Journal of KIIT. Vol. 19, No. 10, pp. 67-77, Oct. 31, 2021. pISSN 1598-8619. eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.10.67

'스마트카드 기반의 사용자 인증에 관한 연구'의 분석 및 개선된 인증 기법

박 미 옥*

Analysis and Improvement Authentication Scheme of 'A Study on Smart-Card based User Authentication'

Mi-Og Park*

요 약

본 논문에서는 Lee가 제안한 스마트카드 기반의 사용자 인증 기법을 분석하고, Lee의 인증 기법의 취약점을 해결하기 위하여 이를 개선한 새로운 three-factor 인증 기법을 제안한다. 본 논문에서 Lee의 인증 기법을 분석한 결과, 공격자는 사용자의 ID와 패스워드 추측 공격을 할 수 있고, 이로 인하여 Lee의 인증 기법은 안전한 사용자 익명성과 전방향 안전성을 제공하지 못한다. 본 논문에서 제안하는 새로운 인증 기법은 이러한 문제점을 개선하기 위하여, RGR의 데이터를 서버의 비밀 키로 사인하여 저장하고, 사용자의 생체정보를 사용하여 스마트카드 분실 공격에 안전하도록 개선하였다. 그래서 공격자는 사용자의 ID와 패스워드 추측 공격에 성공할 수 없고, 이로 인하여 본 논문에서 제안하는 새로운 인증 기법은 사용자 익명성과 전방향 안전성, 그리고 사용자 가장 공격과 재생 공격 등에 안전하다.

Abstract

In this paper, we analyze Lee's proposed smart card-based user authentication scheme and propose a new three-factor authentication scheme that improves this to solve the Lee's weaknesses. As a result of analyzing Lee's authentication scheme in this paper, an attacker can do the user's ID and password guessing attack and due to this, Lee's authentication scheme does not provide safe user anonymity and forward secrecy. To improve this problem, the new authentication scheme proposed in this paper signs and stores RGR data with a server's secret key and uses user's biometric information to ensure safety against smart card loss attack. So, the attack cannot be successful the user's ID and password guessing attack and for this reason, the new authentication scheme proposed in this paper is secure for user anonymity, forward secrecy, and user impersonation attack and replay attack etc.

Keywords

insider attack, user anonymity, session key disclosure, smart-card, user authentication

* 성결대학교 컴퓨터공학과
- ORCID: https://orcid.org/0000-0002-2022-4875

· Received: Sep. 08, 2021, Revised: Oct. 19, 2021, Accepted: Oct. 22, 2021

· Corresponding Author: Mi-Og Park
Dept. of Computer Engineering, Sungkyul University, Anyang, Korea,
Tel.: +82-31-467-8426, Email: mopark777@hanmail.net

Ⅰ. 서 론

스마트카드 기반의 원격 사용자 인증 기법이란 스마트카드를 사용하여 원거리의 사용자를 인증하는 방식으로, 1981년 Lamport가 제시한 패스워드 기반의 인증 기법 [1]로부터 출발하여, 그 이후로 스마트카드를 이용한 다수의 원격 사용자 인증 기법들 [2]-[4]가 제안되었다. 스마트카드 기반의 사용자 인증 기법은 주로 사용자의 ID와 패스워드를 사용하여 원격 사용자를 인증하는 방식으로, 이러한 인증 기법을 two-factor 인증 기법이라고 한다. Two-factor 인증 기법은 three-factor 인증 기법으로 발전하여, 원격의료정보시스템(TMIS, Telecare Medical Information Systems)과 같은 의료 분야[5]-[11]에서도 활용되고 있다.

2013년에 Jiang 기법[5]는 TMIS 환경을 위한 two-factor 인증 기법을 제안하였고, 자신들의 인증 기법은 다양한 공격에 안전하다고 주장하였다. 그러나 Kumari 기법[6]은 Jiang 기법이 내부자 공격(Insider attack)과 스마트카드 분실 공격(Lost smart-card attack)에 취약하다고 분석하고, 이를 개선한 새로운 인증 기법을 제안하였다. Kumari 기법은 기존의 문제점을 해결하기 위해서 서버의 RGR(registration record)에 평문으로 저장했던 데이터를 서버의 비밀 키로 사인하여 저장하였다. 이로 인하여 내부 공격자가 서버의 비밀 키를 알아야 만이 사용자의 ID 획득이 가능하게 함으로써, 내부자 공격에 안전하다고 주장하였다.

또한 Kumari 기법은 TMIS 환경에서 중요한 사용자 익명성을 보장하기 위하여, 동적 ID AID를 사용하였고, 이 AID는 사용자의 ID와 새로운 난수 R*를 생성하여 Ex(ID ‖ R*)와 같이 대칭키로 암호화하였다. 그러나 2014년에 Kim-Lee 기법[7]은 Kumari 기법과 Das-Goswami 기법[8]이 모두 스마트카드 분실 공격에 취약하고 전방향 안전성(Forward secrecy)을 보장하지 못한다고 분석하였다.

2016년 Lee 등이 제안한 문헌[9]는 Kim-Lee 기법에서와 동일하게 Kumari 기법이 전방향 안전성과 스마트카드 분실 공격에 안전하지 않다고 분석하고, 이러한 문제점을 해결하기 위하여 대칭키 기반의 새로운 인증 기법을 제안하였다. Lee 등이 제안한 문헌[9]는 사용자의 익명성 기능도 보장한다고 주장하였다. 2017년 Moon 기법[10]은 문헌[9]에 대한 안전성을 분석하여, 문헌[9]의 인증 기법이 ID 추측 공격(Guessing attack)과 패스워드 추측 공격에 안전하지 않음을 보였다. 이로 인하여 공격자가 사용자와 서버의 세션 키 생성이 가능하다고 분석하였다.

또한 Moon 기법이 분석한 문제점 중의 하나는 서버에서 사용자를 검증하기 위해서 사용자의 ID를 계산해낼 수 있어야 하는데, 서버에서 사용자의 ID를 계산해낼 수 없는 문제가 존재한다고 분석하였다. Moon 기법은 이러한 문제들을 해결하기 위하여, 대칭 키 기반의 새로운 인증 기법을 제안하면서, 패스워드 추측 공격, 스마트카드 분실 공격, 그리고 내부자 공격에 안전하고, 사용자 익명성과 전방향 안전성 등을 보장한다고 주장하였다.

2018년 Lee 기법[11]은 문헌[9]에 대한 취약점을 언급하면서, 문헌[9]의 기법이 스마트카드를 분실하였을 경우, 공격자가 사용자의 ID와 패스워드를 쉽게 획득할 수 있다는 문제점을 언급하였다. Lee 기법은 이러한 문제점을 해결하기 위하여, 사용자의 ID와 패스워드를 하나의 식에 함께 사용하여, 사용자의 ID가 노출된다하더라도 사용자의 패스워드는 노출되지 않는다고 주장하였다. 또한 Lee 기법은 RGR에 저장하는 데이터를 {IDi⊕x, Ri, IDi‖x}처럼 변경하여 저장하였다.

그러나 본 논문에서 Lee 기법을 분석한 결과, RGR의 변경된 {IDi‖x} 형태가 Lee 기법의 안전성을 더욱 침해하였다. 이로 인하여 공격자가 RGR의 정보 획득에 성공할 경우, 사용자의 IDi와 함께 저장된 서버의 비밀 키까지도 손쉽게 획득 가능하였다. 또한 공격자가 사용자의 IDi를 획득할 경우, 스마트카드 분실 공격 등을 통해 패스워드 추측 공격과 가장 공격 등 다양한 공격에 취약하고, Lee 기법에서 강조한 사용자 익명성과 전방향 안전성도 제공하지 못하였다. 본 논문에서는 이러한 Lee 기법의 문제점을 해결하기 위해서, 사용자의 생체정보를 사용하는 새로운 three-factor 인증 기법을 제안한다. 제안한 인증 기법은 본 논문에서 분석한 결과, 스마트카드 분실공격에 안전하여 사용자의 ID와 패스워드 추측 공격, 사용자 가장 공격과 내부자 공격 등에도 안전하다. 또한, 본 논문에서 제안한 인증 기

법은 동적 ID를 간단히 계산하도록 개선하여, Lee 기법의 사용자 ID 검색 오버헤드 문제를 해결하고 사용자에게 안전한 익명성을 제공한다.

본 논문의 구성은 먼저 2장에서 Lee가 제안한 인증 기법에 대해 살펴보고, 3장에서는 Lee의 인증 기법에 대해 분석한다. 그리고 4장에서는 Lee의 기법을 개선한 새로운 three-factor 인증 기법을 제안한다. 5장은 제안한 인증 기법에 대한 안전성을 분석하고, 6장에서 결론을 내리고 본 논문을 마친다.

II. 관련 연구

2.1 Lee의 인증 기법

본 절에서는 Lee가 제안한 인증 기법의 등록 단계와 로그인 단계, 그리고 서버의 인증 단계를 살펴본다. 표 1은 본 논문에서 사용한 기호들이다.

2.1.1 등록 단계

1. 사용자는 자신의 IDi, 패스워드 PWi, 그리고 난수 ri를 생성한다.
2. 사용자는 자신의 패스워드 PWi와 난수 ri를 이용하여 RPWi=h(ri||PWi)를 해시연산하고, 안전한 채널을 통해 자신의 IDi와 RPWi를 서버로 전송한다.
3. 사용자의 IDi와 PRWi를 전송받은 서버는 사용자 IDi의 타당성을 확인하고, 등록 요청한 횟수인 Ni에 값을 부여한다. 만약 첫 등록이라면 Ni=0을 등록하고, 재등록은 Ni=Ni+1 값을 부여한다.
4. 서버는 사용자의 IDi, RPWi, Ni, 서버가 생성한 난수 b, 그리고 서버의 비밀 키 x를 이용하여 다음 값들을 계산한 후, RGR에 {IDi⊕x, Ni, IDi||x}를 저장한다.
   $Ji=h(x||IDi\oplus x||Ni)$, $Qi=h(IDi||x)\oplus RPWi$
   $Yi=h(RPWi||IDi\oplus x)$, $Ri=h(b||x)\oplus h(IDi||x)$
   $Li=Ji\oplus h(RPWi)\oplus h(b||x)$, $Ai=Li\oplus h((IDi||x)\oplus h(b||x))$
   $Mi=h(Ji||RPWi||IDi)$, $AIDi=Ex((IDi\oplus x)\oplus h(Yi||b))$
5. 서버는 {Ri, Ai, AIDi, Mi, h(·), Ek, Dk}를 스마트카드에 저장하고, 스마트카드와 앞에서 계산한 Qi를 안전한 채널을 통해 사용자에게 전송한다.

표 1. 본 논문에서 사용된 기호들
Table 1. Symbols used in this paper

IDi	User Ui's identity
S	Remote server
PWi	Ui's password
RGR	Registration recode
Ni	Number of times Ui register with the server
ri	Random number of the user Ui
x	Secret key of the server S
b	Random number of the server S
Ek, Dk	Encryption/Decryption with k
h(.)	Secure one way hash function
T	Time stamp
⊕	Exclusive-OR operation
||	Concatenation operation

6. 스마트카드와 Qi를 수신한 임의 사용자는 $Ki=h(IDi||PWi)\oplus ri$와 $Bi=Qi\oplus ri$를 계산하여 스마트카드에 추가로 저장한다.

2.1.2 로그인 단계

1. 사용자는 스마트카드 SC를 카드 리더기에 넣고 자신의 IDi와 패스워드 PWi를 입력한다.
2. 스마트카드 SC는 사용자의 IDi와 패스워드 PWi, 그리고 SC의 저장 데이터 Ki를 이용하여 $ri^*=Ki\oplus h(IDi||PWi)$와 $RPWi^*= h(ri^*||PWi)$를 계산한다.
3. 계산된 RPWi*와 ri*, 그리고 스마트카드에 저장된 Bi를 이용하여 다음 값들을 계산한다.
   $h(IDi||x)^*=Bi\oplus RPWi^*\oplus ri^*, h(b||x)^*=Ri\oplus h(IDi||x)^*$
   $Li^*=Ai\oplus h(IDi||x)^*\oplus h(b||x)^*$
   $Ji^*=Li^*\oplus h(RPWi^*)\oplus h(b||x)^*$
   $Mi^*=h(Ji^*||RPWi^*||IDi)$
4. 계산 결과값 Mi*와 스마트카드의 저장 데이터 Mi의 값을 비교하여, 두 값이 같으면 타임스탬프 Ti를 생성하여 $Ci=h(Ti||Ji^*)$를 계산한다. 만약 값이 같지 않으면 여기서 세션을 종료한다.
5. 사용자는 서버에게 로그인 요청 메시지 {AIDi, Ti, RPWi, Ci}를 보낸다.

2.1.3 인증 단계

1. 로그인 요청 메시지 {AIDi, Ti, RPWi, Ci}를 전송받은 서버는 타임스탬프 $T'-Ti\leq\Delta T$를 확인하여 적절한 값인지 확인한다. 만약 적절하지 않을 경

우, 여기서 세션을 종료한다. T'는 로그인 요청 메시지를 전송받은 시점의 타임스탬프를 의미한다.

2. 서버는 전송받은 RPWi와 RGR의 저장 데이터 IDi⊕x를 이용하여 Yi*=h(RPWi||IDi⊕x)를 계산한 후, 계산한 Yi*와 난수 b, 그리고 서버의 비밀 키 x를 이용하여 (IDi⊕x)⊕h(Yi*||b)를 계산한다. 이렇게 계산된 값은 전송받은 AIDi를 복호화 한 값과 같은지의 여부를 확인하여, 만약, 두 값이 같으면 Ji*=h(x||IDi⊕x||Ni)를 계산하고, 계산 결과값 Ji*와 전송받은 Ti를 이용하여 Ci*=h(Ti||Ji*)를 계산한다.
3. 서버는 앞 단계에서 계산한 Ci*와 전송받은 Ci가 같은지 확인하여, 두 값이 같을 경우 AIDi*=Ex((IDi⊕x)⊕h(Yi*||b))를 계산하고, 타임스탬프 Ts를 생성하여 Cms=EJi*(AIDi*||Ci||Ts)를 계산한다. 만약 두 값이 같지 않을 경우, 여기서 세션을 종료한다.
4. 서버는 사용자에게 {Cms, Ts}를 전송한다.
5. {Cms, Ts}를 전송받은 사용자는 AIDi||Ci||Ts를 계산하고, 이 값이 서버로부터 전송받은 Cms를 복호화한 결과 값과 같은지 확인한다. 또한 전송받은 Cms를 복호화 한 시점의 타임스탬프 T''를 이용해, T''-Ts≤ΔT를 확인한다. 만약 두 조건이 맞지 않으면, 세션은 여기서 종료한다.
6. 사용자는 복호화해서 얻은 Ci*과 로그인 단계에서 자신이 계산한 Ci를 비교하여 두 값이 같을 경우, AIDi*과 AIDi가 같은지 확인한다. 만일, 두 값이 다를 경우 AIDi를 AIDi*로 대체한다.

그림 1은 Lee 기법의 로그인 단계와 인증 단계를 나타낸 것이다.

III. Lee의 인증 기법에 대한 분석

본 논문에서는 Lee가 미분석한 내부자 공격의 분석을 통해, 사용자의 IDi 뿐만 아니라 서버의 비밀 키까지도 손쉽게 획득 가능함을 보인다. 이로 인하여 Lee 기법은 Lee가 강조한 사용자 익명성과 전방향 안전성을 보장하지 못하며, 가장 공격과 스마트 카드 분실 공격 등에도 취약하다.

3.1 내용상 오류와 ID 검색 오버헤드

본 절에서는 Lee 기법에 존재하는 내용상의 오류와 서버에서 사용자 IDi를 검색하는 오버헤드 문제에 대하여 먼저 분석한다.

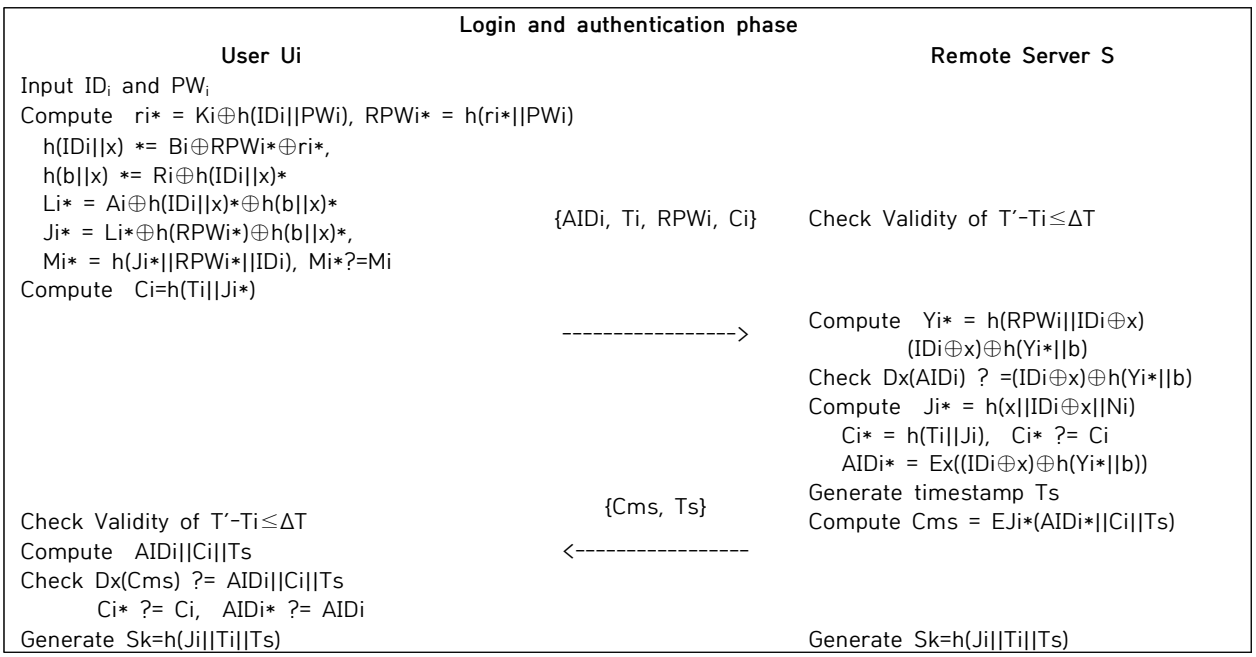

그림 1. Lee의 로그인과 인증 단계
Fig. 1. Lee's login and authentication phase

3.1.1 RGR에서 난수 b의 누락

Lee 기법은 서버에서 사용자로부터 전송받은 메시지가 AIDi와 같은 값인지 비교하기 위하여, (IDi⊕x)⊕h(Yi*||b)를 계산한다. 그러나 RGR에 {IDi⊕x, Ni, IDi||x}만 저장되어 있기 때문에 난수 b를 알 수 없는 서버는 (IDi⊕x)⊕h(Yi*||b)를 계산할 수 없다. 그러므로 Lee 기법의 RGR에는 난수 b가 저장되어 있어야 한다.

3.1.2 새로운 난수 b를 사용하지 않는 문제

Lee 기법은 동적 ID의 기능을 제공하기 위해서 AIDi를 구성하는 난수 b를 매 세션마다 새롭게 생성해야한다. 그러나 서버는 새로운 난수에 대한 언급이 없이, 난수 b를 사용한다고만 되어있다. 다른 인증 기법들[5][6]처럼 AIDi가 동적 기능을 제대로 하려면, 서버에서 새로운 난수를 생성해야 한다. 그렇지 않을 경우, 항상 동일한 AIDi로 인하여 사용자 익명성을 안전하게 보장할 수 없다.

3.1.3 인증단계 5의 설계 오류

Lee의 인증단계 5는 타임스탬프와 Cms의 두 조건이 만족하지 않을 경우, 세션을 종료한다. 그런데 Lee 기법은 설계오류가 없는 상태라면, AIDi가 매번 변하기 때문에 새로운 AIDi*를 이용하여 계산한 Cms 값은 사용자가 계산한 Cms 값과 매번 다르게 된다. 매번 Cms가 달라지기 때문에 인증단계 6에서 자신이 계산한 AIDi||Ci||Ts에서 Ci 값을 비교하여 사용자가 전송한 값과 서버에서 보내준 값이 일치하는지 비교하는 것이다. 이 값이 일치하면 서버를 인증하고 변경된 새로운 AIDi*를 이용하여 기존의 AIDi를 업데이트한다. 그러므로 Lee의 인증단계 5는 두 조건을 만족하지 않았을 경우, 세션을 종료하는 것이 아니라 타임스탬프가 조건을 만족하지 않을 경우에만 세션을 종료해야 한다. 그리고 타당한 타임스탬프일 경우에는 Cms의 복호화를 진행하는 것으로 수정되어야 인증단계 6을 실행할 수 있다. 이와 같은 설계오류는 본 논문에서 분석한 결과 문헌 [9]의 인증단계에도 동일하게 존재하였다.

3.1.4 사용자 ID 검색의 오버헤드

문헌 [9]는 로그인 요청 메시지 AIDi와 서버에 저장된 값들로 사용자의 IDi를 계산해낼 수 없는 문제가 있으며, Lee 기법은 사용자로부터 전송받은 AIDi로부터 사용자의 IDi를 곧바로 계산해낼 수 없는 문제가 존재한다. Lee 기법의 인증 단계는 먼저 타임스탬프를 체크한 후에 곧바로 Yi*=h(RPWi||IDi⊕x)를 계산한다. RPWi는 로그인 요청 메시지이고, RGR에 저장된 여러 IDi⊕x 값들 중 어떤 값이 로그인 요청 메시지를 보낸 해당 사용자인지 알 수 없기 때문에 저장된 모든 IDi⊕x 값들과 전송받은 RPWi를 가지고 Yi*=h(RPWi||IDi⊕x)를 계산한다. 그런 다음 저장된 난수 b와 (IDi⊕x)⊕h(Yi*||b)를 계산한 후에, 이 값이 AIDi를 복호화 한 값과 동일한지 체크한 후에야 해당하는 IDi가 무엇인지 알 수 있다. 그러므로 XOR 연산과 같이 간단히 사용자의 IDi를 계산해내는 다른 인증 기법들과 달리, Lee 기법은 사용자의 IDi를 찾을 때까지의 계산 오버헤드가 상대적으로 큰 편이다.

표 2는 본 논문에서 Lee 기법과 관련성이 높은 다른 인증 기법들의 연산 횟수를 비교한 것으로, Ex와 Dx는 각각 비밀 키 x로 암ㆍ복호화의 횟수를 나타내는 것으로 결국 Ts와 동일한 연산을 나타낸다. Tid는 각 인증 방식에서 사용자의 IDi를 검색하는 시간으로, 인증 단계에서는 Tid로 단순히 표기하였으나 총 연산 횟수를 나타낼 때는 Tid를 실제 필요한 연산 횟수로 변경하여 표기하였다.

표 2. 본 논문에서 분석한 인증 기법들의 연산 비교

Table 2. Computation comparison of authentication schemes analyzed in this paper

Phase and computation	Jiang [5]	Kumari [6]	Reference [9]	Lee [11]
Registration phase	2Th+Ex	4Th+Ex	10Th+Ex	8Th+Ex
Login phase	3Th+Ex	3Th	6Th	5Th
Authentication phase	3Th+2Ex+Dx	4Th+2Ex+2Dx	6Th+2Ex+2Dx+Tid	7Th+2Ex+2Dx+Tid
Total computation	8Th+5Ts	11Th+5Ts	12Th+5Ts+N*2Th	12Th+5Ts+N*2Th

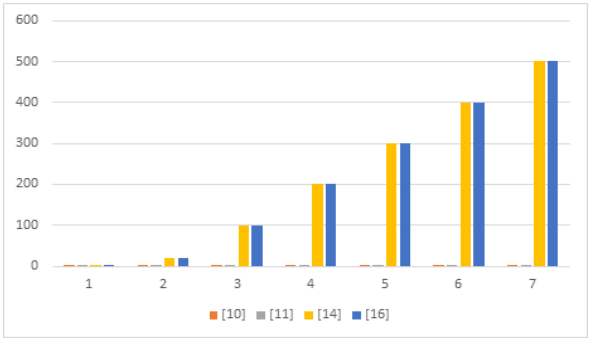

그림 2. 사용자 ID 검색의 복잡도
Fig. 2. Complexity of user ID search

그림 2는 사용자 수가 증가함에 따라 서버에서 사용자 ID 검색 시간의 증가를 간단히 비교한 것이다.

3.2 안전성 분석

3.2.1 내부자 공격

Lee 기법은 등록 단계에서 RGR에 {IDi⊕x, Ni, IDi||x}를 평문으로 저장한다. 만약 공격자가 RGR에 저장된 데이터 획득에 성공하였을 경우, 공격자는 사용자의 IDi 획득을 위해 다음 과정을 수행한다.

1. {IDi||x}의 전체 길이가 n일 경우, 처음 한 자리는 IDi의 값이라 가정하면, 나머지 n-1 길이의 값은 서버의 비밀 키 x가 된다. 이 과정을 다시 수행할 때는 IDi의 자리 수 i를 한 자리씩 늘려가고, 서버의 비밀 키를 나타내는 나머지 길이는 한 자리씩 길이가 줄어들어 n-i가 되게 한다.
2. 전체 길이 n 중 앞에서부터 i 자리수를 차지하는 사용자의 ID' 값과 나머지 자리 수 n-i를 차지하는 서버의 비밀 키 x' 값을 IDi'⊕x'를 계산하여, RGR에서 획득한 {IDi⊕x}와 비교한다. 비교결과가 같은 값이 나오면, 올바른 ID'와 x'일 확률이 높으므로 여기서 과정을 마치고, 값이 다를 경우 1번 단계로 가서 반복한다.
3. 2번 단계에서 {IDi⊕x}와 비교하여 같은 결과가 나왔다고 해도, 올바른 ID와 x 값이 아닐 수도 있다. 이럴 경우에는 RGR에서 획득한 ID', x', Yi', 그리고 b'를 가지고 ((IDi'⊕x')⊕h(Yi'||b')를 계산한 후 서버의 비밀 키 x'로 로그인 요청 메시지 AIDi를 복호화 한 결과 값 (IDi⊕x)⊕h(Yi||b)와 같은지 비교한다. 두 값이 같으면, 획득한 두 값이 모두 정확하다는 의미이다. 여기서 Yi의 계산은 h(RPWi||IDi⊕x)이기 때문에, 획득한 ID', x', 그리고 RPWi를 사용하여 계산가능하다.

3.2.2 스마트카드 분실 공격

스마트카드를 획득한 공격자는 다음 시나리오에 따라 사용자의 IDi와 PWi를 추측 공격한다.

1. 임의의 IDia와 PWia를 추측하여, 스마트카드의 Ki를 이용해 난수 ria=Ki⊕h(IDia||PWia)를 계산한다. 이 과정에서 ria가 올바른 값인지 확인하기 위해서, RPWi를 이용해 RPWi ?=h(ria||PWia)가 동일한 값인지 확인할 수 있다. Lee는 사용자의 IDi와 PWi를 하나의 식에 사용하여 추측 공격에 대한 저항성을 가진다고 하였으나, IDi와 PWi는 둘 다 낮은 엔트로피이기 때문에 시간 복잡도 $O(|D_{ID}|*|D_{PW}|*Th)$로 다항식 시간 안에 추측 공격이 가능하다[12][13]. 여기서 $|D_{ID}|$는 space ID의 수, $|D_{PW}|$는 space PW의 수를 나타내고, Th는 해시함수의 연산 횟수를 나타낸다.
2. 로그인 요청 메시지 RPWi와 스마트카드의 저장 데이터 Bi, 그리고 난수 ria를 이용해 h(IDi||x)a=Bi⊕RPWi⊕ria를 계산한다.
3. h(b||x)를 계산하기 위해서 스마트카드의 Ri와 h(IDi||x)a를 이용하여 h(b||x)a=Ri⊕h(IDi||x)a를 계산한다.
4. Li를 계산하기 위해서, h(b||x)a, h(IDi||x)a, 그리고 스마트카드의 Ai를 이용해 Lia=Ai⊕h(IDi||x)a⊕h(b||x)a 계산한다.
5. Ji를 계산하기 위해서, RPWi, h(b||x)a, Lia를 이용해 Jia=Lia⊕h(RPWi)⊕h(b||x)a를 계산한다.
6. RPWi, Jia, 앞에서 추측한 IDia를 이용해 h(Jia||RPWi|| IDia)를 계산한 후, 스마트카드의 Mi와 비교한다. 두 값이 같을 경우, 여기서 과정을 마치고, 다를 경우 1번으로 가서 두 값이 동일할 때까지 반복한다.

3.2.3 가장 공격

공격자가 정당한 사용자로 가장하려면 로그인 요청 메시지 {AIDi, Tia, RPWi, Cia}를 생성할 수 있어야한다. 앞에서 제시한 시나리오를 통해 공격자는 Lee 기법의 핵심인 Ji를 획득 가능하고, 로그인 요청 메시지의 Ci를 제외한 나머지는 모두 공공 채널상에서 획득한 값을 사용하면 된다. 그러나 Ci의 계산도 Ji와 타임스탬프 Ti로 구성되기 때문에, 공격자는 새로운 타임스탬프 Tia와 Cia=h(Tia||Ji*)를 계산하여 새로운 로그인 요청 메시지 {AIDi, Tia, RPWi, Cia}를 서버에 보낼 수 있다. 또한 Lee 기법은 사용자의 IDi 뿐만 아니라 서버의 비밀 키 x를 획득할 수 있고, RGR에 저장된 데이터를 함께 사용할 경우, 정당한 서버로 가장할 수 있다.

3.2.4 세션 키 노출

Lee의 세션 키는 Sk=h(Ji||Ti||Ts)이고, Ti와 Ts는 타임스탬프로 쉽게 획득가능하고, Ji는 h(x||IDi⊕x||Ni)로 구성되기 때문에 서버의 비밀 키 x*를 안다고 가정할 경우, 사용자의 IDi는 서버의 비밀 키 x*와 한번의 XOR 연산에 의해 획득가능하다. Ni는 등록요청 횟수를 나타내므로 값을 증가시키는 반복을 통하여 추측할 수 있다. 그래서 공격자는 앞에서 획득한 타임스탬프와 Ji*를 사용해서 이전의 세션 키 h((Ji*||Ti||Ts)를 계산할 수 있다. 서버의 비밀 키를 모른다고 가정할 경우, 사용자측에서 Ji*의 계산은 Ai⊕h(IDi||x)*⊕h(b||x)*⊕h(RPWi*)⊕h(b||x)와 같고, 이 식은 Ji*=Ai⊕h(IDi||x)*⊕h(RPWi*)가 되기 때문에, 스마트카드 분실 공격에서 획득한 h(IDi||x)a를 h(IDi||x)* 대신에 사용하고, 스마트카드의 Ai와 RPWi를 사용하여 Ji*를 계산해 낼 수 있다. 그러므로 Lee의 기법은 세션 키 노출에 안전하지 않다.

Ⅳ. 개선된 새로운 three-factor 인증 기법

본 장에서는 본 논문에서 분석한 Lee 기법에 대한 문제점을 해결하기 위하여, 개선된 새로운 three-factor 인증 기법을 제안한다. 그림 3은 제안 기법의 로그인 단계와 인증 단계를 나타낸 것이다.

Login and authentication phase

User Ui		Remote Server S
Input ID_i, PW_i and Bio_i		
Compute ri* = Ki⊕h(IDi||PWi||Bioi)		
RPWi* = h(ri*||PWi)		
h(IDi||x)*=Bi⊕RPWi*⊕ri*		
h(b||x)* = Ri⊕h(IDi||x)*		
Li* = Ai⊕h(IDi||x)*⊕h(b||x)*		
Ji* = Li*⊕h(RPWi*)⊕h(b||x)*		
Mi* = h(Ji*⊕RPWi*⊕IDi)		
Check Mi*?=Mi, compute Ci=h(Ti||Ji*)	{AIDi, Ti, RPWi, Ci}	Check Validity of T′-Ti≤ΔT
	---------->	Compute Dx(AIDi)
		Extract IDi, check the format of IDi
		Compute Yi* = h(RPWi||IDi⊕x)
		Check Dx(AIDi)?=(IDi||h((IDi⊕x)⊕h(Yi*||b)
		Compute Ji* = h(x||IDi⊕x||Ni)
		Ci* = h(Ti||Ji), Ci* ?= Ci
		Generate new random number b
		Compute AIDi*=Ex((IDi||h((IDi⊕x)⊕h(Yi*||b))
		Generate time stamp Ts
Check Validity of T′-Ti≤ΔT	{Cms, Ts}	Compute Cms = EJi*(AIDi*||Ci||Ts)
Compute AIDi||Ci||Ts, Dx(Cms)	<----------	
Check Ci* ?= Ci, AIDi* ?= AIDi		
Generate Sk=h(Ji||Ti||Ts||IDi)		Generate Sk=h(Ji||Ti||Ts||IDi)

그림 3. 제안 기법의 로그인과 인증 단계
Fig. 3. Login and authentication phase of proposed authentication scheme

4.1 등록 단계

1. 사용자는 자신의 IDi, 패스워드 PWi, 그리고 난수 ri를 생성한다.
2. 사용자는 자신의 패스워드 PWi와 난수 ri를 이용하여 RPWi=h(ri||PWi)를 해시연산하고, 안전한 채널을 통해 자신의 IDi와 RPWi를 서버로 전송한다.
3. 사용자의 IDi와 PRWi를 전송받은 서버는 사용자 IDi의 타당성을 확인하고, 사용자가 서버에 등록을 요청한 횟수인 Ni에 값을 부여한다. 만약 첫 등록이라면 Ni=0을 저장하고, 재등록이라면 Ni=Ni+1 값을 부여하여 값을 증가시킨다.
4. 서버는 사용자의 IDi, RPWi, Ni, 서버가 생성한 난수 b, 그리고 서버의 비밀 키 x를 이용하여 다음 값들을 계산한다.

   $Ji = h(x||IDi \oplus x||Ni)$, $Qi = h(IDi||x) \oplus RPWi$

   $Yi = h(RPWi||IDi \oplus x)$, $Ri = h(b||x) \oplus h(IDi||x)$

   $Li = Ji \oplus h(RPWi) \oplus h(b||x)$

   $Ai = Li \oplus h((IDi||x) \oplus h(b||x))$

   $Mi^* = h(Ji^* \oplus RPWi^* \oplus IDi)$

   $AIDi = Ex((IDi||h(IDi \oplus x) \oplus h(Yi||b))$

   서버는 자신의 비밀 키를 사용하여 RGR에 {IDi ⊕x, Ni, b, yi}를 저장한다.
5. 서버는 {Ri, Ai, AIDi, Mi, h(·), Ek, Dk}를 스마트카드에 저장하고, 안전한 채널을 통해 스마트카드와 앞에서 계산한 Qi를 사용자에게 전송한다.
6. 스마트카드와 Qi를 전송받은 사용자는 Ki와 Bi를 Ki=h(IDi||PWi||Bioi)⊕ri, Bi=Qi⊕ri와 같이 계산하여 스마트카드에 저장한다.

4.2 로그인 단계

1. 사용자는 스마트카드를 카드 리더기(Card reader)에 넣고 자신의 IDi와 PWi, 그리고 자신의 생체정보 Bioi를 입력한다.
2. 스마트카드는 사용자의 IDi와 PWi, Bioi, 그리고 스마트카드에 저장되어 있는 Ki를 사용하여 다음을 계산한다.

   $ri^* = Ki \oplus h(IDi||PWi||Bioi)$, $RPWi^* = h(ri^*||PWi)$.
3. 앞에서 계산한 ri*와 RPWi* 그리고 스마트카드에 저장되어 있는 Bi를 이용하여 다음 값들을 차례로 계산한다.

   $h(IDi||x)^* = Bi \oplus RPWi^* \oplus ri^*, h(b||x)^* = Ri \oplus h(IDi||x)^*$

   $Li^* = Ai \oplus h(IDi||x)^* \oplus h(b||x)^*$

   $Ji^* = Li^* \oplus h(RPWi^*) \oplus h(b||x)^*$

   $Mi^* = h(Ji^* \oplus RPWi^* \oplus IDi)$
4. 스마트카드에 저장되어 있는 Mi와 앞에서 계산한 Mi*를 비교하여, 두 값이 동일할 경우 타임스탬프 Ti를 생성하여 Ci=h(Ti||Ji*)를 계산한다. 만약 비교 결과가 동일하지 않을 경우, 세션을 종료한다.
5. 사용자는 서버에게 로그인을 요청하는 메시지 {AIDi, Ti, RPWi, Ci}를 서버에게 전송한다.

4.3 인증 단계

1. 로그인 요청 메시지를 전송 받은 서버는 타임스탬프 Ti가 $T'-Ti \leq \Delta T$의 조건을 만족하는지 먼저 체크하여, 조건을 만족할 경우 다음 과정을 진행한다. 만약 조건을 만족하지 않을 경우에는 여기서 세션을 종료한다.
2. 서버는 자신의 비밀 키 x를 사용하여 AIDi를 복호화하고, 그 결과 값 IDi||(h(IDi⊕x)⊕h(Yi*||b))로부터 사용자의 IDi를 추출해낸다. 그런 다음 사용자의 IDi 형식의 타당성을 체크한다. 만약 타당할 경우 전송받은 RPWi와 추출한 IDi를 이용하여 IDi⊕x를 계산하고, Yi*=h(RPWi||IDi⊕x)를 계산한다. 그런 다음 해당 IDi에 일치하는 난수 b를 사용하여 IDi||(h(IDi⊕x)⊕h(Yi*||b))를 계산하고, AIDi를 복호화 한 결과값 Dx(AIDi)과 동일한지 비교한다. 만약 두 값이 동일할 경우, Ji*=h(x||IDi⊕x||Ni)를 계산하고, 계산한 Ji*와 전송 받은 Ti를 이용하여 Ci*=h(Ti||Ji*)를 계산한다.
3. 서버는 자신이 계산한 Ci*와 전송 받은 Ci의 값을 비교하여, 두 값이 동일할 경우 새로운 난수 b*를 생성하여 AIDi*=Ex(IDi||(h(IDi⊕x)⊕h(Yi*||b))를 계산한다. 그런 다음 타임스탬프 Ts를 생성하여 Cms=EJi*(AIDi*||Ci||Ts)를 계산한다.
4. 서버는 응답 메시지 {Cms, Ts}를 사용자에게 전송한다.
5. 응답 메시지 {Cms, Ts}를 전송 받은 사용자는

타임스탬프 Ts가 T''-Ts≤ΔT의 조건을 만족하는지 체크한다. 만약 타당한 타임스탬프이면, 사용자는 AIDi||Ci||Ts를 계산하고, 전송받은 Cms를 복호화한다.

6. 사용자는 자신이 계산한 Ci와 복호화해서 얻은 Ci*를 비교하여 두 값이 같을 경우, AIDi*과 AIDi가 같은지 비교한다. 만약, 두 값이 다르면 기존의 AIDi를 전송받은 AIDi*로 업데이트한다.
7. 사용자와 서버는 각자 자신들이 계산한 Ji, Ti, Ts, 그리고 IDi를 사용하여 각자의 세션 키 Sk=h(Ji||Ti||Ts||IDi)를 생성한다.

V. 안전성 분석

본 장에서는 본 논문에서 제안한 새로운 three-factor 인증 기법에 대한 안전성 측면을 분석한다.

5.1 주요 공격에 대한 안전성 분석

5.1.1 스마트카드 분실 공격

스마트카드 분실 공격은 전송 메시지들과 스마트카드에 저장된 정보들을 사용한다고 가정한다. 먼저 공격자가 사용자의 패스워드를 획득하려면 전송 메시지 RPWi로부터 패스워드를 획득하거나 스마트카드의 Ki를 이용하여 ri*를 획득해야한다. 그러나 RPWi는 h(ri||PWi)처럼 해시함수로 계산되어있고, ri 값을 알려면 ri=Ki⊕h(IDi||PWi||Bioi)를 계산해야한다. 그러나 공격자가 스마트카드에 저장된 Ki를 안다고 할지라도 사용자의 생체정보 Bioi가 높은 엔트로피의 특징을 가지므로, 사용자의 IDi와 PWi를 계산하기 힘들다. 그로 인하여 공격자는 ri를 계산해 낼 수 없다. 그러므로 제안한 인증 기법은 스마트카드 분실 공격에 안전하다.

5.1.2 가장 공격

공격자가 사용자를 가장하기 위해서는 사용자의 IDi와 패스워드 PWi, 그리고 생체정보 Bioi를 알아야한다. 본 논문에서 제안한 인증 기법은 스마트카드 분실 공격 절에서 분석한 바와 같이, 로그인 요청 메시지와 분실된 스마트카드를 공격자가 획득한다 할지라도 사용자 가장 공격에 필요한 정보들을 획득할 수 없다. 또한 전송 메시지 RPWi는 난수 ri와 함께 해시연산 되어 있으므로, 높은 엔트로피의 난수 특성으로 인하여 패스워드 추측 공격에 안전하다. 사용자의 ID 추측 공격은 전송 메시지 Mi와 RPWi를 사용할 수 있으나, Mi의 구성 요소인 Ji는 스마트카드 분실 공격에 안전하다. 그러므로 기존의 Ji가 노출되었던 Lee 기법의 문제점을 해결하여 사용자의 IDi가 노출되는 것을 해결하였다. 또한 Mi의 구성 요소들을 기존의 연결 연산자 대신에, XOR 연산하여 공격에 더 안전하도록 구성하였다.

5.1.3 내부자 공격

제안한 인증 기법은 h(ri||PWi)를 등록 서버에 보내기 때문에 내부자 공격에 안전하다. 또한 제안한 인증 기법은 서버의 비밀 키를 사용하여 RGR의 데이터를 저장하기 때문에, 공격자가 서버의 비밀 키를 획득하기 전까지는 RGR의 데이터는 안전하다. 그러므로 제안한 인증 기법은 저장 데이터 측면에서도 내부 공격에 안전하다.

5.1.4 세션 키 노출

제안한 인증 기법에서 공격자가 세션 키를 알려면 Ji, Ti, Ts, 그리고 사용자의 IDi를 알아야 한다. 공격자는 타임스탬프 Ti와 Ts를 획득할 수 있지만, Ji와 IDi는 스마트카드 분실 공격과 ID 추측 공격에 안전하여 이 값을 획득하기 어렵다. 그러므로 제안한 인증 기법은 세션 키 노출 없이 안전하다.

5.1.5 재생 공격

제안한 인증 기법은 전송 메시지들에 서버와 사용자가 각각 생성한 타임스탬프 Ti와 Ts를 사용한다. 그리고 서버와 사용자는 메시지를 주고받을 때마다 타임스탬프의 임계값을 체크하여 타임스탬프의 타당성을 조사한다. 그러므로 제안한 인증 기법은 재생 공격에 안전하다.

표 3은 본 논문에서 제안한 인증 기법과 다른 인증기법들을 비교 분석한 결과로, 0은 해당 항목에 대한 안전성 기능을 제공하거나 해당 공격에 안전하다는 것을 나타낸다.

표 3. 인증 기법들의 안전성 분석 결과
Table 3. Analysis result of the authentication schemes

Type of attack	Kumari [6]	Reference [9]	Lee [11]	Proposed scheme
Insider attack	O	O	X	O
Session key disclosure	X	X	X	O
User anonymity	X	X	X	O
User impersonation attack	O	X	X	O
Server impersonation attack	O	O	X	O
Stolen smart card attack	X	X	X	O
ID guessing attack	O	X	X	O
Password guessing attack	O	X	X	O
Mutual authentication	O	O	X	O
Replay attack	O	O	O	O
Efficient ID search time	O	X	X	O

Ⅵ. 결 론

본 논문에서는 Lee 기법의 문제점을 분석하고, 이 문제점을 해결하기 위하여 개선된 three-factor 인증 기법을 제안하였다. 본 논문에서 분석한 Lee 기법의 문제점들 중 사용자 ID 검색 오버헤드 문제를, 제안한 인증 기법에서는 서버가 복호화만 실행하면 사용자의 ID를 곧바로 추출해 낼 수 있도록 개선하였다. 또한 RGR의 데이터를 서버의 비밀 키로 사인하여 저장하고, RGR의 저장 데이터 형태도 안전하게 변경하였다. 이로 인하여 제안한 인증 기법은 사용자의 ID와 서버의 비밀 키가 손쉽게 노출되는 기존의 문제점도 해결하였다.

또한 본 논문의 제안 기법은 스마트카드분실 공격에 안전하고, 이로 인하여 사용자 가장 공격, 재생 공격, 세션 키 노출 등의 위험에도 안전한 것으로 분석되었다. 그리고 항상 동일한 동적 ID 값을 가졌던 Lee 기법의 문제점을 해결하여, 제안한 인증 기법은 사용자에게 안전한 익명성을 제공한다. 그러므로 제안한 인증 기법은 사용자의 프라이버시(Privacy)와 중요한 의료정보를 다루는 TMIS 환경에서 안전한 사용자 익명성을 보장하는 개선된 인증 기법이라고 할 수 있다.

References

[1] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, Vol. 24, No. 11, pp. 770-772, Nov. 1981. https://doi.org/10.1145/358790.358797.

[2] B. M.. Suh and Y. S. Lee, "An Improved User Authentication Scheme Based on Random Nonce and Timestamp", Journal of Korean Institute of Next Generation Computing, Vol. 8, No. 6, pp. 69-76, Dec. 2012. https://www.earticle.net/Article/A189845.

[3] M. O. Park, "Vulnerability Analysis of 'A Remote User Authentication Scheme with Anonymity for Mobile Devices", Journal of Korean Institute of Next Generation Computing, Vol. 10, No. 6, pp. 6-13, Dec. 2014. http://dx.doi.org/10.5772/50912.

[4] H. J. Park and Y. H. Lee, "Survey on Privacy-preserving Techniques for Biometric Authentication", Journal of Korean Institute of Information Technology, Vol. 16, No. 4, pp. 109-122, Apr. 2018. http://dx.doi.org/10.14801/jkiit.2018.16.4.109.

[5] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A Privacy Enhanced Authentication Scheme for Telecare Medical Information Systems", Journal of Medical Systems, Vol. 37, No. 1, pp. 1-18, Jan. 2013. https://10.1007/s10916-012-9897-0.

[6] S. Kumari, M.K. Khan, and R. Kumar, "Cryptanalysis and Improvement of 'A Privacy

Enhanced Scheme for Telecare Medical Information System'", Journal of Medical Systems, Vol. 37, No. 4, pp. 1-11, Aug. 2013. https://doi.org/10.1007/s10916-013-9952-5.

[7] K. W. Kim and J. D. Lee, "On the Security of Two Remote User Authentication Schemes for Telecare Medical Information Systems", Journal of Computer Communications, Vol. 38, No. 5, pp. 1-11, Apr. 2014. https://doi.org/10.1007/s10916-014-0017-1.

[8] A. K. Das and A. Goswami, "A secure efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care", Journal of Medical Systems, Vol. 37, No. 3, Jun. 2013. https://doi.org/10.1007/s10916-013-9948-1.

[9] S. Y. Lee, K. S. Park, Y. H. Park, and Y. H. Park, "Symmetric Key-Based Remote User Authentication Scheme With Forward Secrecy", Journal of Korea Multimedia Society, Vol. 19, No. 3, pp. 585-594, Mar. 2016. http://dx.doi.org/10.9717/kmms.2016.19.3.585.

[10] J. H. Moon and D. H. Won, "An Enhanced Symmetric Key-Based Remote User Authentication Scheme with Forward Secrecy", Journal of Korea Multimedia Society, Vol. 20, No. 3, pp. 500-510, Mar. 2017. http://dx.doi.org/10.9717/kmms.2017.20.3.500.

[11] J. Y. Lee, "A Study on Smart-Card Based User Authentication", Journal of the Korea Society of Digital Industry and Information Management, Vol. 14, No. 2, pp. 27-33, Jun. 2018. https://doi.org/10.17662/ksdim.2018.14.2.027.

[12] S. Qiu, G. Xu, H. Ahmad, G. Xu, X. Qiu, and H. Xu, "An Improved Lightweight Two-Factor Authentication and Key Agreement Protocol with Dynamic Identity Based on Elliptic Curve Cryptography", KSII Transactions on Internet and Information Systems, Vol. 13, No. 2, pp. 978-1002, Feb. 2019. https://doi.org/10.3837/tiis.2019.02.027.

[13] D. Wang, Z. Zhang, and P. Wang, "Targeted online password guessing: An underestimated threat", in Proc. of ACM CCS, Vienna Austria, Vol. 16, pp. 1242-1254, Oct. 2016. https://doi.org/10.1145/2976749.2978339.

저자소개

박 미 옥 (Mi-Og Park)

1993년 2월 : 숭실대학교 컴퓨터학과(공학석사)
2004년 8월 : 숭실대학교 컴퓨터학과(공학박사)
2005년 ~ 현재 : 성결대학교 컴퓨터공학과
관심분야 : 모바일 보안/시큐리티 프로토콜, IoT 보안