Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Cryptanalysis of Biometric-based to Lin et al'.s Multi-Server User Authentication Scheme

Kwang-Cheul Shin*

Division of Industrial Management Engineering, Sungkyul University

ABSTRACT

The use of biomedical technology has been applied to all smart devices such as smart phones and tablet PCs, mainly shopping malls, medical systems, and financial institutions. The core of biomedical technology is the authentication function. Authentication verifies the validity of the identity at the remote server by the registered user. It is also a basic security service that allows access to remote servers. Passwords, smart cards, and biometrics are three commonly used elements in authentication. Remote user authentication schemes for various multi-server environments have been proposed by many researchers. Lin et al.'s suggested that the scheme of Baruah et al.'s is vulnerable to impersonation attacks, smart card theft attacks, etc. in a multi-server environment and proposed an improved scheme. However, there is a weakness of some parameter calculations as a result of Lin et al.'s analysis of the authentication scheme. It was revealed that users and servers were colluding, or when users' smart cards were stolen, they were vulnerable to impersonation attacks, smart card stolen attacks, replay attacks, and denial of service attacks. Thus, this paper logically reanalyzes and compares the vulnerabilities of the Lin et al 's scheme.

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

ARTICLE INFO: Received 11 August 2018, Revised 8 September 2018, Accepted 12 October 2018.

*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

생체인식기술의 활용은 쇼핑몰, 의료시스템, 금융권을 중심으로 스마트폰, 태블릿PC 등 모든 스마트기기에 생체인식 기술이 적용, 확대되고 있으며 이에 대한 중요성은 날로 증가되고 있다. 그동안 많은 연구에서 저비용과 효율성을 고려한 패스워드기반의 스마트카드 인증방식이 제안되었다[1-5]. 그러나 패스워드 인증스킴은 단순한 사전 공격에 쉽게 노출될 뿐만 아니라 낮은 보안 엔트로피로 인해 스마트카드에 저장된 정보가 전력 소모 분석(SPA:Simple Power Analysis)에 의해 추출될 수 있어 다중 서버환경에는 제약이 있다[6]. 따라서 스마트카드와 함께 사용자의 생체 인식 및 패스워드를 결합한 인증방식이 제안되었다[7-10].

2010년 Li and Hwang[11]은 생체인식, 스마트카드 및 인증을 위한 난수를 기반으로 하는 원격 사용자 인증스킴을 제안했다. 그러나 2011년에 Li et al.' s[12]은 그들의 스킴이 적절한 인증을 제공하지 않고 중간자 공격에 저항할 수 없다는 것을 증명하였다. 2014년 Chuang과 Chen은 스마트카드와 생체 인식을 사용하여 사용자 익명으로 다중 서버 인증키 동의 스킴을 제안했다[13]. 그러나 Mishra et al. 's[14]은 그들의 스킴이 스마트카드 공격과 위장공격에 안전할 수 없다는 것을 발견하고 개선된 원격 사용자 인증스킴을 제안했다. 이어서 Baruah et al.' s[15]은 Mishra et al. 's 스킴 역시 스마트카드 공격과 위장(impersonation) 공격을 저지할 수 없다는 것을 증명하고 개선된 스킴을 제안했다.

최근, Lin et al. 's[16]은 Baruah et al.' s 스킴이 스마트카드가 도난되었을 때 오프라인공격에 견딜 수 없다는 사실을 발견하고 퍼지 추출기 기술을 이용한 향상된 사용자 인증스킴를 제안했다[17]. 그러나 Lin et al. 's 스킴 또한 위장(impersonation) 공격, 서비스거부공격과 스마트카드 도난공격에 효과적으로 방어하지 않는다.

본 논문에서는 Lin et al's 등이 제안한 스킴의 세 가지 보안 취약점에 대해 중점적으로 분석하고 이전의 스킴들과 비교한다.

2. 관련연구

2.1 Review of Lin et al.'s Scheme

이 절에서는 Lin et al에 의해 다중 서버환경에 대한 사용자 인증스킴의 생체인식을 검토하고 이 스킴의 보안 취약점을 분석한다. Lin et al. 's 스킴은 퍼지 추출기 기법을 사용하였으며, 등록, 로그인, 인증, 패스워드변경 단계의 네 단계로 본 논문에서는 등록, 로그인, 인증단계에서의 취약점을 살펴본다. 사용되는 표기법은 <표 1> 같이 요약된다.

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

표기	정의
ID_i	i번째 사용자 식별자
SID_j	j번째 서버의 식별자
PSK	서버의 Pre-shared key
x	등록센터의 마스터키
RC	등록센터
pw_i	i번째 사용자 패스워드
BIO_i	i번째 사용자 생체정보
$h(\cdot)$	단방향 해시함수
$\oplus$	Exclusive-OR 연산
$\|$	연접

2.1.1 등록 단계

2.1.1.1 서버등록

1) 서버는 <그림 1>과 같이 자신의 식별자 SIDj를 등록하기 위해 안전한 채널로 등록센터(RC : Registration Center)에 전송한다.

2) RC는 안전한 채널로 서버 SIDj에 비밀정보인 h(SIDj ‖ h(PSK))와 h(PSK ‖ x)를 전송한다.

2.1.1.2 사용자등록

등록된 서버에서 제공하는 서비스에 액세스하려면 RC에 등록해야 한다.

1) 사용자 Ui는 식별자 IDi 및 패스워드 PWi를 선택하고 센서 단말기에 자신의 생체 정보 BIOi를 입력하여 Gen(BIOi)=(Ri, Pi)를 얻는다. Gen은 생체 정보가 시간이나 상황에 따라 달라지는 특성을 고려해서 정상적 로그인이 될 수 있도록 하는 암호학적 기법으로 랜덤문자열 Ri와 헬퍼문자열 Pi를 생성한다.

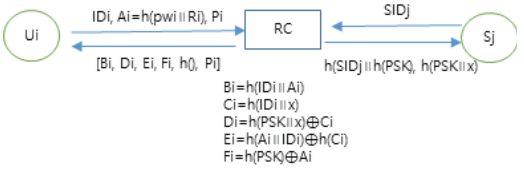

그림 1. 등록단계
Figure 1 Registration phase

2) Ui는 [IDi, Ai=h(PWi ‖ Ri), Pi]를 안전한 채널을 통해 RC에 전송한다.

3) RC는 다음을 계산하고 사용자의 스마트카드(SCi)에 저장[Bi, Di, Ei, Fi, h(), Pi]하여 안전한 채널로 사용자에게 전송한다.

Bi=h(IDi ‖ Ai)

Ci=h(IDi ‖ x)

Di=h(PSK ‖ x)⊕Ci

Ei=h(Ai ‖ IDi)⊕h(Ci)

Fi=h(PSK)⊕Ai

2.1.2 로그인 단계

등록 된 서버 SIDj에 액세스하기 위해, 사용자 Ui는 먼저 스마트카드 SCi를 사용하여 서버에 로그인한다<그림 2>.

1) Ui는 스마트카드를 카드 판독기에 삽입하고 IDi와 PWi, 퍼지추출기로 센서에 생체 정보 BIOi를 제시하고 Ri=Rep(BIOi', Pi)를 얻는다.

2) SCi는 사용자의 식별자, 패스워드, 바이오 메트릭의 유효성을 검사하고 로그인 요청을 생성하기 위해 다음 단계를 실행한다.

① SCi는 Ai'=h(PWi ‖ Ri), Bi'=h(IDi ‖ Ai'), Bi'가 Bi와 일치여부를 확인한다. 동일하지 않으면 세션이 종료된다. 일치하면 다음 단계가 실행된다.

② SCi는 임의의 수 Ni를 생성하고 다음을 계산한다.

h(Ci)=h(Ai'‖IDi)⊕Ei

h(PSK)=Fi ‖ Ai'

M1=h(SIDj‖h(PSK))⊕Ni

M2=Di⊕Ni

M3=h(h(Ci)‖Ni)

3) 스마트카드는 로그인 요청 메시지 [M1, M2, M3]를 공개채널을 통해 서버 SIDj로 전송한다.

2.1.3 인증단계

로그인 요청 메시지를 수신 한 서버(SIDj)와 사용자(Ui)는 <그림 2>와 같이 상호작용을 수행하여 서로를 인증하고 세션 키에 동의한다.

1) SIDj는 Ni'=M1⊕h(SIDj ‖ h(PSK))를 계산하고 Ci'=M2⊕h(PSK ‖ x)⊕Ni', M3'=h(h(Ci') ‖ Ni), M3'가 M3와 같은지 여부를 확인한다. 동일하지 않으면 세션은 SIDj에 의해 종료된다. 그렇지 않으면 Ui의 유효성이 서버에 의해 인증되고 SIDj는 다음 단계를 수행한다.

2) SIDj는 임의의 수 Nj를 생성하고 SKji=h(h(Ci') ‖ SIDj ‖ Ni ‖ Nj)를 계산한다.

3) SIDj는 M4=Ni'⊕Nj, M5=h(SKji ‖ Nj)를 계산하고 응답 메시지 [M4, M5]를 Ui에 전송한다.

4) 메시지 [M4, M5]를 수신 한 Ui는 Nj=M4⊕Ni, SKij=h(h(Ci) ‖ SIDj ‖ Ni ‖ Nj)를 계산한다.

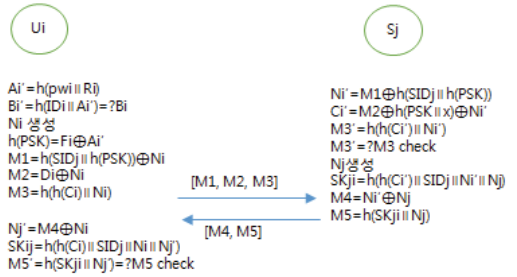

그림 2. 로그인 및 인증단계
Figure 2. Login and authentication phase

5) Ui는 M5'=h(SKij ‖ Nj)를 계산하고 M5'가 M5와 같은지 여부를 확인한다. 일치하지 않으면 세션이 거부된다. 그렇지 않으면, SIDj는 사용자 Ui에 의해 인증되고 마지막으로 세션 키 SKij(=SKji)를 공유한다.

2.2 인증스킴의 비교

2.2.1 Baruah et al's 스킴의 분석

Baruah et al'.s 인증스킴에 대한 안전성을 분석하기 위해 제3자는 합법적인 사용자로 가장하여 SC_i 내에 저장된 정보들에 대해서 전력소비를 탐색[6]함으로써 불법적으로 추출이 가능하다고 가정한다.

Baruah et al'.s 스킴의 특징은 RC로부터 발급받은 비밀정보 h(SIDj ‖ h(PSK))가 각 서버마다 서로 다른 유일한 값을 갖는다. 또한 RC에서 서버로 발급한 파라미터 h(PSK ‖ x)는 모든 서버에게 공통이며 파라미터 h(PSK)는 모든 사용자들에게 공통된 값을 가진다. Baruah et al'.s 스킴의 가장 큰 취약성은 제3자가 사용자의 패스워드나 생체정보를 알지 못하고도 사용자와 서버 간 전송되는 메시지를 가로채서 추출한 정보를 바탕으로 세션 키를 생성할 수 있다는 것이다. RC에 등록된 합법적인 모든 사용자는 파라미터 h(PSK)가 동일하기 때문에 함정이 있다. 이로 인하여 공개채널에서 사용자와 서버의 통신정보를 도청하게 되면 세션 키를 계산할 수 있다.

Baruah et al'.s의 주장과 달리 위장공격, 중간자 도청공격, 재생공격, 서비스거부공격 등에 취약함을 보이고 있다. <표 2>는 Lin et al'.s가 제안한 스킴이 안전하다고 주장한 논리와 본 논문에서 제기한 스킴의 취약성을 주제별로 토의하기 위한 요약물이다.

2.2.2 Lin et al's 스킴의 분석 토의

Lin et al'.s 스킴의 특징은 Baruah et al'.s와 같이 비밀정보 h(SIDj ‖ h(PSK))가 각 서버마다 서로 다른 유일한 값을 가지며 RC에서 서버로 발급한 파라미터 h(PSK ‖ x)는 모든 서버에게 그리고 h(PSK)는 모든 사용자들에게 공통된 값을 가진다. Lin et al'.s 스킴의 가장 큰 취약성은 사용자와 서버 간 공모(colluding)하여 서버가 사용자에게 h(PSK ‖ x)를 제공하였을 경우일 때와 스마트카드 도난 시 제3자는 사전공격으로 합법적 사용자의 식별자(ID)를 쉽게 알아낼 수 있다. 이로 인해 합법적 사용자인 것처럼 서버에 접근할 수 있다.

또한 모든 사용자(Ui, Uj,....Un)들은 서버의 식별자를 알고 있으므로 로그인 메시지 M1의 도청에 의해 임의난수 Ni를 쉽게 계산할 수 있다. 등록 센터에서 사용자에게 제공하는 파라미터에 서버의 식별자가 포함된 계산이 없기 때문이다. 그러므로 합법적 사용자는 Fi로부터 공통파라미터 h(PSK)를 계산할 수 있고 도청된 메시지 M1으로부터 Ni를 구할 수 있다.

표 2. Lin et al'.s 스킴의 주장에 대한 토의
Table 2. Discussion of Lin et al'.s scheme

주제	Lin et al'. 스킴의 주장	토의
3.1 위장공격	· Di와 h(Ci):unknown · h(SIDk ‖ h(PSK)):not compute	· 사용자와 서버 간 공모(colluding)를 가정
3.2 패스워드변경	· $R_1=h(pw_i \| BIO_i)$	· 스마트카드 도용을 가정
3.3 익명성	· 식별자노출 없음	· 서버에 의한 상호인증(사용자)결여
3.4 서비스거부공격	· not attention (언급없음)	· 새로운 파라미터 점검기능 여부
3.5 재전송공격	· 세션마다 N_i, Nj의 새로운 값	· 동일한 메시지에 대한 검증 없음
3.6 상호인증과 신선성	· M3=?M'3, · M5=?M'5 · random nonce N_i, Nj 사용	· 서버 측에서 사용자의 식별불가로 사용자인증 부재
3.7 스마트카드 도난	. IDi가 해쉬함수의 일방향 성질에 의해 보호되어 제3자는 추측불가	. 오프라인에서 사전공격 시 노출

로그인 메시지의 M1을 가로채었을 때 h(SIDj ‖ h(PSK))는 제3자가 은행, 대형쇼핑몰, 의료정보서버, 기밀문서 등 한정된 식별자만 적용되어도 쉽게 구할 수 있다. 또한 합법적 사용자는 도청한 메시지 M2에서 Ni를 사용하여 합법적 사용자 Ui의 Di를 구할 수 있다. 그러므로 Lin et al'.s의 주장과 달리 위장공격, 스마트카드 도난공격, 재생공격, 서비스거부공격 등에 취약함을 보이고 있다.

특히 서버에서 사용자 식별자 인증부재로 Lin et al.'s 스킴은 로그인을 요청하는 사용자가 누구인지에 대한 사용자 식별자의 적절성 여부를 검증하지 않는다. 이러한 식별자의 검증부재는 어떠한 식별자가 로긴 요청을 했을 때 서버는 정해진 메커니즘을 수행함으로 위장공격과 서비스거부공격에 취약하다. 어떤 사용자의 로긴 메시지의 파라미터로 인증단계 2.3의 (1)을 수행한 후 그 결과 값을 비교하여 로긴 요청에 대한 허락 또는 거절을 수행한다.

3. Review of Lin et al.'s Scheme의 취약성

3.1 서버/사용자 위장(Impersonation) 공격

Lin et al.'s 스킴은 서버에서 사용자 식별자에 대해 검증하지 않는 결과는 인증부재로 로그인을 요청하는 사용자가 누구인지에 대한 사용자 식별자의 적절성 여부를 검증하지 않는 문제이다. Lin et al'.s 스킴에서는 사용자 또는 서버가 각각 위장공격을 성립하려면 서버는 h(PSK)를 알아야 하고 사용자들은 파라미터 h(PSK ‖ x)를 알아야 한다. 그러므로 사용자와 서버는 위장공격에 강하다고 주장하고 있다. 본 시나리오는 사용자와 서버간 공모(colluding)하여 서버가 사용자에게 h(PSK ‖ x)를 제공하였을 경우를 가정한다. 악의적 사용자(Adversary, $_A$로 표기)는 $C_i=h(ID_i \| x)$를 임의로 $A_A=h(R_A)$와 같이 생성한다. 악의적 사용자 또는 서버의 위장공격 시나리오는 다음과 같다.

---

step 1 : $A_A=h(R_A)$를 임의로 생성
$B_A=h(PSK \| x)\oplus A_A$
random nonce N_A생성
$M1_A=h(SIDj \| h(PSK))\oplus N_A$

$M2_A=N_A\oplus D_A=NA\oplus h(PSK \| x)\oplus Ci=NA\oplus h(PSK \| x)\oplus A_A$

$M3_A=h(A_A) \| N_A)$

step 2 : 서버 J에게 $M1_A$, $M2_A$, $M3_A$ 전송

step 3 : 서버 J는 다음을 계산한다.

$N_A=M1_A\oplus h(SIDj \| h(PSK))$

$Ci' =M2_A\oplus h(PSK \| x)\oplus N_A=h(PSK \| x)\oplus Ci \oplus N_A\oplus h(PSK \| x)\oplus N_A=A_A$

$M3_A' =h(h(Ci') \| N_A)=?M3_A$

Nj생성

SKji=h(h(Ci') ‖ SIDj ‖ Ni' ‖ Nj)

$M4=N_A\oplus Nj$

M5=h(SKji ‖ Nj)

[M4, M5]

step 4 : 서버 J는 $M4_A$, $M5_A$를 악의적 사용자 A에게 전송한다.

step 5 : 악의적 사용자 A는 다음과 같이 세션키를 생성하고 검증한다.

$Nj=M4_A\oplus N_A)$

$SK_Aj=h(A_A \| SIDj \| NA \| Nj)$

$N5'_A=?h(SK_Aj \| Nj)=?M5A$

이와 같이 사용자와 서버가 공모하였을 경우 누구나 위장하여 세션을 성립시킬 수 있다. Lin et al'.s 스킴의 위장공격에 대한 취약점은 정상적인 로긴 메시지 M1의 해시 값 $h(ID_i \| N_j)$와 C_i의 해시 값 $h(ID_i \| x)$를 다른 임의 값으로 대치했을 때 응용서버 측에서 정당한 사용자의 정보인지를 검증하는 프로토콜의 결여이다.

3.2 스마트카드 도난 공격

Lin et al'.s 스킴에서는 제3자는 스마트카드 정보 {Bi, Di, Ei, Fi, Pi, h(.)}를 추출 할 수있으며 스마트카드로부터 h(PSK)를 계산할 수 있다. 이것은 outsider 공격의 문제이다. 그러면 Fi를 사용하여 Ai를 계산할 수 있다. 그러나 아이디 IDi는 해시함수의 일방향 성질에 의해 보호되기 때문에 제3자에게 추측 할 수 없다. 따라서 분실 된 스마트 카드가 등록되었지만 악의적 인 사용자에 의해 획득된 경우, 도난당한 스마트 카드를 사용하여 암호를 변경하거나 유효한 로그인을 생성하기에 충분한 정보를 얻을 수 없기 때문에 위조 공격을 수행 할 수 없다고 주장했다.

그러나 Ua가 Ui의 스마트카드를 획득했을 때 Ui의 식별자(IDi)를 구하기 위한 오프라인 식별자 추측의 시나리오는 다음과 같다.

---

step 1 : Ua는 공통파라미터 h(PSK)를 알고 있으므로 Ai를 계산한다.

Ai=Fi⊕h(PSK)

step 2 : Ua는 Ui의 가상 식별자를 무작위 또는 사전파일에서 선택(ID^*i)하여 $h(ID^*i \| Ai)$를 계산하여 Bi와 비교한다. Bi와 동일하면 ID^*i는 Ui의 식별자이고 그렇지 않으면 Ua는 다른 식별자 후보자를 선택하여 유효한 ID를 찾을 때까지 동일한 프로세스를 수행한다.

step 3 : Ui의 식별자가 확인되면 Ua는 다음을 계산할 수 있다.

h(Ci)=Ei⊕h(Ai ‖ IDi)

step 4 : Ua는 Ui의 로긴 메시지 M1, M2, M3를 계산할 수 있다.

3.3 사용자 위장 공격

앞에서 기술한 3.2 스마트카드 도난 공격에 성공한 Ua는 Ui의 Di와 h(Ci)를 획득하여 원격 서버에 로그인을 위한 메시지를 쉽게 계산할 수 있다.

---

step 1 : Ua는 임의의 랜덤난수 N^*i를 생성한다.

step 2 : Ua는 다음을 계산한다.

M1=h(SIDj ‖ h(PSK))⊕N*i

M2=Di⊕N*i

M3=h(h(Ci)‖N*i)

step 3 : Ua는 서버접근을 위한 로그인 메시지 M1, M2, M3을 공개채널을 통해 서버 SIDj로 전송한다.

3.4 서비스 거부공격

Lin et al'.s 스킴은 로그인 메시지에 대해 실시간으로 생성된 정보인지를 판단할 수 있는 새로운 메시지(신선성)에 대한 어떠한 질문도 하지 않는다. 다음 시나리오는 n개의 동일한 로긴 메시지를 전송했을 때의 경우이다.

제3자는 이전의 채널에서 로긴 메시지 <M_1, M_2, M_3>를 획득한다.

step 1 : 제3자는 메시지 수정없이 <M_1, M_2, M_3>를 대량(n개) 복사해서 서버 j로 전송한다.

step 2 : 서버 j는 <M_1, M_2, M_3>를 수신하지만 새로 작성된 메시지인지 확인과정이 없다. 또한 연속되는 수신메시지가 동일한 메시지인지 확인하는 과정이 없다.

step 3 : <그림 3>에서와 같이 서버 j는 n개의 로긴 메시지에 대해서 ①-⑧의 과정을 n회 반복 수행한다.

step 4: 서버 j는 제3자에게 응답 메시지 <M_4, M_5>를 n개를 전송한다.

서버 j는 1회의 로긴 메시지에 대해 연산과정은 해시함수 4번 수행, ⊕연산 5번, 랜덤넘버 1회생성이 포함되어 있다. 제3자가 가로챈(intercept)메시지를 동시에 다수를 사용한다면 서버나 네트워크 자원을 사용할 수 없도록 만들기 위해 시도할 수 있다.

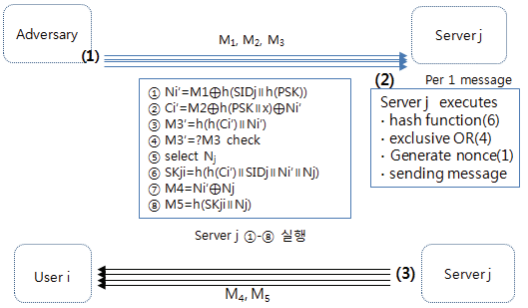

그림 3. 서비스거부공격 시나리오
Figure 3. Denial of Service attack scenario

이와 같이 Lin al's 스킴은 서버 j가 사용자 i로부터 인증메시지의 신선성을 검사하지 않는다. 제3자가 서버 j에 대해 가로챈 메시지를 보냈을 때 서버 j는 이 메시지가 과거데이터인지 현재 데이터인지 알 수가 없다.

3.5 재생공격

앞 3.4의 서비스 거부공격에서와 같이 제3자는 로긴 메시지<M_1, M_2, M_3>를 도청하여 보관하고 있다가 서버 j에게 로긴 메시지를 그대로 전송했을 때를 가정한다.

---

step 1 : 서버 j는 약속된 프로토콜을 진행할 것이다.

Ni' =M1⊕h(SIDj ‖ h(PSK))

Ci' =M2⊕h(PSK ‖ x)⊕Ni'

M3' =h(h(Ci') ‖ Ni')

M3' =?M3 check계산한다.

step 2 : 수신한 M3와 계산한 M3'가 일치하면 임의의 수 N_j를 생성하여 SKji=h(h(Ci') ‖ SIDj ‖ Ni' ‖ Nj), M4=Ni' ⊕Nj, M5=h(SKji ‖ Nj)를 계산한다.

step 3 : 메시지 <M_4, M_5>를 U_i로 전송한다.

step 4 : <M_4, M_5>를 수신한 U_i는 Nj' =M4⊕Ni,

SKij=h(h(Ci) ‖ SIDj ‖ Ni ‖ Nj'), M5'=h(SKji ‖ Nj')를 계산하고 M5와 M5'를 비교한다.

step 5 : 비교하여 일치하면 서버를 인증한다.

이와 같이 Lin et al's 스킴은 로긴 메시지 <M_1, M_2, M_3>와 응답 메시지 <M_4, M_5>에서 임의의 난수 N_i와 N_j가 매 세션마다 새롭게 생성되었다는 것을 확인하는 과정(프로토콜)이 없으므로 제3자의 재전송공격은 성공된다.

3.6 신선성의 결여

Lin et al'.s 스킴에서 사용자의 무작위 수 N_i와 서버의 무작위 수 N_j는 매 세션마다 다르기 때문에 이 프로세스는 데이터의 신선성(freshness)이 있다고 말할 수 있다.

그러나 서버에서 N_i와 사용자의 N_j와 같이 양쪽 모두 N_i와 N_j가 이전에 생성된 무작위 수인지 확인하는 기능이 없다. 그러므로 제3자가 재생공격으로 동일한 메시지를 전송했을 때 이전의 N_i와 N_j가 현재의 N_i와 N_j가 다르게 새로운 파라미터로 생성되었다는 확인기능이 없으므로 신선성 결여라고 할 수 있다.

4. 분석결과

Lin et al'.s 등은 제안스킴에서 스마트카드 정보는 전력소비 시험으로 추출될 수 있다고 가정하고 제3자는 인터넷 공개채널을 통제할 수 있고 사용자와 서버간의 통신을 도청할 수 있다. 또한 제3자는 메시지를 도청, 수정하여 재전송할 수 있으며 제3자는 합법적인 사용자일 수도 있다는 위협을 가정하여 설계하였다.

그러나 분석한 결과 공격의 시나리오에서와 같이 제3자의 위장공격, 스마트카드 도난공격, 재생공격, 서비스거부공격, 패스워드변경 공격 등에 취약함이 드러났다. <표 3>에서 Lin et al'.s 등은 Baruah et al'.s 스킴이 RC에서 사용자들에게 발급하는 공유키 h(PSK)와 등록하는 모든 서버에게 제공되는 공통 비밀키 h(PSK ‖ x)에 의해 사용자의 익명성과 스마트카드 도난공격 등에 취약하다고 분석하였다.

본 논문에서 Lin et al'.s 스킴을 재분석한 결과 모든 사용자는 outsider 공격으로 h(PSK)를 얻을 수 있으며 합법적 사용자와 서비스제공 서버와 공모시에 사용자 및 서버의 위장공격이 쉽게 성립됨을 보였다. 합법적 사용자의 파라미터 Ci를 모르더라도 임의의 값으로 설정하면 인증서버에서 Ci를 검증할 수 없는 문제점이 있었다.

또한 스마트카드 도난 시 합법적인 제3자는 스마트카드내의 파라미터들을 모두 추출할 수 있으며 공통파라미터 h(PSK)의 취약함으로 이를 이용하여 Ai를 얻고 사전공격으로 합법적 사용자의 식별자를 알아냄으로써 사용자의 위장공격이 성립하였다.

Lin et al'.s 등은 임의의 난수 Ni와 Nj가 세션마다 새롭게 생성됨으로 재생공격을 저지할 수 있다고 주장했으나 서버와 사용자의 인증 프로시저에서 Ni와 Nj가 이전의 값이 아니라는 신성성에 대한 체크항목이 없어서 대안이 될 수 없다. 이로 인해 동일한 메시지가 대량 복사되어 반복적으로 로그인을 했을 때 반복적인 인증처리로 프로세서에 부하가 발생하여 자원을 고갈 시킬 수 있다.

Lin et al'.s 스킴에서 로그인 메시지에 사용자의 식별자가 노출되지 않음으로 익명성은 보장되나 서버측에서 사용자에 대한 인증이 간접으로 이루어짐으로 상호인증이 결여(△)되어 있다.

그러므로 세션 키에 대한 합의(△)도 사용자와 서버간에 완전히 인증결과(사용자와 서버의 식별자 확인)에 동의하기 어렵다.

표 3. 보안속성의 재분석 결과
Table 3. The Reanalysis result of security properties

security components	Mishra et al'.s scheme analysis	Baruah et al'.s scheme analysis	Assertion of Lin et al'.s scheme	Reanalysis result for Lin et al'.s scheme
Resist impersonation attack	No	Yes	Yes	No
Smart card stolen attack	No	No	Yes	No
Resist DoS attack	No	No	not attention	No
User anonymity	No	Yes	Yes	Yes
Resist reply attack	Yes	No	Yes	No
Mutual authentication	Yes	Yes	Yes	△
Session key agreement	Yes	Yes	Yes	△
Free password change	Yes	Yes	Yes	Yes
Perfect forward secrecy	No	No	Yes	Yes
Data freshness	No	No	not attention	No

5. 결 론

최근 인터넷과 같은 다중서버구조에서의 사용자와 서버간의 상호인증은 필수적이다. 그러나 그동안 연구되어온 인증 스킴들은 공통적으로 다중서버 환경에서 필수적인 보안의 특성들을 모두 수용하여 설계하는 데는 부족했다.

Lin et al. ‘s 스킴은 Baruah et al.’ s 스킴의 생체인식 기반의 사용자 인증 스킴을 개선하여 제안했으며 익명성과 스마트카드도난 공격에 대한 저항성을 증명하였다.

그러나 그들의 스킴에서 <표 3>에서와 같이 위장공격 및 도난당한 스마트카드 공격, 서비스거부공격, 재생공격 등에 대해 안전하지 않다는 것을 3장의 취약성 분석에서 발견했다. 또한 매 세션마다 새롭게 생성된 로긴 메시지임을 점검할 수 있는 처리 프로토콜을 추가하여야 서비스거부공격, 재생공격에 대한 안전하고 메시지의 신선성을 제공할 수 있다고 본 논문에서 판단하였다.

References

[1] W. J. Tsaur, C. C. Wu, and W. B. Lee, *A smart card-based remote scheme for password authentication in multi-server Internet services*, Computer Standard & Interfaces, Vol. 27, No. 1, pp. 39-51. 2004.

[2] J. L. Tsai, *Efficient multi-server authentication scheme based on one-way hash function without verification table*, Computers & Security, Vol. 27, No. 3, pp. 115-121. 2008.

[3] Y. P. Liao, and S. S. Wang, *A secure dynamic ID based remote user authentication scheme for multi-server environment*, Computer Standards & Interfaces, Vol. 31, No. 1, pp. 24-29. 2009.

[4] H. C. Hsiang, and W. K. Shih,

Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces, Vol. 31, No. 6, pp. 1118-1123. 2009.

[5] T. Wan, N. Jiang, and J. F. Ma, *Cryptanalysis of two dynamic identity based authentication schemes for multi-server architecture*, Communications, China, Vol. 11, No. 11, pp. 125-134. 2014.

[6] T. S. Messerges, E. A. Dabbish, and R. Sloan, *Examining smart-card security under the threat of power analysis attacks*, *IEEE Transactions on Computers*, Vol. 51, No. 5, pp. 541−52, 2002.

[7] C. T. Li, and M. S. Hwang, *An efficient biometrics-based remote user authentication scheme using smart cards*, Journal of Network and Computer Applications, Vol. 33, Issue 1, pp. 1−5, Jan. 2010.

[8] J. Moon, Y. Choi, J. Jung, and D. Won, *An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards,* PLoS ONE, Vol. 10, No. 12, pp. 1-15, 2015.

[9] Y. R. Lu, L. X. Li, H. P. Peng, and Y. X. Yang, *An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem*, Journal of Medical Systems, Vol. 39, No. 32, pp. 1-8, 2015.

[10] Y. Choi, Y. Lee, and D. Won, *Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction*, International Journal of Distributed Sensor Networks, vol. 2016, pp. 1-16, 2016.

[11] C. Li, and M. Hwang, *An efficient biometrics-based remote user authentication scheme using smart card*, Journal of Network and Computer Applications, Vol. 33, pp. 1-5, 2010.

[12] X. Li, J. Niu, J. Ma, W. Wang, and C. Liu, *Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards*, Journal of Network and Computer Applications, Vol. 34, pp. 73-79, 2011.

[13] 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.

[14] 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.

[15] 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.

[16] Y. Lin, K. Wang, B. Zhang, Y. Liu, and X. Li, *An enhanced biometric-based three factors user authentication scheme for multi-server environments*, International Journal of Security and Its Applications,

Vol. 10, No. 1, pp. 315-328, 2016.

[17] Y. Dodis, L. Reyzin, and A. Smith, *Fuzzy extractors: How to generate strong keys from biometrics and other noisy data*, Advances in Cryptology, Vol. 3027, pp. 523-540, 2004.

생체정보 기반의 Lin et al.'s 다중서버 사용자 인증 스킴에 대한 안전성 분석

신광철

성결대학교 산업경영공학부 교수

요 약

생체인식기술의 활용은 쇼핑몰, 의료시스템, 금융권을 중심으로 스마트폰, 태블릿PC 등 모든 스마트기기에 기술이 적용되고 있으며 생체기술의 핵심은 인증기능이다. 인증은 등록된 사용자가 원격서버에서 신원확인의 유효성을 검증하는 것이다. 또한 원격서버에 접근할 수 있게 해주는 기본적인 보안 서비스이다. 암호, 스마트카드 및 생체인식은 인증에서 자주 사용되는 세 가지 요소이다. 다양한 멀티서버 환경에서 원격사용자 인증 스킴들이 많은 연구자들에 의해 제시되었다. Lin et al. 's은 Baruah et al.' s의 스킴이 다중서버환경에서 위장공격, 스마트카드 도난공격 등에 취약하다고 주장하고 개선된 스킴을 제안하였다. 그러나 Lin et al. 's의 인증 스킴을 분석한 결과 일부 파라미터 계산의 취약함이 존재하였다. 그것은 사용자와 서버가 공모하였거나 사용자의 스마트카드가 도난 되었을 때 위장공격, 스마트카드 도난공격, 재생공격, 서비스거부공격에 취약함을 드러냈다. 이와 같이 본 논문에서는 Lin et al'.s 스킴의 취약성을 논리적으로 재분석하고 비교한다.

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