Journal of The Korea Society of Computer and Information
Vol. 18, No. 2, February 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.2.087

# Khan 인증기법의 취약점 분석과 개선된 사용자 익명성 제공 인증기법

박 미 옥

# Weaknesses Cryptanalysis of Khan's Scheme and Improved Authentication Scheme preserving User Anonymity

Mi-Og Park

## 요 약

본 논문에서는 2011년 Khan[7] 등에 의해 제안된 사용자 익명성 제공 인증기법에 대한 취약점을 분석하고, 이러한 취약점을 개선한 새로운 사용자 익명성 제공 인증기법을 제안한다. Khan의 인증기법은 내부자 공격에 취약하고 서버에 대한 사용자 익명성을 제공하지 못한다. 또한, 패스워드 변경 단계를 제안하고 있음에도 불구하고, 여전히 패스워드 오입력시의 취약점이 존재한다. 본 논문에서는 Khan 기법이 스마트카드를 분실할 경우의 취약점과 강력한 서버/사용자 가장 공격에도 취약함을 보인다. 제안 인증기법은 이러한 취약점들을 개선하여 사용자에게 보다 안전한 프라이버시를 제공할 수 있는 향상된 사용자 익명성을 제안한다.

▸ Keywords : 사용자 익명성, 스마트카드, 내부자 공격, 강력한 가장 공격, 사용자 프라이버시

## Abstract

In this paper, we analyse the weaknesses of authentication scheme preserving user anonymity proposed by Khan et al in 2011 and we propose a new authentication schemes preserving user anonymity that improved these weaknesses. Khan et al's authentication scheme is vulnerable to insider attack and doesn't provide user anonymity to the server. Also, this scheme is still a weakness of wrong password input by mistake in spite of proposing the password change phase. In this paper, we will show that Khan et al's scheme is vulnerable to the stolen smart card attack and the strong server/user masquerade attack. The proposed authentication scheme propose the improved user anonymity, which can provide more secure privacy to user by improving these weaknesses.

▸ Keywords : User Anonymity, Smart Card, Insider Attack, Strong Masquerade attack, User Privacy

• 제1저자 : 박미옥
• 투고일 : 2012. 11. 13, 심사일 : 2012. 12. 5, 게재확정일 : 2013. 1. 9.
* 성결대학교 컴퓨터공학부(Division. of Computer Science Engineering, Sungkyul University)

# I. 서 론

원격 사용자 인증기법은 1981년 Lamport[1]가 처음으로 제안한 인증기법으로부터 시작하여, 1991년에는 Chang과 Wu[2] 등이 스마트카드와 패스워드를 기반으로 하는 원격 사용자 인증기법을 제안하였다. 스마트카드와 패스워드를 기반으로 하는 많은 인증기법들은 원격 서버에서 패스워드 검증 테이블(password verification table)을 저장하지 않는 특성을 가진다[3-5]. 2004년에는 Das 등[6]이 최초로 통신채널상의 제3자에 대한 사용자 익명성을 보장하는 인증기법을 제안하였다. 이 인증기법은 동적 아이디(dynamic-ID)에 기반한 인증기법으로서, 로그인시마다 사용자의 식별자(ID)를 변경하여 통신채널상에 존재하는 제3자에게 사용자의 식별자가 노출되지 않도록 하는 기법이다. 최근에 제안된 사용자 익명성 제공 인증기법 중 2011년에 Khan[7] 등은 2009년에 Wang[8] 등이 제안한 사용자 익명성 제공 인증기법의 취약점을 지적하고, 개선된 사용자 익명성 제공 인증기법을 제안하였다. Wang[8]이나 Khan[7] 등의 인증기법들은 해쉬함수와 XOR 연산만을 사용하여, 계산 소비적인 멱승 연산을 수행하는 인증기법들에 비해 훨씬 계산 효율적이라 할 수 있다. 2012년에는 Madhusudhan[9] 등이 Khan의 인증기법이 내부자 공격과 패스워드 오입력시에 취약하다는 것을 지적하였다. Khan 등의 인증기법은 패스워드 변경 단계를 제안하고 있음에도 불구하고, 로그인 단계에서 패스워드 오입력에 대한 검증단계가 부재하여 여전히 패스워드 오입력의 취약점이 존재한다는 것이다. 패스워드 변경 단계가 부재하여 패스워드 오입력의 취약점이 존재하는 인증기법들[10]도 많지만, 패스워드 변경 단계를 제안하고 있음에도 불구하고, 패스워드 오입력의 취약점이 여전히 존재하는 인증기법들[6-8][11]도 적지 않다. 또한, Khan 등은 사용자 익명성을 보장하는 인증기법을 제안하였지만, 내부자 공격에 취약하기 때문에 사용자가 신뢰할 수 있는 프라이버시를 제공할 수 없다. 그러므로 본 논문에서는 사용자에게 보다 신뢰할 수 있는 프라이버시 제공을 위해 서버 내에 존재하는 악의적인 내부자 공격에 대한 저항성과 서버에 대한 사용자 익명성을 제공하는 개선된 인증기법을 제안하고자 한다. 또한, 본 논문에서는 Madhusudhan[9] 등이 지적하지 않은 Khan 기법의 다른 취약점들을 분석함으로써, 제안된 인증기법도 분석된 취약점들에 노출되지 않도록 보다 향상된 인증기법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 Khan의 인증기법을 살펴보고, 3장에서는 이 인증기법의 취약점을 분석한다. 4장에서는 분석된 취약점들을 개선한 향상된 사용자 익명성 제공 인증기법을 제안하고, 5장에서는 제안 인증기법을 안전성 및 효율성 측면에서 비교·분석한다. 마지막으로 6장에서 결론을 맺고 본 논문을 마친다.

# II. 관련 연구

본 장에서는 2011년 Khan[7] 등이 제안한 사용자 익명성 제공 인증기법에 대해 살펴본다.

표 1. 표기법
Table 1. Notation

| 기호 | 의미 |
|---|---|
| IDi | IDentity of user |
| PWi | Password of user |
| h(·) | Secure one-way hash function |
| x, y | Secret key and value of server |
| ‖ | Concatenation operator |
| ⊕ | XOR operation |

## 2.1 Khan 등의 인증기법

### 등록 단계

등록 센터에 등록을 원하는 사용자는 다음을 수행한다.

[단계1] 사용자는 $ID_i$와 $PW_i$를 선택하고, 난수 r을 생성하여 $h(r \| PW_i)$를 계산한다.

[단계2] $ID_i$, $h(r \| PW_i)$를 안전한 채널을통해 서버에 제출한다.

[단계3] 서버는 사용자 $ID_i$의 데이터베이스 존재여부를 검증한다. 서버는 사용자의 등록 기록을 확인하여 처음 등록하는 사용자일 경우, N=0으로 저장하고 재등록일 경우는 N=1로 저장한다.

[단계4] 서버는 $J=h(x \| IDU)$를 계산한다. $IDU=(ID_i \| N)$이다.

[단계5] 서버는 $L=J \oplus RPW$를 계산한다.

[단계6] 서버는 {L, y}를 스마트카드에 저장하여 안전한 채널을 통해 사용자에게 발급한다.

[단계7] 사용자는 난수 r을 스마트카드에 저장한다.

### 로그인 단계

사용자는 자신의 $ID_i$와 $PW_i$를 입력한다.

[단계1] 스마트카드는 저장된 난수 r를 이용하여, $RPW=h(r \| PW_i)$, $J=L \oplus RPW$를 계산한다.

[단계2] 타임스탬프 $T_i$를 생성하고 $C_1=h(T_i \| J)$를 계산한다.

[단계3] 난수 d를 생성하여 $AID_i=ID_i \oplus h(y \| T_i \| d)$를 계산

한다.

〔단계4〕 사용자는 $\{T_i, AID_i, d, C_1\}$을 서버에 전송한다.

인증 단계

원격 서버는 사용자 인증을 위해 다음 단계를 수행한다.

〔단계1〕 타임스탬프 $T_i$의 시간간격 타당성을 체크하여, 타당한시간간격일 경우에만 다음 단계를 수행한다.

〔단계2〕 $ID_i=AID_i\oplus h(y\|T_i\|d)$를 계산하여, 사용자 $ID_i$가 타당한 식별자인지 체크한다. 타당한 식별자가 아닌 경우, 서비스를 거절한다.

〔단계3〕 데이터베이스 안의 N값을 조사하여, $IDU=(ID_i\|N)$를 계산한다.

〔단계4〕 $J=h(x\|IDU)$를 계산하고, $h(T_i\|J)$와 $C_1$ 값의 동일성 여부를 체크해, 동일할 경우 로그인 요청을 받아들인다. 그렇지 않을 경우, 서비스를 거절한다.

〔단계5〕 상호인증을 위해, 서버는 타임스탬프 $T_s$를 생성하고 $C_2=h(C_1\oplus J\oplus T_s)$를 계산하여 사용자에게 $\{C_2, T_s\}$를 전송한다.

〔단계6〕 사용자는 타임스탬프 $T_s$의 시간간격 타당성을 체크하여, 타당한 시간간격일 경우에만 다음 단계를 수행한 다. 그렇지 않을 경우 이 과정을 중단한다.

〔단계7〕 사용자는 $h(C_1\oplus J\oplus T_s)$를 계산하여 $C_2$와 동일한지 비교한다. 동일할 경우, 사용자는 서버를 인증하고, 그렇지 않을 경우 이 과정을 중단한다.

패스워드 변경 단계

사용자가 $ID_i$와 $PW_i$를 입력하면, 카드는 다음을 수행한다.

〔단계1〕 $RPW^*=h(r\|PW_i)$와 $J^*=L\oplus RPW^*$를 계산한다. 만약, J와 $J^*$가 동일하면, 패스워드 변경이 가능하고, 그렇지 않을 경우 이 단계를 종료한다.

〔단계2〕 새로운 패스워드 $PW_i'$를 선택하여, $L=J\oplus RPW\oplus RPW^*\oplus h(r\|PW_i')$를 계산한 후, 새로운 L 값을 스마트카드에 저장한다.

## III. Khan 기법의 취약점 분석

### 3.1 기존의 취약점

본 절에서는 Madhusudhan〔9〕의 인증기법에서 지적한 Khan〔7〕의 취약점들을 살펴본다.

내부자 공격

Khan 기법은 등록 단계에서 $ID_i$와 $RPW=h(r\|PW_i)$를 제출하고, 난수 r은 제출하지 않는다. 사용자의 $ID_i$가 그대로 서버에 드러나기 때문에, 서버내의 공격자는 모든 가능한 난수 r′과 $PW_i'$를 선택하여, $RPW=h(r\|PW_i)$값과 동일할 때까지 전수조사 등을 통해 $PW_i$를 추측할 수 있다〔9〕.

패스워드 오입력시의 취약점

이 기법은 패스워드 변경 〔단계1〕과 같이, 입력한 패스워드를 이용한 계산값이 $J\ ?=J^*$인지 비교하여, 패스워드 오입력 여부를 확인한다. 그러나 로그인 단계에서는 입력한 $PW_i$를 이용해 $RPW=h(r\|PW_i)$를 계산한 다음 $J=L\oplus RPW$을 계산하기 때문에, 패스워드 오입력을 확인할 수 있는 방법이 부재하여, 패스워드 오입력의 취약점이 여전히 존재한다. 또한, 이러한 취약점으로 인하여, 원격 서버로까지 계산로드가 전이되는 문제도 발생한다.

### 3.2 취약점 분석

본 절에서는 Khan 기법의 취약점을 새롭게 분석해본다.

서버에 대한 사용자 익명성

이 기법은 서버에 로그인을 위한 요청 메시지 $\{T_i, AID_i, d, C_1\}$을 전송하여, 사용자의 $ID_i$가 노출되지 않는다. 그러므로 이 기법은 서버와 사용자를 제외한 제3자에 대한 사용자 익명성은 제공한다. 그러나 이 기법은 등록 단계에서 $ID_i$와 $RPW=h(r\|PW_i)$를 제출하기 때문에, 서버가 $ID_i$ 값을 알게 된다. 또한, 로그인 단계에서도 $ID_i=AID_i\oplus h(y\|T_i\|d)$를 계산하여 서버측에서 $ID_i$가 노출된다. 그러므로 이 기법은 서버에 대한 사용자 익명성은 제공하지 못한다.

카드 분실의 취약점

이 인증기법은 스마트카드에 $\{L, y, r\}$을 저장한다. 평문형태로 저장된 y는 서버의 비밀 값이기 때문에, 카드 분실시 가장 민감한 정보 중의 하나가 공격자에게 그대로 노출되는 취약점이 존재한다. 그러므로 공격자가 로그인 〔단계4〕의 메시지 $\{T_i, AID_i, d, C_1\}$을 가로채고, $AID_i=ID_i\oplus h(y\|T_i\|d)$를 구성하는 타임스탬프 $T_i$, 난수 d, r, 비밀값 y를 알기 때문에, $ID_i=AID_i\oplus h(y\|T_i\|d)$의 단 한번의 XOR 연산만으로 $ID_i$를 알아낼 수 있다. 그러므로 이 기법은 카드 분실시 제3자에 대한 사용자 익명성을 제공하지 못한다.

강력한 서버·사용자 가장 공격

정당한 사용자가 공격자라고 가정할 경우, 공격자는 서버와 공유하는 비밀값 y를 알고, 자신의 패스워드 $PW_i$를 이용해, $L\oplus h(x'\|IDU)$이 $h(r\|PW_i)$ 값과 동일해질 때까지 전수조사 공격이나 사전 공격 등을 통해 서버의 비밀키 x′를 유

추할 수 있다. 또한, 이 기법은 서버의 비밀값 y가 평문형태로 저장되기 때문에 공격자가 서버와 관련된 비밀키 x와 비밀값 y를 모두 획득할 수 있는 취약점이 존재한다. 이 두 값을 획득한 공격자는 다른 타겟 사용자의 전송 메시지 {$T_i$, $AID_i$, d, $C_1$}, {$C_2$, $T_s$}를 가로채어, $ID_i=AID_i\oplus h(y\|T_i\|d)$를 계산해 사용자의 $ID_i$를 획득하고, 서버의 비밀키 x와 비밀값 y 등을 이용해, $C_1$과 $h(T_i\|h(x'\|ID\|N'))$ 값이 동일해질 때까지, $C_2$와 $h(C_1\oplus h(x'\|ID\|N')\oplus T_s)$ 값이 동일해질 때까지 지속적인 계산을 통해 적당한 N′ 값을 유추할 수 있다. 적당한 N′ 값 유추에 성공할 경우, 다른 사용자의 패스워드를 유추하기 위해, 임의의 $PW_i'$ 값을 선택해 $h(r\|PW_i')$ 값과 $L\oplus h(x'\|h(ID\|N'))$ 값이 동일해질 때까지 전수조사 공격 등을 통해 $PW_i'$를 유추할 수 있다. 그러므로, 이 기법은 강력한 가장 공격에 취약할 수 있다.

분실카드 해지시의 취약점

이 기법에서는 카드를 분실할 경우, 사용자가 서버에 카드 해지신청을 하면, 서버는 사용자의 생일, 국제 ID 카드 번호 등 사용자의 신분을 증명 가능한 비밀정보를 이용해 사용자의 신분을 검증한다. 이 검증과정을 통과하면, 서버는 데이터베이스의 N 값을 1 증가시킨다. 이 기법은 카드를 분실할 때마다 N을 1 증가시킨다. 만약 내부 공격자가 데이터베이스 액세스에 성공할 경우, 평문형태의 N을 획득할 수 있고, N값의 증가도 카드 재등록할 경우에만 1씩 증가하기 때문에 현재의 N 값을 모른다 할지라도 이전에 획득한 N 값을 1씩 증가시키면서 올바른 값을 유추할 수 있다. N 값 유추에 성공할 경우엔, 공격자는 L, $h(r\|PW_i)$, $ID_i$ 등을 알 수 있기 때문에, $L=J\oplus h(r\|PW_i)$ 연산을 이용해, $L\oplus h(r\|PW_i)=h(x'\|ID_i\|N)$를 계산하여 서버의 비밀키 x를 유추할 수도 있다. 또한, 이 기법은 N 값이 매 세션마다 증가하는 형태도 아니기 때문에, 일반적인 사용자는 재등록을 자주하지 않을 가능성이 아주 높기 때문에 N 값 자체가 작은 숫자일 확률도 높아진다. 그러므로 데이터베이스에 접근불가하다 할지라도 내부 공격자 이외의 공격자들이 N 값을 유추할 가능성이 높아진다. 그러므로 이 기법에서 제시하고 있는 카드 분실시의 해지과정은 취약점이 존재한다고 할 수 있다.

표 2. Khan 기법의 안전도 비교
Table 2. Security Comparison of Khan Scheme

| 비교 항목 | Wang | Khan | 분석결과 |
|---|---|---|---|
| 사용자 익명성 | No | Yes | No |
| 안전하게 선택된 패스워드 | No | Yes | Yes |
| 세션키 설정 동의 | No | Yes | Yes |
| 스마트카드의 해지 | No | Yes | No |
| 내부자 공격 | No | No | No |

〈표2〉는 Khan의 논문에 나타난 기존 기법과의 비교표의 내용 중 안전성 측면만 따로 나타낸 것이다. 이 표의 "분석결과"부분은 본 논문에서 분석한 결과를 새롭게 추가하여 도식화함으로써, Khan 기법에서 주장했던 안전성 기능들 중 일부는 보장되지 못함을 보인다. Khan 기법은 사용자 익명성 제공을 위해 제시된 인증기법이지만, 이 기법의 취약점 중 서버와 공유하는 비밀값 y를 평문형태로 저장하여 카드 분실시 중요정보가 그대로 노출되는 문제로 인해, $ID_i=AID_i\oplus h(y\|T_i\|d)$의 단 한번의 XOR 연산만으로 사용자의 $ID_i$가 노출된다. 전수조사 공격을 할 필요도 없이, 단 한번의 XOR 연산만으로 정당한 사용자의 $ID_i$가 그대로 노출되는 것은 사용자 프라이버시 보장 측면에서 매우 취약한 문제라고 할 수 있다.

## IV. 제안 인증기법

본 장에서는 최근에 제안된 Khan 인증기법의 취약점들을 개선하여, 제3자에 대한 사용자 익명성뿐만 아니라 서버에 대한 사용자 익명성 제공, 내부자 공격에 대한 안전성, 패스워드 오입력에 대한 취약점 등의 문제를 함께 해결하고자 한다.

### 4.1 등록 단계

〔단계1〕 스마트카드는 난수 b를 이용해 $h(ID_i)$, $h(b,PW_i)$, $h(b\oplus ID_i\oplus PW_i)$를 계산하여 서버에 제출한다.

〔단계2〕 서버는 자신의 비밀키 x와 비밀값 y를 이용해, 다음을 계산한 후 스마트카드에 저장한다.
$L=h(h(x)\oplus h(ID_i))\oplus h(b,PW_i)$,
$M=h(x\oplus y)\oplus h(b\oplus ID_i\oplus PW_i)$,
$N=h(h(x)\oplus h(ID_i))\oplus h(x\oplus y)\oplus h(h(b\oplus PW_i))$

〔단계3〕 등록 센터는 {L, M, N, h()}가 저장된 스마트카드를 안전한 채널을 통해 정당한 사용자에게 발급한다.

〔단계4〕 사용자는 스마트카드에 난수 b를 저장한다.

### 4.2 로그인 단계

〔단계1〕 스마트카드는 다음을 계산하여, $ID_i$와 $PW_i$가 올바로 입력되었는지 확인한다. $L'\oplus M'$과 N′값이 동일하면 두 값 모두 올바로 입력된 걸로 간주하고, 다음 단계를 진행한다.

$L' = L \oplus h(b, PW_i)$, $M' = M \oplus h(b \oplus ID_i \oplus PW_i)$
$N' = N \oplus h(h(b \oplus PW_i))$, $L' \oplus M' \stackrel{?}{=} N'$

〔단계2〕 서버는 $h(b \oplus ID_i)$를 연산한 후, $L'$, $M'$을 이용하여 다음 을 수행한다. $T_i$는 타임스탬프, d는 난수이다.
$AID_i = h(b \oplus ID_i) \oplus h(h(x \oplus y) \| T_i \| d)$
$C_1 = h(x \oplus y) \oplus h(b \oplus ID_i) \oplus h(b \oplus PW_i)$
$C_2 = h(h(x) \oplus h(ID_i)) \oplus h(b \oplus PW_i))$
$D = h(T_i \| C_1 \oplus C_2)$

〔단계3〕 사용자는 로그인 전송 메시지 $\{T_i, d, AID_i, C_1, C_2, D\}$를 원격 서버에게 전송한다.

### 4.3 인증 단계

〔단계1〕 서버는 타임스탬프 $T_i$의 시간간격 타당성을 체크하여 타당한 시간간격일 경우 다음 단계를 진행하고, 그렇지 않을 경우 로그인 요청을 거절한다.

〔단계2〕 서버는 전송 메시지 중 $T_i$, $C_1$, $C_2$를 이용해, $D' = h(T_i \| C_1 \oplus C_2)$를 계산하여 D와의 동일성 여부를 체크한다. 두 값이 동일하면 다음 단계를 진행하고, 그렇지 않을 경우 세션을 종료한다.

〔단계3〕 서버는 $T_i$, 난수 d, 자신의 비밀키 x와 비밀값 y를 이 용해 다음을 계산하여, $h(b \oplus ID_i)$ 값을 계산해낸다. $h(b \oplus ID_i) = AID_i \oplus h(h(x \oplus y) \| T_i \| d)$

〔단계4〕 계산한 $h(b \oplus ID_i)$를 이용해 다음 순서대로 계산하여, $h(b \oplus PW_i)$와 $h(h(x) \oplus h(ID_i)$ 값을 계산해 낸다.
$h(b \oplus PW_i) = C_1 \oplus h(x \oplus y) \oplus h(b \oplus ID_i)$
$h(h(x) \oplus h(ID_i)) = C_2 \oplus h(b \oplus PW_i)$

〔단계5〕 서버는 타임스탬프 $T_s$를 생성하여 다음을 계산한 후, 사용자에게 전송 메시지 $\{T_s, E\}$를 전송한다.
$E = h(D \oplus h(x \oplus y) \oplus h(b \oplus PW_i) \oplus T_s \oplus d)$

〔단계6〕 사용자는 타임스탬프 $T_s$의 시간간격 타당성을 검증하여, 타당한 시간간격일 경우 $T_s$와 자신의 정보 $h(x \oplus y)$, $h(b \oplus PW_i)$, 난수 d를 이용하여 E와 동일한지 체크한다. 동일할 경우, 서버를 인증하고 그렇지 않을 경우 상호 인증은 실패이며 세션을 종료한다.

〔단계7〕 서버와 사용자는 세션키 $S_K = h(E \oplus h(h(x) \oplus h(ID_i)) \oplus T_s \oplus d)$를 생성한다.

### 4.4 패스워드 변경 단계

〔단계1〕 사용자는 $ID_i$와 $PW_i$를 입력한다.

〔단계2〕 카드는 다음을 계산하여, 난수 b를 이용해 패스워드 오입력을 체크한다. $L' \oplus M'$과 $N'$이 동일하면 올바른 패스워드가 입력된 것이다.

$L' = L \oplus h(b, PW_i)$, $M' = M \oplus h(b \oplus ID_i \oplus PW_i)$,
$N' = N \oplus h(h(b \oplus PW_i))$

〔단계3〕 새로운 난수 b′과 새로운 패스워드 $PW_i'$를 입력하여, 〔단계2〕와 동일한 과정을 수행하여 새로운 패스워드가 올바로 입력되었는지 확인한다. 새로운 패스워드가 올바로 입력되었으면, $L'$, $M'$, $N'$를 새로운 값으로 업데이트한다.
$L_{new} = L' \oplus h(b', PW_i')$, $N_{new} = N' \oplus h(h(b' \oplus PW_i'))$
$M_{new} = M' \oplus h(b' \oplus ID_i \oplus PW_i')$

## V. 제안 인증기법의 분석

본 장에서는 제안 인증기법과 비교 기법들을 안전성 및 계산 효율성을 비교분석하여, 제안 인증기법의 효율성을 보인다.

### 5.1 안전성 분석

#### 서버에 대한 사용자 익명성

Wang〔8〕 기법은 로그인 요청 메시지 $\{ID_i, CID_i, N_i, T\}$를 서버에 전송한다. 서버에서 $ID_i$가 그대로 드러나기 때문에 서버에 대한 사용자 익명성도 제공하지 못한다. 제안 인증기법에서 $AID_i$를 전송받은 서버는 $h(b, ID_i) = AID_i \oplus h(h(x \oplus y) \| T_i \| d)$를 수행한다. $h(b, ID_i)$와 같이 사용자의 $ID_i$는 난수 b와 함께 해쉬함수 처리되었으므로, 서버에 노출되지 않는다. 그러므로 제안 인증기법은 서버에 대한 사용자 익명성을 제공한다.

#### 제3자에 대한 사용자 익명성

Wang〔8〕은 로그인 요청 메시지 $\{ID_i, CID_i, N_i, T\}$를 서버에게 전송한다. 그러므로, $ID_i$가 드러나 제3자에 대한 익명성을 제공하지 못한다. Bindu〔14〕은 $\{C, T, E_R\{ID_i, r_u, T\}\}$처럼 $ID_i$를 암호화하여 전송하므로 제3자에 대한 사용자 익명성을 제공한다. 제안 인증기법은 $\{T_i, d, AID_i, C_1, C_2, D\}$를 서버에 전송하고, $AID_i$는 $h(b, ID_i) \oplus h(h(x \oplus y) \| T_i \| d)$과 같이 계산하기 때문에, $ID_i$가 곧바로 드러나지 않아, 제3자에 대한 사용자 익명성을 제공한다.

#### 내부자 공격

등록단계에서 Bindu〔10〕는 $ID_i$, $h(PW_i)$를, Hsiang〔11〕은 $ID_i$, $h(b \oplus PW_i)$를 제출한다. 두 기법 모두 사용자의 $ID_i$가 노출되어 내부자 공격에 취약할 수 있고, $h(PW_i)$는 패스워드가 변경되지 않는 한, 고정된 값이므로 전수공격 등을 통해 올바른 $PW_i$를 유추할 수 있다. $h(b \oplus PW_i)$은 Hsiang 기법에서 난수 b

를 서버에 제공하지 않지만, 전수 공격 등을 통해 유추할 수 있다. 제안 인증기법은 $h(b\oplus ID_i)$, $h(b\oplus PW_i)$ 형태로 제출한다. 그러므로 제안 인증기법은 패스워드에 대한 내부자 공격에서는 Hsiang 기법과 동일한 안전성을 제공하며, 사용자 식별자 측면에서 가장 안전하여 사용자 식별자와 패스워드 모두를 고려할 경우, 제안 인증기법이 내부자 공격에 가장 안전한 저항성을 보인다고 할 수 있다.

### 카드 분실시의 취약점

제안 인증기법은 카드 분실시 $ID_i$가 그대로 드러나는 문제와 서버의 비밀값 y가 평문형태로 저장된 취약점을 해결하기 위해, 평문형태의 $ID_i$ 대신에 $NID_i=h(b,ID_i)$를, 평문형태의 y값 대신에 $h(x\oplus y)$를 이용해 $AID_i=NID_i\oplus h(h(x\oplus y)\|T_i\|d)$ 값을 계산한다. 공격자는 사용자의 $ID_i$를 획득하기 위해, $NID_i$ 값과 동일한 $AID_i\oplus h(h(x\oplus y)\|T_i\|d)$를 유추해야한다. 그러나, x와 y는 해쉬함수 처리되어 있으므로 두 값 모두를 유추해야 하기 때문에 Khan[7]의 기법보다 추측 공격이 더 어려워진다. 또한, 카드에 저장된 정보 {L,M,N,h(),r}을 이용하여, 이들의 다양한 XOR 연산을 통해 획득할 수 있는 정보들도 곧바로 $h(x)$, $h(x\oplus ID_i)$, $h(PW_i)$ 등의 값을 획득할 수 없다. 그러므로 제안한 인증기법은 카드 분실시에도 사용자 익명성을 안전하게 제공한다고 할 수 있다.

### 패스워드 오입력시의 취약점

제안 인증기법은 [단계1]에서 기존 패스워드 오입력을 체크하고, [단계2]에서 새로운 패스워드 오입력 체크를 위해 [단계1]을 다시 실행한다. 로그인 [단계1]에서도 입력된 패스워드에 대한 오입력 여부를 체크하기 때문에, 제안 인증기법은 패스워드 변경 단계뿐만 아니라 로그인 단계에서도 패스워드 오입력시의 취약점을 해결하였다. 또한, 이러한 취약점 해결로 인해, 제안 인증기법은 원격 서버의 계산로드 증가 문제까지도 함께 해결한 비교 인증기법들 중 유일한 인증기법이다.

### 강력한 가장 공격

정당한 사용자가 공격자라고 가정할 경우, Bindu[10]은 $C\oplus h(ID_i,x)\oplus h(PW_i)\oplus r_u$를 통해, $h(x')$값을 획득가능하다. 획득한 $h(x')$을 사용해, 서버의 비밀키 x를 전수조사 공격 등을 통해 유추가능하고, $C\oplus h(x')\oplus h(PW_i)\oplus r_u$를 수행해 얻은 값 $h(ID_i,x')$를 이용해, 유추한 $x'$가 올바른 값인지 비교할 수도 있다. 제안 인증기법은 $M\oplus h(b\oplus ID_i\oplus PW_i)=h(x\oplus y)$와 $L\oplus h(b,PW_i)=h(h(x)\oplus h(ID_i))$ 연산을 통해 $h(x\oplus y)$와 $h(h(x)\oplus h(ID_i))$를 얻어낸다. $h(x\oplus y)$에서 사용자는 비밀값 x와 비밀값 y 모두 모르기 때문에, 다른 기법들에 비해 유추하기가 더 어렵다. 또한, 공격자는 $h(h(x)\oplus h(ID_i))$ 값을 통해서 $(h(x))'$ 값을 유추할 수 있고, 유추한 결과값은 x가 아니라 $h(x)$ 값이므로, $h(x)$로부터 다시 x 값을 유추해야 한다. 그러므로 제안 인증기법은 $h(x')$가 아니라 $(h(x))'$ 값을 유추하게 되어, $h(x')$ 형태보다 더 안전하다고 할 수 있다. 그러므로 정당한 사용자가 공격자라고 가정한 강력한 가장 공격에 대해, 제안 인증기법은 비교 기법들 중 가장 안전하다고 할 수 있다.

### 재전송 공격

〈표2〉와 같이 대부분의 비교 기법들과 제안 인증기법은 타임스탬프를 사용하여 재전송 공격에 대한 저항성을 가진다.

표 3 안전성 비교
Table 3. Comparison of Security Properties

| 비교 기능들 | Das[6] | Wang[8] | Bindu[10] | Hsiang[11] | Khan[7] | 제안 기법 |
|---|---|---|---|---|---|---|
| 서버에 대한 사용자 익명성 | X | X | X | X | X | O |
| 제3자에 대한 사용자 익명성 | X | X | O | O | O | O |
| 내부자 공격에 대한 저항성 | X | X | X | X | X | O |
| 강력한 가장 공격 | X | X | X | X | X | O |
| 패스워드 오입력시 체크여부 | slow | slow | slow | slow | slow | fast |
| 스마트카드 분실시의 저항성 | X | X | O | O | X | O |
| 패스워드 변경 단계 | O | O | X | O | O | O |
| 상호 인증 | X | O | O | O | O | O |
| 세션키 설정 | X | X | O | O | O | O |
| 재전송 공격에 대한 저항성 | O | O | O | O | O | O |
| 위장 공격에 대한 저항성 | O | X | O | O | O | O |

Hsiang 기법은 타임스탬프를 사용하지 않기 때문에, 첫 단계에서 재전송 공격을 차단할 수는 없으나, 원격 서버의 계산로드를 증가시킬 수 있다.

서버·사용자 위장 공격

공격자는 전송 메시지 $\{T_i, d, AID_i, C_1, C_2, D\}$, $\{T_s, h(T_s \| E)\}$로부터 서버의 비밀키 x, 비밀값 y, $ID_i$와 $PW_i$ 획득시도를 할 것이다. $C_1$이나 $C_2$로부터 $h(x \oplus y) \oplus NID_i \oplus h(h(x) \oplus h(ID_i))$을 계산하여, 중요 정보를 획득하기 위해서는 $h(x \oplus y)$나 $h(h(x) \oplus h(ID_i))$, 또는 $NID_i = h(b \oplus ID_i)$에 대한 일방향 해쉬함수를 깨야하며, $NID_i$는 난수 b에 의해 계속 전체 값이 변할 경우 유추하기가 쉽지 않다. 그러므로 제안 인증기법은 사용자·서버 가장 공격에 안전하다고 할 수 있다.

### 5.2 효율성 분석

계산의 효율성 측면에서 각 인증기법들을 비교·분석한 결과는 〈표3〉과 같다. 제안 인증기법은 8H~10H의 연산을 수행하는 비교 인증기법들에 비해 더 많은 14H의 연산을 수행한다. Bindu[10]은 5H+6S+2E의 연산이 필요하여 2번의 멱승 연산(2E)을 수행한다. 횟수로는 2번인 멱승 연산이지만 멱승 연산이 계산 소비적인 연산이기 때문에, 제안 인증기법보다 더 많은 계산시간이 걸릴 수 있다. 또한, S와 H가 동일한 수행시간을 가진다고 가정할 경우에도, 전체 11H+2E이기 때문에 14H의 연산이 필요한 제안 인증기법보다 더 많은 시간이 걸릴 것이다. 결과적으로 계산 효율성 측면과 제공하는 기능, 그리고 안전성 측면을 전체적으로 고려할 경우, 제안 인증기법은 14H의 해쉬연산을 수행함으로써 패스워드 오입력의 취약점과 서버에 대한 사용자 익명성 제공, 그리고 내부자 공격에 대한 저항성을 제공하여, 가장 안정적이고 효율적인 인증기법이라고 할 수 있다. 더욱이, 제안 인증기법은 스마트카드를 분실할 경우와 정당한 사용자가 공격자라고 가정한 강력한 가장 공격에서도 가장 안전한 비도(security level)를 제공하였다.

## VI. 결 론

본 논문에서는 최근에 제안된 사용자 익명성 제공 인증기법 중 Khan 인증기법의 새로운 취약점을 분석하고, 서버에 대한 사용자 익명성과 내부자 공격에 대한 저항성을 가지는 인증기법을 제안하였다. 제안 인증기법에서는 비밀정보가 카드에 그대로 노출되는 Khan의 취약점을 개선하였으며, 특히 정당한 사용자가 공격자일 경우를 가정한 강력한 가장 공격에 대해서도 가장 높은 안전도를 제공하였다. 또한, 제안 인증기법은 패스워드 변경 단계를 제시하고 있음에도 불구하고 여전히 패스워드 오입력의 취약점이 존재하는 많은 인증기법들의 문제도 해결하였고, 이러한 문제 해결로 원격 서버의 계산로드 증가문제도 함께 해결하였다.

## 참고문헌

[1] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol.24, pp.770-772, November 1981.

[2] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," IEEE Proceedings-Computers and Digital Techniques, Vol.38, No.3, pp.165-168, May 1991.

[3] H. S. Kim, S. W. Lee, and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating

표 4. 계산 효율성의 비교
Table 4. Comparison of Computation Costs

| 비교 항목 | Das[6] | Wang[8] | Bindu[10] | Hsiang[11] | Khan[7] | 제안 기법 |
|---|---|---|---|---|---|---|
| 등록 단계의 연산 | 2H | 2H | 3H | 6H | 2H | 5H |
| 로그인단계의 연산 | 5H | 2H | 1H+1S+1E | 7H | 3H | 5H |
| 인증 단계의 연산 | 3H | 4H | 1H+5S+1E | 20H | 5H | 4H |
| 총 연산횟수 | 10H | 8H | 5H+6S+2E | 33H | 10H | 14H |
| 지수계산 필요여부 | X | X | O | X | X | X |
| 암호화 방식 | 해쉬함수 | 해쉬함수 | 해쉬함수,대칭키암호 | 해쉬함수,멀티서버환경 | 해쉬함수 | 해쉬함수 |
| H:Secure one-way hash operation, S:Symmetric key cryptosystem, E:Exponential operation | | | | | | |

Systems Review, Vol.37, No.4, pp.32-41, October 2003.
[4] C. L. Hsu, "Security of Chien et al's remote user authentication scheme using smart cards," Computer Standards and Interfaces 26, pp.167-169, May 2004.
[5] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Efficient Remote User Authentication Scheme base on Generalized ElGamal Signature Scheme," IEEE Transactions on Consumer Electronics, Vol.50, No.2, pp.568-570, May 2004.
[6] 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, May 2004.
[7] M. K. Khan, S. K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme," Computer Communications, Vol.34, Issue.3, pp.305-309, March 2011.
[8] Y. Y. Wang, J. Y. Liu, F. X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme,"Computer Communications 32, pp.583 - 585, March 2009.
[9] R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards : A review," Journal of Network and Computer Applications 35, pp.1235-1248, July 2012.
[10] 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.
[11] H. C. Hsiang and W. K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standard and Interfaces 31, pp.1118-1123, November 2009.

## 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