情報保護學會論文誌
第17卷 第2號, 2007. 4

익명성을 제공하는 스마트카드 사용자 인증 프로토콜

김 세 일,† 이 현 숙, 이 동 훈‡
고려대학교 정보경영공학전문대학원

Anonymous Remote User Authentication Scheme with Smart Card

Seil Kim,† Hyun Sook Rhee, Dong Hoon Lee‡
Graduate School of Information Management and Security, Korea University

요 약

인터넷의 급성장과 정보화 시대가 도래함에 따라 개인정보보호에 대한 중요성이 증대되고 있다. 이러한 개인정보보호와 프라이버시의 요구에 발맞춰서 개인정보보호를 위한 여러 기술들이 제안되어 지고 있다. 스마트카드를 이용한 인증 시스템에 대한 연구에서도 개인정보보호를 위한 일환으로 사용자 익명성 제공에 관심이 높아지고 있다. 2004년 Das et al.는 동적 아이디를 사용함으로서 처음으로 사용자의 익명성을 제공한 인증 프로토콜을 제안하였다. 그러나 로그인 단계에서 서버에게 보내는 데이터를 통해 사용자를 구분할 수 있게 됨으로써 사용자 익명성을 제공하지 못했다. 2005년 Chien et al.은 사용자 익명성을 제공하는 인증 프로토콜을 제안하였지만 제3자에게만 안전한 사용자 익명성을 제공하였다. 본 논문은 스마트카드를 이용하여 사용자와 서버간의 상호 인증을 만족하며 사용자 프라이버시를 위해 제3자뿐만 아니라 원격서버에게도 안전한 익명성을 제공하는 효율적인 사용자 인증 시스템을 제안한다.

ABSTRACT

Due to the increasing use of Internet and spread of ubiquitous environment, the security of private information became an important issue. For this reason, many suggestions have been made in order to protect the privacy of users. In the study of authentication system using a smart card which is one of the methods for protecting private information, the main idea is to offer user anonymity. In 2004, Das et al. suggested an authentication system that guarantees anonymity by using a dynamic ID for the first time. However, this scheme couldn't guarantee complete anonymity as the identity of the user became revealed at log-in phase. In 2005, Chien at al. suggested a authentication system that guarantees anonymity, but this was only safe to the outsider(attacker). In this paper, we propose a scheme that enables the mutual authentication between the user and the server by using a smart card. For the protection of the user privacy, we suggest an efficient user authentication system that guarantees perfect anonymity to both the outsider and remote server.

Keywords : *Privacy, Smart Card, Anonymity, Mutual Authentication*

I. 서 론

최근, 컴퓨터 네트워크 사용의 증가로 인해 많은 사람들이 분산된 컴퓨터 환경에서 원격 서버에 접속하는 일이 빈번해 지고 있다. 그러나 믿을 만한 보호시스템 없이 안전하지 않은 채널을 통하는 데이터는 도청이나

접수일: 2007년 1월 15일; 채택일: 2007년 2월 28일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터지원사업의 연구결과로 수행되었음 (IITA-2006-(C1090-0603-0025))
† 주저자, sell82@korea.ac.kr
‡ 교신저자, donglee@korea.ac.kr

불법적인 수정, 의도된 변경 등과 같은 문제점에 노출되어 있다. 이러한 악의적인 공격들을 막기 위해 다양한 암호화 기술들이 제안되고 있다. 이러한 스마트카드를 이용한 인증프로토콜들은 스마트카드가 temper-resistant한 성질을 갖는다는 가정 하에 활발히 연구되어지고 있다[1-14]. 초기 스마트카드를 이용한 원격 사용자 인증 프로토콜을 살펴보면, 서버는 사용자 인증 요청에 대한 검증을 위해 검증 테이블(verification table)을 저장하고 있어야 했다[11]. 하지만 서버에 대한 높은 안전성이 요구되고 저장 공간과 사용자에 대한 패스워드 정보의 관리를 요구하는 측면에서 기존의 패스워드 기반 연구들과 상이하지 않은 특성을 갖고 있었다. 하지만 이후, 스마트카드를 이용한 논문들은 계속적으로 많은 연구가 진행되어지면서 서버 측면에서 사용자에게 패스워드 정보를 제공하지 않고 사용자가 직접 패스워드를 선택하여 서버에 등록하는 형태로 진행되어져 왔으며[1-7,9,10,12-14] 또 사용자가 직접 스마트카드만을 이용하여 패스워드를 변경할 수 있는 형태로까지 발전되어져 왔다[8]. 2000년에는 Hwang et al.[10]은 ElGamal's Cryptosystem을 기반으로 한 새로운 개념의 원격 사용자 인증 프로토콜을 제안하였다. 그러나 이 프로토콜은 악의적인 공격자에 의해 정당한 ID와 패스워드 쌍을 쉽게 만듦으로서 가장공격이 가능하다[2]. 2002년 Chien et al.[5]은 Sun et al.[13]의 인증 프로토콜을 효율적인 상호 인증 프로토콜로 발전 시켰다. 그러나 Chien et al.의 프로토콜은 악의적인 공격자가 도청을 통해서 사용자의 패스워드 없이 정당한 사용자인척 가장하는 것이 가능하다는 사실을 Hsu[9]가 지적하였다. 또한 Liu et al.[12]는 사용자 가장 공격에 안전한 상호인증 프로토콜을 제안하였다. 그러나 Liu et al.의 프로토콜은 상호인증 성질을 만족하지 못한다.

최근 유비쿼터스 환경에서는 개인 정보보호와 프라이버시에 많은 관심을 갖고 있다. 이로 인해 스마트카드를 이용한 원격 인증 시스템에서도 개인정보보호를 위한 일환으로 사용자 익명성을 제공하는 인증 시스템에 대한 연구가 시작되었다[3,7]. 하지만 기존의 익명성을 제공하는 스마트카드를 이용한 인증에 대한 연구들은 다음과 같은 문제점을 갖는다. (1) 2004년 Das et al.[7]는 동적 아이디를 사용함으로써 처음으로 사용자의 익명성을 제공한 인증 프로토콜을 제안하였다. 그러나 로그인 단계에서 서버에게 보내는 데이터를 통해 사용자를 구분할 수 있고 그로인해 사용자 익명성을 제공하지 못한다. (2) 2005년 Chien et al.[3]은 사용자 익명성을 제공하는 인증 프로토콜을 제안하였지만 사실 제3자에게만 안전한 사용자 익명성을 제공하였다.

우선 제3자와 서버에 대하여 사용자 익명성을 제공하는 Das et al.[7]프로토콜에 대한 문제점을 살펴 볼 것이다. 이런 분석을 통해서 본 논문에서는 tamper-resistant한 성질을 갖는 스마트카드를 이용하여 등록 단계에서 고정된 사용자의 아이디를 사용하는 대신에 동적으로 아이디를 생성하여 사용한다. 이 동적 아이디는 사용자의 로그인 요청 때마다 아이디를 변화시킴으로서 제 3자와 서버에 대한 사용자 익명성을 제공한다. 또한 사용자와 서버간의 안전한 상호 인증프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 3장에서 Das et al.의 프로토콜을 분석한다. 4장에서는 새로운 프로토콜을 제안한다. 다음으로 5장에서 제안된 프로토콜의 안전성과 효율성을 분석한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. Notation

이번 장에서는 앞으로 프로토콜에서 사용될 용어에 대한 정의이다.

- C_{ID} : 사용자의 동적 ID
- r, e : 스마트카드가 생성한 랜덤 값
- x_s, y : 서버의 비밀 키
- $h()$: Full domain Hash Function
- T : 타임 스탬프(Time stamp)

Ⅲ. Das et al. 프로토콜

이번 장에서는 Das et al.[7]의 프로토콜에 대한 특성과 구성을 알아본다.

3.1 Das et al.의 프로토콜

Das et al.의 프로토콜에서 사용자의 익명성이 만족되지 않는 것을 중점으로 살펴볼 것이다. 이 프로토콜은 등록 단계, 로그인 단계, 검증 단계로 구성되어 있다.

<등록 단계>

1. 등록단계에서 새로운 사용자 U_i는 자신의 PW_i를 안전한 채널을 통해 서버 S에게 제출한다.
2. S는 N_i를 계산 하고 U_i의 스마트카드에 $h(),N_i,y$

를 저장한다.

$N_i = h(PW_i) \oplus h(x_s)$

<로그인 단계>

로그인 단계에서 U_i가 원격 서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입한다. 스마트카드는 다음 과정을 수행한다.

1. $C_{ID_i} = h(PW_i) \oplus h(N_i \oplus y \oplus T)$
2. $B_i = h(C_{ID_i} \oplus h(PW_i))$
3. $C_i = h(N_i \oplus B_i \oplus y \oplus T)$
4. 스마트카드는 $\{C_{ID_i}, N_i, C_i, T\}$를 S에게 보낸다.

<검증 단계>

S는 데이터 $\{C_{ID_i}, N_i, C_i, T\}$를 T'시간에 받고 다음과 같은 수행을 한다.

1. T와 T' 사이의 시간 간격(time interval)을 확인한다.
2. $h(PW_i) = C_{ID_i} \oplus h(N_i \oplus y \oplus T)$를 계산한다.
3. $B_i = h(C_{ID_i} \oplus h(PW_i))$를 계산한다.
4. 다음 식이 성립하는지 확인한다. 만약 식이 일치하면 요청을 받아들인다.

$C_i = h(N_i \oplus B_i \oplus y \oplus T)$

3.2 Das et al.의 프로토콜 분석

Das와 Saxena, Gulati[7]는 동적 아이디를 사용함으로써 처음으로 사용자의 익명성을 제공한 인증 프로토콜을 제안하였다. 그러나 Chien 과 Chen[3]은 사용자 U_i가 데이터$\{C_{ID_i}, N_i, C_i, T\}$를 서버에게 보낼 때, $N_i = h(PW_i) \oplus h(x_s)$는 고정된 값으로 등록단계에서의 정보를 이용하여 사용자를 추적하는 것이 가능하다는 것을 지적하였다. 즉, 로그인 단계에서 서버에게 보내는 데이터를 통해 사용자를 구분할 수 있게 됨으로써 사용자 익명성을 제공하지 못한다. 또한 이 프로토콜은 사용자 인증만을 제공한다.

Ⅳ. 제안된 프로토콜

본 논문에서는 사용자와 서버간의 상호 인증 프로토콜을 제안한다. 이때, 사용자 프라이버시를 위해 제3자뿐만 아니라 원격 서버에대해서도 안전한 익명성을 제공하는 효율적인 다음의 인증 시스템을 제안한다.

4.1 제안된 프로토콜

본 프로토콜은 다음의 등록 단계, 로그인 단계, 인증 단계인 3단계로 구성되어 있다.

<등록 단계>

1. 등록단계에서는 새로운 사용자 U_i가 안전한 채널을 통해 서버 S에게 자신의 ID_i와 PW_i를 제출한다.
2. S는 다음과 같은 계산을 수행한다.
   (1) $R_i = h(ID_i \oplus x_s) \oplus h(x_s)$
   (2) $I = h(ID_i \oplus x_s) \oplus PW_i$
   (3) $I_c = h(ID_i \oplus x_s)$
3. S는 U_i의 스마트카드에 $I, R_i, h(), I_c$ 그리고 y를 저장하여 발급한다.

<로그인 단계>

1. U_i는 자신의 스마트카드를 리더기에 삽입하고 자신의 PW_i를 입력한다.
2. 다음은 스마트카드가 다음과 같은 수행을 한다.
   (1) $I \oplus PW_i = I_c$를 체크하고 일치하는 경우 다음 단계로 넘어간다.
   (2) $C_i = R_i \oplus I \oplus PW_i \oplus h(PW_i \oplus r)$
   $= h(x_s) \oplus h(PW_i \oplus r)$
   (3) $C_{ID} = h(C_i \oplus h(y \oplus T))$
   (4) $M = h(e \oplus T)$
   (5) $V = h(M \oplus y) \oplus h(PW_i \oplus r)$
3. 인증을 위해 S에게 메시지 $\{T, C_{ID}, M, V\}$을 보낸다.

<검증 단계>

1. S는 메시지 $\{T, C_{ID}, M, V\}$를 T'시간에 받는다.
2. S는 다음과 같은 수행을 한다.
   (1) T와 T'사이의 시간 간격(time interval)을 확인한다.

〔표 1〕 기능 분석

프로토콜	상호 인증	익명성*		패스워드‡
		제3자	서버	
Our scheme	o	o	o	o
Das et al.[7]	x	x	x	o
Chien et al.[3]	o	o	x	o
Liu et al.[11]	x	x	x	o

· 패스워드‡ : 사용자가 자유롭게 선택가능 여부
· 익명성* : 제3자와 서버에게 익명성 제공 여부

〔표 2〕 효율성 분석

프로토콜	로그인 단계	인증 단계
Our scheme	5H	4H
Das et al.[7]	5H	3H
Chien et al.[3]	1E+1H+1S	2H+3S+3E
Liu et al.[11]	3H	4H

·H : 해쉬 함수 ·S : 암호화 ·E : 지수 계산

(2) S는 다음 계산을 통해 C_i 값을 얻어 낸다.

i) $V \oplus h(M \oplus y) = h(PW_i \oplus r)$

ii) $C_i = h(PW_i \oplus r) \oplus h(x_s)$

(3) 다음 식이 성립하는지 확인 한다.

$C_{ID} = h(C_i \oplus h(y \oplus T))$

(4) 만약 C_{ID} 와 식이 일치 하면 S는 메시지 M_s를 계산하여 U_i에게 보낸다.

$M_s = h(h(PW_i \oplus r) \oplus M) \oplus y$

(5) U_i는 메시지 M_s를 받고 다음 식을 확인해서 일치 하는지 확인한다.

$M_s \oplus y = h(h(PW_i \oplus r) \oplus M)$

V. 분석

이 장에서는 제안된 프로토콜의 안전성과 효율성을 분석한다.

• **Stolen-verifier attack** : 제안된 프로토콜은 검증 테이블을 필요로 하지 않기 때문에 서버로부터 검증 할 수 있는 정보를 어느 누구도 얻어 낼 수 없다. 그러므로 제안된 프로토콜은 Stolen-verifier attack에 대해서 안전 할 수 있다.

• **Replay attack(재사용공격)** : 제안된 프로토콜에서는 인증단계에서 타임스탬프(time stamp) T를 사용하여 시간 간격을 확인한다. 또한 M과 V값을 생성할 때 스마트카드에 의해 생성된 랜덤 값이 사용된다. 이 값은 매번 사용할 때 마다 바뀐다. 따라서 제안된 프로토콜에서는 재사용 공격에 안전하다.

• **Offline Guessing attack(오프라인 추측 공격)** : 사용자와 서버와의 통신에서 패스워드 값이 직접 보내지지 않는다. 따라서 공격자는 통신채널을 통해서 패스워드를 얻을 수 없다. 또한 C_{ID}, V 값에 스마트카드가 생성한 랜덤 값이 포함되기 때문에 공격자는 사용자의 패스워드를 접근 할 수 없다.

• **Impersonation attack(가장 공격)** : 공격자가 정당한 로그인 정보를 위조하기 위해서는 V값 안에 포함된 $h(PW_i \oplus r)$와 서버의 비밀 값 y를 알아야만 한다. 또한 공격자는 $\{T, C_{ID}, M, V\}$을 저장해 두고 재사용하여 사용자인척 하려고 해도 y값을 모르기 때문에 $h(y \oplus T)$를 생성할 수 없다. 따라서 제안된 프로토콜에서는 가장 공격에 안전하다.

VI. 결 론

본 논문에서 Das와 Saxena, Gulati[7]가 제안한 프로토콜이 제3자와 서버에 대하여 사용자 익명성이 제공되지 않는 것을 살펴보았다. 제안한 프로토콜은 tamper-resistant한 성질을 갖는 스마트카드를 이용하여 등록 단계에서 고정된 사용자의 아이디를 사용하는 대신에 동적으로 아이디를 생성하여 사용한다. 이 동적 아이디는 사용자의 로그인 요청 때마다 아이디를 변화시킴으로서 제 3자와 서버에 대한 사용자 익명성을 제공하며 다음과 같은 장점을 갖는다. 1. 정당한 사용자는 아이디를 매번 동적으로 생성함으로서 서버와 제3자에게로부터 안전한 사용자 익명성을 제공한다. 2. 사용자와 서버간의 상호인증을 제공한다. 3. 일반적인 패스워드를 이용한 프로토콜과 다르게 서버는 검증 테이블 또는 패스워드 테이블을 저장할 필요가 없기 때문에 사용자의 프라이버시가 향상된다. 4. 해시 함수와 X-OR연산만을 사용함으로써 연산량 측면에서 효율적이다. 5. 등록 단계에서 사용자는 자신의 패스워드를 자유롭게 선택함으로서 사용자의 편리성을 증대 시켰다. 6. 재사용 공격과 가장 공격, 오프라인 추측 공격에 안전하다. 향후에는 인증을 통과한 사용자가 누구인지를 알고 싶을 때 서버가 사용자를 추적 가능한 인증프로토콜에 대한 연구가 요구되어진다.

참고문헌

〔1〕 A.K. Awasthi and S. Lal, A remote user authentication scheme using smart cards with forward secrecy, IEEE Trans. Consumer Electronics, Vol. 49, pp. 1246-1248, 2003.

〔2〕 C.K. Chan and L.M. Cheng, Cryptoanalysis of a remote user authentication scheme using

smart cards, IEEE Trans. Consumer Electronics, Vol. 46. pp. 992-993, 2000.

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

[4] C.C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatics Vol. 14 (3), pp. 289-294, 2003.

[5] H.Y. Chien, J.K. Jan and Y.M. Tseng, An efficient and practical solution to remote authentication : smart card, Computers & Security, Vol. 21 (4), pp. 372-375, 2002.

[6] C.C Chang and T.C Wu, A password authentication scheme without verification tables: Proc. 8th IASTED Int. Symp. Applied Informatics, Innsbruck, Austria. pp. 425-429, 1990.

[7] 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.

[8] C. I. Fan, Y. C. Chan, Z. K. Zhang, Robust remote authentication scheme with smart cards, Computers and Security Vol. 24, pp.619-628, 2005.

[9] C.L. Hsu, Security of two remote user authentication schemes using smart cards, IEEE Trans. Consumer Electronics, Vol. 49, pp. 1196-1198, 2003.

[10] M.S. Hwang, and L.H. Li, A new remote user authentication scheme using smart cards, IEEE Trans. On Consumer Electronics, Vol. 46, No.1, pp. 28-30, 2000.

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

[12] J. Liu, J. Sun, T. Li, An Enhanced Remote Login Authentication with Smart Card, IEEE SIPS 2005 workshop on signal processing systems, Athens, Greece, 2005.

[13] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Trans. on Consumer Electronics, Vol. 46, No.4, pp.958-961, 2000.

[14] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consumer Electronics Vol. 49, No.2, pp. 414-416, 2003.

〈著者紹介〉

김 세 일 (Seil Kim) 학생회원
2005년 2월: 고려대학교 수학과 학사
2005년 3월~현재: 고려대학교 정보보호대학원 석사과정
<관심분야> 암호 프로토콜, 익명성 연구, PET 기술

이 현 숙 (Hyun Sook Rhee) 학생회원
1998년 2월: 단국대학교 수학과 학사
2000년 2월: 단국대학교 수학과 석사
2001년 3월~현재: 고려대학교 정보보호대학원 박사과정
<관심분야> 암호 프로토콜, 암호 이론, 익명성 연구, PET 기술

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사
1987년 12월: Oklahoma University 전산학 석사
1992년 5월: Oklahoma University 전산학 박사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보보호대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술