사용자 익명성을 제공하는 스마트카드 기반 원격 인증 프로토콜

A Remote Authentication Protocol Using Smartcard to Guarantee User Anonymity

백 이 루* 길 광 은** 하 재 철***
YiRoo Baek KwangEun Gil JaeCheol Ha

요 약

원격 사용자 인증에 대한 문제를 해결하기 위해 자신이 알고 있는 패스워드와 소지한 스마트카드를 동시에 이용한 원격 사용자 인증 방식이 연구되었다. 최근에는 개인의 프라이버시를 보호하는 차원에서 통신 채널상에서 사용자의 익명성을 제공할 수 있는 방향으로 연구가 진행 중에 있다. 2004년도에 Das 등에 의해 동적 아이디를 사용한 사용자 익명성 제공 인증 기법이 처음으로 제안하였다. 그 후 Chien 등은 Das 등의 인증 기법이 사용자 익명성을 제공하지 못함을 지적하고 보다 개선된 인증 기법을 제안하였다. 그러나 Chien 등의 개선된 인증 기법도 내부자 공격, 서비스 거부 공격, 제한적 재전송 공격 등에 취약하다. 따라서 본 논문에서는 Chien 등의 방식이 가지는 취약점을 해결하는 향상된 인증 기법을 제안한다. 제안하는 원격 인증 방식은 사용자의 Nonce 값을 사용하여 내부자 공격을 방지하고, 타임 스탬프(time stamp) 대신 랜덤수를 사용하여 제한적 재전송 공격을 방어할 수 있도록 하였다. 또한, 복잡한 멱승 연산을 사용하지 않으므로 계산 효율성을 높였다.

ABSTRACT

To solve user authentication problem, many remote user authentication schemes using password and smart card at the same time have been proposed. Due to the increasing of interest in personal privacy, there were some recent researches to provide user anonymity. In 2004, Das et al. firstly proposed an authentication scheme that guarantees user anonymity using a dynamic ID. In 2005, Chien et al. pointed out that Das et al.'s scheme has a vulnerability for guaranteing user anonymity and proposed an improved scheme. However their authentication scheme was found some weaknesses about insider attack, DoS attack, and restricted replay attack. In this paper, we propose an enhanced scheme which can remove vulnerabilities of Chien et al.'s scheme. The proposed authentication protocol prevented insider attack by using user's Nonce value and removed the restricted replay attack by replacing time stamp with random number. Furthermore, we improved computational efficiency by eliminating the exponentiation operation.

☞ KeyWords : 원격 인증 프로토콜, 스마트카드, 사용자 익명성

1. 서 론

네트워크의 발전으로 분산된 컴퓨터 환경에서 원격 서버로 접근하는 일이 빈번해짐에 따라 원격 사용자 인증이 매우 중요한 요소가 되었고, 그로 인해 안전하지 않은 네트워크상에서 사용자와 원격 서버간의 인증을 위한 원격 사용자 인증 기법들이 많이 연구되었다. 원격 사용자 인증 기법은 1981년 Lampord에 의해 처음 제안되었으며[1] 이를 시작으로 안전성과 효율성을 높이기 위한 연구가 계속되어왔다. 초기의 원격 사용자 인증 기법은 서버에서 검증 테이블을 저장하는 방식을 사용

* 정 회 원 : 호서대학교 정보보호학과 석사과정
blr83@nate.com
** 정 회 원 : 호서대학교 정보보호학과 석사과정
kke0805@nate.com
*** 종신회원 : 호서대학교 정보보호학과 부교수
jcha@hoseo.edu(교신 저자)
[2009/02/18 투고 - 2009/02/20 심사(2009/06/18 2차) - 2009/7/31 심사완료]

하였다[2, 3]. 그러나 공격자가 이 검증 테이블을 알게 될 경우 시스템을 공격할 수 있는 취약점이 발견하였고, 그 후에 이런 취약점을 해결하기 위해 서버에서 검증 테이블을 저장하지 않는 형태로 발전되었다[4-7].

패스워드와 스마트카드를 이용한 원격 사용자 인증 기법은 1991년 Chang과 Wu가 제안한 이후로 활발한 연구가 진행되었으며[8], 2000년에는 Hwang 등이 ElGamal 암호시스템[9]을 기반으로 한 새로운 인증 기법을 제안하였다[10]. 그러나 이 기법은 공격자에 의해서 정당한 아이디와 패스워드 쌍을 쉽게 만들 수 있게 됨으로써 위장 공격이 가능한 취약점이 존재했고[11], 계산량이 많은 단점이 있었다. 이후 2002년에는 인증의 효율성을 높이기 위해 해쉬 함수를 기반으로 하는 인증 기법을 Sun이 제안하였고[12], 같은 해에 Chien 등은 Sun의 인증 기법이 상호 인증을 제공하지 못함과 사용자가 패스워드를 자유롭게 선택할 수 없는 취약점을 지적하고, 이를 해결할 수 있는 보다 효율적인 인증 기법을 제안하였다[13]. 그러나 Chien 등의 프로토콜은 공격자가 사용자의 패스워드가 없어도 정당한 사용자로 위장할 수 있다는 점이 Hsu에 의해 지적되었다[14].

이후 개인정보 보호와 프라이버시에 대한 중요성이 더욱 증대되면서 패스워드와 스마트카드를 이용한 원격 사용자 인증 방식은 사용자의 익명성을 제공할 수 있는 형태로 연구가 진행되었고, 2004년 Das 등은 동적 아이디를 사용하여 사용자 익명성을 제공하는 인증 기법을 처음으로 제안하였다[15]. 그러나 2005년 Chien 등은 Das 등의 인증 기법이 로그인 단계에서 서버로 전송되는 데이터를 통해 사용자를 구분할 수 있게 됨으로써 사용자의 익명성을 제대로 제공하지 못함을 지적하고, 이를 해결할 수 있는 방법을 제안하였다[16]. 하지만 Chien 등의 인증 기법도 내부자 공격(insider attack), 제한적 재전송 공격(restricted replay attack), 서비스 거부 공격(denial of service attack)에 취약함이 발견되었다[17].

본 논문에서는 Chien 등의 인증 기법의 취약점을 분석하며 이를 해결할 수 있는 효율적인 인증 기법을 제안한다. 여기에서는 물리적으로 안전한 특성(tamper-resistant)을 갖는 스마트카드를 이용하므로 사용자나 공격자가 스마트카드에 저장된 정보나 중간 계산 결과를 얻을 수 없다고 가정한다. 제안하는 인증 기법은 대칭 키 암호를 사용하여 사용자의 익명성을 제공하면서 사용자와 서버간의 안전한 상호 인증을 수행한다. 또한 패스워드 변경 단계를 추가하여 사용자가 자유롭게 패스워드를 변경할 수 있도록 설계하였다.

2. 표기 및 관련연구

2.1 기호 및 표기

본 논문에서 원격 사용자 인증 프로토콜을 설명하는데 사용될 기호 및 표기를 정리하면 아래와 같다.

- U_i : 사용자 i
- PW_i : 사용자 i의 패스워드
- ID_i : 사용자 i의 아이디
- S : 서버
- $h(\cdot)$: 일방향 해쉬 함수
- $\oplus$: XOR 연산
- p : 1024-bit 소수
- g : 순환군 Z_p의 생성자
- T : 타임 스탬프(time stamp)
- x : 서버의 long-term 비밀 키
- r_u, r_s : 랜덤 수
- SK_{us} : 세션 키
- $E_k[X]$: 대칭 키 k를 사용한 X의 암호문

2.2 관련 연구

이 절에서는 본 논문과 관련된 연구들을 살펴본다. 패스워드와 스마트 카드를 이용한 원격 사용자 인증 기법은 Chang과 Wu가 처음 제안하였고[8], 2000년에 Hwang 등은 ElGamal 암호시스템을 기반으로 한 새로운 인증 기법을 제안하였다[10]. 이 기법은 ElGamal 암호시스템[9]을 이용하여 아이디와 패스워드 쌍을 만들어 사용한다. 이 기법은 사용자가 패스워드를 자유롭게 선택하고 변경할 수 있지만 공격자가 아이디와 패스워드 쌍을 쉽게 만들 수 있기 때문에 위장 공격이 가능한 취약점을 가지고 있고, 계산량이 많은 단점이 있다. 같은 해 Sun이 이러한 문제점을 지적하고 일방향 해쉬 함수를 기반으로 하는 효율적인 인증 기법을 제안하였다[12]. 이 기법은 해쉬 함수만을 사용함으로써 연산량이 적은 장점이 있지만 Chien 등에 의해서 상호 인증을 제공하지 못한다는 취약점이 발견되었다[13].

이후에 개인정보 보호와 프라이버시에 대한 관심이 높아지면서 사용자의 익명성을 보장할 수 있는 새로운 관점의 인증 기법을 2004년 Das 등이 처음 제안하였다[15]. 이 기법은 매 인증 시 사용자의 아이디를 변경하는 동적 아이디 방식을 사용하였고, 일방향 해쉬 함수를 기반으로 하여 효율적인 장점이 있지만 전송되는 데이터를 통해 사용자를 구분할 수 있게 됨으로써 익명성을 제공하지만 사용자에 대한 추적이 가능한 취약점이 발견되었다. 2005년에 Chien 등은 이러한 취약점을 해결할 수 있는 방법을 제안 하였다[16]. 이 기법은 대칭키 암호를 이용하여 사용자의 아이디와 비밀 정보들을 암호화 하여 보냄으로써 사용자의 익명성을 보장하는 방법을 제안하였다. 그러나 내부자 공격과 제한된 재전송 공격 등의 취약점이 지적되었고, 2007년에 Hu 등이 Chien 기법의 취약점을 해결할 수 있는 향상된 인증 기법을 제안하였다. 이 기법은 타임 스탬프를 사용하지 않고, 카운터를 사용하여 제한된 재전송 공격을 방지하였고, Nonce 값을 이용하여 내부자 공격을 방지하였다.

본 논문에서는 Chien 등이 제안한 인증 기법의 취약점을 분석하고 이를 해결할 수 있는 향상된 인증 기법을 제안한다.

3. Chien 등의 익명성 제공 인증 기법

이 장에서는 Chien 등의 인증 기법에 대해서 알아보고, 그에 대한 안전성을 분석해 본다.

3.1 Chien 등의 인증 기법

패스워드와 스마트카드를 이용한 원격 사용자 인증 방식은 초기에는 단순히 상호 인증만 수행하다가 개인정보 보호 및 프라이버시 문제가 대두되면서 통신 채널상에서 사용자의 익명성을 제공할 수 있는 방향으로 연구되었다. 사용자 익명성을 제공하는 인증 기법으로서 2004년 Das 등은 동적 아이디를 사용하는 형태로 처음 제안되었다[15]. 그 후 Chien 등은 Das 등의 인증 기법이 사용자의 익명성을 제대로 제공하지 못함을 지적하고, 이를 해결할 수 있는 방법을 제안하였다[16]. 본 절에서는 Chien 등의 인증 기법이 내부자 공격, 제한적 재전송 공격, 서비스 거부 공격에 취약함을 자세히 설명하고자 한다. Chien 등의 인증 기법은 크게 등록 단계, 로그인 단계, 검증 단계로 구성되어 있으며 이를 도시한 것이 그림 1이다.

■ 등록 단계

① 사용자 U_i는 ID_i와 PW_i를 원격 서버에 제공한다.

② 서버 S는 $m = h(ID_i \oplus x) \oplus h(x) \oplus PW_i$와 $I = h(ID_i \oplus x)$를 계산한 후,

m, I, p, $h(\cdot)$를 스마트카드에 저장하여 사용자에게 발급한다.

■ 로그인 단계

로그인 단계에서 사용자 U_i는 스마트카드를 리더기에 삽입하고, 자신의 ID_i와 PW_i를 입력한다.

① 스마트카드는 랜덤 수 $r_u = g^a \bmod p$를 생성하고, $M = m \oplus PW_i$, $C = M \oplus r_u$, $R = I \oplus r_u$를 순서대로 계산한 후, R을 이용하여 r_u, ID_i, T를 암호화한다.

② 사용자는 메시지 $\{C, T, E_R[r_u, ID_i, T]\}$를 서버 S에게 전송한다.

■ 검증 단계

① 서버 S는 메시지를 수신하고 $R = C \oplus h(x)$를 계산하여 암호화된 메시지 $E_R[r_u, ID_i, T]$를 복호화 한다. 그리고 서버는 $\triangle T \geq T' - T$ 를 계산하여 타임 스탬프를 확인한다. 시차 확인이 되면 $R = h(ID_i \oplus x) \oplus r_u$를 계산하여 R 값을 검증한다. 만약 값이 다르면 서비스 요청을 거부한다.

② 서버 S는 $r_s = g^b \bmod p$를 계산한 후, R을 이용하여 $r_s, r_u + 1$을 암호화한다.

③ 서버 S는 메시지 $E_R[r_s, r_u + 1]$을 사용자에게 전송한다. 그리고 사용자와의 공통 세션 키 $SK_{su} = r_u^b = g^{ab}$를 계산해 둔다.

사용자		원격 서버
등록 단계		
ID_i, PW_i	ID_i, PW_i ⟶	$m = h(ID_i \oplus x) \oplus h(x) \oplus PW_i$ $I = h(ID_i \oplus x)$
	⟵ *smart card*	Store m, I, p, $h(\cdot)$ in smart card
로그인 단계		
$r_u = g^a \bmod p$ $M = m \oplus PW_i$ $C = M \oplus r_u$ $R = I \oplus r_u$	$\{C, T, E_R[r_u, ID_i, T]\}$ ⟶	
검증 단계		
		$R = C \oplus h(x)$ Decrypt $E_R[r_u, ID_i, T]$ Check $\triangle T \geq T' - T$ Check $R = ?\, h(ID_i \oplus x) \oplus r_u$
Decrypt $E_R[r_s, r_u + 1]$	$E_R[r_s, r_u + 1]$ ⟵	$r_s = g^b \bmod p$
Check $r_u + 1$ $SK_{su} = r_u^b = g^{ab}$		$SK_{su} = r_u^b = g^{ab}$

(그림 1) Chien 등의 인증 기법

④ 사용자 U_i는 메시지를 수신하여 $E_R[r_s, r_u+1]$을 복호화하여 r_u+1을 확인한다. 검증이 통과되면 세션 키 $SK_{us} = r_s^a = g^{ab}$를 계산할 수 있고, 이 세션 키를 이용하여 비밀 정보를 서버 S에게 암호화하여 전송할 수 있다.

3.2 취약점 분석

Chien 등의 인증 기법을 다음과 같은 취약점을 가지고 있다[17].

1) 내부자 공격(insider attack)

등록 단계에서 사용자의 패스워드 PW_i는 안전한 채널로 전송되지만 서버의 내부자에게 노출된다. 만약 사용자들이 편의를 위해서 다른 서버의 서비스를 이용할 때도 같은 아이디나 패스워드를 사용한다면, 악의적인 서버의 내부자가 사용자의 아이디나 패스워드를 이용해서 그 사용자로 위장하여 다른 서버로 접속을 시도할 수 있다. Chien 등의 인증 방식에서는 사용자의 패스워드가 등록 단계에서 서버로 전송되므로 내부자 공격에 취약하다.

2) 서비스 거부 공격(denial of service attack)

Chien 등의 인증 기법은 타임 스탬프를 이용하여 요청 메시지의 정당성을 보증한다. 만약 공격자가 서버로 가는 요청 메시지를 차단한다면, 일정 시간이 지난 다음에 사용자는 요청 메시지를 서버에게 재전송하게 된다. 그런데 재전송되는 요청 메시지는 새로운 타임 스탬프를 사용하는 것이 아닌 이전에 보낸 요청 메시지를 다시 보내는 것이기 때문에 타임 스탬프 T가 예상된 지연 시간을 초과하게 되므로 서버의 예상된 지연 시간 체크에서 통과될 수 없게 된다. 따라서 서비스 거부 공격으로 인해 일정한 시간만큼 처리 지체가 발생하면 합법적인 사용자에 대한 시간 검증 처리가 자동으로 지연되고 연속적인 서비스를 제공할 수가 없게 된다.

3) 제한적 재전송 공격(restricted replay attack)

공격자는 로그인 단계의 요청 메시지 $\{C, T, E_R[r_u, ID_i, T]\}$를 가로채서 마치 사용자인 것처럼 다시 서버로 전송한다. 이 때, 서버는 $\triangle T \geq T' - T$이 되는 한 로그인 요청을 무조건 받아들일 것이다. 그러므로 공격자는 $\triangle T$시간이내에서는 재전송 공격이 가능하다[18]. 여기서 T'은 서버가 메시지를 수신했을 때 타임 스탬프이고, $\triangle T$는 전송 지연이 예상되는 적합한 시간 간격이다.

이와 더불어 Chien 등의 인증 기법의 효율성을 분석해 볼 필요가 있다. 먼저 이 방식에서는 Diffie-Hellman의 키 교환 방식을 이용하여 세션 키를 공유하지만, 이 경우 스마트 카드내에 멱승 연산 기능이 필요하고 이는 해쉬 연산이나 암호 연산에 비해 계산량이 많아 매우 비효율적일 수 밖에 없다.

또한, 스마트카드내에서 서버와 동일한 타임 스탬프를 유지해야 하는데 이것은 현실적인 측면을 고려하면 쉬운 가정이 아니다. 즉, 타임 스탬프를 유지하기 위해서는 스마트카드에 항상 전원이 공급되거나 리더기로부터 이 정보를 읽어와야 하는데 리더기 역시 다른 시스템으로부터 타임 스탬프를 가져와야 한다. 따라서 스마트 카드내에서 서버와 동일한 타임 스탬프를 유지하는 것은 현실적으로 매우 어렵고 이를 타 시스템으로부터 받아오는 것도 새로운 위협 요소가 될 수 있다.

4. 익명성을 제공하는 효율적인 인증 기법

이 장에서는 Chien 등의 인증 기법의 취약점을 극복할 수 있는 더 효율적인 인증 기법을 제안한다. 제안 기법은 물리적 공격에 강인한(tamper-resistant) 스마트카드를 사용하므

로 스마트카드 내부의 비밀 정보는 읽을 수 없음을 가정한다. 제안 방식은 Chien 등의 인증 기법에 적용되던 내부자 공격, 제한적 재전송 공격 그리고 서비스 거부 공격 등을 방지하고, 안전한 상호 인증을 수행할 수 있다. 더불어 패스워드 변경 단계를 추가함으로써 사용자가 자유롭게 패스워드를 선택하여 변경할 수 있도록 개선하였다. 제안 기법은 등록 단계, 로그인 단계, 검증 단계 그리고 패스워드 변경 단계로 구성된다.

■ 등록 단계

① 사용자는 ID_i와 PW_i를 선택하고 N을 생성하여 $HPW_i = h(PW_i \oplus N)$을 계산한 후, ID_i와 HPW_i를 서버에게 전송한다.

② 서버는 $m = h(ID_i) \oplus h(x) \oplus HPW_i$와 $M = h(ID_i) \oplus h(x)$를 계산하고, ID_i, m, M, $h(\cdot)$를 스마트카드에 저장하여 사용자에게 발급한다.

③ 사용자는 스마트카드에 N을 입력한다.

■ 로그인 단계

사용자는 스마트카드를 리더기에 삽입하고, 자신의 ID_i와 PW_i를 입력한다.

① 스마트카드는 $M \oplus h(PW_i \oplus N)$를 계산한 후 패스워드가 제대로 입력되었는지 m과 비교하여 확인한다. 확인이 되면 랜덤 수 r_u를 생성하여 $C = M \oplus r_u$, $R = h(ID_i) \oplus r_u$를 순서

사용자		원격 서버
등록 단계		
ID_i, PW_i, $nonce\ N$ $HPW_i = h(PW_i \oplus N)$ Store N in smart card	ID_i, HPW_i ⟶ $smart\ card$ ⟵	$m = h(ID_i) \oplus h(x) \oplus HPW_i$ $M = h(ID_i) \oplus h(x)$ Store ID_i, m, M, $h(\cdot)$ in smart card
로그인 단계		
Check $m\ ? = M \oplus h(PW_i \oplus N)$ $C = M \oplus r_u$ $R = h(ID_i) \oplus r_u$	$\{C, E_R[r_u, ID_i]\}$ ⟶	
검증 단계		
		$R = C \oplus h(x)$ Decrypt $E_R[r_u, ID_i]$ Check $R\ ? = h(ID_i) \oplus r_u$ Generate r_s
Decrypt $E_R[r_s, r_u + 1]$ Check $r_u + 1$	$E_R[r_s, r_u + 1]$ ⟵	
	$E_R[r_s + 1]$ ⟶	Decrypt $E_R[r_s + 1]$ Check $r_s + 1$
$SK_{us} = r_u \oplus r_s$		$SK_{us} = r_u \oplus r_s$

(그림 2) 제안하는 익명성 제공 인증 기법

대로 계산한 후, R을 이용하여 r_u, ID_i를 암호화한다.

② 메시지 $\{C, E_R[r_u, ID_i]\}$를 서버에게 전송한다.

■ 검증 단계

① 서버는 메시지를 수신하여 $R = C \oplus h(x)$를 계산하여 암호화된 메시지 $E_R[r_u, ID_i]$를 복호화한 후, $h(ID_i) \oplus r_u$를 계산하여 R과 같은지 검증한다. 만약 값이 다르면 서비스 요청을 거부한다.

② 서버는 랜덤 수 r_s를 생성한 후, R을 이용하여 $r_s, r_u + 1$을 암호화한다. 서버는 메시지 $E_R[r_s, r_u + 1]$을 사용자에게 전송한다.

③ 사용자는 수신한 메시지 $E_R[r_s, r_u + 1]$을 복호화하여 $r_u + 1$을 확인함으로써 서버를 인증하고, 세션 키 $SK_{us} = r_u \oplus r_s$를 계산한다. 그런 다음 사용자는 R을 이용하여 $r_s + 1$를 암호화한 후, $E_R[r_s + 1]$를 서버에게 전송한다.

④ 서버는 수신한 메시지 $E_R[r_s + 1]$을 복호화 하여 $r_s + 1$을 확인함으로써 사용자를 인증하고, 세션 키 $SK_{us} = r_u \oplus r_s$를 계산한다.

■ 패스워드 변경 단계

사용자는 스마트카드를 리더기에 삽입하고, 자신의 PW_i를 입력한다.

① 스마트카드는 $M \oplus h(PW_i \oplus N)$를 계산한 후 패스워드가 제대로 입력되었는지 m과 비교하여 확인한다. 확인이 되면 사용자는 새로운 패스워드 PW_i'를 입력한다.

② 스마트카드는 다음을 계산하여 기존의 m을 m^*로 교체한다.

$$m^* = m \oplus h(PW_i \oplus N) \oplus h(PW_i' \oplus N)$$

제안 방식에서는 내부자 공격에 방어될 수 있도록 등록 단계에서 패스워드를 그대로 서버에 전송하는 것이 아니라 $HPW_i = h(PW_i \oplus N)$와 같이 해쉬 연산을 수행한 후 보내지게 된다. 이 경우 서버의 내부자는 패스워드를 추측할 수 없게 된다. 그런데 이러한 방식의 불편한 점은 사용자가 일회용 랜덤 수 N을 기록하였다가 스마트카드를 발급받은 후 이를 저장하는 과정이 필요하다는 것이다.

만약 사용자가 N을 기록할 수 없을 경우 N을 저장하는 간단한 방법은 임시 패스워드 $TempPW$를 생성한 후 $E_{TempPW}(N)$로 암호화하여 서버로 전송한다. 서버는 카드를 발급할 때 $E_{TempPW}(N)$를 그대로 스마트카드에 저장한다. 사용자는 발급받은 카드에서 $E_{TempPW}(N)$를 복호화한 후 N을 스마트카드에 저장하도록 하면 된다. 이 경우에도 공격자가 PW_i와 $TempPW$를 동시에 추측할 수 있으면 내부자 추측 공격이 가능할 수도 있으므로 $TempPW$는 비교적 기억이 가능한 긴 문장(string)을 해쉬하여 $TempPW = h(string)$와 같이 사용하면 내부자에 의한 패스워드 추측을 방어할 수 있다.

제안 방식이 Chien 등의 인증 기법과 다른 하나는 타임 스탬프를 이용하지 않는다는 점이다. 사실 Chien 등의 인증에서는 타임 스탬프를 통해 재전송 공격을 방어한다고 할 수 있다. 즉, 서버에서는 적절한 타임안에 수신된 정보만 올바른 정보로 수용할 수 있도록 하여 재전송 공격을 방어하도록 하였다. 그러나 제안 방식에서는 타임 스탬프를 사용하지 않으면서 재전송 공격에 방어되도록 설계하였다. 이러한 이유로 인해 Chien 등의 기법의 검증

과정은 1-pass만으로 이루어져 있지만 제안 방식에서는 2-pass 형태로 검증을 수행함으로써 상호 인증을 수행한다. 즉, 서버는 사용자에게 자신이 보내는 시도(challenge) r_s에 대해 정확한 응답(response) r_s+1을 정해진 내에 확인할 수 있는지를 검사하여 재전송 공격을 방어하게 된다. 이 과정에서 Chien 등의 검증 과정보다 1-pass가 더 늘어나게 된다.

5. 안전성 및 효율성 분석

이 장에서는 제안 기법의 안전성과 효율성을 분석한다. 단, 본 논문에서는 tamper-resistant한 스마트카드를 사용하므로 사용자 혹은 공격자가 스마트카드에 저장된 정보나 중간 계산 결과를 얻을 수 없다고 가정한다.

5.1 안전성 분석

제안 방식의 안전성을 분석하여 타 방식과 비교하여 정리한 것이 표 1이다.

(표 1) 안전성 분석

구 분	Hwang et al. [10]	Das et al. [15]	Chien et al. [16]	Hu et al. [17]	제안 방식
사용자 익명성	no	no	yes	yes	yes
내부자 공격	no	no	no	yes	yes
서비스 거부 공격	no	no	no	no	yes
제한적 재전송 공격	no	no	no	yes	yes
서버/사용자 위장 공격	no	yes	yes	yes	yes
도난된 검증자 공격	yes	yes	yes	yes	yes

1) 사용자 익명성

로그인 단계에서 사용자의 ID_i는 비밀 키 R을 사용하여 암호화된 메시지로 전송된다. 이 때 비밀 키 R은 서버의 비밀 값인 x를 알아야 얻을 수 있으므로 서버만이 암호화된 메시지를 볼 수 있으며 제 3자가 암호화된 메시지를 복호화할 수가 없다. 따라서 제안 기법은 제 3자에 대해 사용자의 익명성을 제공할 수 있다.

2) 내부자 공격

등록 단계에서 PW_i대신 HPW_i를 서버에게 전송하므로 해쉬 함수의 일방향성에 의해 서버의 내부자가 HPW_i를 이용해서 PW_i를 추출할 수 없다. 또한, 랜덤 수 N은 사용자만 알고 있는 정보로서 서버의 내부자는 이 값을 알 수 없으므로 제안 기법은 오프라인(off-line) 패스워드 추측 공격에도 안전하다.

3) 서비스 거부 공격

제안 기법에서는 타임 스탬프를 사용하지 않으므로 Chien 등의 기법에서 적용되었던 타임 스탬프를 이용한 서비스 거부 공격에 안전하다. 즉, 제안 방식은 일정한 시간이 지난 후 시간을 검사하는 방법이 아니므로 일정한 시간 지체가 있다 하더라도 합법적인 사용자에 대한 서비스를 순차적으로 처리해 줄 수 있다.

4) 재전송 공격

제안 기법에서는 매 로그인마다 랜덤 수 r_u, r_s를 생성하므로 공격자가 이전 세션에서 사용된 메시지를 이용하여 재전송 공격을 하는 것이 불가능하다. 만약 공격자가 로그인 단계에서 요청 메시지 $\{C, E_R[r_u, ID_i]\}$를 가로채 재전송하더라도 공격자는 랜덤 수 r_u, r_s

를 모르기 때문에 검증 단계에서 사용자 인증 메시지인 $E_R[r_s+1]$를 계산할 수 없으므로 인증 과정을 통과할 수 없다. 또한 $\{C, E_R[r_u, ID_i]\}$와 $E_R[r_s+1]$ 쌍을 가로채서 재전송하더라도 이 때 서버에서 생성한 랜덤 수 r_s와 재전송한 메시지 쌍의 r_s가 다르므로 인증을 통과할 수 없다. 또한 제안 기법은 타임 스탬프를 사용하지 않으므로 Chien 등의 기법에서 취약점이었던 제한적 재전송 공격에 대해서도 안전하다.

5) 서버/사용자 위장(masquerading) 공격

공격자가 서버 혹은 사용자로 위장하기 위해서는 로그인 단계에서 요청 메시지 $\{C, E_R[r_u, ID_i]\}$나 상호 인증을 위한 메시지 $E_R[r_s, r_u+1]$, $E_R[r_s+1]$를 계산할 수 있어야 한다. 따라서 공격자는 위의 메시지들을 계산하기 위해 필요한 비밀 값 x, r_u, r_s, PW_i, N 들을 얻을 수 있어야 한다. 그런데 스마트카드에 저장된 정보를 추출할 수가 없으며, 통신상의 메시지를 가로채더라도 비밀 값 x를 알 수 없으므로 암호에 사용된 비밀 키 R을 얻을 수 없게 되어 암호화된 정보를 복호화할 수가 없다. 따라서 제안 기법에서는 공격자가 서버 혹은 사용자로 위장하기 위해 필요한 비밀 값들을 얻을 수가 없으므로 서버/사용자 위장 공격에 안전하다.

5.2 효율성 분석

관련된 인증 기법과 제안 기법의 효율성을 비교 분석하여 이를 정리한 것이 표 2이다. 단, 여기서 XOR 연산량은 해쉬나 암·복호, 멱승 함수 연산량에 비해 무시할만큼 적어 표시하지 않았다.

(표 2) 효율성 분석

구 분	로그인 단계		검증 단계	
	사용자	서버	사용자	서버
Hwang et al. [10]	3E, 1H	-	-	3E, 1H
Das et al. [15]	5H	-	-	3H
Chien et al. [16]	1E, 1S	-	1S, 1E	2H, 2S, 2E
Hu et al. [17]	1E, 2H, 1S	-	1S, 1E	3H, 2S, 2E
제안 방식	2H, 1S	-	2S	2H, 3S

E : 지수 연산
H : 해쉬 연산
S : 대칭키 암호화/복호화

표 2에서 볼 수 있듯이 제안한 기법에서는 로그인 단계에서 2번의 해쉬 연산 그리고 1번의 암호화 연산이 필요하며 인증 단계에서는 사용자가 2번의 암호화/복호화 연산, 서버가 2번의 해쉬 연산과 3번의 암호화/복호화 연산이 필요하다.

이러한 결과는 Das 등의 방법보다는 많은 연산이 필요하지만 Hwang 등의 방식, Chien 등의 방식 그리고 Hu 등의 방식보다는 훨씬 연산량이 적다. 그 이유는 타 방식에서 세션 키 분배 등에 Diffie-Hellman의 키 교환 방식을 사용하게 되는데 이때 사용하는 멱승 연산은 해쉬나 암·복호 연산에 비해 시간이 많이 소요된다. 또한 Hwang 등도 ElGamal 암호시스템을 사용함으로써 멱승 연산이 많다. Das 등은 해쉬 함수만으로 구현되어 계산량 측면에서는 효율적이지만 앞서 언급한 바와 같이 안전성에서는 매우 취약하다.

효율성 증가를 사용자와 서버측 관점을 나누어 볼 필요가 있는데 일반적으로 서버의 용량이나 성능은 뛰어난 반면, 사용자는 스마트카드를 이용하게 되므로 사용자 측에서 연산량이 적은 것이 더 효율적이다. 그러나 제안한 기법에서는 사용자나 서버 모두 멱승 연산을 수행하지 않기 때문에 인증 프로토콜은 전체적으로 효율적임을 알 수 있다. 다만,

Hwang이나 Das 등의 기법과 비교해 볼 때 검증 단계에서는 사용자측에서는 2번의 암호화/복호화 연산이 필요하다. 그 이유는 Hwang이나 Das 등의 방법에서는 사용자 일방향 인증을 제공하는 반면, 제안한 기법에서는 상호 인증을 제공하기 위해 사용자의 연산이 추가되기 때문이다.

6. 결 론

본 논문에서는 Chien 등의 인증 기법의 취약점을 해결할 수 있는 패스워드와 스마트카드를 이용한 효율적인 원격 사용자 인증 기법을 제안하였다. 제안한 기법은 타임 스탬프를 사용하지 않고 랜덤 수를 이용하여 서비스 거부 공격과 제한적 재전송 공격을 방지하고, 안전한 상호 인증을 수행한다. 또한 서버가 패스워드를 추측하는 것을 방지하므로 내부자 공격에도 강인한 특성을 가진다. 이와 더불어 패스워드 변경 단계를 추가하여 사용자가 자유롭게 패스워드를 선택하여 변경할 수 있도록 하였다. 결국, 제안 방식은 통신로 상에서 사용자의 익명성을 보장하면서 패스워드와 스마트카드를 이용하는 원격 사용자 인증시스템에 효과적으로 사용할 수 있다.

참 고 문 헌

[1] L. Lamport, "Password authentication with insecure communications," Communication. of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[2] T. Y. Hwang, "Passwords Authentication Using Public-Key Encryption," Proc. of international Carnahan Conference on Security Technology, pp. 35-38, 1983.

[3] C. S. Laih, L. Harn, D. Huang, "Password authentication using quadratic residues," Proceedings of International Computer Symposium, pp. 1478-1483, 1988.

[4] T. Hwang, Y. Chen, and C.S. Laih, "Non-interactive password authentications without password tables," IEEE Region 10 Conference on Computer and Communication Systems, IEEE Computer Society, pp. 429-431, 1990.

[5] S. J. Wang, J. F. Chang, "Smart card based secure password authentication scheme," Computers and Security, Vol. 15 No. 3 pp. 231-237, 1996.

[6] W. H. Yang, S. P. Shieh, "Password authentication schemes with smart cards," Computers and Security, Vol. 18 No. 8, pp. 727-733, 1999.

[7] C. C. Lee, M. S. Hwang, W. P. Yang, "A flexible remote user authentication scheme using smart cards," ACM Operating Systems Review, Vol. 36 No. 4 pp. 23-29, 2002.

[8] C. C. Chang, T. C. Wu, "Remote password authentication with smart cards," IEE Proceedings-Computers and Digital Techniques, Vol. 138 No. 3, pp. 165-168, 1991.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, Vol. IT-31, pp. 469-472, 1985.

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

[11] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp. 992-993, Nov. 2000.

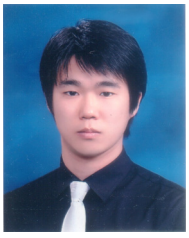
[12] H. M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Trans. On Consumer Electronics, Vol. 46, No. 4, pp. 958-961, 2000.

[13] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An

efficient and practical solution to remote authentication: Smart Card," Computers and Security, Vol. 21, No. 4, pp. 372-375, 2002.
[14] C. L. Hsu "Security of two remote authentication schemes using smart cards," IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp. 1196-1198, 2003.
[15] 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, May 2004.
[16] H. Y Chien, C. H. Chen. "A remote authentication scheme preserving user anonymity," IEEE AINA'05, Vol. 2, pp. 245-248, March 2005.
[17] L. Hu, Y. Yang, X. Niu. "Improved remote user authentication scheme preserving anonymity," Fifth Annual Conference on Communication Network and Services Research(CNSR), pp. 323-328, 2007.
[18] L. Gong, "A security risk of depending on synchronized clocks," Operating Systems Review, Vol. 26, No. 1, pp. 49-53, 1992.

◐ 저 자 소 개 ◑

백 이 루 (YiRoo Baek)
2008년 : 호서대학교 정보보호학과 (공학사)
2008년 ~ 현재 : 호서대학교 대학원 정보보호학과(석사과정)
관심분야 : 네트워크 보안, 프로토콜, 암호 알고리듬
E-mail : blr83@nate.com



길 광 은 (KwangEun Gil)
2008년 : 호서대학교 정보보호학과 (공학사)
2008년 ~ 현재 : 호서대학교 대학원 정보보호학과(석사과정)
관심분야 : 네트워크 보안, 프로토콜, 암호 알고리듬
E-mail : kke0805@nate.com

하 재 철 (JaeCheol Ha)
1989년 경북대학교 전자공학과 졸업
1993년 경북대학교 전자공학과 석사
1998년 경북대학교 전자공학과 박사
1998년~2006년 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년~2007년 나사렛대학교 정보통신학과 부교수
2006년~2006년 QUT in Australia 연구 교수
2007년~현재 : 호서대학교 정보호호학과 부교수
2002년~현재 : 한국정보보호학회 이사, 논문지 편집위원
2008년~현재 : 한국인터넷정보학회 논문지 편집위원
E-mail : jcha@hoseo.edu