JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 24 No. 10, pp. 41-48, October 2019
https://doi.org/10.9708/jksci.2019.24.10.041

Design Flaws and Cryptanalysis of Cui et al's User Authentication Scheme

Mi-Og Park*

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

[Abstract]

In 2018, Cui et al proposed a three-factor remote user authentication scheme using biometrics. Cui et al claimed that their authentication scheme is vulnerable to eavesdropping attack, stolen smart card attack, and especially Dos(denial-of-service) attack. Also they claimed that it is safe to password guessing attack, impersonation attack, and anonymity attack. In this paper, however, we analyze Cui et al's authentication scheme and show that it is vulnerable to replay attack, insider attack, stolen smart card attack, and user impersonation attack, etc. In addition, we present the design flaws in Cui et al's authentication scheme as well.

▸ **Key words**: User authentication, Biometrics, Stolen smart-card attack, Dynamic identity

[요 약]

2018년 Cui 등은 생체 정보를 사용하는 three-factor 원격 사용자 인증 프로토콜을 제안하였다. Cui 등은 자신들의 인증 프로토콜이 도청 공격, 스마트카드 분실 공격, 특별히 DoS(denial-of-service) 공격에 안전하다고 주장하였다. 또한 그들은 패스워드 추측 공격, 가장 공격, 그리고 익명성 공격 등에 안전하다고 주장하였다. 그러나 본 논문에서는 Cui 등의 인증 프로토콜을 분석하고, 이 인증 프로토콜이 재생 공격, 내부자 공격, 스마트카드 분실 공격, 그리고 사용자 가장 공격 등에 취약함을 보인다. 게다가 우리는 Cui 등의 인증 프로토콜의 설계 오류도 함께 제시한다.

▸ **주제어**: 사용자 인증, 바이오메트릭스, 스마트카드 분실 공격, 동적 ID

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@hanmail.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2019. 08. 29, Revised: 2019. 10. 21, Accepted: 2019. 10. 21.

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

I. Introduction

스마트카드 기반의 원격 사용자 인증 스킴은 사용자의 ID와 패스워드를 사용하여 원격 사용자를 인증하는 two-factor 인증 스킴들[1][2][3][4]이 주로 연구되고 있다. 최근의 원격 사용자 인증 스킴들에서는 사용자의 ID와 패스워드뿐만 아니라 사용자의 생체 정보를 함께 사용하는 three-factor 인증 스킴들[5][6][7][8]이 연구되고 있는 추세이다. 2018년 Cui 등[9]은 사용자의 생체 정보를 사용한 three-factor 인증 스킴을 제안하였다. Cui 등은 생체 정보를 사용한 인증 스킴들과 multi-server 환경에서 동적 ID(dynamic identity)를 사용한 인증 스킴[10], 그리고 multi-server 환경에서 사용자의 생체 정보를 사용한 인증 스킴[11] 등에 대해 언급하였다. Li 등[12]은 Li-Hwang 등[13]이 제안한 three-factor 인증 스킴이 중간자 공격(man-in-the-middle attack)과 적절한 인증을 보장하지 못한다고 분석하고, 이를 개선한 three-factor 인증 스킴을 제안하였다. Li 등의 인증 스킴과 Li-Hwang 등의 인증 스킴은 두 인증 스킴 모두 동적 ID는 사용하지 않는다. Li-Hwang 등의 인증 스킴은 본 논문에서 분석한 결과, 등록 단계에서 사용자의 ID와 패스워드, 그리고 사용자의 생체 정보를 원본 그대로 등록 센터에 제공하기 때문에 내부자 공격(insider attack)에 취약하다. 이를 개선한 Li 등의 인증 스킴은 등록 단계에서 사용자의 ID와 생체 정보는 원본 그대로 등록 센터에 제공하고, 사용자의 패스워드는 난수 N으로 해쉬 연산한 $h(N||PW_i)$를 등록 센터에 제공하여 ID와 생체 정보는 내부자 공격에 취약하다. Xue 등의 인증 스킴[10]은 multi-server 환경에서 사용자의 동적 ID를 위한 CID_i와 서버의 ID인 SID_j를 사용하고, Li 등의 인증 스킴처럼 비밀 공유 값(secret number) y를 사용한다. He-Wang의 인증 스킴[11]은 ECC를 사용한 multi-server 환경의 three-factor 인증 스킴으로, 사용자의 동적 ID와 서버의 ID를 사용하며 사용자가 등록 센터에 등록하는 단계에서 퍼지 추출(fuzzy extractor)을 사용한다. 또한 He-Wang의 인증 스킴은 계산 비용과 통신 비용의 효율성을 다른 인증 스킴들과 비교.분석함으로써, 자신들의 인증 스킴이 분산 멀티 환경에서 활용하기 적절한 인증 스킴이라고 주장하였다. Vanga 등[14]는 He-Wang의 인증 스킴에 대한 안전성을 분석하여, He-Wang 등의 인증 스킴이 재생 공격(replay attack), 사용자 익명성(user anonymity), 사용자 가장 공격(user impersonation attack), 그리고 사용자의 잘못된 패스워드 로그인으로 인하여 정당한 사용자에 의한 DoS(denial-of-service) 공격 등에 안전하지 않음을 보였다. Cui 등의 인증 스킴은 multi-server 환경에서의 인증 스킴들을 언급하였으나, 자신들의 인증 스킴은 multi-server 환경이 아닌 일반적인 사용자 인증 환경상에서의 새로운 three-factor 인증 스킴을 제안하였다. Cui 등은 자신들의 인증 스킴이 도청 공격(eavesdropping attack), 스마트카드 분실 공격(stolen smart card attack), 그리고 DoS 공격에 특별히 안전하다고 주장하였으며, 이 외에도 패스워드 추측 공격(password guessing attack), 가장 공격, 익명성 공격 등에 안전하다고 주장하였다. 그러나 본 논문에서 Cui 등의 인증 스킴을 분석한 결과, 그들의 주장과 달리 Cui 등의 인증 스킴은 스마트카드 분실 공격에 취약하고, 이로 인하여 사용자 가장 공격과 DoS 공격 등에도 취약하였다. 본 논문에서는 Cui 등의 인증 스킴에서 미분석한 안전성 항목으로 재생 공격, 내부자 공격, 패스워드 오입력 등에 대해서도 분석하여, 이 모든 항목들에서도 Cui 등의 인증 스킴이 안전하지 않음을 보일 것이다. 또한 본 논문에서는 Cui 등의 인증 스킴이 다른 인증 스킴들에 비해 설계상의 여러 오류가 존재함을 보인다.

본 논문의 구성은 2장에서 Cui 등의 인증 스킴에 대한 각 단계를 살펴보고, 3장에서 Cui 등의 인증 스킴에 대한 안전성 분석과 함께 설계상의 여러 오류가 존재함을 보인다. 마지막으로 4장에서 결론을 내리고 본 논문을 마친다.

II. Related Works

1. Cui et al's Authentication Scheme

본 장에서는 Cui 등이 제안한 생체 정보 기반의 three-factor 인증 스킴[9]에 대해 살펴본다. Cui 등의 인증 스킴에서 사용한 기호는 Table 1과 같다.

1.1 Registration Phase

사용자 U_i가 등록 센터 RC에 자신의 정보를 등록하기 위해서, 자신의 ID_i와 패스워드 P_i, 그리고 자신의 생체 정보 B_i를 입력하면, 스마트카드는 난수 N을 생성하여, 등록 센터에 $\{ID_i, B_i, P_i, N\}$을 전송한다. 등록 요청 메시지를 받은 RC는 Fig. 1.과 같이 다음 과정을 실행한다.

(1)사용자의 패스워드 P_i와 난수 N을 사용하여 $RPW_i=h(N||P_i)$를 계산한다.

(2)사용자의 ID_i와 난수 N을 사용하여 동적 ID $CID_i=h(N||ID_i)$를 계산한다.

(3)사용자의 생체 정보 B_i와 RPW_i를 XOR하여 $BPW_i=B_i \oplus h(RPW_i)$를 계산한다.

(4)사용자의 정당성 검증을 위해 사용하는 $e_i=h(CID_i||x) \oplus RPW_i$를 계산한다.

(5)사용자의 ID_i와 패스워드 P_i의 정당성 검증을 위해 사용하는 $T_i=h(CID_i||RPW_i)$를 계산한다.

(6)$H_i=h(T_i)$를 계산한다.

(7)등록 센터는 스마트카드에 {BPW_i, H_i, e_i, h(.), y, N}을 저장한다.

(8)사용자 U_i에게 스마트카드를 보낸다.

1.2 Login Phase

단계1.사용자 U_i가 자신의 ID_i와 패스워드 P_i를 입력하면, 스마트카드는 다음 단계를 실행한다.

(1)사용자의 ID_i와 스마트카드에 저장된 난수 N을 이용하여 사용자의 동적 ID인 $CID_i=h(N||ID_i)$를 계산한다.

(2)입력받은 사용자의 패스워드 P_i와 난수 N을 이용하여 $RPW_i=h(N||P_i)$를 계산한다.

(3)앞에서 계산한 CID_i와 RPW_i를 이용하여 $T_i=h(CID_i||RPW_i)$를 계산한다.

(4)앞에서 계산한 T_i에 해쉬 연산하여 $h(T_i)$를 계산한 후, 스마트카드에 저장된 H_i와의 동일성 여부를 체크한다. 두 값이 동일하지 않을 경우 세션을 종료하고, 동일할 경우 다음 단계를 계속 실행한다.

(5)스마트카드는 사용자의 생체 정보 B_i'를 입력받는다.

(6)RPW_i를 해쉬 연산($h(RPW_i)$)한 후, 스마트카드에 저장된 BPW_i와 함께 $B_i=BPW_i \oplus h(RPW_i)$를 계산한다. B_i'과 계산한 B_i와의 동일성 여부를 체크하여 임계값 보다 작으면 세션을 종료하고, 임계값이 크거나 동일하면 다음 단계 2를 진행한다.

단계2.스마트카드는 다음 과정들을 실행한다.

(1)e_i와 RPW_i를 이용하여 $M_1=e_i \oplus RPW_i$를 계산한다.

(2)난수 R_c를 생성하여 $M_2=M_1 \oplus R_c$를 계산한다.

(3)비밀 키 y와 R_c를 이용해 $M_3=h(y||R_c)$를 계산한다.

(4)M_3와 RPW_i를 이용하여 $M_4=RPW_i \oplus M_3$를 계산한다.

(5)M_2, M_3, M_4를 이용해 $M_5=h(M_2||M_3||M_4)$를 계산한다.

(6)서버 S_j에게 {CID_i, M_2, M_4, M_5}를 전송한다.

1.3 Authentication Phase

단계1.서버 S_j는 다음 과정을 실행한다.

(1)서버 S_j는 전송받은 CID_i와 자신의 비밀 키 x를 이용하여 $M_6=h(CID_i||x)$를 계산한다.

(2)계산한 M_6과 전송받은 M_2를 이용하여 $M_7=M_2 \oplus M_6$을 계산한다.

(3)계산한 M_7과 y를 사용하여 $M_8=h(y||M_7)$를 계산한다.

(4)전송받은 M_5와의 동일성 여부 검증을 위해, $h(M_2||M_8||M_4)$를 계산한다. 만약 두 값이 동일할 경우 사용자는 정당한 사용자라고 인증하여, 다음 단계를 계속 실행하고 그렇지 않을 경우 세션을 종료한다.

단계2.서버 S_j는 다음 과정들을 실행한다.

(1)전송받은 M_4와 앞에서 계산한 M_8을 사용하여 $M_9=M_4 \oplus M_8$을 계산한다.

(2)서버의 ID SID_j와 앞에서 계산한 M_6과 M_8, 그리고 M_9를 사용하여 $M_{10}=h(M_9||SID_j||M_8||M_6)$를 계산한다.

(3)난수 R_s를 생성하여 $M_{11}=h(M_9||SID_j||y) \oplus M_8 \oplus R_s$를 계산한다.

(4)$M_{12}=h(M_6||M_9||R_s||y)$를 계산한다.

(5)서버 S_j는 {M_{10}, M_{11}}을 스마트카드로 전송한다.

단계3.{M_{10}, M_{11}}을 전송받은 스마트카드는 다음 과정들을 실행한다.

(1)M_{10}과 $h(RPW_i||SID_j||M_3||M_1)$를 계산한 결과 값의 동일성 여부를 체크한다. 두 값이 동일할 경우 스마트카드는 서버를 정당한 서버로 인증하고 다음 과정을 계속 실

Table 1. Notations

Symbols	Description
RC	Registration center
S_j	The j-th server
U_i	The i-th User
ID_i	The ith user's IDentity
P_i	The password of the user U_i
B_i	The biometrics of the user U_i
SID_j	The identity of S_j
x	The master key selected by RC that shared with the server
y	One key shared by the RC, server, and the user
N, R_u, R_s, R_c	Random number
CID_i	The dynamic identity generated by U_i for authentication
SK	Session key
h(.)	One way hash function
||	Concatenation operation
$\oplus$	Exclusive-OR operation

User U_i(smart card)		Registration Center(RC)
The user select ID_i, P_i		
Enter biometric information B_i		
Smart card generates		
random number N	$\{ID_i, B_i, P_i, N\}$ ---------->	Compute $RPW_i = h(N\|\|P_i)$
		$CID_i = h(N\|\|ID_i)$
		$BPW_i = B_i \oplus h(RPW_i)$
		$e_i=h(CID_i\|\|x) \oplus RPW_i$
		$T_i=h(CID_i\|\|RPW_i)$
		$H_i=h(T_i)$
Users get smart card	<----------	Store $\{BPW_i, H_i, e_i, h(.), y, N\}$ in smart-card

Fig. 1. Cui et al's Authentication scheme – Registration Phase

는 서버를 정당한 서버로 인증하고 다음 과정을 계속 실행한다. 그렇지 않을 경우 세션을 종료한다.

(2)$M_{13}=h(RPW_i||SID_j||y) \oplus M_3 \oplus M_{11}$을 계산한다.

(3)스마트카드는 세션 키 $SK=h(M_1||RPW_i||R_c||M_{13}||y)$을 계산하고, 서버는 세션 키 $SK=h(M_6||M_9||M_7||R_s||y)$를 계산한다.

1.4 Password Change Phase

사용자가 자신의 ID_i와 패스워드 P_i를 입력하면 스마트카드는 다음 과정들을 실행한다.

(1)$RPW_i=h(N||P_i)$와 $CID_i=h(N||ID_i)$, 그리고 $T_i=h(CID_i||RPW_i)$를 계산한다.

(2)$h(T_i)$와 H_i의 동일성 여부를 검증하여, 동일하지 않을 경우 세션을 종료하고, 그렇지 않을 경우 새로운 패스워드 P_i^{new}를 입력받는다.

(3)$RPW_i^{new}=h(N||P_i^{new})$와 $T_i^{new}=h(CID_i||RPW_i^{new})$를 계산한다.

(4)$H_i^{new}=h(T_i^{new})$와 $B_i=BPW_i \oplus h(RPW_i)$를 계산한다.

(5)$RPW_i=B_i \oplus h(RPW_i^{new})$와 $h(CID_i||X)=e_i \oplus RPW_i$를 계산한다.

(6)$e_i^{new}=h(CID_i||X) \oplus RPW_i^{new}$를 계산한다.

(7)새로운 $\{BPW_i^{new}, H_i^{new}, e_i^{new}, h(.), y\}$를 저장한다.

III. Analysis of Cui et al's Authentication Scheme

1. Cryptanalysis and Design Flaws

3.1 Cryptanalysis

본 절에서는 Cui 등의 인증 스킴에 대한 안전성을 분석하여, Cui 등의 인증 스킴이 스마트카드 분실 공격, 사용자 가장 공격, 패스워드 추측 공격, 그리고 DoS 공격 등에 취약함을 보인다. 또한 본 논문에서는 Cui 등의 인증 스킴에서 미분석한 항목인 재전송 공격, 내부자 공격, 그리고 패스워드 업데이트 단계에서 사용자의 실수로 인한 패스워드 오입력 등에 대한 안전성에 대해서도 분석한다. 본 논문에서 재분석한 안전성 결과는 Table 2에 나타내었다.

스마트카드 분실 공격

Cui 등이 스마트카드 분실 공격에 대한 안전성을 분석할 때, 그들이 가정했던 것과 동일한 가정 하(순서)에 Cui 등의 인증 스킴이 스마트카드 분실 공격에 취약함을 보인다. 다음의 과정(1), (2), (3)은 Cui 등이 스마트카드 분실 공격에 대한 안전성을 분석할 때 나열한 순서 그대로 나열하되, Cui 등이 잘못 분석한 내용을 본 논문에서 올바르게 분석한 것이다.

(1) $CID_i= h(N||ID_i)$

Cui 등은 이 식에서 공격자가 사용자의 ID_i를 계산할 수 없기 때문에 안전하다고 분석하였다. 그러나 전송 메시지에 CID_i가 있고 스마트카드의 저장 정보 중 난수 N과 해쉬함수 h(.)가 있기 때문에, 위의 양쪽 식이 동일해질 때까지 계속 계산을 진행하여 사용자의 ID_i를 획득할 수 있다[3][15].

(2) $BPW_i = B_i \oplus h(RPW_i)$

Cui 등은 (2) 식을 통하여 패스워드 P_i가 틀릴 경우, 공격자는 사용자의 올바른 생체 정보 B_i를 획득할 수 없기 때문에 자신들의 인증 스킴이 안전하다고 분석하였다. 그러나 본 논문에서는 공격자가 스마트카드를 획득하였을 경우, 다음에서 제시하는 과정에 의해 공격자가 패스워드 추측 공격에 성공할 수 있고, 결과적으로 사용자의 생체 정보 B_i를 획득할 수 있음을 보인다. 다음 식과 전송 메시지 CID_i, 그리고 스마트카드의 저장 정보 H_i와 난수 N을

User U_i(smart card)		Server S_j
Inputs ID_i, P_i		
Smart card compute		
$CID_i = h(N\|\|ID_i)$		
$RPW_i = h(N\|\|P_i)$		
$T_i = h(CID_i\|\|RPW_i)$		
Verify $H_i' \stackrel{?}{=} h(T_i)$		
Input biological feature B_i'		
Smart card compute $B_i = P_i \oplus h(RPW_i)$		
Verify $B_i \stackrel{?}{=} B_i'$		
Generate random number R_c		
Compute $M_1 = e_i \oplus RPW_i$		
$M_2 = M_1 \oplus R_c$		
$M_3 = h(y\|\|R_c)$		
$M_4 = RPW_i \oplus M_3$		
$M_5 = h(M_2\|\|M_3\|\|M_4)$	$\{CID_i, M_2, M_4, M_5\}$ ---------->	Compute $M_6=h(CID_i\|\|x)$
		$M_7=M_2 \oplus M_6$
		$M_8=h(y\|\|M_7)$
		Verify $h(M_2\|\|M_8\|\|M_4) \stackrel{?}{=} M_5$
		Generate random number R_s
		Compute $M_9=M_4 \oplus M_8$
		$M_{10}=h(M_9\|\|SID_j\|\|M_8\|\|M_6)$
		$M_{11}=h(M_9\|\|SID_j\|\|y) \oplus M_8 \oplus R_s$
Verify	$\{M_{10}, M_{11}\}$	$M_{12}=h(M_6\|\|M_9\|\|R_s\|\|y)$
$h(RPW_i\|\|SID_j\|\|M_3\|\|M_1) \stackrel{?}{=} M_{10}$	<----------	
Compute		
$M_{13}=h(RPW_i\|\|SID_j\|\|y) \oplus M_3 \oplus M_{11}$		
$SK=h(M_1\|\|RPW_i\|\|R_c\|\|M_{13}\|\|y)$	<---------->	$SK=h(M_6\|\|M_9\|\|M_7\|\|R_s\|\|y)$

Fig. 2. Cui et al's Authentication scheme – Login Phase and authentication Phase

이용한다.

$H_i \stackrel{?}{=} h(T_i) = h(h(CID_i||RPW_i))$

$\stackrel{?}{=} h(h(h(N||ID_i)||h(N||P_i)))$

사용자의 P_i의 추측 공격에 성공하면, $B_i=P_i \oplus h(RPW_i)$를 사용하여 사용자의 B_i를 단 한번의 XOR 연산으로 쉽게 계산할 수 있다. 이 과정을 통해 공격자는 사용자의 가장 중요한 정보들 즉, 사용자의 ID_i와 패스워드 P_i, 그리고 생체정보 B_i까지 획득할 수 있다.

(3) $e_i = h(CID_i||x) \oplus RPW_i$

Cui 등은 앞의 두 과정(1), (2)에서 사용자의 ID_i와 P_i를 계산할 수 없다고 분석하였고, 그래서 이 과정(3)도 공격자가 성공할 수 없다고 분석하였다. 그러나 본 논문에서 분석한 바와 같이 공격자는 사용자의 ID_i, P_i, 그리고 B_i까지 모두 획득할 수 있고, 스마트카드를 획득하였을 경우 카드의 저장 정보 e_i와 난수 N, 그리고 과정(2)에서 획득한 $RPW_i=h(N||P_i)$를 이용하여 $e_i \oplus RPW_i=h(CID_i||x)$를 계산한다. 공격자는 단 한번의 XOR 연산으로 $h(CID_i||x)$계산해 낼 수 있다.

사용자 가장 공격

공격자는 앞의 과정들에서 획득한 사용자의 ID_i, P_i, B_i, $h(CID_i||x)$, 그리고 스마트카드 분실 공격에서 획득한 정보들을 사용하면, 로그인 단계에 필요한 모든 정보를 다 가지고 있기 때문에 정당한 사용자가 로그인 단계에서 행하는 모든 계산을 성공적으로 해낼 수 있다. 그러므로 Cui 등의 인증 스킴은 사용자 가장 공격에 취약하다.

패스워드 추측 공격

Cui 등의 인증 스킴은 스마트카드 분실 공격 절에서 분석한 바와 같이 공격자가 스마트카드를 획득한 경우, 패스워드 추측공격에 성공할 수 있으므로 Cui 등의 인증 스킴은 패스워드 추측공격에 취약하다고 할 수 있다.

내부자 공격

Cui 등의 인증 스킴은 등록 단계에서 사용자가 등록 센

Table 2. The Results of Reanalysis of the Cui et al's Authentication Scheme

Function	Cui et al's Scheme	Reanalysis Results of Cui's scheme
Resist Stolen smart card attack	Yes	No
Resist Password guessing attack	Yes	No
Resist Dos attack	Yes	No
Resist Impersonation attack	Yes	No
Resist Anonymity attack	Yes	No
Correct Password update	Yes	No
Resist Insider attack	-	No
Resist Wrong password login	-	No
Resist Replay attack	-	No
Mutual authentication	Yes	No

터에게 평문 형태의 {ID_i, B_i, P_i, N}을 전송한다. 그러므로 서버의 내부 공격자는 사용자의 정보들을 유추 공격할 필요 없이 원형 그대로의 정보를 획득하여 사용할 수 있다.

패스워드 오입력

Cui 등의 인증 스킴은 패스워드 변경 단계 (2)에서 사용자가 새로운 패스워드 P_i^{NEW}를 입력하면 이 P_i^{NEW}를 사용하여 (3)에서 새로운 RPW_i^{NEW}를 곧바로 계산한다. (2)와 (3)에서 사용자가 패스워드를 잘못 입력하는 것을 체크하는 과정이 부재하기 때문에, 사용자가 패스워드를 잘못 입력한 후 새롭게 로그인을 한다면, 스마트카드의 정당한 소유자임에도 불구하고 카드를 사용할 수 없는 문제가 발생할 수 있다.

재전송 공격

공격자가 이전의 전송 메시지를 재전송할 경우, 서버는 인증 절차에 따라 전송받은 CID_i에 자신의 비밀 키 x를 해쉬 연산하여 M_6를 계산하고, 전송 메시지 M_2와 M_6을 사용하여 $M_7=M_2 \oplus M_6$을 계산한다. 그런 다음 비밀 공유키 y를 이용하여 $M_8=h(y||M_7)$를 계산한다. 이렇게 계산된 값들은 사용자의 정당성 체크를 위해 전송 메시지 M_5와 서버가 계산한 값 $h(M_2||M_8||M_4)$를 비교하여 사용자의 정당성을 체크한다. 이러한 인증 과정을 볼 때 Cui 등의 인증 스킴은 재전송 메시지를 체크할 수 있는 방법이 부재하여 재전송 공격에 취약하다.

DoS 공격

Cui 등의 인증 스킴은 로그인 단계에서 사용자의 ID_i와 P_i, B_i'을 입력받은 후 T_i, B_i와 각각 비교하여 카드 소유자를 검증하고, 이러한 과정은 서버에 대한 DoS 공격을 막을 수 있다. 그러나 스마트카드를 분실한 경우에는 앞에서 분석한 바와 같이, 공격자가 로그인 단계를 모두 통과할 수 있으므로 Cui 등의 인증 스킴은 DoS 공격에 취약하다.

3.2 Design Flaw

본 절에서는 Cui 등의 인증 스킴에 대한 설계상의 오류로 인하여 발생하는 문제점들을 분석한다.

서버 ID 분배 방법의 부재

Cui 등의 인증 스킴은 서버의 ID SID_j를 사용하여 M_{10}과 M_{11}을 계산한다. 인증 단계3에서 스마트카드는 서버의 정당성 확인을 위해 $h(RPW_i||SID_j||M_3||M_1)$를 계산하여 M_{10}과 동일한지 체크하고, M_{13}을 계산하기 위해 SID_j를 사용한다. 그러나 Cui 등의 인증 스킴은 사용자에게 서버의 SID_j를 전달하는 메커니즘을 제시[16][17][18]하거나 사용자가 이 SID_j를 알고 있다는 가정 등이 없다. 그러므로 Cui 등의 인증 스킴은 정당한 사용자라할지라도 $h(RPW_i||SID_j||M_3||M_1)$를 계산하기 위한 SID_j를 모르기 때문에, 서버의 정당성 여부를 제대로 검증할 수 없다. 또한 세션 키 생성 시에도 사용자는 SID_j를 알 수 없기 때문에, 세션 키를 성공적으로 생성할 수 없다.

패스워드 변경 단계

Cui 등의 패스워드 변경 단계를 살펴보면, (2)에서 새로운 패스워드 P_i^{new}를 생성하고, (3)에서 새로운 RPW_i^{new}와 T_i^{new}를, (4)에서 H_i^{new}를, (6)에서 e_i^{new}를 계산한다. 그러나 새로운 BPW_i^{new}를 업데이트하지 않고 이전의 BPW_i가 그대로 사용되어, 사용자가 다음 세션에서 로그인할 경우, 새로운 패스워드를 입력해도 H_i'?=$h(T_i)$ 과정을 통과할 수 없기 때문에 스마트카드의 소유자임에도 불구하고 로그인 단계를 통과할 수 없다.

불안전한 사용자 익명성

Cui 등은 동적 ID CIDi가 매 세션마다 변경되기 때문에 익명성 공격에 안전하다고 주장하였다. 그러나 Cui 등의 인증 스킴을 분석한 결과, 로그인 단계에서 매번 스마트카드에 저장된 난수 N과 함께 사용자의 ID_i를 해쉬 연산하기 때문에, 난수 N이 변경되지 않아 매 세션마다 CID_i 값이 동일하게 된다. 그러므로 Cui 등의 인증 스킴은 안전한 사용자 익명성을 제공하지 못한다.

계산 오버헤드

Cui 등의 인증 스킴은 M_{12}를 계산하지만 단 한 번도 사용하지 않는다. 그러므로 M_{12}의 불필요한 계산으로 인하여 서버의 계산 오버헤드를 발생시킨다.

y에 대한 정의

Cui 등의 인증 스킴은 y를 등록 센터와 서버, 그리고 사용자가 함께 공유하는 키라고 Table. 1에 나타내었으나, 이 y의 사용 용도를 고려할 때 비밀 값(secret number)으로 정의하는 것이 더 타당한 것으로 보인다[10][12][19].

3.3 Simple Method of Improvement

Cui 등의 인증 스킴을 개선하기 위한 간단한 방법은 등록 단계에서 사용자의 패스워드와 생체 정보를 평문형태로 서버에 제출하는 것이 아니라, 각각을 난수로 해쉬 연산한 $RPW_i=h(N||P_i)$나 $BPW_i=h(B_i)\oplus h(RPW_i)$와 같은 형태로 서버에 제출함으로써, 사용자의 패스워드와 생체 정보가 공격자에게 그대로 노출되는 것을 막을 수 있다. 서버 내의 공격자는 RPW_i와 BPW_i의 결과 값만을 알 수 있고 해쉬 함수에 사용한 난수는 모르기 때문에, 사용자가 짧은 패스워드 P_i를 사용한다 할지라도 패스워드 추측공격에 성공하기 어렵다. 해쉬 연산한 사용자의 생체 정보($h(B_i)$)와 같은 형태도 해쉬 연산과 생체 정보의 높은 엔트로피 때문에 공격자가 사용자의 생체 정보를 추측해내기 어렵다. 또한 재생공격에 취약한 Cui 등의 인증 스킴은 메시지의 구성에 타임스탬프를 추가하는 간단한 방법으로 재생공격을 막을 수 있다.

IV. Conclusions

Cui 등은 자신들의 인증 스킴이 여러 공격에 안전한 인증 스킴이라고 주장하였으나 본 논문에서 분석한 결과, 사용자의 ID와 패스워드 추측 공격, 스마트카드 분실 공격, 재생 공격, 내부자 공격, 패스워드 오입력 등에 취약하였으며, 공격자가 XOR 연산으로 사용자의 생체 정보까지 획득할 수 있어 사용자 가장 공격에도 취약하였다. 게다가 Cui 등의 인증 스킴은 설계상의 많은 오류가 존재하였으며, 사용자가 서버의 SID_j를 알 수 있는 방법의 부재로 인해 사용자측에서 서버에 대한 상호인증과 세션 키를 제대로 생성할 수 없는 문제가 존재하였다. 그러므로 Cui 등의 인증 스킴은 안전한 사용자 인증 스킴이라고 할 수 없다.

앞으로의 향후 과제는 본 논문에서 분석한 결과를 토대로 하여 보다 안전한 사용자 인증 스킴의 설계가 필요할 것으로 보인다. 특별히 내부자 공격과 스마트카드 분실 공격에 취약할 경우 다른 대부분의 여러 공격에도 취약한 경우가 많기 때문에, 이 두 공격에 안전한 two-factor 인증 스킴이나 three-factor 인증 스킴에 대한 연구가 필요할 것으로 보인다.

REFERENCES

[1] Y.J. Liu, C.C. Chang, and S.C. Chang, "An Efficient and Secure Smart Card Based Password Authentication Scheme," International Journal of Network Security, Vol. 19, No. 1, pp. 1-10, January 2017.

[2] P. Chandrakar and H. Om, "An Efficient Two-Factor Remote User Authentication and Session Key Agreement Scheme Using Rabin Cryptosystem," Arabian Journal for Science and Engineering, Vol. 43, No. 2, pp. 661-673, February 2018.

[3] Y. Choi, "Security Enhanced Anonymous Two Factor Mutual Authentication Scheme with Key Agreement," Korea Digital Content Society, Vol. 19, No. 12, pp. 2415-2422, December 2018.

[4] W. Zheng, Z..Gui, D. Liu., X. Li, and B. Chen, "Lightweight Certificateless Two-Factor Authentication Protocol Using Smart Cards," Journal of Internet Technology, Vol. 19 No.7, pp. 2227-2234, 2018.

[5] A. K. Das, "Analysis and Improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, Vol. 5, No. 3, pp. 541-552, 2011.

[6] Y. An, "Analysis and Improvements of a Biometrics-based User Authentication Scheme Using Smart Cards," Journal of the Korean Society of Computer Information, Vol. 17 No. 2 pp. 159-166, February 2012.

[7] Y. An, "Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards," Journal of Biomedicine and Biotechnology, Vol.

2012, Article ID 519723, pp. 1-6, 2012.
[8] S. Ibjaoun, A.E. Kalam, V. Poirriez, A. Ouahman, and M. Montfort, "Analysis and enhancements of an efficient biometric based remote user authentication scheme using smart cards," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications, 2016.
[9] J. Cui, R. Sui, X. Zhang, H. Li, and N. Cao, "A Biometrics-Based Remote User Authentication Scheme Using Smart Cards," 3rd International Conference on Computer and Communication Systems 2018, pp. 531-542, 2018. https://doi.org/10.1007/978-3-030-00015-8_46
[10] K.P. Xue, P.L. Hong, and C.S. Ma, "A Lightweight Dynamic Pseudonym Identity based Authentication and Key Agreement Protocol without Verification Tables for Multi-server Architecture," Journal Computer and System Sciences, Vol. 80, Issue. 1, pp. 195-206, February 2014.
[11] D.B. He, and D. Wang, "Robust Biometrics-based Authentication Scheme for Multi Server Environment," IEEE System Journal Vol. 9, Issue. 3, pp. 816-823, September 2015.
[12] X. Li, J.W. Niu, J. Ma, W.D. Wang, and C.L. Liu, "Cryptanalysis and Improvement of a Biometrics-based Remote User Authentication Scheme using Smart Cards," Journal of Network and Computer Applications, Vol. 34, No. 1, pp. 76-79, 2011.
[13] 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, No. 1, pp. 1-5, 2010.
[14] V. Odelu, A.K. Das, and A. Goswami, "A Secure Biometrics-based Multi-server Authentication Protocol using Smart Cards," IEEE Transactions on Information Forensics and Security, Vol. 10, No. 9, pp. 1953-1966, 2015.
[15] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A Hybrid Password Authentication Scheme Based on Shape and Text," Journal of Computers, Vol. 5, No. 5, pp. 765-772, May 2010.
[16] Y.S. Choi, J.H. Nam, D.H. Lee, J.Kim, J.W. Jung, and D.G. Won, "Security Enhanced Anonymous Multi Server Authenticated Key Agreement Scheme using Smart Cards and Biometrics," Scientific World Journal, Vol. 2014, Article ID 281305, pp. 1-15, 2014. http://dx.doi.org/10.1155/2014/281305
[17] M. Qi, J. Chena, and Y. Chen, "A Secure Biometrics-based Authentication Key Exchange Protocol for Multi-server TMIS using ECC," Computer Methods and Programs in Biomedicine, Vol. 164, pp. 101-109, 2018. https://doi.org/10.1016/j.cmpb.2018.07.008
[18] W.S. Juang, "Efficient Multi-server Password Authenticated Key Agreement Using Smart Cards," IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 251-255, February 2004.
[19] W.J. Tsuar, C.C. Wu, and W.B. Lee, "A Flexible User Authentication for Multi-server Internet Services," Networking -ICN 2001 First International Conference on Networking 2001, Vol. 2094, pp. 174-183, July 2001.

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.