제22회 한국정보처리학회 추계학술발표대회 논문집 제11권 제2호 (2004. 11)

스마트카드를 이용한 사용자 인증

이건직*, 이병직
*강원대학교 전기전자정보공학부
경북대학교 컴퓨터공학과
e-mail : othiin@emapl.com

User Authentication Scheme using Smart Card

Keon-Jik Lee*, Byeong-Jik Lee
*Dept. of Electrical & Computer Eng., Kangwon National University
Dept. of Computer Eng., Kyungpook National University

요 약

원격 사용자가 시스템에 로그인 할 경우에 그 로그인 사용자를 인증하기 위한 많은 방안들이 제안되고 있다. 본 논문에서는 스마트 카드를 이용한 향상된 사용자 인증 방법을 제안한다. 제안된 기법의 안전성은 이산대수 문제의 어려움과 일방향 해쉬 함수의 특성에 기반하고 있으며, 재전송 공격과 위장 공격에 취약점을 드러내지 않는다.

1. 서론

Lamport 는 안전하지 않은 통신 선로상에서 원격 사용자를 인증(authentication)하기 위하여 패스워드 인증 방법을 제안했다 [1]. 그러나, 이 방법은 시스템이 로그인(login) 유저를 인증하기 위하여 패스워드 테이블을 저장해야 하는 문제점을 가지고 있었다. Hwang 등은 Shamir 의 ID 서명에 기반하여 스마트 카드(smart card)를 이용한 인증 방법을 제안했다 [2]. Wu 는 유클리드 평면에서의 기하학적 특성에 기반한 사용자 인증 방법을 제안했다 [3]. 그러나, 이 방법은 보안상의 결점이 발견되었다. 최근에 Hwang 과 Li 는 시스템에 패스워드 파일을 저장하지 않고 스마트 카드를 사용하여 사용자를 인증하는 방법을 제안하였다 [4]. 하지만 Chen 과 Chang 은 Hwang 과 Li 의 방법이 위장 공격(masquerade attack)에 취약함을 지적하였다 [5]. 이 공격 하에서 공격자는 다른 합법적인 사용자의 패스워드 정보를 유추해 낼 수 있으며 이를 이용하여 시스템에 다른 유저로 위장하여 로그인 할 수 있다. Sun 은 스마트 카드를 사용한 수정된 사용자 인증 방안을 제안했다 [6]. 그러나 이 방안의 안전성은 단지 일방향 해쉬(oneway hash) 함수의 특성에만 의존한다. Shen 등은 Hwang 과 Li 의 방법에 대해서 Chen 과 Chang 의 방법과 유사한 위장 공격 방안을 제안했다 [7]. 이 방법의 단점은 사용자 등록과 사용자 로그인 과정이 보안(secure) 채널상에서 수행되어야만 한다는 것이다. 이 외에도 원격 사용자 로그인을 인증하기 위한 많은 연구가 수행되어 왔다 [8 – 19].

본 논문에서는 스마트 카드를 사용하여 원격 사용자를 효율적으로 인증하는 방안을 제안한다. 먼저 기존 제안된 방안을 간단히 살펴보고 프로토콜을 향상시키기 위한 방법을 제안한다. 제안된 방안의 안전성은 이산 대수 문제의 어려움과 일방향 해쉬 함수의 특성에 의존한다. 그리고 제안된 방안은 재전송 공격(replay attack)과 위장 공격에 취약점을 드러내지 않는다.

2. 이산 대수 문제

제안된 기법의 안전성은 유한 필드(finite field)상에서 이산 대수 문제(discrete logarithm problem)의 어려움에 기반하고 있다. p 는 솟수 (prime number), 그리고 α 는 솟수 p 의 원시 원소(primitive element)라고 가정하자. 그러면 원시 원소 α의 거듭제곱은 1 부터 p - 1 사이의 모든 정수를 생성한다. 다시 말해서 어떤 정수 X에 대해 $Y = \alpha^X \bmod p$ $(1 \le X \le p\text{-}1)$를 만족하는 X가 반드시 존재한다. 여기서 X 로부터 Y 의 계산은 비교적 쉽지만, 반대로 Y 로부터 X 의 유추는 계산학적으로 매우 어렵다는 것이 이산 대수 문제이다.

3. 기존 기법의 분석

본 절에서는 Shen 등이 제안한 기법을 간략히 분석한다. 이 기법은 3 개 단계, 즉 등록(registration) 단계, 로그인(login) 단계, 그리고 인증(authentication) 단계로 구성된다: 각 사용자는 등록 단계에서 비보안 채널 상에서 원격 시스템에게 자신의 식별 정보들을 전송한다. 시스템은 사용자가 식별된 후 비보호 채널을 통해서 사용자에게 스마트 카드를 발급한다. 그리고 또한 시스템은 보안 채널을 통해서 시스템과 사용자만이 알고 있는 비밀 식별 정보와 패스워드를 사용자에게 전송한다. 사용자가 시스템으로부터 서비스를 받기 위해서 시스템을 접근할 때 사용자는 자신이 가지고 있는 스마트 카드를 시스템에 연결된 입력 장치로 삽입하고, 등록 단계에서 시스템으로부터 받은 비밀 식별 정보와 패스워드를 입력한다. 시스템은 인증단계에서 사용자를 검사하고 최종적으로 사용자의 시스템 진입을 수락한다.

등록 단계:
등록 단계는 보안 채널 상에서 수행된다고 가정한다. 서버는 두 시스템 파라미터 p 와 x 를 준비한다. 여기서 p 는 매우 큰 솟수이고, x 는 시스템의 비밀 키이다. 또한 일방향 해쉬함수 h 도 존재한다. 먼저 새로운 사용자 U_i 는 등록을 위해서 J_i 를 시스템에 제출한다. 여기서 J_i 는 U_i 를 유일하게 구별해 주는 식별 스트링들이다. 시스템은 $SID_i = Red(J_i)$와 $PW_i = SID_i^x \bmod p$ 를 계산한다. 여기서 $Red(\,)$는 시스템과 사용자만이 알고 있는 비밀 식별자를 생성한다. 즉 SID_i 는 특정 시스템과 비밀리에 간직하는 U_i 의 식별자이다. 다음으로 시스템은 파라미터 h 와 p 를 담고 있는 스마트 카드를 사용자에게 발급한다. 그리고 보안 채널을 통해서 U_i 에게 SID_i와 PW_i를 전달한다. 그 단계별 과정은 아래 Fig. 1 과 같다.

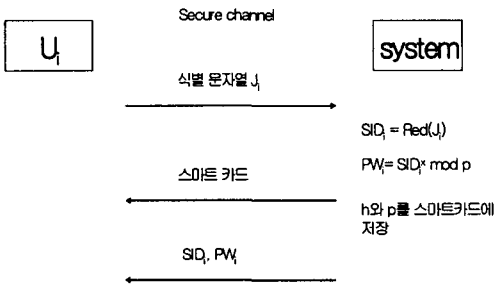

Fig. 1. 등록 단계

로그인 단계:
로그인 단계도 보안 채널상에서 수행된다고 가정한다. 사용자 U_i 는 발급받은 스마트 카드를 로그인 디바이스로 삽입하고 비밀 식별자 SID_i 와 패스워드 PW_i 를 입력한다. 스마트 카드는 입력 받은 정보를 가지고 다음의 작업들을 수행한다.

1. 무작위 숫자 r 을 생성한다.
2. $C_1 = SID_i^r \bmod p$ 를 계산한다.
3. $t = h(T \oplus PW_i) \bmod p - 1$ 를 계산한다. 여기서 T 는 로그인 디바이스의 현재 시간과 날짜 정보이며, $\oplus$는 배타적 논리합 연산자이다.
4. $M = SID_i^t \bmod p$ 를 계산한다.
5. $C_2 = M \cdot PW_i^r \bmod p$ 를 계산한다.
6. 로그인 요구 메시지 $C = (SID_i, C_1, C_2, T)$를 보안 채널을 통해서 시스템에게 전송한다.

인증 단계:
로그인 요구 메시지를 받은 후, 시스템은 다음의 과정을 통해서 사용자를 인증하게 된다.

1. SID_i 와 T를 검사한다. 만약 $T' - T$가 ΔT보다 크다면, 시스템은 로그인 요구를 거절한다. 여기서 T'는 시스템의 현재 시간과 날짜 정보이고, ΔT는 전송 지연을 고려한 유효한 타임 간격이다.
2. $PW_i = SID_i^x \bmod p$ 를 계산한다.
3. $t = h(T \oplus PW_i) \bmod p - 1$ 을 계산한다.
4. $C_2(C_1^x)^{-1} \bmod p = SID_i^t \bmod p$ 인지를 검사한다. 만약 같지 않으면, 시스템은 사용자의 로그인 요청을 거절한다.

4. 제안된 기법

본 절에서는 이산대수 문제와 일방향 해쉬 함수의 특성에 기반한 스마트 카드를 이용한 향상된 사용자 인증 방안을 제시한다. 앞서의 Shen 등의 방법과 달리 등록 단계와 로그인 단계는 패스워드의 전달을 제외하고는 비보안 채널상에서 수행된다. 시스템 파라미터의 정의는 Shen 등의 방법과 유사하다.

등록 단계:
새로운 사용자 U_i 는 자신의 식별 정보 ID_i 를 등록을 위해서 시스템에게 전송한다. 시스템은 사용자 U_i 를 위한 패스워드 PW_i 를 다음 과정을 통해서 계산한다.

1. $ID_i' = h(ID_i)$를 계산한다.
2. $PW_i = (ID_i')^x \bmod p$ 를 계산한다.
3. 시스템 파라미터 h 와 p 를 포함한 스마트 카드를 사용자 U_i 에게 비보안 채널을 통해서 발급한다. 그리고 시스템은 보안 채널을 통해

서 PW_i 를 전달한다.

로그인 단계:
사용자 U_i 는 스마트 카드를 로그인 디바이스에 삽입하고, 식별자 ID_i 와 패스워드 PW_i 를 입력한다. 스마트카드는 다음 단계를 수행하고 그 결과를 시스템에게 전달한다.

1. $S = h(T \oplus ID_i \oplus PW_i)$를 계산한다. 여기서 T는 로그인 디바이스의 현재 시간과 날짜 정보이고, ID_i 는 송신자의 식별 정보, 그리고 PW_i 는 시스템으로부터 받은 패스워드 정보이다.
2. 로그인 요청 메시지 $M = (ID_i, S, T)$를 비보안 채널상에서 시스템에게 전달한다.

인증 단계:
시스템은 다음 단계를 거쳐서 사용자를 인증하게 된다.

1. $T' - T$가 ΔT보다 크다면, 시스템은 로그인 요청을 거부한다.
2. $ID_i' = h(ID_i)$를 계산한다.
3. $PW_i = (ID_i')^x \bmod p$ 를 계산한다.
4. $S = h(T \oplus ID_i \oplus PW_i)$인지를 검사한다. 만약 같으면 로그인 요청을 받아들인다.

제안된 방법은 기본적으로 이산대수 문제의 어려움에 기반하므로, 공격자 U_a가 $PW_a = (ID_a')^x \bmod p$ 에서 x를 계산해 내는 것은 계산학적으로 불가능하다. 그리고 시간 정보의 수정 없는 재전송 공격도 성공할 수 없다. 왜냐하면 인증 단계의 스텝 1 에서 그 변조가 발견되기 때문이다.
또한 유효한 시간 정보의 수정을 가한 재전송 공격도 성공할 수 없다. 이 경우도 역시 인증 단계의 스텝 4 에서 그 변조가 발견된다. 그리고, 어느 누구도 전송중인 로그인 요청 메시지 M 을 위조할 수 없다. 왜냐하면 S 값은 T 와 ID_i, 그리고 PW_i 의 올바른 조합으로부터 유도가 되기 때문이다. 여기서 T 와 ID_i 는 공개 정보이고, PW_i 는 비공개 정보이다. 공격자는 패스워드 정보를 알 수 없기 때문에 올바른 조합을 가지는 메시지를 만드는 것은 불가능하다.

5. 결론

본 논문에서 제안된 기법은 스마트 카드를 사용한 향상된 원격 사용자의 시스템으로 로그인을 효율적으로 인증할 수 있다. 기존의 Shen 등의 방법에 비해서, 제안된 방안은 비보안 채널상에서 등록 과정과 로그인 과정이 수행되므로 훨씬 효율적이고 실용적이며, 또한 재전송 공격과 위장 공격에 취약점을 가지지 않는다. 그리고 제안된 기법의 안전성은 이산 대수의 어려움과 일방향 해쉬 함수의 특성에 기반하고 있다.

참고문헌

[1] L. Lamport, Password authentication with insecure communication, Communications of ACM, Vol. 24, 1981, pp. 770–772

[2] T. Hwang, Y. Chen, and C. S. Laih, Non-interactive password authentications without password tables, IEEE Region 10 Conference on Computer and Communications Systems, IEEE Computer Society, 1990, pp. 429–431

[3] T. C. Wu, Remote login authentication scheme based on a geometric approach, Computer Communications, Vol. 18, No. 12, 1995, pp. 959–963.

[4] M. S. Hwang and L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, 2000, pp. 28–30

[5] C. K. Chan and L. M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Trans. Consumer Electron., Vol. 46, 2000, pp. 992–993

[6] H. M. Sun, An efficient remote use authentication scheme using smart cards, IEEE Trans. Consumer Electron., Vol. 46, 2000, pp. 958–961.

[7] J. J. Shen, C. W. Lin, and M. S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consumer Electron., Vol. 49, 2003, pp. 414–416

[8] M. Udi, A simple scheme to make passwords based on one-way function much harder to crack, Computers and Security, Vol. 15, No. 2, 1996, pp. 171-176

[9] M. Peyravin, and N. Zunic, Methods for protecting password transmission, Computers and Security, Vol. 19, No. 5, 2000, pp. 466-469

[10] L. H. Ki, I. C. Lin, and M. S. Hwang, A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transactions on Neural networks, Vol. 12, No. 6, 2001, pp. 1498-1504

[11] C. C. Lee, L. H. Li, and M. S. Hwang, A remote user password authentication using hash functions, ACM Operating Systems Review, Vol. 36, No. 4, 2002, pp. 23-29

[12] Y. L. Tang, M. S. Hwang, and C. C. Lee, A simple remote user authentication scheme, Mathematical and Computer Modeling, Vol. 36, 2002, pp. 103-107

[13] C. C. Lee, M. S. Hwang, and W. P. Yang, A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review, Vol. 36, No. 3, 2002, pp. 46-52

[14] M. S. Hwang, C. C. Lee, and Y. L. Tang, An improvement of SPLICE/AS in WIDE against guessing attack, International Journal of Informatica, Vol. 12, No. 2, 2001, pp.297-302

[15] M. S. Hwang, Cryptanalysis of remote login authentication scheme, Computer Communications, Vol. 22, No. 8, 1999, pp. 742-744

[16] L. Guillou, and J. J. Quisquater, A paradoxical identity-based signature scheme resulting from zero-knowledge, Advances in Cryptology, CRYPT88, Vol. LNCS 430, 1988, pp. 216-231

[17] L. Guillou, and J. J. Quisquater, Efficient digital public-key signatures with shadow, Advances in Cryptology, CRYPT87, Vol. LNCS 239, 1987, pp. 238

[18] C. C. Chang, and T. C. Wu, Remote password authentication with smart cards, IEE Proceedings-E, Vol. 138, No. 3, 1991, pp. 165-168

[19] C. C. Chang, and S. J. Hwang, Using smart cards to authenticate remote passwords, Computers and Mathematics with Applications, Vol. 26, No. 7, 1993, pp. 19-27