디지털산업정보학회 논문지 제14권 제2호-2018년 6월
http://dx.doi.org/10.17662/ksdim.2018.14.2.027

스마트카드 기반의 사용자 인증 기법에 관한 연구

이 재 영*

A Study on Smart-Card Based User Authentication

Lee Jaeyoung

〈Abstract〉

User authentication scheme is a method for controlling unauthorized users' access to securely share the services and resources provided by the server and for verifying users with access rights. Initial user authentication scheme was based on passwords. Nowadays, various authentication schemes such as ID based, smart-card based, and attribute based are being researched. The study of Lee et al. suggested a user authentication scheme that provides forward secrecy and protects anonymity of users. However, it is vulnerable to attacks by outsiders and attackers who have acquired smart-cards. In this paper, we propose a modified smart-card authentication scheme to complement the weakness of the previous studies. The proposed user authentication scheme provides the security for the ID guessing attack and the password guessing attacks of the attacker who obtained the login request message and the user's smart-card.

Key Words : ID Guessing Attack, Password Guessing Attack, Session key. Smart-card, User Authentication,

Ⅰ. 서론

사용자 인증이란 서버가 로그인을 요청하는 사용자를 검증하여 서버의 자원이나 서비스에 대한 접근 권한을 부여하는 것이다. 모든 정보가 네트워크로 전달되는 원격 환경의 특성상, 사용자 인증은 순방향 안전성을 제공하기 어렵고, 위장 공격, ID나 패스워드의 추측 공격, 메시지의 위·변조, 재전송 공격 등의 위험에 노출되기 쉽다[1]. 때문에 서버와 사용자 사이에 전송되는 모든 메시지는 기밀성, 무결성, 가용성이 보장되어야 하고, 서버의 비밀키가 노출되더라도 서버와 사용자 사이의 세션키의 안전성은 보장되어야 한다[1-5].

1981년 Lamport가 공공 채널을 통한 패스워드 기반의사용자 인증 기법을 제안한 이후로 초기의 사용자 인증은 대부분 패스워드에 기반을 둔 것들이 대부분이었으나 다양한 보안 요구사항을 만족하기 위하여 ID 기반, 스마트카드 기반, 속성 기반 등의 다양한 사용자 인증 기법이 제안되어 왔다[2, 5].

Kumari등이 제안한 사용자 인증 기법은 사용자의 익명성을 보장하지 않고 전방향 안전성을 제공하

* 세명대학교 정보통신학부 조교수

지 않으며 서버의 비밀키가 노출되면 세션키의 안전성을 유지할 수 없는 등의 문제점이 지적되었다[6]. 본 논문에서는 Kumari 등이 제안한 사용자 인증 기법의 취약점을 개선한 Lee 등이 제안한 사용자 인증 기법[1]을 분석하고, Lee 등의 사용자 인증 기법의 취약점을 개선한 사용자 인증 기법을 제안하려한다.

Lee 등이 제안한 사용자 인증 기법은 사용자의 익명성을 보호하고 전방향 안전성을 제공하지만, 외부자의 위장 공격과 스마트카드를 취득한 공격자의 ID 추측 공격, 패스워드 추측 공격 등에 취약하고, 사용자의 ID가 노출되면 세션키의 안전성을 보장할 수 없는 등의 문제가 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 사용자 인증 기법에 대해 설명하고, Lee 등이 제안한 사용자 인증 기법을 살펴본다. 3장에서는 Lee 등이 제안한 사용자 인증 기법의 취약점을 개선한 사용자 인증 기법을 제안하고, 4장에서는 제안한 사용자 인증 기법의 안전성을 분석한다. 마지막 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 사용자 인증 기법

2011년 Khan등은 Wang 등이 제안한 인증 기법이 공격자가 사용자의 로그인 요청 메시지를 획득하고, 이를 이용하여 공격하면 사용자의 익명성을 보장하지 못하고, 서버가 사용자의 패스워드를 임의로 부여하므로 내부자 공격에 취약하다는 것을 증명하였고[7], 이것을 개선한 동적 ID 기반의 사용자 인증 기법을 제안하였다. 2012년에 Chen 등은 Khan 등이 제안한 동적 ID 기반의 사용자 인증 기법이 내부자 공격에 취약하고, 등록되지 않은 변수를 이용하는 등의 문제가 있다고 주장하여 이 문제를 개선하였고 더불어 사용자 난수를 공개 채널로 전송하지 않는 새로운 인증 기법을 제안하였다. 2013년에 Jiang 등은 Chen 등이 제안한 인증 기법이 사용자의 익명성과 불추적성을 보장하지 않기 때문에 ID 추측 공격과 추적(tracking)공격에 취약하다는 것을 증명하였고, 이에 불추적성이 제공되는 대칭키 기반의 사용자 인증 기법을 제안하였다. 또한 , 2013년에 Kumari 등은 Jiang 등의 사용자 인증 기법이 사용자로의 위장 공격, 패스워드 추측 공격, DoS 공격에 취약함을 증명하였고, 이를 개선한 새로운 인증 기법을 제안하였다[2, 4, 8].

2.2 Lee 등이 제안한 사용자 인증 기법

Lee 등이 제안한 사용자 인증 기법은 Kumari 등이 제안한 사용자 인증 기법의 장점은 그대로 보존하면서 장기간 이용하는 서버의 비밀키가 노출되더라도 세션키의 안전성을 보장하는 전방향 안정성을 제공한다[2, 5]. <표 1> 은 본문에 이용되는 표기법을 기술한 것이다.

등록 단계

1) 사용자는 IDi와 PWi를 선택하고 난수 ri를 생성한다.

2) 사용자는 PWi와 난수 ri를 이용하여 RPWi를 계산하고 안전한 채널을 통하여 IDi와 RPWi를 서버에게 전송한다. RPWi=h(ri||PWi)

3) 서버는 먼저 IDi의 형태를 확인하고, 사용자의 등록 요청 횟수 Ni에 값을 부여한다. 등록이 처음이면 Ni=0, 재등록이면 Ni=Ni+1이다.

4) 서버는 Ji, Qi, Yi, Ri, Li, Ai, Mi, AIDi를 계산하고, RGR에 {IDi⊕x, Ni}를 저장한다.

Ji=h(x||IDi||Ni), Qi=h(IDi||x)⊕RPWi,

Yi=h(RPWi||IDi), Ri=b⊕h(IDi||x),
Li=Ji⊕h(RPWi||b), Ai=Li⊕h(IDi||b),
Mi=h(Ji||RPWi||IDi),
AIDi=Ex(IDi⊕h(Yi||b).

5) 서버는 스마트카드에 {Ri, Ai, AIDi, Mi, h(·), Ek, Dk}를 저장하고, 스마트카드와 Qi를 안전한 채널을 통해 사용자에게 전송한다.

6) 사용자는 스마트카드와 Qi를 수신한 후, Ki와 Bi 계산하고, 스마트카드에 추가로 저장한다.

Ki=h(IDi||PWi)⊕ri, Bi=Qi⊕ri를 계산.

<표 1> 표기법

Symbol	Description
Ui	User
S	remote Server
IDi, PWi	Identity and password of Ui
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
||	Concatenation operation
⊕	XOR operation
T	time stamp
SK	Session key
ΔT	The maximum of transmission delay time

로그인 단계

1) 사용자는 스마트카드를 카드 리더에 넣고 IDi와 PWi를 입력한다.

2) 스마트카드는 스마트카드에 저장된 정보와 입력된 IDi와 PWi를 이용하여 ri*와 RPWi*를 계산한다.

ri*=Ki⊕h(IDi||PWi), RPWi*=h(ri*||PWi)

3) 스마트카드는 계산된 RPWi*와 ri*를 이용하여 h(IDi||x)*, b*, Li*, Ji*, Mi*를 계산한다.

h(IDi||x)*=Bi⊕RPWi*⊕ri*, b*=h(IDi||x)*⊕Ri,

Li*=Ai⊕h(IDi||b*), Ji*=Li*⊕h(RPWi*||b*)

Mi*=h(Ji*||RPWi*||IDi)

4) 스마트카드는 계산의 결과인 Mi*와 스마트카드에 저장된 Mi가 일치하는지 확인한다. 두 값이 같으면 Ci=h(Ti||Ji)를 계산하고, 아니면 세션을 종료한다.

Ti는 Ci를 계산하는 시점의 타임스탬프이다.

5) 사용자는 로그인 요청 메시지 {AIDi, Ti, RPWi, Ci}를 공개 채널을 통해 서버에게 전송한다.

인증 단계

1) 서버는 사용자의 로그인 요청 메시지 {AIDi, Ti, RPWi, Ci}를 수신한 후 T'-Ti≤ΔT를 확인한다. 조건이 맞지 않으면 세션을 종료한다.

T'는 로그인 요청 메시지 수신 시점의 타임스탬프이다.

2) 서버는 RPWi를 이용하여 Yi*를 계산한다. Yi*를 이용하여 IDi⊕h(Yi*||b)를 계산하고, 계산 결과와 Dx(AIDi)의 결과가 같은지 비교한다. 두 값이 같으면 Ji*, Ci* 계산한다.

Yi*=h(RPWi||IDi)

Ji*=h(x||IDi||Ni), Ci*=h(Ti||Ji).

3) 계산된 Ci*와 로그인 요청 메시지의 Ci가 일치하는 지 확인한다. 일치하지 않으면 세션을 종료하고 일치하면 AIDi*와, Cms 계산한다.

Ts는 Cms를 계산하는 시점의 타임스탬프이다.

AIDi*=Ex(ID⊕h(Yi*||b)), Cms=EJi(AIDi*||Ci||Ts)

4) 서버는 Cms와 Ts를 공개 채널을 통해 사용자

에게 전송한다.

5) Cms를 수신한 사용자는 AIDi||Ci||Ts를 계산한 결과가 DJi(Cms)와 일치하는지 확인하고, T''-Ts≤ΔT를 확인한다. 만일 두 조건이 맞지 않으면 세션을 종료한다.

T''는 Cms를 수신하여 복호화 한 시점의 타임스탬프이다.

6) Cms를 복호화해서 얻은 Ci*와 로그인 요청 메시지의 Ci가 일치하면 AIDi*과 AIDi가 같은지 확인한다. 두 값이 서로 다르면 AIDi를 AIDi*로 재배치한다.

7) 사용자와 서버는 세션키 Sk=h(Ji||Ti||Ts)를 생성 하고 인증 단계를 마친다.

Ⅲ. 제안하는 사용자 인증 기법

3.1 Lee 등의 사용자 인증 기법의 취약점

Lee 등이 제안한 사용자 인증 기법은 공격자가 사용자의 로그인 요청 메시지와 스마트카드를 획득하면 사용자의 ID와 패스워드를 쉽게 추측할 수 있다는 취약점이 있다[2].

공격자가 사용자의 로그인 요청 메시지 {AIDi, Ti, RPWi, Ci}와 스마트카드 {Ri, Ai, AIDi, Mi, h(·), Ki, Bi, Ek, Dk}를 획득하면, 공격자의 ID 추측 공격을 시도할 수 있다.

공격자는 사용자의 IDi*를 추측 한다. 추측한 IDi*를 이용하여 Ci*를 계산하고, 로그인 요청 메시지의 Ci와 비교한다.

만약 Ci*와 Ci가 같으면 추측한 IDi*는 사용자의 ID임이 확인하고, 같지 않으면 다른 IDi*를 추측하여 동일한 연산을 반복한다. 또한 공격자는 로그인 단계에서 계산하여 구할 수 있는 서버의 난수 b와 ID 추측 공격으로 알아낸 사용자의 ID를 이용하여 패스워드 추측 공격을 시도할 수 있다.

공격자는 스마트카드의 Ri와 서버의 난수 b를 이용하여 h(IDi*||x)를 계산하고, 스마트카드의 Bi, 로그인 요청 메시지의 RPWi를 이용하여 ri*를 계산한다.

공격자는 임의의 패스워드 PWi*를 추측하여 h(ri*||PWi*)를 계산하고 이 값이 로그인 요청 메시지의 RPWi와 일치하는지 비교한다.

만약 두 값이 같으면 사용자 Ui의 패스워드는 PWi*이고, 두 값이 다르면 다른 패스워드 PWi*를 추측하여 동일한 연산을 수행한다.

3.2 제안하는 사용자 인증 기법

본 논문에서 제안하는 사용자 인증 기법은 공격자가 임의의 사용자의 로그인 요청 메시지와 스마트카드를 획득하여도 사용자의 ID를 추측할 수 없게 하고 사용자의 ID를 추측할 수 없게 함으로써 패스워드를 추측할 수 없게 한다.

등록 단계

1) 사용자는 IDi, PWi, 난수 ri를 생성한다.

2) 사용자는 PWi와 ri를 이용하여 RPWi=h(ri||PWi)를 계산하고, 계산된 RPWi와 IDi를 안전한 채널을 통해 서버로 전송한다.

3) IDi와 PRWi를 수신한 서버는 IDi를 확인하고, 사용자가 서버에 등록을 요청한 횟수인 Ni에 값을 부여한다. 등록이 처음이면 Ni=0, 재등록이면 Ni=Ni+1이다.

4) 서버는 수신한 IDi와 RPWi, 서버의 난수 b, 비밀키 x, 그리고 Ni를 이용하여 다음의 값을 계산한다.

Ji=h(x||IDi⊕x||Ni), Qi=h(IDi||x)⊕RPWi,

Yi=h(RPWi||IDi⊕x), Ri=h(b||x)⊕h(IDi||x),
Li=Ji⊕h(RPWi)⊕h(b||x),
Ai=Li⊕h((IDi||x)⊕h(b||x)),
Mi=h(Ji||RPWi||IDi),
AIDi=Ex((IDi⊕x)⊕h(Yi||b))
RGR에 {IDi⊕x, Ni, IDi||x}를 저장한다.

5) 서버는 스마트카드에 {Ri, Ai, AIDi, Mi, h(·), Ek, Dk}를 저장하고, 스마트카드와 계산한 Qi를 안전한 채널을 통해 사용자에게 전송한다.

6) 사용자는 스마트카드와 Qi를 수신한 후, Ki=h(IDi||PWi)⊕ri, Bi=Qi⊕ri를 계산하여 스마트카드에 추가로 저장한다.

로그인 단계

1) 사용자는 스마트카드를 카드 리더에 넣고 IDi와 PWi를 입력한다.

2) 스마트카드는 사용자가 입력한 IDi와 PWi, 스마트카드에 저장된 Ki를 이용하여 ri*=Ki⊕h(IDi||PWi)와RPWi*=h(ri*||PWi)를 계산한다.

3) 계산된 RPWi*와 ri*, 그리고 스마트카드에 저장된 Bi를 이용하여 다음의 값들을 계산한다.

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).

4) 계산 결과인 Mi*와 스마트카드에 저장된 Mi가 일치하는지 확인하고 두 값이 같으면 Ci=h(Ti||Ji*)를 계산한다. 만일 두 값이 같지 않으면 세션을 종료한다.

Ti는 Ci를 계산하는 시점의 타임스탬프이다.

5) 사용자는 로그인 요청 메시지{AIDi, Ti, RPWi, Ci}를 공개 채널을 통하여 서버에게 전송한다.

인증 단계

1) 서버는 사용자의 로그인 요청 메시지{AIDi, Ti, RPWi, Ci}를 수신한 후 T′-Ti≤ΔT를 확인한다. 조건이 맞지 않으면 세션을 종료한다.

T′는 로그인 요청 메시지를 수신한 시점의 타임스탬프이다.

2) 서버는 수신한 RPWi와 RGR에 저장된 IDi⊕x를 이용하여 Yi*=h(RPWi||IDi⊕x)를 계산하고, Yi*와 난수 b, 비밀키 x를 이용하여 (IDi⊕x)⊕h(Yi*||b)를 계산한다. 계산 결과가 로그인 요청 메시지의 AIDi를 복호한 값과 같은지 확인한다. 두 값이 같으면 Ji*=h(x||IDi⊕x||Ni)를 계산하고, Ji*를 이용하여 Ci*=h(Ti||Ji)를 계산한다.

3) 서버는 계산한 Ci*와 로그인 요청 메시지의 Ci가 일치하는지 확인한다. 일치하지 않으면 세션을 종료하고, 일치하면 AIDi*=Ex((IDi⊕x)⊕h(Yi*||b)), Cms=EJi*(AIDi*||Ci||Ts)를 계산한다.

Ts는 Cms를 계산하는 시점의 타임스탬프이다.

4) 서버는 Cms와 Ts를 공개 채널을 통해 사용자에게 전송한다.

5) 사용자는 Cms와 Ts를 수신한다. 사용자는 AIDi||Ci||Ts를 계산하고, 계산된 결과가 수신한 Cms를 복호화한 결과와 일치하는지 확인한다. 또한 T′′-Ts≤ΔT를 확인한다. 만일 두 조건이 모두 맞지 않으면 세션을 종료한다.

T′′는 Cms를 수신하여 복호화한 시점의 타임스탬프이다.

6) 복호화해서 얻은 Ci*과 로그인 요청 시 전송했던 Ci가 일치하면, AIDi*과 AIDi가 같은지 확인한다. 두 값이 서로 다르면 AIDi를 AIDi*로 재배치한다.

7) 사용자와 서버는 각각 세션키 Sk=h(Ji||Ti||Ts)를 생성한다.

Ⅳ. 안전성 분석

Lee 등이 제안한 사용자 인증 기법에서 공격자는 사용자의 로그인 요청 메시지와 스마트카드를 획득한 후, 로그인 요청 메시지와 스마트카드에 저장된 정보를 이용하여 사용자의 ID와 패스워드를 추측하는데 필요한 값들을 계산한다.

공격자는 사용자의 IDi*를 추측하여 Ji*=Ai⊕h(PPWi||b)⊕H(IDi*||b)를 계산한다. 계산한 Ji*를 이용하여 Ci*=h(Ti||Ji*)를 계산한다. 계산된 Ci*와 로그인 요청 메시지의 Ci를 비교하여 두 값이 같으면, Ii*에 이용된 추측한 IDi*가 사용자의 ID임을 확인하는 것이다. 사용자의 ID를 알아내면, 패스워드 추측 공격에 사용자의 ID가 이용된다.

본 논문에서는 Lee 등의 사용자 인증 기법의 문제점을 개선하여, 공격자가 사용자의 로그인 요청 메시지와 스마트카드를 획득하여도 ID와 패스워드를 추측하는데 필요한 값들을 계산하여 얻을 수 없게 하였다. 제안한 사용자 인증 기법에서 Ji*는 다음과 같이 계산한다.

Ji*=Ai⊕h(IDi||x)*⊕h(b||x)*⊕h(RPWi*)⊕h(b||x)*

공격자가 Ji*를 계산하기 위해서 사용자의 로그인 요청 메시지, 스마트 카드, 서버의 비밀키 x, 추측한 사용자의 IDi*가 있어야 한다. 서버의 비밀키 x를 알지 못하면 Ji*를 계산할 수 없고, Ji*를 계산할 수 없으면, Ci*를 계산하지 못하면 로그인 요청 메시지의 Ci와 비교할 수 없다. 때문에, 본 논문에서 제안한 사용자 인증 기법은 스마트카드와 로그인 요청 메시지를 획득한 공격자에 의한 ID 추측 공격으로부터 안전하다.

Ⅴ. 결론

본 논문에서는 로그인 요청 메시지와 스마트카드를 획득한 공격자에 의한 ID 추측 공격에 대응할 수 있는 사용자 인증 기법을 제안하였다.

Lee 등이 제안한 사용자 인증 기법에서 공격자는 사용자 로그인 요청 메시지와 스마트카드를 획득한 후, 저장된 정보를 이용하여 사용자의 ID와 패스워드를 추측하는데 필요한 값들을 계산할 수 있었다. 공격자가 계산된 값을 이용하여 사용자의 ID를 알아내면 ID는 다시 패스워드를 추측하는데 이용되고, 사용자의 ID와 패스워드를 알아낸 공격자는 정당한 사용자로 위장하는 공격이 가능하다. 본 논문에서는 공격자가 사용자 로그인 요청 메시지와 스마트카드를 획득하여도 사용자의 ID를 추측하는데 이용되는 값을 계산할 수 없게 함으로써, ID 추측 공격에 안전한 사용자 인증 기법을 제안하였다.

ACKNOWLEDGMENTS

본 논문은 2016학년도 세명대학교 교내학술연구비 지원에 의해 수행된 연구임.

참고문헌

[1] 이성엽·박기성·박요한·박영호, “순방향 안전성을 제공하는 대칭키 기반의 원격 사용자 인증 방식,” 한국멀티미디어학회논문지, 제19권, 제3호, 2016, pp.585-594.

[2] 문종호·원동호, “전방향 안전성을 제공하는 개선된 대칭키 기반의 원격 사용자 인증 방식,” 한국멀티미디어학회논문지, 제20권, 제3호, 2017, pp.500-510.

[3] https://jjaiwook79.blog.me/30153115340
[4] 이용재・김영곤・박태성・전문석, "스마트 폰의 QR-Code의 인식 기법을 이용한 사용자 인증 기법설계," 디지털산업정보학회논문지, 제7권, 제3호, 2011, pp.85-95.
[5] 김현성, "전방향 안정성을 제공하는 키 동의 및 원격 사용자 인증 기법," 보안공학연구논문지, 제12권, 제 1호, 2015, pp.1-12.
[6] KW. Kim, JD. Lee, "On the Security of Two Remote User Authentication Schemes for Telecare Medical Information Systems," Journal of medical systems, Vol. 38, No. 5, 2014, pp.1-11.
[7] Mj. Kim, KW. Lee, SJ. Kim, DH. Won, "An Efficient and Secure Authentication Scheme Preserving User Anonymity," 디지털산업정보학회논문지, 제6권, 제3호, 2010, pp.69-77.
[8] 박기성·이성엽, 박요한·박영호, "사물인터넷에서 ID 기반 원격 사용자 인증 방식," 멀티미디어학회논문지, 제18권, 제12호, 2015, pp.1483-1491.

■ 저자소개 ■

이 재 영
(Lee Jaeyoung)

2012년 9월~현재
세명대학교 정보통신학부 조교수
2007년 2월 충북대학교 컴퓨터공학과(공학박사)
2000년 8월 세명대학교 전산교육학과
(교육학석사)
1996년 2월 세명대학교 전산학과(이학사)

관심분야 : 정보보안, 네트워크보안
E-mail : klitie@semyung.ac.kr

논문접수일 : 2018년 06월 05일
수 정 일 : 2018년 06월 11일
게재확정일 : 2018년 06월 12일