JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 10, pp. 101-108, October 2021
https://doi.org/10.9708/jksci.2021.26.10.101

Design Errors and Cryptanalysis of Shin's Robust Authentication Scheme based Dynamic ID for TMIS

Mi-Og Park*

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

[Abstract]

In this paper, we analyze Shin's proposed dynamic ID-based user authentication scheme for TMIS(Telecare Medicine Information System), and Shin's authentication scheme is vulnerable to smart card loss attacks, allowing attackers to acquire user IDs, which enables user impersonation attack. In 2019, Shin's proposed authentication scheme attempted to generate a strong random number using ECC, claiming that it is safe to lose a smart card because it is impossible to calculate random number r'i due to the difficulty of the ECC algorithm without knowing random number ri. However, after analyzing Shin's authentication scheme in this paper, the use of transmission messages and smart cards makes it easy to calculate random numbers r'i, which also enables attackers to generate session keys. In addition, Shin's authentication scheme were analyzed to have significantly greater overhead than other authentication scheme, including vulnerabilities to safety analysis, the lack of a way to pass the server's ID to users, and the lack of biometric characteristics with slightly different templates.

▸ **Key words**: User Authentication, Stolen Smart-Card attack, Password Guessing attack, TMIS(Telecare Medicine Information System), ECC(Elliptic curve cryptography)

[요 약]

본 논문에서는 Shin이 제안한 TMIS를 위한 동적 ID 기반의 강력한 사용자 인증기법을 분석하고, Shin의 인증 기법이 스마트카드 분실 공격에 취약하여, 공격자가 사용자의 ID를 획득할 수 있고, 이로 인하여 사용자 가장 공격 등이 가능함을 보인다. 2019년에 Shin이 제안한 인증 기법은 ECC를 사용하여 강력한 난수 생성을 시도함으로써, 난수 ri를 모르면 ECC 알고리즘의 난이도에 의하여 난수 r'i를 계산해낼 수 없어서, 스마트카드를 분실하여도 안전하다고 주장하였다. 그러나 본 논문에서 Shin의 인증 기법을 분석한 결과, 전송 메시지와 스마트카드를 사용하면 난수 r'i를 쉽게 계산할 수 있고, 이로 인하여 공격자는 세션키 생성도 가능하였다. 또한 Shin의 인증 기법은 안전성 분석에 대한 취약점뿐만 아니라, 서버의 ID인 SID를 사용자들에게 전달하는 방식의 부재, 사용 시마다 약간씩 다른 템플릿을 가지는 생체정보의 특성을 고려하지 않은 점 등 다수의 설계상의 오류들이 존재하였고, 서버에서 사용자의 ID를 계산해내는 시간 복잡도가 다른 인증 기법들에 비하여 상당히 큰 오버헤드를 가진 것으로 분석되었다.

▸ **주제어**: 사용자 인증, 스마트카드 분실 공격, 패스워드 추측공격, TMIS(원격의료 정보시스템), ECC(타원곡선알고리즘)

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@hanmail.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2021. 09. 06, Revised: 2021. 09. 28, Accepted: 2021. 09. 29.

Copyright © 2021 The Korea Society of Computer and Information
http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

2021년 현재 우리는 4차 산업혁명을 논하는 사회에 살고 있으며, 의료산업은 4차 산업혁명에서 주목받는 분야로 그 중 원격진료는 이미 초고령층 사회가 된 일본이나 프랑스, 독일, 미국 등에서는 이미 자리를 잡았고, 실버시대로 접어든 국가들에서는 TMIS(Telecare Medical Information System, 원격 의료정보시스템)의 중요성이 더욱 커질 것으로 보인다. TMIS란 말 그대로 환자(사용자)가 의사를 직접 대면하지 않고도 진료 서비스를 받을 수 있는 형태로, 환자의 건강상태나 개인정보가 인터넷을 통하여 전송되기 때문에 사용자의 프라이버시(privacy)나 사용자의 익명성(user anonymity)이 매우 중요하고, 전송 데이터의 기밀성(confidentiality), 환자와 의사간의 상호 인증(mutual authentication) 등이 보장되어야한다.

상호 인증을 위한 원격 사용자의 인증은 1981년 Lamport가 패스워드기반의 원격 사용자 인증 기법[1]을 처음 제안한 것을 시초로 하여, 다수의 two-factor 인증 기법들이 제안되었고, 현재는 생체정보를 같이 사용하여 two-factor 인증 기법들의 문제점을 개선하는 three-factor 인증 기법들로 발전하게 되었다. 또한 이러한 인증 기법들은 TMIS 환경의 사용자 인증 기법으로도 발전하였으며, 인증 기법의 향상된 안전성을 위하여 RSA 알고리즘[2][3][4]이나 ECC 알고리즘[5][6][7]과 같은 공개키 암호방식을 사용한 TMIS 사용자 인증 기법들도 제안되고 있다. ECC 알고리즘은 RSA 알고리즘에 비하여 더 작은 키 사이즈, 예를 들어 1024-bits 키의 RSA 알고리즘은 160-bits 키의 ECC 알고리즘과 동일한 안전성을 가지는 특성 때문에, 원격 사용자들이 주로 사용하는 제한적인 한계의 모바일 디바이스에 적합하다.

ECC를 사용한 인증 기법은 Durlanik-Sogukpinar[8]가 2005년에 처음으로 제안한 이후로, TMIS의 원격 사용자 인증 기법에서도 ECC를 사용한 인증 기법들이 제안되고 있으며, 2014년 Xu 등[9]은 ECC를 사용한 two-factor 인증 기법을 제안하였다. Xu 등은 그들의 인증 기법에서 여러 인증 기법들을 논하면서, 그 인증 기법들이 사용자 익명성의 문제에 주의를 기울이지 않았고, 그 중 일부의 인증 기법들은 오프라인 패스워드 추측 공격(offline password guessing attack)에 취약하다고 주장하였다. 2014년 Islam-Khan[10]은 Xu 등의 인증 기법에 대한 취약점을 분석하고, 보다 향상된 익명의 TMIS two-factor 인증 기법을 제안하였다. Islam-Khan 등이 분석한 Xu 등의 취약점은, 사용자의 ID와 패스워드가 올바른지 체크하는 과정이 부재하여 로그인과 인증 단계에서 강력한 인증을 할 수 없고, 이로 인하여 패스워드 변경 단계에서도 입력한 패스워드의 정확성 체크를 할 수 없어서, 패스워드를 올바르게 업데이트하지 못한다고 분석하였다. 또한 분실된 스마트카드의 철회과정을 제공하지 않는 점, 그리고 강력한 재생 공격(strong replay attack)에 안전하지 않다고 분석하였다. Islam-Khan은 서버의 DB에 (IDi, N, T1)를 저장하여 다음의 전송 메시지가 오면 DB의 타임스탬프 T1과 전송 메시지의 T1'을 비교하여 강력한 재생 공격을 막을 수 있고, T1을 이용한 동적 ID CIDi를 사용하여 사용자 익명성을 제공할 수 있다고 주장하였다. 또한 Islam-Khan은 Xu 등의 인증 기법이 실제 사용에서 비효율적이나 자신들의 인증 기법은 다른 인증 기법들에 비해 안전하고 계산측면에서도 더 효율적이라고 주장하였다.

그러나 2015년 Chaudhry 등[11]은 Islam 등의 인증 기법이 정당한 사용자이면 누구나 Ks.G를 쉽게 계산 가능하여 사용자와 서버 가장 공격에 취약하다고 분석하고, 사용자마다 다른 값을 사용하여 취약점을 개선하여, 모든 공격에 안전하다고 주장하였다. 2017년 Qui[12] 등은 Chaudhry 등의 인증 기법이 오프라인 패스워드 추측 공격, 사용자 및 서버 가장 공격, 그리고 중간자 공격(man-in-middle attack)에 취약하다고 분석하고, 이 취약점을 개선한 새로운 인증 기법을 제안하였다. Qui 등은 Chaudhry 등의 취약점뿐만 아니라 Islam-Khan 등의 취약점도 함께 개선하고, 상호 인증과 다양한 공격에 대한 저항성을 가진다고 주장하였다. 그에 대한 안전성은 BAN 로직(Burrows-Abadi-Needham Logic)을 사용하여 증명하였다.

2019년 Shin[13]은 ECC를 사용하는 동적 ID기반의 강력한 TMIS 인증 기법을 제안하면서, Qui 등의 인증 기법이 내부자 공격과 서비스 거부 공격에 취약하다고 간단히 언급하고 있다. 또한 Shin은 자신의 인증 기법이 Chaudhry 등과 Islam-Khan 등의 취약점인 사용자 가장 공격과 서버 가장 공격, 그리고 중간자 공격에 안전한 새로운 인증 기법이라고 주장하였고, 설계의 중점은 사용자 익명성과 효율적인 인증 단계에 중점을 두었고, 사용자와 서버 간의 ECC 생성자 r'i를 사용하여 재생 공격에 대한 저항성을 가진다고 주장하였다.

본 논문에서 Shin의 인증 기법을 분석한 결과, Shin의 인증 기법은 Qui 등의 인증 기법에서 생성한 난수와 ID 검색 방법을 많이 사용한 것으로 보이며, 서버에서 ID 검색과정을 살펴보면, Qui 등의 인증 기법은 서버의 DB에 {IDi, rs}를 저장하여, 사용자가 로그인 메시지 {PIDi, Gi}를 전송하면 서버가 자신의 비밀키 x와 DB에 저장된 {IDi, rs}를 사용하여

T=h(IDi||Ks||rs)를 계산한 후, 사용자의 IDi를 계산해내기 위하여 ID'i||C'i=PIDi⊕T를 계산한다. 그러나 Shin의 인증 기법은 IDi를 DB에 저장하지 않고, IDi가 Di를 계산한 다음에 Ai안에 해시함수로 처리되어 있어서, 정당한 서버라 할지라도 사용자의 IDi를 알려면 사용자의 IDi를 추측공격 해야 하는 문제가 존재하였다. Shin 인증 기법은 이러한 설계상의 오류 외에도 다른 오류가 더 존재하였고, 무엇보다도 스마트카드를 공격자가 획득한다 할지라도 ECC 알고리즘의 난이도에 의하여 ECC 생성자 r'i를 공격자가 알 수 없어서 안전하다고 하였으나, 스마트카드와 전송 메시지를 사용할 경우, ECC 생성자를 간단히 계산할 수 있고, 이로 인하여 사용자 가장 공격과 세션키 생성까지 가능하였다.

본 논문의 구성은 먼저 2장에서 Shin 등의 인증 기법을 살펴보고, 3장에서 Shin의 인증 기법에 존재하는 설계상의 오류와 ID 검색의 오버헤드를 분석한다. 4장에서는 Shin의 인증 기법이 스마트카드 분실 공격에 취약함으로써 다양한 공격에 안전하지 않음을 보이며, 마지막으로 5장에서 결론을 내린다.

II. Related Work

1. Shin's User Authentication Scheme

본 장에서는 Shin이 제안한 TMIS를 위한 인증 기법의 각 단계에 대하여 살펴본다. 2019년에 Shin은 강력한 인증 기법을 위하여, ECC를 사용하여 일반적인 인증 기법에서 난수가 노출되는 문제를 해결하려고 하였고, 재생 공격에 대한 저항성을 위하여 타임스탬프 대신에 ECC 생성자 r'i를 사용하였다. Shin의 인증 기법은 등록 단계, 로그인과 인증 단계, 그리고 패스워드 변경 단계를 제시하였고, 사용된 기호와 의미는 Table 1과 같다.

Registration Phase

등록 과정은 다음과 같이 진행한다.

1.사용자 Ui는 자신의 패스워드 PWi와 생체정보 Bioi를 사용하여 h(PWi⊕Bioi)를 계산한다.

2.사용자 Ui는 안전한 채널을 통하여 자신의 IDi와 h(PWi⊕Bioi)를 서버 Sj에게 전송한다.

3.서버 Sj는 사용자 IDi의 비밀번호에 해당하는 yi를 생성하여 다음을 계산한다.

Ai=h(IDi⊕yi), Bi=h(Ai), Ci=h(PWi⊕Bioi)⊕Bi,
Di=yi⊕Ai⊕h(yi), Ei=h(yi)⊕h((PWi⊕Bioi)

4.서버 Sj는 사용자 Ui에게 {Ci, Di, Ei, p, G}가 저장된 스마트카드를 안전한 채널을 통하여 전송한다.

5.사용자 Ui는 전송받은 Ci와 h(PWi⊕Bioi)를 사용하여 B'i=Ci⊕h(PWi⊕Bioi)를 계산한 후 스마트카드에 추가로 저장한다.

6.서버 Sj는 데이터베이스에 Ai와 로그인 메시지 인증 시에 추출된 ECC 생성자(r'i)를 공란으로 만들고, 상태비트는 0으로 저장한다.

Table 1. Notifications and abbreviations

Symbol	Description
U, S	User, Server
IDi	Ui's Identity
PWi	Ui's Password
Bioi	Ui's Biometric data
G	Generator of Cyclic group Zp
X	Private key of Server
y	Number of secret
p	1024 bit prime
h(.)	One-way hash function
⊕	Exclusive-OR operation
||	Concatenation operation

Login Phase

Shin의 로그인 단계는 사용자의 IDi와 패스워드 PWi, 그리고 생체정보 Bioi를 사용하여, 로그인 요청 메시지를 생성한다. 그에 대한 과정은 다음과 같다.

1.로그인 요청을 원하는 사용자 Ui는 스마트카드를 카드 리더기에 삽입하고 자신의 IDi와 패스워드 PWi를 입력하고 생체정보 센서를 사용하여 자신의 생체정보 Bioi를 입력한다.

2.스마트카드는 사용자가 입력한 PWi와 생체정보 Bioi를 사용하여 h(PWi⊕Bioi)를 계산하고, 스마트카드에 저장된 Ci를 사용하여 Bi=Ci⊕h(PWi⊕Bioi)를 계산한다. 계산 결과가 스마트카드에 저장된 Bi'과 일치하면 Ei를 사용하여 h(yi)를 추출해내고, 일치하지 않을 경우 과정을 종료한다.

3.스마트카드는 랜덤넘버 ri∈Z*p를 선택하고 r'i=riG를 생성하여 다음을 계산한다.

M_1=h(Bi)⊕r'i⊕h(yi), AIDi=h(r'i)⊕IDi⊕h(yi)
M_2=h(r'i ‖ AIDi ‖ Di ‖ SIDj)

4.스마트카드는 서버 Sj에게 로그인 요청 메시지 {M_1, M_2, Di}를 전송한다.

Authentication Phase

1.로그인 요청 메시지 {M_1, M_2, Di}를 수신한 서버 Sj는 비밀키 x와 데이터베이스에 저장된 datum을 사용하

여 $D'i=h(x \| Ai)$를 계산하고 수신한 Di와 $D'i$의 일치 여부를 확인한다. 일치한 Di는 사용자의 식별자를 포함하므로, IDi를 검색해 낼 수 있다.

2.검색된 IDi와 로그인 요청 메시지 M_1을 이용하여 $r'i=M_1 \oplus h2(Ai) \oplus h(yi)$와 $AIDi=h(r'i) \oplus IDi \oplus h(yi)$를 계산한다. 사용자의 ECC 생성자 (r'i)는 데이터베이스에 저장하고 상태비트를 0에서 1로 변환하여 재생공격과 세션유지에 사용한다.

3.서버 Sj는 사용자의 정당성 검증을 위해 $M'_2=h(r'i \| AIDi \| Di \| SIDj)$를 계산하여 전송 받은 M_2와 값이 일치하는지 비교한다. 만약 두 값이 일치하면 사용자를 정당한 사용자로 인증하고, 그렇지 않을 경우 세션을 여기서 종료한다.

4.서버는 랜덤넘버 $rs \in Z*p$를 선택하고 $r's=rsG$를 생성하여 세션키 $SKji=h(IDi \| r'i \| r's \| SIDj)$와 $M_3=r's \oplus h(r'i) \oplus h(yi)$, $M_4=h(SIDj \| r's \| AIDi)$를 계산한다.

5.서버 Sj는 인증 메시지 $\{M_3, M_4\}$를 Ui에게 전송한다.

6.$\{M_3, M_4\}$를 전송받은 사용자는 $r's = M3 \oplus h(r'i) \oplus h(yi)$를 계산하고 서버가 정당한 서버인지 확인하기 위하여 $M'_4=h(SIDj \| r's \| AIDi)$를 계산한다. M'_4와 서버로부터 전송받은 M_4의 값이 일치하면, 사용자는 서버를 정당한 서버로 인증하고 세션키 $SKji=h(IDi \| r'i \| r's \| SIDj)$를 계산한다.

Password Change Phase

패스워드를 변경하기 원하는 사용자는 현재의 패스워드 PWi와 자신의 IDi, 그리고 생체정보 Bioi를 입력하여 자신의 패스워드를 변경할 수 있다.

1.사용자는 자신의 IDi와 PWi를 입력한다.

2.스마트카드는 사용자의 IDi를 확인하고, 생체정보를 입력받아 스마트카드의 정당한 사용자인지 확인한다.

$$h(yi)=Ei \oplus h(PWi \oplus Bioi)$$

$$h(PWi \oplus Bioi) \oplus Ci \oplus h(yi) \ ?= Bi$$

3.사용자는 새로운 패스워드 PWi^{new}를 입력하고, Ci^*를 $Ci^*=Ci \oplus h(PWi \oplus Bioi) \oplus h(PWi^{new} \oplus Bioi)$와 같이 계산하여 Ci 대신에 저장한다.

III. Analysis of Shin's Authentication Scheme

1. Design Errors

본 장에서는 본 논문에서 분석한 Shin의 인증 기법에 존재하는 설계상의 오류 및 ID 검색시간의 오버헤드 등에 대하여 분석한다.

Server SIDj's lack of delivery method

Shin의 인증 기법은 로그인 단계에서 사용자가 $M_2=h(r'i \| AIDi \| Di \| SIDj)$를 계산하고, 인증 과정을 통과하면 세션키 $SKji=h(IDi \| r'i \| r's \| SIDj)$를 계산한다. 사용자가 M_2와 세션키 SKji를 계산하기 위해서는, 서버의 ID인 SIDj를 알고 있어야 한다. 그러나 Shin의 인증 기법에서는 SIDj를 어떤 방식으로 사용자들에게 전송하는지에 대한 언급이 전혀 없이, 사용자가 이 값을 사용하고 있다.

Missing stored data on smart-card

Shin의 인증 기법은 두 개의 해시함수 h()와 h_2()를 사용하는 것으로 보이나, 이에 대한 설명이 부재하다. 일부 수식에서 h_2() 사용하고, 다른 수식에서는 h()를 사용한 것으로 보아, Shin의 인증 기법은 두 개의 해시함수를 사용하는 것으로 보인다. 그러나 스마트카드에는 두 개의 해시함수가 누락되어있고, 이럴 경우 사용자는 해시함수 연산을 할 수 없게 되어 로그인 및 인증 단계를 진행할 수 없다.

```
                          Registration phase
User Ui                                          Registration Center Sj
                          IDi, h(PWi⊕Bioi)       1.Generate secret number yi
                         -------------------->   2.Ai=h(IDi⊕yi)
                                                  3.Bi=h(Ai)
                                                  4.Ci=h(PWi⊕Bioi)⊕Bi
                                                  5.Di=h(x||Ai)
                                                  6.Ei=h(yi)⊕h(PWi⊕Bioi)
                          Ci, Di, Ei, p, G        7.Save datum
1.Bi' = Ci⊕h(PWi⊕Bioi)   <---------------------
2.Insert Bi into the smart card
```

Fig. 1. Shin's Registration Phase

2. Overhead of ID Search and Complexity

Overhead of ID search

Shin의 인증 단계1는 전송받은 Di와 일치하는 D'i 값을 찾기 위해서, DB의 모든 Ai와 D'i=h(x||Ai)를 계산해야한다. 일치하는 D'i 값을 찾았을 경우, D'i에 일치하는 Ai는 h(IDi⊕yi)이기 때문에, DB에 저장된 yi를 사용하여 사용자의 IDi를 찾아야한다. 그러나 Shin의 인증 기법에서는 IDi 저장에 대한 설명은 없고, 인증 단계1에서 이 단계를 수행하면 사용자의 IDi를 계산해 낼 수 있다고 했기 때문에, 수식에 의하여 서버가 IDi를 계산해낼 수 있어야 한다. 그러나 IDi가 DB에 저장되어 있지 않고, 해시함수로 처리되어있기 때문에 정당한 서버가 Ai와 yi를 알고 있음에도 불구하고 그에 해당하는 정확한 IDi 값이 무엇인지 알 수 없다. 그러므로 정당한 서버라 할지라도 사용자의 IDi 값을 곧바로 계산해 낼 수 없어서, 사용자의 ID를 추측공격해야 하는 문제가 발생한다. 그러므로 Shin의 인증 기법은 인증 단계에서 사용자 ID 검색에 대한 설계 오류가 존재한다고 할 수 있다.

Time complexity

Shin의 인증 기법에서 일치하는 Ai를 계산하는 시간 복도는 n개의 Ai가 저장되었다고 가정할 경우, 해시함수(Th) 1번, 연결 연산(||, Tc) 1번으로 n(1Th+1Tc)로 표기할 수 있다. 해당 IDi가 DB에 저장되어 있을 경우에는 해시함수 연산 1번, XOR 연산(Tx) 1번으로, 1Th+1Tx이나 Shin의 인증 기법에서는 IDi를 추측 공격해야 하므로, |Did|의 시간이 걸린다. Did는 ID를 추측공격하기 위한 공간(space)을 의미한다.

본 논문에서 분석한 Table 2는 Islam이나 Chaudhry 등의 인증 기법은 서버에서 간단한 계산을 하여, IDi를 검색해 낼 수 있고, Qui 등의 인증 기법과 Shin 등의 인증 기법에서는 IDi 검색 오버헤드가 존재하는 것을 볼 수 있다. Chaudhry 등의 인증 기법에서 IDi 계산은 ID'i=PIDi⊕(Ci · Ks^{-1})와 같이 곧바로 계산되며, 역(inverse) 연산은 Ti로 표기하였다. Qui 등의 인증 기법은 그들의 인증 단계3에서 {PIDi, Gi}를 전송받은 서버는 T를 계산한 후, IDi'||Ci'=PIDi⊕T를 계산하여 IDi'?=IDi를 비교한다. 그런데 T는 h(IDi||Ks||rs)로 계산하기 때문에, T를 계산하는 시점에서 사용자의 IDi를 알아야 한다. 그래서 등록 단계에서 저장한 {IDi, rs}를 사용한다. 그리고 T를 계산하려면 DB에 저장된 모든 IDi와 rs를 사용해 T를 계산해야하고, 그런 다음 IDi'||Ci'=PIDi⊕T를 계산해야 로그인을 요청한 사용자의 IDi를 알아낼 수 있다. 그러므로 Qui 등의 인증 기법은 사용자의 IDi 검색 오버헤드가 존재한다. 그러나 서버가 사용자의 IDi를 추측 공격해야하는 설계 오류는 존재하지 않는다.

IV. Cryptanalysis of Shin's Authentication Scheme

1. Analysis of Various Attacks

본 장에서는 Shin의 인증 기법에 대한 안전성 측면을 분석한다. Shin이 제안한 인증 기법은 TMIS 환경 때문에 무엇보다도 사용자의 프라이버시가 중요하다고 강조하였고, 이러한 사용자 프라이버시를 위하여 동적 ID를 사용하

Login and Authentication phase

Patient Ui		Medical Server MS
1.Input ID_i, PW_i, Bioi		
2.Check Bi=Ci⊕h(PW_i⊕Bioi)		
3.h(yi)=Ei⊕h(PWi⊕Bioi)		
4.generate ECC ri, ri'=riG		
5.M_1=h(Bi)⊕ri'⊕h(yi)		
6.AIDi=h(ri')⊕IDi⊕h(yi)		
7.M_2=h(ri'||AIDi||Di||SIDj)	M_1, M_2, D_i ---------->	1.Search datum: Ai, Aj, Ak,... An Di ?= h(x||Ai)
		2.r'i=M_1⊕h_2(Ai)⊕h(yi)
		3.AIDi=h(r'i)⊕IDi⊕h(yi)
		4.Check M_2 ?=h(r'i||AIDi||Di||SIDj)
		5.Generate ECC rs, r's=rsG
		6.SKji=h(IDi||r'i||r's||SIDj)
9.r's=M_3⊕h(r'i)⊕h(yi)	M_3, M_4 <----------	7.M_3=r's⊕h(r'i)⊕h(yi)
10.M_4' ?= M_4		8.M_4=h(SIDj||r's||AIDi)
11.SKji=h(IDj||r'i||r's||SIDi)		

Fig. 2. Shin's Login and Authentication Phase

Table 2. Time complexity of ID search

Computational cost	Islam et al's scheme[10]	Chaudhry et al's scheme[11]	Qui et al's scheme[12]	Shin's scheme[13]
Hash operation	1Th		mTh	(n+1)Th
Multiplication operation	-	1Tpm, 1Ti	-	-
XOR operation	1Tx	1Tx	mTx	1Tx
Concatenate(||) operation	1Tc	-	2mTc	nTc
Total operation	1Th+1Tx+1Tc	1Tpm+1Tx+1Ti	m(1Th+2Tc+1Tx)	(n+1)Th+1Tx+1Tc

여 사용자에게 안전한 익명성을 보장하고, 다른 인증 기법들에 비하여 더 빠른 계산 시간 때문에 더 효율적인 인증 기법이라고 Shin은 주장하였다. 그러나 본 논문에서 Shin의 인증 기법을 분석한 결과, Shin의 인증 기법은 스마트카드 분실 공격에 취약하여 사용자의 IDi 획득이 가능하였고, 이로 인하여 세션키 노출과 함께 사용자 가장 공격 등 다양한 공격이 가능하였다.

Stolen smart-card attack

본 논문에서 제안하는 스마트카드 분실 공격의 시나리오는 다음과 같다.

1. 공격자는 스마트카드에 저장된 Bi와 Ci를 사용하여 다음을 계산한다.

$$h(PWi \oplus Bioi)^* = Bi \oplus Ci$$

2. 스마트카드의 Ei와 앞에서 계산한 $h(PWi \oplus Bioi)^*$를 이용하여 $h(yi)^* = Ei \oplus h(PWi \oplus Bioi)^*$를 계산한다.
3. 전송 메시지 $M_1 = h(Bi) \oplus r'i \oplus h(yi)$와 스마트카드의 Bi, 그리고 바로 앞 단계에서 계산한 $h(yi)^*$를 사용하여 $r'i^* = M1 \oplus h(Bi) \oplus h(yi)^*$를 계산한다.
4. M_2를 계산하는 데 필요한 값들 중 r'i는 앞에서 계산한 $r'i^*$를 사용하고, 스마트카드의 Di를 그대로 사용하여 추측한 사용자의 IDi가 맞을 때까지 계속 반복한다.

$$M_2 \ ?= h(r'i^* \| AIDi \| Di \| SIDj)$$
$$?= h(r'i^* \| h(r'i^*) \oplus IDi \oplus h(yi)^* \| Di \| SIDj)$$

Shin의 인증 기법에서는 서버의 SIDj에 대한 언급이 없으나, 서버의 SIDj는 모든 사용자들이 공통으로 동일한 값을 사용하고, 정당한 모든 사용자가 아는 공개 정보이기 때문에, 서버의 SIDj는 추측공격 할 필요 없이 악의적인 정당한 사용자가 서버로부터 전송받아 획득한 SIDj를 사용하면 된다.

5. 서버에서 생성한 난수 r's는 전송 메시지 M_3과 앞에서 계산한 $r'i^*$, $h(r'i^*)$, $h(yi)^*$를 사용하여 계산해낸다.

$$r's^* = M_3 \oplus h(r'i^*) \oplus h(yi)^*$$

인증단계4는 $M_3 = r's \oplus h(r'i) \oplus h(yi)$인데, r'i는 로그인 단계에서 계산가능하기 때문에 공격자는 $h(r'i^*)$를 계산할 수 있고, h(yi)도 로그인 단계에서 계산 가능하다. 그러므로 서버가 생성한 난수 r's를 XOR 연산을 통해 간단히 획득할 수 있다.

6. 전송 메시지 M_4는 h(SIDj||r's||AIDi)이고, 앞에서 획득한 $SIDj^*$와 $AIDi^*$, 그리고 계산한 $r's^*$를 사용하여 다음을 계산한다. 계산 결과가 M_4와 동일하면 추측에 성공한 것이고, 아닐 경우 4번, 6번을 반복한다.

$$M_4 \ ?= h(SIDj^* || r's^* || AIDi^*)$$

7. 앞에서 계산해 낸 난수 $r'i^*$와 $r's^*$, 그리고 사용자와 서버의 ID 추측 공격에 성공할 경우, 공격자는 세션키 SKji를 계산할 수 있다.

$$SKji = h(IDi^* \| r'i^* \| r's^* \| SIDj^*)$$

그러므로 Shin의 인증 기법은 스마트카드 분실 공격에 취약하다고 할 수 있다.

2. Analysis of Security Features

본 절에서는 안전성 기능에 대해 분석한다.

Forward secrecy

Shin은 ECC의 난해함으로 인하여 공격자가 r'i와 r's를 계산해낼 수 없어 안전하다고 하였다. 그러나 앞에서 분석한 바와 같이 공격자는 ri나 rs를 계산해내려고 시도할 필요 없이, $r'i^*$와 $r's^*$를 계산해 낼 수 있고, 세션키도 생성 가능하였다. 그러므로 Shin의 인증 기법은 전방향 안전성을 제공한다고 할 수 없다.

Table 3. Comparison of computation complexity

Computational cost	Islam et al's scheme[10]	Chaudhry et al's scheme[11]	Qui et al's scheme[12]	Shin's scheme[13]
User	5Th+3Tpm+1Tpa	5Th+4Tpm+1Tpa	8Th+2Tpm	6Th+1Tpm+1Tpa
Server	4Th+3Tpm	4Th+3Tpm+1Tpa	5Th+2Tpm	6Th+1Tpm+1Tpa
User + Server	9Th+6Tpm+1Tpa	9Th+7Tpm+2Tpa	13Th+4Tpm	12Th+2Tpm+2Tpa
Total cost with ID Search	1Th+1Tx+1Tc	18Th+14Tpm+4Tpa	m(1Th+2Tc+1Tx)	(n+1)Th+1Tx+1Tc

User impersonation attack

Shin의 인증 기법에서 공격자가 PWi와 Bioi의 값을 따로 따로 획득하지 못한다할지라도, 모든 과정에서 PWi와 Bioi는 항상 동일한 식으로 계산되기 때문에, 두 개의 값을 따로 획득할 필요가 없다. 그러므로 스마트카드 분실공격에서 제안한 시나리오에 의하여 공격자는 $h(PWi \oplus Bioi)^*$을 획득할 수 있으므로, 이 값을 이용하여 사용자를 가장할 수 있다.

Password guessing attack

Shin의 인증 기법은 스마트카드 분석에서 분석한 바와 같이, 공격자가 정당한 사용자로 가장할 수 있다. 그러나 패스워드 PWi는 Bioi와 함께 모든 과정에서 해시 연산되어 사용되기 때문에, 패스워드 추측공격은 어렵다.

Mutual authentication

Shin의 인증 기법은 난수 r'i와 r's를 사용하여 상호 인증을 제공하나, 스마트카드를 분실할 경우 공격자가 r'i와 r's를 쉽게 계산할 수 있고 세션키까지 생성할 수 있으므로, 민감한 개인정보를 다루는 TMIS를 위한 안전한 상호 인증이라고 할 수 없다. 본 논문에서 스마트카드분실 공격을 분석한 결과, Islam 등의 인증 기법과 Chaudhry 등의 인증 기법도 스마트카드 분실 공격에 안전하지 않아 결국, 안전한 상호 인증을 제공하지 않았다.

User anonymity

Shin의 인증 기법은 스마트카드를 분실할 경우 공격자가 세션키를 생성할 수 있으므로, 세션키로 이전의 메시지를 복호화 할 수 있다. 또한 세션키 생성에는 사용자의 IDi가 사용되므로 안전한 사용자 익명성을 보장한다고 말할 수 없다.

본 논문에서 분석한 결과는 Table 4와 같고, Yes는 해당 항목의 공격에 대한 저항성이 있거나 안전성 기능을 제공한다는 의미이고, No는 그 반대를 의미이다.

V. Improvement plan

본 논문에서는 Shin이 제안한 인증 기법을 분석하였고, 분석한 결과 Shin의 인증 기법은 서버의 ID를 전달하는 방식의 부재, 스마트카드의 정보의 누락, 그리고 ID 검색 오버헤드가 크고, 최악의 경우 서버가 ID를 추측 공격해야 하는 상황까지 발생할 수 있었다. 게다가 Shin의 인증 기법은 공격자가 스마트카드를 획득할 경우, Shin이 강조하였던 ECC 생성자 r'i를 쉽게 계산할 수 있고, 이로 인하여 사용자 가장 공격, 세션키의 노출, 전방향 안전성, 사용자 익명성 등의 문제점이 존재하였다.

이러한 문제점을 해결하기 위한 개선방안 중, 서버의 사용자 IDi 검색 오버헤드에 대한 문제는 사용자의 IDi를 DB에 저장하되, 서버의 비밀키로 사인하여 저장함으로써, 사용자의 IDi가 곧바로 노출되는 문제와 사용자의 IDi를 추측 공격해야하는 문제를 개선할 수 있다. 또한 ECC 생성자 r'i로 인한 스마트카드 분실 공격에 대한 문제는, 각 단계의 계산과정에서 ri와 rs를 사용함으로써 Shin의 인증 기법을 ECC 비도에 의하여 안전하게 개선할 수 있을 것으로 본다. 이로 인하여 스마트카드 분실 공격에 의하여 발생하는 세션키 값의 노출이나 전방향 안전성, 불안전한 사용자 익명성 등의 문제를 개선할 수 있다.

Table 4. Comparison of security features

Security and Functionary features	Islam et al's scheme[10]	Chaudhry et al's scheme[11]	Qui et al's scheme[12]	Shin's scheme[13]
User anonymity	No	Yes	Yes	No
User impersonation attack	No	Yes	Yes	No
Server impersonation attack	No	No	Yes	Yes
Replay attack	No	Yes	Yes	Yes
Man in the middle attack	Yes	Yes	Yes	Yes
Disclosure of Session key	No	No	Yes	No
Offline password guessing attack	No	Yes	Yes	Yes
ID guessing attack	No	No	Yes	No
Privilege insider attack	Yes	Yes	Yes	Yes
Stolen smart card attack	No	No	Yes	No
Mutual authentication	Yes	Yes	Yes	Yes
Biometric renewability	two-factor scheme	two-factor scheme	two-factor scheme	No
Checking the accuracy of new password	No	No	No	No

VI. Conclusions

본 논문에서 Shin의 인증 기법을 분석한 결과, Shin의 인증 기법은 스마트카드 분실 공격에 취약하고, 이로 인하여 사용자의 가장 공격과 프라이버시 등을 보장할 수 없고, Shin이 강조하였던 사용자 익명성과 전방향 안전성도 보장할 수 없다. TMIS 환경에서 스마트카드 분실 공격이나 세션키 노출은 사용자들에게 매우 심각한 상황을 초래할 수 있다. 그러므로 Shin의 인증 기법은 TMIS를 위한 강력한 사용자 인증 기법이라고 말할 수 없다.

REFERENCES

[1] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, Issue. 11, pp. 770-772, Nov. 1981. DOI: 10.1145/358790.358797

[2] B. B. Gupta, V. Prajapati1, N. Nedjah, P. Vijayakumar, A. A. El-Latif, X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS)," Neural Computing and Applications, June 2021. 10.1007/s00521-021-06152-x

[3] 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. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09307564

[4] D. Dharminder, D. Mishra, and X. Li, "Construction of RSA-Based Authentication Scheme in Authorized Access to Healthcare Services," Journal of Medical Systems, Vol. 44, Article number. 6, pp. 1-9, Nov. 2020. DOI: 10.1007/s10916-019-1471-6

[5] C. T. Li, D. H. Shin, C. C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," Computer Methods and Programs in Biomedicine, Vol. 157, No. pp. 191-203, Apr. 2018. DOI: 10.1016/j.cmpb.2018.02.002

[6] D. Mahto, D and K. Yadav, "Cloud-based Secure TeleMedicine Information System using Crypto-Biometric Techniques," EAI Endorsed Transactions on Pervasive Health and Technology, Vol. 5, No. 20, pp. 1-11, Mar. 2020.

[7] O.S. Arezou, A.M. Dariush, 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

[8] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY, Vol. 8. pp. 350-353, Oct. 2005. http://ms11.voip.edu.tw/~xinfu/ref/ecdh.pdf

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

[10] S. Islam and M. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," Journal of Medical Systems, Vol. 38, No. 10, pp. 1-13, Sept. 2014. DOI: 0.1007/s10916-014-0135-9

[11] S.A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M. S. Farash, "Cryptanalysis and Improvement of an Improved Two Factor Authentication Scheme for Telecare Medicine Information Systems," Journal of Medical Systems, Vol. 39, No. 6, pp. 1-11, Apr. 2015. DOI: 10.1007/s10916-015-0244-0

[12] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," IEEE Access, Vol. 6, pp. 7452-7463, Mar. 2017. DOI: 10.1109/ACCESS.2017.2780124

[13] Kwangcheul Shin, "A Robust Authentication Scheme Based on ECC and Dynamic ID for Remote Telecare Medical Information Systems," Journal of Korean Institute of Information Technology, Vol. 17, No. 6, pp. 123-132, June 2019. DOI: 10.14801/jkiit.2019.17.6.123

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.