Journal of The Korea Society of Computer and Information
Vol. 19, No. 10, October 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.10.099

'스마트카드를 이용한 생체인식기반 사용자 인증스킴의 분석 및 개선'의 내용 오류와 안전성 분석

박 미 옥*, 오 기 욱**

Contents Error and Security Analysis of 'Security Analysis and Improvements of a Biometrics-based User Authentication Scheme Using Smart Cards'

Mi-Og Park*, Gi-Oug OH**

요 약

본 논문에서는 An이 제안한 생체인식기반 사용자 인증스킴의 취약점을 분석한다. 본 논문에서 제안한 로그인 성공 시나리오에 의해 An의 인증스킴을 분석한 결과, 공격자는 전송 메시지만을 이용하여 사용자의 난수 획득에 성공할 경우, 정당한 서버에서의 사용자 인증단계를 통과할 수 있다. 또한 본 논문에서 제안한 생체정보 추측 시나리오에 의해 스마트카드 분실시 정당한 사용자의 생체정보가 노출되는 것을 보인다. An의 인증스킴은 평문형태의 사용자 ID와 생체정보를 서버에 제출하기 때문에 내부자 공격에 매우 취약하고, 평문 형태의 사용자 ID로 인하여 제3자에 대한 사용자 익명성뿐만 아니라 서버에 대한 사용자 익명성도 보장하지 못한다. 게다가 An의 인증스킴은 내용 문맥상의 오류도 존재하며, 이로 인해 스마트카드 소유자의 정당성을 체크하지 못하는 취약점 등이 있다.

▸ Keywords : 생체 정보, 스마트카드, 상호 인증

Abstract

In this paper, we analyze weaknesses of the biometrics-based user authentication scheme proposed by An. The result of analysis An's authentication scheme by the login success scenario proposed in this paper, if the attacker successes to get user's random number, he/she can pass user authentication phase of the legal server. Also the biometrics guessing scenario proposed in this paper shows the legal user's the biometric information is revealed in lost smart card. Since An's authentication scheme submit user ID

•제1저자 : 박미옥 •교신저자 : 오기욱
•투고일 : 2014. 5. 31, 심사일 : 2014. 8. 2, 게재확정일 : 2014. 9. 27.
* 성결대학교 컴퓨터공학부(Division of Computer Science Engineering, Sungkyul University)
** 가천대학교 글로벌 교양대학(College of Global General Education, Gachon University)

and biometrics in plain text to the server, it is very vulnerable to inner attack and it is not provide the user anonymity to the server as well as the one to the third by user ID in plain text. Besides An's authentication scheme is contextual error too, due to this, it has weakness and so on that it did not check the validity of the smart card holder.

▸ Keywords : Biometric Information, Smart Card, Mutual Authentication

I. 서 론

최근에는 생체정보 중 지문인식 기술을 이용한 스마트폰들도 등장하였으며, 팬택의 베가 시크릿, 베가 시크릿 노트, 베가 LTE-A[1], 애플의 아이폰5S, 삼성전자의 갤럭시S5 등이 있다. 본 논문에서는 이러한 생체정보를 이용한 스마트카드기반의 원격 사용자 인증스킴들 중, 2012년에 An이 제안한 스마트카드기반의 원격 사용자 인증스킴[2]에 대해 살펴본다. 2010년에 Chang 등[3]은 생체정보의 특성을 이용한 스마트카드기반의 원격 사용자 인증스킴을 제안하였다. Chang 등의 인증스킴은 2010년에 Li-Hwang 등[4]이 제안한 인증스킴의 취약점을 개선한 것으로, 오프라인 추측 공격에 불안전하다는 점이 Li-Hwang 등의 취약점이다. Chang 등의 인증스킴은 이러한 취약점을 개선하여, 중간자 공격, 오프라인 생체인식 추측 공격 등에 안전하고, 이로 인하여 서버와 사용자간의 상호인증도 안전하게 보장한다고 주장하였다[3]. 그러나 2012년에 An의 인증스킴은 Chang 등의 인증스킴이 중간자 공격, 오프라인 생체인식 추측 공격에 취약하여, 상호인증을 보장하지 못함을 증명하였고[2], 이러한 취약점들을 개선한 생체정보를 이용한 스마트카드기반의 원격 사용자 인증스킴을 제안하였다. An의 인증스킴은 Chang 등의 인증스킴의 취약점 중의 하나인 스마트카드 분실시 사용자의 생체정보가 노출되는 문제를 개선하였다고 주장하였다[2]. Chang 등의 인증스킴은 스마트카드 분실시 사용자의 중요한 생체정보가 카드에 저장된 정보들을 이용하여 한 번의 XOR 연산만으로 그대로 노출되는 심각한 취약점이 존재하였다. An의 인증스킴이나 Chang 등의 인증스킴에서는 스마트카드 분실시 공격자가 카드의 소비전력을 모니터링[5-7]함으로써, 카드에 저장된 정보를 추측할 수 있다고 가정한다. An의 인증스킴은 스마트카드 분실시에도 중요정보의 비노출로 인해, 사용자 가장 공격, 서버 가장 공격 등에 안전하여 안전한 상호인증을 보장한다고 주장하였다[2].

그러나 본 논문에서 분석한 결과 An의 인증스킴은 정당한 사용자의 생체정보와 사용자 ID가 그대로 노출되어 내부 공격에 매우 취약하다. 또한 이 인증스킴은 전송 메시지들만을 이용하여 정당한 서버에서의 인증 단계를 공격자가 통과할 수 있고, 스마트카드 분실시 An의 주장과 달리 정당한 사용자의 생체정보가 노출가능하다는 것을 보인다. 특히 An의 인증스킴은 스마트카드 분실시 중요 정보의 비노출과 서버 비밀키의 비노출을 중요한 보안 특성으로 강조하였으나, 본 논문에서 제시하는 시나리오들에 의해 서버의 비밀키를 모르더라도 공격자에 의한 서버에서의 로그인 성공과 스마트카드의 정보노출의 취약점이 존재함을 보인다. 게다가 An의 인증스킴은 내용 서술시 전·후의 내용이 일치하지 않는 문제점이 존재하며, 이러한 문제점으로 인한 An의 인증스킴의 또 다른 취약점들도 살펴본다.

본 논문의 구성은 다음과 같다. 2장은 An의 인증스킴의 단계를 살펴보고, Chang 등의 인증스킴과 비교·분석한다. 3장에서는 추측 시나리오들을 제시하고, 4장에서 An의 인증스킴의 안전성 분석과 내용 문맥상의 오류문제를 분석한다. 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

2.1. 안의 사용자 인증스킴

등록 단계

[단계1] 등록을 원하는 사용자는 안전한 채널을 통해 자신의 ID와 생체정보 Q를 등록 센터에 제출한다.

[단계2] 등록 센터는 난수 R_1을 생성한 후, $f=Q\oplus R_1$과 $m=h(ID \| X_S)\oplus f$를 생성한다. 여기서 난수 R_1은 생체정보를 보호하기 위한 첫 번째 난수이다.

[단계3] 등록 센터는 스마트카드에 $\{ID,m,h(),R_1\}$을 저장하여, 안전채널을 통해 사용자에게 전달한다.

표 1. 표기법
Table 1. Notation

기호	의미
ID_i	IDentity of user
S	Remote system
X_s	Secret key of server
Q	Biometric information of the user
N_u, N_s	A nonce generated by user and server
$h(\cdot)$	Secure one-way hash function
$\|$	Concatenation operator
$\oplus$	XOR operation

로그인 단계

〔단계1〕 사용자는 자신의 스마트카드를 카드리더기에 입력하고, 자신의 생체정보 Q를 제공한다.

〔단계2〕 스마트카드는 $f'=Q\oplus R_1$을 계산하여, f'과 f가 동일한지 비교한다.

〔단계3〕 두 값이 동일하면, 스마트카드는 난수 N_u를 생성하고 $S_1=m\oplus f'\oplus N_u$와 $C_1=h(S_1 \| N_u)$을 계산한다.

〔단계4〕 사용자는 원격 서버에 로그인 요청을 위한 전송메시지 $m_1=\{ID, S_1, C_1\}$을 전송한다.

인증 단계

〔단계1〕 서버는 $N_u'=h(ID \| X_S)\oplus S_1$을 계산하여, C_1과 $h(S_1 \| N_u')$이 동일한지 체크한다.

〔단계2〕 두 값이 동일하면, 서버는 로그인 메시지를 받아들이고, 사용자를 정당한 사용자로 인증한다.

〔단계3〕 서버는 난수 N_s를 생성하여 $S_2=h(h(ID \| X_S) \| N_u')\oplus N_s$와 $C_2=h(S_2 \| N_s)$를 계산한다.

〔단계4〕 서버는 응답 메시지 $m_2=\{S_2, N_s\}$를 전송한다.

〔단계5〕 스마트카드는 $N_s'=h((m\oplus f') \| N_u)\oplus S_2$를 계산하여 C_2와 $h(S_2 \| N_s')$의 동일성 여부를 체크한다.

〔단계6〕 동일할 경우, 사용자는 서버로부터의 메시지를 받아들이고, 서버를 정당한 서버로 인증한다.

2.2 두 인증스킴의 비교·분석

본 절에서는 An과 Chang 등의 인증스킴을 간단히 비교분석하며, An의 인증스킴에 대한 분석은 본 논문에서 새롭게 분석한 결과이다.

ID 적절성 여부 체크

An의 인증스킴은 사용자 ID의 적절성 여부를 체크하지 않는다. 이러한 ID 체크과정 부재로 인해, 어떤 ID가 들어와도 서버에서 일차적으로 막아내지 못하고, 전송받은 ID를 가지고 인증 단계의 〔단계1〕을 수행한 후, 그 결과값의 비교여부에 따라 로그인 요청에 대한 허락/거절을 수행한다. 그러므로 An의 인증스킴은 부적절한 ID에 대한 계산수행의 오버로드가 존재한다. Chang 등의 인증스킴은 ID 체크여부가 존재하므로, An의 인증스킴이 Chang 등의 인증스킴보다 취약하다.

사용자 익명성

An의 인증스킴은 등록 및 로그인 단계에서 평문형태의 사용자 ID가 그대로 노출되어 제3자에 대한 사용자 익명성뿐만 아니라 서버에 대한 사용자 익명성도 보장하지 못한다. Chang 등의 인증스킴도 등록 및 로그인 단계에서 평문의 사용자 ID로 인하여, 제3자에 대한 사용자 익명성과 서버에 대한 사용자 익명성을 보장하지 못한다.

내부자 공격

An과 Chang 등의 인증스킴은 등록단계의 〔단계1〕과 〔단계2〕가 동일하고, 〔단계1〕에서 {ID, Q}를 등록 서버에 제출

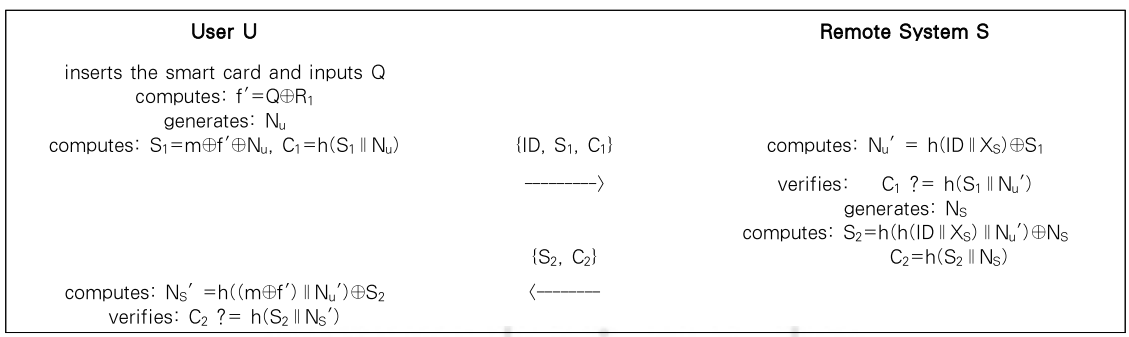

그림 1. An의 로그인 단계와 인증 단계
Fig. 1. An' Login Phase and Authentication Phase

한다. 서버내의 공격자에게 ID와 사용자의 가장 중요한 생체정보 Q가 그대로 노출되어 내부 공격자가 사용자 가장 공격에 성공할 수 있다.

제안 단계에 의한 불안전성

두 인증스킴은 등록/로그인/인증 단계만을 제시하고, 패스워드 변경 단계와 세션키 설정 단계의 미제안으로 사용자가 패스워드를 자유롭게 변경할 수 없고, 오픈 통신채널상의 데이터 암호화 방식 부재로 인해, 두 인증스킴 모두 안전한 데이터전송을 보장하지 못한다.

상호인증 방식

Chang 등의 인증스킴은 사용자가 서버에 로그인을 요청하면, 서버는 ID의 적법성을 체크한 후, 응답 메시지를 사용자에게 전송한다. 이 과정을 통해 사용자는 서버의 정당성 여부를 체크한다. 서버는 사용자로부터의 응답 메시지 $\{S_4\}$와 서버가 생성한 난수 N_S 등의 값의 비교여부를 통해 사용자의 정당성 여부를 검증한다. 그러므로 Chang 등의 인증스킴은 각 객체에서 상대 객체에 대한 명시적 상호인증 방식을 사용한다. An의 인증스킴은 서버에서 사용자인증 후, 응답 메시지 S->U:$\{S_2, C_2\}$에 의해 사용자측에서 서버를 인증한다. 사용자측에서의 서버 인증결과 후, 인증결과를 서버에 다시 응답하지 않는 형태이기 때문에 서버에 대한 인증은 묵시적 형태의 인증방식이라 할 수 있다. Chang 등의 인증스킴은 3번의 전송 메시지를 요하는 상호인증 방식으로, 마지막 단계에서 공격자는 서버에게 응답 메시지를 반드시 전송해야한다. 그러나 공격자가 서버로부터 온 응답 메시지에서 올바른 난수 획득을 하지 못할 경우, 공격자는 서버에 전송할 올바른 메시지를 작성할 수 없다. 그러므로 두 인증스킴의 상호인증 절차만을 고려할 경우, Chang 등의 인증스킴이 더 안전하다.

III. 추측 시나리오

본 장에서 제안하는 시나리오들을 통해 An의 인증스킴은 전송 메시지만을 이용하여 공격자가 로그인 단계를 통과할 수 있고, 스마트카드 분실시에는 사용자의 생체정보에 대한 취약점이 존재함을 보인다.

3.1 로그인 성공 시나리오

〔L1S1〕 $m_1=\{ID, S_1, C_1\}$ 중 S_1, C_1은 공개정보이고, $C_1=h(S_1 \| N_u')$로 구성되기 때문에 $C_1 ?= h(S_1 \| N_u')$ 식이 서로 일치할때까지의 난수 N_u'을 추측해낸다.

〔L1S2〕 $S_1=m\oplus f\oplus N_u=h(ID \| X_s)\oplus N_u$이기 때문에, 추측해낸 N_u'을 이용해 $S_1\oplus N_u' ?= Z$를 계산해낸다. 여기서, $Z=h(ID \| X_s)'$라고 가정한다.

〔L1S3〕 공개정보 S_2, 계산해 낸 Z, 그리고 추측해낸 난수 N_u' 값을 이용해, 서버가 생성한 난수 N_s'을 계산해낸다.

$$N_s' ?= h((m\oplus f) \| N_u')\oplus S_2=h(Z \| N_u')\oplus S_2$$

〔L1S4〕 공격자는 획득한 Z 값을 이용해, 자신이 생성한 난수 N_a를 $S_{a1}=h(ID \| X_s)'\oplus N_a$, $C_{a1}=h(S_{a1} \| N_a)$과 같이 연산하여 로그인 요청 메시지 $m_{a1}=\{ID, S_{a1}, C_{a1}\}$을 전송한다.

사용자의 로그인 요청 메시지는 $S_1=m\oplus f\oplus N_u$은 $h(ID \| X_s)'\oplus N_u$와 동일하기 때문에, 획득한 값 Z와 공격자 자신이 생성한 난수 N_a를 XOR 연산하여 서버에 전송한다. 서버는 사용자 인증을 위해 인증단계를 수행한다. 로그인 요청 메시지는 〔L1S2〕의 식에서와 같이 $S_1=m\oplus f\oplus N_u$은 $h(ID \| X_s)'\oplus N_u$와 동일하기 때문에, 획득한 값 Z와 공격자 자신이 생성한 난수 N_a를 XOR 연산하여 서버에 전송한다. 서버는 사용자 인증을 위해 인증단계를 수행한다. 서버는 자신의 비밀키 X_s와 공개정보 ID를 이용해 계산한 $h(ID \| X_s)$ 값과 공격자가 〔L1S2〕에서 획득한 $Z=h(ID \| X_s)'$ 값은 동일하기 때문에, 서버는 $N_a' ?= Z\oplus S_{a1}=h(ID \| X_s)\oplus S_{a1}$ 식으로부터 공격자가 생성한 난수 N_a' 값을 계산해낼 수 있다. 그런 다음, $C_{a1}' ?= h(S_{a1} \| N_a')$ 식의 값이 전송받은 C_{a1}과 동일한지 체크한다. 공격자는 추측공격에 의해 획득한 값 $Z=h(ID \| X_s)'$을 이용하여, S_{a1}과 C_{a1}을 계산하였기 때문에 사용자의 ID와 서버의 비밀키가 변경되지 않는 한 $C_{a1}' ?= h(S_{a1} \| N_a')$의 동일성 여부에 의한 사용자 인증과정을 성공적으로 통과할 수 있다.

3.2 서버의 비밀키 추측 시나리오

본 절에서는 공격자가 전송 메시지만을 이용하여 서버의 비밀키에 대한 추측가능성을 보인다.

서버의 비밀키 추측 시나리오

로그인 단계의 로그인 요청 메시지 U->S:$m_1=\{ID, S_1, C_1\}$을 이용한 서버의 비밀키 추측 시나리오는 다음과 같다.

〔S1S1〕 S_1, C_1은 공개정보이고, $C_1=h(S_1 \| N_u')$로 구성되기 때문에, $C_1?=h(S_1 \| N_u')$이 일치하는 난수 N_u'을 추측하여, 정당한 사용자의 난수 N_u'을 추측해낸다.

〔S1S2〕 공개정보 ID와 추측해낸 난수 N_u'을 이용하여, $S_1\oplus N_u'?=h(ID \| X_s')$이 일치하는 서버의 비밀키 X_s'을 추측해낸다.

서버의 비밀키 추측 시나리오II

두 번째 추측 시나리오는 인증 단계의 전송 메시지 S->U:m_2={S_2, C_2}를 이용하여, 서버의 비밀키를 추측한다.

〔S2S1〕 공격자는 공개정보 S_2, C_2를 이용하여 C_2?=h(S_2‖N_s') 식이 서로 일치하는 서버의 난수 N_s'을 추측해낸다.

〔S2S2〕 사용자의 ID와 〔S1S1〕에서 추측해 낸 사용자의 난수 N_u'를 이용하여, S_2⊕N_s' ?=h(h(ID‖X_s')‖N_u') 식이 일치할 때까지 서버의 비밀키를 추측 공격한다.

3.3 생체정보 추측 시나리오

본 절에서는 공격자가 사용자의 스마트카드를 획득할 경우 정당한 사용자의 생체정보 Q에 대한 추측가능성을 제시한다.

생체정보 추측 시나리오I

이 추측 시나리오는 스마트카드에 f를 저장하지 않았다고 가정한 경우이며, 이러한 가정은 An의 인증스킴의 내용문맥상의 오류에 의한 것이다.

〔Q1S1〕 스마트카드 분실시 m⊕R_1=h(ID‖X_s)⊕f⊕R_1=h(ID‖X_s)⊕Q이기 때문에 생체정보를 획득하기 위해 Z=h(ID‖X_s)′ 값을 알아야한다. 이를 위해 〔L1S1〕과 〔L1S2〕를 수행한다.

〔Q1S2〕 공격자는 획득한 Z 값을 이용해 Q′?=m⊕R_1⊕h(ID‖X_s)′=m⊕R_1⊕Z과 같이 XOR 연산한다.

획득한 Z=h(ID‖X_s)′ 값이 올바른 값일 경우, 사용자의 Q는 추측공격 할 필요 없이 XOR 연산만으로 알아낼 수 있다. 만약 획득한 Q′이 올바른 값일 경우 f=Q⊕R_1이기 때문에, Q′⊕R_1을 연산하여 f′ 값을 획득할 수 있다.

생체정보 추측 시나리오II

본 절에서는 앞에서 제시한 시나리오에 의해 획득한 서버의 비밀키 X_s'을 이용하여 사용자의 생체정보를 획득하는 시나리오이다. 생체정보 추측 시나리오I에서는 생체정보 Q′를 추측해내기 위해서 h(ID‖X_s)′ 값을 이용하였고, 여기서는 앞 절에서 제시한 서버의 비밀키 추측 시나리오I, II를 통해 획득해낸 서버의 비밀키 X_s'을 이용하여 정당한 사용자의 생체정보를 추측해낸다. 생체정보 추측 시나리오II는 다음과 같다.

〔Q2S1〕 공격자는 스마트카드에 저장된 정보 m과 R_1, 그리고 서버의 비밀키 추측시나리오에 의해 획득해낸 서버의 비밀키 X_s'을 이용하여 Q′?=m⊕R_1⊕h(ID‖X_s')을 계산한다.

m⊕R_1=h(ID‖X_s')⊕Q′이기 때문에, 사용자의 생체정보 Q′을 획득하기 위해서는 이들 값을 위의 식처럼 XOR 연산, 연접 연산, 그리고 해쉬연산만 수행하면 된다. 만약, m⊕R_1 ?= h(ID‖X_s')⊕Q′의 양쪽 식이 동일하게 된다면 획득해낸 서버의 비밀키 X_s'이 올바른 값이라는 것을 확인할 수 있다. 또한 m′=h(ID‖X_s')⊕Q′⊕R_1의 연산을 통해 원래의 m과 비교하여 올바른 값인지 확인여부도 가능하다. 두 값이 동일하면 추측한 생체정보 Q′이 올바른 생체정보라는 의미이기 때문에, f 값을 구하기 위해 Q′⊕R_1을 계산한다.

IV. 안전성 분석

본 장에서는 An의 인증스킴에 대한 안전성을 분석한다. 또한 An의 인증스킴은 내용 서술시 문맥상의 오류가 발견되었으며, 이로 인해 발생하는 문제점도 함께 분석한다.

4.1 내용 문맥상의 오류문제 분석

An의 인증스킴의 등록 단계와 그의 논문의 그림 4는 스마트카드에 {ID, m, h(), R_1}만을 저장한다. 로그인/인증 단계나 안전성 분석절과 같은 전체 내용에서도 스마트카드에 다른 정보를 추가로 저장하는 내용은 언급되어 있지 않다. 이러한 내용에 근거하여 f를 스마트카드에 저장하지 않기 때문에, 카드에 저장된 정보들을 이용해 단 한번의 XOR 연산만으로 생체정보 Q 값을 획득할 수 없다. 그러나 로그인 단계-〔단계 2〕에서는 "스마트카드는 f′=Q⊕R_1을 계산하여, f′과 f가 동일한지 비교한다."는 내용이 있다. 새로 입력한 생체정보 Q와 카드에 저장된 값 R_1을 f′=Q⊕R_1연산처리 후, f 값과의 비교여부를 확인하려면, f 값이 카드에 저장되어 있거나, 다른 연산을 통한 결과비교를 통해 입력한 생체정보의 정당성 체크가 이루어져야 한다. 그러나 다른 연산을 통한 결과비교도 전혀 언급되어 있지 않다. An의 인증스킴의 "5.1.4 Biometrics guessing attack"절에서 An은 공격자가 Q=f⊕R_1을 계산하여 사용자의 생체정보 Q에 대한 추측공격을 시도하지만, 공격자는 비밀값 f를 모르기 때문에 Q를 추측할 수 없다고 주장하였다. 이러한 전체적인 내용 서술로 보아, An의 인증스킴에서는 f를 스마트카드에 저장하지 않는 것을 가정하는 것으로 보인다.

본 논문에서는 이러한 내용 서술상의 오류를 몇 가지 가정을 제시함으로써, An의 사용자 인증스킴의 취약점을 분석한다.

〔가정1〕 만약 로그인 단계의 내용서술이 오류이고, 등록 단계가 올바른 내용서술이었다고 가정할 경우.

로그인 단계-[단계2]의 f′과 f의 동일여부 비교부분이 오류라고 가정하면, 두 값의 동일성 여부 비교과정이 부재하다. 정당한 사용자나 공격자가 생체정보를 입력한 후, 정당한 사용자 여부 체크부분이 부재하기 때문에 어떤 생체정보가 입력되어도 스마트카드는 정당한 사용자 여부를 체크하지 않고, 새롭게 입력된 생체정보 Q와 카드에 저장된 R_1을 이용해 [단계2]의 $f' = Q \oplus R_1$ 연산 후, [단계3]을 진행한다. [단계3]과 [단계4]는 새로 입력한 생체정보를 가지고 계산만을 수행하기 때문에, [단계2]에서 사용자의 생체정보 여부에 의한 정당성 체크가 부재할 경우, 그 다음 단계들을 계속 진행하는 문제점이 발생한다. 공격자가 스마트카드를 획득할 경우, 이 인증스킴에서는 모든 공격자가 추측공격을 할 필요 없이, 공격자 자신의 생체정보를 입력하여도 정당한 사용자로 인식되어 다음 과정을 통과하게 된다. 다른 연산처리 과정을 통해서라도, 새롭게 입력한 생체정보에 대한 사용자 정당성 체크여부가 있어야하는데, 이러한 다른 과정에 대한 내용서술도 전혀 없다.

[가정2] 만약, 로그인 단계가 맞고 등록 단계가 올바른 내용서술이 아니라고 가정할 경우.

이 가정에서는 등록 단계에서 스마트카드에 f가 저장되어 사용자에게 전달되어야 한다는 것이기 때문에, An 논문의 biometrics guessing attack절에서 공격자가 f를 알 수 없다고 주장한 것은 모순이 된다. 이 가정하에서는 스마트카드 분실시 카드에 f가 저장되어 있으므로 공격자가 f를 알 수 있고, 카드에 저장된 또 다른 정보 R_1과 $f \oplus R_1$ 연산을 수행하면 단 한번만의 XOR 연산만으로 사용자 생체정보 Q를 아주 쉽게 획득할 수 있다. 이것은 카드 분실시 Chang 등의 인증스킴과 동일한 수준에 의해 An의 인증스킴의 생체정보가 노출되는 것이므로, An의 인증스킴은 스마트카드 분실시 Biometrics guessing attack에 매우 취약하다고 할 수 있다. An의 인증스킴이 모든 항목의 안전성 분석에서 안전하다 한다할지라도, 내용문맥상의 내용 불일치로 인하여 An의 인증스킴은 알고리즘 자체가 불안전하다.

4.2 안전성 분석

본 절에서는 제안 추측 시나리오들과 2장의 분석결과에 근거하여, An의 인증스킴에 대한 안전성을 분석한다.

생체정보 추측공격(Biometrics guessing attack)

An의 인증스킴에서는 스마트카드 분실시 생체정보 추측공격에 안전하다고 주장하였으나, 제안 생체정보 추측 시나리오는 카드분실시 사용자의 생체정보 획득가능성을 보였다. 생체정보 추측 시나리오I는 [Q1S1]에서 Z값을 획득하기 위해 [L1S1]에서 난수 획득에 걸리는 시간 Tn, [L1S2]에서 1번의 XOR 연산시간 1Tx, [Q1S2]에서 두 번의 XOR 연산을 수행하여, 총 Tn+3Tx 연산시간이 필요하다. 시나리오I는 카드에 f를 저장하지 않은 경우의 연산시간이고, f를 저장했다고 가정할 경우 단 한번의 XOR 연산만 필요하므로, 1Tx로 사용자 생체정보를 획득할 수 있다. Chang 등의 인증스킴도 한번의 XOR 연산만으로 생체정보 획득이 가능하므로, 두 사용자 인증스킴은 생체정보 추측공격에 매우 취약하다.

표 2. 안전성의 재분석 결과
Table 2. The Reanalysis Result of Security Properties

Security components	Chang 등의 인증 스킴	안이 분석한 Chang 등의 인증 스킴	안의 인증 스킴	재분석 결과
Mutual authentication	supported	not supported	supported	impossible
Biometrics guessing attack	impossible	impossible	impossible	possible
Server impersonation attack	impossible	impossible	impossible	possible
User impersonation attack	impossible	impossible	impossible	possible
Man-in-the-middle attack	-	impossible	impossible	possible
Replay attack	impossible	-	-	possible
User anonymity to the third	-	-	-	not supported
User anonymity to server	-	-	-	not supported
Insider attack	-	-	-	possible
Freely change password	-	-	-	not supported
Session key agreement	-	-	-	not supported

서버 가장 공격(Server masquerading attack)

An의 인증스킴은 스마트카드 분실시 획득한 정보 m⊕f=h(ID‖X_S)=Z의 1Tx 연산만으로 Z를 계산해 낼 수 있다는 것에 의해 Chang 등의 인증스킴이 중간자 공격을 이용하여 서버와 사용자를 가장할 수 있다고 하였다. An의 인증스킴도 내용상의 오류로 인하여, 카드에 f가 저장되었을 경우 1Tx 연산으로 Z를 획득가능하므로, 이 경우에는 두 인증스킴 모두 1Tx 연산만으로 서버 가장 공격에 취약하다. 카드에 f가 저장되어 있을 않을 경우, An의 인증스킴은 h(ID‖X_S) 값을 획득하기 위해 Tn+1Tx 연산시간이 필요하다. 전송 메시지만을 이용하여 Z를 획득하는 로그인 성공 시나리오는 Tn+1Tx, 전송 메시지만을 이용하여 서버의 비밀키를 획득하는 서버의 비밀키 추측 시나리오는 〔S1S1〕에서 사용자 난수를 추측해내는데 걸리는 시간 Tn, 〔S1S2〕에서 서버의 비밀키를 추측하기 위한 Ts의 연산시간이 필요하다. Chang 등의 인증스킴은 전송 메시지만을 사용하여 Z를 추측 공격할 경우, 전송 메시지를 추측하기 위한 정보들이 모두 비공개 정보이므로 이들 전송 메시지로부터 Z를 구하는 것이 어렵다. 그러므로 카드 분실시에는 Chang 등의 인증스킴이 An의 인증스킴보다 취약하지만, 전송 메시지만을 이용하여 서버가장 공격에 필요한 정보 획득에는 An의 인증스킴이 더 취약하다.

사용자 가장 공격(User impersonation attack)

An은 Chang 등의 인증스킴 분석시 스마트카드 분실의 가정 하에 카드로부터 획득한 정보를 이용하여 사용자 가장 공격이 가능하다고 분석하였고, 자신의 인증스킴은 서버의 비밀키와 사용자의 생체정보를 알 수 없기 때문에, 공격자가 위조된 S_1, C_1을 계산 불가하여 안전하다고 주장하였다. 그러나 로그인 성공 시나리오에 의해 공격자는 스마트카드를 획득하지 않고도, 서버에서의 사용자 인증단계를 통과할 수 있음을 보였다. 또한, 제안한 생체정보 추측 시나리오에서는 공격자가 스마트카드 정보를 획득하여 생체정보를 알아냄으로써 An의 인증스킴이 사용자 가장 공격에 취약함을 보였다. 그러므로 본 논문에서 두 사용자 인증스킴을 재분석한 결과, An의 인증스킴의 공격자는 전송 메시지만을 이용하여 사용자 가장 공격에 성공할 수 있으나, Chang 등의 인증스킴은 전송 메시지로부터 정보획득이 어렵다. 그러므로 카드를 분실하지 않는 한, An의 인증스킴이 사용자 가장 공격에 더 취약하다.

중간자 공격(Man-in-the-middle attack)

An의 인증스킴은 공격자가 스마트카드의 비밀 정보를 획득한다 할지라도, 공격자가 서버의 비밀키 X_S나 사용자의 생체정보 Q를 모르기 때문에 위조된 메시지를 생성불가하여 중간자 공격에 안전하다고 주장하였다. 그리고 An은 Chang 등의 인증스킴이 중간자 공격에 취약하다고 분석하였고, 이러한 분석결과는 공격자가 스마트카드의 정보를 획득할 수 있다는 가정하에 분석된 것이다. 그러나 로그인 성공 시나리오와 서버의 비밀키 추측 시나리오에 의해 An의 인증스킴은 공격자가 스마트카드 획득없이 전송 메시지들만을 이용하여 사용자와 서버의 난수, 그리고 서버의 비밀키 등의 정보를 획득해 낼 수 있다. 스마트카드 분실시에는 제안한 생체정보 추측 시나리오에 의해 사용자의 생체정보까지 노출가능성이 있다. 그러므로 An의 인증스킴은 중간자 공격에 대한 취약성이 존재한다.

재전송 공격(Replay attack)

An의 인증스킴은 서버의 비밀키 추측 시나리오에 의해 서버 비밀키 추측공격에 실패할지라도, 로그인 성공 시나리오에 의해 사용자 난수와 인증단계의 h(ID‖X_s)을 획득해낼 수 있다. 로그인 성공 시나리오에서 보듯이, C_1과 S_1이 공개정보이므로 C_1?=h(S_1‖N_u′)의 두 항이 동일한 값을 가질때까지의 난수를 추측해낼 수 있다. 난수 획득이 성공하면, 다음 단계의 〔L1S2〕는 Z를 구하기 위해 한번의 XOR 연산만 수행하면 되고, 〔L1S3〕는 서버의 난수획득을 위해 한 번의 해쉬함수, 한 번의 연접, 한 번의 XOR 연산만 수행하면 된다. 그러므로 An의 인증스킴은 로그인 성공 시나리오에 의해 재전송 공격에 취약하고, Chang 등의 인증스킴은 스마트카드 미분실시 재전송공격에 안전하다.

상호인증(Mutual authentication)

An의 인증스킴에서는 Chang 등의 인증스킴 상호인증 분석시, 스마트카드 분실시 생체정보의 노출 때문에 Chang 등의 인증스킴이 불안전하다고 주장하였다. An의 인증스킴도 제안 추측 시나리오에 의해 스마트카드 분실시 사용자의 생체정보 노출가능성이 있다. 그러므로 An의 인증스킴에서는 안전한 상호인증을 보장한다고 주장하였지만, 분석결과 상호인증을 안전하게 보장하지 못한다. 공격자가 사용자의 스마트카드를 획득하지 않고도, 전송 메시지들만을 이용하여 서버에서의 인증 단계를 통과할 수 있는 점은 심각한 취약점이라 할 수 있다. An의 인증스킴을 분석한 결과는 표 2와 같다. 기호 -는 각 인증스킴이 각 항목에 대해 미제안/미분석을, supported와 not supported는 기능의 제공/미제공을 의미한다.

V. 결론

본 논문에서 An의 인증스킴을 분석한결과 이 인증스킴은

로그인 성공 시나리오에 의해 전송 메시지만을 이용하여 사용자 생성 난수 획득에 성공할 경우, 인증에 필요한 정보를 획득하여 공격자에 의한 인증단계 통과가능성을 보였다. 공격자가 스마트카드 획득시, 생체정보 추측 시나리오에 의해 사용자의 생체정보에 대한 획득가능성을 보였다. 제안추측 시나리오의 모든 공격이 실패한다 하더라도, An의 인증스킴은 제3자에 대한 사용자 익명성과 서버에 대한 사용자 익명성을 보장하지 못하며, 사용자의 생체정보를 서버에 그대로 제출하여 내부자 공격에 매우 취약하다. 또한 An의 인증스킴은 내용 문맥상의 오류가 존재할 뿐만 아니라, 스마트카드 소유자의 정당성도 체크하지 못하므로 안전한 상호인증에 적합한 인증스킴이라고 할 수 없다.

참고문헌

〔1〕 http://news.inews24.com/php/news_view.php?g_serial=795478&g_menu=020800

〔2〕 Y.H.An, "Security Analysis and Improvements of a Biometrics-based User Authentication Scheme Using Smart Cards," Journal of Korea Society of Computer and Information, Vol.17, No.2, pp. 159-166, Feburary 2012.

〔3〕 C.C. Chang, S.C. Chang, and Y.W. Lai, "An Improved Biometrics-based User Authentication Scheme without Concurrency System," International Journal of Intelligent Information Processing, Vol.1, No.1, pp.41-49, September 2010.

〔4〕 C.T. Li, 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, January 2010.

〔5〕 E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," Lecture Notes in Computer Science, Vol.3156, pp.135-152, August 2004.

〔6〕 T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M.T.M. Shalmani, "On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme," CRYPTO 2008, pp.203-220, August 2008.

〔7〕 H. J. Mahanta and A.K. Khan, "Side Channel Attacks and its Impact on Symmetric Algorithms through Power Analysis," Vol.3. No.1 pp.14-18, March 2014.

저 자 소 개

박 미 옥

1993: 숭실대학교 컴퓨터학과 공학석사.
2004: 숭실대학교 컴퓨터공학과 공학박사.
현 재: 성결대학교 컴퓨터공학부 조교수
관심분야: 모바일 보안, 암호 프로토콜
Email : mopark777@hanmail.net

오 기 욱

1991: 가천대학교 전자계산학과 공학사
1993: 숭실대학교 컴퓨터학과 공학석사
2007: 숭실대학교 컴퓨터학과 공학박사.
현 재: 가천대학교 글로벌교양대학
관심분야:RFID, USN, 네트워크 보안, 암호 프로토콜
Email : ohgiug@daum.net