Journal of The Korea Society of Computer and Information
Vol. 17, No. 11, November 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.11.083

추적 가능성을 위한 스마트카드 기반의 개선된 사용자 익명성 인증기법

박미옥

Improved User Anonymity Authentication Scheme using Smart Card for Traceability

Mi-Og Park

요 약

사용자 익명성 제공 인증기법은 Das 등에 의해 처음으로 제안되었으며, 대부분의 사용자 익명성 기법들은 통신 채널상의 외부공격에 대한 사용자 익명성을 제공한다. 본 논문에서는 서버 공격에 의한 개인정보 노출 사고가 증가함에 따라, 외부공격에 대한 사용자 익명성뿐만 아니라 서버에 대한 사용자 익명성을 제공하는 새로운 인증기법을 제안한다. 더욱이 제안 인증기법은 원격 서버가 악의적인 사용자를 추적할 수 있는 기능을 제공하며, 패스워드 오입력시의 취약점을 개선하여 원격 서버의 계산로드가 증가하는 문제도 함께 해결한다.

▸ Keywords : 사용자 익명성, 추적가능성, 내부자 공격, 물리적으로 강인한 스마트카드

Abstract

Authentication schemes preserving user anonymity have first been proposed by Das et al, and most of user anonymity schemes provide user anonymity against outside attacks in the communication channel. In this paper, according to the increasing of personal information exposure incidents by server attack, we propose a new authentication scheme that provides user anonymity against server as well as one against outside attacks in the communication channel. Furthermore, the proposed authentication scheme provides traceability that remote server should be able to trace the malicious user and it also solves the problem of increasing computational load of remote server by solving weakness of wrong password input by mistake.

▸ Keywords : User Anonymity, Traceability, Insider Attack, Tamper-resistant Smart Card

•제1저자 : 박미옥
•투 고 일 : 2012. 11. 06, 심사일 : 2012. 11. 12, 게재확정일 : 2012. 11. 15.
* 성결대학교 컴퓨터공학부(Division. of Computer Science Engineering, Sungkyul University)

I. 서 론

사용자 인증 서비스는 원격 로그인 시스템을 위한 기본적인 보안 메커니즘으로서, 일반적으로 3가지 형태의 기본 정보 즉, 사용자의 식별자인 ID와 개인의 비밀 정보인 패스워드 PW, 그리고 사용자가 소유하고 있는 스마트카드(smart card)를 사용한다. 원격 사용자 인증기법은 크게 등록 단계, 로그인 단계, 인증 단계로 구성되며, Lamport에 의해 처음으로 제안되었다. Lamport의 기법은 원격 서버가 안전하지 않은 네트워크를 통해 사용자의 식별자와 패스워드를 기반으로 하여 사용자를 인증하는 기법이다[1]. 그러나 이 인증기법은 원격 서버에서 사용자의 패스워드에 대한 검증 테이블을 저장해야한다. Jon과 Chen 등은 원격 서버에 패스워드 검증 테이블을 저장하지 않아도 되는 패스워드 기반의 인증기법을 제안하였고, 이 외에도 패스워드 검증 테이블이 필요 없는 다양한 인증기법들이 제안되었다[2-6]. Hwang과 Li[2]는 ElGamal 공개키 암호시스템을 사용하는 스마트카드 기반의 인증기법을 제안하였으며, 이들의 인증기법은 원격 서버에서 서버 자신의 비밀키만 유지할 뿐 사용자의 패스워드 테이블을 유지하지 않아도 되는 장점이 있다. 이 후 사용자의 정보보호와 프라이버시에 대한 중요성이 날로 증대되면서, 2004년 Das 등이 동적 아이디(dynamic-ID)를 이용하여 사용자 익명성을 제공하는 최초의 인증기법을 제안하였다[7]. Das 등이 제안한 사용자 익명성은 정당한 사용자와 원격서버를 제외한 제3자에 대한 사용자 익명성 제공을 의미한다. 그러나 Chien 등은 2005년에 Das 등의 인증기법이 서버로 전송되는 로그인 요청 메시지를 통해 사용자를 구분할 수 있게 됨으로써, 안전한 사용자 익명성을 제공하지 못함을 지적하면서, 그들의 취약점을 해결한 인증기법을 제안하였다[8]. Chien 등의 인증기법은 대칭키 암호방식을 이용하여 사용자의 식별자와 비밀 정보를 암호화하여 전송함으로써 사용자의 익명성을 보장하는 기법이다. 2007년에 Hu[9] 등은 물리적으로 강인한(tamper-resistant) 스마트카드를 사용하지 않을 경우, 강력한 가장 공격(strong masquerading attack)에 취약하여, 결국 Chien 등의 기법이 상호인증을 제공하지 못함을 지적하였다. 또한, Horng[10] 등은 Hu[9] 등의 인증기법이 강력한 서버/사용자 가장 공격에 취약하고, 스마트카드 분실시 패스워드 추측 공격에 취약하여 사용자 익명성을 안전하게 제공하지 못한다고 지적하였다.

스마트카드 기반의 인증기법들이 사용하는 카드는 물리적으로 강한 스마트카드와 일반적인 스마트카드(non tamper-resistant)로 분류할 수 있다. 물리적으로 강한 스마트카드는 이 카드에 저장된 정보나 중간 계산결과를 얻을 수 없다는 특성이 있다. 그러나 최근 연구들은 물리적으로 강한 스마트카드의 소비전력(power consumption)을 모니터링하거나 노출된 정보를 분석함으로써, 카드에 저장된 비밀정보를 획득 가능함을 보였다[10-13]. 그러므로 물리적으로 강한 스마트카드를 사용한다는 가정 하에 제안된 논문들은 제안 인증기법에 따라 사용자의 식별자나 패스워드를 평문형태 그대로 저장함으로써, 사용자의 비밀 정보가 그대로 노출되는 취약점이 존재하여, 사용자/서버 가장 공격, 스마트카드 분실시의 패스워드 추측 공격 등의 공격에 매우 취약할 수 있다.

본 논문에서는 날로 증가하는 개인정보 침해사고를 방지하고, 사용자 프라이버시를 보다 안전하게 제공할 수 있도록 서버에 대한 사용자 익명성을 제공하는 개선된 인증기법을 제안한다. 또한, 제안 인증기법은 원격 서버가 사용자의 악의적인 행동을 감지하거나 다른 문제가 발생할 경우를 대비해 사용자를 추적할 수 있는 기능도 제공한다. 그리고 서버내의 내부자 공격과 패스워드 오입력시의 취약점 등도 함께 개선하여, 패스워드 오입력으로 인해 원격서버로까지 전이되는 계산로드 문제를 해결한다. 제안 인증기법은 물리적으로 강인한 스마트카드를 사용한다고 가정하지만, 이러한 카드도 소비전력 모니터링 등을 통해 제3자에 의한 정보획득이 가능하므로, 카드 분실시에도 사용자의 비밀 정보가 곧바로 노출되는 기존의 인증기법들의 취약점을 개선한다.

본 논문의 구성은 2장에서는 기존의 사용자 익명성을 제공하는 인증기법을 간단히 살펴보고, 3장에서는 이들의 취약점을 분석한다. 4장에서는 기존의 취약점을 개선한 추적 가능한 사용자 익명성을 제공하는 개선된 인증기법을 제안한다. 5장에서는 제안한 인증기법을 안전성과 효율성 측면에서 비교·분석하고, 6장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 물리적 공격에 강인한 스마트카드를 사용한다는 가정 하에 사용자 익명성을 제공하는 인증기법 중 백이루 등[14]의 인증기법에 대해 살펴본다. 이들의 인증기법과 Chien[8], Hu[9], Horng[10], Bindu[15] 등의 비교 인증기법도 모두 대칭키 암호방식을 사용한다. 먼저 본 논문에서 사용하는 기호와 그에 대한 의미는 다음과 같다.

표 1. 표기법
Table 1. Notation

기 호	의 미
IDi	Identity of user
PWi	Password of user
INFi	Personal information
h(·)	Secure one-way hash function
ER{X}	Symmetric Encryption using secret key R
x	Secret key of server
y	Secret value of server
⊕	XOR operation
N, r	Random number
T	Time Stamp

2.1 백이루 등의 인증기법

이 기법의 등록 단계, 로그인 단계, 인증 단계는 다음과 같이 수행한다.

등록 단계

〔단계1〕 사용자는 IDi와 PWi를 선택하고 난수 N을 생성하여 h(PWi⊕N)을 계산한 후, 서버에 전송한다.

〔단계2〕 서버는 비밀키 x를 이용해, 다음을 계산한 후, {IDi,m,M,h()}를 스마트카드에 저장하여 사용자에게 발급한다.

m=h(IDi)⊕h(x)⊕h(PWi⊕N), M=h(IDi)⊕h(x)

〔단계3〕 사용자는 스마트카드에 난수 N을 저장한다.

로그인 단계

사용자는 스마트카드를 카드 리더기에 삽입하고, 자신의 IDi와 PWi를 입력한다.

〔단계1〕 카드는 M⊕h(PWi⊕N)를 계산하여 올바른 패스워드가 입력되었는지 m과 비교하여 체크한다. 두 값이 동일할 경우, 난수 ru를 생성해 C=M⊕ru, R=h(IDi)⊕ru를 계산한 후 R을 이용하여, {ru, IDi}를 암호화한다.

〔단계2〕 카드는 {C, ER{ru, IDi}}를 서버에게 전송한다.

인증 단계

〔단계1〕 메시지를 수신한 서버는 자신의 비밀키 x를 이용해, R=C⊕h(x)를 계산한 후 암호화된 메시지 ER{ru, IDi}를 복호화한다. 복호화로 얻어낸 사용자의 IDi와 난수ru를 이용해, h(IDi)⊕ru를 계산하여 R과 같은지 검증한 다. 만약 값이 다르면 로그인 요청 서비스를 거부한다.

〔단계2〕 서버는 난수 rs를 생성한 후, R을 이용하여 rs, ru+1을 암호화한 후, ER{rs,ru+1}을 사용자에게 전송한다.

〔단계3〕 사용자는 메시지 복호화 후 ru+1을 확인해, 서버를 인증하고 세션키 SK=ru⊕rs를 계산한다. 그런 다음 사용자는 rs+1을 암호화하여 ER{rs+1}을 서버에 보낸다.

〔단계4〕 서버는 복호화 후, rs+1의 타당성을 체크하여, 사용자를 인증하고 세션키 SK=ru⊕rs를 계산한다.

패스워드 변경 단계

사용자는 자신의 패스워드 PW_i를 입력한다.

〔단계1〕 카드는 M⊕h(PW_i⊕N)를 계산한 후 올바른 패스워드가 입력되었는지 m과 비교하여 타당성 여부를 체크한다. 올바른 패스워드이면 사용자는 새로운 패스워드 PW_i' 를 입력한다.

〔단계2〕 카드는 다음을 계산하여 기존의 m을 m^*로 교체한다.

m^*=m⊕h(PWi⊕N)⊕h(PW_i' ⊕N)

III. 취약점 분석

본 절에서는 백이루〔14〕 등의 인증기법에 대한 취약점을 분석한다. 이 기법은 물리적 공격에 강인한 스마트카드를 사용한다는 가정 하에 제안된 사용자 익명성 제공 인증기법이나, 여러 논문들에서 소비전력의 모니터링 등을 통해 카드에 저장한 데이터를 얻어낼 수 있음을 증명하였다〔11-13〕. 본 절에서는 소비전력 모니터링 등에 의해 카드에 저장된 정보노출이 가능하다는 점에 근거하여 백이루〔14〕 기법의 취약점을 분석한다.

3.1 카드 분실시의 취약점

이 인증기법의 등록 단계는 {IDi,m,M,h()}와 같이 카드에 사용자의 IDi를 평문형태로 저장한다. 그러므로 카드를 습득한 공격자는 평문형태의 IDi를 획득 가능하며, 다음에 제시되는 시나리오에 의해 정당한 사용자를 가장할 수 있다.

1. m과 M을 XOR 연산하여, h(PWi⊕N) 값을 얻는다.
2. 패스워드 값 h(PWi⊕N)를 이용해 로그인 단계에 맞게 새로운 난수 ru′을 생성하여 C′=M⊕ru′을 계산한다.
3. 평문형태의 IDi 값을 이용해, R′=h(IDi)⊕ru′을 계산한 후, {C′, ER{ru′,IDi}}를 서버에 전송한다.
4. 서버는 R′=C′⊕h(x)를 계산하여 h(IDi)를 얻어내고, h(IDi)값을 다시 C′⊕h(IDi)⊕h(x) 계산하여 난수 ru′을 얻어낸다. 공격자가 생성한 난수와 h(IDi)는 올바른 값이기 때문에, 서버가 계산한 비밀키 R은 공격자가 계산한 R′과 동일하다. 그러므로 사용자 인증은 성공하고, 서버는 난수 rs′을 생성한다.

5. 서버는 ER{rs′, ru+1}을 계산하여 사용자에게 전송한다.
6. 정당한 사용자로 가장한 공격자는 암호화키 R을 알기 때문에, 메시지를 복호화하여 rs′를 알아낸 후ER{rs′+1}을 암호화한 후 서버에 전송한다. 그런 다음 세션키로 사용할 SK=rs⊕ru를 계산한다.
7. 서버는 $E_R\{r_s'+1\}$을 복호화하여, r_s+1의 타당성을 체크한 후 올바른 값이기 때문에 세션키로 사용한 $SK=r_s\oplus r_u$를 계산한다.

결국 이 기법은 물리적으로 강인한 스마트카드를 사용한다고 할지라도 카드 분실시 사용자 익명성을 제공하지 못한다.

3.2 다른 취약점들에 대한 분석

이 기법은 재전송 공격에 취약하며 패스워드 변경단계를 제시하였지만, 여전히 패스워드 오입력시의 취약점 등이 존재한다. 또한, 사용자의 식별자가 서버에 노출됨으로써 서버내의 악의적 내부 공격에도 취약함을 살펴본다.

1. 재전송 공격

공격자가 로그인 요청 메시지 {C, ER{ru, IDi}}를 가로채어 서버에 재전송할 경우, C는 h(IDi)⊕h(x)⊕ru로 구성되기 때문에, 서버는 공격자가 재전송한 C값에 h(x)를 XOR 연산하여, R=h(IDi)⊕ru 값을 계산한다. 계산한 암호화키 R로 메시지를 복호화한 후에 얻어낸 정보 ru와 IDi를 이용하여 서버가 직접 계산한 h(IDi)⊕ru 값과 비교하면, 두 값이 동일하기 때문에 서버는 공격자를 정당한 사용자로 인증하고, 다음 과정들을 진행하게 된다. 그러므로 이 기법은 공격자가 암호화키 R을 몰라도 가로챈 정보를 재전송하여, 최소한 서버에 계산로드를 발생시킬 수 있는 취약점이 존재한다.

2. 패스워드 오입력시의 취약점

이 기법은 기존의 패스워드 PWi를 입력하면, M⊕h(PWi⊕N)과 저장된 값 m을 비교하여 패스워드 오입력을 체크한다. 그러나, 〔단계2〕는 새로운 패스워드 PWi′ 를 입력받은 후 m*=m⊕h(PWi⊕N)⊕h(PWi′ ⊕N)을 계산하여 기존의 m을 새로운 m*로 갱신한다. 그러므로 〔단계2〕는 새로운 패스워드 PWi′ 의 오입력 여부를 체크하지 않기 때문에, 전체적인 패스워드 변경단계는 여전히 패스워드 오입력의 취약점이 존재한다.

3. 사용자 익명성과 내부자 공격

이 기법은 로그인 요청 메시지 {C, ER{ru, IDi}}를 서버에 전송한다. 서버에서 메시지 복호화시, 정당한 사용자의 IDi가 그대로 노출되기 때문에, 이 기법은 제3자에 대한 사용자 익명성은 제공하지만, 서버 자체에 대한 사용자 익명성은 제공하지 못한다. 또한, 서버에서 노출되는 IDi는 내부 공격자가 획득할 수 있으며, 공격자는 가로챈 IDi를 이용하여, 정당한 사용자를 가장하여 다른 서버의 로그인 시도를 통해, 정당한 사용자의 개인 정보 등을 얻어낼 수 있다. 이는 일반적으로 동일한 IDi를 여러 서버에서도 사용하는 경우가 많기 때문에 가능하다.

IV. 제안 인증기법

본 장에서는 3장에서 살펴본 기존의 사용자 익명성 제공 인증기법의 취약점들을 개선한 새로운 사용자 익명성 제공 인증기법을 제안한다. 제안 인증기법은 날로 증가하는 개인정보 침해사고에 보다 안전하게 대응하기 위해서, 서버에 대한 사용자 익명성도 함께 제공하며, 원격 서버가 사용자의 악의적인 행동을 감지하거나 다른 문제가 발생할 경우를 대비해 사용자를 추적할 수 있는 기능도 제공한다. 또한, 본 논문에서 제안하는 인증기법은 내부자 공격의 저항성도 함께 제공하며, 패스워드 오입력시의 취약점도 해결하여, 패스워드를 오입력할 경우 계산로드가 원격 서버로까지 전이하는 문제도 해결한다.

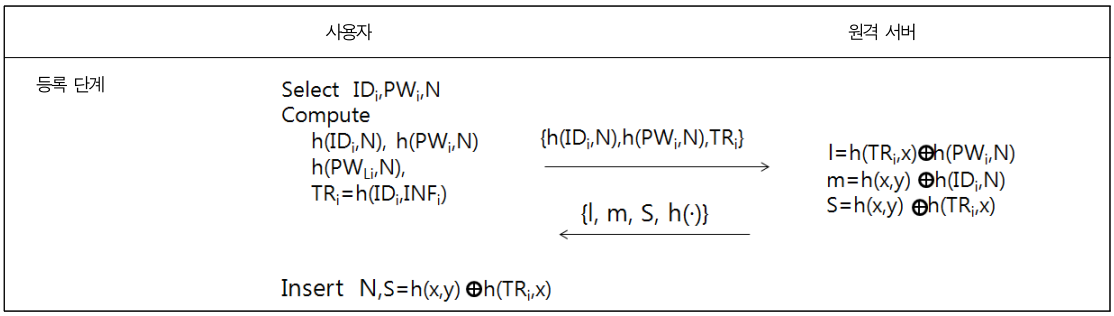

그림 1. 제안 인증기법의 등록 단계
Fig. 1. Registration Phase of The Proposed Authentication Scheme

4.1 등록 단계

등록 서버에 등록을 원하는 사용자는 자신의 IDi와 PWi, INFi를 입력하여 다음 과정을 진행한다. INFi는 사용자의 개인 정보로서, 취미, 좋아하는 색, 가족이나 친척 관계 등을 나타내는 개인 정보이다.

〔단계1〕 카드는 난수 N을 생성한 후, h(PWi,N), h(IDi,N), h(PWLi,N), TRi=h(IDi,INFi)를 계산해, 서버에 제출한다.

〔단계2〕 서버는 등록요청 메시지, 자신의 비밀키 x, 비밀값 y를 이용하여 l=h(TRi,x)⊕h(PWi,N), m=h(x,y)⊕h(IDi,N), S=h(x,y)⊕h(TRi,x)를 계산한 후, {m, l, S, h()}를 스마트카드에 등록한다.

〔단계3〕 서버는 안전한 채널을 통해 스마트카드를 사용자에게 발급한다.

〔단계4〕 카드는 S와 h(PWLi,N)를 XOR 연산하여, 난수N과 함께 저장한다. 여기서, PWLi은 입력한 전체 패스워드값 중 왼쪽 절반 값을 의미한다.
S=h(x,y)⊕h(TRi,x)⊕h(PWLi,N)

4.2 로그인 단계

사용자는 자신의 스마트카드를 카드 리더기에 삽입한 후, 자신의 IDi와 PWi를 입력한다.

〔단계1〕 스마트카드에 저장된 난수 N과 함께 h(PWi,N), h(IDi,N), h(PWLi,N)을 계산한 후 다음을 계산한다.
l′ =l⊕h(PWi,N), m′=m⊕h(IDi,N)
l′⊕m′ ?= S⊕h(PWLi,N)
l′⊕m′과 S⊕h(PWLi,N)을 비교하여 두 값이 동일할 경우, IDi와 PWi 모두 올바로 입력되었다고 간주한다.

〔단계2〕 카드는 난수 ru를 생성하여 다음을 계산한다.
C=m⊕ru = h(x,y)⊕h(IDi,N)⊕ru,
X=S⊕h(PWLi,N), R=h(IDi,N)⊕ru

〔단계3〕 타임스탬프 Tu를 생성한 후, R로 암호화하여 {Tu,C,ER{Tu,ru,h(IDi,N),l,X}}를 서버에 전송한다.

4.3 인증 단계

로그인 요청 메시지를 전송받은 서버는 다음을 진행한다.

〔단계1〕 서버는 타임스탬프의 시간간격 타당성을 체크한 후, 타당한 시간간격일 경우에만 다음 단계를 진행하고, 그렇지 않을 경우 로그인 요청을 거절한다.

〔단계2〕 서버는 자신의 비밀키 x와 자신의 비밀정보 y를 이용해서 C⊕h(x,y)=h(IDi,N)⊕ru를 계산한다.

〔단계3〕 서버는 R′=h(IDi,N)⊕ru을 이용해 암호화된 메시지를 복호화한 후, h(IDi,N)과 ru을 얻어내어 h(IDi,N)

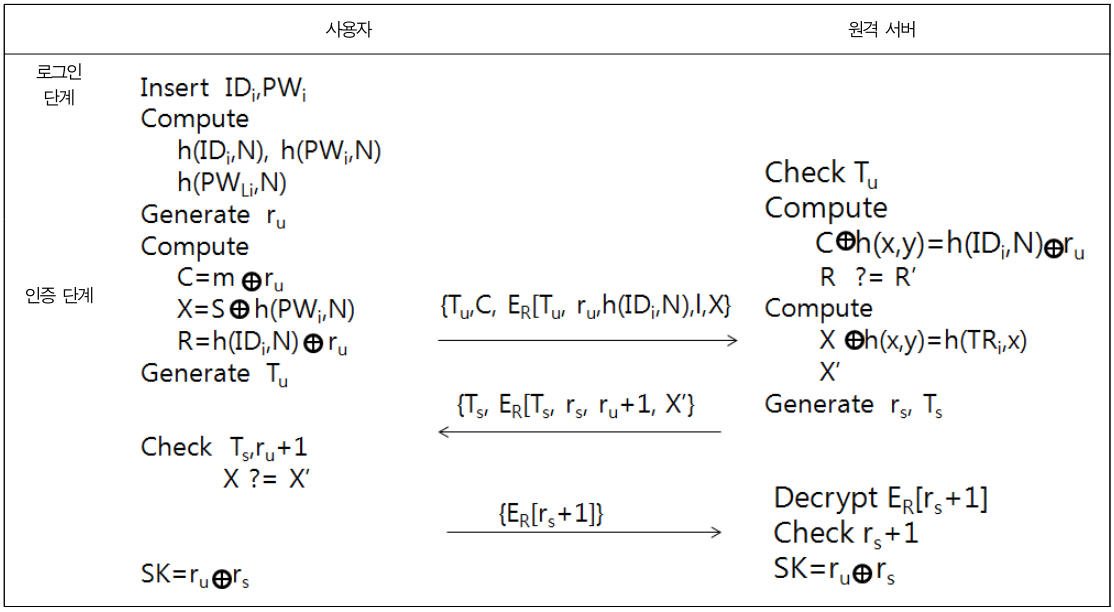

그림 2. 제안 인증기법의 로그인 단계와 인증 단계
Fig. 2. Login Phase and Authentication Phase of The Proposed Authentication Scheme

⊕ru을 계산한 후 R′과의 동일성을 체크한다. 동일하지 않을 경우, 서비스를 중단한다.

〔단계4〕 서버는 X⊕h(x,y)를 계산한 후, 사용자의 추적정보 h(TRi,x)를 계산하고 데이터베이스에 저장한다.

〔단계5〕 h(TRi,x)를 이용해 l⊕h(TRi,x)=h(PWi,N)을 계산한 후, h(x,y), h(TRi,x), h(PWi,N) 값을 이용해 X′=h(x,y)⊕h(TRi,x)⊕h(PWi,N)⊕(ru+1)를 계산한다.

〔단계6〕 서버는 난수 rs와 타임스탬프 Ts를 생성하여 암호화한 후, {Ts,ER{Ts,rs,ru+1,X′}}을 사용자에게 전송한다.

〔단계7〕 사용자는 타임스탬프 Ts의 시간간격 타당성을 체크한 후, 타당할 경우에만 다음 단계를 진행한다.

〔단계8〕 사용자는 메시지를 복호화하여 자신의 난수에 ru+1을 계산해, 서버가 전송한 ru+1과의 동일성 여부를 체크한다. 동일할 경우, 자신의 정보를 이용해 X′의 타당성을 체크한 후, 타당하면 서버인증 성공이고, ER{rs+1}을 암호화한 후 서버에 전송한다.

〔단계9〕 서버는 복호화 후, rs+1의 타당성을 체크하여, 타당할 경우, SK=rs⊕ru를 생성하여 세션키로 사용한다.

4.4 패스워드 변경 단계

사용자는 원격서버의 도움 없이 패스워드를 변경할 수 있다.

〔단계1〕 자신의 IDi와 현재의 패스워드 PWi를 입력하면, 카드에 저장된 난수 N과 함께 h(PWi,N), h(IDi,N), h(PWLi,N)을 계산하여 다음과 같이 계산한다.

l′ =l⊕h(PWi,N), m′=m⊕h(IDi,N),

l′⊕m′ ?= S⊕h(PWLi,N)

l′⊕m′과 S⊕h(PWLi,N)을 비교하여 동일할 경우, IDi와 PWi 모두 올바른 값이 입력되었다고 간주한다.

〔단계2〕 새로운 패스워드 PWi′와 새로운 난수 N′을 생성하여, 〔단계1〕을 실행한 후, 새로운 패스워드의 오입력 여부를 체크한다. 정당한 새로운 패스워드인 경우, l′, m′, S′을 새로운 lnew, mnew, Snew 값으로 갱신한다.

lnew=l′⊕h(PWi′,r′), mnew=m′⊕h(IDi,N′), Snew=h(x,y)⊕h(TRi,x)⊕h(PWLi′,N′)

V. 제안 인증기법의 분석

본 장에서는 새롭게 제안한 인증기법을 안전성 측면과 효율성 측면에서 비교·분석함으로써, 제안 인증기법이 향상된 사용자 프라이버시를 제공함을 보인다.

5.1 안전성 분석

1. 사용자 익명성

Chien[8]은 로그인 요청 메시지 {C,T,ER{IDi,ru,T}}, Hu[9]는 {C,T,ER{IDi,ru,Nu}}, Horng[10]는 {C,ER{IDi,M1}}, Bindu[15]는 {C,T,ER{IDi,ru,T}}을 전송하여 통신채널상에 사용자의 IDi가 드러나지 않는다. 그러므로 이들 기법들은 제3자에 대한 사용자 익명성은 제공한다. 그러나, 암호화 키 R을 아는 서버와

표 2. 안전성 비교
Table 2. Comparison of Security Properties

기호	Chien[8]	Hu[9]	Bindu[15]	백이루[14]	Horng[10]	제안기법
추적가능성	X	X	X	X	X	O
서버에 대한 사용자익명성	X	X	X	X	X	O
제3자에 대한 사용자 익명성	X	X	O	O	O	O
내부자 공격	X	X	X	X	X	O
패스워드 오입력 체크여부	slow	slow	slow	slow	slow	fast
스마트카드 분실시의 저항성	X	X	O	X	O	O
패스워드 변경단계	O	O	X	O	O	O
세션키 설정	O	O	O	O	O	O
재전송 공격의 저항성	O	X	O	X	X	O
위장공격의 저항성	X	X	O	O	O	O
상호 인증	X	X	O	O	O	O

사용자는 복호화가 가능하기 때문에, 서버에서 사용자의 IDi가 노출되어 서버에 대한 사용자 익명성은 제공하지 못한다. 그러므로 이들 기법들은 모두 서버에 대한 사용자 익명성은 제공하지 못한다. 제안한 인증기법은 로그인 요청 메시지 {Tu,C,ER{Tu,ru,NIDi,l,X}}를 전송하기 때문에, 제3자에 대한 사용자 익명성을 제공한다. 또한, 제안 인증기법은 서버에서 NIDi=h(IDi,N)값만 알 수 있고, 인증 단계의 모든 과정에서도 평문형태의 사용자 IDi는 드러나지 않는다. 결과적으로 비교 기법들 중 제안 인증기법만이 서버에 대한 사용자 익명성을 제공한다.

2. 추적 가능성

원격 서버는 사용자의 악의적인 행동을 감지하거나 다른 문제가 발생할 경우, 악의적인 사용자를 찾아낼 수 있어야하며, 사용자는 자신의 행위에 대해 책임져야한다[16]. 이러한 추적 가능성을 제공하기 위해, 제안 인증기법에서는 등록 단계에서 TRi=h(IDi,INFi)를 계산하여 서버에 제출한다. TRi값 자체는 해쉬처리되어 있으므로 서버에서 곧바로 드러나지 않으며, 서버의 비밀키 x와 함께 해쉬함수 처리된다. 인증시 [단계4]에서 서버는 사용자의 전송 메시지를 통해 h(TRi,x)를 계산해내고, 나중에 문제 발생시 사용자 추적과 사용자의 행위 입증을 위해 이 값을 데이터베이스에 저장한다. 문제 발생시 사용자의 IDi와 INFi 값의 제출을 통해, 사용자의 행위를 판별할 수 있다. 그러므로 제안 인증기법은 사용자의 IDi값 대신에 NIDi=h(IDi,N) 값에 의해 서버에 대한 사용자 익명성을 제공하면서, TRi 값에 의한 추적가능성을 제공한다.

3. 내부자 공격

Chien[8]은 등록시 IDi, PWi를 서버에 제출하고, Bindu[15]는 IDi, h(PWi)를 제출, Hu[9], Horng[10] 등은 모두 IDi, h(PWi,r)를 제출하다. 그러므로 이 기법들은 내부 공격자가 IDi를 알 수 있고, 가로챈 IDi를 가지고 다른 서버에 접속을 시도하여 사용자의 다른 정보를 수집할 수 있다. Chien 기법은 IDi, PWi 모두 평문형태로 노출되므로 내부자 공격에 매우 취약하다. 제안 인증기법은 등록 단계에서 사용자가 계산한 h(PWi,N), h(IDi,N), TRi를 서버에 제출하고, 인증 단계에서 서버의 계산과정에서도 사용자의 IDi나 PWi가 드러나지 않는다. 그러므로, 제안 인증기법은 비교 기법들과 달리 내부자 공격에 안전성을 제공한다고 할 수 있다.

4. 패스워드 오입력시의 취약점

Hu[9]의 인증기법은 백이루[14]의 기법과 동일한 패스워드 변경 방법을 사용한다. 그러므로 3.2절의 취약점 분석과 동일한 방법에 의해, Hu 기법도 패스워드 오입력의 취약점이 존재한다. 제안 인증기법은 [단계1]에서 $l'\oplus m'$과 $S\oplus h(PWLi,N)$을 비교하여 오입력 여부를 체크하고, [단계2]에서도 새로운 패스워드 PWi' 입력시, [단계1]을 다시 실행하여 [단계1]에서 한 것처럼, l'이 $l^*=l'\oplus h(PWi',N')$, m'은 $m^*=m'\oplus h(IDi,N')$ 계산 후, $l^*\oplus m^*$과 $S'\oplus(PWLi',N')$ 값을 비교하여 새로운 패스워드 PWi'에 대한 오입력 여부를 체크한다. 그러므로 제안 인증기법은 패스워드 오입력의 취약점을 해결하였음을 알 수 있다.

5. 서버/사용자 위장 공격

공격자가 정당한 사용자나 서버로 위장하기 위해서는 전송 메시지 {Tu, C, ER{Tu,ru,NIDi,l,X}}, {Ts, ER{rs,Ts,ru+1,X'}}, ER{rs,ru+1} 등으로부터 서버의 비밀키 x, 비밀값 y, PWi, IDi, 난수 등을 얻어낼 수 있어야한다. 공격자가 전송 메시지 $C=h(x,y)\oplus h(IDi,N)\oplus ru$로부터, 이들 정보를 얻어낼려면 h(x,y)와 h(IDi,N)의 값을 알아야한다. 그러나 해쉬함수는 일방향의 특성상 안전하여 공격자는 비밀 정보를 획득하기 어렵다. 다른 기법들도 사용자 익명성 부분에서 살펴본 것처럼, 전송 메시지 중 암호화되지 않은 평문 C의 구성이 Bindu는 $C=h(x)\oplus h(IDi,x)\oplus h(PWi)\oplus ru$, Horng은 $C=gal \bmod p$ 등을 사용해 일방향 해쉬함수나 멱승을 사용하여, 이 C값들을 통해 암호화 키 R을 얻어내기 힘들다. 그러므로 비교 기법 일부와 제안 인증기법들은 서버/사용자 위장 공격에 안전하다고 할 수 있다.

6. 카드 분실시의 취약점

Hu[9] 기법은 {IDi,m,I,M,N,b,h(),p,g}를 카드에 저장한다. 카드 분실시, 3장 취약점에서 살펴본 백이루 등의 인증기법과 동일하게 사용자의 IDi를 평문형태로 카드에 저장함으로써, 다른 정보들이 안전하다고 할지라도 카드 분실시에는 사용자의 IDi가 그대로 노출되어 사용자 익명성을 안전하게 제공할 수 없다. Chien 기법은 카드에 $m=h(IDi,x)\oplus h(x)\oplus PWi$, $I=h(IDi,x)$를 저장하고, 전송 메시지는 $C=h(IDi,x)\oplus h(x)\oplus ru$, $ru=ga \bmod p$이다. PWi가 평문이기 때문에, $1\oplus m$ 연산에서 $h(x)\oplus PWi$를 얻어내고, 공격자가 h(x)를 모른다할지라도 m의 h(IDi,x)와 h(x)는 고정된 값이기 때문에, 전수조사 등을 통해 PWi를 얻어낼 확률도 높아, 이 기법도 사용자 익명성을 안전하게 제공하기 어렵다. 제안 인증기법은 난수 N을 사용하여 h(IDi,N), h(PWi,N), h(x,y), h(TRi,x)처럼 해쉬처리한 값들을 저장하고, I, m, S 등은 여러 연산에 의해서도 평문형태의 비밀정보는 얻어내기 어렵다. 안전한 해쉬함수의 특성과 매 세션마다 난수 N을 이용해 매번 다른 값의 메시지 전송이 가능하기 때문에, 공격자가 이미 얻어낸 값들은 현재의 세션에서는 유효하지 않아, 제안 인증기법은 스마트카드 분실시 해쉬함수를 깨지 않는 한 안전성을 제공한다고 할 수 있다.

7. 재전송 공격

Chien[8] 기법은 로그인 요청 메시지 {C,T,ER{IDi,ru,T}}에 타임스탬프 T를 사용하고, Bindu[15] 기법도 {C,T,ER{IDi,ru,T}}에 타임스탬프 T를 사용하여, 재전송 공격에 안전하다. 제안 인증기법도 타임스탬프를 사용하여 재전송 공격에 대한 저항성을 가진다.

8. 전방향 안전성

전방향 안전성(forward secrecy)이란 오랜 기간 사용하는 비밀키가 노출되었을 때 이전 세션들에서 생성된 세션키를 획득할 수 있는지의 여부를 통해 결정된다. 제안 인증기법은 서버의 비밀키 x나 사용자의 PWi가 노출된다 할지라도 세션키 생성은 사용자와 서버가 각각 생성한 난수 ru, rs를 사용하기 때문에, 공격자는 세션키를 유도하기 힘들다. 그러므로 제안 인증기법은 전방향 안전성을 제공한다.

5.2 효율성 분석

본 절에서는 각 인증기법들이 각 단계에서 필요한 연산 횟수 등을 통해 계산의 효율성을 비교한다. <표3>과 같이 제안 인증기법은 등록 단계에서는 5H로 다른 기법들보다 더 많은 해쉬연산을 필요로 한다. 그러나 모든 단계를 총괄하여 비교한 연산에서는 제안 인증기법은 9H+6S 연산이 필요하고, Chien은 5H+4E+4S, Horng은 9H+8E+4S 연산으로 가장 많은 연산이 필요하다. 멱승연산(E)은 계산소비적이기 때문에, 멱승을 사용하는 기법들은 실제로는 제안 인증기법에 비해 더 많은 시간이 필요할 수 있다. 그러므로 단순히 총괄한 연산횟수 비교만으로도 제안 인증기법은 서버에 대한 사용자 익명성, 추적가능성, 내부자 공격 등에 안전한 기능을 제공하면서 패스워드 오입력으로인한 원격 서버의 계산로드까지 해결하였기 때문에, 안전성 및 효율성 측면을 모두 고려할 경우 제안 인증기법이 가장 안전하면서 효율적인 인증기법이고 할 수 있다.

VI. 결 론

본 논문에서는 날로 증가하는 개인정보 침해사고를 방지하고, 사용자 프라이버시를 보다 안전하게 제공할 수 있도록 서버에 대한 사용자 익명성을 제공할 뿐만 아니라 원격 서버가 악의적인 사용자를 추적할 수 있는 기능도 함께 제공하였다. 또한, 제안한 인증기법은 패스워드 오입력의 취약점을 해결함으로써, 계산로드가 원격서버로까지 전이되는 문제를 개선하여, 전체 시스템의 계산로드를 줄였다. 제안 인증기법은 물리적으로 강인한 스마트카드를 사용한다고 가정하지만, 소비전력 모니터링 등을 통해 제3자에 의한 정보획득이 가능하기 때문에, 카드 분실시 평문형태의 비밀정보가 노출되는 취약점도 함께 개선하였다. 결과적으로 제안 인증기법은 사용자에게 보다 안전한 프라이버시를 제공한다고 할 수 있다. 향후 과제로는 추적가능성을 제공하는 인증기법들에 대한 분석을 통해, 보다 안전한 비도를 제공하는 사용자 추적 가능한 인증기법을 연구하는 것이다.

참고문헌

[1] E. Smirni, and G. Ciardo, "Workload-Aware Load Balancing for Cluster Web Servers," IEEE Trans. on Parallel and Distributed Systems, Vol. 16, No. 3, pp. 219-232, March 2005.

[2] M. S. Hwang, C. C. Lee, Y. L. Tang, "A Simple Remote User Authentication Scheme," Mathematical and Computer Modeling 36, pp.103-107, 2002.

[3] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "An improvements of Hwang-Lee-Tang's simple remote user authentication

표 3. 계산 비용의 비교
Table 3. Comparison of Computation Costs

기호	Chien[8]	Hu[9]	Bindu[15]	백이루[14]	Horng[10]	제안기법
등록 단계	3H	3H	3H	3H	3H+1E	5H
로그인단계	1H+1E+1S	2H+1E+1S	1H+1S+1E	2H+1S	1H+3E+1S	3H+1S
인증 단계	2H+3E+3S	3H+1E+1S	1H+5S+1E	2H+5S	5H+4E+3S	1H+5S
전체 필요 연산	6H+4E+4S	8H+2E+2S	5H+6S+2E	7H+6S	9H+8E+4S	9H+6S
승수계산 필요여부	O	O	O	X	O	X
암호 방식	h(·),S	h(·),S	h(·),S	h(·),S	h(·),S	h(·),S
H: 해쉬 함수, S: 대칭키 암호, E: 지수 계산, h(·):해쉬함수						

scheme," Computer and Security24, pp.50-56, 2005.
[4] H. M. Sun, "An Efficient Remote Use Authentication Scheme Using Smart Cards," IEEE Transaction on Consumer Electronics, Vol.46, No.4, pp.958-961, November 2000.
[5] H.Y.Chien, J.K.Jan, and Y.M.Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," Computer and Security, Vol.2, No.4, pp.372-375, 2002.
[6] H.C.Hsiang and W.K.Shih, "Weakness and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications 32, pp.649-652, 2009.
[7] K. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, Vol.50, No.2, pp.629-631, 2004.
[8] H.Y.Chien, and C.H.Chen, "A remote authentication scheme preserving user anonymity," IEEE AINA'05, Vol.2, pp.245-248, March 2005.
[9] L. Hu, Y, Yang, and X. Niu, "Improved Remote User Authentication Scheme Preserving User Anonymity," Fifth Annual Conference on Communication Network and Services Research(CNSR), pp.323-328, 2007.
[10] W. B. Horng, C. P. Lee, and J.W. Peng, "A Secure Remote Authentication Scheme Preserving User Anonymity with Non-Tamper Resistant Smart Cards," WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Issue 5, Vol.7, pp.619-628, May 2010.
[11] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," Lecture Notes in Computer Science, Vol.3156, pp.135-152, 2004.
[12] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully attacking masked AES hardware implementations," Lecture Notes in Computer Science, Vol.3659, pp.157-171, 2005.
[13] O. Choudary (osc22), "Breaking Smartcards Using Power Analysis", University of Cambridge.
[14] Y. R. Baek, K. E. Gil, J.C.Ha, "A remote Protocol Using Smart Card to Guarantee User Anonymity", Journal of Korea Society for Internet Information, Vol.10, No.6, pp.229-239, 2009.
[15] C. S. Bindu, P. C. S. Reddy, and B. Satyanarayana, "Improved Remote User Authentication Scheme Preserving User Anonymity," IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.3, pp.62-66, March 2008.
[16] S. I. Kim, J. Y. Chun, and D. H. Lee, "Anonymity User Authentication Scheme with Smart Cards preserving Traceability", Journal of Korea Institutes Information Security and Cryptology, Vol.18, No.5, pp.31-39, 2008. 10.

저 자 소 개

박 미 옥
1993 : 숭실대학교 컴퓨터학과 공학석사
2004 : 숭실대학교 컴퓨터공학과 공학박사
현 재 : 성결대학교 컴퓨터공학부 조교수
관심분야 : 모바일 보안, 암호 프로토콜
Email : mopark777@hanmail.net