스마트카드를 이용한 인증된 키 교환 프로토콜

*조윤진 **이동훈
고려대학교 정보보호대학원
*crypto72@hanmail.net **donghlee@korea.ac.kr

An Authenticated Key Exchange Protocol Using Smart Cards

*Cho, Youn-Jin **Lee, Dong-Hoon
Center for Information Security Technologies (CIST), Korea University

요약

최근에 제안되고 있는 원격 서버에 로그인하기 위한 방법은 ID와 패스워드뿐만 아니라 스마트카드를 함께 사용한다. 기존의 ID 와 패스워드를 사용한 인증은 공격자에 의해 추측이 가능하므로 사용자 가장 공격이 가능하다는 약점을 가지고 있다. 하지만 스마트카드와 ID, 패스워드를 사용하면 ID와 패스워드가 추측가능할지라도 스마트카드를 소지하고 있지 않다면 사용자 가장 공격 (impersonate attack)을 할 수 없다. 이 논문에서는 스마트카드와 ID, 패스워드를 함께 사용하여 원격 서버에 인증과 더불어 안전한 키 교환을 하며, 기존에 다른 논문들에서 언급한 조건들을 모두 만족하면서 안전한 키 교환까지 제안하였다. 기존의 스킴은 해쉬 기반으로 제안 되었으나 이 논문에서 제안한 스킴은 페어링 (pairing) 연산을 기반으로 제안 되었다. 또한, Computational Diffie-Hellman 문제를 기반으로 스킴을 제안하여 안전성에 대한 증명이 가능하다. 최근에 스마트카드를 사용한 인증에서 요구 되는 성질의 모든 조건을 만족한다는 장점을 가지고 있다.

1. 서론

최근에 제안되고 있는 원격 서버에 로그인하기 위한 방법은 ID와 패스워드 뿐만 아니라 스마트카드를 함께 사용한다. 과거 원격 서버에 로그인하기 위해 ID와 패스워드를 입력하여 원격 서버에게 사용자 인증을 받았다. 하지만, ID는 일반적으로 공개된 정보로 생각할 수 있으며 패스워드 또한, 우리가 추측 가능한 값을 사용하므로 단순히 ID와 패스워드만으로 사용자를 인증하는 것에는 문제가 있다. 뿐만 아니라 컨텐츠 제공자의 입장에서 볼 때 ID와 패스워드만으로 로그인하는 경우 동시에 여러 사람이 동일한 ID 와 패스워드를 사용하여 컨텐츠를 이용할 수 있다는 것이다. 그러나 로그인할 때, ID, 패스워드 그리고 스마트카드를 이용하여 사용자 인증을 하면 동시에 여러 명이 같은 ID와 패스워드로 로그인할 수 없다. 뿐만 아니라, 원격 서버에 로그인하기 위해 스마트카드를 이용하는 방법은 최근에 사용되는 모바일 환경에서도 적용이 가능하다. 핸드폰에 스마트 칩을 탑재하여 자유롭게 사용자의 인증과 키 교환을 할 수 있으므로 안전한 모바일 서비스를 제공 받을 수 있다.

스마트카드를 사용하여 원격 서버에 사용자 인증을 받는 경우 원격 서버는 검증 테이블 (verification table)을 서버에 저장하지 않고 사용자를 인증할 수 있다는 장점이 있다. 이것은 서버의 데이터 저장량을 줄이고 서버는 자신의 개인키만을 안전하게 관리하면 되기 때문에 서버의 보안 수준을 낮출 수 있다. 만약 서버에 검증 테이블 (verification table)을 저장한다면 서버의 데이터가 공격자에게 노출되는 경우 모든 사용자에 대한 위장공격이 가능하다. 이러한 사용자 위장 공격을 막기 위해 Hwang 과 Li [1]는 패스워드 테이블 (password table)을 사용하지 않는 스킴을 제안하였다. 그러나 Hwang 과 Li [1]의 스킴은 Chan 과 Cheng [2]에 의해 위조가 가능하다는 사실이 알려졌다. 또한 Hwang 과 Li [1]의 스킴에서는 스마트카드에 인증정보를 등록 할 때 단지 사용자의 ID를 서버에 등록하면 스마트카드에 ID와 원격서버가 선택한 패스워드를 저장하기 때문에 사용자 입장에서 패스워드를 기억하기 어렵다. 그러므로 사용자의 편의를 생각할 때 기억하기 쉬운 패스워드를 사용하기 위해선 등록 시 사용자는 자신의 ID와 사용자가 선택한 패스워드를 사용하는 것이 효율적이라고 본다. 물론 기억하기 쉬운 패스워드란 누구든지 추측이 가능하다. 그러므로 패스워드 기반의 키 교환은 항상 사전 공격의 가능성을 배제 할 수 없다. 그래서 최근 스마트카드를 사용한 인증에서는 서버가 스마트카드에 저장한 값에서 패스워드 정보를 제거하여 서버와 통신을 한다. 이를 통해 패스워드가 외부에 유출되더라도 스마트카드를 소유하지 않고서는 서버의 심어준 값을 공격자는 알 수 없으므로 패스워드에 대한 사전공격에 안전하다.

기존의 스마트카드를 사용한 사용자 인증은 스마트카드의 연산능력의 한계성으로 인해 단순히 연산량이 작은 해쉬 함수를 사용하여 스킴을 구성하였다. 그러나 2006년 Manik Lal Das [3]의 "A novel remote user authentication scheme using bilinear pairings"에 의해 처음으로 페어링 (pairing)기반의 연구가 시작되었다. 그러나 이 논문에서 제안한 스킴은 chou 와 그 외 [4]에 의해 가장공격이 가능하다고 증명되었으면 chou 와 그 외 [4]는 개선된 스킴을 제안하였으나 Thulasi Goriparthi 와 그 외 [5]에서 Manik의 스킴과 같이 가장 공격이 가능하다고 알려졌다. 이후 Fang 과 Huang [6]에 의해 Thulasi

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-(C1090-0603-0025)).

Goriparthi 와 그 외 [5]의 스킴의 문제가 제기되었으며 새로운 스킴을 제안하였다. 하지만 최근 Fang의 스킴도 Debasis Giri [7]에 의해 깨졌다. 그러나 Debasis [6]의 스킴은 스마트카드의 등록 값에 패스워드 정보와 서버와의 통신에 사용되는 값을 분리하여 저장하므로 스마트카드를 훔친 공격자는 패스워드를 추측하여 스마트카드와 사용자간의 인증을 한 후 서버와 통신을 하게 되므로 패스워드 추측공격이 가능하다. 그러므로 스마트카드를 통한 안전한 인증을 하기 위해서는 패스워드 정보와 서버의 비밀정보가 함께 하나의 값으로 스마트카드에 저장되어야 한다고 하겠다. 또한 Debasis [6]의 스킴은 타임스탬프(time-stamp)를 사용하므로 시간에 대한 동기를 맞춰야 한다는 약점이 있으며 서버가 사용자만을 인증하는 단방향 인증프로토콜이므로 중간의 공격자에 의해 서버 가장 공격이 가능하다. 그러므로 지향해야 할 프로토콜은 양방향 인증 프로토콜이라 하겠다. 또한 양방향 인증만으로는 안전한 통신이 가능한가에 대해서도 생각해보아야 할 주제라 하겠다. 인증 후 사용자와 서버가 키를 교환하는 경우 중간에 공격자가 인증 후 서버를 가장하거나 사용자를 가장하는 경우 사용자나 서버 모두 공격자와의 키 교환이 이뤄진다. 그러므로 안전한 통신을 위해서는 키 교환이 인증과 함께 이뤄져야 한다.

이 논문의 공헌은 기존의 스마트카드를 사용한 원격서버 인증의 경우 인증만을 주안점으로 삼았으나 이 논문에서는 스마트카드를 이용하여 상호인증과 키 교환을 동시에 하므로 인증과 키 교환을 분리할 때 보다 통신 량도 줄이고 또한 중간자 공격도 막는 프로토콜을 제안한다. 또한 제안한 스킴에서는 난수를 사용하므로 시간에 대한 동기를 맞출 필요가 없으며 서버에서는 페어링 (pairing) 연산을 하지만 스마트카드는 단순 곱셈 연산만을 하므로 스마트카드에서 사용가능하며 안전성에 대한 증명이 된다는 장점을 가지고 있다. 또한 검증 테이블(verification table)이 필요하지 않으며 기존의 페어링 (pairing) 연산을 사용하여 사용자 인증을 하는 스킴 [3,4,5,6,7]은 모두 타임 스탬프(time-stamp)를 사용하였지만 이 논문에서는 처음으로 난수를 사용하여 안전한 인증과 키 교환 스킴을 설계하였다. 그리고 패스워드의 변경이 원격서버의 도움 없이 사용자와 스마트카드사이의 연산을 통하여 변경이 가능하다.

이 논문은 다음과 같이 구성되었다. 2단원에서는 수학적 배경에 대해 알아본다. 3단원은 스킴을 제안하고 4단원은 스킴의 안전성에 대해 논의한다. 5단원에는 논문의 결론을 내린다.

2. 수학적 배경

이 단원은 수학적 배경에 대해 알아본다. 이 논문에서 사용되는 수학 이론은 Bilinear Pairing 과 Computation Diffie-Hellman 문제 이다.

(1) Bilinear Pairing : G_1은 generator P에 의해 구성되는 additive cyclic group으로 order 가 p이다. 그리고 G_2는 G_1과 같은 order를 갖는 multiplicative cyclic group이다. Bilinear Pairing 함수 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 는 다음과 같은 성질을 가진다.

1. $Bilinear: \hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$
   for all $P,Q \in G_1$ and for all $a,b \in Z_p^*$
2. $Non-degenerate: \hat{e}(P,Q) \neq 1$ for any $P,Q \in G_1$
3. $Computable: \hat{e}(P,Q)$ for all $P,Q \in G_1$를 효율적으로 계산하는 알고리즘이 존재한다.

(2) Computational Diffie-Hellman Problem (CDH): G_1 은 order가 p인 additive cyclic group이다. random 하게 주어진 $P \in G_1$ 에 대해서 $a,b \in Z_q^*$를 모르고, aP, bP 가 주어질 때, abP 를 계산한다.

이 논문에서는 CDH 문제가 어렵다는 가정 하에 스킴을 제안하였다.

3. 제안하는 스킴

이 단원에서 스마트카드를 사용한 인증된 키 교환 스킴을 제안한다. 이 스킴은 5개의 단계로 구성되어진다.:설정. 등록, 로그인, 인증과 키 교환, 패스워드 변경단계.

설정 단계: 이 단계는 원격 서버에서 진행된다. 원격 서버는 두개의 그룹 (groups), G_1, G_2를 선택한다. G_1은 크기 (order) 가 p 인 덧셈 순환 그룹 (additive cyclic group)이고 G_2은 크기 (order)가 q인 곱셈 순환 그룹 (multiplicative cyclic group)이다. 원격 서버는 Bilinear 함수 $\hat{e}$를 정의 한다. Bilinear 함수 $\hat{e}$는 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 이며, P는 G_1의 생성자 (generator)이다. 원격 서버는 난수 s 를 비밀 값으로 선택하고 공개키로 sP 를 선택한다. 또한, 해쉬 함수 H, H_1를 $H, H_1: \{0,1\}^* \rightarrow G_1$ 으로 정의 한다. 원격 서버는 시스템 파라미터로 $< G_1, G_2, p, q, P, Pub(s) = sP, H, H_1 >$ 를 정의하고 s 는 자신의 개인키로 선택한다.

등록 단계: 사용자는 원격 서버에게 자신의 ID와 패스워드를 비밀채널 (secure channel)을 통해 전달한다. 원격 서버는 사용자로부터 받은 ID와 패스워드를 이용하여 다음과 같이 $Reg(ID)$를 계산한다.

$$Reg(ID) = sH(ID) + H(PW)$$
$$A(ID) = \hat{e}(sH(ID), P).$$

원격 서버는 $< ID, Reg(ID), A(ID), sP, H, H_1 >$를 스마트카드에 저장하여 비밀 채널 (secure channel)을 통해 사용자에게 전달한다.

로그인 단계: 사용자는 스마트카드를 스마트카드 리더기에 넣는다. 이후 언급하는 스마트카드는 리더기를 포함해서 사용한다. 사용자는 자신의 ID와 패스워드를 스마트카드에 입력한다. 스마트카드는 입력된 값을 가지고 다음과 같은 방법으로 계산한다.

1. 스마트카드는 난수 r_1 을 선택한다.
2. 스마트카드에 저장된 값 $Reg(ID)$ 에서 패스워드 정보를 삭제한 후, $sH(ID)$ 를 계산한다: $Reg(ID) - H(PW) = sH(ID)$.
3. 스마트카드는 $B = r_1 P + sH(ID)$를 계산하여 원격 서버에게 $< ID, B >$ 를 보낸다.

인증과 키 교환 단계: 원격 서버는 스마트카드로부터 받은 정보를 통해 스마트카드를 인증하며 또한 동시에 키 교환을 한다.

1. 원격 서버는 스마트카드로부터 받은 값 B와 자신의 비밀 값 s를 사용하여 다음 값을 계산 한다: $r_1 P = B - sH(ID)$.
2. 원격 서버는 난수 r_2 를 선택한다.
3. 원격 서버는 다음 과정을 통해 C와 D를 계산한다.

$C = \hat{e}(sH(ID), r_1P)$

$D = r_1sP + r_2P.$

4. 원격 서버는C와 D를 스마트카드에게 전송한다.

5. 스마트카드는 $A(ID)^{r_1}$와 C가 같은지 체크한다. 만약 C와 다르다면 스마트카드는 원격 서버에 로그인을 취소한다.

6. 위의 (5)번 조건을 만족한다면 스마트카드는 $r_2P = D - r_1sP$를 계산하고, $K = H_1(ID||r_1r_2P||r_1P||r_2P)$를 계산하고 K를 사용하여 r_2P를 암호한 $E_K(r_2P)$를 원격 서버에게 전송한다.

7. 원격 서버는 K를 계산하여 $E_K(r_2P)$를 복호화 하여 r_2P를 확인한다. 만약 유효하지 않다면 원격 서버는 사용자의 로그인을 취소한다.

패스워드 변경 단계 : 사용자는 원격 서버의 도움 없이 패스워드를 변경할 수 있다.

1. 사용자는 ID, 기존의 패스워드(PW)를 변경하고자 하는 패스워드(PW')를 스마트카드에 입력한다.

2. 스마트카드는 $H(Pw')$를 계산한다.

3. 스마트카드는 $Reg_{ID}' = Reg_{ID} - H(Pw) + H(Pw')$를 새로운 등록 값으로 갱신한다.

4. 안전성

이 단원에서는 제안한 스킴에 대한 안전성에 대해 논의하고자 한다. 제안한 스킴은 다음의 공격에 안전하다.

1. 재생 (Replay) 공격: 제안된 스킴에서는 스마트카드가 원격 서버에게 인증 받기 위해 난수 r_1를 사용하여 메시지 B를 보낸다. 공격자가 그 메시지를 보고 나중에 원격 서버에게 B를 보낼지라도 매번 원격서버는 다른 r_2를 선택하므로 공격자는 원격서버에게 정당한 답을 보낼 수 없다. 그러므로 제안된 스킴이 난수를 사용했음에도 불구하고 재생 (Replay)공격에 안전하다.

2. 메시지 위조 공격: 스마트카드는 변형 억제 (Tamper Resistance) 성질을 가지고 있으므로 공격자는 스마트카드의 정보를 읽을 수 없다. 그러므로 원격 서버에게 위조 공격을 하기 위해서는 공격자는 사용자의 스마트카드뿐만 아니라 패스워드와 ID 모두를 알고 있거나 원격서버의 비밀 값 s 을 알고 있어야 한다. 이는 정당한 사용자나 원격 서버만이 가능하므로 공격자는 위조공격을 할 수 없다.

3. 세션키 안전성: 사용자와 원격 서버가 세션키를 생성하는데 각각 r_1, r_2를 선택하고 원격 서버의 비밀 값 s 을 이용하여 r_1P, r_2P를 교환하므로 원격 서버의 비밀 값을 모르는 공격자는 세션키를 알 수 없다. 그러므로 원격 서버와 사용자외에는 세션키를 얻을 수 없으므로 세션키의 안전성을 보장한다.

4. Known-Key 안전성: 세션키가 노출되더라도 세션키를 생성하는데 매번 다른 난수 r_1, r_2를 선택하므로 공격자는 노출된 세션키로 사용된 세션키를 알 수 없다.

5. Forward Secrecy: 원격서버의 비밀값 s 이 노출되면 공격자는 r_1P, r_2P는 알 수 있지만 r_1r_2P는 위의 스킴이 CDH 문제의 안전성에 기반 하므로 공격자는 r_1r_2P를 계산할 수 없으므로 전에 사용된 세션키를 공격자가 알 수 없다. 그러므로 Forward Secrecy를 만족한다.

5. 결론

본 논문에서는 스마트카드를 사용하여 원격서버에 사용자의 인증과 동시에 안전한 키 교환을 제안하였다. 기존의 논문에서 사용하던 해쉬 함수를 사용하는 대신 페어링 (Pairing)연산을 사용하였으며 타임스탬프 (time stamp)대신 난수를 사용하였으나 재생 (replay) 공격에 안전하며, 뿐만 아니라 인증과 동시에 키 교환을 함께 하므로 중간자 공격에도 안전하다. 또한 검증 테이블 (verification table)을 사용하지 않으면서 패스워드의 변경이 원격서버의 도움 없이 자유롭게 이뤄진다. 제안한 스킴의 안전성은 CDH문제의 어려움에 기반을 두고 있다.

참고문헌

[1] M. S. Hwang and L. H. Li: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 46(2000) 28-30

[2] C. K. Chan and L. M. Cheng: Cryptanalysis of a remote user authentication using smart cards. IEEE Transactions on Consumer Electronics 46(2000)

[3] Manik.L.Da, Ashtosh Saxena, V.P.Gulati, D.B.Phatak: A novel remote user authentication scheme using binear pairings. computers & Security(in press), 2005

[4] J.S.chou, Y.Chen, j.Y.Lin: Improvement of manik et al.'s remote user authentication scheme. http://eprint.iacr.org/2005/450.pdf

[5] Thulasi Goriparthi, manik Lal Das, Atul Negi and Ashutosh Saxena: Cryptanalysis of recently proposed remote user Authentication Schemes.

[6] Guanfei Fang and Genxun Huang: Improvement of recently proposed remote user authentication schemes. http://eprint.iacr.org/2006/200.pdf

[7] Debasis Giri and P.D.Srivastava: An Improved Remote User Authentication Scheme with Smart Cards using Bilinear Pairings. http://eprint.iacr.org/2006/274.pdf

[8] D. Boneh and M. Franklin: Identity-based Encryption from the Weil pairing. Crypto 2001, Springer-Verlag, LNCS vol. 2139, 213-229 2001

[9] Wen-Shenq Jaung: Efficient Three-Party key exchange using smart cards. IEEE Transactions on Consumer Electronics 50, 619-624 (2004)

[10] Chun-I Fan, Yung-Cheng Chan and Zhi-Kai Zhang: Robust remote authentication scheme with smart cards. Elservier Computers & Security (2005) 24, 619-628

[11] Jun-Cheol Jeon, Byung-Heon Kang, Se-Min Kim, Wan-Soo Lee and Kee-Young Yoo: An Improvement of Remote User Authentication S초듣 Using Smart Cards. MSN 2006 LNCS 4325, 416-423, 2006