2013년 6월 전자공학회 논문지 제 50 권 제 6 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 6, June 2013 http://dx.doi.org/10.5573/ieek.2013.50.6.159

논문 2012-50-6-18

정보추출 가능한 스마트카드 환경에서 익명성과 추적성을 제공하는 원격 사용자 인증 기법

(A Remote User Authentication Scheme Preserving Anonymity and Traceability with Non-Tamper Resistant Smart Cards)

권 혁 진*, 류 은 경**, 이 성 운*

(Hyuck-Jin Kwon, Eun-Kyung Ryu, and Sung-Woon Lee©)

요 약

최근 개인 프라이버시 보호에 대한 관심과 요구가 증대됨에 따라 스마트카드 기반의 원격 사용자 인증 기법들에서도 사용자 익명성을 제공하는 연구들이 활발히 진행되고 있다. 2008년, Kim 등은 스마트카드 기반의 사용자 인증에서 외부 공격자와 원격서버 모두에 대하여 사용자 익명성을 보장하고 사용자의 악의적인 행동으로 인한 문제 발생 시에는 추적서버의 도움으로만 악의적인 사용자를 추적하기 위한 인증 기법을 처음으로 제안하였다. 그러나, 2010년에 Lee 등은 Kim 등의 기법에서 원격서버가 추적서버의 도움 없이도 사용자를 추적할 수 있는 문제점이 있음을 지적하고, 이를 개선한 인증 기법을 제안하였다. 한편, 2010년에 Horng 등은 정보추출이 가능한 스마트카드 환경, 즉 공격자가 전력 소비 모니터링 등과 같은 특수한 정보 분석 기법을 통하여 스마트카드 안에 저장된 비밀 정보를 알아낼 수 있는 환경에서도 다양한 공격들에 대하여 안전하고 외부 공격자에 대하여 사용자 익명성을 제공할 수 있는 인증 기법을 제안하였다. 본 논문에서는 정보추출 가능한 스마트카드 환경에서 외부 공격자뿐만 아니라 원격서버에 대해서도 익명성을 보장하고 필요시에는 추적서버의 도움으로만 사용자를 추적할 수 있는 원격 사용자 인증 기법을 제안하고자 한다.

Abstract

Recently, because the interest and needs in privacy protection are growing, smartcard-based remote user authentication schemes have been actively studied to provide the user anonymity. In 2008, Kim et al. first proposed an authentication scheme in order to ensure the user anonymity against both external attackers and the remote server and track malicious users with the help of a trusted trace sever. However, in 2010, Lee et al. showed that Kim et al.'s scheme cannot provide the user anonymity against remote server, which is because the server can trace users without any help of the trace server, and then proposed a improved scheme. On the other hand, in 2010, Horng et al. proposed an authentication scheme with non-tamper resistant smart cards, in which the non-tamper resistant smart card means that an attacker may find out secret information stored in the smart card through special data analysis techniques such as monitoring power consumption, to be secure against a variety of attacks and to provide the user anonymity against external attackers. In this paper, we will propose a remote user authentication scheme with non-tamper resistant smart cards not only to ensure the user anonymity against both external attackers and the remote server but also to track malicious users with only the help of a trusted trace sever.

Keywords : 정보보호, 인증, 스마트카드, 익명성, 추적, 키교환

* 정회원, 동명대학교 정보보호학과(Department of Information Security, Tongmyong University)
** 정회원, 경북대학교 컴퓨터공학과(Department of Computer Engineering, Kyungpook National University)
※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 연구임 (2011-0008890)
© Corresponding Author(E-mail: staroun@tu.ac.kr)
접수일자 2013년2월7일, 수정완료일 2013년5월22일

Ⅰ. 서 론

스마트카드의 편리성과 안전성 때문에 지금까지 다양한 스마트카드 기반의 원격 사용자 인증 기법들이 제안되어 왔다[1-9]. 이러한 기법들의 대부분은 스마트카드가 부정조작이 어렵다(tamper resistant)는 가정 하에서 제안되었다. 즉, 스마트카드 안에 저장된 비밀 정보들은 안전하다는 것이다. 그러나 몇몇 연구들[3,9,10,11]은 스마트카드 안에 저장된 비밀 정보들이 전력 소비 모니터링 등과 같은 어떤 특수한 방법들에 의하여 추출될 수 있다는 것을 보여 주고 있다. 만약 이처럼 스마트카드가 부정조작이 가능하다면 기존의 거의 모든 스마트카드 기반의 인증 기법들은 위장 공격과 오프라인 패스워드 추측 공격 등과 같은 다양한 공격들에 취약할 수밖에 없다.

2007년, Hu 등[3]은 스마트카드가 정보추출이 가능한 환경에서 다양한 공격에 안전하면서 사용자 익명성을 제공하기 위하여 원격 사용자 인증 기법을 제안하였다. 그러나 2010년에 Horng 등[9]은 Hu 등의 기법이 강한 사용자/서버 위장 공격뿐만 아니라 오프라인 패스워드 추측 공격에도 취약함을 보여 주었고 이를 개선한 기법을 제안하였다.

한편, 개인 프라이버시 보호에 대한 관심과 요구가 증가됨에 따라 스마트카드 기반의 원격 사용자 인증 기법은 2004년 Das 등[1]이 제안한 기법 이후로 익명성을 제공하기 위한 연구가 활발히 진행되어 왔다[2-9]. 이러한 연구들의 대부분은 원격서버를 제외한 외부 공격자에 대한 사용자 익명성을 제공하는 데 초점을 맞추고 있다.

그러나 기업 내부의 고의나 실수로 인한 정보 유출 사고가 증가함으로서 국가 및 기업 내부의 고객 개인정보 또는 내부 비밀의 외부 유출을 막기 위한 관심이 증대되고 있다. 2006년에 Chai 등[6]은 이전 기법들과는 달리 외부공격자에 대한 사용자 익명성뿐만이 아니라 원격서버에 대한 사용자 익명성을 보장하기 위한 인증 기법을 처음으로 제안하였다. 그러나 이 기법은 원격서버가 매번 한 명의 사용자 인증을 위해 전체 사용자 수만큼의 연산량과 통신량을 필요로 한다는 점에서 매우 비효율적이다. 한편, 원격서버에 대한 사용자 익명성을 보장하기 위해서는 원격서버가 사용자의 악의적인 행동을 감지했을 때 추적 기관의 협조를 얻어 악의적인 사용자가 누구인지를 밝혀낼 수 있는 추적 기능이 요구된다. 그러나 Chai 등의 기법에서는 이러한 사용자 추적 기능을 전혀 고려하지 않았다.

2008년, Kim 등[7]은 처음으로 외부공격자와 원격서버에 대하여 사용자 익명성을 제공할 뿐 아니라 사용자의 악의적인 행동에 따른 문제 발생 시에 추적서버의 도움으로 사용자를 추적할 수 있는 스마트카드 기반의 원격 사용자 인증 기법을 제안하였다. 그러나 2010년, Lee 등[8]은 Kim 등의 기법에서 원격서버가 추적서버의 협조 없이도 사용자를 추적할 수 있어 원격서버에 대한 사용자 익명성이 완전하게 보장될 수 없을 뿐만 아니라 사용자의 행위가 다른 스마트카드 소유자에 의해 분석될 수 있는 문제점들이 있음을 보여주었다. 또한 이러한 문제점들을 개선한 새로운 인증 기법을 제안하였다.

본 논문에서는 정보추출이 가능한 스마트카드 환경에서 외부공격자에 대해서 뿐만 아니라 원격서버에 대해서도 사용자 익명성을 보장하고 필요시에는 추적서버를 통해서만 사용자를 추적할 수 있는 원격 사용자 인증 기법을 제안한다. 제안된 인증 기법은 스마트카드가 정보추출이 가능하다 할지라도 오프라인 패스워드 추측 공격과 위장 공격 등과 같은 다양한 공격들에 대해서 안전성을 제공할 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 Horng 등의 기법에 대해 살펴보고, Ⅲ장에서는 본 논문에서 제안하고자 기법에 대하여 기술한다. 그리고 Ⅳ장에서는 제안된 인증 기법의 안전성과 기능적 특징들을 살펴보고, 마지막 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 관련 연구

이 장에서는 본 논문 전반에서 사용할 표기들에 대하여 먼저 기술하고, 본 논문에서 제안하고자 하는 인증 기법의 기반이 되는 Horng 등의 기법[9]에 대하여 살펴보고자 한다.

1. 표기

본 논문에 기술된 여러 기법들에서 공통적으로 사용할 표기 방법은 다음 표와 같다.

표 1. 표기
Table 1. Notations.

기호	설명
A	사용자
S	원격서버
T	신뢰할 수 있는 추적서버
pw	사용자의 패스워드

x, y	서버의 비밀키와 비밀값
PR_A, PU_A	사용자 A의 개인키와 공개키
h(·)	안전한 일방향 해쉬 함수
p	큰 소수
g	순환군 Z_p의 생성자
⊕	XOR 연산
$E_K[m]$	메시지 m에 대한 대칭키 암호화 연산
$E_K\{m\}$	메시지 m에 대한 공개키 암호화 연산
$cert_A$	사용자 A의 인증서
-----→	안전한 채널
——→	안전하지 않은 채널

2. Horng 등의 인증 기법

Horng 등의 기법은 정보추출이 가능한 스마트카드 환경에서 외부공격자에 대하여 사용자 익명성을 제공하기 위하여 제안된 인증 기법이다. 이 기법은 등록 단계, 로그인/인증 단계, 패스워드 변경 단계로 구성되어 있다. 각 단계의 세부적인 과정은 다음과 같다.

가. 등록 단계

등록 단계는 사용자 A가 원격 서버 S에 자신을 등록하고 스마트카드를 발급 받고자 할 때 수행된다. 이 단계는 안전한 채널을 통하여 수행되며 그 과정은 다음과 같다.

(1) A는 자신의 아이디 A와 패스워드 pw, 임의의 정수 b를 선택한다.
(2) A는 안전한 채널을 통하여 A, h(b,pw)을 S에 전송한다.
(3) S는 $W = h(A,x) \oplus h(b,pw)$, $w = g\ h(A,x)h(x) \bmod p$, 여기서 x는 S의 비밀키이다.
(4) S는 W, w, h(·), p, g을 스마트카드에 저장한 후 A에게 안전한 채널을 통하여 전달한다.
(5) A는 S로부터 스마트카드를 받은 후에 b를 스마트카드에 저장한다.

나. 로그인/인증 단계

로그인/인증 단계는 사용자 A가 원격 서버 S로부터 서비스를 제공받기 위하여 S에 로긴 요청하고 A와 S가 서로 정당한지를 검증하기 위하여 수행된다. 먼저 사용자는 자신의 스마트카드를 카드 리더기에 넣고 자신의 아이디 A와 패스워드 pw를 입력한다. 그 과정은 다음과 같다.

(1) 스마트카드는 $I = W \oplus h(b,pw) = h(A,x)$을 계산한다.
(2) 스마트카드는 임의의 정수 a, u를 생성하고 $C = g^{aI} \bmod p$, $R = w^a \bmod p = g^{aIh(x)} \bmod p$, $N_A = g^u \bmod p$, $M1 = I \oplus N_A$를 순서대로 계산한다. 그리고 메시지 C, $E_R[A,M_1]$을 S에 전송한다.
(4) S는 A로부터 로긴 요청 메시지를 받은 후 $R = C^{h(x)} \bmod p = g^{aIh(x)} \bmod p$를 계산한 후 A와 M_1을 얻기 위하여 메시지 $E_R[A,M_1]$를 복호화한다.
(5) S는 사용자의 아이디 A가 타당한지를 검사한다. 그리고 $I = h(A,x)$, $N_A = I \oplus M_1$ 값을 계산한다.
(6) S는 $N_V = g^v \bmod p$, $M_2 = I \oplus N_V$, $K_{AS} = (N_A)^v \bmod p = gu^v \bmod p$, $M_3 = h(A,K_{AS},N_A)$을 각각 계산한다. 그리고 A에게 메시지 $E_R[M_2,M_3]$을 전송한다.
(7) 스마트카드는 $E_R[M_2,M_3]$을 대칭키 R로서 복호화한다. 그리고 $N_V = I \oplus M_2$, $K_{AS} = (NV)^u \bmod p = g^{uv} \bmod p$를 각각 계산하고 M_3 ?= $h(A,K_{AS},N_A)$ 체크하여 같으면 S에게 $M_4 = h(N_V,K_{AS})$을 전송한다.
(8) 마지막으로 S는 A로부터 M_4을 받은 후에 M_4 ?= $h(N_V,K_{AS})$ 체크하고 같다면 인증은 완성된다.

다. 패스워드 변경 단계

패스워드 변경 단계는 사용자 A가 자신의 패스워드를 변경하고자 할 때 수행된다. 여기서는 서버의 도움을 받고 상호인증 후에 패스워드를 변경한다. 그 과정은 다음과 같다.

(1) 사용자 A는 스마트카드를 리더기에 삽입한 후 새로운 패스워드 pw^*를 입력한다.
(2) 스마트카드는 $W^* = h(A,x) \oplus h(b,pw^*)$를 계산하고, W^*를 W로 변경하여 저장한다.

Horng 등의 기법은 외부공격자에 대한 사용자 익명성 제공만을 고려하여 설계되었다. 따라서 이 기법에서 원격서버는 현재 로긴하는 사용자가 누구인지를 바로 알 수 있다. 그러므로 Horng 등의 기법은 원격 서버에 대한 사용자 익명성이 요구되는 환경에서 사용하기에 적합하지 않다고 할 수 있다.

Ⅲ. 제안하는 인증 기법

이 장에서는 정보추출이 가능한 스마트카드 환경에

서 외부 공격자뿐만 아니라 원격 서버에 대해서도 사용자 익명성을 제공할 수 있고, 필요시에는 원격서버가 추적서버의 협조를 받아 악의적인 사용자를 추적할 수 있는 인증 기법을 제안한다. 제안한 기법은 등록 단계, 로그인/인증 단계, 추적 단계, 사용자 패스워드 변경 단계로 구성되어 있다.

가. 등록 단계

등록 단계는 사용자 A가 원격 서버 S에 자신을 등록하고 스마트카드를 발급 받고자 할 때 수행된다. 그 세부 과정은 다음과 같다.

(1) A는 자신의 아이디 A와 패스워드 pw를 선택한 후 임의의 난수 b를 생성하고 h(pw,b)를 계산하여 A, h(pw,b), $cert_A$를 안전한 채널을 통해 S에 전송한다. 이때 $cert_A$는 A의 인증서를 의미한다.
(2) S는 A로부터 등록 요청을 받으면 I = h(A,x)를 계산한 후, A, S, y, I, $cert_A$를 안전한 채널을 통해 추적서버 T에 전송한다. 이때 y는 S가 모든 사용자들에 대하여 공통으로 사용할 비밀값이다.
(3) T는 S로부터 사용자 A에 대한 등록 요청을 받으면 TR = E_z[A,n], STR = E_s{y,TR}, ATR = E_{PUA}{I,STR}을 각각 계산하고 안전한 채널을 통해 ATR을 S에게 전송한다. 이때 z는 T의 비밀키이며, PU_A는 A의 공개키를 의미한다.
(4) S는 W = I⊕h(A,h(pw,b))와 $w = g^{Ih(x)} \bmod p$를 계산하고 W, w, ATR, h(·), p, g를 스마트카드에 저장한 후 안전한 채널을 통해 A에게 발급한다.
(5) 마지막으로, A는 b를 자신의 스마트카드에 저장한다.

나. 로그인/인증 단계

로그인/인증 단계는 사용자 A와 데이터베이스 서버 S가 서로 정당한지를 검증하면서 한 개의 동일한 세션키를 공유하기 위하여 수행된다. 그 과정은 다음과 같다.

(1) 사용자는 자신의 아이디 A와 패스워드 pw, 그리고 사용자의 개인키 PR_A를 입력한다. 스마트카드는 PR_A를 이용하여 ATR을 복호화 한 후, I ?= w⊕h(A,h(pw,b))를 검사하여 사용자의 아이디와 패스워드, 그리고 개인키가 정확하게 입력되었는지를 검증한다. 또한 스마트카드는 두 개의 임의의 정수 a, u를 생성한 후, $C = g^{aI} \bmod p$, $R = w^a = g^{aIhx)} \bmod p$, $N_A = g^u \bmod p$를 순차적으로 계산하고 N_A와 STR을 대칭키 R로 암호화하여 C, E_R[N_A,STR]를 S에게 전송한다.
(2) S는 $R = C^{h(x)} = g^{aIh(x)} \bmod p$를 계산하고 E_R[N_A,STR]를 복호화한다. 또한 자신의 비밀키로 STR을 복호화하고 y를 검사하여 사용자가 정당한지를 검증한다. S는 사용자를 추적할 때 사용하기 위하여 TR를 안전한 장소에 저장할 수 있다. 또한 S는 임의의 정수 v을 생성한 후, $N_S = g^v \bmod p$, $K_{AS} = (N_A)^v = g^{uv} \bmod p$, $M_S = h(K_{AS},N_A)$을 순차적으로 계산하고 NS와 MS를 암호화하여 E_R[N_S,M_S]를 스마트카드에게 전송한다.
(3) 스마트카드는 E_R[N_S,M_S]를 복호화하고 세션키 $K_{AS} = (N_S)^u = g^{uv} \bmod p$를 계산한 후, M_S ?= $h(K_{AS},N_A)$ 검사하여 S가 정당한지와 자신과 동일한 세션키를 생성하였는지를 검증한다. 그리고 $M_A = h(K_{AS},N_S)$를 계산하여 M_A를 S에 전송한다.
(4) S는 $M_A = h(K_{AS},N_S)$를 검사하여 스마트카드가 자신과 동일한 세션키를 생성하였는지를 검증한다.

다. 추적 단계

추적 단계는 데이터베이스 서버 S가 사용자의 악의적인 행동을 감지했을 때 추적 서버 T의 협조를 받아 그 사용자가 누구인지를 추적하기 위하여 수행된다. S가 악의적인 사용자 A를 추적하기 위한 과정은 다음과 같다.

(1) S는 악의적인 사용자가 로긴할 때 사용하였던 TR과 CS(Complain Sheet)을 안전한 채널을 통하여 T에게 전송한다. 여기서 CS는 악의적인 사용자의 행위들에 대하여 기술한 내용을 의미한다.
(2) T는 CS의 내용을 확인하고 TR = Ez{A,n}를 복호화하여 n을 검사함으로써 자신이 발급하여준 TR값인지를 검증한다.
(3) T는 안전한 채널을 통하여 사용자의 아이디 A를 전송한다.
(4) S는 악의적인 사용자가 누구인지를 알 수 있고, 과거에 어떠한 행동을 했는지를 추적할 수 있다.

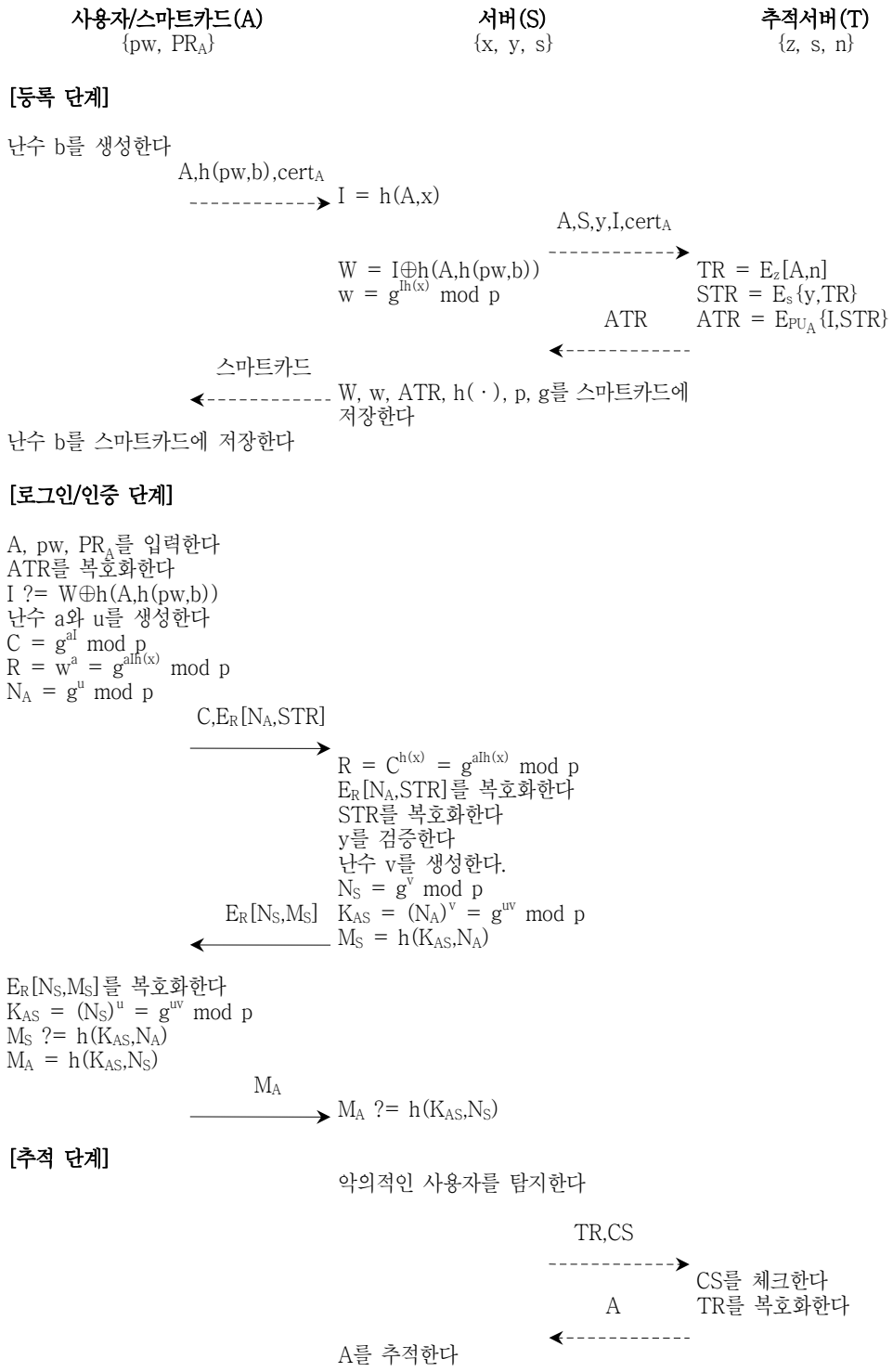


그림 1. 제안된 기법

Fig. 1. The proposed scheme.

라. 패스워드 변경 단계

패스워드 변경 단계는 사용자 A가 자신의 패스워드 pw를 새로운 패스워드 pw^*로 바꾸고자 할 때 수행된다. 그 과정은 다음과 같다.

(1) A는 자신의 스마트카드를 리더기에 삽입한 후 자신의 아이디 A, 현재의 패스워드 pw, 새로운 패스워드 pw^*를 순서대로 입력한다.
(2) 스마트카드는 $I \stackrel{?}{=} W \oplus h(A,h(b,pw))$를 검사하여 정당한 사용자인지를 검증한다. $W^* = I \oplus h(A,h(b,pw^*))$를 계산한다.
(3) 스마트카드는 새롭게 생성된 W^*을 W로 대신하여 저장한다.

제안된 기법은 Horng 기법을 기반으로 하여 서버에 대한 사용자 익명성을 제공할 수 있도록 하고 추적서버를 두어 필요시에는 사용자를 추적할 수 있는 추가적인 기능들을 제공할 수 있도록 설계되었다. 서버에 대하여 사용자 익명성을 제공하기 위해서는 서버가 사용자에 대하여 등록 단계에서 얻을 수 있는 정보들과 로그인/인증 단계에서 얻을 수 있는 정보들 사이에 공통적인 값이 없어야 한다. 제안된 기법에서는 이 문제를 해결하기 위하여 공개키 암호시스템을 사용하였다. 추적서버는 등록 단계에서 사용자의 신원정보가 포함된 TR을 사용자의 공개키로 암호화하여 서버를 통해 사용자에게 전달함으로써 서버는 등록 단계에서 사용자의 TR 값을 알 수 없다. 서버는 로그인/인증 단계에서 현재 로그인한 사용자의 TR 값을 얻을 수 있지만 어느 사용자의 TR인지는 알기 어렵다.

Ⅳ. 제안된 기법에 대한 분석

1. 안전성 분석

본 절에서는 제안된 기법이 다양한 공격들에 대하여 안전함을 보이고자 한다. 제안된 기법은 정보추출이 가능한 스마트카드 환경, 즉 공격자가 전력 소비 모니터링 등과 같은 특수한 정보 분석 기법을 통하여 스마트카드 안에 저장된 비밀 정보를 알아낼 수 있다고 가정한다. 제안된 기법은 이러한 정보추출이 가능한 스마트카드 환경일지라도 이산대수 문제의 어려움과 안전한 공개키 암호시스템, 대칭키 암호시스템, 해쉬함수의 사용에 기반하여 다음과 같은 안전성을 제공할 수 있다.

가. 오프라인 패스워드 추측 공격에 안전

오프라인 패스워드 추측 공격은 공격자가 프로토콜 수행 중에 얻을 수 있는 값들을 이용하여 추측된 패스워드 값이 맞는지를 반복적으로 확인함으로써 정확한 패스워드를 알아낼 수 있는 공격이다. 제안된 기법에서 인증 메시지들은 사용자의 패스워드를 전혀 포함하고 있지 않다. 그러므로 인증 메시지들을 이용한 오프라인 패스워드 추측 공격은 불가능하다고 볼 수 있다. 한편 제안된 기법은 스마트카드가 정보추출이 가능하다는 가정 하에 제안되었기 때문에 스마트카드 내의 정보들이 공격자들에게 노출된다 할지라도 오프라인 패스워드 추측 공격에 안전할 수 있어야 한다. 제안된 기법에서 스마트카드 내에 저장된 정보들은 W, w, ATR, b 등이다. 공격자가 이 정보들을 알아낸다 할지라도 사용자의 개인키 PR_A를 알지 못한다면 I을 모르기 때문에 사용자의 아이디와 A′와 패스워드 pw′를 추측한 후에 $W \stackrel{?}{=} I \oplus h(A',h(pw',b))$를 검사하기 어려워 정확한 패스워드를 알아내는 것은 불가능하다. 그러므로 제안된 기법은 오프라인 패스워드 추측 공격에 안전하다.

나. 사용자 위장 공격에 안전

제안된 기법에서 공격자는 사용자 A로 위장하려 할 수 있다. 이를 위해서는 S의 검증을 통과할 수 있는 첫 번째 로긴 메시지 C, $E_R[N_A, STR]$를 생성할 수 있어야 한다. 그러나 공격자는 서버의 비밀키 x와 A의 STR을 알지 못하기 때문에 C를 이용하여 S가 사용할 R을 계산할 수 없을 뿐만 아니라 S의 검증을 통과할 수 없다. 더욱이, 공격자가 A의 스마트카드를 습득하여 스마트카드 내의 모든 정보들을 추출할 수 있다 할지라도 공개키 암호시스템 때문에 A의 개인키를 알지 못하면 ATR로부터 STR을 얻을 수 없고 서버가 y를 검사하는 검증을 통과할 수 없어 A로 위장할 수 없다.

다. 서버 위장 공격에 안전

제안된 기법에서 공격자는 서버 S로 위장하려 할 수 있다. 이를 위해서는 사용자의 $M_S \stackrel{?}{=} h(K_{AS},N_A)$ 검증을 통과할 수 있어야 한다. 그러나 공격자는 S의 비밀키 x를 알지 못하기 때문에 A가 보낸 N_A를 알 수 없어 사용자의 검증을 통과할 수 있는 정확한 M_S를 계산할 수 없다. 그러므로 제안된 기법은 서버 위장 공격에 안전하다.

라. 재사용 공격에 안전

제안된 기법에서 공격자는 사용자 A가 이전 세션에서 사용하였던 로긴 메시지 C, $E_R[N_A,STR]$ 또는 M_A를 재사용함으로써 서버 S의 인증을 통과하려 할 수 있다. 그러나 S는 매 세션마다 새로운 난수 v를 생성하여 사용하기 때문에 A가 이전 세션에서 생성하여 사용하였던 난수 a, u와 S의 비밀키 x를 알 수 있어야 S의 M_S ?= $h(K_{AS},N_A)$ 검증을 통과할 수 있어야 한다. 그러므로 제안된 기법은 재사용 공격에 안전하다.

마. 사용자 익명성 제공

제안된 기법은 외부공격자와 서버 S 모두에 대해서 사용자 익명성을 제공할 수 있도록 설계되었다. 제안된 기법의 로그인/인증 단계에서 외부 공격자, 다른 스마트카드 사용자, 그리고 S에 대하여 자신의 아이디를 드러내지 않고 프로토콜을 수행할 수 있다. 로그인 및 인증 단계 중에 유일하게 사용자의 아이디 'A'를 포함하고 있는 값은 STR이다. 오직 S 만이 사용자의 로긴 메시지로부터 STR를 얻을 수 있다. 또한 서버는 STR이 정당한 사용자의 것인지 검증할 수 있다. 그러나 등록 단계의 정보들을 이용한다 할지라도 사용자의 아이디 정보를 알아내기는 어렵다. 그러므로 제안된 기법은 사용자 익명성을 제공할 수 있다.

바. 추적성 제공

제안된 기법은 서버 S가 악의적인 사용자의 행위를 발견했을 때 추적 서버 T의 도움을 받아 해당 사용자의 아이디를 알 수 있는 추적 기능을 제공한다. 로그인/인증 단계에서 S는 사용자의 악의적인 행위를 발견했을 때 안전한 채널을 통하여 추적 사유가 기술된 CS와 함께 사용자의 TR을 추적서버 T에 제공한다. T는 추적 사유가 정당하다고 판단되면 자신의 비밀키 z를 이용해 TR 값을 복호화하여 n을 검증한 후 S에게 해당 사용자의 A를 알려준다. 이때 TR은 비밀키 z를 아는 T 만이 복호화할 수 있어 T만이 사용자가 누구인지를 추적할 수 있음을 보장한다. 또한 제안된 기법에서는 원격 서버가 추적서버 없이도 사용자를 추적할 수 있는 문제는 발생할 수 없다. 왜냐하면 등록 단계에서 서버는 사용자의 개인키로 암호화되어 있는 ATR 내에 포함된 TR을 전혀 알 수 없기 때문이다.

사. 전방향 안전성 제공

전방향 안전성(forward secrecy)은 참여하는 개체들의 롱텀(long-term) 비밀키가 노출되었을 때에도 과거에 사용되었던 세션키들의 안전성이 보장될 때 제공된다. 이는 현재 시간에 각 개체의 실수 등으로 사용자의 패스워드와 같은 비밀값이 노출된다 해도 이전의 비밀 통신 내용은 보호되어야 한다는 점에서 매우 중요한 안전성 평가 요소로 사용되고 있다. 제안된 기법에서 공격자가 이전 세션들의 통신 메시지들을 모두 도청한 후에 사용자의 패스워드나 서버의 비밀키인 x 값을 알아낸다 할지라도 이산대수 문제로 인하여 이전 세션들에서 생성되어 사용된 세션키를 알아내기는 어렵다.

2. 기능 분석

다음 표는 몇 가지 주요 기능들 면에서 제안된 기법을 다른 관련 기법들과 비교하여 보여준다. 이 표에서 사용자 익명성은 효과적인 비교를 위해 외부 공격자와 서버로 구분하였다. 그리고 추적성은 추적서버만이 사용자를 추적가능한지를 보여주는 항목이다.

표 2. 관련 기법들과의 기능 비교
Table 2. Function comparison of the related schemes.

항목 / 기법	스마트카드 환경	사용자 익명성		추적성	키교환
		외부자	서버		
제안된 기법	N	o	o	o	o
Lee 등[8]	T	o	o	o	o
Horng 등[9]	N	o	x	x	o

N: 정보추출 가능, T: 정보추출 불가능
o: 제공, x: 기능제공안함

Ⅴ. 결 론

본 논문에서는 정보추출이 가능한 스마트카드 환경에서 사용자 익명성과 추적성을 제공할 수 있는 원격 사용자 인증 기법을 제안하였다. 즉, 제안된 기법은 공격자가 전력 모니터링 분석 등과 같은 특수한 방법들을 통하여 스마트카드 내의 비밀정보들을 알아낼 수 있는 상황에서도 다양한 공격들에 대하여 안전하고 외부 공격자들에 대해서 뿐만 아니라 원격서버에 대해서도 사용자 익명성을 보장하도록 설계되었다. 또한 완전하게 원격서버에 대한 사용자 익명성을 보장하기 위하여 원격서버는 단독으로 사용자가 누구인지 알 수 없으며, 악의적인 사용자를 탐지하였을 때와 같은 상황에서는 추적서버의 도움을 통해서만 사용자를 추적할 수 있도록 설계하였다. 한편 제안된 기법에서는 서버에 대한 사용자 익명성과 추적성을 제공하기 위하여 공개키 암

호시스템을 사용하였다. 스마트카드 내에서 공개키 암호시스템의 사용은 부담이 될 수 있다. 향후 공개키 암호시스템을 사용하지 않고 이 문제를 해결할 수 있는 방법을 연구하고자 한다.

Acknowledgement

본 논문은 [12]의 학술대회에서 발표된 논문을 수정 보완한 후 재구성하였다.

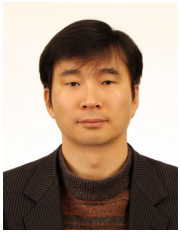
REFERENCES

[1] M. L. Das, A. Saxena and V. P. Gulathi, “A dynamic ID-based remote user authentication scheme,” IEEE Trans. on Consumer Electronics, Vol.50, no. 2, 2004.
[2] H. Y. Chien and C. H. Chen, “A remote authentication scheme preserving user anonymity,” IEEE AINA′05, Vol. 2, 2005.
[3] L. Hu, Y. Yang, X. Niu, “Improved remote user authentication scheme preserving anonymity,” Fifth Annual Conference on Communication Networks and Services Research(CNSR), 2007.
[4] C. S. Bindu, P. C. S. Reddy, B. Satyanarayana, “Improved remote user authentication scheme preserving anonymity,” International Journal of Computer Science and Network Security (IJCSNS), Vol. 8, no. 3, 2008.
[5] I. E. Liao, C. C. Lee, M. S. Hwang, “Security enhancement for a dynamic ID-based remote user authentication scheme,” IEEE Proceedings of the international conference on Next Generation Web Services Practices (NWeSP′′05), 2005.
[6] Z. Chai, Z. Cao, R. Lu, “Efficient password-based authentication and key exchange scheme preserving user privacy,” WASA’06, LNCS 4138, 2006.
[7] 김세일, 천지영, 이동훈, “추적이 가능한 스마트카드 사용자 인증 기법,” 한국정보보호학회논문지, 제18권 제5호, 2008.
[8] 이성운, 권혁진, 류은경, 하금숙, “스마트카드 기반의 추적 가능한 사용자 인증 기법에 대한 안전성 개선,” 보안공학연구논문지, 제7권 제2호, 2010
[9] W. B. Horng, C. P. Lee, J. W. Peng, “A Secure Remote Authentication Scheme Preserving User Anonymity with Non-Tamper Resistant Smart Cards,” WSEAS Transactions on Information Science and Applications, issue 5, Vol. 7, 2010.
[10] E. Brier, C. Clavier, F. Oliver, Correlation power analysis with a leakage model, Lecture Notes in Computer Science, Vol. 1, no. 2, 2004.
[11] 조종원, 한동국, “마스킹-셔플링 부채널 대응법을 해독하는 실용적인 편중전력분석,” 전자공학회논문지, 제49권 9호, 2012.
[12] 권혁진, 이성운, “추적 가능한 Non-Tamper Resistant 스마트카드 인증 기법,” 한국정보기술융합학회 동계학술대회, 2012.

저 자 소 개

권 혁 진(정회원)
2008년 경일대학교 컴퓨터공학과 학사 졸업.
현재 동명대학교 정보보호학과 석사과정.
<주관심분야 : 암호 프로토콜, RFID/USN 보안>

류 은 경(정회원)
1995년 경일대학교 컴퓨터공학과 사 졸업.
1999년 계명대학교 정보통신공학과 석사 졸업.
2005년 경북대학교 컴퓨터공학과 박사 졸업.
2006년～2007년 (일) 未來函館대학 시스템정보공학과 Post-doc.
2007년～2010년 경북대학교 전자전기컴퓨터학부 초빙교수
2010년～현재 경북대학교 전자전기컴퓨터학부 대학원 Post-doc.
<주관심분야 : 암호응용, 네트워크 보안>



이 성 운(정회원)
1993년 전남대학교 전산통계학과 학사 졸업.
1996년 전남대학교 전산통계학과 석사 졸업.
2005년 경북대학교 컴퓨터공학과 박사 졸업
2005년～현재 동명대학교 정보보호학과 부교수.
<주관심분야 : 암호 프로토콜, RFID/USN 보안>