한국산학기술학회논문지
Vol. 10, No. 10, pp. 2750-2759, 2009

제 3자에게 사용자 익명성을 제공하는 스마트 카드 기반 원격 인증 시스템 구현

백이루[1], 오두환[1], 길광은[1], 하재철[1*]
[1]호서대학교 정보보호학과

Implementation of a Remote Authentication System Using Smartcards to Guarantee User Anonymity to Third Party

Yi-Roo Baek[1], Doo-Hwan Oh[1], Kwang-Eun Gil[1] and Jae-Cheol Ha[1*]
[1]Dept. of Information Security, Hoseo University

요 약 본 논문은 2008년 Bindu 등이 제안한 프로토콜의 취약점을 분석하고, 이를 해결할 수 있는 향상된 프로토콜을 제안한다. 제안한 프로토콜은 안전성면에서 타임 스탬프를 사용하지 않고 랜덤 수를 사용하여 제한된 재전송 공격과 서비스 거부 공격을 방지할 수 있다. 이와 더불어 사용자의 ID 정보를 AES로 암호화하여 전송함으로써 사용자의 익명성을 제공하였다. 또한, 멱승 연산을 제거하고 사용자가 자유롭게 패스워드를 변경할 수 있는 패스워드 변경 단계를 추가하여 프로토콜의 효율성을 높였다. 논문에서는 제안한 프로토콜을 STM 스마트 카드에 직접 구현하고 인증 서버를 설치하여 그 동작이 정확하고 효율적임을 검증하였다.

Abstract In this paper, we analyze vulnerabilities in a remote authentication protocol using smartcards which was proposed by Bindu et al. and propose an improved scheme. The proposed scheme can prevent from restricted replay attack and denial of service attack by replacing time stamp with random number. In addition, this protocol can guarantee user anonymity by transmitting encrypted user's ID using AES cipher algorithm. The computational load in our protocol is decreased by removing heavy exponentiation operations and user efficiency is enhanced due to addition of password change phase in which a user can freely change his password. Furthermore, we really implement the proposed authentication protocol using a STM smartcard and authentication server. Then we prove the correctness and effectiveness of the proposed remote authentication system.

Key Words : Smart Card, Remote Authentication Protocol, Password, User Anonymity

1. 서론

네트워크의 발전과 함께 분산된 컴퓨팅 환경에서 원격 서버로 접근하는 일이 빈번해짐에 따라 원격 사용자 인증이 매우 중요한 요소가 되었다. 원격 사용자 인증을 위해 네트워크상에서 주고받는 데이터가 악의적인 공격자로 인한 도청될 수도 있고 변조와 같은 공격이 발생함에 따라 네트워크상에서 사용자와 원격 서버간의 원격 사용자 인증 기법들이 많이 연구되었다. 원격 사용자 인증 기법은 1981년 Lampord에 의해 처음 제안되었다[1]. 초기의 원격 사용자 인증 기법은 서버에서 검증 테이블을 저장하는 방식을 사용하였다[2]. 그러나 공격자가 이 검증 테이블을 알게 될 경우 시스템을 공격할 수 있는 취약점이 발견되었고, 그 후에 이런 취약점을 해결하기 위해 서버에서 검증 테이블을 유지하지 않는 형태로 발전되었다[3-5].

패스워드와 스마트 카드를 이용한 원격 사용자 인증 기법은 1991년 Chang과 Wu가 처음으로 제안하였으며

*교신저자 : 하재철(jcha@hoseo.edu)
접수일 09년 07월 13일 수정일 (1차 09년 09월 29일, 2차 09년 10월 12일) 게재 확정일 09년 10월 14일

[6], 그 이후 많은 연구가 진행되었다. 2000년에는 Hwang 등이 ElGamal 암호시스템[7]을 기반으로 한 새로운 인증 기법을 제안하였고[8], 2002년에는 인증의 효율성을 높이기 위해 해쉬 함수를 기반으로 하는 인증 기법을 Sun이 제안하였다[9]. 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[10]. 논문에서는 물리적으로 안전한 특성(tamper-resistant)을 갖는 스마트 카드를 이용하므로 사용자나 공격자가 스마트 카드에 저장된 정보나 중간 계산 결과를 얻을 수 없다고 가정한다.

최근 개인정보 보호와 프라이버시에 대한 중요성이 증대되면서 원격 사용자 인증 방식은 사용자의 익명성을 제공할 수 있는 형태로 연구가 진행되었다. 2004년 Das 등은 동적 아이디를 사용하여 사용자 익명성을 제공하는 인증 기법을 처음으로 제안하였고[11], 2005년 Chien 등은 Das 등의 인증 기법이 로그인 단계에서 사용자의 익명성을 제대로 제공하지 못함을 지적하고, 이를 해결할 수 있는 방법을 제안하였다[12]. 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[13]. 사용자 익명성을 제공하는 가장 최근의 연구결과로는 2008년에 Bindu 등이 Chien 등의 인증 기법이 내부자 공격과 중간자 공격에 취약함을 지적하고 이를 해결할 수 있는 인증 기법을 제안하였다[14].

본 논문에서는 Bindu 등의 인증 기법의 취약점을 분석하고, 이를 해결할 수 있는 효율적인 인증 기법을 제안한다. 제안하는 기법은 타임 스탬프 대신 랜덤 수를 사용하여 제한적 재전송 공격과 서비스 거부 공격을 방지하고, 멱승 연산을 제거하여 프로토콜의 효율성을 높였다. 또한 패스워드 변경 단계를 추가하여 사용자가 자유롭게 패스워드를 선택하여 변경할 수 있도록 하였으며 사용자의 ID 정보를 AES-128[15]로 암호화하여 전송함으로써 사용자의 익명성을 제공하였다. 또한 제안 프로토콜을 STM 스마트 카드에 구현하고 인증 서버를 설치하여 그 동작이 정확하고 효율적임을 검증하였다.

2. 익명성을 제공하는 기존 인증 기법

패스워드와 스마트 카드를 이용한 원격 사용자 인증 방식 중에서 사용자의 익명성을 제공하기 위해서는 전송되는 정보 중 사용자의 ID가 공격자에게 노출되지 않아야 한다. Das 등은 동적 아이디를 사용하여 사용자 익명성을 제공하는 방법을 제시하였으며[11] Chien 등은 Das 등의 인증 기법이 로그인 단계에서 사용자의 익명성을 제대로 제공하지 못함을 지적하고, 이를 해결할 수 있는 방법을 제안하였다[12]. 단, 여기서 익명성이란 서버조차도 사용자의 ID를 알지 못하는 경우의 익명성과 제 3자에게 사용자의 ID를 알지 못하는 경우의 익명성으로 나눌 수 있는데 본 논문에서의 익명성은 제 3자에게 사용자의 ID를 알지 못하는 경우로 제한하고자 한다. Bindu 등은 Chien 등의 인증 기법이 내부자 공격과 중간자 공격에 취약함을 지적하고 이를 해결할 수 있는 새로운 인증 기법을 제안하였다[14]. 최근에는 Bindo 등의 방식에서의 위장 공격의 위험성을 분석한 것[16]과 제 3자와의 중간 통신을 이용한 익명성 제공 방식[17]도 제안되기도 하였다. 따라서 본 장에서는 Bindu 등의 인증 기법을 분석하여 그 취약성을 도출해 내고자 한다. 이를 위해 사용되는 기호 및 표기를 정리하고 Bindu 등의 프로토콜 취약점을 분석해 본다.

2.1 기호 및 표기

본 논문에서 사용하는 기호 및 표기는 표 1과 같다.

[표 1] 기호 및 표기

기호	내 용
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 Bindu 등의 인증 기법

Bindu 등이 제안한 인증 기법은 등록 단계, 로그인 단계, 검증 단계로 구성되어 있다. 이를 나타낸 것이 그림 1이다.

사용자		원격 서버
등록 단계		
$ID_i,\ h(PW_i)$	$ID_i,\ h(PW_i)$ ----------▶	$m = h(ID_i \oplus x) \oplus h(x) \oplus h(PW_i)$ $I = h(ID_i \oplus x) \oplus x$
	◀---------- $smart\ card$	Store $ID_i, m, I, p, g, h(\cdot)$ in smart card
로그인 단계		
$r_u = g^a \bmod p$ $M = m \oplus h(PW_i)$ $C = M \oplus r_u$ $R = I \oplus r_u$ $E_R[r_u, ID_i, T_1]$	$\{C, T, E_R[r_u, ID_i, T_1]\}$ ----------▶	
검증 단계		
		$R = C \oplus h(x) \oplus x$ Decrypt $E_R[r_u, ID_i, T_1]$ Check $\triangle T \geq T' - T_1$ Check $R = ?h(ID_i \oplus x) \oplus x \oplus r_u$
	$E_R[r_s, r_u + 1, T_2]$	$r_s = g^b \bmod p$
Decrypt $E_R[r_s, r_u + 1, T_2]$	◀----------	$SK_{us} = r_u^b = g^{ab}$
Check $\triangle T \geq T' - T_2$		
Check $r_u + 1$	$E_{SK_{us}}[r_s + 1]$	
$SK_{us} = r_u^b = g^{ab}$	----------▶	Decrypt $E_{SK_{us}}[r_s + 1]$
$E_{SK_{us}}[r_s + 1]$		Check $r_s + 1$

[그림 1] Bindu 등의 인증 기법

[등록 단계]

① 사용자 U_i는 ID_i와 $h(PW_i)$를 원격 서버에 제공한다.

② 서버는 다음을 계산한 후, $ID_i, m, I, p, g, h(\cdot)$를 스마트 카드에 저장하여 사용자에게 발급한다.

$m = h(ID_i \oplus x) \oplus h(x) \oplus h(PW_i)$

$I = h(ID_i \oplus x) \oplus x$

[로그인 단계]

사용자 U_i는 스마트 카드를 리더기에 삽입하고, 자신의 ID_i와 PW_i를 입력한다.

① 스마트 카드는 랜덤 수 를 생성하고 다음 식을 순서대로 계산한 후, R을 이용하여 r_u, ID_i, T_1를 암호화한다.

$r_u = g^a \bmod p$

$M = m \oplus h(PW_i)$

$C = M \oplus r_u$

$R = I \oplus r_u$

② 사용자는 메시지 $\{C, T, E_R[r_u, ID_i, T_1]\}$를 서버 S에게 전송한다.

[검증 단계]

① 서버는 메시지를 수신하고 $R = C \oplus h(x) \oplus x$를 계산하여 암호화된 메시지 $E_R[r_u, ID_i, T_1]$를 복호화 한다. 그 다음 서버는 $\triangle T \geq T' - T_1$ 를 계산하여 타임 스탬프를 확인한 후 시차 확인이 되면

$R = h(ID_i \oplus x) \oplus x \oplus r_u$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 $r_s, r_u + 1, T_2$을 암호화한다.

③ 서버 S는 메시지 $E_R[r_s, r_u + 1, T_2]$을 사용자에게 전송한다. 그리고 사용자와의 공통 세션 키 $SK_{us} = r_u^b = g^{ab}$를 계산해 둔다.

④ 사용자 U_i는 메시지를 수신하여 $E_R[r_s, r_u + 1, T_2]$을 복호한 후 $\triangle T \geq T' - T_2$를 계산하고, 타임 스탬프를 확인한 후 시차 확인이 되면 $r_u + 1$을 확인한다. 검증이 통과되면 세션 키 $SK_{us} = r_s^a = g^{ab}$를 계산하고, $r_s + 1$을 세션 키 SK_{us}로 암호화하여 서버에게 전송한다.

⑤ 서버는 $E_{SK_{us}}[r_s + 1]$를 복호화하여 $r_s + 1$을 확인한다.

2.3 Bindu 등의 인증 기법에 대한 안전성 분석

이 절에서는 Bindu 등의 원격 인증 기법에 대한 안전성을 분석해 본다.

① 내부자 공격 (insider attack)

사용자는 패스워드를 일방향 해쉬 함수를 적용하여 전송하기 때문에 악의적인 서버 관리자나 내부자가 해쉬 값을 통해 패스워드를 추출할 수 없으므로 내부자 공격에 안전하다.

② 중간자 공격 (man-in-the-middle attack)

본 논문에서는 앞서 언급했듯이 물리적으로 안전한 스마트 카드의 사용을 가정하기 때문에 공격자가 스마트 카드 내부의 비밀 정보를 추출할 수 없으므로 암호화된 메시지를 복호화할 수 없다. 따라서 서버 위장 공격이나 사용자 위장 공격을 할 수 없으므로 중간자 공격에 안전하다.

③ 제한적 재전송 공격 (restricted replay attack)

네트워크의 발전과 함께 최근 공격 기법들은 거의 실시간으로 이루어짐에 따라서 타임 스탬프를 사용하는 시스템들은 제한된 재전송 공격이 큰 위협이 되고 있다. Bindu 등의 인증 기법에서 제한된 재전송 공격은 아래와 같이 수행될 수 있다.

공격자는 로그인 단계의 요청 메시지 $\{C, T, E_R[r_u, ID_i, T_1]\}$를 가로채서 마치 사용자인 것처럼 다시 서버로 전송한다. 이 때, 서버는 $\triangle T \geq T' - T_1$이 되는 한 로그인 요청을 무조건 받아들일 것이다. 그러므로 공격자는 $\triangle T$시간이내에서는 재전송 공격이 가능하다[18]. 따라서 Bindu 등의 인증 기법은 제한적 재전송 공격에 취약하다. 여기서 T'은 서버가 메시지를 수신했을 때 타임 스탬프이고, $\triangle T$는 전송 지연이 예상되는 적합한 시간 간격이다.

④ 서비스 거부 공격 (denial of service attack)

Bindu 등의 인증 기법은 타임 스탬프를 이용하여 요청 메시지의 정당성을 보증한다. Bindu 등의 인증 기법에서 서비스 거부 공격은 다음과 같이 수행될 수 있다. 만약 공격자가 서버로 가는 요청 메시지를 차단한다면, 일정 시간이 지난 다음에 사용자는 요청 메시지를 서버에게 재전송하게 된다. 재전송되는 요청 메시지는 새로운 타임 스탬프를 사용하는 것이 아닌 이전에 보낸 요청 메시지를 다시 보내는 것이기 때문에 타임 스탬프 T_1이 예상된 지연 시간을 초과하게 되므로 서버의 예상된 지연 시간 체크에서 통과될 수 없게 된다. 그런데 서버는 들어오는 메시지에 대해 무조건 복호를 수행해야 하므로 시간 체크 이전에 복호화 시간만큼 처리 지체가 발생하게 된다. 따라서 합법적인 사용자에 대한 시간 검증 처리가 지연됨으로써 정당한 사용자도 시간 체크에 걸려 서비스를 제공할 수가 없게 된다. 따라서 Bindu 등의 인증 기법은 서비스 거부 공격에 취약하다.

⑤ 사용자 익명성 (user anonymity)

Bindu 등의 인증 기법에서는 사용자의 ID가 암호화되어 전송되고, 공격자는 비밀키를 알지 못하므로 암호화된 메시지를 복호화 할 수 없다. 따라서 Bindu 등의 인증 기법은 사용자 익명성을 제공하지만 암호화 키를 생성하는 단계에서 멱승 연산이 사용되어 비효율적이다.

3. 제안하는 원격 사용자 인증 기법

이 장에서는 Bindu 등의 인증 기법의 취약점을 해결할

수 있는 향상된 인증 기법을 제안한다. 제안하는 인증 기법은 다음과 같은 특징을 가지고 있다.

첫째, 타임 스탬프 대신 랜덤 수를 사용하여 제한적 재전송 공격과 서비스 거부 공격을 방지할 수 있도록 하였다.

둘째, 스마트 카드나 서버쪽에서 많은 계산량이 필요한 Diffie-Helman의 키 일치(key agreement) 방식을 사용하지 않음으로써 멱승 연산을 제거하여 연산 효율성을 높였다.

셋째, 패스워드 변경 단계를 추가하여 사용자가 자유롭게 패스워드를 변경할 수 있도록 하였다.

넷째, 사용자의 익명성을 제공하기 위해서는 전송되는 ID 정보를 AES 암호 알고리듬을 이용하여 암호화하여 전송하였다.

제안하는 프로토콜은 다음과 같이 등록 단계, 로그인 단계, 검증 단계, 그리고 패스워드 변경 단계로 이루어져 있으며 패스워드 변경은 필요한 경우에만 수행한다.

[등록 단계]

① 사용자는 ID_i와 PW_i를 선택하고. $h(PW_i)$을 계산하여 ID_i와 $h(PW_i)$를 서버에게 전송한다.

② 서버는 다음을 계산하고, ID_i, m, M, $h(\cdot)$를 스마트 카드에 저장하여 사용자에게 발급한다.

$m = h(ID_i) \oplus h(x) \oplus h(PW_i)$

$M = h(ID_i) \oplus h(x)$

[로그인 단계]

사용자는 스마트 카드를 리더기에 삽입하고, 자신의 ID_i와 PW_i를 입력한다.

① 스마트 카드는 $M \oplus h(PW_i)$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 순서대로 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 계

사용자		원격 서버
등록 단계		
Select ID_i, PW_i $h(PW_i)$	ID_i, $h(PW_i)$ ----------▶ *smart card* ◀----------	$m = h(ID_i) \oplus h(x) \oplus h(PW_i)$ $M = h(ID_i) \oplus h(x)$ Store ID_i, m, M, $h(\cdot)$ in smart card
로그인 단계		
Check $m ? = M \oplus h(PW_i)$ Generate r_u $C = M \oplus r_u$ $R = h(ID_i) \oplus r_u$	$\{C, E_R[r_u, ID_i]\}$ ----------▶	
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 원격 사용자 인증 기법

산하여 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. 그 다음 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 다시 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 인증한 후 세션 키 $SK_{us} = r_u \oplus r_s$를 계산한다.

[패스워드 변경 단계]

사용자는 스마트 카드를 리더기에 삽입하고, 자신의 PW_i를 입력한다.

① 스마트 카드는 입력된 패스워드를 이용하여 $M \oplus h(PW_i)$를 계산한 후 패스워드가 제대로 입력되었는지 m과 비교하여 확인한다. 확인이 되면 사용자는 새로운 패스워드 $PW_i^{'}$를 입력한다.

② 스마트 카드는 다음을 계산하여 기존의 m을 m^*로 교체한다.

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

4. 안전성 및 효율성 분석

이 장에서는 제안한 인증 기법의 안전성과 효율성을 분석하고, 관련된 인증 기법들과 비교해 본다.

4.1 안전성 분석

① 내부자 공격

사용자는 패스워드를 일방향 해쉬 함수를 적용하여 전송하기 때문에 악의적인 서버 관리자나 내부자가 해쉬값을 통해 패스워드를 추출할 수 없으므로 내부자 공격에 안전하다.

② 중간자 공격

제안한 인증 기법에서는 물리적으로 안전한 스마트 카드의 사용을 가정하기 때문에 공격자가 스마트 카드 내부의 비밀 정보를 추출할 수 없다. 따라서 공격자는 사용자와 서버 간의 전송되는 메시지를 가로채더라도 그것을 이용하여 비밀 정보를 알 수 없기 때문에 서버 위장 공격이나 사용자 위장 공격을 할 수 없으므로 중간자 공격에 안전하다.

③ 제한적 재전송 공격

제안한 인증 기법에서는 타임 스탬프 대신 랜덤 수를 사용하므로 제한적 재전송 공격에는 안전하다. 만약 공격자가 재전송 공격을 한다고 가정했을 경우, 사용자 랜덤 수 r_u는 매 인증 시 바뀌기 때문에 서버는 재전송 공격을 탐지할 수 있다.

④ 서비스 거부 공격

제안한 인증 기법에서는 타임 스탬프를 사용하여 메시지의 정당성을 확인하는 방식을 사용하지 않으므로 타임 스탬프를 이용한 서비스 거부 공격에 안전하다. 즉, 연속적이 메시지 재전송 공격이 오더라도 시간에 대한 검사를 하지 않으므로 한번 접속을 시도한 합법적인 사용자가 서비스를 받지 못하는 경우는 발생하지 않는다.

⑤ 사용자 익명성

제안한 인증 기법에서는 Bindu 등의 인증 기법에서와 같이 사용자의 ID가 암호화 되어 전송되고, 공격자는 비밀키를 알지 못하므로 암호화된 메시지를 복호화 할 수 없다. 따라서 Bindu 등의 인증 기법과 같이 사용자 익명성을 제공한다.

표 2는 제안한 인증 기법과 관련된 다른 인증 기법의 안전성을 비교한 것이다. 특히, Bindu 등의 방식을 비롯한 타 방식에서는 제한적 재전송 공격과 서비스 거부 공격에 대한 취약성을 보였으나 제안 방식에서는 이러한 취약점을 제거하였다.

4.2 효율성 분석

표 3은 관련된 인증 기법과 제안 기법의 효율성을 비교 분석하여 이를 정리한 것이다. 단, 여기서 XOR 연산량은 해쉬나 암·복호, 멱승 함수 연산량에 비해 무시할 만큼 적어 분석에서 고려하지 않았다.

[표 2] 안전성 분석

구 분	Hwang et al.[8]	Das et al. [11]	Chien et al.[12]	Bindu et al.[14]	제안 방식
사용자 익명성	no	no	yes	yes	yes
내부자 공격	no	no	yes	yes	yes
서비스 거부 공격	no	no	no	no	yes
제한적 재전송 공격	no	no	no	no	yes
서버/사용자 위장 공격	no	yes	yes	yes	yes

[표 3] 효율성 분석

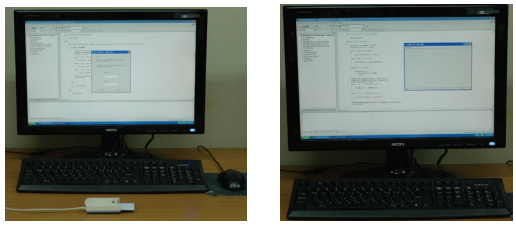
구 분	로그인 단계		검증 단계	
	사용자	서버	사용자	서버
Hwang et al. [8]	3E, 1H	-	-	3E, 1H
Das et al. [11]	5H	-	-	3H
Chien et al. [12]	1E, 1S	-	1S, 1E	2H, 2S, 2E
Bindu et al. [14]	1E, 2H, 1S	-	2S, 1E	3H, 3S, 2E
제안 방식	2H, 1S	-	2S	2H, 3S
E : 멱승 연산, H : 해쉬 연산 S : 대칭키 암호화/복호화				

표 3에서 볼 수 있듯이 제안 기법에서는 Diffie-Hellman의 키 일치 방식을 사용하지 않음으로써 계산량 측면에서 Chien 등의 기법과 Bindu 등의 기법보다 효율성이 높다. 또한, Hwang 등도 ElGamal 암호시스템을 사용함으로써 멱승 연산이 사용되고 이것은 사용자나 서버가 많은 연산 부하를 갖게 한다. Das 등의 기법은 해쉬 함수만으로 구현되어 제안방식 보다 적은 연산이 필요하여 계산 효율성은 뛰어나지만 언급한 바와 같이 안전성에서는 매우 취약하다.

효율성 증가를 사용자와 서버 측의 관점으로 나누어 분석해 보면 일반적으로 서버의 용량이나 성능은 뛰어난 반면, 사용자는 스마트 카드를 이용하게 되므로 사용자 측에서 연산량이 적은 것이 더 효율적이다. 그러나 제안한 기법에서는 사용자나 서버 모두 멱승 연산을 수행하지 않기 때문에 인증 프로토콜이 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.

5. 구현 결과

제안한 인증 알고리듬을 실제 스마트 카드에 구현하고 인증 서버를 설치함으로써 하나의 원격 인증 시스템을 개발하여 프로토콜을 검증하였다. 구현 환경을 살펴보면, 먼저 스마트 카드는 STM사의 ST19WR66을 사용하였으며 중간에 스마트 카드 리더기를 설치하였다. 스마트 카드에 저장될 프로그램은 Metrowerks의 CodeWarrior를 사용하였다. 구현 환경은 클라이언트 PC가 Intel Dual Core 3GHz, 2GB RAM이고, 서버 PC는 AMD 애슬론 3500, 2GB RAM을 사용하였다. 구현 환경을 나타낸 것이 그림 3이다.



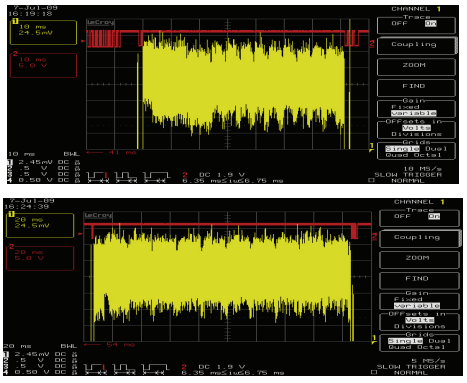
<사용자> <서버>

[그림 3] 구현된 원격 사용자 인증 시스템

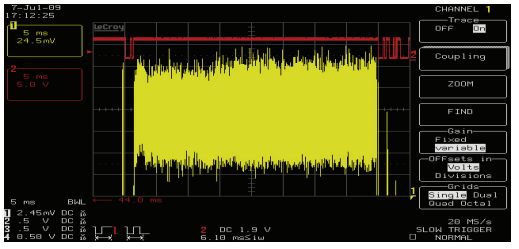
먼저, 프로토콜의 성능을 측정하기 위해 스마트 카드에서 암호화와 해쉬의 수행 시간과 소프트웨어로 구현한 프로토콜의 수행 시간을 측정해 보았다. 원격 서버와 클라이언트 프로그램은 Visual C++ 6.0을 사용하여 구현하였다. 사용한 암호 알고리듬은 AES-128[15]를 사용하였으며 해쉬 함수는 SHA-1[19]을 이용하였다. AES는 128비트의 비밀 키와 128비트의 평문을 사용하며 128비트의 암호문을 출력하는 표준 암호 알고리듬이며 SHA-1은 임의 길이의 메시지를 축약하여 160비트의 결과 값을 출력한다. 또한, 구현에 사용된 랜덤 수 r_u와 r_s는 각각 160비트로 설정하였다.

인증 시스템의 전체 수행 시간을 측정하기 위해 AES-128과 SHA-1을 스마트 카드에 소프트웨어로 구현한 후 연산 시간을 측정해 보았다. 그림 4는 스마트 카드에서 AES-128의 암호화와 복호화 수행 시간을 측정한 것이며 그림 5는 스마트 카드에서 SHA-1의 수행 시간을 측정한 것이다. 스마트 카드에서 AES-128로 암호화 하는 시간은 약 71.4ms가 소요되었으며 복호화하는 데에는 178.8ms, 그리고 SHA-1의 수행 시간은 38.5ms정도 소요

되었다.

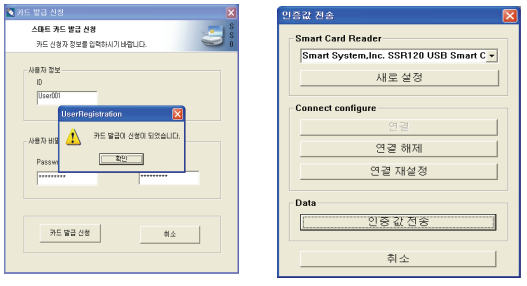


[그림 4] 스마트 카드에서 AES-128 암호화/복호화 수행 시간



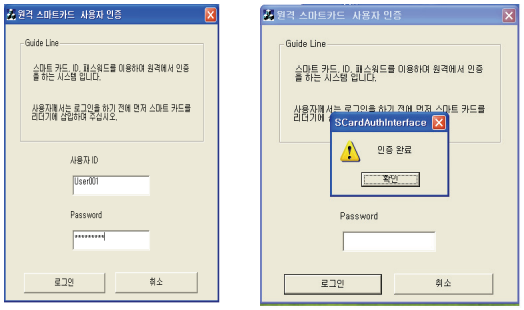
[그림 5] 스마트 카드에서 SHA-1의 수행 시간

그림 6의 왼쪽은 등록 단계에서 사용자가 카드 발급을 위해 아이디와 패스워드를 입력하여 카드 발급을 신청하는 화면이고, 그림의 오른쪽은 서버가 카드 발급 신청을 받아 스마트 카드에 ID_i, m, M 을 저장하는 과정이다. 이런 과정을 통해 사용자가 스마트 카드를 발급 받게 되고, 사용자는 발급 받은 스마트 카드를 통해 원격지에서 서버로 로그인을 시도하게 된다.



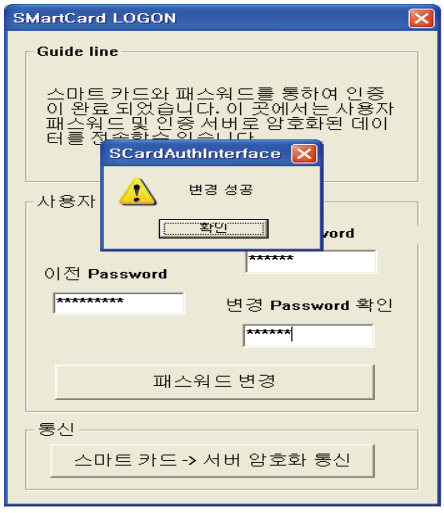
[그림 6] 카드 발급신청(사용자) 및 카드 만들기(서버)

그림 7의 왼쪽은 사용자가 원격지에서 로그인을 시도하는 화면이다. 사용자가 아이디와 패스워드를 입력하면, 로그인 요청 메시지가 서버로 전송되고, 검증 과정을 통해 검증이 성공할 경우에는 그림의 오른쪽 같이 인증이 성공했다는 메시지가 나타나게 된다. 이렇게 인증이 성공한 이후에는 세션키를 이용하여 사용자와 서버가 암호화 통신을 할 수 있다.



[그림 7] 로그인(사용자) 및 인증 완료(서버)

그림 8은 패스워드 변경 단계로서 새로운 패스워드를 입력하여 패스워드를 변경할 수 있다.



[그림 8] 패스워드 변경

서버 및 인증 시스템을 구현한 후 한 번에 인증에 필요한 시간은 사용자와 서버의 네트워크 환경에 따라 다소 차이는 있지만 한 번의 인증을 수행하는데 900ms정도의 시간이 소요되었다. 측정 시간 분석 시 주의할 점은 4장에서 분석한 바에 의하면 스마트 카드나 로그인 단계나 검증 단계에서 한 번의 암호 연산이 필요하다고 분석하였다. 그러나 실제로는 각각 2번이나 3번의 암호화나

복호화 연산이 필요하다. 그 이유는 랜덤 수를 160비트로 잡았는데 이 길이는 AES 입력 길이인 128비트 보다 크기 때문이다.

5. 결론

본 논문에서는 Bindu 등의 인증 기법의 취약점을 분석하고, 이를 해결할 수 있는 향상된 인증 기법을 제안 하였다. 제안한 기법은 타임 스탬프를 사용하지 않는 대신 랜덤 수를 이용함으로써 제한적 재전송 공격과 서비스 공격을 방지할 수 있고, 멱승 연산을 제거하여 효율성을 높였으며, 패스워드 변경 단계를 추가하여 사용자가 자유롭게 패스워드를 변경할 수 있게 하였다.

본 논문에서는 안전성과 효율성을 관련된 다른 인증 기법들과 제안한 기법을 비교 분석함으로써 제안한 기법이 더 안전하고 효율적임을 보였다. 또한, 제안한 프로토콜을 상용 스마트 카드에 구현하여 실제 원격 인증 시스템을 구현하여 동작 과정을 검증하였고 그 성능을 확인하였다.

제안한 프로토콜은 제 3자에게만 사용자 익명성을 제공하도록 설계되었다. 따라서 향후 연구 과제로 제 3자뿐만 아니라 서버에도 익명성을 제공함으로써 완전한 의미의 익명성을 제공하기 위한 연구가 필요하다.

참고문헌

[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] 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.

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] H. Y Chien, C. H. Chen. "A remote authentication scheme preserving user anonymity," IEEE AINA'05, Vol. 2, pp. 245-248, March 2005.

[13] 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.

[14] 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.

[15] National Institute of Standard and Technology, Advanced Encryption Standard, NIST FIPS PUB 97, 2001.

[16] 정민경, 신승수, 한군희, 오상영, “스마트카드를 이용한 원격 시스템 사용자 인증 프로토콜,” 한국산학기술학회, 제10권, 제3호, pp. 572-578, 2009. 3

[17] 최종석, 신승수, 한군희, “사용자 익명성을 제공하는 스마트 카드 기반 3자 참여 키 교환 프로토콜,” 한국산학기술학회, 제10권, 제 2호, pp. 388-395, 2009. 2

[18] L. Gong, "A security risk of depending on synchronized clocks," Operating Systems Review, Vol. 26, No. 1, pp. 49-53, 1992.

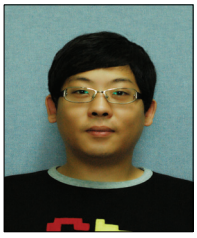
[19] National Institute of Standard and Technology, Secure Hash Standard, NIST FIPS PUB 180-1, 1995.

백 이 루(Yi-Roo Baek) **[준회원]**

- 2008년 8월 : 호서대학교 정보보호학과 (공학사)
- 2008년 9월 ~ 현재 : 호서대학교 대학원 정보보호학과 (석사과정)

<관심분야>
네트워크 보안, 프로토콜, 암호 알고리듬

오 두 환(Doo-Hwan Oh) **[준회원]**



- 2003년 3월 ~ 현재 : 호서대학교 정보보호학과 재학 중

<관심분야>
스마트 카드 보안, 네트워크 보안

길 광 은(Kwang-Eun Gil) **[준회원]**

- 2008년 2월 : 호서대학교 정보보호학과 (공학사)
- 2008년 3월 ~ 현재 : 호서대학교 대학원 정보보호학과 (석사과정)

<관심분야>
스마트 카드 보안, 네트워크 보안, 부채널 공격

하 재 철(Jae-Cheol Ha) **[종신회원]**

- 1989년 2월 : 경북대학교 전자공학과 (공학사)
- 1993년 8월 : 경북대학교 전자공학과 (공학석사)
- 1998년 2월 : 경북대학교 전자공학과 (공학박사)
- 1998년 3월 ~ 2007년 2월 : 나사렛대학교 정보통신학과 부교수
- 2007년 3월 ~ 현재 : 호서대학교 정보보호학과 부교수

<관심분야>
정보보호, 네트워크 보안, 부채널 공격