情報保護學會論文誌
第18卷 第5號, 2008. 10

추적이 가능한 스마트카드 사용자 인증 기법*

김 세 일†, 천 지 영, 이 동 훈‡
고려대학교 정보경영공학전문대학원

Anonymity User Authentication Scheme with Smart Cards preserving Traceability*

Seil Kim†, Ji Young Chun, Dong Hoon Lee‡
Graduate School of Information Management and Security, Korea University

요 약

최근 스마트카드를 이용한 원격 사용자 인증 기법은 개인 프라이버시 보호에 대한 관심 및 요구가 증가됨에 따라 사용자 익명성을 제공하려는 방향으로 활발히 진행되고 있다. 초기에 제안된 인증 기법에서는 사용자와 사용자가 서비스를 제공받고자 하는 서버를 제외한 제3자에 대한 사용자 익명성만을 고려하였으나 최근 서비스 제공자에 의한 개인정보유출 사고 등이 증가하면서 제3자뿐만 아니라 원격 서버에 대해서도 사용자의 익명성이 보장되는 기법이 요구되고 있다. 하지만 이러한 사용자 익명 인증 기법은 원격 서버가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적할 수 있는 기능 또한 필요하다. 따라서 본 논문에서는 제3자뿐만 아니라 원격 서버에 대해서도 사용자의 신원에 대한 익명성을 보장하며, 악의적인 사용자의 행동에 따른 문제 발생 시에 이를 추적 가능한 익명 인증 기법을 제안한다.

ABSTRACT

Recently, remote user authentication schemes using smart cards has been researched to provide user privacy because of increasing interest and demands. Previously, provided authentication schemes were only concerned about providing user privacy against outside attackers, but the scheme, which guarantees user privacy against both a remote server and outside attackers, has been recently demanded because the user's information has leaked out through the service providers. When the remote server perceives a user doing a malicious act, the server should be able to trace the malicious user by receiving help from a trust agency. In this paper, we suggest a scheme which not only guarantees user privacy against both a remote server and outside attackers, but also provides traceable anonymity authentication.

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

접수일 : 2008년 4월 7일; 수정일 : 2008년 7월 19일;
채택일 : 2008년 7월 26일
* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-(C1090-0801-0025))
† 주저자, sell82@korea.ac.kr
‡ 교신저자, donglee@korea.ac.kr

Ⅰ. 서 론

최근 컴퓨터 네트워크 사용의 증가로 인해 많은 사람들이 분산된 컴퓨팅 환경에서 원격 서버에 접속하는 일이 빈번해 지고 있다. 원격 서버에 접속하기 위해서는 사용자 인증 과정이 필요한데, 이러한 인증과정 중 사용

자와 원격 서버가 안전하지 않은 통신을 통해 주고받는 인증 데이터가 도청이나 불법적인 수정, 의도된 변경 등과 같은 문제점에 노출되어 ID 도용 등과 같은 사용자 프라이버시 침해 문제를 야기하고 있다. 이러한 문제를 해결하기 위해 안전한 인증 기법들에 대한 연구가 활발히 진행되고 있고, 그 중 스마트카드를 이용한 원격 사용자 인증은 스마트카드가 지닌 이동성과 기능적 보안 특성으로 인해 특히 주목 받고 있다.

초기 스마트카드를 이용한 원격 사용자 인증 기법에서는 서버가 사용자 인증 요청에 대한 검증을 위해 사용자 아이디와 패스워드를 서버에 검증 테이블(verification table) 형태로 저장하였다.[5] 하지만 이후 서버에 대한 전적인 신뢰의 요구와 사용자 아이디와 패스워드 관리를 위한 추가적인 비용부담 등을 해결하기 위해 검증 테이블 없이도 사용자 인증이 가능한 기법들이 연구되었다. 이러한 기법들은 서버 측면에서 사용자에게 패스워드를 제공하지 않고 사용자가 직접 패스워드를 선택하여 서버에 등록하는 형태로 연구가 진행되어 왔으며, 스마트카드만을 이용한 패스워드 변경이 가능하고 서버와 사용자간의 상호인증이 가능한 형태로까지 발전되어 왔다.

하지만 개인 프라이버시 보호에 대한 관심이 증가되면서 스마트카드를 이용한 원격 사용자 인증 시 사용자 익명성을 제공하려는 기법들이 제안되고 있다. 2004년 Das 등[3]은 고정된 아이디를 사용함으로써 원격 인증 시 사용자의 부분 개인정보가 유출되는 것을 막기 위해 동적 아이디(dynamic ID)를 사용하여 사용자와 원격 서버를 제외한 제3자에게 대해 익명성을 보장하는 기법을 제안하였다. 이 기법은 도청자에 대한 익명성이 보장되는 익명 통신(anonymous communication)을 제공하는 최초의 기법이다. 2005년 Chien 등[1]은 Das 등의 프로토콜이 실제로 익명 통신을 만족하지 않음을 보이고 익명 통신을 제공하면서 키 교환이 가능한 사용자 인증 프로토콜을 제안하였다. 하지만 2007년, 이 기법 역시 Hu 등[4]에 의해 가장 공격(impersonation attack)과 재생 공격(replay attack)에 취약함이 밝혀졌고 이를 개선하여 익명 통신에 안전한 기법이 제안되었다.

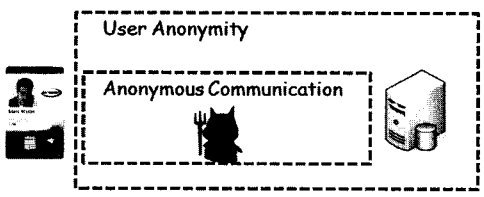
최근 기업 내부자의 고의나 실수로 인한 외부로의 정보 유출사고 등이 증가하면서 국가 및 기업 내분의 고객 개인정보 혹은 내부비밀의 외부 유출을 막기 위한 정보보호 기술의 개발이 요구되고 있다. 이러한 요구에 따라 2006년 Chai 등[2]이 원격 서버에 대해서도 사용자 익명성을 제공하는 스마트카드를 이용한 프로토콜을 처음으로 제안하였으나 원격 서버가 매번 한명의 사용자 인증을 위해 사용자 수만큼의 연산량과 통신량을 필요로 한다는 점에서 비효율적이다. 또한 이러한 익명 인증 기법은 필요시 사용자를 추적할 수 있는 기능이 필요한데, 원격 서버가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적하는 것이 가능해야 하지만 Chai 등이 제안한 기법은 추적할 수 있는 방법을 제공하지 못한다. 따라서 본 논문에서는 제3자뿐만 아니라 원격 서버에 대해서도 사용자의 신원에 대한 익명성을 보장하며, 악의적인 사용자의 행동에 따른 문제 발생 시에 이를 추적 가능한 익명 인증 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 배경지식을 통해 익명성과 추적성에 대해 정의하고 제안하는 기법이 사용되기에 적절한 환경을 살펴본다. 3장에서는 제안하는 기법에 사용될 용어에 대해 살펴본다. 4장에서 익명성과 연관된 기존의 기법과 문제점을 분석한다. 5장에서는 제안하는 기법에 대해 살펴본다. 6장에서 안전성과 효율성을 분석한 후 마지막 7장에 결론을 맺는다.

Ⅱ. 배경지식

2.1 익명성 정의

최근 개인 프라이버시 보호에 대한 관심 및 요구가 증가됨에 따라 사용자가 자신의 신원(identity)을 드러내지 않고 서비스나 리소스를 사용하는 것을 제공하는 방향으로 연구가 활발히 진행되고 있다. 익명성이란 어떤 행위를 한 사람의 신원(Identity)이 드러나지 않는 특성으로서, 통신채널 상에서 도청자로부터 정당한 사용자의 신원이 드러나지 않아야하는 익명 통신(anonymous communication)과 제3자뿐만 아니라 원격 서버에 대해서도 사용자의 신원이 보장되는 사용자 익명성(user anonymity)으로 정의된다.



〔그림 1〕 익명성 정의

2.2 추적성 정의

원격서버는 사용자의 신원을 신뢰기관을 통해 얻을 수 있다. 이때 악의적인 서버(compromised server)일 경우에도 정당한 사용자임을 알 수 없어야 한다.

서비스 제공자에 의한 개인정보유출사고 등이 증가하면서 제3자뿐만 아니라 원격 서버에 대해서도 익명성이 보장되는 기법이 요구되고 있다. 하지만 이러한 익명 인증 기법은 원격 서버가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 찾아낼 수 있어야 한다. 이때, 시스템 내의 각 사용자는 유일하게 식별되어야 하며 각 사용자는 자신의 행위에 대해서 책임을 지어야한다.

2.3 환경

초기의 인증 기법들을 살펴보면, 등록단계에서 사용자가 원격 서버에 자신의 아이디와 비밀번호를 제출하고 서버는 사용자의 아이디와 비밀번호를 데이터베이스에 저장함으로써 등록이 이루어졌다. 하지만 이러한 기법은 정당한 사용자의 개인 프라이버시를 만족하지 않는다. 예를 들어, 정당한 사용자가 콘텐츠를 다운받기 위해 로그인을 할 때, 사용자는 제 3자 뿐만 아니라 서버관리자에게 자신이 다운받는 콘텐츠에 대한 사용자가 자신임을 알리기 원하지 않을 것이다. 하지만 미디어 콘텐츠를 다운 받는 사용자가 등록되지 않는 다수의 사용자에게 콘텐츠를 불법으로 배포할 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적하는 것이 가능해야 한다. 이러한 환경에서처럼 제 3자뿐만 아니라 서버에 대해서도 사용자 익명성이 제공됨과 더불어, 신뢰기관의 협조를 얻어 악의적인 사용자를 추적할 수 있는 기법이 절실히 필요하다.

Ⅲ. Notation

이번 장에서는 앞으로 프로토콜에서 사용될 용어에 대한 정의이다.

- U_i : i번째 사용자
- S : 원격 서버
- C_{ID_i} : i번째 사용자의 동적 ID
- r, e : 매 세션 마다 스마트카드에 의해 생성된 랜덤 값
- x_s : 서버의 개인 키
- y : 서버의 비밀 값
- $h(.)$: Full domain Hash Function
- PTR : 신뢰기관의 공개키
- UIN_i : i번째 사용자의 개인 정보
- SK_{us} : 서버와 사용자 간의 세션 키
- CS : 신뢰기관에 제출되는 악의적인 사용자에 대한 Complain Sheet

Ⅳ. 기존 기법들

이번 장에서는 기존 기법들에 대한 특성과 구성을 알아본다.

4.1 Review of Das et al.

Das 등[3]은 고정된 아이디를 사용함으로써 원격 인증 시 사용자의 부분 개인정보가 유출되는 것을 막기 위해 동적 아이디(dynamic ID)를 사용하여 사용자와 원격 서버를 제외한 제3자에게 대해 익명성을 보장하는 기법을 제안하였다. 이번 장에서는 Das 등의 기법에서 사용자의 익명성이 만족되지 않는 것을 중점으로 살펴볼 것이다. 이 기법은 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, y를 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. $C'_{ID_i} = h(PW_i) \oplus h(N_i \oplus y \oplus T)$를 계산한다.
2. $B_i = h(C_{ID_i} \oplus h(PW_i))$를 계산한다.
3. $C_i = h(N_i \oplus B_i \oplus y \oplus T)$를 계산한다.
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 다음

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

4.1.1 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.

4.2 Review of Chien and Chen

Chien 등[1]은 원격 서버와 사용자간의 상호인증과 키 교환을 함에 있어서 안전한 사용자 익명 통신 기법을 제안하였다. 하지만 이 기법 역시 가장 공격과 재생 공격에 취약점이 존재한다. 그중에서 이 장에서는 Chien 등의 기법이 가장 공격에 안전하지 않음을 중점으로 살펴볼 것이다. 이 기법은 등록 단계, 로그인 단계, 검증 단계로 구성되어 있다.

〈등록 단계〉

1. 등록단계에서 새로운 사용자 U_i는 서버 S에게 자신의 ID_i와 PW_i를 제출한다.
2. S는 m과 I를 계산 하고 U_i의 스마트카드에 $\{m, I, h(.), p\}$를 저장한다.
   - $m = h(ID_i \oplus x_s) \oplus h(x_s) PW_i$
   - $I = h(ID_i \oplus x_s)$

〈로그인 단계〉

로그인 단계에서 U_i가 원격 서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입하고 ID_i, PW_i를 입력한다. 스마트카드는 다음 과정을 수행한다.

1. $r_u = g^a \bmod p$를 계산한다.
2. $M = m \oplus PW_i$를 계산한다.
3. $C = M \oplus r_u$를 계산한다.
4. $R = I \oplus r_u = h(ID_i \oplus x_s) \oplus r_u$를 계산한다.
5. 스마트카드는 $\{C, T, E_R[r_u, ID_i, T]\}$ 를 S에게 보낸다. ($E_R[r_u, ID_i, T]$는 비밀 키R로 암호화된 값)

〈검증 단계〉

S는 데이터 $\{C, T, E_R[r_u, ID_i, T]\}$를 T'시간에 받고 다음과 같은 수행을 한다.

1. S의 비밀 키x_s를 이용하여 복호화 하는데 필요한 비밀 키R을 구한다.
   i) $R = C \oplus h(x_s)$
   ii) $E_R[r_u, ID_i, T]$을 복호화 하여 다음을 계산한다.
2. T와 T' 사이의 시간 간격(time interval)을 확인한다.
3. 다음 식이 성립하는지 확인한다.
   i) $R = h(ID_i \oplus x_s) \oplus r_u$를 계산한다.
   만약 식이 일치 한다면 S는 다음을 계산하여 U_i에게 보낸다.
   ii) $E_R[r_s, r_u + 1]$, $(r_s = g^b \bmod p)$
4. U_i는 $E_R[r_s, r_u + 1]$를 복호화 하여 $r_u + 1$을 확인한다. 만약 식이 일치하면 U_i는 다음을 수행하여 S와 키 교환을 한다.
   i) $K_{us} = r_s^a = g^{ab}$

4.2.1 Chien and Chen의 기법 분석

Chien 등은 Das 등의 기법이 실제로 익명 통신을 만족하지 않음을 보이고 도청자에 대한 익명 통신을 제공하면서 키 교환이 가능한 사용자 인증 기법을 제안하였다. 그러나 Chien 등의 기법은 스마트카드가 tamper-resistance하지 않고 정당한 사용자가 공격자일 경우, $C_E \oplus R_E$ 값을 통해 $h(x_s)$를 얻음으로서 다른 정당한 사용자 인척 할 수 있게 된다. 따라서 이 기법은 내부자에 의한 가장 공격(strong masquerading server/user attack)에 안전하지 않다.[4] 또한 로그인 단계에서 사용자의 패스워드가 잘못 입력이 됐을 경우, 인증 단계에서 오직 서버에 의해 확인될 수 있어 비효율적이다.

V. 제안된 프로토콜

본 논문에서는 제3자뿐만 아니라 원격 서버에 대해서도 익명성을 제공 받을 수 있는 악의적인 사용자 추적이 가능한 익명 인증 프로토콜을 제안한다.

5.1 제안된 프로토콜

본 프로토콜은 다음의 등록 단계, 로그인 단계, 인증 단계와 추적 단계인 4단계로 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) $R_i = h(ID_i \oplus x_s) \oplus h(x_s) \oplus h(PW_i)$
   (2) $I = h(ID_i \oplus x_s)$
   (3) $I_c = h(ID_i \oplus x_s) \oplus h(ID_i) \oplus h(PW_i)$
   (4) $TR = E_{PTR}[ID_i, UIN_i]$
   (5) $ATR = h(TR \oplus x_s)$
3. S는 U_i의 스마트카드에 $\{I, I_c, R_i, h(.), TR, p, y, ATR\}$를 저장하여 발급한다.
   • R_i는 사용자의 익명성을 제공하는 동적 아이디 C_{ID_i}를 생성하기 위해 필요한 값이며, I와 I_c는 사용자의 아이디와 패스워드를 로그인 단계에서 빠르게 확인함으로서 효율성 증대를 위해 생성되었다. TR은 신뢰기관의 공개키로 암호화된 사용자의 정보로서 악의적인 사용자를 추적하기 위해 생성된 값이며, ATR은 정당한 사용자를 검증함과 동시에 내부 공격자의 공격을 막기 위해 사용되는 값이다.

〈로그인 단계〉

1. U_i가 원격 서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입하고 ID_i, PW_i를 입력한다.
2. 스마트카드가 다음과 같은 수행을 한다.
   (1) 다음 식을 통해 사용자의 ID_i, PW_i를 확인한다.
   $I \oplus h(ID_i) \oplus h(PW_i) = I_c$
   (2) $X = g^a \bmod p$ (a는 스마트카드에 의해 생성된 랜덤 값)
   (3) $C_i = R_i \oplus I \oplus h(PW_i) \oplus h(PW_i \oplus r)$
   $= h(x_s) \oplus h(PW_i \oplus r)$
   (4) $UTR = h(PW_i \oplus r) \oplus TR$
   (5) $OAR = h(PW_i \oplus r) \oplus ATR$
   (6) $M = h(e \oplus T)$
   (7) $V = h(M \oplus y) \oplus h(PW_i \oplus r)$
   (8) $C_{ID_i} = h(C_i \oplus h(y \oplus T), X, OAR)$
3. 인증을 위해 S에게 메시지 $\{T, C_{ID_i}, M, V, X, UTR\}$을 보낸다.
   • 사용자는 스마트카드를 통해 자신의 아이디와 패스워드를 확인 받은 다음, 키 교환을 위한 값(X)과 사용자 익명성을 위한 값(C_{ID_i})를 생성한다. V는 인증 단계에서 원격 서버의 사용자 인증을 위해 필요한 값이며 이때 사용된 값 $\{a, r, e\}$는 스마트카드에 의해 생성된 랜덤 값이다. UTR은 악의적인 사용자를 추적하기 위해 필요한 값 TR을 원격 서버에 안전하게 보내기 위해 생성한 값이다.

〈인증 단계〉

1. S는 메시지 $\{T, C_{ID_i}, M, V, X, UTR\}$를 T'시간에 받는다.
2. S는 다음과 같은 수행을 한다.
   (1) T 와 T'사이의 시간 간격(time interval)을 확인한다.
   (2) S는 다음 계산을 통해 C_{ID_i}를 검증하는데 필요한 값을 얻어 낸다.
   i) $h(PW_i \oplus r) = V \oplus h(M \oplus y)$
   ii) $C_i = h(PW_i \oplus r) \oplus h(x_s)$
   iii) $TR = UTR \oplus h(PW_i \oplus r)$
   iv) $OAR = h(TR \oplus x_s) \oplus h(PW_i \oplus r)$
   (3) 다음 식이 성립하는지 확인 한다.
   $C_{ID_i} = h(C_i \oplus h(y \oplus T), X, OAR)$
3. 만약 C_{ID_i} 와 식이 일치 하면 S는 다음과 같은 수행을 한다.
   (1) $SK \leftarrow X^b \bmod p$, ($b$는 서버에 의해 생성된 랜덤 값)
   (2) $Y = g^b \bmod p$
4. S는 U_i에게 메시지 M_s를 계산하여 Y와 함께 보낸다.
   $M_s = h(OAR \oplus M \oplus y, SK, Y)$
5. U_i는 메시지 M_s와 Y를 받고 다음과 같은 수행을 하고 식을 확인해서 일치 하는지 확인한다.

(1) $SK \leftarrow Y^a \bmod p$, ($a$는 스마트카드에 의해 생성된 랜덤 값)

(2) $M_s = h(OAR \oplus M \oplus y, SK, Y)$

6. M_s값이 일치 한다면 U_i와 S는 SK를 이용해 다음과 같이 세션 키를 맺는다.

$h(SK) = SK_{us}$

• 원격 서버는 사용자로부터 받은 메시지{T, C_{ID_i}, M, V, X, UTR}를 이용하여 C_{ID_i} 검증에 필요한 값을 얻어낸다. 이때 OAR값은 서버의 개인 키(x_s)를 이용하여 생성되기 때문에 오직 서버만이 할 수 있으며 이를 통해 내부 공격자에 대한 가장 공격에 안전하다. M_s는 상호인증을 위해 서버에 의해 생성된 값으로 사용자에게 전송되어 지며 SK는 사용자와 원격 서버간의 세션 키(session key)이다.

〈추적 단계〉

S가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적하기 위해 인증 단계에서 다음과 같은 수행을 한다.

1. S는 메시지 {T, C_{ID_i}, M, V, X, UTR}를 T'시간에 받는다.
2. S는 다음과 같은 수행을 한다.
   (1) T 와 T'사이의 시간 간격(time interval)을 확인한다.
   (2) S는 다음 계산을 통해 TR값을 얻어 낸다.
      i) $h(PW_i \oplus r) = V \oplus h(M \oplus y)$를 얻어 낸다.
      ii) $C_i = h(PW_i \oplus r) \oplus h(x_s)$: 서버의 개인키를 이용해 C_i를 생성하고 C_{ID_i}를 확인한다. 그 값이 서로 일치 한다면 다음 계산을 통해 TR을 얻는다.
      iii) $TR = UTR \oplus h(PW_i \oplus r)$
3. S는 TR값과 CS을 함께 신뢰기관에 제출한다.
4. 신뢰기관은 CS를 확인하고 TR값을 자신의 개인키로 복호화하여 서버에 사용자 정보를 알려준다.
   • 원격 서버는 사용자로부터 받은 메시지{T, C_{ID_i}, M, V, X, UTR} 중에서 V값을 이용하여 사용자 추적을 위해 필요한 값($h(PW_i \oplus r)$)을 얻어 낸다. 이 값은 UTR값과 X-OR연산을 통해 TR을 얻게 되며 신뢰기관에 제출되는 악의적인 사용자에 대한 Complain Sheet(CS)와 함께 신뢰기관에 제출된다.

〈사용자의 패스워드 변경〉

U_i가 자신의 PW_i를 새로운 PW_i^*로 바꾸고자 할 때, U_i는 서버와 상관없이 스마트카드만을 이용하여 새로운 PW_i^*로 교체 할 수 있다. 스마트카드는 다음과 같은 수행을 한다.

1. U_i는 자신의 스마트카드를 리더기에 삽입 후, 자신의 ID_i와 PW_i를 입력한다.
2. 스마트카드는 다음을 확인한다.
   (1) $I \oplus h(ID_i) \oplus h(PW_i) = I_c$
3. 만약 값이 일치하면 스마트카드는 다음과 같은 수행을 하여 PW_i를 교체한다.
   (1) $I_c \oplus h(PW_i) \oplus h(PW_i^*) = I_c^*$
   (2) $R_i \oplus h(PW_i) \oplus h(PW_i^*) = R_i^*$
4. 스마트카드는 새롭게 생성된 I_c^*와 R_i^*값을 저장한다.

Ⅵ. 분 석

이번 장에서는 제안된 기법의 안전성과 기능에 대해 논하고, 기존 논문들과의 비교를 통해 효율성을 살펴본다.

6.1 안전성 분석

1. 초기 스마트카드를 이용한 원격 사용자 인증 기법에서는 서버가 사용자 인증 요청에 대한 검증을 위해 사용자 아이디와 패스워드를 서버에 검증 테이블(verification table) 형태로 저장하였다. 이때, 공격자가 서버의 검증 테이블을 얻는다면 정당한 사용자인척 가능하게 된다. 하지만 제안된 기법에서는 원격 서버가 자신의 개인키(x_s)와 비밀 값(y)를 갖고 있지만 검증 테이블을 따로 저장하지 않는다. 그러므로 제안된 기법은 stolen-verifier 공격에 안전하다.
2. 제안된 기법에서 사용자는 자신의 아이디와 패스워드를 자유롭게 생성 가능 하고 사용자가 패스워드를 변경하기를 원할 때 서버의 도움 없이 스마트카드만을 이용해 사용자의 패스워드를 자유롭게 변경 할 수 있다.
3. 제안된 기법의 인증단계에서 서버는 타임스탬프

(time stamp)를 이용하여 정당한 시간 간격 안에서의 새로운 메시지(freshness)임을 확인 할 수 있다. 따라서 제안된 기법은 재생 공격(replay attack)에 안전하다. 또한 M과 V값을 생성할 때 스마트카드에 의해 생성된 랜덤 값이 사용된다. 이 값은 매번 사용자가 로그인을 요청 할 때 마다 바뀌므로 제안된 기법은 parallel session attacks에 안전하다.

4. 로그인 단계에서는 I값과 I_r값을 사용하여 사용자의 아이디와 패스워드를 체크함으로써 정당한 사용자임을 스마트카드를 통해 미리 확인 할 수 있어 효율적이다.
5. 서버는 사용자로부터 받은 메시지{T, C_{ID_i}, M, V, X, UTR}와 자신이 갖고 있는 서버의 비밀 값과 개인키를 이용하여 동적 아이디를 생성하여 정당한 사용자임을 인증한다. 이때, 서버는 사용자의 아이디가 드러나지 않기 때문에 정당한 사용자임을 확인 할 수 있지만 누구인지 알지 못함으로써 서버에 대해 사용자 익명성을 제공한다. 하지만 제안된 기법은 서버가 매번 같은 TR값을 얻기 때문에 서버는 사용자가 누구인지는 정확하게 알 수 없으나 이전 세션과 같은 사용자임은 알 수 있다. 만약 서버에 대해 완전한 익명성을 제공하려면 매 세션 TR값이 동적 아이디와 같이 변해야 하고 추후 추적을 고려한다면 매 세션 변화된 TR값을 서버 측에서 저장하고 있어야한다. 이는 모든 사용자에 대해 매 세션 저장되어야 하기 때문에 서버의 저장량의 부담이 크다. 따라서 서버에 대한 익명성 정도와 서버의 저장량 사이에는 trade-off 관계가 있다. 제안된 기법은 서버에 대해 완전한 익명성은 보장되지 않으나 서버에게 ID가 드러나지 않는다.
6. 제안된 기법은 외부·내부 공격자에 의한 가장 공격(impersonation attack)에 안전하다. 외부 공격자가 정당한 사용자의 아이디와 패스워드를 얻었다고 가정하였을 때, 정당한 로그인 정보를 위조하기 위해서는 V값 안에 포함된 비밀 값y를 알아야 $h(M \oplus y)$를 만들 수 있다. 하지만 공격자는 서버의 비밀 값을 알지 못하기 때문에 정당한 사용자인척 가장 할 수 없다. 내부 공격자일 경우 $h(x_s)$를 얻어도 TR값과 서버의 비밀 키(x_s)로 이루어진 OAR값을 생성 할 수 없기 때문에 C_{ID_i}를 구성할 수 없다. 또한 상호 인증을 위해 생성된 M_s값에 OAR값이 포함이 되어져 있어서 내부 공격자에 의한 가장 공격은 불가능하다.
7. 제안된 기법은 서버와 사용자 간의 상호 인증이 가능하다. 서버는 사용자로부터 받은 메시지 중에서 동적아이디를 비교함으로써 사용자를 인증 할 수 있다. 사용자는 서버로부터 생성된 값(M_s)을 통해 정당한 서버인지를 확인 할 수 있다.

6.2 기능 분석

본 논문에서 제안하는 기법은 사용자의 프라이버시를 보호하기 위해 필요한 다양한 기능들을 제공함과 동시에 기존의 사용자 인증기법 보다 기능대비 연산량면에서 효율적이다. 제안된 기법과 유사 기능을 가진 논문을 살펴보면 다음과 같다. Chai 등[2]의 기법은 원격 서버가 매번 한명의 사용자 인증을 위해 사용자 수만큼의 연산량과 통신량을 필요로 한다는 점에서 제안된 기법과 비교하여 비효율적이다. Hu 등[4]의 기법은 로그인 단계와 인증 단계에서 1번씩의 암·복호화 연산을 필요로 하지만 제안된 기법은 등록 단계에 신뢰기관의 공개키로 암호화된 값을 스마트카드에 저장하여 사용하기 때문에 로그인과 인증 단계에서 추가적인 암·복호화 연산이 요구되어 지지 않는다. 제안된 기법에서 서버가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적하기 위한 추적 단계에서는 $5H$만큼의 연산만이 더 요구된다.

다음은 프로토콜의 기능과 연산량을 분석하기 위해 필요한 표기이다. · 익명성※ : 제3자와 서버에게 익명성 제공 여부; · FWP : 빠른 잘못된 패스워드 탐지가능 여부; · FC : 패스워드 변경가능 여부; · L.P : 로그인 단계; · A.P : 인증 단계; · P.C : 사용자 패스워드 변경단계; · T.P : 추적 단계; · Exp : 지수 계산; · Hash : 해쉬함수; · S : 암·복호화; · RC : 사용자가 패스워드 자유롭게 선택가능 여부; · △ : 서비스제공 실패; · n : 한명의 사용자가 인증을 하기위해 필요한 아이디의 개수로써 하나의 진짜 아이디와 n-1개의 가짜 아이디로 구성되어 있음; · α : 등록 단계 없이 패스워드를 변경 시 서버와의 통신을 통해 패스워드의 validity를 확인한 다음 변경 가능. 따라서 서버가 validity 확인만큼의 연상량을 추가로 요구 [2]; · - : 해당 논문에서 고려되지 않은 기능.

〔표 1〕 프로토콜과의 기능 분석

프로토콜	익명성*		추적 가능성	상호 인증	FWP	키 교환	패스워드†	
	제3자	서버					FC	RC
Our scheme	○	○	○	○	○	○	○	○
Das[3]	△	×	×	×	×	×	×	○
Chien[1]	○	×	×	△	×	○	×	○
Hu.[4]	○	×	×	○	○	○	○	○
Chai[2]	○	○	×	○	×	○	○	○

〔표 2〕 프로토콜과의 연산량 분석

프로토콜	L.P	A.P	P.C	T.P
Our scheme	6H+1E	4H+2E	3H	5H
Das[3]	5H	3H	-	-
Chien[1]	1H+1E+1S	2H+3E+3S	-	-
Hu.[4]	2H+1E+1S	3H+1E+1S	2H	-
Chai[2]	n(4H+2E)	n(3H+1E)	1H+α	-

Ⅶ. 결 론

스마트카드를 이용한 원격 사용자 인증 기법은 개인 프라이버시 보호에 대한 관심 및 요구가 증가됨에 따라 사용자 익명성을 제공하는 방향으로 진행되고 있다. 본 논문에서 제안된 기법은 tamper-resistant한 성질의 스마트카드를 이용한 사용자의 익명성을 제공하는 프로토콜로써 인터넷 환경에서 인증을 필요로 하는 다양한 분야에 활용 가능하게 될 것이다. 사용자가 등록 단계에서 자신의 아이디와 패스워드, 서버로부터 발급받은 스마트카드의 정보를 이용하여 인증 메시지를 생성할 때, 고정된 사용자의 아이디를 사용하는 대신에 동적으로 아이디를 생성하여 사용하며, 이 동적 아이디는 사용자의 로그인 요청 때마다 아이디를 변화시킴으로서 제 3자와 서버에 대한 사용자 익명성을 제공한다. 또한 인증 메시지에서 *UTR*을 통해 원격 서버가 사용자의 악의적인 행동을 감지했을 때 신뢰기관의 협조를 얻어 악의적인 사용자를 추적할 수 있게 한다. 로그인 단계에서 사용자의 아이디와 패스워드를 사전에 체크함으로써 정당한 사용자임을 스마트카드를 통해 미리 확인 할 수 있어 효율적이다. 본 기법은 향후에는 스마트카드를 이용한 익명성을 제공하는 사용자 속성기반 인증 기법에 대한 연구를 통하여 직위에 따른 접근 권한을 줌으로써 사용자 정보의 과다 누출을 방지하는 연구가 요구되어진다.

참고문헌

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

[2] Z. Chai, Z. Cao, and R. Lu, Efficient Password-Based Authentication and Key Exchange Scheme Preserving User Privacy, WASA'06, LNCS 4138, pp. 467-477, 2006.

[3] 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.

[4] L. Hu, Y. Yang, X. Niu, Improved Remote User Authentication Scheme Preserving User Anonymity, IEEE CNSR'07, pp. 323-328, 2007

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

[6] W.C. Ku, C.M. Chen, and H.L. Lee, Cryptanalysis of a variant of Peyravian-Zunic's password authentication scheme, IEICE Trans. Commun., Vol. E86-B, No. 5, pp. 1682-1684, 2003.

[7] H.M. Qiu, Y.X. Yang, and Z.M. Hu, A new mutual user authentication scheme using smart card, Application Research of Computers, No. 12, pp. 103-105, 2005.

[8] E.J. Yoon, K.Y. Yoo, More efficient and secure remote user authentication scheme using smart cards, IEEE ICPADS'05, Vol. 2, pp. 73-77, 2005.

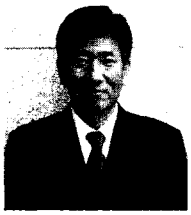
〈著者紹介〉

김 세 일 (Seil Kim) 학생회원

2005년 2월 : 고려대학교 수학과 학사
2008년 2월 : 고려대학교 정보보호대학원 석사
2008년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 암호 프로토콜, 익명성 연구, PET 기술

천 지 영 (Ji Young Chun) 학생회원

1997년 2월 : 이화여자대학교 수학과 학사
2006년 2월 : 단국대학교 수학과 석사
2006년 3월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 암호 이론, PET 기술, 유비쿼터스 보안



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