情報保護學會論文誌
第19卷 第6號, 2009. 12

Chang-Lee-Chiu 익명 인증 기법의 취약성 분석

윤 택 영,[1†] 박 영 호[2‡]
[1]고려대학교, [2]세종사이버대학교

Security analysis of Chang-Lee-Chiu's anonymous authentication scheme

Taek-Young Youn,[1†] Young-Ho Park[2‡]
[1]Korea University, [2]Sejong Cyber University

요 약

최근, 익명 인증 서비스를 제공하는 기법이 Chang 등에 의해 제안되었다. 본 논문에서는 Chang-Lee-Chiu 익명 인증 기법이 안전하지 않음을 보인다. 취약성을 보이기 위해 사용자의 신원 정보를 쉽게 알아낼 수 있는 공격 방법을 설명한다.

ABSTRACT

Recently, an anonymous authentication scheme has been proposed by Chang, Lee, and Chiu. In this paper, we show the insecurity of the scheme. To prove the insecurity of the scheme, we describe some attacks that can be used to recover an user's identity.

Keywords: Security, Anonymity, Authentication

I. 서 론

근래에 이르러 모바일 장비를 기반으로 구현되는 통신 환경에서의 안전성에 대한 논의가 활발하게 이루어지고 있다. 기존 유선 환경에서의 통신과 달리 부각된 안전성 요건의 하나는 모바일 사용자의 프라이버시를 보호하는 것이다. 이에 따라 사용자의 신원 정보에 대한 익명성을 제공함으로써 각 사용자의 프라이버시를 보호하기 위한 기술의 하나인 익명 인증 기법에 대한 연구가 활발히 이루어지고 있다[1-5]. 최근, Chang 등은 Lee 등에 의해 제안된 익명 인증 [3]이 제공되는 로밍 기법이 모바일 사용자에게 익명성을 제공할 수 없음을 보이고 안전성이 개선된 익명 인증 기법을 제안하였다[2].

본 논문에서는 Chang 등에 의해 제안된 익명 인증 기법의 안전성을 분석하여 해당 기법이 사용자의 익명성을 제공하지 못함을 밝힌다. Chang 등의 기법이 익명성을 제공하지 못함을 보이기 위해 모바일 사용자의 신원 정보를 알아낼 수 있는 공격 방법을 기술한다. 제안하는 공격 방법은 정상적인 사용자의 통신 정보를 획득하면 쉽게 시도할 수 있는 공격이기 때문에 Chang 등의 기법에 대한 현실적이고 위협적인 공격이다.

접수일(2009년 6월 29일), 게재확정일(2009년 10월 29일)
† 주저자, taekyoung@korea.ac.kr
‡ 교신저자, youngho@sjcu.ac.kr

II. Chang-Lee-Chiu 익명 인증 기법

본 장에서는 Chang-Lee-Chiu 익명 인증 기법의 구성에 대해 간략히 살펴본다. 해당 기법에서는 외부 에이전트 FA와 내부 에이전트 HA가 키 K_{FH}를 공유하고 있는 것으로 가정한다. HA는 비밀키 x를 보유하고 있고 $h(\cdot)$는 충돌저항 해쉬함수이다.

2.1 등록단계

등록단계에서는 새로운 모바일 사용자 MN이 자신

의 신원 정보 id_{MN}과 패스워드 pw_{MN}을 내부 에이전트 HA에게 제출한다. HA는 $R=h(id_{MN}\|x)\oplus pw_{MN}$와 $h(x)$를 계산한다. HA는 $id_{MN}, id_{HA}, R, h(x), h(\bullet)$를 담고 있는 스마트카드를 생성하여 안전한 채널을 통해 MN에게 전달한다.

2.2 인증 및 키 교환 단계

MN이 외부 네트워크에서 에이전트 FA를 통해 내부 에이전트 HA의 도움을 받아 인증을 받는 경우를 고려한다.

단계 1. (MN ⇒ FA): MN가 스마트카드를 통신 장비에 삽입하고 패스워드 pw_{MN}를 입력하면 카드는 난수 n_{MN}에 대해 $C=R\oplus pw_{MN}\oplus n_{MN}$을 계산하고 C와 n_{MN}을 반환한다. Req_{Login}는 MN와 FA사이의 새로운 세션을 알리는 메시지로 정의한다. MN는 로그인을 위한 메시지 $m_1=(Req_{Login}, n_{MN}, id_{HA})$를 FA에게 전송한다.

단계 2. (FA ⇒ HA): FA는 난수 n_{FA}를 생성하고 $m_2=(Req_{Auth}, n_{FA}, id_{FA})$를 HA에게 전송한다. Req_{Auth}는 HA에게 로밍 사용자 MN를 인증해달라는 요청 메시지이다.

단계 3. (HA ⇒ FA): HA는 id_{FA}가 적법한 외부 에이전트인지 확인하고, 적법한 서비스 대상이면 난수 n_{HA}를 생성하고 $m_3=(n_{HA}, id_{HA})$를 FA에게 전송한다.

단계 4. (FA ⇒ MN): FA는 $m_4=(n_{HA}, n_{FA}, id_{FA})$를 MN에게 전송한다.

단계 5. (MN ⇒ FA): MN은 $sid=id_{MN}\oplus h(h(x)\|n_{HA})$, $V_1=h(n_{HA}\|C)$, $sk=h(h(x)\|id_{MN}\|id_{FA}\|n_{MN}\|n_{FA})$, $V_2=sk\oplus h(n_{HA}\|id_{MN})$, 그리고 $S_1=h(n_{FA}\|sid\|V_1\|V_2\|n_{MN})$를 계산하고 $m_5=(sid, V_1, V_2, n_{MN}, S_1, id_{HA})$를 FA에게 전송한다.

단계 6. (FA ⇒ HA): FA는 $S_1'=h(n_{FA}\|sid\|V_1\|V_2\|n_{MN})$를 계산하고 $S_1'=S_1$를 확인한다. 해당 조건이 만족하면 FA는 $S_2=h(K_{FH}\|n_{HA}\|sid\|V_1\|V_2\|n_{MN})$를 계산하고 $m_6=(sid, V_1, V_2, n_{MN}, S_2, id_{FA})$를 HA 에게 전송한다.

단계 7. (HA ⇒ FA): HA는 id_{FA}가 적법한 외부 에이전트인지 확인하고, 적법한 서비스 대상이면 S_2와 $S_2'=h(K_{FH}\|n_{HA}\|sid\|V_1\|V_2\|n_{MN})$를 비교한다. $S_2\neq S_2'$이면 HA는 프로토콜을 종료한다. $S_2=S_2'$이면 HA는 $h(h(x)\|n_{HA})$와 $id_{MN}=sid\oplus h(h(x)\|n_{HA})$를 계산한다. HA는 id_{MN}를 검증하고, 올바른 신원 정보가 아니면 프로토콜을 종료한다. 올바른 신원 정보인 경우, HA는 $V_1'=h(n_{HA}\|n_{MN}\oplus h(id_{MN}\|x))$를 계산한다. $V_1'\neq V_1$이면 HA는 프로토콜을 종료한다. $V_1'=V_1$이면 HA는 $sk=V_2\oplus h(n_{HA}\|id_{MN})$, $K_1=sk\oplus h(K_{FH}\|n_{FA})$, $V_3=h(id_{FA}\|h(x)\|n_{MN})$, $S_3=h(K_{FH}\|n_{FA}\|K_1\|V_3)$를 계산하고 $m_7=(K_1, V_3, S_3)$를 FA에게 전송한다.

단계 8. (FA ⇒ MN): FA는 $S_3'=h(K_{FH}\|n_{FA}\|K_1\|V_3)$를 계산하고 $S_3'=S_3$를 확인한다. 해당 조건이 만족하면 FA는 $sk=K_1\oplus h(K_{FH}\|n_{FA})$와 $K_2=sk\oplus h(sk\|n_{MN})$을 계산하고 $m_8=(V_3, K_2)$를 MN에게 전송한다.

단계 9. (MN ⇒ Finish): MN은 $h(id_{FA}\|h(x)\|n_{MN})=V_3$를 확인하고, 조건이 만족하는 경우 $sk'=K_2\oplus h(sk\|n_{MN})$를 계산한다. $sk'=sk$이 만족하면 MN은 sk를 FA와의 통신을 위한 세션키로 사용한다.

HA와 FA는 두 에이전트간의 안전한 통신을 위해 비밀키 K_{FH}를 공유한다. K_{FH}는 통신 데이터를 암호화하기 위한 목적으로는 사용되지 않고 키를 사용한 해쉬를 생성함으로써 통신 데이터의 신뢰성을 제공하기 위한 목적으로 사용된다. 즉, 두 주체는 비밀키를 공유하고 있으므로 데이터의 암호화를 통한 비밀통신을 수행할 수 있다. 그러나 Chang-Lee-Chiu의 기법에서는 K_{FH}를 통신 데이터의 인증을 위한 목적으로 사용하고 통신은 공개채널을 통해 이루어진다.

III. Chang-Lee-Chiu 익명 인증 기법의 취약성

본 장에서는 Chang-Lee-Chiu 익명 인증 기법이 안전하지 않음을 보인다. Chang-Lee-Chiu의 취약성을 보이기 위해 모바일 사용자의 신원 정보를 획득할 수 있는 공격 방법을 제시한다.

[4]에서 명시된 바와 같이 사용자의 신원 정보는 길지 않은 정보를 특정 포맷으로 작성한다. 따라서 공격자가 특정 신원 정보를 추측하고 이를 검증할 수 있는 정보를 획득하는 경우 공격자는 모든 가능한 신원 정보에 대해 정당성을 검사하기 위한 전수조사를 수행함으로써 통신을 하고 있는 모바일 사용자의 올바른

신원정보를 찾아낼 수 있다. 이와 같은 관점에서 Chang-Lee-Chiu 익명 인증 기법의 안전성을 살펴보도록 하자.

Chang-Lee-Chiu 익명 인증 기법은 모바일 사용자의 통신 내용을 도청함으로써 공격을 시도하는 공격자에 대한 안전성을 제공하지 못한다. 모바일 통신 환경에서는 통신 메시지를 도청하는 것이 유선 통신환경에 비해 매우 쉽기 때문에 모바일 통신을 위한 프로토콜의 경우 도청에 매우 취약하다. 즉, 도청만 수행하여 성공할 수 있는 공격이 있으면 안전성 측면에 매우 큰 위협이 된다. Chang-Lee-Chiu 익명 인증 기법에 대해 도청을 수행하는 공격자는 도청을 통해 V_2와 K_2를 획득할 수 있고, 수집된 정보를 통해 사용자의 신원 정보를 찾을 수 있다. 우선, $V_2 = sk \oplus h(n_{HA} \| id_{MN})$와 $K_2 = sk \oplus h(sk \| n_{MN})$임을 기억하자. 공격자는 다음의 과정을 반복하여 수행함으로써 모바일 사용자의 신원 정보를 알 수 있다. 우선, 공격자는 신원 정보의 후보 id를 추측하고 $sk' = V_2 \oplus h(n_{HA} \| id)$를 계산하여 K_2와 $K_2' = sk' \oplus h(sk' \| n_{MN})$를 비교한다. $K_2 = K_2'$이면 추측한 신원 정보의 후보 id는 공격 대상이 되는 모바일 사용자의 신원 정보와 동일함을 알 수 있다. $K_2 \neq K_2'$인 경우 추측한 신원 정보 id는 올바른 값이 아님을 알 수 있고, 공격자는 위 과정을 다른 신원 정보의 후보 값으로 다시 수행한다. 위 과정을 올바른 값을 찾을 때까지 반복함으로써 공격자는 도청을 통해 얻은 V_2와 K_2로 올바른 신원 정보를 찾을 수 있다. 본 공격의 효율성은 id의 길이 또는 개수에 의존한다. 즉, id의 길이가 전수조사의 공격범위 안에 속하는 경우 본 논문에서 제안하는 공격이 효율적으로 적용될 수 있다. [4]에서 명시된 바와 같이 사용자의 신원 정보는 일반적으로 길지 않은 정보를 특정 포맷으로 작성되어 있어 본 공격의 효율적인 적용이 가능한 범주에 포함된다. 길이가 긴 id가 사용된다고 하더라도 알고 있는 id들에 대한 공격은 여전히 가능하다.

공격자가 올바른 신원 정보 id_{MN}를 획득한 경우를 고려해보자. 이 경우, 공격자는 모바일 사용자 MN이 생성했던 세션키도 다음의 계산을 통해 복원할 수 있다: $sk = V_2 \oplus h(n_{HA} \| id_{MN})$. 결과적으로, 사용자의 신원이 밝혀지는 것은 단지 익명성의 문제로 국한되지 않는다. 모바일 사용자의 신원 정보가 공개되면 해당 사용자와 외부 에이전트간에 생성된 세션키로 통신된 모든 데이터에 대한 안전성이 제공되지 않는다. 즉, 본 논문에서 제안하는 공격 방법은 Chang-Lee-Chiu 익명 인증 기법이 익명성만 제공하지 못하는 것이 아니라 근본적으로 안전하지 않음을 보여준다.

Ⅳ. 결 론

본 논문에서는 최근 Chang 등에 의해 제안된 익명 인증 기법의 안전성을 분석하였다. 가장 소극적인 형태의 공격인 도청을 수행하는 공격자가 사용자의 신원 정보를 획득할 수 있음을 보임으로써 Chang-Lee-Chiu 익명 인증 기법이 익명성을 보장하지 않음을 보이고, 공격자가 사용자의 신원 정보를 획득함으로써 통신에 사용된 세션키를 획득할 수 있음을 보임으로써 프로토콜의 기본적인 안전성이 제공되지 않음을 보였다.

참 고 문 헌

[1] L. Buttyan, C. Gbaguidi, S. Staamann, and U. Wilhelm, “Extensions to an authentication technique proposed for the global mobility network,” IEEE Transactions on Communications, vol. 48, no. 3, pp. 373-376, Mar. 2000.

[2] C.C. Chang, C.Y. Lee, and Y.C. Chiu, “Enhanced authentication scheme with anonymity for roaming service in global mobility networks,” Computer Communications, vol. 32, issue. 4, pp. 611-618, Mar. 2009.

[3] C.C. Lee, M.S. Hwang, and I.E. Liao, “Security enhancement on a new authentication scheme with anonymity for wireless environments,” IEEE Trans. Industrial Electron, vol. 53, no. 5, pp. 1683-1687, Oct. 2006.

[4] C.C. Wu, W.B. Lee, and W.J. Tsaur, “A Secure Authentication Scheme with Anonymity for Wireless Communications,” IEEE Communications Letters, vol. 12, no. 10, pp. 722-723, Oct. 2008.

[5] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments,” IEEE Trans. Consumer Electron, vol. 50, no. 1, pp. 230-234, Feb. 2004.

<著者紹介>

윤 택 영 (Taek-Young Youn) 학생회원
2003년 2월: 고려대학교 수학과 이학학사
2005년 2월: 고려대학교 정보경영공학대학원 공학석사
2009년 8월: 고려대학교 정보경영공학대학원 공학박사
2009년 9월 ~ 현재: 고려대학교 정보경영공학대학원 연구교수
<관심분야> 암호 이론, 정보보호 이론, 암호 프로토콜, 부채널 공격

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 3월 ~ 현재: 세종 사이버 대학교 부교수
<관심분야> 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격