www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2012.17.4.001

Shieh and Wang's의 스마트카드 상호인증 스킴에 대한 중간자공격 개선

Vulnerability Analysis and Improvement in Man-in-the-Middle Attack for Remote User Authentication Scheme of Shieh and Wang's using Smart Card

신광철(Kwang-Cheul Shin)*

초 록

최근 Shieh and Wang[10]은 Lee et al.[6] 스킴의 연산비용 효율성과 Chen and Yeh[1] 스킴의 보안성과 키 합의를 조합한 효율적인 상호인증 스킴을 제안했다. 그러나 Shieh and Wang[10] 스킴은 패스워드 기반의 스마트카드를 이용한 원격 사용자인증 스킴에서 고려해야 하는 제 3자(중간자, 공격자)에 대한 보안요구 내용들을 만족시키지 못하고 있다. Shieh and Wang 스킴의 약점은 3-way handshaking 상호인증에서 위조된 메시지를 검증하지 못하는 부적절과 시스템(서버)의 비밀키가 쉽게 노출되는 취약성을 갖는다. 본 논문에서는 Shieh and Wang 스킴의 도청에 의해 위조된 메시지의 검증절차의 문제점을 지적한다. 제안 스킴은 사용자의 패스워드정보와 시스템의 비밀정보를 노출하지 않을 뿐 아니라 서버에서 무결성 검사를 할 수 있는 기능을 추가하여 다양한 공격에 안전한 강력하고 개선된 two-way 원격사용자 인증 스킴을 제안한다.

ABSTRACT

Shieh and Wang [10] recently proposed an efficient mutual authentication scheme that combined the cost-effectiveness of operations of Lee et al. [6]. scheme and the security and key agreement of Chen and Yeh scheme. Shieh and Wang [10] scheme, however, does not satisfy the security requirements against a third party (the man-in the middle, attacker) that have to be considered in remote user authentication scheme using password-based smart cards. Shieh and Wang weaknesses are the inappropriateness that it cannot verify the forged message in 3-way handshaking mutual authentication, and the vulnerability that the system (server) secret key can easily be exposed. This paper investigates the problems of Shieh and Wang scheme in the verification procedure of the forged messages intercepted by the eavesdrop. An enhanced two-way remote user authentication scheme is proposed that is safe and strong against multiple attacks by adding the ability to perform integrity check on the server, and proposed scheme is not expose user password information and the system's confidential information.

키워드 : 상호인증, 중간자공격, 위장공격, 도청, 서비스거부공격, 스마트카드
Mutual Authentication, Man-In-The-Middle Attack, Impersonation Attack, Eavesdrop, DoS Attack, Smart Card

이 논문은 2012년도 성결대학교 교내연구비 지원에 의해 연구되었음.

* Corresponding Author, Industrial Management Engineering, Sungkyul University(E-mail : skcskc12@hanmail.net)
2012년 08월 13일 접수, 2012년 09월 06일 심사완료 후 2012년 09월 24일 게재확정.

1. 서 론

전자상거래나 인터넷 뱅킹이 이루어지고 있는 신뢰할 수 없는 공중망에서 원격접근을 위해 두 통신객체 간 식별자 인증은 보안요구사항으로 매우 중요한 메커니즘이다.

사용자 인증은 서버와 클라이언트 간에 서로 상대방을 확인하고 검증을 수행하는 과정으로 사용자는 미리 자신의 신원을 확인받기 위해 자신의 정보를 시스템(서버)에 등록하고 시스템이 제공한 인증정보에 의해 언제든지 정당한 사용자임을 검증받고 시스템이 제공하는 서비스를 받는다.

그동안 인증 스킴들은 효율성과 보안성측면에서 해시함수, 비밀키암호, 공개키암호 등 암호기법을 이용하여 개선되어 왔다. Lamport [4]는 불안전 통신망에서 원격 패스워드 인증 스킴을 최초로 제안했다[4].

그러나 이 스킴은 서버에 사용자들이 등록한 패스워드 리스트를 저장해야 하므로 중간자 공격(man-in-the-middle attack)에 대한 대책이 필요하다. 2000년 Hwang and Li[2]이 엘가말 공개키 암호에 기반을 둔 스마트카드 원격사용자 인증 스킴을 발표한 이래 지금까지 스마트카드 기반 원격사용자 인증 스킴들이 많이 제안되었다[2, 3, 5, 9, 12].

2005년 Lee et al.[6]은 효율성을 강조한 임의 난수(nonce) 기반의 원격사용자 인증 스킴을 제안하였다[6].

그러나 곧 이어 Shieh[9]는 Lee et al.[6] 스킴의 문제점으로 메시지 인증코드가 취약하다는 점을 지적하였다[9].

또한 2005년 Chen and Yeh[1]는 키 합의(key agreement)를 갖는 임의 난수기반의 원격사용자 인증 스킴을 제안하였다[1].

이 스킴은 병행세션공격, 재전송공격, 중간자공격에 안전하다는 장점이 있으나 인증을 위해 많은 해시연산을 요구한다.

이어 2008년 Shieh and Wang[10]은 Lee et al.[6] 스킴은 효율적이나 안전하지 않고 Chen and Yeh[1] 스킴은 안전하나 불필요한 연산을 필요로 한다고 주장하면서[10] Lee et al.[6] 스킴의 효율성과 Chen and Yeh[1] 스킴의 보안성, 그리고 키합의 방식을 조합한 효율적인 상호인증 스킴을 제안했다.

또한 Qi et al.[8]은 Liao et al.[7] 스킴이 중간자의 위장공격에 취약함을 지적하면서 스마트카드 분실이 있어도 안전한 개선된 스킴을 발표했다[8].

그러나 Qi et al.[8] 스킴은 로그인 및 인증과정에서 시도-응답에 의한 메시지 정보의 노출과다라는 문제가 있으며 도청 : intercept 가로채기) 공격으로 패스워드 추측(guess)이 가능하고 이로 인해 위장공격(forge attack)의 취약함을 가지고 있다.

이와 같이 취약한 메커니즘은 공격자가 비보호 채널에서 사용자와 서버 간에 주고받는 메시지를 쉽게 위조할 수 있으며 악의적인 공격자는 서버와 사용자를 속이기 위해 특별한 비밀정보 없이도 서버나 사용자로 위장할 수 있다.

강력한 패스워드 인증의 핵심은 사용자 인증으로 프라이버시 보호를 위한 도청방지이고 무결성(integrity)과 익명성(anonymity)을 보장받기 위해서는 추측에 의한 위장공격의 대책이 필요하다.

본 논문에서는 Shieh and Wang[10] 스킴이 중간자의 도청에 의해 쉽게 위조될 수 있으

며 그 위조된 메시지를 서버(시스템)에서 확인하지 못하는 검증절차의 문제점을 논한다.

또한 위조공격이 이루어지는 과정과 중간자 공격을 분석하고 임의 난수와 패스워드 기반 인증 스킴에서 취약한 Shieh and Wang[10] 스킴을 개선하여 내부자 공격, 추측공격, 재전송공격, 위장공격, 아이디 스푸핑(spoofing) 공격에 안전한 개체 간 상호인증 스킴을 제안한다.

제안 방법으로 사용자의 안전한 등록정보를 통해서 패스워드 정보가 노출되지 않도록 하고 서버(시스템)에서 무결성 검사를 할 수 있는 기능을 추가함으로써 중간자 공격에 안전한 강력하고 개선된 two-way 원격사용자 인증 스킴이다.

인증세션이 종료된 이후 재전송공격과 중간자공격을 방지하기 위해 사용자는 필요할 때에 자신의 스마트카드 패스워드를 임의로 변경할 수 있는 메커니즘을 추가하였다.

논문의 구성은 다음과 같다. 제 2장에서 Shieh and Wang[10] 인증 스킴을 검토, 분석하고 제 3장에서 개선된 프로토콜을 제시하며 제 4장에서 제안된 프로토콜의 안전성과 기능성을 분석한다. 제 5장에서 결론을 맺는다.

2. Shieh and Wang's 인증 스킴 검토

본 장에서는 Shieh and Wang[10]이 제안한 스마트카드 기반의 원격사용자 인증 스킴을 간략히 기술하고 안전성을 분석한다.

이 스킴의 가장 큰 특징은 스마트카드를 사용하는 환경에서 임의 난수기반의 상호인증 스킴으로 Lee et al.[6] 스킴의 효율성과 Chen and Yeh[1] 스킴의 키 합의 기능을 결합한 논문으로 인증에 필요한 메시지 교환을 최소화하기 위해 3-way handshake 프로토콜로 구성되어 있다.

본 논문에서 사용된 표기법은 다음과 같다.

〈Table 1〉 Parameters

Symbol	Description
⊕	exclusive-or
Ui	User i
IDi	Identifier of user i
x	Confidential information of system(server)
pwi	Password of user I(128bit)
S	System(server)
Nc	Random number of user i
Ns	Random number of system(server)
--->	common channel transfer
‖	Concatenation
h()	One way hash function

2.1 인증 스킴 절차

2.1.1 등록 단계

사용자 Ui는 아이디 IDi와 패스워드 pwi를 선택하여 다음 단계들을 수행한다.

(1) Ui는 패스워드 pwi, 식별자 IDi의 등록을 위해 안전한 채널을 통해 시스템 S에 전송한다.

(2) 시스템 S는 다음을 연산(식 (2.1))한다.

- $Ru = h(IDi \oplus x) \oplus pwi$ (2.1)

(3) 시스템 S는 스마트카드에 (Ru, h())를 저장하고 안전한 채널로 Ui에게 전송한다.

2.1.2 3-way handshake 스킴

3-way handshake 스킴은 사용자가 상호 인증과 키 합의를 위해 로긴할 때 마다 사용된다.

사용자는 카드리더기에 삽입하고 IDi, pwi를 입력하면 시스템과 스마트카드 사이에 시도응답을 위한 3개의 메시지가 생성되는 역할을 한다.

(1) 사용자 Ui는 로그인을 하기 위해 IDi, pwi를 입력한다.

(2) 스마트카드는 입력된 패스워드 pwi를 사용하여 식 (2.2)를 연산하고 임의 난수(Nc)를 생성하여 식 (2.3)을 산출해 낸다.

- SS = Ru⊕pwi = h(IDi⊕x) ⊕pwi⊕pwi = h(IDi⊕x) (2.2)
- 임의 난수 Nc 생성
- M1 = SS⊕Nc (2.3)

(3) 사용자 Ui는 자신의 식별자와 함께 M1을 시스템으로 전송한다.

- Ui--->S : IDi, M1

IDi, M1 메시지를 수신한 시스템은 인증단계인 메시지 교환(핸드세이킹)동안 메시지의 재전송 공격을 방지하기 위해 인증과정이 종료될 때까지 일시적으로 저장한다.

(4) 시스템은 IDi를 검증하여 유효여부를 판단한다.

(5) IDi, M1이 이미 메모리의 임시저장소에 저장되어 있다면 요청을 거절한다.

(6) M2와 M3를 생성하기 위해 사용자 Ui와 공유하는 공유비밀정보 SS 식 (2.4)를 연산하고 임의 난수(Ns)를 생성한다.
M2를 생성하기 위해 시스템은 공유비밀정보 SS를 x와 IDi를 이용하여 XOR 연산하고 사용자에게 요청을 위한 새로운 임의 난수 Ns를 생성한다.

- SS = h(IDi⊕x) (2.4)
- 임의 난수 Ns 생성
- M2 = SS⊕Ns (2.5)

(7) 사용자 Ui의 임의 난수(Nc)를 도출하기 위해 식 (2.4)을 이용하여 식 (2.6)을 연산한다.

- Nc = M1⊕SS (2.6)

(8) 사용자 Ui의 인증을 위해 M3를 생성한다.

- M3 = h(SS ‖ Nc ‖ M2) (2.7)

M2는 시스템의 임의 수 Ns로부터 보호되었다.
M3 연산을 위해 시스템만이 비밀공유정보 SS를 알고 있으며 수신한 M1에서 Nc를 추출할 수 있다.
M3 또한 M2를 위한 메시지인증코드(MAC)로써 역할이다.

(9) 시스템 S는 M2, M3를 사용자 Ui에게 전송한다.

- S-->Ui : M2, M3

(10) 시스템 S로부터 두 개의 메시지(M2, M3)를 수신한 Ui의 절차는 다음과 같다.
시스템 S를 인증하기 위하여 수신한

M2와 자신이 보유하는 SS, Nc를 이용하여 h(SS ‖ Nc ‖ M2)를 연산한 다음 식 (2.8)과 같이 수신한 M3와 비교함으로써 시스템 S를 인증하게 된다.

- M3 = ?h(SS ‖ Nc ‖ M2) (2.8)

(11) M3의 검증이 이루어지면 사용자 Ui는 M2로부터 Ns를 추출(식 (2.9))하고 Ns를 이용해서 M4 = h(SS ‖ Ns)를 연산(식 (2.10))한다.

- Ns = M2⊕SS (2.9)
- M4 = h(SS ‖ Ns) (2.10)

(12) 사용자 Ui는 M4를 시스템 S로 전송하여 자신의 정당함을 최종적으로 인증하도록 요청한다.

- Ui ---> S : M4

(13) 시스템 S는 3번째 메시지를 수신하여 h(SS ‖ Ns)를 연산하고 수신된 M4와 비교(식 (2.11))하여 사용자 Ui를 인증한다.

- M4 = ?h(SS ‖ Ns) (2.11)

(14) 시스템 S와 사용자 Ui의 최종인증이 완료되면 데이터 전송을 위한 동일한 세션키를 시스템 S와 사용자 Ui는 생성(식 (2.12))한다.

- h(SS ‖ Nc ‖ Nc) (2.12)

2.2 안전성 분석

본 절에서는 Shieh and Wang[10] 인증 스킴에 대해 중간자(Attack A)의 중간자 공격과 이로 인해 파생되는 안전성의 불안요인에 대해 분석한다.

3-way handshake에서 메시지는 비보호채널을 통해 전송되는 과정에서 공격자 A는 채널을 완전히 장악하여 메시지를 가로채 변조할 수 있다.

그때 시스템 S는 사용자 Ui의 인증 요청메시지 자체에 대해 IDi의 유효성을 확인하고 IDi와 M1 정보를 인증 세션동안 재전송공격을 차단하기 위해 임시저장소에 저장하고 있다.

그러나 IDi 외에 메시지가 유효한지 아닌지에 대해 검증할 장치가 없다.

또한 사용자 Ui는 시스템 S의 인증정보에 대해 정당한 시스템 S의 메시지임에도 불구하고 중간자의 개입으로 세션을 끊어 종료시킨다.

이것이 Shieh and Wang[10] 스킴에 대한 중대한 결점으로 이러한 가정 하에 이 스킴은 중간자 공격에 대해 불안한 인증 스킴이라는 것을 보여주고자 한다.

2.2.1 중간자 공격

<Figure 1>은 중간자인 공격자 A에 의해 중간자 공격이 이루어지고 이로 인해 파생되는 서비스거부를 도식하였다. 그림에서 공격자가 메시지 M1를 가로채서 공격자의 임의 난수 Na를 XOR하여 수정된 M1′(식 (2.13))로 대치하면 위조된 메시지는 S의 인증을 통과할 수 있다.

- M1′ = M⊕Na (2.13)

그러나 사용자 Ui는 시스템 S에 의해서 사용자의 아이디 IDi 이외에는 인증에 필요한

검증요소가 없다는 결점이 있다.

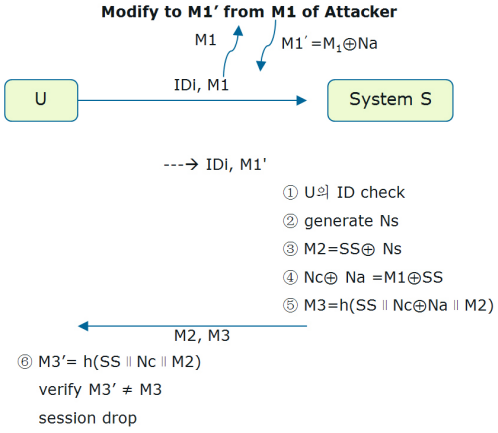
로그인단계에서 사용자 Ui는 시스템 S로 로그인 메시지 IDi, M1를 전송할 때 공격자 A는 이를 가로챈다. 공격자는 임의의 수 Na를 선택하여 M1′ = M1 ⊕ Na를 계산한다. 그리고 공격자는 위조된 메시지 IDi. M1′를 S로 전송한다. 이 경우 시스템 S는 다음과 같은 일이 발생한다.

로그인 메시지(IDi, M1)의 유효성은 사용자 IDi에 의존한다. 즉, 로그인 메시지(IDi, M1)의 유효성을 제 2.1.2절의 (4)항 밖에 검증할 요소가 없다는 것이다. 그러므로 공격자는 메시지를 위조하기가 아주 쉽다.

(1) 시스템 S는 메시지(IDi, M1)를 수신하여 임의 난수 Ns를 생성하고 M2(식 (2.14))를 연산한다.

- M2 = SS⊕Ns (2.14)

(2) 이어서 사용자 Ui의 난수를 획득하기 위해 식 (2.15)를 계산한다.



〈Figure 1〉 Example-1 : Denial of Service of Man in the middle attack

- Nc⊕Na = M1⊕SS (2.15)

(3) 시스템 S는 자신의 인증자 M3(식 (2.16))를 생성하여 M2와 함께 사용자 Ui로 전송한다.

- M3 = h(SS ‖ Nc⊕Na ‖ M2) (2.16)
- S---->Ui : M2, M3

(4) M2, M3를 수신한 사용자 Ui는 M3′(식 (2.17))를 생성한다.

- M3′ = h(SS ‖ Nc ‖ M2) (2.17)

(5) 시스템 S로부터 전송된 M3와 자신이 생성한 M3′를 비교하여 시스템 S를 인증하게 된다. 그러나 식 (2.18)과 같이 값이 동일하지 않는다. 결국 사용자 Ui는 정당한 시스템 S인데도 정당하지 않은 시스템으로 인식하여 인증을 거부하고 세션을 종료시킨다.

- M3′≠M3 (2.18)

2.2.2 비밀키 x(bit XOR 연산)의 취약성

<Figure 2>는 시스템 S의 공통비밀키의 취약성이 미치는 영향을 보여주고 있다.

모든 사용자들은 등록 단계에서 시스템 S에 의해 공통비밀키 x와 ID, pw를 사용하여 Ru = h(ID⊕x)⊕pw를 구하고 스마트카드에 저장하고 있다. 시스템 S의 공통비밀키 x의 취약점은 모든 가입자(멤버)들에게 동일하게 적용되는데 문제가 있다.

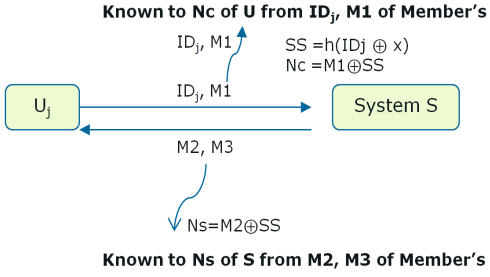
공통비밀키 x가 모든 사용자들에게 공통으로 적용되지 않았다면 시스템 S는 ID, M1을 수신한 후 식 (2.4) SS = h(IDi⊕x)를 계산할

수 없다. 계산이 가능하다면 시스템 S는 모든 멤버들에게 사용된 비밀키들을 저장하고 있어야 한다. 이것은 Shieh and Wang[10]이 주장한 비밀정보 테이블을 사용하지 않는다는 원칙에 위배된다.

<Figure 2>는 공격자 A가 임의로 추출한 추측 비밀키 x′를 적용하여 SS를 구할 수 있다.

공격자 A는 SS와 ID를 알고 있기 때문에 SS′ = h(IDi⊕x′)를 계산한 후 SS와 비교하여 일치여부를 확인한다.

수식계산에서 ⊕는 bit 연산이므로 고정된 ID의 bit수에 따라 결정되며 ID가 16bit이면 해시연산을 2^{16}회, 32bit이면 2^{32}회 반복하여 x를 알아낼 수 있다.



〈Figure 2〉 Secret key Guess of Member's

3. 제안스킴

본 논문에서는 제 2.2절 Shieh and Wang [10] 스킴의 중간자공격 결점을 보완한 개선된 스마트카드 기반의 원격 사용자인증 스킴으로 등록단계, 로그인단계, 인증 및 패스워드 변경 단계로 제안한다.

제 2.1절에서 정당한 사용자와 시스템(서버)간의 인증에서 중간자의 위장된 메시지에 의해 상호인증 결여와 일방적으로 중간자 공격에 의한 세션이 종료되는 일종의 서비스거부공격이 발생한다.

제안 스킴은 중간자의 변조, 위조공격을 근본적으로 차단할 수 있는 사용자와 서버간의 강력한 상호인증 프로토콜을 제안한다.

세부 제안내용은 서버(시스템)에 등록할 때 패스워드를 해시 값으로 생성하여 보안성을 유지하고 사용자 로그인 정보에 대해서 서버(시스템)에서 무결성 검사를 하여 메시지 위조여부를 검증한다. 또한 해시함수를 이용하여 중간자가 위조된 인증 데이터를 생성할 수 없도록 구성하고 스마트카드의 사용자패스워드를 임의로 변경할 수 있도록 함으로써 중간자에 의한 도청 및 재 전송공격, 위장공격을 효율적으로 차단할 수 있는 프로토콜이다.

본 인증 스킴은 공격자가 로그인 단계 및 인증 단계에서 시스템과 사용자간의 통신과정을 모두 통제할 수 있으며 통신과정에서 메시지를 도청, 삽입, 삭제, 수정할 수 있다는 가정으로 논의하고자 한다.

3.1 등록 단계

사용자 Ui는 원격시스템에 등록을 할 때 다음의 절차를 갖는다.

(1) 사용자 Ui는 임의의 패스워드 pwi를 IDi와 함께 연산 (h(pw‖IDi))하여 안전한 채널로 IDi, h(pwi‖IDi)를 시스템 S에 전송한다. 사용자의 패스워드 정보는 자신만이 아는 비밀정보로 시스템 S에게 노출되지 않는다.

(2) 시스템 S는 자신의 비밀키 x를 이용하

여 식 (3.1)과 스마트카드 소유자 인증을 위한 정보 식 (3.2)를 연산한다.

- As = h(IDi ‖ x)⊕h(pwi ‖ IDi) (3.1)
- K = h(pwi ‖ IDi)⊕h(As) (3.2)

시스템 S의 비밀키 x는 모든 스마트카드 발급자에게 공통으로 사용되며 각 사용자에 대한 비밀정보 테이블을 보유하지 않는다. 시스템 S는 스마트카드에 As, K, h()를 저장하여 안전한 채널을 이용, 사용자 Ui에게 전송한다.

3.2 로그인 단계

사용자 Ui는 다음과 같은 단계로 로그인 과정을 갖는다.

(1) 사용자 Ui는 스마트카드를 삽입하고 단말입력장치를 통해 IDi와 pwi(3회 입력 제한)를 입력한다.
스마트카드는 식 (3.3)을 연산하여 스마트카드 소유자에 대한 카드유효성을 검증한다.

- h(As) = ? K ⊕ h(pwi ‖ IDi) (3.3)

(2) 스마트카드와 소유자를 검증 후 시스템 시간 t1를 획득하여 다음 식 (3.4)~식 (3.6)을 연산한다.

- CID = h(pwi ‖ IDi)⊕h(As ‖ t1) (3.4)
  // CID : Changable ID
- F = h(CID ‖ h(pwi ‖ IDi)) (3.5)
  // F : Factor
- R1 = h(t1 ‖ As ‖ F) (3.6)
  // R1 : Result1

(3) 사용자 Ui는 R1, t1, As를 비보호채널을 통해 시스템 S로 전송한다.

- Ui--->S : R1, t1, As

3.3 인증단계

시스템 S는 R1, t1, As를 수신하여 다음과 같은 인증과정으로 이루어진다.

(1) 사용자 Ui의 IDi를 체크하여 유효성을 검사하고 메시지를 전달받은 시각 t을 구하고 (t-t1)≥△t이면 사용자 Ui의 로그인 요청을 거절한다. 여기서 △t는 전송시간을 고려한 최소 인증시간이다.

(2) 시스템 S는 R1의 유효성 판단을 위해 F를 생성할 수 있어야 한다. F를 생성하기 위해 CID를 생성하여야 하고 CID를 생성하기 위해서는 h(pwi ‖ IDi)를 도출할 수 있어야 한다.
다음은 식 (3.7)에서 h(pwi ‖ IDi)를 도출하고 식 (3.8)~식 (3.9)을 통해서 CID와 F를 연산한 이후에 유효성 식 (3.10)을 인증한다.

- h(pwi ‖ IDi) = As⊕h (IDi ⊕ x) (3.7)
- CID = h(pwi ‖ IDi)⊕ h (As ‖ t1) (3.8)
- F = h(CID ‖ h(pwi ‖ IDi)) (3.9)

(3) 식 (3.10)을 체크하여 사용자 IDi를 인증한다.

- R1 = ?h(t1 ‖ As ‖ F) (3.10)

(4) 사용자 Ui에 대한 인증이 이루어지면

인증결과를 사용자 Ui에게 보내 시스템 S의 적법성 인증을 요구한다.
시스템 S는 시스템시간(t2)을 획득하여 사용자 Ui가 시스템 S를 인증할 수 있도록 시스템 S가 검증을 위해 생성한 CID, h(pwi ‖ IDi)를 사용하여 D 식 (3.11)를 생성한다.

- 시스템 시간 t2를 얻는다.
- R2 = h(t2 ‖ F) (3.11)
  //R2 : Result2

(5) 시스템 S는 사용자 Ui로 R2, t2를 전송하여 정당한 시스템임을 증명한다.

- S-->Ui : R2, t2

(6) 사용자 Ui는 R2, t2를 수신하여 정당한 시스템 S임을 확인하기 위하여 (t-t2) ≥△t이면 시스템 S의 메시지를 거절한다. 또한 사용자 Ui는 자신이 생성하여 보관하고 있는 F를 사용하여 식 (3.12)을 통해 시스템 S로부터 전송된 R2를 비교한 후 일치하면 합법적인 시스템 S로 인증된다.

- R2 = ? h(t2 ‖ F) (3.12)

이와 같이 시스템 S에서 h(pwi ‖ IDi), CID, F를 생성할 수 있는 능력이 있다는 것은 사용자 Ui에게 시스템 S는 정당하게 인증되었음을 확인시키는 것이다.

3.4. 패스워드 변경

사용자 Ui는 임의 새로운 패스워드(pwi′)를 선택하여 시스템 S와는 독립적으로 스마트카드에 내장된 h(pwi⊕IDi)의 값을 변경할 수 있다.

(1) 사용자 Ui는 IDi, pwi 입력을 통해 로그인 인증프로세스가 정상적으로 수행된다.

(2) 현재의 pwi와 임의 새로운 pwi′ 입력하면 식 (3.13)이 연산되어 스마트카드는 현재의 As를 As′로 변경되고 K값 대신에 K″ 식 (3.16)로 대체되어 저장된다.

- As′ = As ⊕h(pwi ‖ IDi)⊕h (pwi′ ‖ IDi) (3.13)
- h(As′) (3.14)
- K′ = K⊕h(As)⊕h(As′) (3.15)
- K″ = K′⊕ h(pwi ‖ IDi)⊕h (pwi′ ‖ IDi) (3.16)

4. 안전성 분석

4.1 보안분석

제안한 인증 스킴의 안전성과 효율성에 대해 평가한다.

4.1.1 내부자 공격(Insider Attack) 대응

<Figure 3>의 (1)에서 사용자 Ui는 시스템 S에 안전한 채널을 통해 등록할 때 128bit의 패스워드를 노출시키지 않고 해시 h(pwi ‖ IDi)한 정보를 제공함으로 사용자의 패스워드를 확인할 수 없으며 시스템 S에서 내부적으로 패스워드를 보관하지 않으므로 내·외부자 공격에 안전하다.

Shieh and Wang[10] 스킴에서는 등록정보(IDi, pwi)를 그대로 시스템에 노출시키고 있어 내부자들이 ID와 함께 쉽게 알 수 있고 탐지여부는 시스템 S의 의지에 달려 있었다.

그러나 본 스킴에서는 pwi를 유추하기 위해서는 pwi와 IDi의 해시연접연산에서 128비트를 사용하므로 bit XOR 연산의 2^{128}보다 훨씬 복잡하고 많은 시간이 소요되고 또한 필요시 세션마다 pwi의 값이 변경되므로 안전하다.

4.1.2 중간자에 의한 위장공격(Forge Attack) 대응

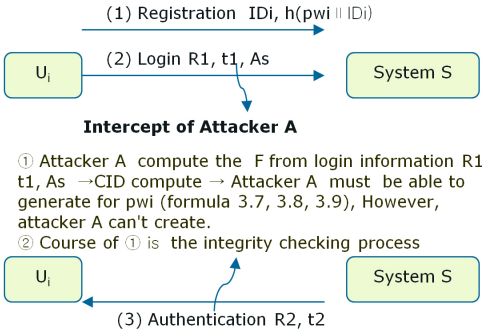
위장 공격은 공격자가 프로토콜에 참여하여 자신을 임의의 합법적인 사용자로 가장하여 정당한 사용자로 행동하는 것으로 사용자의 식별자와 패스워드를 알아야 한다.

Shieh and Wang[10] 스킴에서는 사용자 Ui에 대한 ID만으로 검증되고 있으며 시스템의 인증정보 생성에서 IDi, M1을 수신하여 M1 메시지에 대한 검증단계가 없이 M1을 이용하여 Nc를 구하고 M2, M3를 생성하고 있다. 그러므로 수신된 메시지의 위조여부를 알 수 없다.

이것은 로그인 메시지에 대해 중간자가 해킹하여 내용을 변조, 위조하여도 시스템은 위조여부를 판단할 수 있는 무결성 검사를 하지 않고 있다는 취약점을 가진다.

본 스킴에서는 <Figure 3>의 (2), (3)과 같이 중간자(Attack A)가 정당한 사용자의 로그인 메시지를 도청(가로채기)하더라도 사용자의 pwi를 알기 위해서는 유기적인 연산(F 연산, CID 연산, pwi 도출)이 이루어져야 한다.

Shieh and Wang[10] 스킴에서 취약점은



〈Figure 3〉 Integrity check of Member's

시스템의 비밀키 x를 가입멤버에게 공통적으로 사용자의 아이디와 적용한 해시 값 h(IDi ⊕x)이므로 비밀키 x를 유추하여 위조, 변조가 가능했다.

본 제안에서는 로그인정보에서 사용자 Ui의 해시 값 h(pwi ‖ IDi)을 적용하여 <Figure 3>의 (2), (3) 정보가 유출되더라도 3단계의 연산과정을 정당하게 통과해야 한다.

등록 단계에서 시스템 S는 As = h(IDi ‖ x) ⊕h(pwi ‖ IDi)를 해시 값으로 생성하여 공격자 A는 비밀키(x)와 패스워드(pwi)를 얻을 수 없으며 이로 인해 식 (3.9)를 생성할 수 없다.

또한 무결성은 송·수신측에서 모두 수신된 메시지의 위조여부를 확인하는 과정으로 시스템 S의 메시지 인증과정 식 (3.7)~식 (3.9)과 같이 메시지의 무결성 체크와 더불어 중간자의 위조여부를 쉽게 알 수 있다.

4.1.3 재전송공격(Replay Attack)대응

메시지의 재전송공격은 이전 세션에서의 메시지를 중간자가 보관하다가 다음 세션에서 재전송하는 방법으로 인증을 시도하는 공격이다.

Shieh and Wang[10] 스킴에서는 사용자

Ui의 로그인 정보를 재전송방지를 위해 인증세션(3-way handshaking)이 이루어지는 동안에만 임시저장소에 저장하여 중간자가 가로챈 사용자 Ui의 IDi, M1 정보가 전달되면 재전송공격으로 간주하고 있다. 인증세션 이후에는 임시저장소는 삭제되기 때문에 실효성에 의문이 생긴다.

제안 스킴에서는 하나의 세션에서 로그인 정보 R1, t1, As를 가로채어 보관하다가 인증단계에서 전에 사용했던 로그인 메시지를 재생한다 해도 $(t-t1) \geq \triangle t$에 의해 실패한다.

또한 매 세션마다 pwi′을 선택하여 As′ = As ⊕h(pwi ‖ IDi)⊕h(pwi′ ‖ IDi), K″ = K′⊕ h(pwi ‖ IDi)⊕h(pwi′ ‖ IDi)를 생성한다.

As′의 생성은 CID, F, R1에 전혀 다른 값으로 영향을 주므로 재전송공격에 안전하다.

공격자가 재전송공격을 하기 위해서는 이전 세션에서 획득한 CID의 타임스탬프 T를 $(t-t1) \geq \triangle t$을 만족하는 새로운 t1으로 변경할 수 있어야 하는데 CID는 식 (3.5)와 같이 해시되어 안전하다.

4.1.4 상호인증(Mutual Authentication)

Shieh and Wang[10] 스킴은 매 세션마다 생성되는 사용자 Ui의 임의 난수 Nc와 시스템의 난수 Ns에 의존하여 3-way handshaking이 완료된 후 인증여부를 확인하고 시스템 S의 서비스를 받는 구조이다.

이 모순된 구조에 의하여 <Figure 1>과 같이 시스템 S의 유효성 검증이 취약하기 때문에 중간자공격이 가능하며 사용자 Ui와 시스템 S의 상호인증과정이 종료되지 않은 채 정당한 사용자나 시스템이 인증정보를 제공했음에도 불구하고 접속이 거절되었다.

제안 스킴은 원격접속을 위한 사용자의 인증과 사용자가 원격시스템을 인증할 수 있는 상호인증을 구조를 제공한다. 정당한 시스템만이 사용자의 비밀정보 h(pwi ‖ IDi)와 CID, F, R1을 생성 유도할 수 있는 구조를 갖는다.

식 (3.7)의 정보 h(pwi ‖ IDi)를 생성할 수 있어야 매 세션마다 변경되는 비밀정보 h(pwi′ ‖ IDi)를 만들 수 있다.

이는 정당한 시스템만이 비밀키 x를 이용하여 h(pwi ‖ IDi), CID, F, R1을 생성할 수 있다. 시스템이 생성한 R2정보는 사용자 Ui의 중요한 인증요소가 된다. CID, R2의 생성은 합법적인 시스템 S가 아니면 생성할 수 없음을 보여준다.

본 스킴의 상호인증은 Shieh and Wang[10] 스킴과 비교해 볼 때 인증메시지의 유효성을 확인하는데 있어서 메시지의 설계에 본질적 결함(확실한 인증요소제공의 미흡)을 M1, M2, M3대신에 CID, F, R1을 설계함에 중점을 두고 있다.

4.1.5 추측 공격(Guess Attack)과 ID Spoofing

<Figure 2>에서 시스템 S의 공통비밀키 x가 미치는 취약성에 대해 분석하였다.

시스템 S의 공통비밀키 x의 취약점은 모든 가입자(멤버)들에게 동일하게 적용되는데 문제가 있다.

식 (2.2)에서 SS = h(IDi⊕x)은 bit연산이므로 고정된 ID의 bit 수에 따라 결정되며 ID가 16bit이면 해시연산을 2^{16}회, 32bit이면 2^{32}회 반복하여 x를 추측하여 알아낼 수 있는 취약성을 갖는다.

이러한 위장공격으로 파생되는 취약성은 중간자에 의한 ID Spoofing으로 이어져 얼마

든지 위장이 가능하다.

제안 스킴에서는 중간자가 사용자 Ui의 로그인 메시지 R1, t, As를 가로채고 스마트카드의 h()를 사용한다고 하더라도 CID, F의 인증 데이터 생성이 불가능하다.

중간자가 패스워드를 획득하기 위해서는 식 (3.4)의 CID = h(pwi ‖ IDi)⊕h(As ‖ t1)에서 128비트의 해시연접연산을 해결해야 한다. 또한 오프라인 추측 공격에 취약한 pwi의 경우에도 직접 사용되지 않고 모든 연산에서 h()로 연산되므로 추측 공격에 대응할 수 있다.

4.2 기존 인증 스킴과의 비교

제 4.1절 보안분석을 기초로 제안된 인증 스킴과 Lee et al.[6], Chen and Yeh[1], Shieh and Wang[10] 스킴에 대한 보안성 분석을 <Table 2>와 같이 비교하였다.

Lee et al.[6] 스킴은 상호인증과정을 단순한 절차로 하여 연산비용에 대한 효율성을 강조하였고 Chen and Yeh[1] 스킴은 Lee et al.[6] 스킴을 보완하였다.

사용자와 시스템 간에 상호인증 과정이 완료된 후 인증에 대한 결과물로써 사용자와 시스템 간에 동일한 세션키를 생성한다.

위에서 언급한 3개의 스킴들은 신속하고 효율성에 맞춘 스킴들인 만큼 전자상거래나 인터넷 뱅킹의 전자지불시스템에서 보안의 위험에 다소 부담이 적은 소액지불 프로토콜에 적용하는 것이 바람직하다고 본다.

분석결과 그 이유는 다음과 같다.

첫째, 시스템 S에서 메시지의 무결성 검사를 누락하여 불안전한 상호인증의 결과를 가져오고 있다.

이로 인해 중간자의 메시지 위조에 대한 검증장치가 없이 3-way handshake 세션 종료 후 사용자 Ui와 시스템 S에 대한 인증이 종료되는 구조를 가지는 있으며 상호인증 스킴으로 적절하지 않다.

둘째, 사용자 Ui는 최초 등록시 패스워드를 그대로 시스템 S에 노출시킴으로써 내부자 공격의 가능성이 항상 존재한다.

셋째, 임시저장소를 사용하여 인증 세션시간 동안 제한적으로 재전송공격을 탐지하고 있는데 이것은 세션 종료 후에는 재전송공격 방지를 위해 모든 가입자 멤버에 대해서 로그인 정보(IDi, M1)를 저장하고 있어야 한다.

마지막으로 시스템 S의 비밀정보(키)는 비밀정보에 대한 크기도 정의되지 않았을 뿐 아니라 사용자의 ID를 bit XOR 연산에 의해 보안의 취약성을 갖는다.

이것은 사용자와 시스템의 임의 난수인 Nc, Ns를 쉽게 알아냄으로써 중간자에 의해 송신자의 ID를 위조하는 spoofing 공격에 취약함을 알 수 있다.

본 절에서의 보안기능 분석은 Shieh and Wang 스킴의 취약성을 중심으로 분석결과를 비교하였다.

<Table 1>에서 기존 Lee et al.[6], Chen and Yeh[1], Shieh and Wang[10] 스킴이 기능분석결과 상호인증의 부적절과 시스템 S의 비밀키에 대한 추측이 가능한 결과로 인해 도래되는 내・외부자 공격대응 기능, 위장 공격대응(무결성) 기능, 재전송공격방지 기능, 추측 공격방지 기능, ID 스푸핑공격, 상호인증 기능에 대한 취약함을 알 수 있다.

Shieh and Wang[10] 스킴이나 제안 스킴에서 replay 공격이 “일부가능”하다는 것은

〈Table 2〉 Function analysis

기능	Lee et al.[6]	Chen and Yeh[1]	Shieh and Wang[10]	Proposed Scheme
Inside attack	vulnerability	password exposure (weakness)	password exposure (weakness)	use the hash value(password) (safety)
Forge attack	vulnerability	no integrity checking(weakness)	no integrity checking(weakness)	integrity checking (safety)
Replay attack	partially vulnerability	vulnerability after the session	vulnerability after the session	depending on the system's △T (weakness)
ID spoofing, Guess attack	vulnerability	weakness of symmetric key x	weakness of symmetric key x	authentication data is not guessing by attacker(safety)
Mutual authentica-tion	partially in-appropriate	vulnerability of verification	vulnerability of verification	legitimate users and the system only generates a secret information (safety)

완전히 공격을 배제하지는 못하기 때문이다.

이와 같이 제안된 인증 스킴은 가변인증자(CID)와 무결성 검사를 통하여 위장공격과 상호인증의 근본적인 취약성을 제거함으로써 재전송공격, 추측 공격 등으로부터의 안전이라는 부수적인 효과를 가진다.

Hwang and Li[2] 스킴, Li et al.[7] 스킴들과 비교하여 제안된 스킴의 해시연산 비용을 <Table 3>에서 보여주고 있다. 제안된 스킴의 연산 복잡도 분석을 위해 단방향함수 연산시간을 Th로 표기한다.

〈Table 3〉 Comparison of Computation, Communication

Step	Lee et al. [6]	Chen and Yeh[1]	Shieh and Wang[10]	Proposed Scheme
Registration	2h, 2⊕	1h, 2⊕	1h, 3⊕	4h, 2⊕
Login	2⊕	1h, 2⊕	2⊕	4h, 2⊕
Authenti_ cation	5h, 4⊕	8h, 4⊕	5h, 4⊕	7h, 2⊕
Password change	no	no	no	7h, 6⊕
Communi_ cation	3	3	3	2

⊕ : XOR bit operation h : hash function

제안한 스킴에서 XOR 연산은 단순연산으로 성능에 영향을 주지 않으므로 해시연산만을 고려하였다.

등록단계와 로그인 단계, 패스워드 변경단계에서 다소 많은 연산 량이 도출되었지만 해시함수 성격상 시스템 전체에 주는 영향은 크지 않다. Shieh and Wang[10] 스킴을 개선시키기 위한 무결성과 비밀정보의 안전성을 확보하였고 공중망(불안전 채널)을 통해 전송되는 정보는 2회로 단순화하여 불필요한 정보의 노출을 축소시켰다.

5. 결 론

전자상거래와 인터넷 뱅킹이 활성화되면서 스마트카드의 사용은 필수적이다.

그 가운데 스마트카드에 대한 안전성 확보

가 가장 중요하며 여러 보안요소 중 객체 간 상호인증은 매우 중요하다.

스마트카드를 이용한 인증 스킴은 공격자가 스마트카드의 내부 정보를 추출한다 하더라도 그 정보를 이용하여 사용자의 패스워드나 시스템의 비밀키를 탐지할 수 없도록 설계되어야 한다.

특히 보안의 취약점이 어느 한곳에서 발생되면 그것으로 파생되어 추가적인 보안의 결함들이 연속적으로 나타나는 가능성을 본 논문에서 증명하고 있다.

Shieh and Wang[10] 스킴은 Lee et al.[6] 스킴과 Chen and Yeh[1] 스킴의 장점을 조합해서 연산비용의 효율성과 인증세션 종료 후 상호간 세션키를 생성하는 키합의 스킴에 중점을 두었을 뿐 보안요소에 대한 고려는 부족했다.

여기서 사용자와 시스템 간에 생성된 세션키는 인증이 완료된 이후에 실제 데이터를 주고받을 때 데이터를 암호화하는 암호키로 사용하기 위한 것으로써 인증 스킴의 인증프로토콜과는 다소 거리가 있는 주장이다.

이러한 문제로 Shieh and Wang[10] 스킴은 제 2.2절에서와 같이 무결성 검사를 누락시켜서 중간자공격에 의한 메시지위조를 확인하지 않고 응답인증메시지를 생성하여 전송함으로써 상호인증의 부적절을 초래했다.

특히 시스템 S의 비밀키 x는 bit XOR 연산에 의해 쉽게 탐지되는 구조를 가짐으로써 연속된 도청으로 인한 추측공격, 메시지 위장공격, ID 스푸핑공격 등에 취약함을 보였다.

등록과정에서 사용자의 패스워드를 시스템 S에 그대로 노출하여 조직 내의 내부자 공격에 빌미를 줄 수 있었고 사용자의 로그인 정보를 임시저장소에 저장하여 재전송 공격을 탐지하는 것도 세션종료 이후에 재전송공격이 이루어 질 경우의 대책은 없었다.

본 논문에서는 Shieh and Wang[10] 스킴의 취약점인 부적절한 상호인증 프로토콜을 보완하여 합법적인 사용자와 시스템을 인증하는 프로토콜을 구성하였다.

사용자의 패스워드 등록정보를 해시 값으로 하여 보안성을 강화하였고 사용자의 로그인정보에 대해 무결성 검사(CID, F값의 유기적 검증)를 함으로써 메시지의 변조, 위조여부를 확인할 수 있었다.

또한 인증세션이 종료된 이후 사용자는 자신의 스마트카드 패스워드를 임의로 변경하여 추측공격에 안전한 메커니즘을 제안하였다.

향후 비도와 인증요소 강화를 위해 생체요소 및 비밀키암호에 의한 강력한 3-factor 인증을 요구한다. 본 논문에서 제안한 프로토콜은 스마트카드를 사용하는 사용자인증에 효율적인 메커니즘으로 기대된다.

References

[1] Chen, Y. C. and Yeh, L. Y., “An Efficient nonce-based authentication scheme with key agreement,” Applied Mathematices and Computation, Vol. 169, pp. 982-994, 2005.

[2] Hwang, M.-S. and Li, L. H., “A New Remote User Authentication Scheme Using Smarts Cards,” IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, 2000.

[3] Kim, S. K. and Chung, M. G., “More se-

cure remote user authentication scheme," Computer Communications, Vol. 32, No. 6, pp. 1018-1021, 2009.

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

[5] Lee, N. Y. and Chiu, Y. C., "Improved remote authentication scheme with smart card," Computer standards and Interface, Vol. 27, No. 2, pp. 177-180, 2005.

[6] Lee, S. W., Kim, H. S., and Yoo, K. Y., "Efficient nonce-based remote user authentication scheme using smart cards," Applied Mathematices and Computation, Vol. 167, pp. 355-361, 2005.

[7] Liao, I. E., Lee, C.-C., and Hwang, M.-S. : IDentity-based deniable authentication protocol from pairings. IMSA 2006 : 112-114.

[8] Qi Xie, Wang, J.-K., Chen, D.-R., and Wang, X.-Y., "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.

[9] Shieh, W. G., "The Weakness of Efficient nonce-based remote user authentication scheme using smart cards," WSEAS Trans. on Information Science and Applicayions, Vol. 3, No. 3, pp. 584-587, 2006.

[10] Shieh, W. G. and Wang, M. T., "A Cost Effective Mutual authentication scheme with Key Agreement using smart cards," International Journal of Information and Management Sciences, Vol. 19, No. 4, pp. 571-587, 2008.

[11] Song, R., "Advanced smart card based password authentication protocol," Computer standards and Interface, Vol. 32, pp. 321-325, 2010.

[12] Xu, J., Zhu, W. T., and Feng, D. G., "An improved smart card based password authentication scheme with provable security," Computer standards and Interface, Vol. 31, No. 4, pp. 723-728, 2009.

저 자 소 개

신광철	(E-mail : skcskc12@hanmail.net)
1985년	서울과학기술대학교 전자계산학과 (학사)
1990년	국방대학원 전자계산학과 (석사)
2003년	성균관대학교 대학원 정보공학과 (박사)
2004년~현재	성결대학교 산업경영공학부 교수
관심분야	스마트카드보안, 전자지불시스템, 네트워크 및 RFID 보안