합법적 멤버에 의한 원격사용자 인증스킴의 취약점 분석 및 개선 (Chien & Bindu et al.′s 프로토콜을 중심으로)

신광철*

요약

원격사용자 인증에서 패스워드와 난수기반의 인증방식이 오랫동안 연구되었고 최근에는 사용자 익명성을 보장하는 연구가 진행되고 있다. 2004년 Das et al.′s이 동적아이디를 사용하여 익명성 보장에 관한 연구가 진행되었고 2005년 Chien et al.′s 등이 개선된 프로토콜을 제안하였다. 2008년도에 Bindu et al.′s 등은 Chien et al.′s 등이 제안한 프로토콜이 내부자 공격과 중간자공격에 취약하다고 지적하여 새로운 프로토콜을 제시했다. 본 논문에서는 Chien et al.′s과 Bindu et al.′s 프로토콜의 취약성을 지적하고 비밀 키 안전성 보장을 위해 난수를 생성하고 이를 사용하여 비밀 키를 해독할 수 없도록 하는 개선된 프로토콜을 제안하였다. 또한 지수연산을 제거하여 연산의 효율성을 높이고 사용자의 패스워드를 임의 변경할 수 있도록 하여 프로토콜의 효율성을 높였다.

Vulnerability Analysis and Improvement of a Remote User Authentication Scheme by Legitimate Members (Oriented Chien & Bindu et al.′s protocol)

Kwang-Cheul Shin*

ABSTRACT

The password and nonce based method of certification has been studied for a long time in the field of remote user authentication and the study for guaranteeing user's anonymity has recently been under way. In 2004 Das et al.′s carried out the study for guaranteeing anonymity using dynamic ID and in 2005 Chien et al.′s proposed an improved protocol. In 2008 Bindu et al.′s suggested a new protocol pointing out that the protocol proposed by Chien et al.′s was vulnerable to the attack from insider and man-in-the-middle attack. This paper points out the vulnerability of the protocol proposed by Chien and Bindu et al.′s and suggests an improved protocol producing nonce for guaranteeing the security of secret key and keeping the secret key indecipherable by using the padding. It also increase efficiency of calculation by removing exponentation operation and increase efficiency of protocol by making it possible to change user's password randomly.

Key Words : Authentication, impersonation attack, Man-in-the-middle attack. replay attack, Anonymity

---

* 성결대학교 산업경영공학부(✉skcskc12@sungkyul.edu)
· 제1저자(First Author) : 신광철 · 교신저자(Correspondent Author) : 신광철
· 접수일(2012년 10월 10일), 수정일(1차 : 2012년 11월 12일), 게재확정일(2012년 12월 18일)

www.kci.go.kr

Ⅰ. 서 론

스마트카드는 사용 및 휴대, 인증의 편리성으로 다양한 분야에서 사용됨에 따라 안전성 보장이 필수적이다. 특히 스마트카드의 수요증가에 따라 각종 보안과 해킹사고에 대한 대비책이 절실하며 이에 따른 보안의 문제가 복잡하고 어려워지고 있다.

여러 보안의 문제 중 공중망에서 사용자 인증은 가장 중요한 비중을 차지한다[1][2].

인증의 방법 중 아이디, 패스워드 및 난수기반의 인증이 간편하며 특히 이들을 혼합한 2-요소 인증방식이 효율적이어서 그동안 많은 연구가 이루어졌고 다양한 분야에서 응용되고 있다[3].

초기에는 서버가 사용자를 검증하기 위하여 미리 저장된 검증테이블을 이용하였으나 이후에는 서버가 사용자 아이디와 패스워드 관리 및 노출 방지를 위해 검증테이블을 사용하지 않는 인증기법이 연구되었다.

또한 사용자의 아이디 보호를 위해 2004년 Das et al.'s[4]은 사용자 익명성(anonymity) 보장을 위해 동적 아이디를 이용하는 프로토콜을 제기하였고 이어 2005년에 Chien et al.'s[5]과 2006년 Liao et al.'s[6]등은 Das et al.'s 프로토콜이 제3자의 추측 공격(guess attack)에 취약하며 패스워드가 원격 시스템에 의해 노출될 수 있다는 문제점을 지적하며 사용자 익명성을 보호하는 새로운 프로토콜을 발표했다.

Qi Xie et al's('2008)은 Liao et al's 스킴이 제3자의 위장공격(impersonation attack)에 취약함을 지적하면서 스마트카드 분실이 있어도 안전한 개선된 스킴을 발표했다.[7]

또한 Bindu et al's('2008)이 Chien, Chen et al.'s 프로토콜은 중간자공격(man-in-the-middle attack)과 내부자공격(insider attack)에 취약하다고 주장하며 새로운 프로토콜을 발표했다[8].

2012년 Shin, K. C는 동적 식별자와 가변인증자를 사용하여 위장공격, 재전송공격(replay attack), 추측공격과 stolen 공격에 안전하고 보다 효율적인 개선된 동적 ID 기반의 OTP(One Time Password) 가변인증자 인증 메커니즘을 제안하였다[9].

강력한 패스워드 인증의 핵심은 사용자 인증으로 프라이버시 보호를 위한 도청방지 보장이며 익명성을 보장받기 위해서는 가로채기에 의한 위장공격의 대책이 필요하다[10].

본 논문에서 연구할 Chien et al.'s, Bindu et al.'s 프로토콜은 정당한 사용자가 다른 정당한 멤버로 위장하는 공격과 재전송공격, 익명성 등에 취약함으로 이 문제점을 해결하기 위해 새로운 프로토콜을 제안하고 제안한 프로토콜을 효율성과 안전성측면에서 연구 및 분석하는 것이 의미가 있다고 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 Chien et al.'s, Bindu et al.'s 프로토콜의 구조 및 취약성을 분석한다. 3장에서는 새로운 프로토콜을 제안하고 4장에서 제안된 프로토콜의 안전성과 효율성을 Chien et al.'s 과 Bindu et al's의 프로토콜과 비교분석한다. 마지막으로 5장에서 결론을 내린다.

Ⅱ. 관련연구

본 장에서는 Chien et al.'s과 Bindu et al.'s 프로토콜의 구조를 고찰한다. 이 스킴들에 대해 서버 비밀키의 안전성 취약으로 전송메시지를 가로채서 합법적 멤버로 위장할 수 있음을 예측하고 이로 인해 파생되는 공격(사용자 위장공격과 중간자공격, 익명성 등)의 취약성을 분석한다.

본 논문에서 다루고자하는 가장 큰 이슈는 서버의 비밀키 노출에 대한 취약점이다.

인증단계에서 공격을 하는 합법적 사용자로 가장한 공격자는 서버에 등록한 멤버중의 하나의 사용자로 다른 정당한 사용자로 위장하며 대상은 서버이다. 공격자는 다른 합법적 멤버가 인증단계에서 서버로 전송되는

www.kci.go.kr

메시지를 스니핑(sniffing)하여 위장공격을 하는 경우로 공격자는 다른 합법적 멤버의 패스워드를 모르고도 인증정보를 획득할 수 있다.

2.1 기호 및 설명

본 논문에서 원격사용자 인증 프로토콜을 설명하는데 사용될 기호를 정리하면 다음과 같다.

기호	설명
U	사용자
pw	사용자의 패스워드
ID	사용자의 아이디
S	시스템서버
h()	단방향 해시함수
SKus	서버와 사용자의 공통 세션키
$E_k[]/D_k[]$	암호화/복호화 알고리즘
T	타임스탬프
x	서버의 long-term 비밀 키
⊕	XOR 연산
p	1024비트 소수
g	순환군 Z_p의 생성자

2.2 Chien et al.'s 프로토콜

초기에 스마트카드를 이용한 원격시스템 상호인증 스킴은 패스워드를 서버에 저장하거나 해시함수를 적용한 값을 저장하는 방식으로 수행되었으나 스마트카드 사용자의 ID가 노출되면서 프라이버시의 문제가 대두되었다.

특히 패스워드가 저장된 서버의 해킹으로 등록된 사용자들의 패스워드를 도용하여 위장공격이 우려되면서 패스워드 테이블을 보유하지 않는 연구가 계속되었고 2004년 Das et el.'s등이 동적 ID를 사용하는 논문을 발표하면서 사용자의 익명성이 강조되었다.

이후 Chien et al.'s등은 Das et el.'s의 익명성에 문제를 보완한 논문을 발표하였다. 본 절에서는 Chien et al.'s의 프로토콜에서 익명성은 보장하고 있으나 서버 비밀 키의 노출이 쉽게 되어 공격자의 위장공격에 취약함을 보인다.

<그림 1>은 Chien et al.'s의 등록단계 스킴으로 패스워드가 노출된 상태로 서버에 등록됨을 보여주고 있다. 이어 로그인단계, 인증단계는 Bindu et al.'s 스킴과 동일함으로 이 스킴의 설명은 Bindu et al.'s 프로토콜에서 다루며 어떤 취약성이 있는지에 대해 분석한다.

구분	사용자 U	서버 S
등록	ID, pw->	m=h(ID⊕x)⊕h(x)⊕pw I=h(ID⊕x) <--m, I, p, g, h()-

그림 1. Chien et al.'s 등록단계
Fig 1. Registration phase of Chien et al.'s

2.3 Bindu et al.'s 프로토콜

1) 인증기법

Chien et al.'s등이 Das et al.'s등의 인증기법에서 사용자의 노출이라는 익명성이 제공하지 못함을 지적하여 해결방안을 제시하였다.

Bindu et al.'s 프로토콜은 Chien et al.'s등의 인증기법에서 나타난 취약점인 내부자공격, 중간자 공격 등을 보완하여 개선시킨 프로토콜이다.

익명성은 전송정보에 사용자 정보가 노출되지 않고 서버도 수신된 메시지에 대해 전송정보의 복호화 이전에는 누구에서서 전송된 메시지인지 알 수 없도록 한 프로토콜이다.

본 절에서는 Bindu et al.'s등의 인증기법을 분석하고 그 취약성을 도출하여 논한다. Bindu et al.'s 등의 프로토콜은 <그림 2>와 같이 등록단계, 로그인단계, 인증단계로 구성되어 있다.

www.kci.go.kr

구분	사용자 U	서버 S
등록	----> ID, h(pw)---->	m=h(ID⊕x)⊕h(x)⊕h(pw) I=h(ID⊕x)⊕x <---ID, m, I, p, g, h()----
로그인	· input ID, pw · random number a, r_u generation · $r_u=g^a \bmod p$ · M=m⊕h(pw) · C=M⊕r_u · R=I⊕r_u -----C, T, $E_R[r_u, ID, T1]$--->	
인증절차	· 복호 $D_R[r_s, r_u+1, T2]$ · check T'-T2≤△T · check $(r_u+1)'=?r_u+1$ compute · SK생성 ==> $SKus=(r_s)^a \bmod p$ $=(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$ · $E_{SKus}[r_s+1]$ ---------->	compute key R · R=C⊕h(x)⊕x=h(ID⊕x)⊕h(x)⊕r_u ⊕h(x)⊕x=h(ID⊕x)⊕x⊕r_u · 복호 $D_R[r_u, ID, T1]$ · check T'-T1≤△T compute · R=h(ID⊕x)⊕x⊕r_u & check · b생성, r_u는 보유중 · $r_s=g^b \bmod p$ · SK생성 ==> $SKus=(r_u)^b \bmod p$ $=(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$ <----$E_R[r_s, r_u+1, T2]$--- · $D_{SKus}[r_s+1]$ · check : $(r_s+1)'=?r_s+1$

그림 2. Bindu et al.'s 프로토콜
Fig 2. Protocol of Bindu et al.'s

2) 등록단계

사용자가 원격시스템에 등록할 때 다음 절차를 수행한다.

Step 1. 사용자는 서버에게 최초 아이디와 h(pw)를 전달한다.

Step 2. 서버는 m=h(ID⊕x)⊕h(x)⊕h(pw)과 I=h(ID⊕x)⊕x를 연산한다.

Step 3. 서버는 스마트카드에 ID, m, I, p, g, h()을 탑재하여 사용자에게 발행한다.

3) 로그인단계

사용자가 서버에 합법적인 인증을 원할 때 스마트카드를 리더기에 삽입하고 ID와 pw를 입력한다.

Step 1. 스마트카드는 난수인 $r_u=g^a \bmod p$를 생성한다.

Step 2. M=m⊕h(pw)을 계산한다.

Step 3. M⊕r_u을 계산한다.

Step 4. R=I⊕r_u을 계산한다.

Step 5. 사용자는 서버에게 메시지 {C, T, $E_R[r_u, ID, T1]$}를 전송한다.

www.kci.go.kr

4) 인증단계

서버는 사용자로부터 메시지를 수신하고 아래와 같은 절차로 사용자인증을 실행한다.

Step 1. 서버는 자신의 비밀키 x를 이용하여 $R=C\oplus h(x)\oplus x$를 계산하여 공통키 R을 구하고 $D_R[r_u, ID, T1]$을 통해 복호화 한다.

Step 2. T와 T'과의 시간간격의 유효성을 테스트한다.

Step 3. 복호화된 r_u, ID, T1을 이용하여 $R=h(ID\oplus x)\oplus x\oplus r_u$을 계산하여 일치하는지 체크한다.

Step 4. 서버는 사용자에게 $E_R[r_s, r_u+1, T2]$를 전송한다.

Step 5. 사용자는 수신된 메시지를 복호화하여 r_u+1를 확인하고 맞으면 세션키 $g^{ba} \bmod p$를 계산하고 이 세션키를 이용하여 서비스를 요청할 수 있다.

III. 프로토콜의 취약성

3.1 Bindu et al.'s 프로토콜 취약성분석

1) 비밀키 안전의 취약성

정당한 공격자가 $h(x)\oplus x$를 구할 수 있다는 문제점이 있다. 이 프로토콜은 모든 정당한 멤버에게 서버의 비밀키 x가 동일하게 적용되어 있다는 맹점을 갖고 있다. 서버로부터 발급받은 자신의 스마트카드를 통해서 $h(x)\oplus x$를 알아낼 수 있다.

정당한 공격자 E는 C와 R을 XOR 연산하여 $C\oplus R=h(ID\oplus x)\oplus h(x)\oplus r_u\oplus h(ID\oplus x)\oplus x\oplus r_u = h(x)\oplus x$를 구할 수 있으며 또 다른 방법으로 M과 I를 XOR 연산하여 $M\oplus I=m\oplus h(pw)\oplus I$를 통해서 $h(x)\oplus x$를 얻게 된다.

정당한 공격자는 전송되는 메시지 C, T, $E_R[r_u, ID, T1]$을 가로채서 C를 확보하고 자신이 구한 $h(x)\oplus x$을 이용하여 비밀키 R을 구할 수 있다.

C에는 전송자의 정보 $(h(ID\oplus x)\oplus h(x)\oplus r_u)$로써 이를 이용하여 다음을 연산한다.

$R=C\oplus h(x)\oplus x = h(ID\oplus x)\oplus h(x)\oplus r_u \oplus h(x)\oplus x = h(ID\oplus x)\oplus r_u\oplus x$

비밀키 R이 계산되면 $D_R[r_u, ID, T1]$을 복호화하여 난수 r_u와 정당한 멤버의 ID, T를 알아내서 공격자 자신이 정당한 멤버로 위장할 수 있다.

2) 내부자공격

Chien 인증기법과 비교해 볼 때 프로토콜의 차이는 서버에 등록할 때 패스워드를 해시한 값으로 제공하여 서버에서 패스워드를 노출하지 않아 내부자 공격을 방지할 수 있도록 하였다.

3) 중간자 공격(위장 공격)

3.1.1에서 언급한 서버의 비밀키 안전의 취약함으로 인해 합법적 공격자 E는 로그인 메시지 C, T, $E_R[r_u, ID, T1]$을 가로채서 C를 확보하고 자신이 구한 $h(x)\oplus x$을 이용하여 비밀키 R을 구할 수 있으므로 r_u, ID, T1을 복호화 할 수 있다. 서버에 로그인하기 위해 정당한 사용자 U로 위장할 수 있다.

4) 사용자 익명성

Bindu et al.'s 프로토콜에서 사용자의 ID는 비밀키 R에 의해 암호화되어 전송되므로 일반적인 공격자(제3자)는 로그인 메시지를 스니핑하여도 사용자를 알 수 없다. 그러나 합법적 멤버에 의해 III.의 1.에서 1)에서와 같이 비밀키의 취약함으로 인해 쉽게 복호화하여 신원을 파악할 수 있다. 익명성을 제공하는 프로토콜은 Das et al.'s에 의해 제기되었고 Bindu et al.'s 프로토콜도 익명성을 제공하는 프로토콜로 제안되었으나 정당한 멤버에 의해 R을 노출시키므로 사용자의 익명성을 보장하지 못한다.

www.kci.go.kr

5) 재전송공격

Bindu et al.'s 프로토콜은 재전송 공격방지를 위한 수단으로 타임스탬프 T를 사용한다.

로그인 메시지 M=C, T, $E_R[r_u, IDi, T]$와 응답메시지 M'=T1, $E_R[r_s, r_u+1, T1]$에서 M과 M'의 T와 T1의 유효성을 검사하여 안전여부를 판단한다.

여기에는 두 가지의 결점을 가지고 있다.

첫째, 타임스탬프는 사용자의 전송시간 T와 서버의 수신시간 T'간의 오차를 허용윈도우 △T 범위에서 인정하기 위한 것으로 공격자는 허용윈도우 △T보다 짧은 시간 내에서 메시지를 재전송할 수 있다. 이로 인하여 Ⅱ. 3. 4)의 Step2에서 T'-T1≤△T를 무난히 검증될 수 있다. 문제는 허용윈도우 △T는 시스템의 통신 트래픽이나 성능에 따라 달라질 수 있다.

둘째, 공격자는 로그인 전송메시지 C, T, $E_R[r_u, ID, T1]$을 가로채서 다시 전송하게 되면 서버는 T'-T1≤△T가 성립되는 한 로그인 요청을 받아드려 검증할 것이다.

3.2 Chien et al.'s 프로토콜 취약성분석

1) 비밀키의 취약성

정당한 멤버가 공격자라고 할 때 h(x)를 얻을 수 있다. 등록하는 모든 정당한 사용자에게 서버의 비밀정보 x를 동일하게 적용되어 있다는 것이다. 자신의 스마트카드를 통해서 구해보자.

로그인 단계에서 정당한 사용자는 C와 R을 연산하였다. 이 두 개의 연산 값을 XOR 연산하게 되면 $C⊕R=h(IDi⊕x)⊕h(x)⊕r_u⊕h(IDi⊕x)⊕r_u=h(x)$와 같이 해시된 비밀키 h(x)를 도출해 낼 수 있다.

공격자는 C, T, $E_R[r_u, ID, T]$을 가로챈다. 공격자는 전송되는 C를 확보하고 자신이 구한 h(x)을 이용하여 비밀키 R을 구할 수 있다. C에는 전송자의 정보인 $(h(ID⊕x)⊕h(x)⊕r_u)$으로써 이를 이용하여 다음을 연산한다.

$R=C⊕h(x)= h(IDi⊕x)⊕h(x)⊕r_u⊕h(x)= h(ID⊕x)⊕r_u$

2) 내부자공격

등록단계에서 사용자의 패스워드 pwi는 안전한 채널에 의해 서버에 등록된다. 그러나 악의적인 내부자에 의해 쉽게 노출되어 정당한 사용자로 위장하여 다른 서버에 접속을 시도할 수 있다.

3) 기타 취약성

Bindu et al.'s 프로토콜은 Chien et al.'s 프로토콜의 패스워드 노출방지를 위해 해시값을 사용한 점과 비밀키 R을 연산할 때 서버의 비밀키 x의 보안성을 강화하기 위해 I 값 연산에 $h(ID⊕x)⊕x$와 같이 서버의 비밀키 x를 추가하여 연산하는 두 가지의 보완대책을 제안했으며 다른 프로토콜은 Chien et al.'s 과 동일하다. 그러므로 Ⅲ.의 1.절 3), 4), 5)와 동일한 취약성을 가진다.

Ⅳ. 제안 프로토콜

본 장에서는 2장에서 분석한 Chien et al.'s & Bindu et al.'s 프로토콜의 문제점인 서버의 비밀 키의 노출을 중심으로 이를 개선한 새로운 프로토콜을 제안한다. 제안한 프로토콜은 등록단계, 로그인 단계, 인증단계로 구성된다. 추가로 제안 프로토콜을 설명하는데 사용될 기호를 정리하면 다음과 같다.

기호	설명
ri/rj	세션마다 생성되는 사용자/서버의 난수
G()	난수생성기
rs	최초 스마트카드에 발급되는 서버의 생성난수
t	스마트카드 발급시간

www.kci.go.kr

IDi 사용자 i의 아이디
pwi 사용자 i의 패스워드

4.1 등록단계

사용자는 원격시스템에 등록 또는 재등록하기를 원할 때 오프라인으로 다음과 같은 절차를 수행한다.

Step 1. U는 등록을 위해 IDi와 h(pwi⊕ri)를 서버 S로 제공한다.

구분	사용자 U	서버 S
등록	IDi, h(pwi ⊕ri)->	rs1=G(x⊕t) m=h(IDi⊕x)⊕h(x⊕rs1) ⊕h(pwi⊕ri) I=h(IDi⊕x)⊕h(rs1) <-IDi, m, I, t, h()--

Step 2. 이 때 시스템 서버 S는 등록하는 사용자에게 서버의 비밀키 보호를 위해 비밀키와 스마트카드 발급시간을 입력으로 난수생성기 G()에 의해 난수(rs1)를 생성한다. rs1=G(x⊕t)

Step 3. S는 m=h(IDi⊕x)⊕h(x⊕rs1)⊕h(pwi⊕ri)와 I=h(IDi⊕x)⊕h(rs1)을 연산한다.

Step 4. S는 U에게 스마트카드에 IDi, m, I, t, h()를 저장하여 발행한다.

4.2 로그인 단계

구분	사용자 U	서버 S
로그인	· input IDi, pwi · input r_i · M=m⊕h(pwi⊕ri) · C=M⊕ri · R=I⊕ri -{t, C, E_R[ri, IDi]}->	

사용자 U가 원격시스템에 로그인하고자 할 때 스마트카드를 리더기에 삽입하고 IDi와 pwi를 입력한다.

Step 1. Ui는 대칭키와 세션키에 적용할 난수 ri를 입력한다.

Step 2. M=m⊕h(pwi⊕ri)를 연산한다.

Step 3. C=M⊕ri를 연산한다.

Step 4. R=I⊕ri를 연산한다.

Step 5. U는 S에게 {t, C, E_R[ri, IDi]} 메시지를 전송한다.

4.3 인증 단계

사용자 U로부터 메시지를 받은 후 원격시스템 S는 다음과 같은 절차로 사용자가 정당한 사용자인지 검증하는 절차이다.

Step 1. S는 {t, C, E_R[ri, IDi]}를 수신하여 어느 사용자로부터 전송되어 온 메시지인지 알지 못하는 상태로 자신의 비밀키 x와 스마트카드 발급시간 t를 사용하여 난수(rs1)를 생성하고 이 난수와 서버의 비밀키, 수신한 메시지 C를 이용하여 암호화에 사용된 대칭키 R을 만들어 내야한다.

rs1=G(x⊕t)

Step 2. rs1과 서버의 비밀키 x, C를 이용하여 R를 연산한다.

R=C⊕h(x⊕rs1)⊕h(rs1)

R이 연산되면 E_R[ri, IDi] 메시지를 복호화하여 IDi와 난수 ri를 확인할 수 있다.

여기에서 IDi와 난수 ri를 인증세션동안 임시테이블에 저장하고 인증처리 과정이나 이후에 다시 동일한 메시지가 전송되어 인증을 요청하는 메시지에 대해서는 재전송 공격으로 간주한다.

Step 3. S는 임의 난수 rj를 선택하고 사용자가 인증할 수 있는 C3=R⊕rj를 연산한다.

Step 4. 수신하여 정상적으로 복호화된 대칭키 R과 각각 생성한 사용자 생성 난수 ri, 서버 생성 rj를 이용하여 세션 키 SKus=h(R⊕rj⊕ri)를 생성하고 보관한다.

www.kci.go.kr

구분	사용자 U	서버 S
인증 단계	· 복호 D_R[C3, ri+1] · check $(r_i+1)'=?r_i+1$ · rj추출 : C3⊕R=rj · SK생성 : SKus=h(R⊕r_j⊕r_i)	· rs1=G(x⊕t) · R=C⊕h(x⊕rs1)⊕h(rs1) · 복호 D_R[r_i, t, IDi] · 임시테이블에 r_i, IDi 저장 · r_j생성 · SK생성 SKus=h(R⊕r_j⊕r_i) · C3=R⊕r_j <----E_R[C3, r_i+1]---

그림 3. 인증 단계
Fig 3. Authentication phase

Step 5. S는 U에게 자신을 검증할 메시지 {C3, ri+1}를 대칭키 R을 사용하여 암호문 E_R[C3, ri+1]으로 전송한다.

Step 6. U는 E_R[C3, ri+1]를 수신하여 자신이 생성한 대칭키 R로 복호화하여 C3로 정당한 S인지 그리고 rj를 구하며 ri+1 값이 포함되어 있는지 유효성을 테스트한다.

rj추출 : C3⊕R=rj

Step 7. rj를 이용하여 세션 키 SKus=h(R⊕rj⊕ri)를 생성한다.

4.4 패스워드 변경단계

세션 키 SKus가 성공적으로 생성되면 비밀키의 노출을 방지하기 위해 자신의 패스워드를 변경, 수정하여 저장한다.

Step 1. 스마트카드 리더기에 카드를 삽입하고 현재의 패스워드(pwi)와 새로운 패스워드(pwi')를 입력하면 m=h(IDi⊕x)⊕h(x⊕rs1)⊕h(pwi⊕ri)값은 New_m=h(IDi⊕x)⊕h(x⊕rs1)⊕h(pwi'⊕ri)로 변경되어 저장된다.

구분	사용자 U	서버 S
패스워드 변경	· pwi와 pwi'입력 · New_m= m⊕h(pwi'⊕ri)⊕h(pwi⊕ri)	

V. 제안 프로토콜 분석

본 장에서는 제안한 프로토콜의 안전성을 분석하고 Chien et al.'s, Bindu et al.'s 프로토콜의 서버 비밀키 x의 취약성으로 인한 내부자공격, 전방향 안전성, 익명

www.kci.go.kr

성, 중간자공격(위장공격)과 같은 문제점에 대해서 분석한다.

그리고 제안한 프로토콜과 Chien et al.'s, Bindu et al.'s 프로토콜을 기능적인 측면과 성능적인 측면에서 비교분석하였다.

5.1 안전성 평가

본 절에서는 제안한 프로토콜에 대한 서버의 비밀키 x에 대한 안전성, 내부자공격, 중간자공격(위장공격), 전방향 안전성, 익명성에 대하여 안전성을 평가한다. Chien et al.'s, Bindu et al.'s 프로토콜은 비밀키 x의 취약성으로 위에서 나열한 여러 공격에 안전을 보장할 수 없다. 제안된 프로토콜은 이러한 공격들에 대해 안전성이 뛰어나다. Chien et al.'s, Bindu et al.'s 프로토콜과 제안된 프로토콜에 대한 안전성 비교는 <표 1>과 같다.

1) 비밀키 x의 안전성

등록단계에서 사용자는 $h(pwi \oplus ri)$를 사용하므로 서버의 내부자는 알 수 없으며 사용자 자신은 서버에서 제공한 m에서 $h(IDi \oplus x)$와 $h(x \oplus rs1)$를 얻을 수 없다는 안전성이 있다. 정당한 멤버인 합법적 공격자는 서버의 비밀키 x와 $h(x \oplus rs1)$ 값을 찾아낼 경우 비밀키 R을 쉽게 얻을 수 있고 이것은 모든 안전성이 무너짐을 의미한다. 비밀키 x와 rs1을 추측하기 위해서는 $2^{128} * 2^{128}$의 연산을 필요로 한다.

또한 위 연산으로 $h(x \oplus rs1)$를 알아내더라도 하나의 인증세션이 이루어진 후 사용자는 자신의 패스워드 $New_m=h(IDi \oplus x) \oplus h(x \oplus rs1) \oplus h(pwi' \oplus ri)$를 변경함으로써 또한 $2^{128} * 2^{128}$의 연산을 필요로 한다.

2) 내부자 공격

내부자공격이란 올바른 경로로 서버에 등록된 사용자가 공격하는 것을 말한다. 제안한 프로토콜에서는 사용자의 $h(pwi \oplus ri)$를 해시함수를 통해 해시한 값만을 서버에 제공하기 때문에 서버의 내부자라 할지라도 사용자의 pw와 ri를 알 수 없으므로 내부자 공격이 전혀 이루어 질 수 없다.

3) 중간자 공격(위장공격)

중간자 공격은 비밀키의 노출에 의해 해독되어 서버나 사용자를 위장하여 메시지를 변조 또는 서비스 거부공격으로 이루어진다.

중간자공격이 성공하기 위해서는 로그인단계의 요청메시지 $\{t, C, E_R[ri, IDi]\}$와 응답메시지 $E_R[C3, r_i+1]$를 계산할 수 있어야 한다. 비밀키 R을 유도하기 위해 메시지 C를 연산해야하는데 이를 위해서는 $h(x \oplus rs1)$의 값을 찾아낼 수 있어야 한다.

따라서 제안 프로토콜에서는 공격자가 정당한 사용자로 위장하기 위해 필요한 비밀값들을 얻을 수 없으므로 사용자의 중간자공격에 의한 위장공격이 불가능하다.

4) 익명성

익명성이란 사용자가 자신의 신원을 드러내지 않고 서비스나 자원을 사용하는 것을 말한다.

사용자 익명성을 제공하는 스마트카드 프로토콜은 Chien et al.'s, Bindu et al.'s 등이 제기하였으나 비밀키 R을 구할 수 있으며 비밀키 R을 구할 수 있는 정당한 공격자는 누구나 사용자의 ID를 얻을 수 있으므로 Chien et al.'s, Bindu et al.'s 프로토콜은 서버 뿐 아니라 정당한 다른 참여자에게도 사용자의 신원이 노출된다. 그러나 제안 프로토콜에서는 시스템 서버 S는 등록하는 사용자에게 비밀키 보호를 위하여 카드발급시간을 사용한 난수(rs1)를 사용한다. 비밀키 x와 난수(rs1)를 XOR 연산하고 이를 해시 값으로 만들어 또 다시 비밀키 x와 XOR 연산함으로써 비밀키를 보호하고 스마트카드 발급시간인 t를 스마트카드에 탑재하여 사용자인증에 사용한다.

www.kci.go.kr

표 1. 안전성 분석
Table 1. Security analysis

구분	Chien et al.'s	Bindu et al.'s	제안
위장공격	Ⅲ. 2. 1)절 서버의 비밀키 x의 노출로 취약	Ⅲ. 1. 1)절 서버의 비밀키 x의 노출로 취약	서버의 비밀키 x의 안전으로 위장공격 미 성립
중간자공격	Ⅲ. 2. 1)절 서버의 비밀키 x의 노출로 취약	Ⅲ. 1. 1)절 서버의 비밀키 x의 노출로 취약	h(x⊕rs1)의 해독불가능으로 중간자 공격 미 성립
내부자공격	취약	강함	h(pwi⊕ri)사용으로 내부자공격 미 성립
재전송공격	제한적 재전송공격	제한적 재전송공격	임시테이블 사용으로 재전송공격 미 성립
익명성	ID노출로 취약	ID노출로 취약	비밀 키 R의 미 해독으로 익명성 보장

표 2. 효율성 분석
Table 2. Efficiency analysis

구분	Chien et al.'s 스킴		Bindu et al.'s 스킴		제안스킴	
	사용자	서버	사용자	서버	사용자	서버
등록단계 연산	0	3h, 3⊕	0	3h, 4⊕	1h, 1⊕	3h, 3⊕, 1G
로그인단계 연산	3⊕, 1E 1e	0	3⊕, 1E 1e, 1h	0	1h, 4⊕, 1E	
인증단계 연산	0	5⊕, 1E 2h	0	3⊕, 1E 2h	D1, 1⊕	2h, 4⊕, E1, D1, G1,
세션키 생성연산	1E, 1e	1E, 1e	1E, 1e	1E, 1e	1h, 2⊕	1h, 2⊕
세션 키 검증	0	0	1E	1E	0	0
스마트카드 정보	M, I, h(), p	0	M, I, h(), p	0	IDi, m, I, t, h()	0
패스워드연산	0	0	0	0	2h, 4⊕	0
통신횟수	3		3		2	

E : 암복호연산, D: 복호화연산, h : 해시연산,
⊕ : XOR연산, e : 지수연산

www.kci.go.kr

5) 재전송 공격

재전송공격의 안전성은 다음 두 가지 요인으로 우선 타임스탬프 T를 사용하지 않고 임시테이블을 사용하는 것과 로그인마다 랜덤수를 사용하는 것이다.

로그인정보 {t, C, E_R[ri, IDi]} 중에서 복호화된 사용자 U의 난수 ri와 IDi를 임시테이블에 다음 인증세션 동안 저장하고 이 기간에 동일한 로그인정보가 전달된다면 제3자의 공격으로 간주된다. 또한 매 로그인마다 랜덤수 ri, rs를 생성함으로 서버는 이를 탐지할 수 있으므로 공격자는 이전의 인증세션에서 사용된 메시지를 이용하는 재전송공격이 불가능하다.

5.2 효율성 평가

<표 1>은 Chien et al.'s, Bindu et al.'s 프로토콜을 효율성 측면에서 제안 프로토콜과 비교분석하였다.

여기에서는 XOR 연산량, 해시, 암.복호, 지수함수 연산 량을 고려하여 분석하였다.

<표 2>에서와 같이 제안기법은 Diffie-Hellman의 키 동의방식을 사용하지 않음으로 지수연산을 필요로 하는 Chien et al.'s, Bindu et al.'s 프로토콜에 비해 연산의 효율성이 높다.

그러나 공격자의 위장공격과 중간자공격, 익명성보장을 위해 등록단계와 로그인, 인증단계에서 추가적인 연산이 필요하다.

Ⅳ. 1. 등록단계에서 다양한 공격에 안전을 확보하기 위해 인증인자들이 필요하고 이들을 보호를 위해 G()함수와 카드발급시간을 사용함으로 추가적인 연산단계를 갖는다.

Bindu. et al.'s 프로토콜은 제안방식보다 적은 연산이 필요하여 계산효율성은 높지만 안전성에는 매우 취약함을 보이고 있다.

Ⅵ. 결 론

원격사용자 인증은 프라이버시 보호를 위한 도청방지 보장이며 익명성을 보장받기 위해서는 추측에 의한 사전공격과 위장공격의 대책이 필요하다. 본 논문에서는 Chien et al.'s, Bindu et al.'s 프로토콜에 대해서 안전성을 평가하고 사용자공격에 취약하다는 것을 보였다. 그리고 새로운 개선된 프로토콜을 제안하였다. Chien et al.'s, Bindu et al.'s 프로토콜의 취약성은 비밀 키가 쉽게 노출될 수 있다는 점이다. 이러한 키의 노출은 보안의 안전성이 모두 무너지는 결과를 가져온다.

서버 관리자는 항상 위험에 노출됨을 대비해야 하며 자신의 비밀키가 노출되었을지도 모를 상황에서 업무를 수행할 가능성이 높다. 또한 제공 서비스의 안전성을 유지하기 위해 많은 노력을 경주한다. 논문의 핵심은 Chien et al.'s, Bindu et al.'s 프로토콜의 비밀키 노출에 대한 안전성 확보와 이로 인한 위장 및 중간자 공격의 방어, 익명성보장에 있다. 이를 위해 Diffie-Hellman의 키 동의 방식 대신에 XOR연산을 사용함으로 지수연산을 제거하여 효율성을 높였고 비밀키 보장을 위해 스마트카드 발급시간에 의한 난수를 생성하여 비밀키 x를 보호하였다.

정당한 공격자의 재생공격을 방지하기 위해 인증세션동안 사용자정보를 임시테이블에 저장, 운용함으로써 허용윈도우 △T를 사용하는 것 보다 실질적이며 비밀키 R을 구할 수 없으므로 익명성이 보장된다.

이로 인하여 중간자공격, 위장공격, 재전송공격, 익명성 유지 등의 차단효과와 세션키 생성의 XOR 사용으로 지수연산의 부담을 줄일 수 있다.

또한 사용자는 매 인증세션 이후 패스워드를 자유롭게 수정, 변경시킬 수 있다. 이와 같이 논문에서는 안전성과 효율성측면에서 Chien et al., Bindu et al. 프로토콜과 비교분석함으로써 제안 기법이 더 안전하고 효율적임을 보였다. 비밀키의 안전성보장이 중간자공

www.kci.go.kr

격과 익명성보장에 직결되어 있음을 알 수 있다.

본 논문에서 제안한 프로토콜은 스마트카드를 사용한 다양한 응용분야에서 사용될 수 있을 것으로 예상된다.

참고문헌

[1] Chih-Wei Lin. Jau-Ji Shen. Min-Shiang Hwang. *"Security Enhancement for Optimal Strong-Password Authentication Protocol"* . ACM Operating Systems Review, Volume 37 Issue 2, April 2003

[2] Cheng-Chi Lee. Li_Hua. Min-Shiang Hwang. *"A Remote User Authentication Scheme Using Hash Functions"*. ACM Operating Systems Review, 36(4):23-29, 2002.

[3] Shen, J.J., Lin, C.W., Hwang, M.S., : *A Modified Remote User Authentication Scheme Using Smart Cards*. IEEE Transaction on Consumer Electronics. Vol. 49. No.2. (2003) 414-416

[4] M.L. Das, A. Saxena, V.P. Gulati, *A dynamic ID-Based remote user authentication scheme*, IEEE Transaction on Consumer Electronics, Vol. 50, No.2, pp.629-631, 2004.

[5] Hung-Yu Chien, and Che-Hao Chen, "A Remote Password Authentication Preserving User Anonymity," *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, (AINA '05), 2005.

[6] I. E. Liao, Cheng-Chi Lee, Min-Shiang Hwang. : *IDentity-based deniable authentication protocol from pairings*. IMSA. pp.112-114, 2006.

[7] Qi Xie, Ji-Kin Wang, De-Ren Chen, Xiu-Yuan Wang. : *A novel user authentication scheme using smart card,* College of Computer Science. Zhejiang University. Hangzhou, 310027, P R China , and. Graduate School. Hangzhou Normal University, 2008.

[8] C.Shoba Bindu, P. Chandra Sekhar Reddy, and B. Satyanarayana, "*Improved Remote User Authentication Scheme Preserving User Anonymity,"* IJCSNS, Vol.8, No. 3, 2008. 3.

[9] Kwang-Cheul Shin, "Analysis & Countermeasure for Authentication Scheme of Qi Xie's Based on Variable Authenticator", *The Korean Institute of Information Technology*, vol. 10, no. 1, pp. 139-146, Jan. 2012.

[10] Rajaram Ramasamy, Amutha Prabakar Muniyandi. *:New Remote Mutual Authentication Scheme using Smart card*, *TRANSACTIONS ON DATA PRIVACY 2*. p141-152. 2009.

저자소개

신광철(Kwang-Cheul Shin)

1985 서울과학기술대학교 전자 계산학과 (학사)

1990 국방대학원 전자계산학과 (석사)

2003 성균관대학교 대학원정보공학과 (박사)

2004~현재 성결대학교 산업경영공학부 교수

※ 관심분야 : 스마트카드보안, 전자지불시스템, 네트워크 및 RFID 보안

www.kci.go.kr