격을 저지 못하거나 속성을 만족시키지 못하는 체계로 x를 표시한다. 이전의 대부분의 생체 인증 방식이 바람직한 보안 속성을 만족하지 않음을 알 수 있다.

표 4. 제안스킴과 기존스킴의 기능비교
Table 4. Functionality comparisons of proposed scheme and previously proposed biometrics-based scheme

| security components | Arshad et al.'s[15] | Lu et al.'s[16] | Propose scheme |
|---|---|---|---|
| User anonymity | x | x | √ |
| Impersonation attack | x | x | √ |
| Replay attack | √ | √ | √ |
| Denial of service attack | √ | x | √ |
| Forward security | x | √ | √ |
| Mutual authentication | √ | √ | √ |
| Session key verification | √ | √ | √ |
| Free password change | √ | √ | √ |
| Stolen smart card attack | √ | √ | √ |

2016년 K.C.Shin은 Mishra et al.'s 스킴이 등록센터가 등록하는 모든 서버들에게 공통으로 공유키(PSK)를 인자로 사용하므로 이를 제3자가 이용하여 위장공격과 서비스거부공격, 스마트카드 도난공격에 취약함을 나타냈고 Baruah et al.'s 스킴은 로그인 및 인증 메시지를 제3자가 도청하였을 때 세션키를 계산할 수 있어서 위장공격과 스마트카드 도난공격, 전방향보안의 취약성을 지적했다[17]. Arshad et al.' s 스킴은 오프라인 패스워드 추측공격과 합법적 제3자에 의해 식별자가 노출되어 익명성의 노출, 사용자 및 서버의 위장공격에 취약하다.

Lu et al.'s의 스킴은 전술한 바와 같이 등록과정에서의 오류로 식별자가 노출되고 이로 인해 익명성의 노출과 사용자/서버의 위장공격이 가능하다.

<표 5>의 제안스킴과 이전스킴의 연산비교에서 TH,:생체정보 해시함수(Biometric hash function)수행시간, Th : 해시함수 수행시간, Tsym : 대칭키(symmetric encryption /decryption) 암복호시간, TECC : 타원곡선암호(Elliptic curve point multiplication)시간비용을 나타내며 일반적인 비용(시간복잡도)는 TECC>Tsym>TH>Th와 같은 차이를 보이나 TECC, Tsym, TH, Th 모두 계산비용이 낮은 공통점이 있다. Mishra et al.'s[13], Baruah et al's[14]의 해시함수 계산은 타원 곡선 포인트 곱셈 비용을 갖는 Lu et al.'s의 스킴에 비해 계산 오버헤드가 적다.

표 5. 제안스킴과 기존스킴의 연산비교
Table 5. Cost comparisons of proposed scheme and previously proposed biometrics-based scheme

| 구분 | | Arshad et al.'s[15] | Lu et al.'s [16] | Propose scheme |
|---|---|---|---|---|
| 등록 | | 3Th, $1T_{ECC}$ | 1Th, $1T_{H,}$ $1T_{ECC}$ | 6Th |
| 로그인 | 사용자 | 3Th, $1T_{ECC}$ | 3Th, $1T_{ECC}$ | 3Th, $1T_{ECC,}$ $1T_{Sym}$ |
| 인증 | 사용자 | 4Th | 2Th | 3Th, $2T_{Sym}$ |
| | 서버 | 7Th, $2T_{ECC}$ | 3Th, $1T_{ECC}$ | 8Th, $1T_{ECC,}$ $1T_{Sym}$ |
| 변경 | 사용자 | 2Th | 2Th | 2Th |

제안스킴에서 대칭키암호 연산비용(AES 256 : 0.8microsecond/ operation)이 해시함수 연산비용(SHA-512 : 0.76microsecond/operation) 과 큰 차이가 없다고 볼 때 연산비용은 다소 높으나 기능적인 보안향상을 높였음을 알 수 있다.

## 6. 결 론

원격서버에 대한 사용자 인증 메커니즘들은 악의적인 또는 합법적인 제3자에 의해 데이터의 도청과 위변조 공격에 쉽게 노출될 수 있다. 따라서 등록단계에서 사용자정보를 보호할 수 있는 파라미터들을 사용한 인증기술이 필요하다.

본 논문에서 Lu et al's 생체기반 인증스킴의 보안성을 분석하였다. 이 스킴은 로긴메시지의 도청에 취약하여 합법적인 제3자에게 위장공격과 익명성 보호가 되지 않음을 살펴보았다.

제안스킴에서는 로긴 메시지의 도청을 무효화시키기 위해 서버의 비밀키 x와 비밀의 수 y를 사용함으로써 도난 또는 분실했을 때 안전하며 대칭키 암호를 사용하여 합법적인 사용자가 아니라면 정당한 로그인 메시지를 생성할 수 없다. 이와 같이 스마트카드정보와 로그인 메시지를 통해서 유도되는 파라미터의 값들을 산출하지 못하도록 설계되었다.

## References


[1] L. Leng, A. B. J. Teoh, M. Li, and M. K. Khan, *A remote cancelable palm print authentication protocol based on multidirectional two- dimensional palm phasor-fusion.* Sec. Commun. Netw. doi:10.1002/sec.900, 2013.

[2] D. B. He, N. Kumar, N. Chilamkurti, and J. H. Lee, *Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol*. J. Med. Syst. Vol. 38, No. 10, pp. 1-6, 2014.

[3] D. B. He, and S. Zeadally , *Authentication protocol for ambient assisted living system*. IEEE Commun. Mag. Vol. 53, No. 1, pp. 2-8, 2015.

[4] Y. R. Lu, L. X. Li, H. P. Peng, X. Yang. and Y. X. Yang, *A lightweight ID based authentication and key agreement protocol for multiserver architecture,* Int. J. Distrib. Sens. N, Article ID 635890, pp. 1-16, 2015.

[5] Y. R. Lu, L. X. Li, and Y. X. Yang, *Robust and efficient authentication scheme for session initiation protocol.* Math. Probl. in press, Article ID 894549, pp. 1-16, 2015.

[6] R. Wang, W. Juang, and C. Lei, *Robust authentication and key agreement scheme preserving the privacy of secret key,* Computer Communications, Vol. 34, No. 3, pp. 274-280, 2011.

[7] J. Wei, X. Hu, and W. Liu, *An improved authentication scheme for telecare medicine information systems,* Journal of Medical Systems, Vol. 36, No.6, pp. 3597-3604, 2012.

[8] C. T. Li, *A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card*, IET Information Security, Vol. 7, No. 1, pp. 3-10, 2012.

[9] D. B. He, J. H. Chen, and R. Zhang, *A more secure authentication scheme for telecare medicine information systems,* Journal of Medical Systems, Vol. 36, No. 2, pp. 1989-1995, 2012.

[10] S. H. Islam, and G. P. Biswas, *Design of improved password authentication and update scheme based on elliptic curve cryptography,* Mathematical and Computer Modelling, Vol. 57, No. 12, pp. 2703-2717, 2013.

[11] 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, 2017.

[12] M. C. Chuang, and M. Chang Chen, *An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,* Expert Systems with Applications, Vol 41, Issue 4, pp. 1411-.1418, Mar. 2014.

[13] D. Mishra, A. K. Das, and S. Mukhopadhyay, *A secure user anonymity-preserving biometric based multi-server authenticated key agreement scheme using smart cards*, Expert Systems with Applications, Vol. 41, No. 18, pp. 8129-8143, 2014.

[14] K. C. Baruah, S. Banerjee, M. P. Dutta, and C. T. Bhunia, *An improved biometric-based multi-server authentication scheme using smart card,* International Journal of Security and Its Applications, Vol. 9, No.1, pp. 397-408, 2015.

[15] H. Arshad, and M. Nikooghadam, *Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems*. J. Med. Syst. Vol. 38, No. 12, pp. 1-12, 2014.

[16] Y. Lu, L. Li, H. Peng, and Y. Yang, *An enhanced biometric-based authentication scheme for telecare medicine information system using elliptic curve cryptosystem*, Journal of Medical Systems, Vol. 39, No. 32, pp. 1-9, 2015.

[17] K. C. Shin, *Cryptanalysis of biometric based Baruah et al.'s multi-server authentication scheme,* Journal of Security Engineering, Vol. 13, No. 5, pp. 379-392, 2016.

## 익명성 및 기밀성을 강화한 원격 사용자 인증스킴 설계에 관한 연구

**신광철**

*성결대학교 산업경영공학부 부교수*

**요 약**

지금까지 원격 인증 시스템의 보안성을 높이기 위해 스마트카드를 이용한 다양한 생체 인식 기반의 인증 방식이 제안되었다. 텔레케어 의료정보시스템(TMIS)은 사용자(환자)의 시간과 비용을 절약해 편리한 의료서비스를 제공한다. 그러므로 시스템은 사용자와 의료서버 간에 안전한 상호인증이 중요하며 민감한 의료정보는 제3자에게 노출되어서는 안 된다. 본 논문에서는 타원 곡선 암호화를 이용한 Lu et al.'s의 인증 프로토콜에 대한 취약점을 분석하고 개선한 스킴을 제안한다. Lu et al.'s 스킴은 Arshad et al.'s 스킴에서 사용자 위장공격에 대한 취약성을 보완하여 향상된 생체인식 및 스마트카드 기반 원격인증 스킴으로 발전시켰다. 그러나 그들의 스킴을 분석한 결과 로긴 메시지의 도청에 의해 사용자의 익명과 로긴 메시지의 기밀성을 노출시키는 문제점이 있다. 그러므로 사용자와 서버의 합법적 위장공격에 취약함을 나타냈다. 제안논문에서는 서버의 비밀 키와 비밀 수의 보안에 중점을 두고 재설계하여 익명성과 메시지의 기밀성, 합법적 사용자 및 서버의 여러 공격에 안전한 사용자 인증 스킴을 제안한다. 향후 인증스킴을 설계할 때 강력한 보안과 구현의 효율성을 제공하는데 기여하고자 한다.

**Kwang Cheul Shin** received the bachelor's degree in the department of Computer Science, National University of Science and Technology in 1985. He received the M.S. degree in the department of Computer Science, Korea National Defense University 1990 and the Ph.D. degree in the department of Information and Communication Engineering, Sungkyunkwan University 2003, respectively. He has been a professor in the Division of Industrial Management Engineering at Sungkyul University since 2004.

*E-mail address*: skcskc12@sungkyul.ac.kr