JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 7, pp. 67-75, July 2023
https://doi.org/10.9708/jksci.2023.28.07.067

Analysis and Improvement of Andola et al.'s Dynamic ID based User Authentication Scheme

Mi-Og Park*

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

[Abstract]

In this paper, we analyze the problem of the user authentication scheme that provides dynamic ID in a multi-server environment proposed by Andola et al. and propose an improved authentication one to solve this problem. As a result of analyzing the authentication scheme of Andrea et al. in this paper, it is not safe for smart card loss attack, and this attack allows users to guess passwords, and eventually, the attacker was able to generate session key. This paper proposed an improved authentication scheme to solve these problems, and as a result of safety analysis, it was safe from various attacks such as smart card loss attack, password guess attack, and user impersonation attack. Also the improved authentication scheme not only provides a secure dynamic ID, but is also effective in terms of the computational complexity of the hash function. In addition, the improved authentication scheme does not significantly increase the amount of transmission, so it can be said to be an efficient authentication scheme in terms of transmission cost.

▸ **Key words**: Multi-server, Authentication, Dynamic ID, Anonymity, Stolen Smart-card attack

[요 약]

본 논문에서는 Andola 등이 제안한 멀티서버 환경에서 동적 ID를 제공하는 사용자 인증 방식에 대한 안전성과 설계상의 문제점을 분석한다. 본 논문에서 Andola 등의 인증 방식을 분석한 결과, 스마트카드 분실 공격에 안전하지 않고, 이 공격으로 인하여 사용자의 패스워드 추측 공격이 가능하고, 결국 공격자는 세션키까지 생성할 수 있다. 본 논문에서는 이러한 문제를 해결하기 위해서 개선된 인증 방식을 제안하고, 이에 대한 안전성 분석한 결과 스마트카드 분실 공격, 패스워드 추측 공격, 사용자 가장 공격 등 여러 공격에 안전하였다. 또한 개선된 인증 방식은 안전한 동적 ID를 제공할 뿐만 아니라 해시함수의 계산 복잡도 측면에서도 효율적이다. 게다가 개선된 인증 방식은 전송량도 크게 증가하지 않아 전송비용의 측면에서도 효율적인 인증 방식이라고 할 수 있다.

▸ **주제어**: 멀티 서버, 인증, 동적 ID, 익명성, 스마트카드 분실 공격

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@daum.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2023. 05. 10, Revised: 2023. 06. 28, Accepted: 2023. 07. 17.

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

I. Introduction

1981년 Lamport[1]가 원거리의 사용자 인증 방식을 제안한 이후로 사용자의 ID와 패스워드를 이용한 많은 사용자 인증 방식들이 제안되어 오고 있으며, 원격 의료 진료 시스템(Telecare Medical Information Systems), IoT, 클라우드 환경 등에서의 사용자 인증 방식 등 그 활용 분야도 다양하다. 본 논문에서 살펴보는 관련 인증 방식 중 Chang 등[2]는 2013년에 사용자의 프라이버시를 위하여 동적 ID를 이용하는 인증 방식을 제안하였다. 이들의 인증 방식은 2009년에 Wang 등[3]이 제안한 인증 방식의 문제점들을 분석하고 이를 개선한 방식으로, Wang 등의 인증 방식이 사용자 가장 공격과 사용자의 추적 가능성(traceability), 그리고 패스워드 변경 단계의 문제가 있음을 보였다. Wang 등의 패스워드 변경 단계의 문제점이란 처음에는 패스워드를 서버에서 생성하나 패스워드 변경 단계 이후로는 사용자가 계속 새로운 패스워드를 생성하여 서버에서는 사용자가 생성한 새로운 패스워드를 알 수 없다는 것이다. 이러한 문제들을 해결한 Chang 등은 자신들의 방식이 사용자 측에서만 패스워드 생성과 업데이트가 가능하게 개선하였고 해시함수와 XOR 연산만을 사용하여 작은 메모리 장치에서 사용가능한 방식이라고 주장하였다.

그러나 2014년에 Kumari 등[4]은 Chang 등의 방식이 오프라인 패스워드 추측 공격, 스마트카드로부터 획득한 비밀정보의 숫자로 인한 사용자 가장 공격, 그리고 서버 가장 공격에 안전하지 않다고 분석하였다. 또한 패스워드 변경 단계의 문제점으로 패스워드 변경 시 서버와의 상호작용이 필요하여 사용자가 자유롭게 패스워드를 변경할 수 없다는 점, 사용자가 패스워드 변경할 때 공격자로 인하여 패스워드 변경 요청이 거절될 수 있는 점, 그리고 패스워드 변경 과정에서 스마트카드가 정당한 사용자의 ID와 패스워드를 검증하지 않는다는 등의 문제들을 지적하였다. 그래서 Kumari 등은 자신들의 인증 방식이 이러한 여러 문제를 해결하면서 추적 불가능성을 가진 가벼운(lightweight) 익명성 제공 인증 방식이라고 주장하였다.

2017년 Nikooghadam 등[5]는 Kumari 등과 Chaudhry 등[6]의 두 인증 방식 모두 오프라인 패스워드 추측 공격의 문제가 있다고 지적하면서 개선된 가벼운 인증 방식을 제안하였다. 또한 Nikooghadam 등은 Kumari 등의 인증 방식에서 공격자가 통신 채널을 도청할 경우, 사용자의 ID 획득이 쉽기 때문에 사용자 익명성을 제공하지 못한다고 지적하였다. 그러면서 자신들의 인증 방식은 여러 공격에 대한 저항성을 가지면서, 사용자 익명성도 제공한다고 주장하였고, 안전성에 대한 분석은 BAN 로직(logic)[7, 8]을 사용하였다.

그러나 2019년 Giu 등[9]는 ECC(Elliptic Curve Cryptography)를 사용하여 동적 ID를 제공하는 가벼운 인증 방식을 제안하면서, Kumari 등의 인증 방식과 Nikooghadam 등의 인증 방식이 전방향 안전성(perfect forward secrecy)과 key-compromise impersonation attack의 문제점이 있다고 지적하였다. 2022년 Andola 등[10]은 Giu 등의 인증 방식이 공격자가 스마트카드를 획득할 경우, 사용자 가장 공격, 서버 가장 공격, 그리고 패스워드 추측 공격 등에 안전하지 않다고 지적하였다. 이러한 문제를 해결하기 위해서 Andola 등은 동적 ID를 이용한 향상된 익명성을 제공하는 패스워드와 스마트카드 기반의 인증 방식을 제안하였다. 그러나 본 논문에서는 Andola 등의 인증 방식을 분석하여, 스마트카드 분실 공격에 대한 저항성이 약하여 공격자가 사용자의 패스워드 뿐만 아니라 사용자가 생성한 난수 그리고 서버의 생성 난수까지도 계산가능하다는 것을 보일 것이다. Andola 등의 인증 방식은 이러한 안전성 문제로 인하여 공격자는 사용자와 서버만이 알고 있어야 하는 세션키까지 계산가능하다. 또한 앞에서 살펴본 인증 방식들을 본 논문에서 분석한 결과, Kumari 등의 인증 방식은 앞에서 언급한 문제점들 외에도 등록 단계에서 등록을 요청한 사용자 ID를 검증하지 않기 때문에, 기존 사용자 ID와의 중복성 문제가 발생하여 정당한 사용자를 제대로 인증하지 못하는 문제점이 있다. 이러한 ID 중복성 문제는 Chang 등의 방식에도 존재하였고, Nikooghadam 등의 인증 방식에서는 이러한 문제를 해결하였다. 그러나 Qiu 등의 방식에서는 또 다시 ID 타당성을 검증을 하지 않아 ID 중복성 문제가 발생하였고, 이를 개선했다는 Andola 등의 인증 방식에서도 여전히 동일한 문제가 존재하였다.

그러므로 본 논문에서는 Andola 등의 인증 방식에 대하여 분석하고, 그들의 인증 방식에 대한 문제점을 해결하기 위하여 개선된 인증 방식을 제안한다. 먼저 2장에서 Andola 등의 인증 방식에 관하여 살펴보고, 3장에서 본 논문에서 분석한 Andola 등의 인증 방식에 대한 여러 문제들을 제시한다. 그리고 이러한 문제들을 해결하기 위한 개선된 인증 방식을 4장에서 제안하고, 5장에서는 개선된 인증 방식에 대한 안전성과 성능 분석 결과를 제시하고 다른 인증 방식들과 비교분석한다. 마지막으로 6장에서 본 논문의 결론을 내리고 본 논문을 마친다.

II. Andola et al.'s Authentication Scheme

2장에서는 Andola 등이 제안한 멀티서버 환경에서 동적 ID를 사용하는 인증 방식에 대하여 살펴본다. 그들이 제안한 인증 방식은 등록 단계, 로그인과 검증(verification) 단계, 그리고 패스워드 변경 단계이다.

1. Registration phase

등록을 원하는 사용자는 다음과 같은 과정을 진행하여 새롭게 등록을 진행할 수 있다.

1. 사용자 Ui는 자신의 IDi와 패스워드 PWi, 그리고 난수 b를 선택한다. 사용자는 RPWi=h(b⊕PWi)를 계산하여 (IDi, RPWi)를 안전한 매체를 통해 등록 센터 RC에 보낸다.
2. 등록 센터 RC는 Ai, Bi, Ci, Di, Ei를 각각 계산한다.
   Ai=h(x||IDi), Bi=Zi⊕IDi⊕RPWi
   Ci=h(RPWi||ID||Zi))⊕Bi, Ei=h(Ai||h(x||y))
3. RC는 스마트카드에 (Ai, Bi, Ci, Ei, h(y), h())를 저장하여, 안전한 매체를 통해 사용자 Ui에게 스마트 카드를 보낸다.
4. 사용자는 난수 b를 스마트카드에 저장한다.

2. Login phase

서비스를 원하는 사용자는 서버 Sj에 로그인을 하기 위하여 다음과 같은 과정을 진행한다. 로그인과 인증 단계의 그림은 Fig. 1과 같다.

1. 사용자 Ui가 IDi와 PWi를 입력하면, 스마트카드는 서버의 ID SIDj를 가지고 다음을 계산하여, Ci′과 Ci가 같은지 비교하여 같지 않으면 세션을 종료한다.
   Zi=IDi⊕h(b⊕PWi)⊕Bi
   Ci′=h(h(b⊕PWi)||IDi||Zi)⊕Bi
2. 스마트카드는 난수 Ni를 생성하여 다음을 계산한다.
   Pij=h(Ni||h(y)||SIDj)⊕Ai, CIDi=Ei⊕h(Ni||SIDj||Ai)
   M1=h(Zi||Ni||Ei), M2=Ni⊕h(SIDj||h(y))
3. 사용자는 공개 매체를 통해 서버 Sj에게 (Pij, CIDi, M1, M2)를 보낸다.

3. Verification phase

1. 서버 Sj는 안전한 매체를 통해 등록 센터로부터 받은 h(x||y)와 h(y)를 가지고 다음을 계산한다.

Table 1. Notations

Notation	Description
Ui	The ith user
Sj	The jth Server
IDi	Ui's identity
PWi	User Ui's password
BIOi	User Ui's biometric information
RC	Registration center
SIDj	Identity of server Sj
CIDi	Ui's dynamic identity
RPWi	Result of h(b⊕PWi)
x	Secret key of RC
y	Secret number of RC
h()	Secure one-way hash function
||	Concatenation operation
⊕	XOR operation

   Ni=M2⊕h(SIDj||h(y)), Ai=h(Ni||h(y)||SIDj)⊕Pij
   Ei=CIDi⊕h(Ni||SIDj||Ai), Zi′=h(h(x||y)||Ai)⊕Ei
   Mi′=h(Zi′||Ni||Ei)
2. 서버 Sj는 M1′과 M1을 비교하여 결과가 다르면 세션을 종료하고 그렇지 않을 경우, 난수 Nj를 생성하여 다음을 계산한 후 M3과 M4를 사용자에게 보낸다.
   M3=h(Zi||Ni||SIDj||CIDi), M4=Ni⊕Nj⊕Ai
3. 사용자 Ui는 Nj=M4⊕Ai⊕Ni를 계산하여 Nj를 알아내고 h(Zi||Ni||SIDj||CIDi)를 계산하여 M3와 동일한지 비교한다. 동일하지 않으면 세션을 종료하고 그렇지 않으면 서버를 성공적으로 인증하여, M5(=h(Zi||Nj||SIDj||CIDi)를 계산한 후 서버에 보내고 세션키 SK=h(Zi||SIDj||Ni||Nj||CIDi)를 계산한다.
4. 서버는 M5′를 계산하여 전송받은 M5와 비교한다. 비교 결과가 동일하지 않으면 세션을 종료하고 그렇지 않으면 사용자를 정당한 사용자로 인증하여 세션키 SK=h(Zi||SIDj||Ni||Nj||CIDi)를 계산한다.

4. Password update phase

패스워드를 업데이트하기 원하는 사용자는 다음과 같은 과정을 통해 패스워드를 업데이트할 수 있다.

1. 사용자 Ui는 IDi와 PWi를 입력한다.
2. 스마트카드는 아래 값들을 계산한 후, Ci′과 Ci를 비교하여 결과가 같으면, 사용자는 새로운 패스워드 PW_{new}를 입력하고, 스마트카드는 새로운 난수 b_{new}를 생성한다.
   Zi=IDi⊕h(b⊕PWi)⊕Bi
   Ci′=h(h(b⊕PWi)||IDi||Zi)⊕Bi
3. 스마트카드는 다음과 같이 Bi_{new}와 Ci_{new}를 계산한다.
   $RPW_{new}=h(b_{new}⊕PW_{new})$

User	Public Medium	Server
input IDi, PWi and SIDj Zi=IDi⊕h(b⊕PWi)⊕Bi Ci′=h(h(b⊕PWi)||IDi||Zi)⊕Bi check Ci′ ?= Ci generate Ni, random number Pij=h(Ni||h(y)||SIDj)⊕Ai CIDi=Ei⊕h(Ni||SIDj||Ai) M1=h(Zi||Ni||Ei) M2=Ni⊕h(SIDj||h(y))	(Pij, CIDi, M1, M2) -->	Ni=M2⊕h(SIDj||h(y)) Ai=h(Ni||h(y)||SIDj)⊕Pij Ei=CIDi⊕h(Ni||SIDj||Ai) Zi′=h(h(x||y)||Ai)⊕Ei M1′=h(Zi′||Ni||Ei) check M1′ ?= M1 generate Nj, random number M3=h(Zi||Ni||SIDj||CIDi) M4=Ni⊕Nj⊕Ai
	<-- (M3, M4)	
Nj=M4⊕Ai⊕Ni M3′=h(Zi||Ni||SIDj||CIDi) check M3′ ?= M3 M5=h(Zi||Nj||SIDj||CIDi) SK=h(Zi||SIDj||Ni||Nj||CIDi)	(M5) -->	M5′=h(Zi||Nj||SIDj||CIDi) check M5′ ?= M5 SK=h(Zi||SIDj||Ni||Nj||CIDi)

Fig. 1. Andola et al.'s Login and Verification Process

Bi_{new}=Zi⊕IDi⊕RPW_{new}

Ci_{new}=h(RPW_{new}||IDi||Zi)⊕Bi_{new}

4. 스마트카드는 새로운 값 Bi_{new}와 Ci_{new}를 저장한다.

III. Analysis of Andola et al.'s Scheme

3장에서는 본 논문에서 분석한 Andola 등의 인증 방식에 대한 안전성과 그 외의 문제들에 대하여 분석한다.

1. Cryptanalysis

3.1.1 Stolen smart card attack

공격자가 스마트카드의 정보들과 공공 매체를 통한 메시지 M2를 사용하여 Ni=M2⊕h(SIDj||h(y))를 계산하면 사용자가 생성한 난수 Ni를 계산해 낼 수 있다. 서버의 ID SIDj는 낮은 엔트로피의 특성을 가질 것이고, 높은 엔트로피라 할지라도 공격자가 정당한 사용자인 것처럼 등록 단계를 통과하면 여러 서버의 SIDj에 대한 정보를 손쉽게 얻어낼 수 있다. 공격자는 Ni와 응답 메시지 M4를 사용하여 서버의 생성 난수 Nj를 간단히 계산할 수 있다.

1. Ni′ 계산

전송 메시지 M2와 스마트카드의 저장 정보 h(y), 그리고 획득한 SIDj를 사용하면 난수 Ni′=M2⊕h(SIDj||h(y))계산이 가능하다.

2. Ni′의 검증

계산한 난수 Ni′ 값의 검증은 획득한 Ni′를 다음 식에 대입하여 검증 가능하다. Pij는 공개 정보이고, Ai와 h(y)는 카드에 저장된 정보를 이용한다. 공개 정보 CIDi를 이용해도 Ni′값의 검증이 가능하다.

검증1. Pij⊕Ai = h(Ni′||h(y)||SIDj)

검증2. CIDi = Ei⊕h(Ni′||SIDj||Ai)

3. 서버의 난수 Nj′

만약 앞의 방식으로 Ni′의 검증에 성공할 경우, 공격자는 다음 과정을 통해 서버가 생성한 난수 Nj를 계산할 수 있다. 공개 정보 M4와 카드의 정보 Ai, 그리고 앞에서 알아낸 Ni′를 이용하여 Nj′=M4⊕Ni′⊕Ai을 계산한다. Zi의 계산은 Zi′=Bi⊕IDi⊕h(b⊕PWi)처럼 카드에 저장된 b와 Bi를 이용할 경우, 낮은 엔트로피의 특성을 가지는 사용자의 IDi와 PWi 추측 공격에 성공할 것이다. 이 값에 대한 검증은 M1 식(=h(Zi′||Na||Ei′))을 이용할 수 있다. 이렇게 획득한 값들을 가지고, 공격자는 사용자로 가장하기 위해서 난수 Na를 자신이 생성하여 로그인 요청 메시지를 작성한다. 하지만 공격자는 난수 Na를 생성하지 않고 이전 세션들 중 하나를 선택하여 서버에 그대로 전송해도 인증 과정을 통과할 수 있다. 그러한 이유는 이 인증 방식이 타

임스탬프를 사용하지 않기 때문이다.

Pij=h(Na||h(y)||SIDj)⊕Ai'

CIDi=Ei'⊕h(Na||SIDj||Ai')

M1=h(Zi'||Na||Ei'), M2=Na⊕h(SIDj||h(y))

그러므로 Andola 등의 인증 방식은 스마트카드 분실 공격에 대한 약한 저항성으로 인하여 패스워드 추측 공격뿐만 아니라 사용자 가장 공격까지 가능하다.

3.1.2 Session key disclosure attack

Andola 등의 인증 방식의 세션키는 SK=h(Zi||SIDj||Ni||Nj||CIDi)와 같이 계산하며, 앞 절의 스마트카드에서 획득한 정보들 Zi', Ni', Nj', SIDj, 공개 정보 CIDi를 사용하여 세션키 SK=h(Zi'||SIDj||Ni'||Nj'||CIDi)를 생성할 수 있다. 그러므로 Andola 등의 인증 방식은 세션키 노출 공격에 대한 저항성이 약하며, 이로 인하여 공격자는 사용자의 중요 정보들에 접근할 수 있다.

3.1.3 Password guessing attack

스마트카드의 소유자를 확인하는 Ci 값은 카드에 저장되어있고, 이에 대한 구성은 Ci=h(h(b⊕PWi)||IDi||Zi)⊕Bi이다. Zi는 IDi⊕h(b⊕PWi)⊕Bi이기 때문에 Zi를 대체하면 Ci=h(h(b⊕PWi)||IDi||IDi⊕h(b⊕PWi)⊕Bi)⊕Bi과 같다. Ci 구성은 IDi, PWi, Bi, 그리고 b로서 난수 b와 Bi는 카드에 저장된 값으로 낮은 엔트로피의 사용자 IDi와 PWi를 추측 공격할 수 있다. 공격에 성공할 경우, Andola 등의 인증 방식은 사용자 가장 공격에 대한 저항성도 가지지 못한다.

3.1.4 Denial of service

Andola 등의 인증 방식은 타임스탬프 대신에 난수를 사용한다. 이들의 인증 방식은 이전 세션의 로그인 요청 메시지를 공격자가 그대로 전송할 경우, 서버는 그 메시지를 정당한 사용자로부터 전송되어 온 것으로 인증하여 메시지를 보낸 사용자에게 응답 메시지 (M3, M4)를 보낸다. 공격자가 스마트카드를 획득하지 못했을 경우, Zi 때문에 세션키 SK를 생성할 수는 없지만, 서버에 대한 응답 메시지 M5는 이전 세션의 값을 그대로 보내어 서버를 속일 수 있다. 그러므로 Andola 등의 인증 방식은 공격자가 순수한 재생 공격에 성공하지 못한다 하더라도 이전 메시지를 그대로 전송하여 서버에 과부하가 걸리도록 할 수 있다.

2. Design Pitfall of Andola et al.'s Scheme

3.2.1 Unchecked validity of ID

Andola 등의 인증 방식은 등록 단계에서 등록을 새롭게 요청하는 사용자의 ID 타당성을 검증하지 않고, 각 사용자의 스마트카드 값들을 곧바로 계산한다. 사용자가 임의 사이트에 가입할 때 ID 타당성 체크는 해당 도메인에서 유일한 사용자를 구별하기 위한 것으로, 이러한 과정이 없는 이 방식은 인증 방식에 적합하지 않다.

3.2.2 Incorrect reference

Andola 등은 Qiu 등의 인증 방식을 분석하면서 Qiu 등의 동작 원리를 그림으로도 제시하고 있다. 그러나 참고문헌에 서술한 Qiu 등의 인증 방식과 Andola 등이 그림으로 제시한 Qiu 등의 방식은 동일한 인증 방식이 아니다. 참고문헌에 나오는 Qiu 등의 인증 방식은 ECC 알고리즘을 사용하지만 Andola 등이 그림으로 제시한 Qiu 등의 인증 방식은 ECC와도 무관하고, 전송 메시지의 갯수 등도 일치하지 않는다. 그러므로 본 논문에서 Qiu 등의 인증 방식을 분석할 때 Andola 등이 그림으로 제시한 인증 방식에 근거하여 분석한다.

IV. Improvement Scheme

본 장에서는 앞 장에서 분석한 Andola 등의 안전성 문제와 설계상의 문제들을 해결하기 위하여 생체정보를 이용한 개선된 인증 방식을 제안한다.

1. Registration phase

등록을 원하는 사용자는 Fig. 2의 과정을 진행한다.

1. 사용자 Ui는 자신의 IDi와 패스워드 PWi, 그리고 생체정보 BIOi를 입력한다. 사용자는 Gen(BIOi)=<Ri, Pi>와 RPWi=h(PWi⊕Ri)를 계산하여 안전한 매체를 통해 (IDi, RPWi)를 등록 센터에 보낸다.
2. 등록 센터 RC는 사용자 ID의 타당성을 확인하여 정당한 ID이면, 다음과 같이 Ai, Bi, Ci, Di, Ei를 각각 계산한다.

   Ai=h(x||IDi), Bi=Zi⊕IDi⊕RPWi

   Ci=h(RPWi||ID||Zi))⊕Bi, Ei=h(Ai||h(x||y))
3. 등록 센터 RC는 스마트카드에 (Ai, Bi, Ci, Ei, h(y), h())를 저장하여, 사용자 Ui에게 안전하게 보낸다.
4. 사용자는 다음을 계산하여 Hi를 카드에 저장한다. 그러면 카드에는 최종적으로 (Ai, Bi, Ci, Ei, Hi, h()) 가 저장된다.

   Zi=Bi⊕IDi⊕RPWi, Hi=Zi⊕h(y).

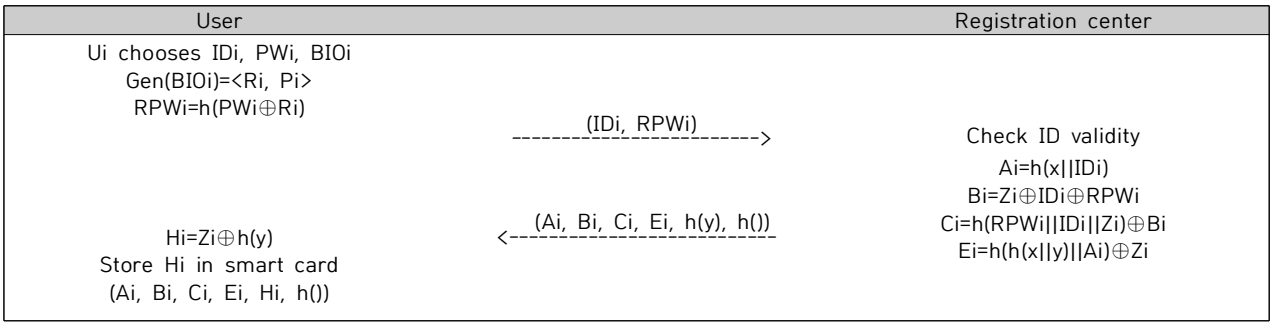

Fig. 2. Improved Registration Process

2. Login phase

로그인을 원하는 정당한 사용자는 Fig. 3과 같은 과정을 진행하여 서비스를 받을 수 있다.

1. 사용자 Ui가 IDi와 PWi, SIDj를 입력하면, 스마트카드는 다음을 계산하여, Ci′과 Ci가 같으면 다음을 과정을 진행하고, 같지 않으면 세션을 종료한다.
   $Zi=IDi\oplus h(PWi\oplus Ri)\oplus Bi$
   $Ci'=h(h(PWi\oplus Ri)||IDi||Zi)\oplus Bi$
2. 스마트카드는 난수 Ni와 타임스탬프 T1을 생성하여 다음을 계산한다.
   $h(y)=Zi\oplus Hi$
   $Pij=h(Ni||h(y)||SIDj||T1)\oplus Ai$
   $CIDi=Ei\oplus h(Ni||SIDj||Ai||T1)$
   $M1=h(Zi||Ni||Ei||Pij||CIDi||M2||T1)$
   $M2=Ni\oplus h(SIDj||h(y)||T1)$
3. 사용자는 공개 매체를 통해 서버 Sj에게 (Pij, CIDi, M1, M2, T1)를 보낸다.

3. Verification phase

1. 서버 Sj는 사용자로부터 받은 타임스탬프 T1의 타당성을 검사하여 타당한 △T1의 값이 나오면 등록 센터로부터 받은 h(x||y)와 h(y)를 가지고 다음을 계산한다. 만약에 △T1의 결과가 타당하지 않으면 세션을 종료한다.
   $Ni=M2\oplus h(SIDj||h(y)||T1)$
   $Ai=h(Ni||h(y)||SIDj||T1)\oplus Pij$
   $Ei=CIDi\oplus h(Ni||SIDj||Ai||T1)$
   $Zi'=h(h(x||y)||Ai)\oplus Ei$
   $Mi'=h(Zi'||Ni||Ei||Pij||CIDi||M2||T1)$
2. 서버 Sj는 M1′과 M1을 비교하여 결과가 다르면 세션을 종료하고 그렇지 않을 경우, 난수 Nj를 생성하여 M3=h(Zi||Ni||Nj||SIDj||CIDi||T2)와 M4=Ni⊕Nj⊕Ai를 계산한 후 M3, M4를 사용자에게 보낸다.
   $SK=h(Zi||SIDj||Ni||Nj||CIDi)$
3. 사용자 Ui는 서버로부터 받은 타임스탬프 T2의 타당성을 검사하여 타당한 △T2일 경우, Nj=M4⊕Ai⊕Ni를 계산하여 Nj를 알아내고 h(Zi||Ni||Nj||SIDj||CIDi||T2)를 계산하여 전송받은 M3과 동일한지 비교한다. M3′과 M3이 동일하지 않으면 세션을 종료하고 그렇지 않으면 서버를 정당한 서버로 인증하여, 세션키 SK=h(Zi||SIDj||Ni||Nj||CIDi)를 계산한다.

4. Password update phase

1. 사용자 Ui는 자신의 IDi와 PWi, BIOi를 입력한다.
2. 스마트카드는 다음 값들을 계산한 후, Ci′과 Ci를 비교하여 결과가 같으면, 사용자는 새로운 패스워드 PW_{new}를 입력하고, 스마트카드는 다음을 계산한다.
   $Zi=IDi\oplus h(PWi\oplus Ri)\oplus Bi$
   $Ci'=h(h(PWi\oplus Ri)||IDi||Zi)\oplus Bi$
3. 스마트카드는 다음과 같이 Bi_{new}와 Ci_{new}를 계산한다.
   $Bi_{new}=Zi\oplus IDi\oplus h(PW_{new}\oplus Ri)$
   $Ci_{new}=h(h(PW_{new}\oplus Ri)||IDi||Zi)\oplus Bi_{new}$
4. 스마트카드는 새로운 값 Bi_{new}와 Ci_{new}를 저장한다.

V. Analysis of Improvement Scheme

본 장에서는 개선된 인증 방식에 대한 안전성과 복잡도를 분석하여, 개선된 방식의 안전성과 효율성을 보인다.

1. Security analysis

Password guessing attack

개선된 방식의 PWi는 h(PWi⊕Ri)와 같이 계산하여 사용하고, Ri는 카드에 저장되지 않고 높은 엔트로피의 특성 때문에 h(PWi⊕Ri)로부터 패스워드를 추측하기 어렵다.

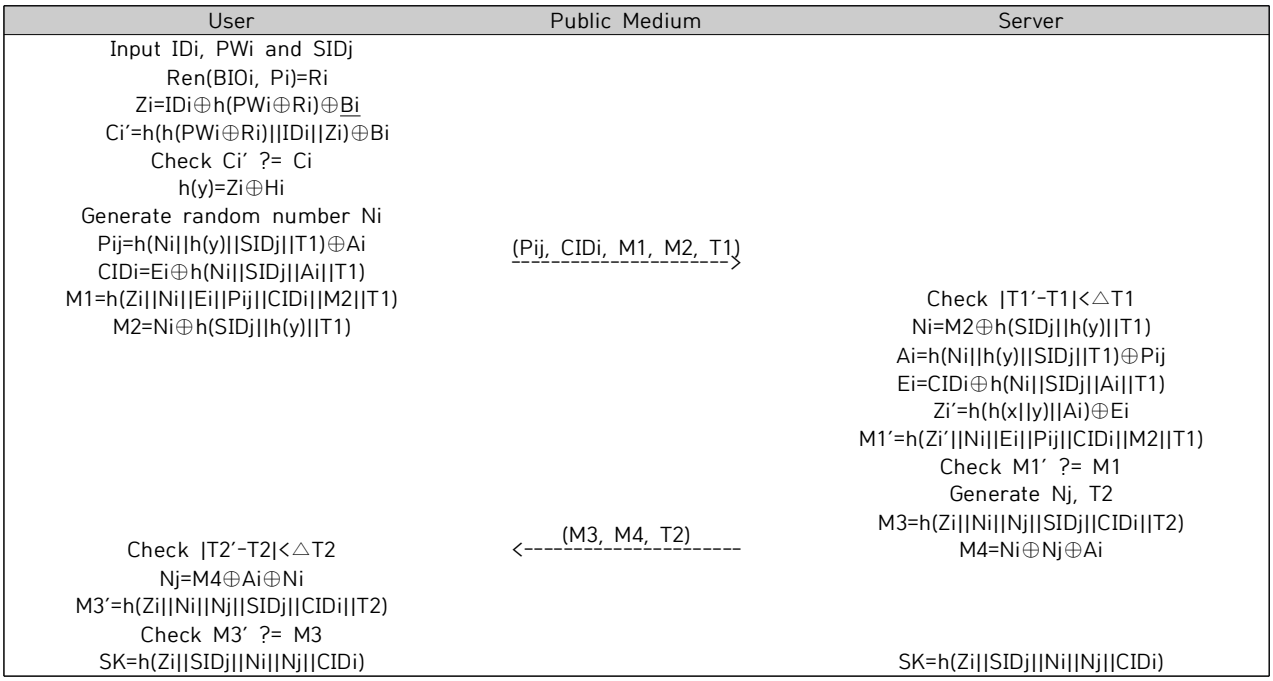

Fig. 3. Improved Login and Verification Process

Smart-card lost attack

개선된 인증 방식은 스마트카드의 Hi로부터 h(y)를 알려면 Zi를 알아야하는데, 이 Zi는 IDi⊕h(PWi⊕Ri)⊕Bi나 Ci'=h(h(PWi⊕Ri)||IDi||Zi)⊕Bi로부터 구해야 한다. 공격자가 카드의 Bi와 Ci'를 사용해서 필요한 값들을 구하려면 IDi, PWi, 그리고 Ri를 알아야한다. 그러나 패스워드 추측 공격에서 분석한 바와 같이, 공격자가 IDi를 알아낸다고 하더라도 Ri와 함께 해시연산한 PWi를 획득하기 어렵다.

User impersonation attack

공격자가 정당한 사용자로 위장하려면 사용자의 IDi와 PWi, 그리고 BIOi를 알아야 한다. 그러나 개선된 방식은 공격자가 사용자의 BIOi를 획득하지 않는 한 사용자의 PWi를 계산하기 어렵다. 사용자의 IDi도 Zi나 Ci'로부터 알아내야 하는데, Zi와 Ci'도 BIOi를 알아야 만이 IDi를 알아낼 수 있다. 공격자가 IDi를 알고 있다고 가정하여 Zi와 Ci'으로부터 다른 정보를 알아내려고 해도 결국 h(PWi⊕Ri)를 알아야 한다. 그러므로 개선된 인증 방식은 사용자 가장 공격에 안전하다.

Replay attack

개선된 인증 방식은 전송 메시지들에 타임스탬프를 이용하여 각 주체가 메시지를 받은 즉시, 타임스탬프의 타당성을 검사한다. 그리고 Pij나 CIDi 등의 메시지 무결성을 위하여 M1과 M3 등의 메시지 구성을 변경하였다. 그러므로 개선된 인증 방식은 재전송에 안전하다.

Session key disclosure attack

개선된 인증 방식에서 세션키를 알아내려면 전송 메시지 CIDi를 알고, 공개 정보는 아니나 획득 가능성이 높은 서버의 SIDj를 알고 있다고 할 경우, 나머지 Zi, Ni, Nj를 알아야 만이 세션키를 계산해낼 수 있다. 그러나 개선된 방식에서 Zi를 알아내려면 h(x||y), Ai, 그리고 Ei를 알아야 한다. 만약 공격자가 스마트카드 분실 공격에 성공하여, Ai와 Ei를 계산 가능하다고 하더라도 h(x||y)의 높은 엔트로피 때문에 Zi는 계산하기 어렵다.

User anonymity

개선된 인증 방식은 전송 메시지들에 CIDi를 사용하여 사용자의 IDi가 드러나지 않도록 하고, 스마트카드 분실 공격에도 안전하여 사용자 익명성을 침해받지 않는다.

Insider attack

개선된 인증 방식은 사용자의 PWi를 높은 엔트로피의 Ri와 함께 해시연산한 값을 서버에 제출한다. 그러므로 이 값으로부터 내주 공격자는 사용자의 패스워드를 계산해내기 어렵다.

2. Performance Analysis

본 절에서는 개선된 인증 방식과 관련 인증 방식들의 계

Table 2. Analysis of Security Functions

	Kumari et al.[4]	Nikooghadam et al.[5]	Qiu et al.[9]	Analysis result of Andola et al.	Improved Scheme
F1	N	Y	Y	N	Y
F2	N	Y	Y	Y	Y
F3	Y	Y	Y	N	Y
F4	Y	Y	Y	Y	Y
F5	Y	Y	N	N	Y
F6	Y	Y	N	N	Y
F7	N	N	Y	Y	Y

F1: User anonymity, F2: User impersonation attack, F3: Server spoofing attack, F4: Session key attack, F5: Replay attack, F6: Insider attack, F7: Password guessing attack

Table 3. Complexity and Performance Analysis

		Registration	Login and Verification	Total	Communication Cost
Kumari et al.[4]		4Th≈0.0092	12Th ≈ 0.0276	16Th	768bits
Nikooghadam et al.[5]		2Th+1Ts≈0.0092	6Th+6Ts≈0.0414	8Th+7Ts	960 or 1088bits
Qiu et al.[9]	A	4Th≈0.0092	19Th ≈ 0.0437	23Th	896bits
	B	4Th+1Tm≈2.2352	15Th+2Ts+3Tm≈6.7217	19Th+2Ts+4Tm	1088 or 1280bits
Andola et al.[10]		8Th≈0.0184	28Th≈0.0644	36Th	896bits
Improved scheme		5Th+1Te≈2.0005	16Th+1Te≈2.0258	21Th+2Te	1024bits

산 복잡도와 전송에 대한 성능을 비교 분석한다. 먼저 [Table 3]에서 Th는 해시함수의 연산횟수를, Ts는 대칭키의 암ㆍ복호화 연산, Tm은 ECC 곱셈 연산, 그리고 Te는 퍼지 추출(fuzzy extractor)을 나타낸다. Nikooghadam 등과 Qiu-B 방식은 대칭키나 ECC를 이용한 인증 방식으로, 각각의 계산 복잡도는 8Th+5Ts와 19Th+2Ts+4Tm이다. Andola 등이 실제로 참고한 Qiu 등의 방식은 [Table 3]에서 A로 표기하였고, 23Th의 계산 복잡도를 나타낸다. Andola 등의 방식은 등록 단계에서 8Th, 로그인과 인증 단계에서 28Th 연산이 필요하다. 개선된 인증 방식은 BIOi를 사용하여 등록 단계와 인증 단계에서 각각 한 번의 Te가 필요하여, 등록 단계에서 5Th+1Te와 로그인과 인증 단계에서 16Th+1Te의 계산 복잡도가 나온다. 개선된 인증 방식에서 Te를 제외할 경우, 로그인과 인증 단계는 Andola 방식의 거의 절반 수준에 해당하는 해시연산의 계산 복잡도를 보인다. 실행 속도는 Th가 0.0023*ms*, Ts는 0.0046*ms*, Tm은 2.226*ms*라 가정하고[9][12], Te는 1.989*ms*이라고 가정[7]하여 인증 방식들의 성능을 비교할 경우, 사용자가 한 번의 서비스를 받기 위해서 Andola와 개선된 인증 방식은 각각 0.0644*ms*와 2.0258*ms* 정도의 시간이 걸린다.

전송 메시지 비용은 사용자의 IDi, PWi, 해시 함수, 그리고 난수의 길이가 각각 128비트라고 가정하면, 개선된 인증 방식의 전송 메시지는 1024 비트이고, Andola 등의 방식은 896 비트, Kumari 등의 방식은 768 비트이다. Nikooghadam 등의 방식은 ECC 방식의 최소 길이가 160 비트여서 최소의 비트 길이로 가정하면 960 비트이나 ECC의 안전성 문제로 인하여 권장 비트인 256 비트를 사용한다고 가정하면, 전송 메시지는 최소 1152 비트이다. Andola 등의 방식에서 참고한 Qiu 등의 A 방식은 896 비트이고, B 방식은 ECC의 최소 비트 길이가 160이라고 가정할 경우, 전송 메시지는 1088 비트이고, 256 비트의 권장 비트를 사용할 경우에는 최소 1280 비트이다. 그러므로 개선된 인증 방식은 관련 인증 방식들보다 여러 공격에 안전하고, 전송 메시지 비용에서도 Nikooghadam 등의 방식과 Qiu-B 방식의 안전성 권장 비트보다 더 효율적인 것을 알 수 있다.

VI. Conclusions

본 논문에서는 동적 ID를 이용한 Andola 등의 인증 방식에 대하여 분석하였고, 그 결과 사용자와 서버가 생성한 각각의 난수를 공격자가 쉽게 계산해 낼 수 있었다. 또한 공격자가 스마트카드 분실 공격에 성공할 경우, 사용자의 ID와 패스워드 획득에 성공하여, 사용자를 가장할 수도 있고, 세션키 계산까지도 가능하였다. 본 논문에서는 이러한 문제들을 해결하기 위하여 개선된 인증 방식을 제안하였고, 안전성을 분석한 결과 스마트카드 분실 공격, 패스워드 추측 공격, 사용자 가장 공격, 재생 공격, 그리고 세션

키 노출 등 여러 공격에 안전하였다. 또한 개선된 인증 방식은 생체정보의 연산을 제외하면 해시함수의 계산 복잡도가 기존의 인증 방식에 비하여 거의 절반 수준으로 줄었고, 전송 메시지 측면에서도 ECC 방식을 사용하는 관련 인증 방식들보다 더 효율적인 것으로 분석되었다. 그러므로 본 논문에서의 개선된 인증 방식은 안전한 사용자 인증 방식에 적합하다고 할 수 있다.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Commun ACM, Vol. 24, Issue. 11, pp. 770-772, 1981. DOI: 10.1145/358790.358797

[2] Y. F. Chang , W. L. Tai, and H. C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, Vol. 27, Issue. 11, pp. 3430-3440, May 2013. DOI: 10.1002/dac.2552.

[3] Y. Y. Wang, J. Y. Liu, F. X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications, Vol. 32, No. 4, pp. 583-585, Mar. 2009.

[4] S. Kumari, M.. Khan and X. Li, "An improved remote user authentication scheme with key agreement," Comput Electr Eng, Vol. 40, No. 6, pp. 1997-2012, Aug. 2014. DOI: 10.1016/j.compeleceng.2014.05.007

[5] M. Nikooghadam, R. Jahantigh, and H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," Multimed Tools Appl Vol. 76, pp. 13401-13423, Jun. 2017. DOI: 10.1007/s11042-016-3704-8

[6] S. A. Chaudhry, M. S. Farash, H. Naqvi, S.Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security," Security Communication Networks, Vol. 8, Issue. 18, pp. 3782-3795, Jun. 2015. DOI: 10.1002/sec.1299

[7] 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, Sep. 2022. DOI: 10.1109/ACCESS.2022.3208347.

[8] M. Fakroon, M. Alshahrani, F. Gebali, and I. Traore, "Secure remote anonymous user authentication scheme for smart home environment," Internet of Things, Vol. 9, pp. 1-20, Mar. 2020. DOI: 10.1016/j.iot.2020.100158

[9] S. Qiu, G. Xu, H. Ahmad, G. Xu, X. Qiu, 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. DOI: 10.3837/tiis.2019.02.027

[10] N. Andola, S. Prakash, R. Gahlot, S. Venkatesan, and S. Verma, "An enhanced smart card and dynamic ID based remote multi-server user authentication scheme," Cluster Computing, Vol. 25, pp. 3699-3717, May 2022. DOI: 10.1007/s10586-022-03585-4

[11] D. He, N. Kumar, J. H. Lee, and R. 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.

[12] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC," Multimedia Tools and Applications, pp. 181-197, Vol. 75, Sep. 2016. DOI 10.1007/s11042-014-2282-x

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.