한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

스마트 카드를 이용한 타임스탬프 기반의 사용자 인증 스킴의 안전성 분석

문종호°, 원동호*
°*성균관대학교 정보통신보호연구실
e-mail:{jhmoon, dhwon}@security.re.kr°*

A Security Analysis of a Timestamp-based User Authentication Scheme with Smart Card

Jongho Mun°, Dongho Won*
°*Sungkyunkwan University Information Security Group

● 요 약 ●

안전하지 않은 네트워크에서 정당한 사용자를 인증하여 접근을 허가하는 사용자 인증 기법은 매우 중요한 기술이다. 스마트카드를 이용한 사용자 인증 기법은 연산의 효율성과 사용의 편리성, 저장 공간 등의 이유로 최근까지 많은 연구가 진행되고 있다. Huang 등은 Awasthi 등이 제안한 기법의 취약점을 개선하고 연산 효율성 및 편리성을 증대시킨 새로운 기법을 제안하였다. 그러나 Huang 등이 제안한 기법 역시 비밀키가 노출되고 위장 공격, 서비스 거부 공격 등에 취약하다는 것이 확인되었다. 본 논문에서는 Huang 등이 제안한 기법을 살펴보고 안전성을 분석한다.

키워드: 스마트카드(Smart Card), 사용자 인증(User Authentication), 보안(Security)

I. 서 론

공개된 네트워크를 통하여 비밀 정보의 송수신이 이루어지는 시스템에서는 사용자의 신원을 확인하는 인증(Authentication) 기능이 필수적이다. 많은 인증 기법들 중에서도 연산의 효율성과 사용의 편리성 때문에 스마트카드 기반의 인증 기법[1, 2, 3, 4]들이 활발하게 연구되고 있다. 스마트카드는 변조방지 기능을 갖는 IC(Integrated Circuit) 칩을 내장한 카드로서 개인정보를 저장할 수 있는 메모리와 산술 연산을 수행할 수 있는 프로세서로 구성되어 있다. 스마트카드를 기반으로 하는 원격 사용자 인증 기법은 일반적으로 설정(Initialization) 단계, 등록(Registration) 단계, 로그인(Login) 및 인증(Authentication) 단계, 비밀번호 변경(Password Change) 단계 등 네 개의 단계로 구성된다. 2011년에 Awasthi 등은 스마트카드를 이용한 타임스탬프 기반의 사용자 인증 기법[5]을 제안하였다. 이후 이 기법이 위장 공격에 취약하며 사용자의 패스워드 변경이 자유롭지 못한 단점이 발견되었다. 최근 Huang 등은 이러한 문제점을 해결하기 위해 새로운 기법[6]을 제안하였다. Huang 등은 자신들이 제안한 기법이 기존의 기법과 달리 원격 서버가 인증을 위한 사용자의 어떠한 정보도 필요로 하지 않으며 자유로운 패스워드 변경을 지원한다고 주장한다. 그러나 Huang 등이 제안한 기법은 키 정보센터의 비밀키를 노출시킬 수 있는 치명적인 취약점을 가지고 있으며 이를 이용한 위장 공격에도 취약하다. 본 논문에서는 Huang 등이 제안한 기법의 안전성을 분석한다. 본 논문의 구성은 다음과 같다. 2장에서는 Huang 등이 제안한 스마트카드를 이용한 타임스탬프 기반의 기법을 개략적으로 살펴본다. 이어서 3장에서는 Huang 등이 제안한 기법의 취약점을 분석하여 안전성을 검증한다. 마지막으로 4장에서 결론을 맺는다.

II. Huang et al. 기법 분석

본 장에서는 Huang 등이 제안한 인증 기법을 개략적으로 살펴본다.

1. 용어

본 논문에서 사용하는 용어의 표기법은 아래의 표 1과 같다.

‡ 교신저자: 원동호(dhwon@security.re.kr)

표 1. 용어

용어	설명
U_i	유저 i
KIC	키 정보센터(서버)
S	서버
ID_i	유저 i의 아이디
PW_i	유저 i의 비밀번호
CID_i	사용자 I의 식별자
Φ	오일러 함수
p, q	큰 소수
e, d	키 정보센터의 공개키 및 비밀키
T	타임스탬프
H	암호학적 일방향 해시 함수

2. Huang et al. 기법의 개요

표 1에서 정의한 용어들을 사용하여 Huang 등이 제안한 기법을 설명한다. 해당 기법은 설정, 등록, 로그인 및 인증, 비밀번호 업데이트의 4단계로 구성되어 있다.

2.1 설정(Initialization) 단계

설정 단계에서는 키 정보센터가 두 개의 큰 소수 p, q를 선택한 후 $n = p \times q$ 및 $\Phi(n) = (p-1)(q-1)$를 계산하여 $ed \equiv 1 \ mod \ \Phi(n)$을 만족하는 공개키 e와 비밀키 d를 구한다.

2.2 등록(Registration) 단계

등록 단계에서 사용자 U_i는 안전한 채널을 이용하여 자신의 아이디 ID_i와 비밀번호 PW_i를 키 정보센터로 전송한다. 키 정보센터는 수신한 값들로부터

$$CID_i = H(ID_i \oplus d)$$
$$S_i = (CID_i^d \ mod \ n) \oplus H(PW_i)$$

를 계산하여 사용자에게 발급할 스마트카드에 (n, e, S_i, ID_i)를 저장한 뒤 안전한 채널을 이용하여 사용자 U_i에게 전달한다.

2.3 로그인(Login) 및 인증(Authentication) 단계

로그인 및 인증단계에서 임의의 사용자 U_i가 카드 리더기에 스마트카드를 삽입하고 자신의 아이디 ID_i와 비밀번호 PW_i를 입력하면 스마트카드는

$$X_i = S_i \oplus H(PW_i)$$
$$Y_i = X_i^{H(ID_i, T_c)} \ mod \ n$$

를 계산한다. T_c는 사용자 U_i의 타임스탬프이다. 계산이 완료되면 스마트카드는 로그인 요청 메시지 (ID_i, n, e, T_c, Y_i)를 서버 S에 전송한다. 사용자의 로그인 요청을 받은 서버 S는 우선 타임스탬프의 유효기간을 검증하여 요청의 수락여부를 결정한다. 타임스탬프가 유효하면 전송된 값들과 키 정보센터의 비밀키 d를 이용하여

$$CID_i = H(ID_i \oplus d)$$

를 계산하여 얻고 추가적으로

$$Y_i^e = H(ID_i \oplus d)^{H(ID_i, T_c)} \ mod \ n$$

을 계산하여 $CID_i == Y_i^e$를 만족하는지 확인한다. 만족한다면 서버 S는

$$R = (H(ID_i \oplus T_s^{'}))^d \ mod \ n$$

을 계산하여 $(R, T_s^{'})$을 사용자에게 전송한다. $T_s^{'}$는 서버 S의 타임스탬프이다. 이 값을 서버 S로부터 수신 받은 사용자 U_i는 먼저 타임스탬프의 유효기간을 검증한다. 타임스탬프가 유효하면

$$R^{'} = R^e \ mod \ n$$

을 계산하여 $R^{'} == H(ID_i, T_s^{'})$를 만족하는지 확인한다. 만족한다면 사용자 U_i는 서버 S와의 상호인증이 이루어진 것으로 간주한다.

2.4 비밀번호 업데이트(Password Update) 단계

비밀번호 업데이트 단계는 사용자 U_i가 자신의 비밀번호 PW_i를 새로운 비밀번호 $PW_i^{'}$으로 변경하고자 할 때 수행되는 단계이다. 해당 단계는 키 정보센터에 새 비밀번호를 등록하지 않으며 사용자 단독으로 수행된다. 사용자 U_i가 새로운 비밀번호 $PW_i^{'}$를 입력하면 스마트카드는

$$S_i^{'} = S_i \oplus H(PW_i) \oplus H(PW_i^{'})$$

을 계산하여 기존의 S_i를 $S_i^{'}$으로 갱신한다.

III. Huang et al. 기법 안전성 분석

본 장에서는 Huang 등이 제안한 기법이 가지고 있는 취약점을 분석한다. 해당 기법은 RSA 암호시스템에 기반하고 있으며 전적으로 비밀키 d의 안전성에 의존하는 기법이다. 안전성 분석을 위해 공격자는 스마트카드에 저장된 값과 사용자와 서버 간의 모든 전송 메시지를 얻을 수 있다고 가정한다.

3.1 키 정보센터의 비밀키 노출

공격자 U_a는 정상적인 등록 과정을 통해 스마트카드를 발급받은

후 자신의 스마트카드에 저장된 값 (n, e, S_a, ID_a)를 얻는다. 얻어낸 값을 이용하여

$$S_a^{'} = (S_a \oplus H(PW_a))^e \ mod \ n$$
$$= CID_a = H(ID_a \oplus d)$$

를 계산한다. 공격자는 계산된 $S_a^{'}$과 자신의 아이디 ID_a를 이용하여 키 정보센터의 비밀키 값 d를 알아낼 수 있다.

3.2 사용자 위장 공격

공격자 U_a는 사용자 U_i의 정상적인 로그인 요청 메시지 (ID_i, n, e, T_c, Y_i)를 탈취한 뒤 사용자 U_i로 위장할 수 있다. 키 정보센터의 비밀키 값 d를 이용하여

$$X_i = H(ID_i \oplus d)$$
$$Y_i^{'} = X_i^{H(ID_i, T_c^{'})} \ mod \ n$$

를 계산하고 서버 S에 로그인 요청 메시지 $(ID_i, n, e, T_c^{'}, Y_i^{'})$을 전송하여 로그인 요청을 하면 서버 S는 해당 요청을 사용자 U_i의 정상적인 로그인 요청으로 인식한다. $T_c^{'}$는 공격자 U_a의 타임스탬프이다.

3.3 서버 위장 공격

공격자 U_a는 사용자 U_i의 정상적인 로그인 요청 메시지 (ID_i, n, e, T_c, Y_i)를 탈취한 뒤 서버 S로 위장할 수 있다. 키 정보센터의 비밀키 값 d를 이용하여

$$R^{'} = (H(ID_i, T_s^{'}))^d \ mod \ n$$

을 계산하고 사용자 U_i에게 $(R^{'}, T_s^{'})$을 전송하여 로그인 응답을 하면 사용자 U_i는 정상적으로 서버 S와 상호 인증이 이루어진 것으로 간주한다.

3.4 서비스 거부 공격

Huang 등이 제안한 기법은 로그인 요청 메시지를 생성하기 이전에 사용자가 입력한 비밀번호가 잘못된 것인지 여부를 검증하지 않는다. 사용자가 패스워드를 잘못 입력한 경우 인증 단계에서 서버의 연산 과정을 거쳐야만 비밀번호 오류 여부를 감지할 수 있다. 공격자가 임의의 패스워드를 사용하여 서버에 끈임 없이 로그인 요청을 한다면 정당한 사용자의 서비스 요청을 처리할 수 없게 되는 상황이 발생하게 된다. 원활한 서비스 제공을 위해 로그인 요청 단계에서 비밀번호 검증을 하거나 서버에 최대 로그인 요청 허용 횟수를 설정할 필요가 있다.

IV. 결 론

스마트카드를 이용하는 인증기법에 대한 다양한 연구가 진행되고 있다. Huang 등은 Awasthi 등이 제안한 기법을 개선하여 스마트카드를 이용한 타임스탬프 기반의 강화된 사용자 인증 기법을 제안하였으나 본 논문에서 키 정보센터의 비밀키 노출, 사용자 및 서버 위장 공격, 서비스 거부 공격 등에 여전히 취약한 것을 확인하였다. 차후에는 이러한 취약점을 개선하여 안전성이 더욱 강화된 사용자 인증 기법에 대한 연구를 진행할 예정이다.

Acknowledge

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014R1A1A2002775).

참고문헌

[1] J. Jung, W. Jeon, and D. Won, “An enhanced remote user authentication scheme using smart card,” ICUIMC, 2014

[2] J. Mun, J. Kim, W. Jeon, Y. Lee, and D. Won, “An Improvement of Encrypted Remote user Authentication Scheme by Using Smart Card”, Multimedia and Ubiquitous Engineering, pp. 451-458, 2014.

[3] C. Chung, and C. Lee, “A smart card-based authentication scheme using user identify cryptography”, International Journal of Network Security, vol. 15, no. 2, pp. 139-147, 2013.

[4] H. Yeh, T. Chen, and W. Shih, “Robust smart card secured authentication scheme on SIP using Eliptic Curve Crptography”, Computer Standards & Interfaces, pp. 397-402, 2014.

[5] K. Awasthi, K. Srivastava, and R. Mittal, “An improved timestamp-based remote user authentication scheme,” Computers and Electrical Engineering, vol. 37, pp. 869-874, 2011

[6] H. Huang, H. Chang, and P. Yu, “Enhancement of timestamp-based user authentication scheme with smart card,” International Journal of Network Security, vol. 16, no. 6, pp. 463-467, Nov. 2014.