KIPS Tr. Comp. and Comm. Sys.
Vol.2, No.12 pp.517~524 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.12.517

Zero-knowledge Based User Remote Authentication Over Elliptic Curve

Jongseok Choi† · Howon Kim††

ABSTRACT

Although password-based authentication as known as knowledge-based authentication was commonly used but intrinsic problems such as dictionary attack remain unsolved. For that the study on possession-based authentication was required. User remote authentication using smartcard is proceeding actively since Lee et al. proposed user remote authentication using knowledge-based information(password) and possession-base information(smartcard) in 2002. in 2009, Xu et al. proposed a new protocol preserving user anonymity and Shin et al. proposed enhanced scheme with analysis of its vulnerabilities on user anonymity and masquerading attack in 2012. In this paper, we analyze Shin et al. scheme on forward secrecy and insider attack and present novel user authentication based on elliptic curve cryptosystem which is secure against forward secrecy, insider attack, user anonymity and masquerading attack.

Keywords : ECC(Elliptic Curve Cryptography), Smart Card, Authentication, Forward Secrecy, Anonymity

타원곡선상의 영지식기반 사용자 원격인증 프로토콜

최 종 석† · 김 호 원††

요 약

지식기반의 패스워드 인증방식이 대중적으로 사용되었으나, 사전공격과 같은 근본적인 문제를 해결하지 못한다. 이에따라 소유기반의 인증기술에 대한 연구가 필요해졌다. 2002년 Lee et al.은 지식기반정보(패스워드)와 소유기반정보(smartcard)를 이용한 사용자 원격 인증기법을 제안하였으며, 그 이후로 스마트카드를 이용한 원격 인증기법에 대한 연구가 활발하게 진행되었다. 2009년 Xu et al.은 사용자 익명성을 보장하는 프로토콜을 제안하였으나, 2012년 Shin et al.은 Xu et al. 기법의 사용자익명성 노출, 위장공격에 대한 취약점을 분석하고 이를 개선한 사용자 익명성을 보장하는 프로토콜을 제안하였다. 본 논문에서는 Shin et al. 기법을 전방향안전성과 내부자공격에 대한 취약점을 분석하고 전방향안전성, 내부자공격, 사용자익명성, 위장공격에 안전한 타원곡선암호기반의 사용자 인증 프로토콜을 제안한다.

키워드 : 타원곡선암호, 스마트카드, 인증, 전방향 안전성, 익명

1. 서 론

1981년 Lamport[1] 가 패스워드 인증 기법을 제안한 이후로 패스워드기반 인증기법은 제어시스템, 온라인 뱅킹, 전자지불시스템, 컴퓨터 네트워크와 같은 다양한 분야에 폭넓게 적용되어왔다. 정적 패스워드의 취약점을 보완하기 위해서 1994년 Haller는 S/Key OTP[2] 기법을 제안하였다. S/Key OTP 방식은 최근까지도 OTP 인증 방법에서 널리 사용되고 있었지만, 2012년 Choi et al.[3]에 의해서 S/Key OTP 해쉬충돌쌍 문제가 지적되었다. 이 두 기법은 사용자 인증을 수행하기 위해서 검증테이블을 유지해야 하는데, 2002년 Chen et al.[4]은 Lamport 기법과 Haller 기법에 대한 검증테이블 취약점을 지적하였다. 2002년 Lee et al.[5]은 이 문제를 해결하기 위해 스마트카드를 이용한 원격 사용자 인증 기법을 제안하였다.

검증테이블 노출문제와 동시에 개인정보 프라이버시 노출문제에 대한 관심이 높아지면서 사용자 익명성에 대한 관심도 높아졌다. 이에 따라 2004년 Das et al.[6]은 동적 아이디를 이용하여 해당 사용자와 원격서버를 제외한 제3자로부터 익명성을 보장하는 기법을 최초로 제안하였다. 2005년 Chien et al.[7]은 Das et al. 기법의 사용자 익명성에 대한 취약점을 분석하고 개선한 프로토콜을 제안하였지만, Hu et al.[8]과 Bindu et al.[9]에 의해서 위장공격, 내부자공격, 재전송공격에 대한 취약점이 알려졌다. 그 외에도 Chai et al.[10], Kim et al.[11], Choi et al.[12,13]이 제안한 사용자 익명성을 보장하는 프로토콜이 있다.

※ 본 논문은 지식경제부 산업융합원천기술개발사업으로 지원된 연구결과임(No.10043907).
† 준 회 원 : 부산대학교 전기전자컴퓨터공학과 박사과정
†† 종신회원 : 부산대학교 정보컴퓨터공학부 부교수
논문접수 : 2013년 10월 11일
심사완료 : 2013년 11월 20일
* Corresponding Author : Howon Kim(howonkim@pusan.ac.kr)

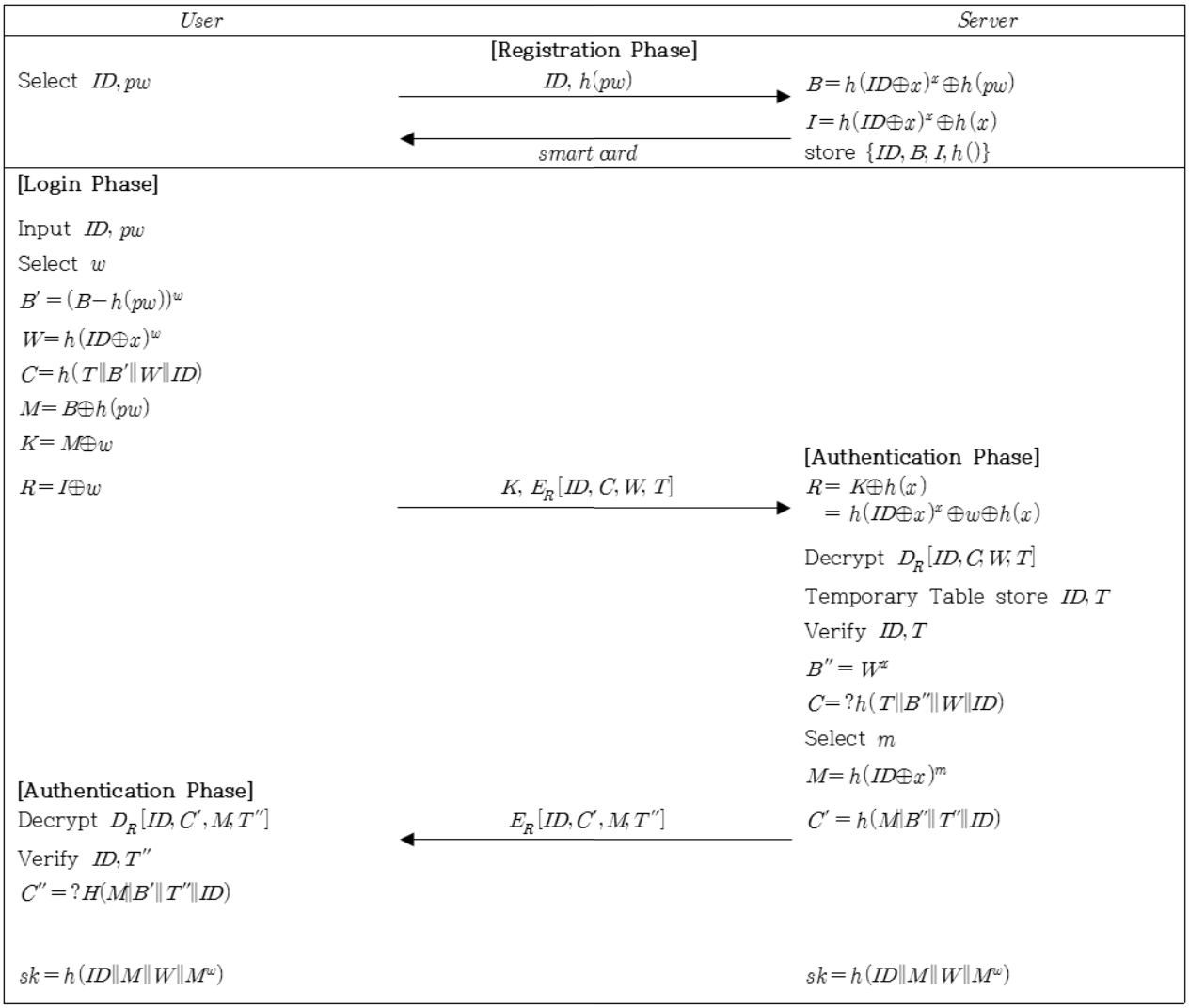

Fig. 1. Shin et al. protocol

본 논문에서는 2009년 제안된 Xu et al.[14] 기법의 사용자 익명성 문제를 개선하여 2012년에 제안된 Shin et al.[15] 기법에 대한 내부자공격과 전방향안전성 문제에 대해 분석하고, 이를 만족하기 위한 새로운 프로토콜을 제안한다. 제안한 프로토콜은 타원곡선상의 영지식 기법을 기반으로 사용자와 서버간의 상호 인증 및 세션키를 확립한다. 제안한 기법을 위장공격, 내부자공격, 사용자익명성, 전방향안전성, 재전송공격에 대해 각각 평가한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 Shin et al. 기법을 살펴보고, 분석한다. 3장에서는 새로운 프로토콜을 제안하고, 4장에서 제안한 프로토콜을 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 관련연구로 Shin et al.[15] 기법을 살펴보고, Shine et al. 기법의 전방향안전성에 대해서 분석한다. 전방향안전성의 부재에 따른 위장공격과 사용자 익명성 보장에 대한 위협을 분석한다. 본 장에서 Shin et al. 기법을 설명하기 위해 아래 Table 1과 같은 기호를 이용한다.

Table 1. Notation

기호	설명
pw	사용자의 패스워드
ID	사용자의 아이디
S	시스템서버
$h()$	단방향 해시함수
sk	서버와 사용자의 공통 세션키
$E_k[]/D_k[]$	암호화/복호화 알고리즘
T	타임스탬프
x	서버의 long-term 비밀키
$\oplus$	XOR 연산

2.1 Shin et al. 기법

Shin et al.은 Xu et al. 기법을 위장공격에 대해 분석하고, 이를 통해 사용자 익명성을 보장할 수 없는 것을 보이고, 이를 개선하기 위한 새로운 사용자 익명성을 보장하는 사용자 인증 프로토콜을 제안하였다. Shin et al. 기법은 등록단계, 로그인 단계, 인증단계로 구성된다. Fig. 1은 Shin et al. 기법의 전체적인 흐름을 그림으로 나타낸 것이다.

1) 등록단계

등록단계는 사용자가 서버에 등록이나 재등록할 때 수행되는 단계이다. 등록단계에서는 사용자의 ID와 pw를 생성하고, 보안파라미터를 저장하고 있는 스마트카드를 발급한다. 이 단계는 오프라인으로 수행한다.

Step 1. 사용자는 등록을 위해 ID와 $h(pw)$를 서버에게 전송한다.

Step 2. 서버는 아래 수식과 같이 B, I를 계산한다.

$$\begin{aligned} B &= h(ID \oplus x)^x \oplus h(pw) \\ I &= h(ID \oplus x)^x \oplus h(x) \end{aligned} \tag{1}$$

Step 3. 서버는 $\{ID, B, I, h()\}$가 저장된 스마트카드를 사용자에게 발급한다.

2) 로그인단계

로그인단계는 사용자가 서비스를 이용하기 위해서 서버에 로그인하고자 할 때 수행되는 단계이다. 이 단계는 안전하지 않은 통신채널에서 수행된다.

Step 1. 사용자는 자신의 ID와 pw를 입력하고, 해당 세션에 사용할 난수 w를 랜덤하게 선택한다.

Step 2. 사용자는 인증파라미터 C를 생성하기 위해 아래와 같이 계산한다.

$$\begin{aligned} B' &= (B \oplus h(pw))^w \\ W &= h(ID \oplus x)^w \\ C &= h(T \| B' \| W \| ID) \end{aligned} \tag{2}$$

Step 3. 사용자는 비밀키 R과 K를 아래와 같이 계산한다.

$$\begin{aligned} K &= M \oplus w \\ R &= I \oplus w \end{aligned} \tag{3}$$

Step 4. 사용자는 K와 암호문 $E_R[ID, C, W, T]$을 서버에게 전송한다.

3) 인증단계

인증단계는 사용자가 서비스를 이용하고자 할 때 로그인 단계 후에 사용자 인증을 수행하고, 세션키를 생성하기 위해서 수행되는 단계이다.

Step 1. 사용자에게 받은 암호문 $E_R[ID, C, W, T]$을 복호화하기 위해서 아래와 같이 R을 계산한다.

$$R = K \oplus h(x) \tag{4}$$

Step 2. 계산된 R을 이용하여 암호문을 복호화하고, 검증하기 위해 아래와 같이 계산한다.

$$\begin{aligned} B'' &= W^x \\ C &= ?\, h(T \| B'' \| W \| ID) \end{aligned} \tag{5}$$

Step 3. 서버는 난수 m을 선택하고 M을 계산한다.

$$M = h(ID \oplus x)^m \tag{6}$$

Step 4. 서버는 사용자에게 암호문 $E_R[ID, C'', M_s, T'']$을 전송한다.

Step 5. 사용자는 암호문 $E_R[ID, C'', M_s, T'']$을 복호화하여 서버가 정상적으로 인증을 했는지, 아래와 같이 검증하여 상호인증을 수행한다.

$$C'' = ?h(M \| B' \| T'' \| ID) \tag{7}$$

Step 6. 사용자와 서버는 각각 세션키 sk를 계산한다.

2.2 관련연구분석

본 장에서는 Shin et al. 프로토콜을 내부자공격, 전방향 안전성에 대해 분석한다. 본 장에서 분석하는 내부자공격과 전방향 안전성을 통해 인증단계를 위해 필요한 세션키 R을 계산할 수 있기 때문에 Shin et al. 기법은 위장공격, 사용자 익명성, 재전송 공격에 대한 안전성도 제공하지 못한다.

1) 내부자공격

내부자공격이란 서버에 등록된 사용자가 악의적인 의도로 공격을 수행하는 것을 의미한다. 따라서 공격자는 자신의 스마트카드의 정보를 얻을 수 있다. Shin et al. 기법은 공개된 파미터K로부터 비밀키 R을 계산하기 위해 서버의 키를 해쉬한 값 $h(x)$를 이용한다. 정상적인 방법으로는 사용자가 x를 알지 못하기 때문에 $h(x)$를 계산할 수 없다. Shin et al. 기법은 내부자공격에 대한 취약점을 가지는데 스마트카드에 저장되는 정보는 다음과 같다.

$$\begin{aligned} B &= h(ID \oplus x)^x \oplus h(pw) \\ I &= h(ID \oplus x)^x \oplus h(x) \end{aligned} \tag{8}$$

공격자는 자신의 스마트카드로부터 B, I 두 개의 정보를 얻을 수 있는데, 두 개를 XOR연산을 수행하면 다음과 같은 정보를 얻을 수 있다.

$$h(pw) \oplus h(x) = B \oplus I \tag{9}$$

공격자는 자신의 스마트카드로 얻은 정보이기 때문에 자신의 패스워드pw를 알고 있다. 따라서 $h(pw)$를 계산할 수

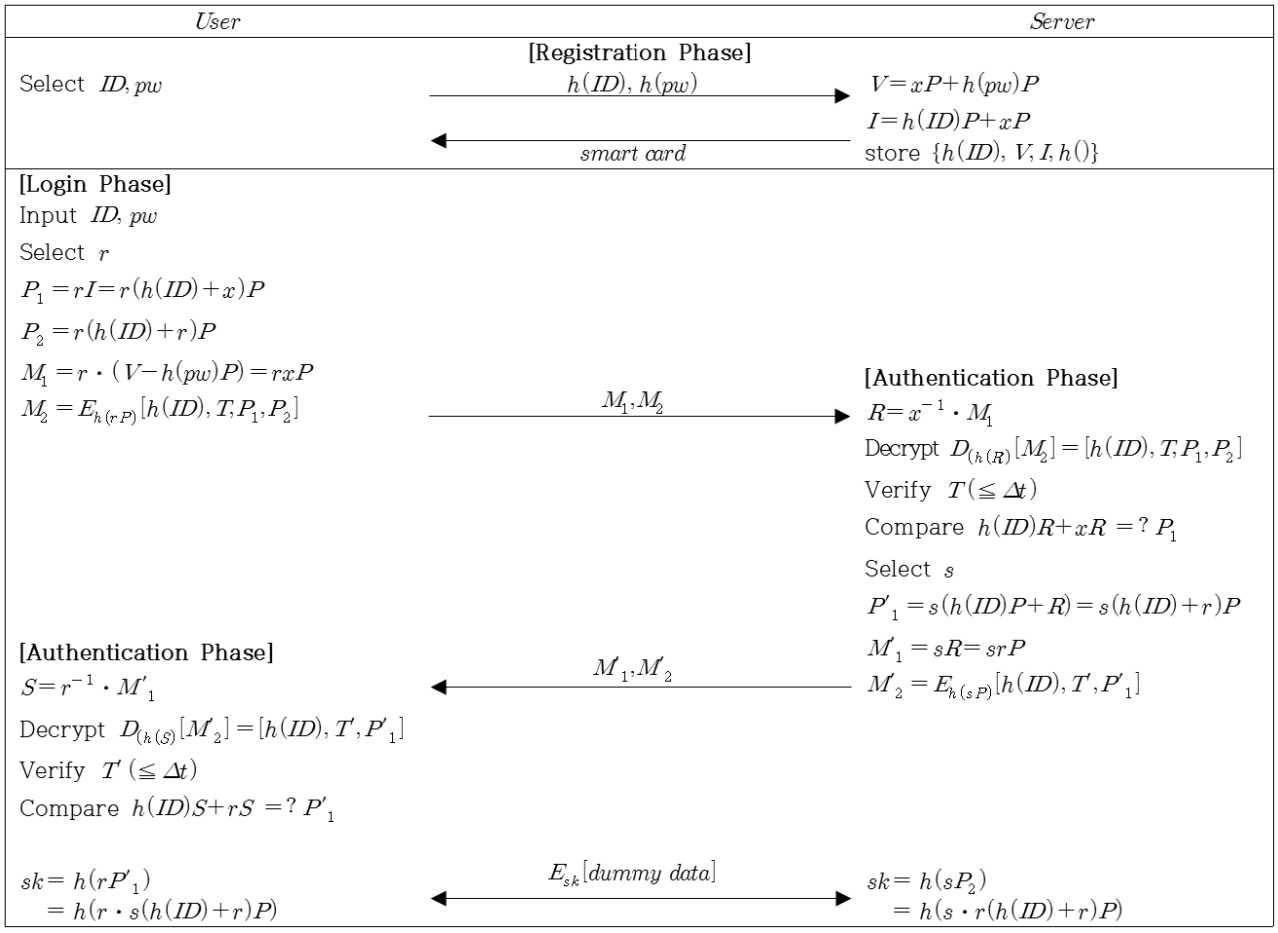

Fig. 2. Proposed protocol

있기 때문에 XOR의 베타적 연산 특성을 이용하여 다음과 같이 $h(x)$를 계산할 수 있다.

$$h(x)=h(pw)\oplus h(x)\oplus h(pw) \tag{10}$$

공격자는 $h(x)$를 알기 때문에 사용자의 비밀키 R을 계산할 수 있으며, 인증단계를 서버대신 수행할 수 있게 된다. 따라서 내부자 공격을 통해서 서버 위장공격을 수행할 수 있다.

2) 전방향 안전성

전방향 안전성(Forward secrecy)란 이전 세션키가 노출되었을 때 앞으로 세션키에 영향을 미치는지를 나타내는 안전성이다. 즉,이전 세션키가 노출되어도 앞으로의 세션키는 알 수 없어야 한다. 만약 공격자가 사용자의 이전 세션키 R'을 알았다고 가정해보자. 공격자는 현재 세션키의 정보로 K를 알 수 있다. 그리고 이전 세션키의 정보로는 R'과 K'을 알고 있다. 각각은 아래와 같이 계산된 파라미터이다.

$$\begin{aligned} M &= B\oplus h(pw) \\ K' &= M\oplus w' \\ R' &= I\oplus w' \\ K &= M\oplus w \end{aligned} \tag{11}$$

여기서 주목해야 할 점은 R'과 R의 차이점은 난수 w'와 w이고, 나머지 I는 고정된 파라미터이다, 마찬가지로 K'와 K도 고정된 파라미터 M을 사용한다. 이전 세션키 정보 K'과 R'을 XOR 연산하면 다음과 같다.

$$E=I\oplus M=K'\oplus R' \tag{12}$$

위에서 계산된 E를 이용하여 현재 세션 정보인 K를 XOR 연산하면 다음과 같은 정보를 알 수 있다.

$$\begin{aligned} R=I\oplus w &= E\oplus K \\ &= I\oplus M\oplus M\oplus w \end{aligned} \tag{13}$$

위와 같이 이전 세션키 R'을 알수 있다면 E를 계산하여, 위와 같이 해당 사용자의 모든 세션키를 계산할 수 있다. 따라서 Shin et al. 기법은 전방향 안전성을 제공하지 못한다.

3. 제안프로토콜

관련연구에서 Shine et al. 기법에 대해 살펴보고 이를 내부자공격, 전방향 안전성, 위장공격, 사용자 익명성, 재전송

공격에 대해서 분석하였다. 특히 내부자공격과 전방향안전성을 통해 공격자가 세션키를 얻어 낼 수 있음을 증명하였으며, 따라서 위장공격, 사용자익명성, 재전송공격에 대해서도 취약함을 알 수 있다. 본 장에서는 앞에서 분석한 공격에 대해 안전한 프로토콜을 제안한다. 제안한 프로토콜을 설명하기 위해서 Table 2와 같은 기호를 사용한다.

Table 2. Notation for proposed scheme

기호	설명
ID,pw	사용자의 아이디, 패스워드
$h()$	Z_p 상의 일방향 함수
$E_k[]/D_k[]$	암호화/복호화 알고리즘
T	타임스탬프
x	서버의 long-term 비밀키
P	타원곡선 상의 생성원

3.1 등록단계

등록단계는 사용자가 서버에 등록 또는 재등록할 때 수행되는 단계로 해당사용자를 위한 초기 파라미터를 설정하고 스마트카드를 발급하는 단계이다.

Step 1. 사용자는 $h(ID)$와 $h(pw)$를 서버에 전송한다. 이때 $h()$는 사용자의 ID와 pw를 정해진 소수 p를 위수로 가지는 Z_p상의 원소로 매핑시켜주는 일방향 함수이다.

Step 2. 서버는 다음 식과 같이 V, I를 계산한다.

$$\begin{aligned} V &= xP + h(pw)P \\ I &= h(ID)P + xP \end{aligned} \tag{14}$$

Step 3. 서버는 $h(ID), V, I, h()$를 저장하고 스마트카드를 발급한다.

3.2 로그인단계

로그인단계는 사용자가 서비스를 받고자 할 때, 인증하기 하기 위해서 정보를 입력하고 서버에게 사용자 인증정보를 전송하는 단계이다.

Step 1. 사용자는 ID와 pw를 입력하고 Z_p상의 난수 r을 선택한다.

Step 2. 사용자를 인증하기 위한 정보 P_1, P_2를 다음과 같이 계산한다.

$$\begin{aligned} P_1 &= rI = r(h(ID) + x)P \\ P_2 &= r(h(ID) + r)P \end{aligned} \tag{15}$$

Step 3. 사용자는 전송할 메시지 M_1, M_2를 계산하고, 서버에게 전송한다.

$$\begin{aligned} M_1 &= r \cdot (V - h(pw)P) = rxP \\ M_2 &= E_{h(rP)}[h(ID), T, P_1, P_2] \end{aligned} \tag{16}$$

3.3 인증단계

인증단계는 사용자의 로그인단계를 마치고, 사용자에게 받은 정보를 이용하여 사용자를 인증하고, 사용자는 서버를 인증하는 상호인증을 수행하는 단계이다.

Step 1. 서버는 R을 계산한다.

$$R = x^{-1} \cdot M_1 = rP \tag{17}$$

Step 2. 서버는 M_2를 R을 이용하여 복호화하고 타임스탬프 T가 최대 시간차 Δt안에 있는지 검증한다.

$$\begin{aligned} D_{(h(R)}[M_2] &= [h(ID), T, P_1, P_2] \\ T &\leqq ? \Delta t \end{aligned} \tag{18}$$

Step 3. 서버는 사용자를 인증한다.

$$h(ID)R + xR \; =? \; P_1 \tag{19}$$

Step 4. 서버는 난수 s를 선택하고, 증명정보 P'_1을 계산한다.

$$P'_1 = s(h(ID)P + R) = s(h(ID) + r)P \tag{20}$$

Step 5. 서버는 전송메시지 M'_1, M'_2를 계산하고, 전송한다.

$$\begin{aligned} M'_1 &= sR = srP \\ M'_2 &= E_{h(sP)}[h(ID), T', P'_1] \end{aligned} \tag{21}$$

Step 6. 사용자는 서버에게 받은 메시지를 통해 서버를 인증하는 단계이다. 먼저 사용자는 S를 다음과 같이 계산한다.

$$S = r^{-1} \cdot M'_1 = sP \tag{22}$$

Step 7. 사용자는 서버의 메시지 M'_2를 복호화하고, 타임스탬프 T'를 검증한다.

$$\begin{aligned} D_{h(S)}[M'_2] &= [h(ID), T', P'_1] \\ T' &\leqq ? \Delta t \end{aligned} \tag{23}$$

Step 8. 사용자는 서버를 인증한다.

$$h(ID)S + rS \; =? \; P'_1 \tag{24}$$

Step 9. 서버와 사용자는 각각 세션키 sk를 계산한고, sk를 이용하여 암호화된 정해진 데이터를 송수신함으로써 상호인증 및 세션키 확립단계를 마친다.

Table 3. Comparison between Shin et al. and proposed scheme

	위장공격	내부자공격	사용자익명성	전방향안전성	재전송공격
Shin et al.	△	×	△	×	△
Proposed scheme	○	○	○	○	○

×:취약, △:복합 공격에 취약, ○:안전

$$sk_u = h(rP'_1) = h(r \cdot s(h(ID)+r)P) \qquad (25)$$
$$sk_s = h(sP_2) = h(s \cdot r(h(ID)+r)P)$$

4. 프로토콜분석

본 장에서는 3장에서 제안한 프로토콜을 위장공격, 내부자공격, 사용자익명성, 전방향안전성, 재전송공격에 대해서 평가한다.

4.1 위장공격

위장공격은 사용자위장공격과 서버위장공격으로 나눌 수 있다. 사용자위장공격이란 공격자가 서버에게 자신이 정당한 사용자로 속이는 공격이며, 서버위장공격은 공격자가 사용자에게 자신이 서버인 것처럼 속이는 공격이다.

사용자위장공격을 수행하기 위해서 공격자는 M_1, M_2메시지를 변조하여 인증을 받을 수 있어야 한다. 여기서 공격자가 사용자를 위장하기 위해서는 M_2를 복호화 해야 한다. M_2를 복호화 하기 위해서는 M_1으로부터 rP를 계산할 수 있어야 하는데, 이를 계산하려면 x를 알아야 한다. 주어진 정보로부터 x를 계산하는 것은 타원곡선상의 이산대수문제의 어려움에 기반하며, 통상적으로 소수 p의 비트길이가 163비트 이상이면 안전한 것으로 알려져 있다.

공격자가 서버위장공격을 수행하기 위해서는 M'_1, M'_2를 변조할 수 있어야 한다. 공격자가 M'_1에서 s대신에 s'을 삽입하기 위해서 rP를 알아야 하는데, 사용자위장공격과 동일하게 공격자는 x를 알 수 없기 때문에 rP를 알 수 없다. 공격자가 임의의 $s'P=\alpha rP$를 M''_1으로하여 M'_2를 생성한다고 가정해보자. 먼저 공격자는 사용자의 ID 모르기때문에 $h(ID)$를 계산할 수 없으며, 설령 어떠한 방법으로 $h(ID)$를 알게 된다고 하더라도, P''_1을 계산해야 하는데 P''_1은 아래 식을 만족해야 한다.

$$P''_1 = \alpha(h(ID)P + R) = \alpha(h(ID)+r)P \qquad (26)$$

위의 식을 만족하는 P''_1을 계산하기 위해서는 R 또는 r을 알아야 하는데, 공격자는 M_1으로부터 rP를 알 수 없기 때문에 P''_1을 계산할 수 없다.

4.2 내부자공격

내부자공격은 서버에 정상적으로 등록된 사용자가 악의적인 의도로 다른 사용자를 위장하는 공격이다. 내부 공격자를 E라고 했을 때, 공격자는 자신의 스마트카드의 정보 V_E, I_E를 알 수 있고, 정상적인 사용자(U)를 위장하기 위해서는 M_1, M_2를 계산해야 하는데, 이를 위해서 $h(ID)$를 알아야 한다. 공격자가 $h(ID_u)$를 알기 위해서는 M_{u1}, M_{u2}에서 M_{u2}를 복호화 할 수 있어야한다. 공격자는 자신의 스마트카드 정보로부터 xP를 알 수 있으며, 주어진 정보로 M_{u1}에서 rP를 구해야 하는데, 이를 위해서는 위장공격과 동일하게 서버의 비밀키 x를 알아야하는데, 이는 타원곡선상의 이산대수 문제의 어려움과 동일하다.

4.3 사용자익명성

사용자익명성은 외부사용자가 서비스를 사용하는 사용자의 ID를 알 수 없는 특성이다. 제안한 프로토콜에서는 사용자의 $h(ID)$를 $h(rP)$로 암호화하여 전송한다. 따라서 외부사용자가 서비스 사용자의 ID를 알기 위해서는 M_2를 복호화할 수 있어야 하는데 이를 위해서 M_1으로부터 rP를 계산할 수 있어야 한다. 하지만 M_1으로부터 rP를 계산하기 위해서는 서버의 비밀키 x를 알아야 하는데, 이것은 타원곡선 상의 이산대수 문제의 어려움에 기반한다.

4.4 전방향안전성

전방향안전성이란 어떠한 방법으로 현재의 키가 알려졌다 하더라도 다음에 이용될 키는 안전할 수 있도록 하는 특성이다. 제안한 프로토콜에서 현재 세션의 비밀정보 rP와 세션키 sk가 노출되었다고 가정해보자. 공격자는 이를 이용하여 다음에 생성될 세션키의 정보를 계산하려고 시도할 수 있다. 사용자가 다음에 생성하는 메시지를 다음과 같이 정의하자.

$$N_1 = r' \cdot (V - h(pw)P) = r'xP \qquad (27)$$
$$N_2 = E_{h(r'P)}[h(ID), T, P_1, P_2]$$
$$sk_N = h(s' \cdot r'(h(ID)+r')P)$$

위의 식에서 알 수 있듯이 다음 세션키 및 비밀정보는 이전 또는 현재의 세션키 및 비밀정보와 완전 독립적으로 생성되는 것을 알 수 있다. 따라서 이전 비밀정보 rP가 노출되더라도 x를 모르면 다음 세션 비밀정보 $r'P$를 알 수 없다. 세션키 sk_N도 마찬가지로 해당 세션에 생성되는 s', r'을 계산할 수 없다면 세션키를 알 수 없다.

4.5 재전송공격

재전송공격이란 이전에 사용된 메시지를 그대로 재전송하

여 인증을 수행하는 공격이다. 제안한 프로토콜에서는 M_2를 복호화하여 구한 T를 Δt를 이용하여 검증하고 인증을 수행한다. 공격자가 재전송공격을 위해서 T를 수정하려면 M_2를 복호화할 수 있어야 하는데, M_2를 복호화하기 위해서는 x를 알아야 한다.

5. 결 론

초기에는 패스워드기반 인증이 널리 사용되었지만, 검증테이블 공격에 대한 취약점이 알려지면서, 스마트카드를 이용한 사용자 원격 인증에 대한 연구가 관심이 높아졌다. 검증테이블의 노출과 함께 개인정보 노출 문제에 대한 관심도 증대되면서, 사용자 익명성을 보장하는 인증 프로토콜을 Das et al.[6]을 필두로 연구하기 시작했다. Das et al. 기법은 사용자익명성을 완벽하게 보장할 수 없었으며, 이에 대한 분석과 사용자익명성을 제공하기 위한 새로운 프로토콜들에 대한 연구가 지속적으로 이어지고 있다. 2012년 Shin et al.[15]은 사용자 익명성을 제공할 수 있는 프로토콜을 제안하였다.

본 논문에서는 Shin et al. 기법을 내부자공격과 전방향안전성에 대해 분석하였으며, 분석된 결과를 토대로 사용자익명성, 위장공격, 재전송공격에도 영향을 미칠 수 있는 것을 보였다. 앞에서 분석한 공격에 대해 만족하기 위해서 타원곡선상의 영지식 기법을 이용한 사용자 원격 인증 프로토콜을 제안하였다. 본 논문에서 제안한 프로토콜은 사용자와 서버가 각 세션마다 난수 r, s를 생성하여 이를 세션키를 확립하는데 사용한다. 따라서 각 세션마다의 세션키를 독립적으로 생성할 수 있었으며, 서버와 사용자가 각각 rP, sP를 알려주고, 서로의 비밀정보 r, s를 공유하지 않기 때문에 영지식 기법에 기반한다. 이를 각각의 세션의 비밀정보로 이용하여 사용자와 서버간의 상호인증을 수행할 수 있다. 제안된 프로토콜에 대한 분석으로 위장공격, 내부자공격, 사용자익명성, 전방향안전성, 재전송공격에 대해 Table 3을 통해 비교 및 정리하였다.

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] N. Haller, “The S/Key one-time password system,” in *Proceedings of the ISOC Symposium on Network and Distributed System Security*, pp.151-157, 1994

[3] J. Choi and H. Kim, “One-Handled The Mobile One-Time Password Scheme,” *The Journal of The Korean Institute of Communication Sciences*, Vol.37, No.6, pp.497-501, 2012

[4] C. M. Chen and W. C. Ku, “Stolen-verifier attack on two new strong-password authentication protocol,” *IEICE Transactions on communications*, Vol.E85-B, No.11, pp.2519-2521, 2002.

[5] C. C. Lee, M. S. Hwang and W. P. Yang, “A Flexible Remote User Authentication Scheme using Smart Cards,” *ACM Operating System Review*, Vol.36, No.4, pp.23-29, 2002.

[6] M. L. Das, A. Saxena and V. P. Gulati, “A dynamic ID-based remote user authentication Scheme,” *IEEE Transactions on Consume Electronics*, Vol.50, No.2, pp.629-631, 2004.

[7] H. Y. Chien and C. H. Chen, “A remote User Authentication Scheme preserving user anonymity,” in *Proceedings of IEEEAINA'05*, Vol.2, pp.245-248, 2005.

[8] L. Hu, Y. Yang and X. Niu, “Improved remote User Authentication Scheme preserving user anonymity,” in *Proceedings of Fifth Annual Conference on Communication Network and Services Research(CNSR)*, pp.323-328, 2007.

[9] C. S. Bindu, P. C. S. Reddy and B. Satyanarayana, “Imporoved Remote User Authentication Scheme Preserving User Anonymity,” *IJCSNS*, Vol.8, No.3, pp.62-66, 2008.

[10] Z. Chai, Z. Cao and R. Lu, “Efficient Password-Based Authentication and Key Exchange Scheme Preserving User Privacy,” in *Proceedings of WASA'06*, LNCS 4138, pp.467-477, 2006.

[11] S. Kim, J. Y. Chun and D. H. Lee, “Anonymity User Authentication Scheme with Smart Cards preserving Traceability,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol.18, No.5, pp.31-39, 2008

[12] J. Choi and S. Shin, “Traceable Authentication Scheme Providing User Anonymity,” *Journal of The Korea Contents Association*, Vol.9, No.4, pp.95-102, 2009

[13] J. Choi, S. Shin and K. Han, “Three-Party Key Exchange Protocol Providing User Anonymity based on Smartcards,” *Journal of the Korea Academia-Industrial cooperation Society*, Vol.10 No.2, pp.388-395, 2009

[14] J. Xu, W. Zhu and D. Feng, “An improved smart card based password authentication scheme provable security,” *Computer Standard & Interface*, Vol.31, No.4, pp.723-728, 2009.

[15] K. Shin and J. Cho, “A Remote Authentication Protocol Design Using Smart Card to Guarantee User Anonymity,” *Korean Institute Of Information Technology*, Vol.10, No.12, pp.77-87, 2012.

최 종 석

e-mail : jschoi85@pusan.ac.kr

2011년 동명대학교 정보보호학과(학사)

2013년 부산대학교 컴퓨터공학과(석사)

2013년~현 재 부산대학교 전기전자컴퓨터공학과 박사과정

관심분야 : IoT, RFID 인증, 컴퓨터보안, 암호이론

김 호 원

e-mail : howonkim@pusan.ac.kr

1993년 경북대학교 전자공학과(학사)

1995년 포항공과대학교 전자전기공학과 석사(공학석사)

1999년 포항공과대학교 전자전기공학과 박사(공학박사)

1998년 12월~2008년 2월 한국전자통신연구원(ETRI) 정보보호 연구단 선임연구원/팀장

2008년 3월~현 재 부산대학교 정보컴퓨터공학부 부교수

관심분야 : IoT, RFID 인증, 컴퓨터보안, 암호이론