한국산학기술학회논문지
Vol. 10, No. 2, pp. 388-395, 2009

사용자 익명성을 제공하는 스마트카드 기반 3자 참여 키 교환 프로토콜

최종석[1], 신승수[1*], 한군희[2]

Three-Party Key Exchange Protocol Providing User Anonymity based on Smartcards

Jong-Seok Choi[1], Seung-Soo Shin[1*] and Kun-Hee Han[2]

요 약 2006년에 공개키 연산 대신 XOR 연산과 해쉬함수만을 사용하는 스마트카드를 이용하는 3자 참여 인증된 키 교환 프로토콜이 제안되었다. 최근에는 개인프라이버시에 대한 관심이 높아지며 사용자 익명성을 보호하기 위한 연구가 진행되고 있다. 본 논문에서는 2006년 제안된 3자 참여 인증된 키 교환 프로토콜이 사용자 익명성을 제공하지 못하며 잘못된 입력값 감지가 늦다는 문제점을 제기하고, 이러한 문제점을 해결하기 위해서 스마트카드 기반 3자 참여 키 교환 프로토콜을 제안하였다.

Abstract Three-party authenticated key exchange protocol based on smartcards using XOR and hash function operation instead of the public key operation has been proposed in 2006. Recently, it is doing for research because of increasing interest in privacy. This paper pointed out that proposed three-party authenticated key exchange protocol in 2006 has some problems; it is user anonymity and slow wrong input detection, and then we proposed new one to overcome these problems.

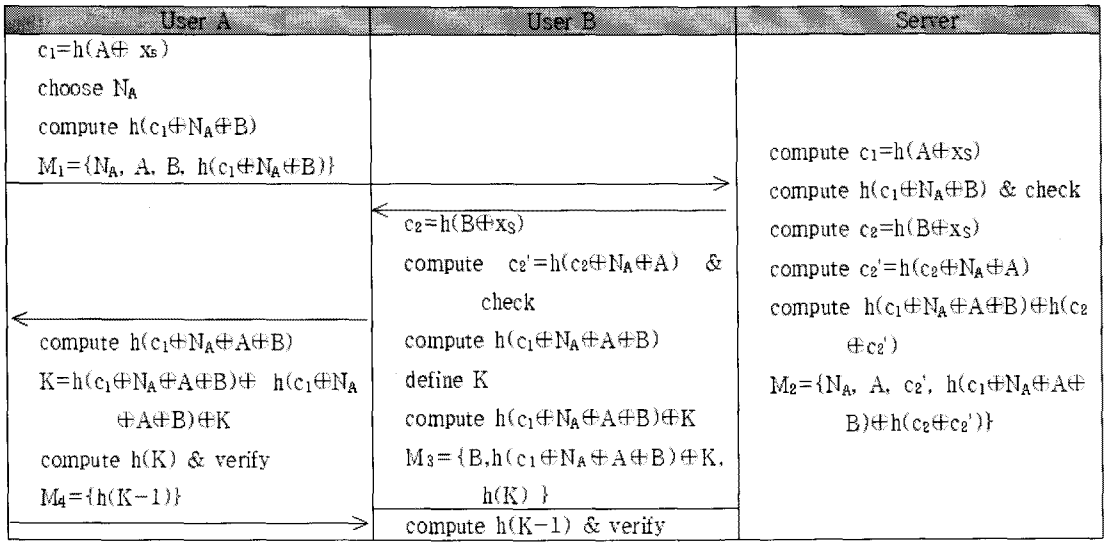
Key Words : Three-party Key Exchange Protocol, User Anonymity, Smartcards

1. 서론

최근 통신기술과 컴퓨터 기술의 급속한 발전으로 인해 분산된 컴퓨터 기술에 대한 연구가 진행되고 있다. 네트워크를 통해 정보를 안전하게 전송하기 위해서는 정보를 암호화하여야 한다. 암호통신을 하기 위해서는 참여자들 사이에 인증과 키 공유가 필요하다. 키 교환 프로토콜로는 2자간 키 교환 프로토콜과 3자간 키 교환 프로토콜과 다자간 키 교환 프로토콜이 있으며, 대표적인 2자간 키 교환 프로토콜로는 Diffie-Hellman 키 교환 프로토콜[1]이 있다. 그러나 Diffie-Hellman 키 교환 프로토콜은 인증을 제공하지 않으므로 중간자 공격에 취약하다. 중간자 공격을 해결하기 위해서 Bellovin과 Merritt는 패스워드 기반 EKE (Encrypted Key Exchange) 기법[2]을 제안하였다. 이 기법은 서버가 공격당하면 공격자가 쉽게 정당한 사용자로 위장할 수 있다. 이러한 문제점을 해결하기 위해 패스워드 대신 검증자를 저장하고 이용하는 기법들[3,4]이 제안 되었다. Steiner등은 EKE를 기반으로 하는 3자 참여 인증된 키교환 프로토콜(STW-3PEKE)[5]을 제안하였다. Lin등은 STW-3PEKE가 오프라인 추측공격에 취약함을 보이고, 이를 개선하기 위해 서버의 공개키를 사용한 프로토콜(LSH-3PEXE)[6]을 제안하였고, 그 후 공개키를 사용하지 않는 새로운 프로토콜(LSSH-3PEKE)[7]을 제안하였다. 최근에는 Sun등이 STW-3PEKE의 문제점을 해결하기 위해 서버의 공개키를 이용한 패스워드 기반의 개선된 프로토콜(SCH-3PEKE)[8]을 제안하였다.

2006년에 제안된 프로토콜[9]에서는 지수연산을 사용하지 않고 해쉬함수와 XOR연산만을 사용하는 스마트카

[1]동명대학교 정보보호학과
[2]백석대학교 정보통신학부
*교신저자: 신승수(shinss@tu.ac.kr)
접수일 09년 01월 19일 수정일 09년 02월 16일 게재확정일 09년 02월 18일



[그림 1] 3자 참여 인증된 키 교환 프로토콜 구조

드 기반 3자 참여 인증된 키 교환 프로토콜이 제안되었다.

이와 같이 스마트카드를 이용하여 인증과 키 교환을 하기 위한 프로토콜들이 제안되고 있으며, 분산된 시스템에서도 개인프라이버시에 대한 관심이 높아지면서 사용자 익명성에 대한 연구가 진행되고 있다.

사용자 익명성을 보호하기 위해 2004년에 Das et al.이 동적 아이디를 이용하여 사용자 익명성을 제공하는 프로토콜[10]을 처음 제안하였다. 2005년에 Chien and Chen은 Das et al. 프로토콜이 사용자 익명성을 제공하지 못한다는 문제점을 제기하고, 이러한 문제를 해결하기 위해 새로운 프로토콜[11]을 제안하였다. 2007년에는 Hu et al.이 Chien and Chen프로토콜을 분석하여 강한 서버/사용자 가장 공격, 제한된 재전송 공격[12], 내부자 공격[13], 서비스 거부 공격, 잘못된 패스워드의 감지가 늦다는 것에 대한 문제점을 제기하고, 이러한 문제를 해결하기 위한 프로토콜[14]을 제안하였다. 2008년에는 Bindu et al.이 Chien and Chen 프로토콜은 내부자 공격과 중간자 공격에 대해 취약하다는 문제점을 제기하고, 개선된 프로토콜[15]을 제안하였다.

본 논문에서는 2006년에 제안된 3자 참여 인증된 키 교환 프로토콜[9]은 사용자 익명성을 제공하지 못하고, 서버가 두 사용자 사이의 세션키를 알 수 있는데도 불구하고 세션키를 생성하는 과정에서 사용자 B의 의견만 받아들여 두 사용자 사이에 세션키에 대한 공평성이 없다. 3자간 프로토콜에서는 서버는 두 사용자가 신뢰하는 기관이어야 한다. 따라서 세션키가 두 사용자에게 공평성 있는 세션키를 만들기 위해서는 두 사용자 모두의 의견이 세션키 생성 과정에 사용되거나 두 사용자가 신뢰하는 기관인 서버가 세션키를 생성하여야 한다. 따라서 본 논문에서는 사용자 익명성과 세션키의 공평성을 만족하는 3자 참여 키 교환 프로토콜을 제안하고, 제안한 프로토콜을 추측공격, 재전송 공격, 위장공격, 전방향 안전성, 사용자 익명성에 대해 비교·분석했다.

본 논문의 구성은 다음과 같다. 2장에서는 3자 참여 인증된 키 교환 프로토콜에 대해서 살펴보고, 3장에서는 기존 프로토콜에 대한 안전성에 대한 문제점 분석과 사용자 익명성, 공평성과 같은 문제점을 해결하기 위한 새로운 프로토콜을 제안한다. 4장에서는 3자 참여 인증된 프로토콜과 제안한 프로토콜과의 안전성 및 효율성을 비교 분석하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

본 논문에서 제안하는 프로토콜 및 관련된 기존 연구의 프로토콜 기술에 사용되는 용어의 표기법을 정의하고, 3자 참여 인증된 키 교환 프로토콜[9]에 대한 문제점을 분석한다.

2.1 표기법 정의

본 논문에서 제안된 프로토콜 및 관련연구에서 사용될 표기법을 [표 1]과 같이 정의한다.

[표 1] 표기법

기호	설명
U, A, B	사용자
PW	사용자의 패스워드
S	서버
x_s, x	서버의 비밀키
N_A, N_B	사용자 A, B의 난수
N_S	서버의 난수
h()	해쉬함수 연산
⊕	XOR 비트연산
=>	안전한 채널
->	공개된 채널

2.2 3자 참여 인증된 키 교환 프로토콜

연산량 감소를 위해 XOR 연산을 사용한 스마트카드를 이용한 3자 참여 인증된 키 교환 프로토콜[9]에 대해 설명한다. 3자 참여 인증된 키 교환 프로토콜은 사용자 등록단계, 로그인단계, 키교환단계로 구성된다.

[등록단계]

Step 1. A는 메시지{A, h(r⊕PW)}를 서버 S에게 전송한다.

Step 2. S는 자신의 비밀키 x_s를 이용하여 $R= h(A⊕x_s) ⊕ h(r⊕PW)$를 계산하고, A에게 R과 h()가 저장된 스마트카드를 발급한다.

Step 3. A는 스마트카드에 랜덤 값 r을 저장하여 등록을 마친다.

[로그인단계]

Step 1. A가 A와 PW를 입력하면 스마트카드는 $R⊕h(r⊕PW)$ 연산을 하여 그 결과로 $c_1=h(A⊕x_s)$를 생성한다 c_1과 랜덤 값 N을 이용하여 스마트카드는 S에게 메시지 {A, N, $h(c_1⊕N)$}을 보낸다.

Step 2. S는 $h(h(A⊕x_s)⊕N)$를 계산하여 받은 메시지 상의 $h(c_1⊕N)$을 검사한다.

[키교환단계]

Step 1. A는 $h(c_1⊕N_A⊕B)$를 계산하고, S에게 메시지 M_1을 보낸다.

M_1 = {N_A, A, B, $h(c_1⊕N_A⊕B)$}

Step 2. S는 $c_1=h(A⊕x_s)$와 $h(c_1⊕N_A⊕B)$를 계산하여, 그 값이 M_1에 포함된 값과 같으면 $c_2=h(B⊕x_s)$와 $c_2'=h(c_2⊕N_A⊕A)$를 계산하고, $h(c_1⊕N_A⊕A⊕B)⊕h(c_2⊕c_2')$를 계산하여 메시지 M_2를 B에게 보낸다.

M2 = {N_A, A, c_2', $h(c_1⊕N_A⊕A⊕B) ⊕ h(c_2⊕c_2')$}

Step 3. B는 $c_2'=h(c_2⊕N_A⊕A)$를 계산하고, 그 값이 M_2에 포함된 값과 같으면 B는 세션키 K를 결정하고 메시지 M_3를 A에게 보낸다.

M_3 = {B, $h(c_1⊕N_A⊕A⊕B)⊕K$, h(K)}

Step 4. A는 $h(c_1⊕N_A⊕A⊕B)$ 를 계산하고, 그 결과와 M_3에 포함된 $h(c_1⊕N_A⊕A⊕B)⊕K$를 XOR하여 세션키 K를 추출한고h(K)를 계산하여 비교한다. 그리고 메시지 M_4를 B에게 보낸다.

M_4 = {h(K-1)}

Step 5. B는 h(K-1)를 계산하여 검사한다.

2.3 관련연구 분석

본 절에서는 3자 참여 인증된 키 교환 프로토콜이 사용자 익명성(User anonymity), 잘못된 입력 값의 느린 감지(Slow wrong input detection)와 같은 문제점에 대해 분석한다.

2.3.1 사용자 익명성

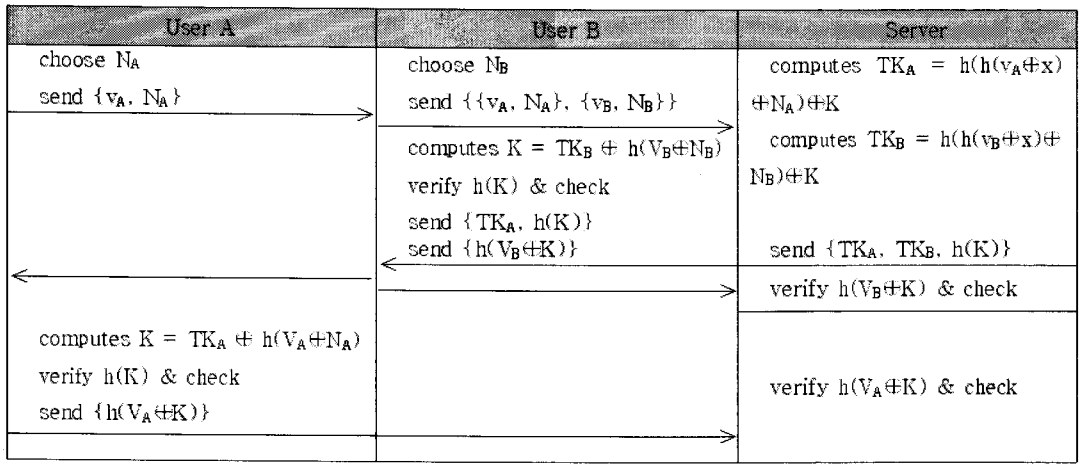
익명성이란 사용자가 자신의 신원을 드러내지 않고 서비스나 리소스를 사용하는 것을 말한다[16]. 최근에는 스마트카드를 이용한 원격 인증 시스템에서도 개인정보보호에 대한 관심이 높아지며 사용자 익명성을 제공하는 인증 시스템에 대한 연구가 시작되었다[17]. 3자 참여 인증된 프로토콜은 사용자의 익명성을 제공하지 않으며, 서버의 비밀키와 세션키를 제외한 나머지 정보를 모두 노출한다. 따라서 개인정보보호의 관점에서 볼 때 개인정보 보호 노출의 위험을 가지고 있다.

2.3.2 잘못된 입력 값의 느린 감지

공격자는 로그인 1단계에서 사용자 A의 {A, N, $h(c_1⊕N)$}를 가로 챌 수 있다. 공격자는 정당한 사용자 A의 {A, N, $h(c_1⊕N)$}를 저장해두고, 공격자가 그 데이터로 재전송 공격을 시도한다고 가정하자.

Step 1. 공격자는 {A, N, $h(c_1⊕N)$}를 S에게 보낸다.

Step 2. S는 {A, N, $h(c_1⊕N)$}로부터 로그인 2단계와 같은 계산을 수행하고 이 메시지가 정상적으로 로그인에 성공했던 메시지라면 로그인을 수락하게 된다.



[그림 2] 제안된 프로토콜 구조

Step 3. 키교환 1, 2단계는 이전에 수행되었던 것과 같이 수행되며, 키교환 3단계에서 B는 이전에 실제 사용자가 수행 했을 때와 다른 K를 생성 할 것이다. 그리고 M_3를 공격자에게 보내게 된다.

공격자는 c_1을 계산할 수 없기 때문에 세션키는 알아낼 수 없다. 이 때 주의해야 할 점은 3자 참여 인증된 프로토콜에서는 타임스탬프와 같은 요소를 사용하지 않고 있기 때문에 재전송된 메시지에 대해서 로그인을 수락하며 불필요한 수행과정을 반복하게 된다.

3. 제안한 프로토콜

본 장에서는 2장에서 분석한 사용자 익명성, 잘못된 입력값의 느린 감지 등의 문제점을 해결하기 위해서 새로운 프로토콜을 제안한다. 제안한 프로토콜은 두 사용자가 서로 익명성을 유지하며 하나의 원격 시스템 또는 서버를 통해 통신하고자 할 때 사용될 수 있다. 제안한 프로토콜은 등록단계, 키교환단계, 인증단계와 같이 3단계로 구성되어 있다.

[등록단계]

사용자가 서버에 등록 또는 재등록을 하고자 할 때 수행되는 단계로 일반적으로 최초 한번 수행된다.

Step 1. U => S : ID, $h(r \oplus PW)$

Step 2. S는 $v = h(ID \oplus N_s)$, $V = h(v \oplus x)$, $m = h(ID \oplus x) \oplus h(r \oplus PW)$, $I = h(ID \oplus x)$를 계산하여 스마트카드에 v, V, m, I, h()를 저장하여 발급한다.

Step 3. U는 스마트카드에 r을 입력한다.

U는 등록단계를 완료 후 난수 r을 외울 필요가 없으며, 스마트카드에는 v, V, m, I, h(), r 이 저장된다.

[키교환 및 인증단계]

어떤 사용자가 다른 사용자와 통신하고자 할 때 수행되는 단계로 서로에 대해 익명성을 보장하며 통신 할 수 있다. 이 때 두 사용자는 악의적인 의도를 가진 사용자가 아니라고 가정한다.

Step 1. A는 스마트카드를 리더기에 삽입하고, ID, PW를 입력한다.

Step 2. $m \oplus h(r \oplus PW)$와 I와 같은지 확인하여 ID와 PW를 검증하며, 같으면 다음단계를 진행한다.

Step 3. A->B : $\{v_A, N_A\}$

Step 4. B->S : $\{\{v_A, N_A\}, \{v_B, N_B\}\}$

Step 5. S는 $TK_A = h(h(v_A \oplus x) \oplus N_A) \oplus K$, $TK_B = h(h(v_B \oplus x) \oplus N_B) \oplus K$를 계산한다.

Step 6. S->B : $\{TK_A, TK_B, h(K)\}$

Step 7. B는 $K = TK_B \oplus h(V_B \oplus N_B)$를 계산하고, h(K)와 같은지 검증하여, 같으면 다음 단계를 진행한다.

Step 8. B->A : $\{TK_A, h(K)\}$

Step 9. A는 $K = TK_A \oplus h(V_A \oplus N_A)$를 계산하고, h(K)와 같은지 검증하여, 같으면 다음 단계를 진행한다.

Step 10. B->S : $\{h(V_B \oplus K)\}$

Step 11. S는 B에게 받은 $h(V_B \oplus K)$를 검증하고, 같으면 로그인을 수락한다.

[표 2] 제안한 프로토콜의 안전성 비교

평가요소 / 프로토콜	추측공격	서버비밀키 추측공격	재전송 공격	전방향 안전성	사용자 익명성	위장공격	FWD	공평성
3자 참여 키교환	O	O	O	O	X	O	X	X
제안된 프로토콜	O	O	O	O	O	O	O	O

FWD : 잘못된 패스워드의 빠른 감지능력(Fast Wrong input Detection)
O : 해당 문제에 강함, X : 해당 문제에 취약함

Step 12. A->S : {h(V_A⊕K)}
Step 13. S는 A에게 받은 h(V_B⊕K)를 검증하고, 같으면 로그인을 수락한다.

키교환 및 인증단계에서 Step 9 이전에 서버는 어떠한 검증도 수행하지 않으며 아주 간단한 계산만 수행한다. Step 11는 Step 7과 동시에 일어나며, 서버는 사용자 A, B가 정확한 세션키 K를 추출하였으므로 정당한 사용자라는 것을 인증할 수 있다.

4. 안전성 및 효율성 비교분석

본 장에서는 제안한 프로토콜의 추측공격, 서버 compromise 공격, 재전송 공격, 위장공격, 전방향 안전성, 사용자 익명성에 대해 안전성을 분석하고, 기능적인 측면과 성능적인 측면에 대한 효율성을 비교분석한다.

4.1 제안 프로토콜의 안전성 분석

본 논문에서 제안한 프로토콜의 추측공격(Guessing attack), 서버 Compromise 공격(Server compromise attack), 재전송 공격(Reply attack), 위장공격(Impersonation attack), 전방향 안전성(Forward secrecy), 사용자 익명성(User anonymity), 잘못된 입력값에 대한 감지(Fast Wrong input Detection)에 대해 안전성을 분석한다. [표 2]에서는 이러한 문제에 대해 3자 참여 인증된 프로토콜과 본 논문에서 제안한 프로토콜을 비교하였다.

4.1.1 추측공격

사용자 익명성이 보장되는 프로토콜에서는 ID와 PW가 추측공격의 대상이 된다. 제안한 프로토콜에서는 통신상에서 PW에 관한 정보는 전송되지 않으며 ID에 관한 정보는 오직 v를 통해서만 추측할 수 있다. 그러나 v=h(ID⊕N_S)로 암호학적 해쉬함수의 일방향성과 난수의 예측불가능성[18, 19]에 의존하고 있으므로 ID도 추측하기 어렵다.

4.1.2 서버의 비밀키 추측공격

서버의 비밀키를 사용하여 암호화된 전송메시지는 네트워크 상에서 많이 사용되므로, 공격자가 서버의 비밀키를 사용한 메시지를 가로챌 수는 있다. 그러나 가로챈 메시지로부터 서버의 비밀키에 관한 정보를 유추하는 것도 암호학적 해쉬함수의 일방향성과 난수의 예측불가능성 때문에 어렵다. 서버의 비밀키를 사용한 정보는 정당한 사용자의 스마트카드에도 저장되지만 정당한 사용자라도 해쉬함수와 난수의 성질 때문에 서버의 비밀키를 알 수 없다.

4.1.3 재전송 공격

제안한 프로토콜에서 서버는 사용자 B에게 처음 메시지를 받고 어떠한 검증도 하지 않는다. 그러나 세션키 K는 매번 달라지기 때문에 공격자가 세션키 K를 알기 위해서는 h(h(v_A⊕x)⊕N_A) 또는 h(h(v_B⊕x)⊕N_B)를 알아야 한다. 그러나 사용자는 네트워크상의 어떠한 정보로부터도 필요한 정보를 얻을 수 없다. h(h(v_A⊕x)⊕N_A) 또는 h(h(v_B⊕x)⊕N_B)를 알아낸다 하더라도 h(V_A⊕K)와 h(V_B⊕K)를 만들 수 없으므로 인증단계를 통과할 수 없다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

4.1.4 위장 공격

공격자는 사용자 A와 B의 첫 번째 메시지 {{v_A, N_A}, {v_B, N_B}}를 만들 수 있다. 그리고 서버는 첫 번째 과정에서 검증을 하지 않기 때문에 세션키를 만들어서 키교환단계를 진행하게 된다. 그러나 공격자가 정당한 사용자 A 또는 B가 아니라면 h(h(v_A⊕x)⊕N_A) 또는 h(h(v_B⊕x)⊕N_B)를 알 수 없기 때문에 세션키 K를 알 수 없다. h(h(v_A⊕x)⊕N_A) 또는 h(h(v_B⊕x)⊕N_B)를 알아낸다 하더라도 공격자는 h(V_B⊕K)와 h(V_B⊕K) 를 만들 수 없으므로 정상적으로 인증단계를 통과할 수 없다. 그러므로 위장공격에 안전하다.

4.1.5 전방향 안전성

공격자가 사용자의 개인키나 패스워드를 알아냈다 하

[표 3] 제안한 프로토콜의 효율성 비교

프로토콜 \ 평가요소		계산비용				통신비용	
		랜덤정수 생성회수	XOR 연산회수	해쉬 연산회수	비교연산	전체 전송데이터	서버 세션연결 후 전송 데이터
3자 참여 키교환 프로토콜	사용자 A	1	7	4	1	12	8
	사용자 B	0	6	4	2		
	서버 S	0	11	6	1		
제안한 프로토콜	사용자 A	1	2	3	1	13	7
	사용자 B	1	2	3	1		
	서버 S	0	6	5	2		

더라도 이전에 사용자가 사용했던 어떠한 세션키도 알 수 없을 경우, 프로토콜이 전방향 안전성을 만족한다고 한다[20]. 공격자가 사용자의 패스워드를 제안한 프로토콜에서는 키교환단계와 인증단계에서는 사용자의 패스워드에 관한 정보를 다루지 않기 때문에 키교환단계와 인증단계에는 영향을 주지 않는다. 따라서 이전에 사용됐던 어떠한 세션키도 얻어낼 수 없으며 공격자가 사용자의 아이디를 안다고 해도 공격자는 서버의 난수 N_S 와 비밀키 x를 모르기 때문에 어떠한 세션키도 알 수 없다.

4.1.6 사용자 익명성

제안한 프로토콜에서는 ID를 포함하고 있는 정보 $v=h(ID \oplus N_S)$만 네트워크 상에서 전송된다. 공격자는 정당한 사용자의 v를 취득할 수 있다. 그러나 해시함수의 일방향성, 난수의 예측불가능성과 무작위성[19]에 의해서 ID는 알 수 없다. 따라서 제안한 프로토콜은 사용자 익명성을 만족한다.

4.1.7 잘못된 입력값 감지

기존 프로토콜에서 사용자는 키교환 단계의 세션이 성립하기전 어떠한 입력값에 대한 검증도 하지 않고, 서버가 사용자에 대한 검증을 수행하여 사용자의 입력값이 잘못 되었다는 것을 알 수 있다. 제안한 프로토콜에서는 키교환 단계의 세션이 성립되기 전 단계인 Step 1, Step 2에서 사용자가 입력한 ID와 PW를 검증한다. 따라서 제안한 프로토콜에서는 세션이 성립되기 전에 잘못된 ID와 PW를 감지할 수 있다.

4.2 기존 프로토콜과의 효율성 비교분석

[표 3]에서 볼 수 있듯이, 제안한 프로토콜은 3자 참여 키 교환 프로토콜[9]에 비해 계산비용이 감소했다. 제안한 프로토콜에서 연산비용을 보면 두 사용자는 연산비용이 모두 같다. 이와 같이 제안한 프로토콜에서는 두 사용자가 동일하게 참여한다. 또한 서버측면에서도 계산비용이 감소하여, 기존 프로토콜보다 많은 사용자에 대해서 원활한 서비스를 제공할 수 있다. 기존 프로토콜은 세션키가 교환되기 전에 서버와의 세션이 먼저 종료되어, 그 이후의 세션에 대해서는 사용자 B가 사용자 A에 비해 키 교환 프로토콜에서 역할의 중요도가 높아지지만, 제안한 프로토콜에서는 서버가 키 교환이 완료된 시점에서 세션을 종료하기 때문에 프로토콜에서 두 사용자를 동등하게 해준다. 모든 데이터가 같은 크기라고 가정했을 때 통신비용은 하나의 정보크기만큼 더 전송하게 된다. 그러나 [그림 2]에서 볼 수 있듯이 제안한 프로토콜에서는 서버와 세션이 연결된 이후에는 7개의 정보를 전송하는 반면에 [그림 1]과 같이 기존 프로토콜에서는 서버와 세션이 연결된 이후에도 8개의 정보를 전송한다. 따라서 제안한 프로토콜은 서버가 세션을 연결한 이후에는 계산비용과 통신비용이 모두 감소하여 서비스거부공격에도 기존 프로토콜에 비해 효율적이다.

5. 결 론

본 논문에서는 동일한 서버에 등록된 두 사용자가 자신의 익명성을 보장받으며 안전한 통신을 하고자 할 때 키 공유를 위한 새로운 프로토콜을 제안하였다. 제안한 프로토콜은 지수연산과 암호화연산을 사용하지 않고, XOR 비트연산과 해쉬연산을 주 연산으로 사용하고, 기존 프로토콜에 비해서 계산비용이 효율적으로 감소하였으며, 사용자 익명성을 보장하기 때문에 두 사용자는 개인프라이버시를 보장받는다. 서버의 측면에서도 계산비용이 효율적으로 감소하였고, 사용자와 서버 간에 세션이 성립된 후에 통신비용이 감소하여 서비스거부공격에도

효율적이다. 본 논문에서 제안한 프로토콜은 사용자 익명성을 제공하면서 암호통신을 하기 위한 스마트카드를 이용한 키 교환 프로토콜 분야 및 다양한 응용분야에서 유용하게 사용 될 수 있을 것이다.

참고문헌

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

[2] S. M. Bellovin and M. Merrit, "Encrypted key exchange: Password based protocols secure against dictionary attacks," Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

[3] S.M. Bellovin and M. Merritt, "Augmented encrypted key exchange : a password-based protocol secure against dictionary attacks and password file compromise," Technical report, AT&T Bell Laboratories, 1994.

[4] T. Kwon and J. Song, "Secure agreement scheme for gxy via password authentication," Electronics Letters Vol.35, No.11, pp. 892-893, 1999.

[5] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and extension of Encrypted Key Exchange," ACM Operating Systems Review, Vol 29, No.3, pp. 22-30, 1995.

[6] C. Lin, H. Sun, and T. Hwang, "Three-party encrypted key exchange: Attacks and a solution," ACM Operating Systems Review, Vol.34, No.4, pp. 12-20, 2000.

[7] C. Lin, H. Sun, M. Steiner, and T. Hwang, "Three-party Encrypted Key Exchange Without Server Public-Keys," IEEE Communication Letters, Vol.5, No.12, pp. 497-499, 2001.

[8] H. Sun, B. Chen, and T. Hwang, "Secure key agreement protocols for three-party against guessing attacks," The Journal of Systems and Software, Vol.75, pp. 63-68, 2005.

[9] 전일수, "스마트카드를 이용한 3자 참여 인증된 키교환 프로토콜", 한국정보보호학회, 제16권, 제6호, pp. 73-80, 2006. 12.

[10] Manik Lal Das, Ashutosh Sacena, Ved P. Gulati, "A Daunamic ID-based Remote User Authentication Scheme," IEEE Trans. on Consumer Electronics, Vol.50, No.2, pp. 629-631, 2004.

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

[12] W.C. Ku, C.M. Chen, and H.L. Lee, "Cryptanalysis of a variant of Peyravian-Zunic' password authentication scheme," IEICE Trans. Commun., Vol.E86-B, No.5, pp. 1682-1684, 2003.3.

[13] H.M. Qiu, Y.X. Yang, and Z.M. Hu, "new mutual user authentication scheme using smart card," Application Research of Computers, No.12, pp. 103-105, 2005.

[14] Lanlan Hu, Yixian Yang, Xinxin Niu, "Improved Remote User Authentication Scheme Preserving User Anonymity," IEEE CNSR'07, pp. 323-328, 2007.

[15] C. Shoba Bindu, P. Chandra Sekhar Reddy, B. Satyanarayana, "Imporoved Remote User Authentication Scheme Preserving User Anonymity," IJCSNS, Vol.8, No. 3, 2008.3.

[16] 김세일, 천지영, 이동훈, "추적이 가능한 스마트카드 사용자 인증 기법", 한국정보보호학회, 제18권, 제5호, pp.31-39, 2008.10.

[17] 김세일, 이현숙, 이동훈, "익명성을 제공하는 스마트카드 사용자 인증 프로토콜", 한국정보보호학회, 제17권, 제2호, pp. 139-144, 2007.4.

[18] 강주성, "난수발생기의 현황 및 안전성 분석 기술동향", 한국정보보호학회, 제16권, 제4호, pp. 23-46, 2006.8.

[19] 양형규, 안영화, "난수와 암호 ", 한국정보보호학회, 제2권, 제3호, pp. 67-80, 1992. 9.

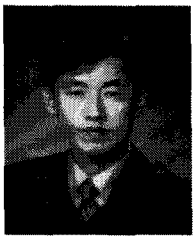
[20] 김용훈, 윤택영, 박영호, "서버의 개입이 없는 스마트카드 기반의 3자간 키 교환 프로토콜", 한국정보보호학회, 제18권, 제2호, 2008.4.

최 종 석(Jong-Seok Choi) **[준회원]**

- 2004년 3월 ~ 현재 : 동명대학교 정보보호학과 학생

<관심분야>
암호프로토콜, USN.

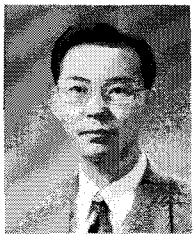
신 승 수(Seung-Soo Shin) **[정회원]**



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

<관심분야>
암호프로토콜, 무선 PKI, 네트워크 보안, USN, 스마트카드

한 군 희(Kun-Hee Han) **[종신회원]**



- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
RFID, 네트워크 보안, USN, 무선 PKI