# 사용자 익명성을 제공하는 추적 가능한 인증 프로토콜

## Traceable Authentication Scheme Providing User Anonymity

최종석, 신승수
동명대학교 정보보호학과

Jong-Seok Choi(bestofcom@gmail.com), Seung-Soo Shin(shinss@tu.ac.kr)

**요약**

최근에는 개인 프라이버시 보호에 대한 관심이 증가하면서 사용자 익명성을 제공하는 스마트카드 기반 인증 프로토콜에 대한 연구가 활발하게 진행되고 있다. 원격시스템 인증프로토콜에서 사용자 익명성을 제공하기 위한 스마트카드 기반 인증 프로토콜을 Das 등이 처음 제안하였지만, Das 등의 프로토콜은 사용자 익명성을 제공하지 못한다는 문제점이 제기되고, Chien 등은 이러한 문제점을 해결하기 위한 새로운 프로토콜을 제안하였다. 사용자 익명성이 제공되면서 악의적인 사용자를 감지하는 것이 어려워지고, 이러한 문제점을 해결하기 위해 Kim 등은 추적 가능한 인증 프로토콜을 제안하였다. 본 논문에서는 Kim 프로토콜의 사용자 익명성과 내부자공격에 대한 문제점을 제기하고, 이러한 문제점을 해결하기 위한 새로운 프로토콜을 제안하고, 제안한 프로토콜의 안전성 및 효율성을 비교분석한다. 제안한 프로토콜은 사용자 익명성을 제공하면서 추적 가능한 인증프로토콜로 Kim 프로토콜에 비해 안전성 측면에서 더 효율적이다.

■ 중심어 : | 개인정보 | 스마트카드 | 사용자 익명성 | 추적성 |

**Abstract**

Recently, remote user authentication scheme protecting user anonymity using smart card has been researched with interest increasing on user privacy. Although authentication scheme providing user anonymity using smart card had been proposed by Das et al, Chien et al. pointed out Das et al. scheme fail to provide user anonymity and proposed new scheme to overcome the problem. A remote system Kim et al. proposed a scheme which is traceable about malicious user with protecting user anonymity. In this paper, we point out that Kim et al. scheme fail to provide user anonymity and propose a scheme for some problems Kim et al. scheme has. And then we analysis our scheme on cryptophic security and efficiency with Kim scheme.

■ keyword : | Privacy | Smart Card | User Anonymity | Traceability |

## I. 서 론

최근 통신기술의 발달과 네트워크 사용의 증가로 인해 분산된 컴퓨팅 환경에서 원격 서버에 대한 접속이 증가하고 있다. 이러한 원격 시스템을 사용하고자 할 때, 대부분의 정보는 네트워크를 통해 전달되기 때문에 도청이나 불법적인 수정, 의도된 변경 등과 같은 문제점에 노출되어 사용자 프라이버시 침해의 원인이 된다. 따라서 원격 서버는 사용자의 신원을 인증해야 한다. 이러한 문제점을 해결하기 위해 안전한 인증 기법들에

접수번호 : #090202-009
접수일자 : 2009년 02월 02일
심사완료일 : 2009년 03월 23일
교신저자 : 신승수, e-mail : shinss@tu.ac.kr

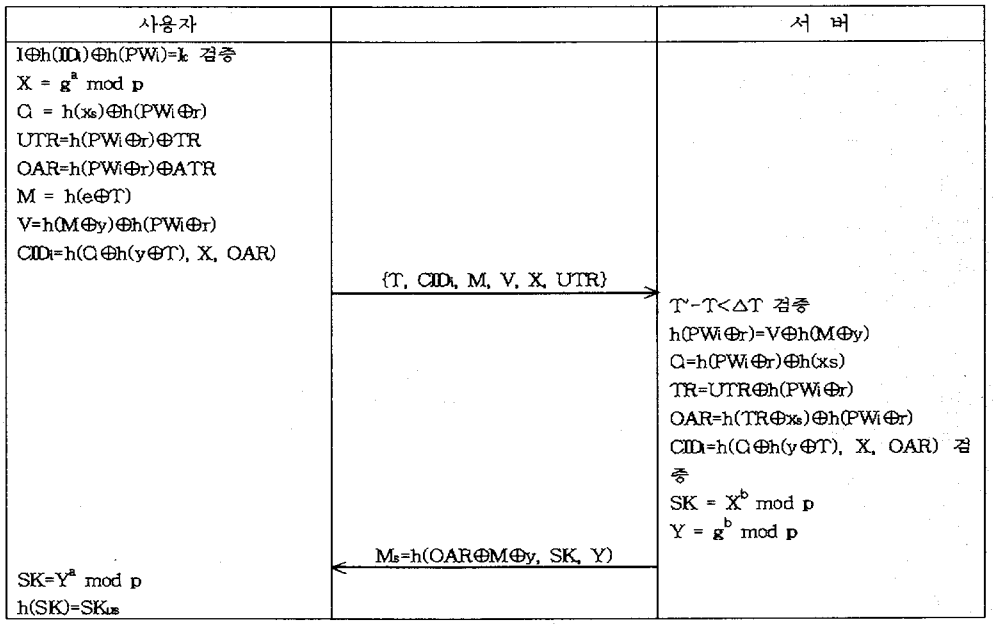


**그림 1. Kim 등의 프로토콜**

대한 연구가 활발히 진행되고 있고, 그 중에서 스마트카드가 가진 이동성과 기능적 보안성 때문에 특히 스마트카드 기반 인증 프로토콜이 주목 받고 있다.

초기 스마트카드 기반 원격 사용자 인증 기법은 검증테이블을 사용하였지만[1], 사용자 아이디와 패스워드 관리 비용부담을 줄이기 위해 검증테이블을 사용하지 않는 인증기법들이 제안되고 있다. 최근에는 개인 프라이버시 보호에 대한 관심이 높아지면서 스마트카드 기반 원격 사용자 인증 시 사용자 익명성을 제공하기 위한 기법들이 제안 되고 있다.

2004년 Das 등[2]은 동적 아이디를 사용하여 사용자와 원격 서버를 제외한 제3자에게 대해 익명성을 보장하는 기법을 최초로 제안하였다. Das 등의 프로토콜이 사용자 익명성을 제공하지 못하는 문제점을 제기하고, 사용자 익명성을 제공하면서 키 교환이 가능한 사용자 인증 프로토콜을 2005년 Chien 등[3]이 제안하였다. Chien 등의 프로토콜이 가장 공격과 재전송공격 등과 같은 문제점에 대해 취약함이 밝혀졌고 이러한 문제점을 해결하기 위한 프로토콜을 2007년에 Hu 등[4]이 제안하였다. 2008년에는 Bindu 등[5]이 Chien 등의 프로토콜을 가장 공격과 내부자 공격에 대해 분석하고, 이 문제점을 해결하기 위한 프로토콜을 제안하였다.

최근 기업 내부자에 의해 사용자의 정보가 유출되는 사고가 증가하면서, 이러한 유출을 막기 위한 정보보호 기술의 개발이 요구되고 있다. 이러한 요구에 따라 2006년 Chai 등[6]은 원격 서버에 대해서도 사용자 익명성을 보장하는 프로토콜을 처음 제안하였다. Chai 등의 프로토콜이 한명의 사용자 인증을 위해 사용자 수만큼의 연산량과 통신량을 필요한 부담을 해결하면서, 원격 서버에 대한 사용자 익명성을 제공할 뿐만 아니라 악의적인 사용자에 대해 추적이 가능한 프로토콜을 2008년에 Kim 등[7]이 제안하였으나, Kim 등의 프로토콜은 정당한 사용자인 공격자에 대해 사용자 익명성을 보장하지 못한다는 문제점이 있다. 따라서 본 논문에서는 정당한 사용자인 공격자에 대해서도 사용자 익명성을 보장하면서, Kim 등의 프로토콜과 같이 추적 가능한 스마트카드 기반 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구로 Kim 등의 프로토콜을 살펴보고 3장에서 Kim 프로토콜을 분석한다. 4장에서 Kim 프로토콜의 문제점을 보완

한 새로운 프로토콜을 제안하고, 5장에서는 제안한 프로토콜을 분석한다. 6장에서는 Kim 등의 프로토콜과 제안한 프로토콜을 성능적인 측면과 기능적인 측면에서 비교·분석한 후 마지막 7장에서 결론을 맺는다.

## II. 관련연구

Kim 등의 프로토콜[7]에 대하여 살펴본다. Kim 등의 프로토콜은 등록단계, 로그인단계, 인증단계, 추적단계, 패스워드변경단계로 이루어진다.

<등록 단계>

Step 1. 등록단계에서는 새로운 사용자 $U_i$ 가 안전한 채널을 통해 서버 에게 자신의 $ID_i$와 $PW_i$ 를 제출한다.

Step 2. S는 다음과 같은 계산을 수행한다.

(1) $R_i = h(ID_i \oplus x_s) \oplus h(x) \oplus h(PW_i)$

(2) $I = h(ID_i \oplus x_s)$

(3) $I_c = h(ID_i \oplus x_s) \oplus h(ID_i) \oplus h(PW_i)$

(4) $TR = E_{PTR}[ID_i, UIN_i]$

(5) $ATR = h(TR \oplus x_s)$

Step 3 S는 U의 스마트카드에 {I, $I_c$, $R_i$, h(.), TR, p, y, ATR}를 저장하여 발급한다.

<로그인 단계>

Step 1. Ui가 원격서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입하고 $ID_i$, $PW_i$를 입력한다.

Step 2. 사용자의 $ID_i$, $PW_i$를 확인한다.

Step 3. U는 [그림 1]과 같이 계산된 메시지 {T, $CID_i$, M, V, X, UTR}를 S에게 보낸다.

<인증 단계>

Step 1. S는 U의 메시지 {T, $CID_i$, M, V, X, UTR}를 T′시간에 받는다.

Step 2. $CID_i$를 검증한다.

Step 3. S는 $U_i$에게 메시지 $M_s$를 계산하여 Y와 함께 보낸다.

$$M_s = h(OAR \oplus M \oplus y, SK, Y)$$

Step 5. $U_i$는 메시지 $M_s$와 Y를 받고 다음과 같은 수행을 하고 식을 확인해서 일치하는지 확인한다.

(1) $SK = Y^a \bmod p$

(2) $M_s = h(OAR \oplus M \oplus y, SK, Y)$

Step 6. $M_s$ 값이 일치한다면 $U_i$와 S는 SK를 이용해 다음과 같이 세션 키를 맺는다.

$$h(SK) = SK_{us}$$

<추적단계>

Step 1. S는 TR값과 CS을 함께 신뢰기관에 제출한다.

Step 2. 신뢰기관은 CS를 확인하고 TR값을 자신의 개인키로 복호화하여 서버에 사용자 정보를 알려준다.

## III. 관련연구 분석

이 장에서는 관련연구의 안전성을 분석한다. Kim 프로토콜[7]은 위장공격, 재전송공격, 은밀한 검증자 공격, 전방향 안전성 대해 효율적이다. 본 논문에서는 Kim 프로토콜이 취약한 사용자 익명성과 내부자공격에 대해 분석한다.

### 1. 사용자 익명성

사용자 익명성은 서버와 제3자에 대하여 각각 분석할 수 있다. 기존의 프로토콜은 서버가 악의적인 의도를 가지고 사용자의 개인정보를 알아내기 위하여 CS를 조작하여 신뢰기관에 제출하면 모든 사용자의 개인정보를 언제든지 얻을 수 있다. 따라서 기존의 프로토콜은 서버에 대한 사용자 익명성을 보장하지 못한다. 그러나 서버는 신뢰할 수 있는 기관이라고 한다면 서버에 대한 사용자 익명성의 보장은 보안에 큰 위협을 주지 않는다. 기존의 프로토콜에서는 서버가 사용자를 추적하기 위해서 TR을 이용한다. 만약 공격자가 사용자의 TR을 얻어내어, 서버로 가장하여 조작한 CS와 함께 신뢰기관에 제출한다면, 공격자는 신뢰기관으로부터

사용자의 ID와 개인정보를 얻어낼 수 있다. 만약 공격자가 사용자와 동일한 서버에 등록된 정당한 사용자라면 다음과 같은 계산을 통해서 사용자의 TR값을 얻을 수 있다.

1. 공격자는 사용자의 {T, $CID_i$, M, V, X, UTR}를 가로챈다.
2. 공격자의 스마트카드에 저장된 서버의 비밀값 y를 이용하여 $h(PW_i \oplus r) = V \oplus h(M \oplus y)$를 계산한다.
3. 공격자는 $TR = UTR \oplus h(PW_i \oplus r)$을 계산한다.

위와 같이 계산하여 공격자는 {TR, CS}를 신뢰기관에 제출하면, 신뢰기관으로부터 사용자의 ID와 개인정보를 얻는다. 따라서 기존의 프로토콜은 제3자에 대한 사용자 익명성을 보장하지 못한다.

### 2. 내부자 공격

만약 서버의 내부자가 악의적인 의도를 가졌다면, 서버의 내부자는 등록단계에서 사용자의 ID, PW를 얻을 수 있다. 일반적으로 사용자들은 자신의 편의성을 위해 다른 서버에서도 동일한 ID, PW를 이용하는 경우가 많으며, 서버의 내부자는 등록단계에서 얻은 ID, PW를 이용하여 다른 서버에서 사용자의 ID, PW를 입력하고 로그인하여, 사용자를 위장할 수 있다.

## IV. 제안 프로토콜

Kim 등의 프로토콜의 기능을 모두 만족하면서 사용자 익명성을 보장하고 내부자 공격을 해결할 수 있는 프로토콜을 제안한다. 제안한 프로토콜은 등록단계, 로그인단계, 인증단계, 추적단계, 패스워드변경단계로 나누어진다.

<등록 단계>

Step 1. $U_i$ 가 안전한 채널을 통해 S에게 $ID_i$와 $h(PW_i)$ 를 제출한다.

Step 2. S는 다음과 같은 계산을 수행한다.

(1) $R_i = h(x) \oplus h(PW_i) \oplus h(h(ID_i) \oplus x_s)$

(2) $I = h(ID_i \oplus x_s)$

(3) $I_c = h(ID_i \oplus x_s) \oplus h(ID_i) \oplus h(PW_i)$

(4) $TR = E_{PTR}[ID_i, UIN_i]$

(5) $ATR = h(TR \oplus x_s)$

Step 3 S는 U의 스마트카드에 {I, $I_c$, $R_i$, h(.), TR, p, y, ATR}를 저장하여 발급한다.

기존의 프로토콜은 $h(ID_i \oplus x_s)$를 사용하여 $R_i$를 계산하였지만, 제안한 프로토콜에서는 사용자 익명성을 제공하기 위해 $h(h(ID_i) \oplus x_s)$를 사용하여 $R_i$를 계산하고, 스마트 카드에 저장되는 정보는 {I, $I_c$, $R_i$, h(.), TR, p, y, ATR}으로 Kim 등의 프로토콜과 동일하다.

<로그인 단계>

Step 1. $U_i$가 원격서버에 로그인을 원할 때, 자신의 스마트카드를 리더기에 삽입하고 $ID_i$, $PW_i$를 입력한다.

Step 2. 스마트카드가 다음과 같은 수행을 한다.

(1) 사용자의 $ID_i$, $PW_i$를 확인한다.
$I \oplus h(ID_i) \oplus h(PW_i) = I_c$

(2) $X = g^a \bmod p$

(3) $Ci = h(x_s) \oplus h(h(ID_i) \oplus x_s)$

(4) $UTR = h(h(ID_i) \oplus x_s) \oplus TR$

(5) $OAR = h(h(ID_i) \oplus x_s) \oplus ATR$

(6) $M = h(e \oplus T)$

(7) $V = h(M \oplus y) \oplus h(ID_i)$

(8) $CID_i = h(C_i \oplus h(y \oplus T), X, OAR)$

Step 3. 인증을 위해 S에게 메시지 {T, $CID_i$, M, V, X, UTR}을 보낸다.

Kim 프로토콜에서는 V를 계산하기 위해 M과 h(PW⊕r)을 사용하고, 공격자는 간단히 h(PW⊕r)을 얻어 TR을 계산할 수 있었다. 제안한 프로토콜에서는 이러한 문제점을 해결하기 위해 V를 계산하기 위해 h(ID)를 사용하고, TR을 계산하기 위해 h(h(ID)⊕x)를 사용하기 때문에 공격자가 서버의 비밀키 x를 알지 못한다면 TR을 계산할 수 없다.

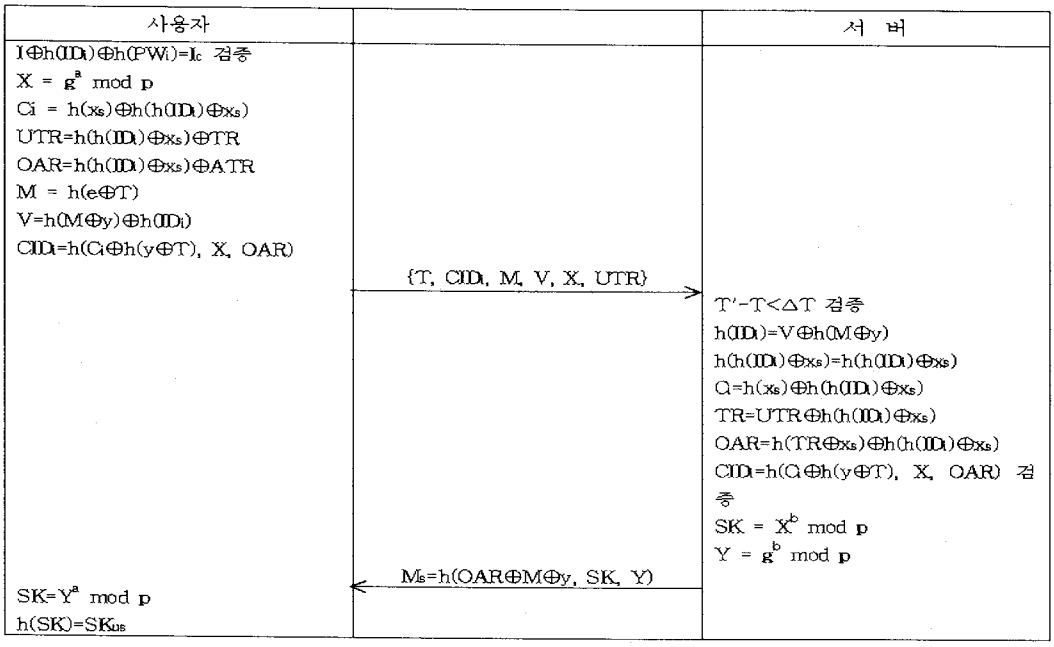


**그림 2. 제안한 프로토콜**

<인증 단계>

Step 1. S는 메시지 {T, $CID_i$, M, V, X, UTR}를 T'시간에 받는다.

Step 2. S는 다음과 같은 수행을 한다.

(1) T와 T'사이의 시간간격(time interval)을 확인한다.

(2) S는 다음 계산을 통해 $CID_i$를 검증하는데 필요한 값을 얻어낸다.

i) $h(ID_i) = V \oplus h(M \oplus y)$

ii) $C_i = h(x_s) \oplus h(h(ID_i) \oplus x_s)$

iii) $TR = UTR \oplus h(h(ID_i) \oplus x_s)$

iv) $OAR = h(TR \oplus x_s) \oplus h(h(ID_i) \oplus x_s)$

(3) 다음 식이 성립하는지 확인한다.

$CID_i = h(C_i \oplus h(y \oplus T), X, OAR)$

Step 3. 만약 $CID_i$와 식이 일치하면 S는 다음과 같은 수행을 한다.

(1) $SK = X^b \bmod p$

(2) $Y = g^b \bmod p$

Step 4. S는 $U_i$에게 메시지 $M_s$를 계산하여 Y와 함께 보낸다.

$M_s = h(OAR \oplus M \oplus y, SK, Y), Y$

Step 5. $U_i$는 메시지 $M_s$와 Y를 받고 다음과 같은 수행을 하고 식을 확인해서 일치하는지 확인한다.

(1) $SK = Y^a \bmod p$

(2) $M_s = h(OAR \oplus M \oplus y, SK, Y)$

Step 6. $M_s$ 값이 일치 한다면 $U_i$와 S는 SK를 이용해 다음과 같이 세션 키를 맺는다.

$h(SK) = SK_{us}$

Kim 프로토콜에서는 V, Ci, TR이 $h(PW \oplus r)$에 의해서 계산되기 때문에 공격자는 V, Ci, TR값을 모두 계산할 수 있다. 제안한 프로토콜에서는 V는 h(ID)로 계산되며, Ci, TR은 $h(h(ID) \oplus x)$를 이용하여 계산된다. 따라서 공격자는 서버의 비밀키 x를 알 수 없기 때문에 Ci, TR을 계산할 수 없다.

<추적단계>

Step 1. S는 인증 2.3단계와 같이 계산된 TR과 CS을 함께 신뢰기관에 제출한다.

Step 2. 신뢰기관은 CS를 확인하고 TR값을 자신의 개인키로 복호화하여 서버에 사용자 정보를 알려준다.

<사용자의 패스워드 변경>

$U_i$가 자신의 $PW_i$를 새로운 $PW_i^*$로 바꾸고자 할 때, $U_i$는 서버와 상관없이 스마트카드만을 이용하여 새로운 $PW_i^*$로 교체 할 수 있다. 스마트카드는 다음과 같은 수행을 한다.

Step 1. $U_i$는 자신의 스마트카드를 리더기에 삽입 후, 자신의 $ID_i$와 $PW_i$를 입력한다.

Step 2. 스마트카드는 다음을 확인한다.

(1) $I \oplus h(ID_i) \oplus h(PW_i) = I_c$

Step 3. 만약 값이 일치하면 스마트카드는 다음과 같은 수행을 하여 $PW_i$를 교체한다.

(1) $I_c \oplus h(PW_i) \oplus h(PW_i^*) = I_c^*$

(2) $R_i \oplus h(PW_i) \oplus h(PW_i^*) = R_i^*$

Step 4. 스마트카드는 새롭게 생성된 $I_c^*$와 $R_i^*$값을 저장한다.

## V. 제안 프로토콜 안전성 분석

본 논문에서 제안한 프로토콜을 위장공격, 내부자 공격, 재전송 공격, 은밀한 검증자 공격, 사용자 익명성, 전방향 안전성에 대해서 분석하였다.

• 위장공격

공격자는 사용자의 메시지 {T, $CID_i$, M, V, X, UTR}를 가로 챌 수 있다. 이 때 공격자가 사용자와 동일한 서버에 등록된 정당한 사용자라면, 자신의 스마트카드의 y를 사용하여 $h(ID)=V \oplus h(M \oplus y)$를 알 수 있다. 그러나 공격자는 서버의 비밀키 $x_s$를 모르기 때문에 $h(h(ID) \oplus x_s)$를 만들어 낼 수 없으므로, UTR과 $CID_i$를 조작할 수 없다. 따라서 공격자는 사용자로 위장할 수 없다. 서버측면에서도 공격자는 자신의 스마트카드의 y를 사용하여 $h(ID)=V \oplus h(M \oplus y)$를 알 수 있다. 그러나 공격자는 서버의 비밀키 $x_s$를 모르기 때문에 $h(h(ID) \oplus x_s)$를 만들어 낼 수 없으므로, 다른 정보 $C_i$, TR, OAR, $CID_i$를 알 수 없기 때문에 서버의 메시지 $M_s$를 만들어 낼 수 없다. 따라서 공격자는 서버로 위장할 수 없으며, 서버/사용자 위장공격으로부터 안전하다.

• 내부자 공격

만약 서버의 내부자가 악의적인 의도를 가졌다고 가정했을 때, Kim 등의 프로토콜에서는 등록단계에서 사용자의 ID, PW를 모두 노출하지만, 제안한 프로토콜에서는 사용자가 서버에게 h(PW)를 전달한다. 암호학적 해시함수의 일방향성 때문에 서버의 내부자라 할지라도 사용자의 패스워드를 추측 또는 알 수 없다.

• 재전송공격

제안한 프로토콜에서는 타임스탬프를 이용하여 메시지의 유효성을 검사하고 있다. 만약 공격자가 사용자의 메시지를 저장하고, 재전송할 경우 그 메시지는 인증 2.1단계에서 T에 대한 검증을 통과 할 수 없다. 공격자가 다른 정보는 변경하지 않고 T만 변경 할 경우 인증 단계에서 2.1을 통과 할 수 있지만, T가 $CID_i$를 생성할 때 사용되기 때문에 $CID_i$에 대한 검증을 통과 할 수 없으며, 공격자는 $CID_i$를 조작할 수 없다.

• 은밀한 검증자 공격

서버에는 비밀값 y, 비밀키 $x_s$를 저장하지만, 검증 테이블을 따로 저장하지 않는다. 그러므로 제안한 프로토콜은 은밀한 검증자 공격에 대해 안전하다.

• 사용자 익명성

제안한 프로토콜에서 제3자는 h(ID)를 얻을 수 있지만, 암호학적 해시함수의 일방향성 때문에 h(ID)로부터 ID를 추측 또는 알아내는 것은 어렵다. 또한 공격자는 사용자의 TR을 알 수 없기 때문에 TR을 이용하여 다른 사용자의 개인정보를 얻을 수 없다.

• 전방향 안전성

공격자가 사용자의 개인키나 패스워드를 알아냈다 하더라도 이전에 사용자가 사용했던 어떠한 세션키도

알 수 없을 경우, 프로토콜이 전방향 안전성을 만족한다고 한다. 제안한 프로토콜에서는 사용자의 패스워드의 관한 정보를 전송하지 않으며, Diffie-Hellman 키 교환 프로토콜[8]에 기반하여 전방향 안전성을 만족한다.

## VI. 성능성 및 기능성 비교분석

이 장에서는 제안한 프로토콜과 Kim 등의 프로토콜을 성능적인 측면과 기능적인 측면에서 비교 분석한다.

### 1. 성능성 분석

Kim 프로토콜은 로그인단계에서 해시연산 6회, 지수연산 1회가 필요하고, 인증단계에서 해시연산 4회, 지수연산 2회가 사용되었으며, 제안한 프로토콜에서는 로그인단계에서 해시연산 6회, 지수연산 1회로 Kim 프로토콜과 동일한 연산이 사용되고, 인증단계에서 해시연산 5회, 지수연산 2회로 Kim 프로토콜에 비해 해시연산이 1회 추가되었다. 그러나 해시함수의 10만 번 연산시 0.1 ~ 0.2초 정도의 시간[9]이 필요하므로, 현대 컴퓨팅 기술에서는 연산속도에 거의 영향을 미치지 않는다. 따라서 Kim 프로토콜과 제안한 프로토콜의 연산속도는 거의 동일하다.

**표 1. 효율성 분석**

| 프로토콜 | L.P. | A.P. | P.C. | T.P. |
|---|---|---|---|---|
| 제안한 프로토콜 | 6H, 1P | 5H, 2P | 3H | 5H |
| Kim 프로토콜 | 6H, 1P | 4H, 2P | 3H | 5H |

H : 해시 연산, P : 지수 연산, L.P. : 로그인단계
A.P. : 인증단계 P.C : 패스워드변경단계 T.P. : 추적단계

### 2. 기능성 분석

기능적인 측면에서는 Kim 프로토콜과 제안한 프로토콜을 내부자 공격, 사용자 익명성, 추적가능성, 상호인증, 빠른 패스워드 감지, 키교환, 패스워드 변경 및 자유에 대해 분석한다. 내부자 공격은 정당한 내부자로 인한 공격이다. Kim 프로토콜은 등록단계에서 서버에 PW를 제출한다. 이 때 만약 서버의 내부자가 악의적인 의도를 가지고 있다면 사용자의 PW를 알 수 있다. 그리고 일반적인 사용자는 편의성을 위해 여러 서버에 같은 ID, PW를 사용하는 경우가 많으며, 이러한 취약점을 이용해 서버의 내부자는 다른 서버에서 정당한 사용자를 위장할 수 있다. 따라서 제안한 프로토콜에서는 h(PW)를 제출하고, 암호학적으로 안전한 해시함수라면 서버의 내부자는 사용자의 PW를 알 수 없다. 제안한 프로토콜에서는 h(ID)의 정보만 노출하며, 공격자는 그 정보로부터 TR을 알 수 없으므로 제안한 프로토콜은 사용자 익명성을 보장한다. 따라서 제안한 프로토콜은 Kim 프로토콜의 내부자공격과 사용자 익명성에 대한 취약성을 보완하였다.

## VII. 결 론

스마트카드 기반 프로토콜은 외부 또는 내부의 원격 서버에 로그인 할 때, 키 교환을 수행하여 암호통신을 하기위해 사용될 수 있다. 최근에는 개인프라이버시에 대한 관심이 높아지면서, 사용자 익명성을 제공하는 프로토콜에 대한 관심이 높아지고 있다. 사용자 익명성을 제공하는 프로토콜은 ID를 노출하지 않고 암호통신을 할 수 있지만, 사용자가 악의적인 행동을 했을 때 악의적인 사용자를 판별하기 힘들다는 문제점이 있다. 이러한 문제점을 해결하기 위해 Kim 등은 서버의 요청에 따라 사용자에 대한 정보를 얻을 수 있는 추적 가능한 프로토콜을 제안하였다.

**표 2. 기능성 분석**

| 프로토콜 | 내부자 공격 | 익명성 | 추적 가능성 | 상호인증 | FWP | 키교환 | 패스워드 | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | 변경 | 자유 |
| 제안한 프로토콜 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Kim 프로토콜 | × | △ | ○ | ○ | ○ | ○ | ○ | ○ |

○: 해당 문제점에 대해 강함
△ : 강하다고 했지만 실제로는 취약함
× : 취약함

FWP : 빠른 패스워드 감지

본 논문에서는 Kim 등의 프로토콜을 사용자 익명성과 내부자공격에 대해 분석하였고, 로그인단계에서 서버에 등록된 공격자에게 ID를 노출하게 되고, 등록단계에서 서버의 내부자에게 ID, PW를 노출하게 되는 문제점을 지적하고, 이러한 문제점을 해결하기 위한 새로운 프로토콜을 제안하였다. 본 논문에서 제안한 프로토콜은 추적단계와 같은 Kim 등의 프로토콜의 기능을 모두 갖추면서 사용자 익명성을 제공한다. 서버에게도 사용자 익명성을 보장하지만, 서버는 악의적인 사용자에 대하여 신뢰기관의 도움을 받아 사용자의 ID, 개인정보 등을 알 수 있다. 따라서 제안한 프로토콜은 사용자의 아이디를 노출하지 않기 때문에 원격서버접속과 같은 사용자 익명성을 보호하기 위한 다양한 응용분야에서 효율적으로 사용할 수 있을 것이다.

## 참 고 문 헌


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

[2] L. D. Manik, S. Ashutosh, P. G. Ved, *"A Daunamic ID-based Remote User Authentication Scheme,"* IEEE Trans. on Consumer Electronics, Vol.50, No.2, pp.629-631, 2004.

[3] H. Y. Chien and C. H. Chen, *"A remote authentication scheme preserving user,"* IEEE AINA'05, Vol.2, pp.245-248, 2005.

[4] H. Lanlan, Y. Yixian, N. Xinxin, *"Improved Remote User Authentication Scheme Preserving User Anonymity,"* IEEE CNSR'07, pp.323-328, 2007.

[5] 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).

[6] Z. Chai, Z. Cao, and R. Lu, *"Efficient Password-Based Authentication and Key Exchange Scheme Preserving User Privacy,"* WASA'06, LNCS 4138, pp.467-477, 2006.

[7] 김세일, 천지영, 이동훈, "추적이 가능한 스마트카드 사용자 인증 기법", 한국정보보호학회, 제18권, 제5호, pp.31-39, 2008(10).

[8] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans, Vol.IT-22, No.6, pp.644-654, 1976.

[9] http://python.kr/viewtopic.php?p=58975&sid=cca60d3798d59c304d8db74e23af340e


## 저 자 소 개


**최 종 석(Jong-Seok Choi)** 준회원

- 2004년 3월 ~ 현재 : 동명대학교 정보보호학과 학생

<관심분야> : 암호프로토콜, USN

**신 승 수(Seung-Soo Shin)** 종신회원

- 1988년 2월 : 충북대학교 수학과 (이학사)
- 1993년 2월 : 충북대학교 수학과 (이학석사)
- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야> : 암호프로토콜, 무선 PKI, 네트워크 보안, USN