스마트카드를 이용한 원격사용자 및 리더기 상호인증 프로토콜†

김세일*, 최은영*, 이동훈*
*고려대학교 정보보호대학원

Improvement of a New Remote User Authentication Scheme Using Smart Card with Check Digits

Se Il Kim*, EunYoung Choi*, Dong Hoon Lee*
*Korea University of Center for Information Security Technology

요 약

본 논문에서는 Awasthi-Lal 이 제안한 프로토콜[1]에 대하여 살펴보고 그들이 제안한 새로운 원격사용자인증 프로토콜의 취약점에 대하여 분석한 다음, 이 취약점을 보완하기위해 신용카드 복제로 부터 안전한 *스마트카드를 이용한 원격사용자 및 리더기 상호인증 프로토콜*을 제안한다.

I. 서론

최근 신용카드 위·변조를 통한 피해 사례가 사회에서의 심각한 문제로 대두 되고 있다. 신용카드의 보안성을 높이기 위해 기존의 마그네틱 카드를 2008년까지 스마트카드로 전환이 의무화 될 예정이다. 그러나 스마트카드 안에 사용자 신용정보가 인증되지 않은 단말기에 의해 읽히고 그로인해 개인 신용정보가 노출이 되어진다면 카드복제가 가능하다.

초기에 스마트카드를 이용한 원격사용자 인증 프로토콜은 사용자가 등록한 패스워드 테이블을 서버가 저장을 하고 있어야했다[6]. 하지만 이는 서버에 대한 높은 안전성이 요구되고 저장 공간을 많이 차지하는 등의 취약점 때문에 패스워드 테이블이 없는 프로토콜이 제안되었다 [3][4][5]. 2000년에 Hwang and Li [7]는 ElGamal's cryptosystem 기반의 새로운 원격 사용자 인증 프로토콜을 제안하였다. Chan and Cheng [2] 은 정당한 사용자일 경우 서버의 비밀 키를 모르고도 쉽게 아이디와 패스워드를 만들 수 있도록 Hwang and Li의 프로토콜을 개선하였다.

이후에도, 이 프로토콜의 많은 개선을 거듭하였으며 최근 2005년 Awasthi and Lal [1]는 Kumar [9] 가 제안한 check digits의 개념을 이용한 새로운 원거리에 있는 사용자를 인증하는 프로토콜을 제안하였다.

기존의 원격사용자 인증 프로토콜에서 서버가 사용자를 검증하거나 사용자의 서버에 대한 검증이 있었지만 리더기를 포함한 상호 인증은 없기 때문에 공격자가 악의적인 리더기를 통해 스마트카드 내의 사용자 정보를 얻어서 카드 복제를 할 수 있다. 따라서 이에 따르는 검증이 필요하다.

† 본 연구는 2006년도 두뇌한국 21사업으로 수행되었음

스마트카드를 이용한 원격 인증 프로토콜이 갖추어야 하는 성질은 다음과 같다.[7]

1) 서버는 사용자의 패스워드를 포함한 테이블을 갖고 있지 않아야 한다.
2) 스마트카드의 계산량이 적어야한다.
3) 사용자는 자신의 패스워드를 자유롭게 선택할 수 있어야 한다.
4) 프로토콜은 시간 동기화 시간 지연 제한에 대해 요구하지 않아야 한다.
5) 프로토콜은 재사용공격에 안전해야한다.
6) 스마트카드의 정보가 노출되었을 때에도 안전해야한다.
7) 프로토콜은 스마트카드에 대한 오프라인 사전 공격에 안전해야 한다.
8) 프로토콜은 상호인증이 가능해야한다.
9) 스마트카드의 패스워드가 알려졌을 때에도 안전해야한다.

본 논문에서는 Awasthi and Lal 가 제안한 프로토콜[1]에 대해 분석하고 취약점을 보완한 프로토콜을 제안한다.

II. Awasthi-Lal이 제안한 프로토콜

Awasthi-Lal이 제안한 프로토콜은 초기단계, 등록단계, 로그인단계, 인증 단계로서 네 개의 부분으로 나뉜다. 다음은 각 단계에 대한 구체적인 설명이다.

1. 초기 단계

서버는 다음과 같은 파라미터를 생성한다.

- p: 큰 소수
- $f(.)$: 일방향 함수
- x_s: 서버의 개인키
- $C_K(.)$: 서버만이 갖고 있는 함수로서 등록된 ID에 대한 check digit 생성.

2. 등록 단계

사용자 U_i는 서버의 서비스들을 접근을 위해 등록을 한다. 이때 사용자는 안전한 채널을 통해 ID_i 를 서버에게 보내준다. 서버는 U_i에 대한 스마트카드 등록번호 R 를 지정하고 패스워드 PW_i 와 C_{ID} 를 계산한다.

$$PW_i = (ID_i \oplus R)^{x_s} \bmod p$$

$$C_{ID} = C_K(ID_i \oplus R)$$

서버는 공개 파라미터 $(f(.), R, p, C_{ID})$ 와 PW_i , C_{ID} 를 저장한다.

4. 로그인 단계

사용자는 스마트카드를 스마트카드 리더기에 접촉을 시키면 다음과 같은 계산을 수행한다.

1) 랜덤 넘버 r을 생성한다.
2) $C_1 = (ID_i \oplus R)^r \bmod p$
3) $t = f(T \oplus PW_i) \bmod p - 1$
4) $m = (ID_i)^t$
5) $C_2 = m(PW_i)^r \bmod p$
6) $C = (ID_i, R, C_{ID}, C_1, C_2, T)$ 를 서버에게 보낸다.

5. 인증 단계

서버가 현재 시간 T'안에 메시지 C 를 스마트카드 리더기로 부터 받았다면 그 서버는 다음과 같은 단계로 인증을 한다.

1) 정당한 ID_i인지 확인한다.
2) $C_{ID} = C_K(ID_i \oplus R)$ 가 올바른 값인지 체크 한다.
3) T와 T'의 시간차가 허용 가능한 시간 안에 도착했는지 체크한다. 만약 아닐 경우, 프로토콜 수행을 멈추고 적절한 메시지를 준다.
4) 다음 식을 통해 인증을 확인한다.

$$C_2 (C_1^{x_s})^{-1} = (ID_i)^{f(T \oplus PW_i)} \bmod p$$

III. Awasthi-Lal 프로토콜의 취약점 분석

기존에 Awasthi-Lal에 의해 제안된 프로토콜은 먼 거리에 있는 사용자가 서버에게 인증을 받기 위해 자신의 스마트카드를 리더기에

접촉 시키는 방법이다. 간단하게 프로토콜을 살펴보면 등록 단계에서 스마트카드 안에 정보를 저장시켜 주는데 이 정보가 악의적인 리더기에 의해 읽혀지게 되면 그 정보를 이용해서 공격자는 충분히 정당한 사용자와 같은 스마트카드를 복제할 수 있게 된다. 따라서 자신의 개인정보가 노출되어 프라이버시를 침해 받을 수 있다. 또한 반복공격을 막기 위해 사용하는 T (time stamp)는 로그인 단계에서 리더기에 의해 생성되는데, 만약 악의적인 리더기일 경우 T 값을 현재 시간과 다른 T'값으로 보냄으로써 원격사용자가 인증 받지 못하도록 방해할 수 있다. 이로 인해 정당한 사용자는 자신이 필요로 할 때, 빠른 시간 안에 자신임을 인증 받을 수 없다. 그렇기 때문에 리더기의 인증은 사용자를 위해 꼭 필요한 단계이다. 기존 프로토콜에 대한 안전성에 리더기에 대한 인증을 포함시켜 이러한 취약점을 보완한 프로토콜을 제안한다.

IV. 제안 프로토콜

Awasthi-Lal이 제안한 프로토콜에서의 취약점을 보완하기 위해서는 스마트카드 리더기의 인증 단계가 포함되어야 한다.

제안 프로토콜은 Awasthi-Lal이 제안한 프로토콜에 한 단계가 추가된 다섯 부분으로 이루어진다. 즉, 초기단계, 등록단계, 리더기 인증 단계, 로그인단계, 인증 단계이다.

1. 초기 단계

Awasthi-Lal의 프로토콜 등록 단계에 다음 두 가지 함수를 추가한다.

- $half\_L()$: 입력되는 값의 왼쪽 반을 출력하는 함수
- $half\_R()$: 입력되는 값의 오른쪽 반을 출력하는 함수

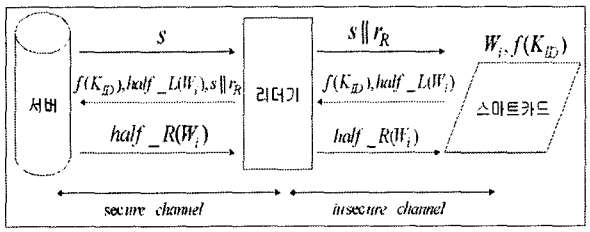
2. 등록 단계

등록 단계에서는 리더기 인증 단계에서 사용될 카드번호 K_{ID}를 생성한다.

서버는 PW_i , C_{ID} , K_{ID}, $half\_L()$, $half_R()$와 공개 파라미터 $(f(.), R, p, C_{ID})$를 안전하게 저장한다.

3. 리더기 인증 단계

사용자 U_i는 자신의 스마트카드를 리더기에 접촉시켰을 경우 [그림1] 같은 프로토콜을 수행한다. 프로토콜 설명은 다음과 같다.



[그림 1] 리더기 인증 단계

1) 서버는 랜덤 값 s를 리더기에 보낸다.
2) 리더기는 스마트카드에게 랜덤 값 s 에 자신의 등록번호 r_R을 붙여서 $s \| r_R$ 스마트카드에 보낸다.
3) 스마트카드는 두 가지 데이터를 생성을 한다. 첫 번째는 $f(K_{ID})$ 값으로 해당 스마트카드의 정보를 찾는데 이용된다. 두 번째로 $W_i = f(K_{ID} \| s \| r_R)$가 생성된다. W_i 는 서버와 스마트카드가 서로 같은 W_i 를 생성했는지 확인함과 동시에 인증을 위해 W_i 의 왼쪽부분인 $half_L(W_i)$만을 전송한다.
4) 리더기는 스마트카드로 부터 받은 정보와 함께 $s \| r_R$ 를 같이 전송한다.
5) 서버는 $f(K_{ID})$ 를 통해 정당한 스마트카드 사용자의 정보를 확인하고, K_{ID} 와 $s \| r_R$를 이용하여 W_i 를 생성한다. 서버는 랜덤 값 s 을 이용해 $s \| r_R$ 로부터 r_R을 얻어 낼 수 있고 리더기의 등록 여부를 확인 할 수 있다. 만약 등록되어 있다면 서버는 생성된 W_i 의 왼쪽부분이 리더기로부터 받은 값과 같은지 확인을 하고 자신의 인증을 위해 W_i의 오른쪽부분인 $half\_R(W_i)$ 을 전송한다.
6) 리더기는 서버로 부터 받을 값을 스마트

카드에 전송하여 값이 같은지 확인하고 통과 시에만 로그인 단계로 넘어간다.

4. 로그인 단계

리더기 인증 단계를 통과 한 후에 스마트카드의 정보가 리더기에 전달되어지기 때문에 카드의 복제를 사전에 막을 수 있다.

다음은 사용자를 서버가 인증하는 단계로 Awasthi-Lal의 프로토콜의 로그인 단계와 같다.

5. 인증 단계

리더기 인증 단계를 통과 한 후 악의적으로 리더기로부터 서버는 현재 시간과 동떨어진 T' 이 포함된 메시지 C를 받지 않는다. 다음은 사용자를 서버가 인증하는 단계로 Awasthi-Lal의 프로토콜의 로그인 단계와 같다.

V. 제안 프로토콜의 안전성 분석

서버가 스마트카드에 개인 정보를 보관하므로 개인 정보 프라이버시를 보장한다. 정당한 리더기가 스마트카드의 K_{ID} 를 알아내려고 해도 해쉬 함수의 성질로 인해 리더기는 W_i 와 s 를 사용하여 K_{ID} 값을 얻어 낼 수 없다. 또한 공격자가 도청을 통해 $f(K_{ID})$ 를 재전송하는 경우, 정당한 리더기는 매번 랜덤한 s 를 전송하게 되므로 공격자는 $half\_L(W_i)$ 을 생성할 수 없어 서버로 부터 인증 받을 수 없다. 따라서 악의적인 리더기일 경우 정당한 사용자의 스마트카드에 대한 정보를 얻어 낼 수 없으며 스마트카드 복제를 미연에 방지할 수 있다. 또한 리더기를 인증함으로서 악의적인 리더기가 T의 값을 변조해서 사용자 인증을 방해 할 여지도 없게 된다.

VI. 결론

본 논문에서는 Awasthi-Lal에 의해서 제안된 프로토콜에서 스마트카드 리더기의 인증을 간과하고 넘어갔을 때 발생될 수 있는 스마트카드 복제에 대한 취약점을 사전에 방지 할 수 있도록 하였다. 제안한 리더기 인증 프로토콜은 RFID에서도 사용 가능할 만큼 적은 연산량만을 필요로 하기 때문에 실제 스마트카드에 적용 가능하다. 또한 앞으로 원격 그룹사용자 인증이 가능하도록 연구가 진행 중에 있다.

[참고문헌]

[1] A. K. Awasthi and S. Lal "A New Remote User Authentication Scheme Using Smart Card with Check Digits" eprint arXivics/0504094, April 2005.

[2] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 46, pp. 992-993, 2000.

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

[4] C. C. Chang and T. C. Wu . : 'A password authentication scheme without verification tables', *Proc. 8th* IASTED *Int. Symp. Applied Informatics,* February 1990, Innsbruck, Austria, pp. 202-204

[5] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E,* vol. 138, no. 3, pp. 165-168, 1993.

[6] LAMPORT, L.: 'Password authentication with insecure communication', *Commun. ACM,* 1981,24, (11). pp. 77C772

[7] H. H. Li, H. K. Kim, J. C. Ha, D. G. Park, B. C. Lee "An Efficient Remote User Authentication Scheme Using Smart Cards" cisc Vol 15, No.2 December 2005

[8] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart

cards," *IEEE Trans. Consumer Electron.*, vol. 46, No. 1, pp. 28-30, 2000.

[9] M. Kumar "New remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 50, No. 2, pp. 597-600, May 2004.