Journal of The Korea Society of Computer and Information
Vol. 17 No. 7 , June 2012

2012-17-7-3-4

Li & Hwang's 생체기반 인증스킴에 대한 취약성 분석 및 개선

신 광 철*

Structural vulnerability analysis and improvement of a biometrics-based remote user authentication scheme of Li and Hwang's

Kwang-Cheul Shin*

요 약

최근 Li & Hwang의 스마트카드를 이용한 생체기반의 원격 사용자 인증 스킴은 난수를 사용하여 스마트카드, 일방향 함수, 생체정보에 기반을 둔 연산비용 효율이 매우 뛰어난 장점이 있다고 주장한다. 하지만 이 스킴은 적절한 인증을 제공하지 못하고 특히 도청, 위장공격에 의한 서비스거부(DoS)공격에 취약한 보안스킴으로 분석되고 있다.

공격자는 비보호 채널에서 사용자와 서버 간에 주고받는 메시지를 쉽게 위조할 수 있으며 악의적인 공격자는 서버를 속이고 사용자를 속이기 위해 비밀정보 없이도 서버나 사용자로 위장할 수 있다. 본 논문에서는 사용자의 패스워드정보를 노출하지 않고 가변인증자와 OSPA를 적용하여 서버에서 무결성 검사를 할 수 있는 기능을 추가하였다. Li & Hwang의 취약점인 가장공격과 상호인증을 보완함으로써 여러 공격에 대응할 수 있는 강력한 개선된 스킴을 제안한다.

▶키워드 : 상호인증, 생체, 정보보안, 서비스거부공격, 스마트카드

Abstract

Recently, Li and Hwang scheme proposed a biometrics-based remote user authentication scheme using smart card. It is asserted that this scheme has very excellent benefits by the operation cost efficiency based on the smart card, one-way function and biometrics using random numbers. But this scheme cannot provide the properly authentication, especially, it is analyzed as the vulnerable

• 제1저자 : 신광철
• 투고일 : 2012. 03. 16, 심사일 : 2012. 04. 16, 게재확정일 : 2012. 05. 14.
* 성결대학교 산업경영공학부(Dept. of Industrial Management Engineering , Sungkyul University)

security scheme for Denial-of-Service(DoS) attacks by impersonate attacks.

The attacker controls the insecure channel, they can easily fabricate messages to pass the user's or server's authentication, and the malicious attacker can impersonate the user to cheat the server and can impersonate the server to cheat the user without knowing any secret information.

This paper proposes the strong improved scheme which can respond to multiple attacks by supplementing the function of integrity check from the server which applied variable authenticator and OSPA without exposing the user's password information. It is supplemented pregnable of disguise attack and mutual authentication of Li and Hwang scheme.

▶Keywords : Mutual Authentication, Biometrics, Information Security, DoS attack, Smart Card

I. 서 론

공중망에서 두 통신객체 간 식별하는데 있어서 네트워크 식별자 인증은 보안의 중요 메커니즘이다.

Lamport('81)는 불안전 통신망에서 원격 패스워드 인증 스킴을 최초로 제안했다[1]. 그러나 이 스킴은 서버에 패스워드 리스트를 저장해야 하고 중간자공격에 대항할 수 없다. 2000년 Hwang & Li의 엘가말 공개키 암호에 기반을 둔 스마트카드 원격사용자 인증 스킴이 제안된 이래 지금까지 스마트카드 기반 원격사용자 인증 스킴들이 많이 제안되었다[2-6].

일반적으로 원격사용자 인증 스킴에 대한 일반적인 보안의 효과는 다음과 같다.

- 반복적인 등록과정 없이 다중 서버 네트워크 구조에 대한 호환성이 있어야 하며 스마트카드의 연산부하를 감소시켜야 한다.
- 검증테이블, 패스워드테이블을 권장하지 않으며 다양한 공격에 방어할 수 있어야 한다.
- 패스워드나 ID를 자유로이 선택, 업데이트할 수 있는 기능을 가져야 한다.

전통적 사용자 인증 방법은 ID, pwi에 의존하기 때문에 잃어버리거나 훔치거나 공개되거나 잊혀질 수 있으며 정당한 사용자로부터 접근권한(ID, pwi)을 획득하려는 제3자를 식별할 수 없다.

이에 반해 생체적 특징인 지문, 얼굴, 홍채는 생체적 행동특징을 측정하는 기반으로 식별자검증 자동화 방법으로 더욱 신뢰를 제공한다. 이들 생체 특징들은 보편적이고 유일하며 분실되거나 잃어버렸을 경우도 복제될 수 없다. 일반적 생체 인증시스템에서 특징정보는 사전 저장된 템플릿과 비교하여 생체데이터를 스캔, 추출하는 것이다.

Li & Hwang[7]이 2010년 제안한 스마트카드를 이용한 생체기반 원격 사용자인증 스킴은 적절한 인증을 제공하지 못하고 특히 도청, 위장공격에 의한 서비스거부공격(DoS : Denial of Service Attack)에 취약한 보안스킴으로 분석되고 있다.

Li et al's는 비보호 채널로 전송되는 로그인과 인증 메시지를 공격자가 가로채서 서버를 속일 수 있는 중간자 공격의 취약점을 지적하였다[8].

공격자는 비보호 채널에서 사용자와 서버 간에 주고받는 메시지를 쉽게 위조할 수 있으며 악의적인 공격자는 서버를 속이기 위해, 또 사용자를 속이기 위해 특별한 비밀정보 없이도 서버나 사용자로 위장할 수 있다.

본 논문에서는 사용자의 패스워드정보를 노출하지 않으면서 Li & Hwang 스킴의 위장공격에 의한 중간자격을 분석하고 패스워드기반 인증스킴에서 취약한 추측공격, 재전송공격, 위장공격, stolen-verifier 공격, Dos공격에 대하여 대안으로 서버에서 무결성 검사를 할 수 있는 기능을 추가하여 여러 공격에 대응할 수 있는 강력한 개선된 생체기반 원격사용자 인증스킴을 제안한다. 논문의 구성은 다음과 같다. 2장에서 Li & Hwang's 인증스킴을 검토, 분석하고 3장에서 개선된 프로토콜을 제시하고 4장에서 제안된 프로토콜의 안전성과 기능성을 분석한다. 5장에서 결론을 맺는다.

II. Li and Hwang's 인증 스킴 검토

이 스킴의 가장 큰 특징은 인증스킴을 효율적으로 하기 위해서 해시함수와 난수만을 사용하였다. 신뢰하는 등록센터

(R), 서버(S), 사용자(U)로 구성되며 R은 비밀키 xs를 선택하여 안전한 채널을 통해 S로 분배하여 서버의 비밀키로 사용된다. 등록단계, 로그인단계, 인증단계, 패스워드 변경단계 4단계로 되어있다.

● 시스템 계수

Li & Hwang's 스킴의 프로토콜에 사용될 용어에 대한 정의이다.

- ID : 사용자의 식별자
- xs : 서버의 비밀키
- pwi :패스워드
- U : 사용자
- S : 서버
- R : 등록센터
- SIDi : 서버의 식별자
- Bi : 사용자의 Biometric template
- Rc, Rs : 사용자 및 서버의 임의 난수

1. Li & Hwang's 인증스킴 절차

1.1 등록단계

step 1 : U는 패스워드 pwi, 식별자 IDi, 개인 생체정보 Bi를 안전한 채널을 통해 신뢰하는 등록센터 R에 등록한다.

step 2 : 등록센터 R은 다음을 연산한다.

- fi = h(Bi)
- ei = h(IDi ‖ xs)⊕h(pwi ‖ fi)

step 3 : 등록센터 R은 스마트카드에 (IDi, h(), fi, ei)를 저장하고 스마트카드를 안전한 채널로 U에게 전송한다.

1.2 로그인단계

U가 원격 S에 로그인 과정은 다음과 같다.

step 1 : U는 스마트카드 삽입 후 개인 검증을 해야 한다. 생체 검증 장치를 통해 생체정보 Bi를 입력한다.

step 2 : 스마트카드의 fi정보와 비교(h(Bi)=? fi)하여 일치하면 pwi의 입력을 허용하고 그렇지 않으면 생체정보 재입력을 요구한다.

step 3 : pwi를 입력하면 ri′, M1, M2가 연산된다.

- ri′ = h(pwi ‖ fi)
- M1=ei⊕ri′
- M2=M1⊕Rc

step 4 : IDi, M2를 S로 전송한다.

1.3 인증단계

S는 IDi, M2를 수신하여 step1-step7과정을 수행한다.

step 1 : IDi를 체크하여 정당성 여부를 판단한다.

step 2 : 정당한 IDi 소유자라면 서버는 다음을 연산한다.

- M3=h(IDi ‖ xs)
- M4=M2⊕M3=Rc
- M5=M3⊕Rs
- M6=h(M2 ‖ M4)

step 3 : 연산결과 중 M5, M6을 U에게 전송한다.

step 4 : U는 자신이 생성한 M2와 Rc를 연접한 후 해시 값을 만들어 수신된 M6과 비교하여 동일하면 S를 인증하고 그렇지 않으면 종료된다.

- M6=? h(M2 ‖ Rc)

step 5 : S가 인증되면 U는 다음을 연산한다.

- M7=M5⊕M1
- M8=h(M5 ‖ M7)

step 6 : M8을 S에게 전송한다.

step 7 : 서버는 자신이 생성한 M52와 Rs를 연접한 후 해시 값을 만들어 수신된 M8과 비교하여 동일하면 U를 인증하고 그렇지 않으면 종료된다.

- M8=?h(M5 ‖ Rs)

1.4 패스워드 변경단계

step 1 : U는 단말기의 리더기를 통해 스마트카드 입력 후 pwi와 새로운 패스워드 pwnew를 입력한다.

step 2 : 스마트카드는 다음을 연산하여 패스워드를 변경시킨다.

- ri′ = h(pwi ‖ fi)
- ei′ = ei⊕ri′ = h(IDi ‖ xs)
- ei′′ = ei′ ⊕ h(pwnew ‖ fi)

2. Li and Hwang's 인증 스킴 분석

로그인단계와 인증단계에서 메시지는 비보호채널을 통해 전송되는 과정에서 공격자 A는 채널을 완전히 장악하여 메시지를 가로채 변조할 수 있다. 그때 S는 요청메시지 자체를 유효한가 아닌가에 대해 검증할 장치가 없다. 또한 U는 S의 인증정보에 대해 위장 메시지 여부를 검증할 수 있는 기능이 없다. 이것이 Li and Hwang's 스킴에 대한 중대한 결점으로 이러한 가정 하에 이 스킴은 중간자 공격에 의한 불확실한 인증 스킴이라는 것을 보여주고자 한다.

그림 1에서 공격자가 메시지 M2를 가로채서 M2′로 대치하면 위조된 메시지는 S의 인증을 통과할 수 있다. 그러나 U는 S에 의해서 인증될 수 없어 세션이 종료된다.

그림 2에서 공격자가 메시지 M5를 가로채서 M5′로 대치하면 위조된 메시지는 U의 인증을 통과할 수 있다. S 또한

U에 의해서 인증될 수 없음에 이른다.

중간자공격에서 공격자는 서버로 위장하기 위해 사용자로 위장한다. 그리고 비밀정보를 모르고서도 사용자로 속이기 위해 서버로 위장할 수 있다.

2.1 인증과 위장공격의 문제

가. 공격자 A에 의한 U의 정보 위장사례

로그인단계에서 U는 S에게로 로그인메시지 IDi, M2를 전송할 때 공격자 A는 이를 가로챈다. 공격자는 임의의 수 Ra를 선택하여 M2′=M2 ⊕ Ra를 계산한다. 그리고 공격자는 위조된 메시지 IDi. M2′를 S로 전송한다. 이 경우 S는 다음과 같은 일이 발생한다.

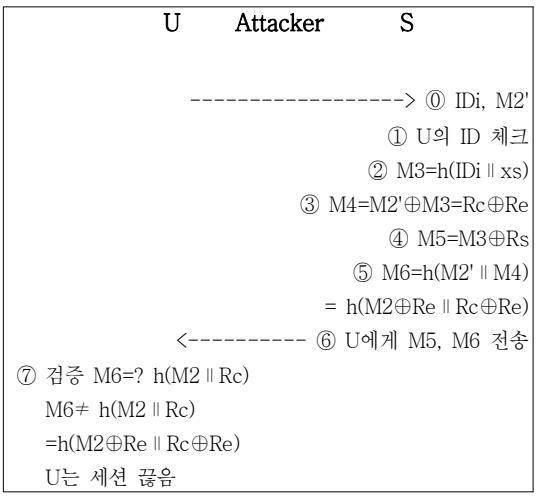


그림 1. 중간자 공격 사례-1
Fig. 1 Man in the middle attack-1

로그인메시지(IDi, M2)의 유효성은 사용자 IDi에 의존한다. 즉, 로그인메시지(IDi, M2)의 유효성을 검증할 수 없다는 것이다. 그러므로 공격자는 메시지를 위조하기가 아주 쉽다. S는 위조된 메시지를 유효한지 검증할 수 있는 방법이 없다. 그림 1에서 S는 IDi만으로 U를 인증하고 M6을 사용자에게 전송함으로써 U로부터 S는 인증을 받지 못한다.

나. 공격자 A에 의한 S의 정보 위장사례

공격자 A는 인증단계 1.3의 step 3에서 U로 전송되는 M5를 해킹(가로채)하여 메시지를 수정(M5′= M5 ⊕ Rs′, 공격자 A는 Rs′를 선택, 메시지 위조(M5′= M5 ⊕ Rs′)하여 M5′를 S에게 전송할 경우이다.

이 경우 S에 대한 인증은 U의 정보만이 관련된 M6=h(M2 ‖ Rc)에 달려 있다. 공격자는 쉽게 U의 인증정보를 위조하여 전송한다. U는 정당한 사용자인데 S는 U를 제3자라고 생각한다. 더구나 S의 인증 메시지는 S의 정보를 갖고 있지 않다는 불합리성이다.

위에서 Li & Hwang′s 스킴은 본질적으로 확실한 인증을 제공하는데 있어서 로그인 메시지와 인증 메시지의 설계에 본질적인 결함이 있음을 알 수 있다.

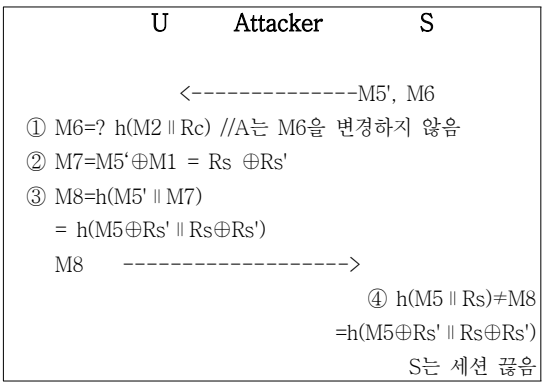


그림 2. 중간자 공격 사례-2
Fig. 2 Man in the middle attack-2

III. 제안스킴

본 논문에서는 2장 Li & Hwang′s 스킴의 결점을 보완한 새로운 개선된 생체기반의 원격 사용자인증 스킴을 제안한다. 2.1의 가, 나에서 보면 정당한 사용자와 서버간의 인증에서 제3자의 위장된 메시지에 의해 상호인증 결여와 일방적으로 중간자 공격에 의한 세션이 종료되는 서비스거부공격이 발생한다.

제3자의 중간자공격을 알아 낼 수 있는 사용자와 서버간의 강력한 상호인증 프로토콜을 제안한다. 제3자에 의한 익명성 및 무결성 보장과 재 전송공격 방지, 서비스거부공격, 가장공격을 효율적으로 차단할 수 있는 프로토콜이다.

프로토콜에서 사용한 기법으로 OSPA(Optimal Strong-Password Authentication)를 이용한 5단계 검증으로 제 3자의 위조여부를 판별할 수 있다.

본 프로토콜은 등록단계, 로그인단계, 인증 및 확인자 변경의 4단계로 구성되어 있다. 본 논문에서 프로토콜에 사용될 수정 용어에 대한 정의이다.

- pwi : password(64bit)
- ri : random number of client(64bit)

1. 등록단계

U가 원격시스템에 등록을 할 때 그림 3의 절차를 갖는다.

step1. U는 임의의 패스워드 pwi와 생체정보 Bi를 연산(h(pwi⊕Bi))하여 안전한 채널로 IDi, Bi, h(pwi⊕Bi)를 서버(S)에 전송한다. 사용자의 패스워드 정보는 자신만이 아는 비밀정보로 S에게 노출되지 않는다.

setp2. S는 fi(식1)를 연산하고 자신의 비밀키 xs를 이용하여 (식2)를 연산한다.

- fi=h(Bi) ----------(식1)
- K=h(pwi⊕Bi)⊕h(x⊕IDi) ----------(식2)

S는 스마트카드에 K, fi, h(), IDi를 저장하여 안전한 채널을 이용, U에게 전송한다.

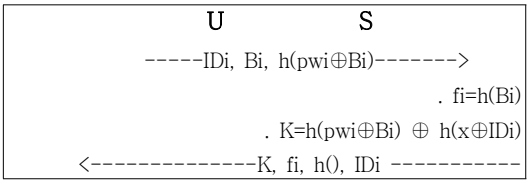


그림 3. 등록 과정
Fig. 3. Registration Phase

2. 로그인 단계

U는 그림 4와 같은 단계를 통해 로그인 과정을 갖는다.

step1. U는 스마트카드를 삽입하고 생체정보 입력 장치를 통해 Bi를 입력한다.

스마트카드는 (식3)을 연산하여 스마트카드에 내장된 fi 정보와 비교하여 일치되면 패스워드 입력을 요구한다.

- fi′=h(Bi) ----------(식3)
- check h(Bi)=?fi′ ----------(식4)

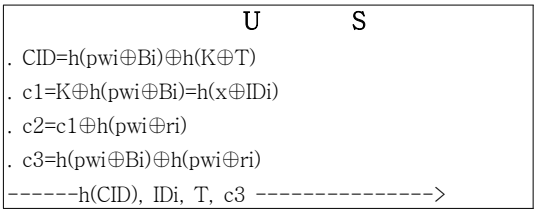
step2. 검증 후 패스워드를 입력(3회 입력 제한)하면 다음 (식5-6)을 연산한다.

- CID=h(pwi⊕Bi)⊕h(K⊕T) ----------(식5)
- c1=K⊕h(pwi⊕Bi)=h(x⊕IDi) ----------(식6)

step3. 임의 난수 ri을 선택, 입력하여 다음 (식7-8)을 연산한다.

- c2=c1⊕h(pwi⊕ri) ----------(식7)
- c3=h(pwi⊕Bi)⊕h(pwi⊕ri) ----------(식8)

S에게 h(CID), IDi, T, c3를 전송한다.



서버의 비밀키 xs는 모든 스마트카드 발급자에게 공통으로 사용되며 각 사용자에 대한 비밀정보 테이블을 보유하지 않는다. h(CID)는 정노노출 방지를 위한 해시 값이다.

3. 인증단계

S는 h(CID), IDi, T, c3를 수신하여 그림 5와 같은 인증과정을 갖는다.

step1. IDi를 체크하여 유효성을 검사하고 (T′-T) ≤ △T를 검증하여 U의 로그인 요청을 승인 또는 거절한다.

step2. S는 CID의 유효성 판단을 위해 (식9)에서 h(pwi⊕Bi)를 도출하고 (식10-11)을 통해서 유효성을 인증한다.

- D0 = K⊕h(x⊕IDi) = h(pwi⊕Bi) -------(식9)
- CID = h(pwi⊕Bi)⊕h(K⊕T) ----------(식10)
- h(CID)′=?h(CID) ----------(식11)

step3. c3 정보의 무결성 검사를 위해 (식12-15)를 연산하여 위조여부를 판단한다.

- D1 = h(x⊕IDi) ----------(식12)
- D2 = c3 ⊕ h(pwi⊕Bi) =h(pwi⊕ri) ----(식13)
- D3 = D1 ⊕ h(pwi⊕ri)
  = h(x⊕IDi)⊕h(pwi⊕ri) ----------(식14)
- D3′ = D3 ⊕ h(x⊕IDi) = h(pwi⊕ri) ----(식15)
- D3′ =? D2
- c3 ⊕ D2=?D0

U에 대한 인증이 이루어지면 인증결과를 U에게 보내 S의 적법성 인증을 요구한다. S가 검증을 위해 생성한 CID, h(pwi⊕ri)를 사용하여 (식16)을 생성한 후 T′, D3, D4를 U로 전송한다.

- D4=h(T*⊕T⊕CID⊕h(pwi⊕ri)) -------(식16)

step4. U는 T′, D3, D4를 수신하여 정당한 S임을 확인한다. 먼저 (T′-T) ≤ △T를 검증하여 S의 타임스탬프를 확인하고 승인 또는 거절한다.

step5. U는 자신이 생성하여 보관하고 있는 c2와 S로부터 전송된 D3를 비교한 후 일치하면 (식17)을 통해 D4′를

생성한 후 수신된 D4와 비교하여 일치하면 합법적인 S로 인증된다.

- c2=? D3
- D4'=h(T'*⊕T⊕CID⊕h(pwi⊕ri)) --------(식17)
- D4'=?D4

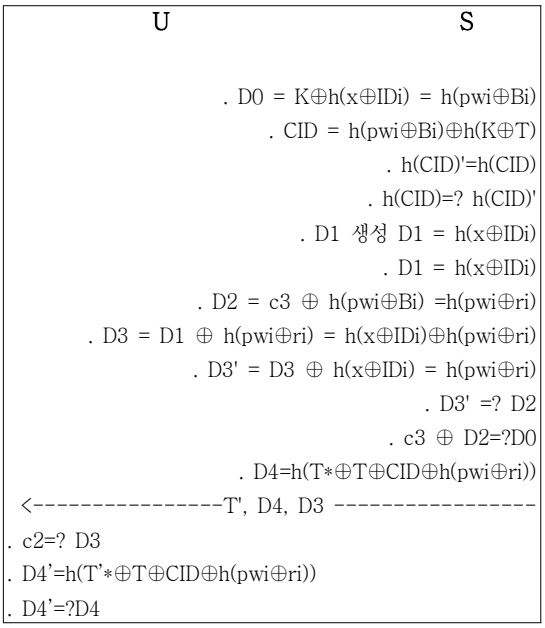


그림 5. 인증 과정
Fig. 5. Authentication Phase

4. 패스워드 변경

U는 임의 새로운 패스워드를 선택하여 S와는 독립적으로 스마트카드에 내장된 K의 값을 변경할 수 있다.

step1. Bi 입력을 통해 로그인 인증프로세스가 정상적으로 수행된다.

step2. 현재의 pwi와 임의 새로운 pwi′ 입력하면 (식18)이 연산되어 스마트카드는 현재의 K값 대신에 Knew 값으로 변경 저장된다.

- Knew=K⊕h(pwi′⊕Bi) ⊕ h(pwi⊕Bi)=h(pwi′⊕Bi)⊕h(x⊕IDi) ----------(식18)

Ⅳ. 안전성 분석

1. 보안분석

제안한 인증스킴의 보안성과 경제성에 대해 평가한다.

1.1 익명성(내·외부자 공격 대응)

로그인과정에서 동적으로 생성 및 변경되는 CID와 c3 정보를 활용하므로 동적 ID의 개념을 계승하고 있으며 익명성을 제공한다. 안전한 채널을 통해 등록할 때 사용자의 패스워드를 노출시키지 않고 h(pwi⊕Bi) 정보를 제공함으로 사용자의 패스워드를 확인할 수 없으며 내부적으로 보관하지 않으므로 내·외부자 공격에 안전하다. Li and Hwang′s 스킴에서는 등록정보(pwi)를 믿을 수 있는 내부자들이 ID와 함께 쉽게 알 수 있고 등록기관의 R의 의지에 달려있다. 즉 Bi와 pwi를 그대로 서버에게 노출시키고 있다. 그러나 본 스킴에서는 U가 pwi 대신에 h(pwi⊕Bi)를 S에 등록한다. 이것을 유추하기 위해서는 pwi와 Bi의 XOR연산에서 128비트를 사용하므로 연산에 2^{128}이 소요되고 또한 필요시 세션마다 pwi의 값이 변경되며 Bi 정보는 노출되더라도 소유자에 의해 생체정보 인증장치를 통해 인증을 수행하기 때문에 안전에 무관하다.

1.2 무결성(가장 공격방어)

가장 공격은 공격자가 프로토콜에 참여하여 자신을 임의의 합법적인 사용자로 가장하여 정당한 사용자로 행동하는 것으로 사용자의 식별자와 패스워드를 알아야 한다. Li and Hwang′s 스킴에서는 U에 대한 ID만으로 인증되고 있으며 S의 인증정보 생성에서 M2 메시지에 대한 검증단계가 없으므로 가장공격에 취약하다. 본 스킴에서는 메시지 검증과정을 3.3 인증단계의 step3에서 검증과정을 5단계(T체크, ID체크, h(CID)체크, D3′와 D2체크, c3⊕D2체크)로 두어 메시지의 무결성 체크와 더불어 제3자의 위조여부를 쉽게 알 수 있다. 로그인 전송정보를 가로채어 동적 CID를 도출해 낼 수 있는 어떤 관련정보도 노출되지 않고 있으며 이로 인하여 서버인증정보인 D1-D3을 생성할 수 없다.

1.3 재전송공격

공격자는 재전송공격이 불가능하다. 하나의 세션에서 로그인 정보 h(CID), IDi, T, c3를 가로채어 보관하다가 인증단계에서 전에 사용했던 로그인 메시지를 재생한다 해도 (T′-T) ≤ △T에 의해 실패한다. 또한 매 세션마다 임의 난수 r을 선택하여 c2=c1⊕h(pwi⊕ri), c3=h(pwi⊕Bi)⊕h(pwi⊕ri)를 생성하여 pwi와 XOR되어 해시됨으로 재전송공격에 안전하다. 공격자가 재전송공격을 하기 위해서는 이전 세션에서 획득한 CID의 타임스탬프 T가 (T′-T) ≤ △T을 만족하는 새로운 T′로 변경할 수 있어야 하는데 CID는 해시되어 안전하다.

1.4 추측 공격

온라인 추측 공격은 패스워드 인증실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있으므로 본 논문에서는 오프라인 패스워드추측 공격에 대해서 고려한다. 공격자가 U의 로그인 메시지 h(CID), IDi, T, c3를 가로채고 스마트카드의 h()를 사용한다고 하더라도 h(CID), c3의 인증데이터 생성이 추측하기 어려운 긴 길이의 비밀정보를 포함하고 있다. 공격자가 패스워드를 획득하기 위해서는 c3=h(pwi⊕Bi)⊕h(pwi⊕ri)를 통해서만 pwi를 추측할 수 있다. 이러한 공격은 K가 안전한 스마트카드에 저장되어 있어서 사용자의 인증과정이 없이 직접 S에 접근할 수 없으며 K를 알고 있다고 하더라도 pwi는 안전하게 유지된다. pwi 또는 ri를 추측하기 위해서는 c3=h(pwi⊕Bi)⊕h(pwi⊕ri)에 의해 2^{128} *2^{128}의 연산을 필요로 하며 추측되었다 하더라도 다음세션에서는 새로운 난수 사용으로 공격할 수 없다. 또한 오프라인 추측 공격에 취약한 pwi의 경우에도 직접 사용되지 않고 모든 연산에서 h()로 연산되므로 추측 공격에 대응할 수 있다.

1.5 상호인증

Li and Hwang's 스킴에서는 중간자공격에 의해 U와 S의 상호인증과정이 수행되지 않은채 정당한 사용자나 서버가 인증정보를 제공했음에도 불구하고 접속이 차단되었다.본 논문은 원격접속을 위한 사용자의 인증과 사용자가 원격시스템을 인증할 수 있는 상호인증을 구조를 제공한다. 정당한 서버만이 사용자의 비밀정보 h(pwi⊕Bi)와 h(pwi⊕ri)를 생성유도할 수 있는 구조를 갖는다. D2의 정보 h(pwi⊕Bi)를 생성할 수 있어야 매 세션마다 변경되는 비밀정보 h(pwi⊕ri)를 만들 수 있다.

이는 정당한 서버만이 비밀키 xs를 이용하여 h(pwi⊕Bi), D1, D2, D3를 생성할 수 있다. S가 생성한 D3정보는 U에서 중요한 인증요소가 된다. D3, D4의 생성은 합법적인 S가 아니면 생성할 수 없음을 보여준다. U가 로그인단계에서 생성하여 비밀리에 보관하고 있는 c2정보와 D3를 비교함으로써 정당한 S를 1차 검증할 수 있으며 D4를 사용자가 생성할 수 있다는 의미는 정당한 U를 의미한다. 본 논문에서의 상호인증은 Li and Hwang's 스킴과 비교해 볼 때 인증메시지의 유효성을 확인하는데 있어서 메시지의 설계에 본질적 결함(확실한 인증요소제공의 미흡)을 검증 5단계로 설계함에 중점을 두고 있다.

1.6 Stolen 공격

사용자의 패스워드를 내부적으로 보관하지 않으므로 내부자 공격에 대응한다. 일반적인 패스워드 기반의 스킴들은 임시 검색테이블 또는 ID에 해당하는 h(pwi‖ri)을 찾아 불루투스 공격을 통해 시도하여 많은 시간을 소요하더라도 성공할 확률을 배제하지 못하지만 본 스킴에서는 생체검증장치를 통해 본인인증이 이루어지므로 스마트카드가 분실되어도 등록단계의 (식1) fi=h(Bi)를 통과할 수 없다. 또한 스마트카드 도난공격에 패스워드 3회입력의 제한도 대응될 수 있다.

1.7 DoS 공격

DoS 공격은 서비스정지, 시스템다운, 네트워크 기능마비 등 여러 가지 형태로 이 중에서 서비스정지 기능에 한정하여 다룬다.

Li and Hwang's 스킴에서는 제3자로부터 가로챈 메시지의 위장공격에 의한 서비스거부공격의 원인이 제공되고 있으나 스킴자체의 연산에서 어떤 공격에 의한 서비스기능 정지인지에 대한 판별능력이 없다.

본 스킴에서는 S의 인증단계에서 D3′ =? D2와 c3 ⊕ D2=?D0를 연산함으로써 수신된 메시지의 무결성 검사과정을 거치게 되며 메시지의 위조여부를 알 수 있다.

2. 기존 인증스킴과의 비교

제안된 인증스킴과 Li and Hwang's 스킴에 대한 보안성 분석을 표 1과 같이 비교하였다.

표 1. 기능 분석
Table 1. Function analysis

기능	Li & Hwang's	제안스킴
익명성	미제공	CID,C3정보(제공)
무결성	미제공	검증과정5단계(제공)
재전송 공격방어	미제공	h(CID),C3생성불가(제공)
추측공격 방어	미제공	ri추측연산2^{128}*2^{128}, ri′(제공)
상호인증	부적절	D3,D4정보생성자(제공)
stolen 공격방어	제공	h(Bi),(제공)
생체인증	제공	h(Bi),K(제공)
DoS공격 확인	확인할 수 없음	D3′=?D2,C3⊕D2=?D0(확인)

보안성 분석은 Li and Hwang's 스킴의 취약성을 중심으로 내·외부자 공격대응(익명성) 기능, 가장 공격대응(무결성) 기능, 재전송공격방지 기능, 추측 공격방지 기능, 상호인증기

능, 도난공격방지 기능, 생체 인증기능, DoS공격 확인기능에 대한 분석결과의 비교이다. 이와 같이 제안된 인증스킴은 가변인증자(CID)와 OSPA를 적용한 무결성 검사를 통하여 가장 공격과 상호인증의 근본적인 취약성을 제거함으로써 재전송공격, 추측 공격 등으로부터의 안전이라는 부수적인 효과를 가진다.

Li and Hwang's 스킴, Li et al 스킴들과 비교하여 제안된 스킴의 해시연산 비용을 표 2에서 보여주고 있다. 제안된 스킴의 연산 복잡도 분석을 위해 단방향함수 연산시간을 Th로 표기한다.

표 2. 계산량, 통신량 비교
Table 2. Comparison of Computation, Communication

단계	Li & Hwang's	제안스킴
등록	3Th	3Th
로그인	2Th	7Th
인증	5Th	10Th
계	10Th	20Th
불안전 통신량	3회	2회

제안한 스킴에서 XOR는 단순연산으로 성능에 영향을 주지 않으므로 해시연산만을 고려하였다. 인증단계의 무결성 검사과정에서 다소 많은 연산 량이 도출되었지만 해시함수 성격상 시스템 전체에 주는 영향은 크지 않다. Li and Hwang's 스킴을 개선시키기 위한 무결성과 익명성보장을 확보하였고 불안전 채널을 통해 전송되는 정보는 2회로 단순화 시켰다.

V. 결 론

원격사용자 인증은 프라이버시 보호를 위한 익명성과 무결성 보장이며 이들을 보장받기 위해서는 추측에 의한 가장 공격, 내부자 공격, 재전송 공격, stolen 공격 등에 대한 대책이 필요하다.

Li and Hwang's 스킴은 스마트카드를 사용한 생체기반 원격사용자 인증스킴으로 인증과정에서 제3자의 메시지 변조에 대해 적절하게 대응하는 메커니즘을 제공하지 못하여 도청, 위장공격을 감지하지 못하고 세션이 종료되는 현상이 발생하였다.

본 논문에서는 Li and Hwang's 스킴에 대한 취약점인 가장 공격 및 상호인증의 문제에 대한 대안으로 익명성과 무결성을 검사하는 기능을 추가하여 개선하였고 보안의 안전성과 계산 및 통신비용 측면을 Li and Hwang's 스킴과 비교하여 평가하였다.

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

참 고 문 헌

[1] Lamport L. password authentication with insecure communication. communications of the ACM 1981. 24(11). p. 770-772

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

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

[4] S. K. Kim and M. G. Chung, "More secure remote user authentication scheme." Computer Communications, Vol. 32, No. 6, pp.1018-1021. 2009.

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

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

[7] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart card." Journal of Network

and Computer Applications, Vol. 33, No. 1, pp. 1-5, 2010.

[8] X. Li, J. W. Niu, J. Ma, W. D. Wang, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart card." Journal of Network and Computer Applications, 2011.

저 자 소 개

신 광 철

2003년 8월 : 성균관대학교 정보공학과 공학박사

2004년 ~ 현재 : 성결대학교 산업경영공학부 교수

관심분야 : 전자지불시스템, 스마트카드 인증 및 보안기술, 라우터보안, RFID 보안응용

Email: skcskc12@sungkyul.edu