한국컴퓨터정보학회 하계학술대회 논문집 제18권 제2호 (2010. 7)

효율적인 스마트카드 사용자 인증 프로토콜

용승림°, 조태남*
°인하공업전문대학 컴퓨터시스템과
*우석대학교 정보보안학과
e-mail: slyong@inhatc.ac.kr, tncho@ws.ac.kr

An Efficient Smartcard Authentication Protocol

Seunglim Yong°, TaeNam Cho*
°Dept. of Computer System and Engineering, Inha Technical college
*Dept. of Information Security, Woosuk University

● 요 약 ●

개인 프라이버시 보호에 대한 관심이 증가하면서 원격 시스템에서 사용자 익명성을 제공하는 스마트카드 기반 인증 프로토콜에 대한 연구가 활발하게 진행되고 있다. 최근의 인증 프로토콜은 사용자 익명성을 제공하는 기법과 더불어 악의적인 사용자를 추적할 수 있는 연구로 발전되고 있다. Kim은 사용자의 익명성을 보장하면서 악의적인 사용자를 감지하여 추적 가능한 인증 프로토콜을 제안하였고 Choi는 Kim의 논문의 익명성 문제를 제기하고 이를 개선한 새로운 프로토콜을 제안하였다.
본 논문에서는 Choi 프로토콜의 계산 오류와 이력 추적 가능 문제점을 제기하고, 이러한 문제점을 해결하는 새로운 프로토콜을 제안하고, 안전성과 효율성을 분석한다.

키워드: 원격 사용자 인증(Remote User Authentication), 스마트카드(SmartCard), 익명성(Anonymity), 추적성(Traceability)

I. 서론

분산컴퓨팅 환경에서 원격으로 작업을 수행하는 일이 빈번해지는 요즘 인증에 대한 많은 연구가 진행되고 있다. 그 중 스마트카드를 이용한 원격 사용자 인증은 스마트카드가 지닌 이동성과 기능적 안전성으로 인하여 특히 주목받고 있다.

초기의 인증 프로토콜들에서 서버는 사용자 인증 요청에 대한 검증을 위해 검증 테이블을 저장하고 있어야 했다[4]. 하지만 서버에 대한 안전성과 신뢰가 요구되고 사용자의 아이디와 패스워드 관리 비용 부담 등의 문제가 제기되면서 검증테이블을 이용하지 않는 인증 기법들이 연구되고 있다. 특히 유비쿼터스 환경 하에서는 개인 정보보호와 프라이버시에 많은 관심이 증가되면서 스마트카드를 이용한 익명성을 제공하는 원격 인증 시스템에 대한 연구들이 수행되고 있다.

2004년 Das 등은 동적 아이디를 사용하여 사용자와 원격 서버를 제외한 제 3자에 대해 사용자 익명성을 제공하려는 기법을 최초로 제안하였고[3], 2006년 Chai는 원격서버에 대해서도 익명성을 보장하는 프로토콜을 처음 제안하였다[2]. 2008년 Kim 등은 추적 가능한 프로토콜을 제안하여 악의적인 사용자에 대해 추적할 수 있는 기능을 제안하였으나 2009년 Choi[6]는 Kim[5]의 논문이 익명성을 보장하지 못하는 문제점을 찾아냈다. 그러나 Choi의 기법은 로그인단계에서 스마트카드가 합법적인 값을 계산하지 못하는 문제점이 있다. 또한 Choi의 기법에서 서버는 사용자가 정확히 누구인지는 알 수 없으나 이전 세션과 같은 사용자임은 알 수 있기 때문에 사용자의 완전한 익명성이 보장되지 않는다. 본 논문에서는 정당한 사용자인 공격자에 대해서도 사용자 익명성을 보장하면서 추적 가능한 스마트카드 기반 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구로 Choi의 프로토콜을 살펴보고 3장에서 개선된 프로토콜을 제안하고 분석한 후 4장에서 결론을 맺는다.

II. 관련 연구

1. 관련연구

1.1 Choi et al. 의 프로토콜

Choi 등의 프로토콜에 대하여 살펴본다. Choi 등의 프로토콜은 등록단계, 로그인단계, 인증단계, 추적단계, 패스워드 변경단계로 구성되어 있다.

□ 〈등록 단계〉

Step1. 등록단계에서는 스마트카드를 사용하는 새로운 사용자 U_i가 자신의 ID_i와 $h(PW_i)$를 안전한 채널을 이용하여 서버에게 전달한다.

Step2. 서버는 사용자의 ID_i와 $h(PW_i)$를 이용하여 다음을 계산한다.

1) $R_i = h(x) \oplus h(PW_i) \oplus h(h(ID_i) \oplus x)$
2) $I = h(ID_i \oplus x)$
3) $I_c = h(ID_i \oplus x) \oplus h(ID_i) \oplus h(PW_i)$
4) $TR = E_{PTR}[ID_i, UIN]$
5) $ATR = h(TR \oplus x)$

Step3. 서버는 스마트카드에 $\{I, I_c, R_i, h(), TR, p, y, ATR\}$를 저장하고 스마트카드를 사용자에게 발급한다.

□ 〈로그인 단계〉

Step1. 사용자는 스마트카드를 리더기에 삽입하고 ID_i와 PW_i를 입력한다.

Step2. 스마트카드가 다음과 같은 수행을 한다.

1) $I \oplus h(ID_i) \oplus h(PW_i) = I_c$
2) $X = g^a \bmod p$(a는 스마트카드에 의해 생성된 랜덤값)
3) $C_i = R_i \oplus h(PW_i)$
   $= h(x) \oplus h(h(ID_i) \oplus x)$
4) $UTR = h(h(ID_i) \oplus x) \oplus TR$
5) $OAR = h(h(ID_i) \oplus x) \oplus ATR$
6) $M = h(e \oplus T)$
7) $V = h(M \oplus y) \oplus h(ID_i)$
8) $C_{ID_i} = h(C_i \oplus h(y \oplus T), X, OAR)$

Step 3. 인증을 위해 서버에게 메시지 $\{T, C_{ID_i}, M, V, X, UTR\}$을 보낸다.

□ 〈인증 단계〉

Step1. S는 메시지 $\{T, C_{ID_i}, M, V, X, UTR\}$를 T' 시간에 받는다.

Step2. 서버는 T시간과 T' 시간 사이의 시간 간격(time interval)을 확인하고 C_{ID_i}를 다음의 식을 이용하여 검증한다.

1) $h(ID_i) = V \oplus h(M \oplus y)$
2) $TR = h(h(ID_i) \oplus x) \oplus UTR$
3) $OAR = h(TR \oplus x) \oplus h(h(ID_i) \oplus x)$

Step3. 만약 C_{ID_i}와 식이 일치하면 $SK = X^b \bmod p$,
$Y = g^b \bmod p$, M_s를 계산하여 Y와 함께 보낸다.
$M_s = h(OAR \oplus M \oplus y, SK, Y)$

Step4. 사용자는 다음을 확인한다.

1) $SK = y^a \bmod p$
2) $M_s = h(OAR \oplus M \oplus y, SK, Y)$

step5. M_s값이 일치하면 사용자와 서버는 SK를 이용하여 세션키를 맺는다.
$h(SK) = SK_{us}$

□ 〈추적 단계〉

Step1. 서버는 TR값과 CS를 함께 신뢰기관에 제출한다.

Step2. 신뢰기관은 CS를 확인하고, TR값을 자신의 개인키로 복호화하여 서버에 사용자 정보를 알려준다.

1.2 분석

Choi가 제안한 프로토콜은 다음과 같은 문제점이 있다.

가. 로그인 단계의 계산 오류

Choi의 기법에서는 로그인 단계의 Step. 2에서 스마트카드가 UTR의 값을 $h(h(ID_i) \oplus x) \oplus TR$을 계산하여 구한다고 하였다. 그러나 프로토콜에서 스마트카드가 알 수 있는 값은 $h(h(ID_i) \oplus x)$와 $h(x)$를 XOR 연산한 C_i 값뿐이다. 스마트카드는 서버의 비밀값 x를 알지 못하기 때문에 C_i로부터 $h(h(ID_i) \oplus x)$ 또는 $h(x)$값을 알아낼 수 없다. 따라서 Choi의 프로토콜에서 스마트카드는 정당한 UTR, OAR 값을 계산할 수 없다.

나. 사용자 추적 가능성

Choi의 기법에서는 인증단계에서 서버가 C_{ID_i}를 확인하는 과정에서 항상 같은 값인 $h(ID_i)$와 TR값을 얻게 된다. 서버는 사용자가 정확히 누구인지는 알 수 없으나 이전 세션과 같은 사용자임은 알 수 있다. 따라서 사용자는 서버에 대한 완전한 익명성을 제공받지 못하게 된다.

III. 본론

1. 제안 프로토콜

본 논문에서는 Choi 등의 프로토콜 기능을 만족하면서 사용자의 완전한 익명성까지 보장해 주는 기법에 대하여 제안한다.

1.1 제안 프로토콜

제안한 프로토콜은 등록단계, 로그인단계, 인증단계, 추적단계, 패스워드 변경단계로 나누어진다.

□ 등록 단계

Step1. 등록단계에서는 스마트카드를 사용하는 새로운 사용자 U_i 가 자신의 ID_i와 $h(PW_i)$를 안전한 채널을 이용하여 서버에게 전달한다.

Step2. 서버는 사용자의 ID_i와 $h(PW_i)$를 이용하여 다음을 계산한다.

1) $R_i = h(x) \oplus h(PW_i) \oplus h(h(ID_i) \oplus h(PW_i) \oplus x)$
2) $I = h(ID_i \oplus x)$
3) $I_c = h(ID_i \oplus x) \oplus h(ID_i) \oplus h(PW_i)$
4) $TR = E_{PTR}[ID_i, UIN] \oplus h(ID_i) \oplus h(PW_i)$
5) $ATR = TR \oplus h(x)$

Step3. 서버는 스마트카드에 $\{I, I_c, R_i, h(), TR, y\ ATR\}$를 저장하고 스마트카드를 사용자에게 발급한다. x,y는 서버의 비밀값이다.

□ 〈로그인 단계〉

Step1. 사용자는 스마트카드를 리더기에 삽입하고 ID_i와 PW_i를 입력한다.

Step2. 스마트카드는 다음과 같이 계산한다.

1) $I \oplus h(ID_i) \oplus h(PW_i) = I_c$
2) $X = g^c \bmod p$(c는 스마트카드에 의해 생성된 랜덤값)
3) $C_i = R_i \oplus h(PW_i)$
   $= h(x) \oplus h(h(ID_i) \oplus h(PW_i) \oplus x)$
4) $UTR = C_i \oplus TR$
5) $OAR = C_i \oplus ATR$
6) $V = h(X \oplus y) \oplus h(ID_i) \oplus h(PW_i)$
7) $C_{ID_i} = h(C_i \oplus h(y \oplus T), X, OAR)$

Step 3. 인증을 위해 서버에게 메시지 $\{T, C_{ID_i}, V, X, UTR\}$을 보낸다.

□ 〈인증 단계〉

Step1. 서버는 메시지 $\{T, C_{ID_i}, V, X, UTR\}$를 T' 시간에 받는다.

Step2. 서버는 T시간과 T'시간 사이의 시간 간격(time interval)을 확인하고 C_{ID_i}를 검증한다.

1) $h(ID_i) \oplus h(PW_i) = V \oplus h(X \oplus y)$
2) $C_i = h(h(ID_i) \oplus h(PW_i) \oplus x) \oplus h(x)$
3) $TR = C_i \oplus UTR$
4) $OAR = C_i \oplus h(x) \oplus TR$
5) $C_{ID_i} = h(C_i \oplus h(y \oplus T), X, OAR)$

Step3. 만약 C_{ID_i}와 식이 일치하면 서버는 $SK = X^d \bmod p$, $Y = g^d \bmod p$, M_s를 계산하여 Y와 함께 보낸다.
$M_s = h(OAR \oplus X \oplus y, SK, Y)$

Step4. 사용자는 다음을 확인한다.

1) $SK = y^a \bmod p$
2) $M_s = h(OAR \oplus X \oplus y, SK, Y)$

step5. M_s값이 일치하면 사용자와 서버는 SK를 이용하여 세션키를 맺는다.
$h(SK) = SK_{us}$

□ 〈추적 단계〉

악의적인 사용자를 추적하기 위해 서버는 다음을 수행한다.

Step1. 악의적인 사용자 발견 시 서버는 $TR \oplus V \oplus h(y \oplus X)$ 값을 계산하여 신뢰기관에 전달한다.

Step2. 신뢰기관은 CS를 확인하고, TR값을 계산하기 위해 자신의 개인키로 복호화하여 사용자 정보를 서버에게 알려준다.

□ 사용자 패스워드 변경

U_i가 자신의 PW_i를 새로운 PW_i^*로 바꾸고자 할 때, U_i는 서버와 상관없이 스마트카드만을 이용하여 새로운 PW_i^*로 교체할 수 있다. 스마트카드는 다음과 같이 수행한다.

Step1. U_i는 자신의 스마트카드를 리더기에 삽입 후, 자신의 ID_i와 PW_i를 입력하고 스마트카드는 다음을 확인한다.
$I \oplus h(ID_i) \oplus h(PW_i) = I_c$

Step2. 만약 값이 일치하면 스마트카드는 다음과 같이 수행하여 PW_i를 교체한다.

$I_c \oplus h(PW_i) \oplus h(PW_i^*) = I_c^*$

$R_i \oplus h(PW_i) \oplus h(PW_i^*) = R_i^*$

$TR \oplus h(PW_i) \oplus h(PW_i^*) = TR^*$

$ATR \oplus h(PW_i) \oplus h(PW_i^*) = ATR^*$

1.2 분석

이 절에서는 제안한 프로토콜에 대한 효율성과 안전성에 대하여 분석한다.

□ 안전성

• 위장공격

공격자는 사용자의 메시지 $\{T, C_{ID_i}, V, X, UTR\}$를 가로챌 수 있다. 만약 공격자가 사용자서버에 등록된 정당한 사용자라면 자신의 스마트카드의 y값을 이용하여 $h(ID_i) \oplus h(PW_i) = V \oplus h(X \oplus y)$을 계산할 수는 있다. 하지만 서버의 비밀키 x를 모르기 때문에 UTR과 C_{ID_i}를 조작할 수 없어 사용자로 위장할 수 없다.

• 사용자 익명성

서버는 자신이 가지고 있는 서버의 비밀값과 사용자로부터 받은 메시지 $\{T, C_{ID_i}, V, X, UTR\}$를 이용하여 동적 아이디를 생성하고 정당성을 인증 받을 수 있다. 이때, 서버는 정당한 사용자임은 확인할 수 있지만 사용자의 아이디는 알 수 없기 때문에 사용자 익명성이 제공된다. 또한 인증단계에서 서버가 C_{ID_i}값을 확인하기 위하여 $h(ID_i) \oplus h(PW_i)$를 계산해내지만 이 값은 사용자가 패스워드를 변경하게 되면 패스워드 변경시마다 변경되게 된다. 따라서 서버는 사용자가 누구인지, 같은 사용자가 계속 사용중인지 등의 이력 추적이 어렵게 된다. 따라서 사용자는 패스워드를 주기적으로 변경하게 될 경우 완전한 사용자 익명성을 보장받을 수 있다.

• 내부자 공격

서버의 내부자 공격을 막기 위하여 사용자의 ID_i는 제공하지만 패스워드는 암호학적 해시함수를 이용하기 때문에 PW_i는 노출되지 않는다.

• 재전송 공격

타임스탬프를 이용하여 메시지의 유효성을 검사하고 있기 때문에 시간차를 두고 공격을 수행하는 재전송 공격으로부터 안전할 수 있다. 만약 공격자가 사용자의 메시지를 저장하고, 재전송할 경우 그 메시지는 인증단계에서 검증을 통과할 수 없다.

□ 효율성

Choi의 로그인단계에서 이용되던 M값을 X로 대체 이용함으

로써 Choi의 프로토콜보다 해쉬 연산수가 1회 감소하였다. 그러나 인증단계와 추적단계에서는 해쉬 연산 수가 1회 증가되었다.

Ⅳ. 결론

최근 스마트카드 기반의 인증 기법들은 사용자 익명성을 제공하면서도 악의적인 사용자를 추적하는 연구가 활발하다.

본 논문에서는 Choi 등이 제안한 프로토콜에서 로그인 단계의 계산 오류 문제점을 제시하고 정당한 사용자가 이력추적을 당할 수 있음을 보였다. 그리고 이를 개선한 새로운 프로토콜을 제안하였다. 제안한 프로토콜은 Choi 등의 계산 오류 문제점을 해결하였으며 사용자 이력 추적이 어렵고 정당한 사용자의 위장공격으로부터 안전하게 설계되었다.

참고문헌

[1] H.Y. Chien, C.H. Chen, A Remote Authentication Scheme Preserving User Anonymity, IEEE AINA'05, Vol. 2, pp. 245-248, 2005.

[2] Z. Chai, Z. Cao, and R. Lu, Efficient Password-Based Authentication and Key Exchange Scheme Preserving User Privacy, WASA'06, LNCS 4138, pp. 467-477, 2006.

[3] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics, Vol. 50, No.2, pp. 629-631, 2004.

[4] L. Lamport, Password authentication with insecure communication, Communications of the ACM, Vol.24, No.11, pp. 770-772, 1981.

[5] 김세일, 천지영, 이동훈, 추적이 가능한 스마트카드 사용자 인증 기법, 한국정보보호학회, 제 18권, 제5호, pp.31-39, 2008.

[6] 최종석, 신승수 , 사용자 익명성을 제공하는 추적 가능한 인증 프로토콜, 한국콘텐츠학회논문지 제9권 제4호 2009.