한국산학기술학회논문지
Vol. 10, No. 3, pp. 572-578, 2009

스마트카드를 이용한 원격 시스템 사용자 인증 프로토콜

정민경[1], 신승수[1*], 한군희[2], 오상영[3]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부, [3]청주대학교 경영학부

Remote System User Authentication Scheme using Smartcards

Min-Kyoung Jeong[1], Seung-Soo Shin[1*], Kun-Hee Han[2] and Sang-Young Oh[3]
[1]**Dept. of Information Security, College of Information &Communication, Tongmyong University**
[2]**Division of Information & Communication Engineering, Baekseok University**
[3]**Department of Business Administration, Cheongju University**

요 약 2008년도에 Bindu et al.는 Chein et. al. 프로토콜이 내부자 공격과 중간자 공격에 취약하다고 지적하였다. 그리고 개선된 프로토콜을 제안하였다. 본 논문에서는 Bindu et al.이 제안한 프로토콜 역시 강한 서버/사용자 가장 공격과 제한된 재전송공격에 대해 취약하다는 것을 발견하고, 새로운 프로토콜을 제안하였다. 제안한 프로토콜에 대해서 강한 서버/사용자 가장 공격, 내부자 공격, 제한된 재전송 공격, 은밀한 검증자 공격, 전방향 안전성에 대해 분석하였다. 본 논문에서 제안된 프로토콜은 Bindu et al. 프로토콜보다 한 번의 연산이 추가되지만, 현대 컴퓨팅 기술로 인해 연산속도의 영향을 미치지 않으며, Bindu et al. 프로토콜에서 제기된 문제점을 해결하였다.

Abstract Bindu et al. pointed out that Chein et al. scheme is insecure insider attack and man-in-middle attack. And then they proposed new one. In the paper, However, Bindu et al's scheme also have some problems; It is strong masquerading server/user attack and restricted reply attack. Hence we proposed improved scheme. Finally, we completely had evaluated the one's security on strong masquerading server/user attack, Insider attack, Restricted attack, Stolen-verifier attack and Forward secrecy. In this paper, although proposed scheme includes more operation than Bindu et al. scheme, our scheme overcomes problems of Bindu et al. scheme by the operation that is light as not to influence on modern computing technology.

Key Words : Authentication, Password, Man-in-middle attack

1. 서론

최근 컴퓨터 네트워크의 급속한 발전에 따라 분산된 컴퓨팅 환경을 통한 원격 접속이 빈번히 이루어지고 있다. 원격 접속을 사용하기 위해서는 네트워크를 통해서 데이터를 주고받아야 한다. 이 때 악의적인 사용자에 의해서 네트워크상의 데이터가 도청 또는 불법적인 수정 등과 같은 공격에 노출되게 된다. 이러한 문제점을 해결하기 위해서 여러 가지 인증 기법에 대한 연구가 진행 되고 있다.

다양한 인증 기법 중에 하나인 개체 인증(Entity authentication)이란 한 개체가 다른 한 개체의 신원을 증명할 수 있도록 설계된 기술을 말한다[1].

개체인증의 방법 중 하나로 패스워드 기반 인증이 있으며, 스마트카드를 이용한 패스워드 기반 인증은 편리하고 효율적인 2-Factor 인증방식으로 다양한 분야에서 응용되고 있다[2].

초기 스마트카드 기반의 원격 사용자 인증 기법은 서버가 사용자를 검증하기 위하여 저장된 검증 테이블을 이용하였다[3]. 이후에는 서버가 사용자 아이디와 패스워드 관리를 위한 추가적인 비용부담 등을 줄이기 위하여 검증 테이블을 사용하지 않는 인증 기법에 대하여 연구되었다.

최근에는 개인 프라이버시 보호에 대한 관심이 증가되면서 사용자 익명성을 보호할 수 있는 스마트카드 기반 프로토콜에 대한 연구가 활발해졌다. 대표적으로 2004년

*교신저자: 신승수(shinss@tu.ac.kr)
접수일 09년 01월 19일 수정일 09년 02월 13일 게재확정일 09년 03월 23일

에 Das et al.[4]은 사용자 익명성을 제공하기 위하여 동적 아이디를 이용하는 프로토콜을 처음 제안하였다. 그리고 2005년에 Chien, Chen[5]은 Das et al[4] 프로토콜이 사용자 익명성을 보호하지 못한다는 문제점을 제기하고, 사용자 익명성을 제공하기 위한 새로운 프로토콜을 제안하였다. 2007년에는 Hu et al.[6]이 Chien and Chen 프로토콜은 강한 서버/사용자 가장 공격, 내부자 공격, 서비스 거부 공격, 제한된 재전송 공격 대한 문제점을 제기하였고, 새로운 프로토콜을 제안하였다. 2008년에는 Bindu et al.이 Chien and Chen 프로토콜은 중간자 공격과 내부자 공격에 대해 취약하다는 문제점을 제기하였다. 그리고 Bindu et al.은 새로운 프로토콜[2]을 제안하였다. 그러나 Bindu et al. 프로토콜은 강한 서버/사용자 가장 공격과 제한된 재전송 공격에 취약하다.

따라서 본 논문에서는 Bindu et al. 프로토콜의 문제점을 해결하기 위해 새로운 프로토콜을 제안하고, 제안한 프로토콜을 강한 서버/사용자 가장 공격, 내부자 공격, 제한된 재전송 공격, 전방향 안전성, 은밀한 검증자 공격 등에 대해 효율성과 안전성 측면에서 강한 서버/사용자 가장 공격과 제한된 재전송 공격에 강한 새로운 프로토콜에 대한 연구측면에서도 의미가 있다고 할 수 있다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 Bindu et al. 프로토콜의 구조 및 취약성을 분석한다. 3장에서는 새로운 프로토콜을 제안한다. 다음으로 4장에서는 제안된 프로토콜의 안전성 분석하고 Bindu et al. 프로토콜과 효율성을 비교분석한다. 마지막으로 5장에서 결론을 끝으로 본 논문을 마무리 짓고자 한다.

2. 관련연구

본 논문에서는 Bindu et al. 프로토콜에 대해 살펴보고, 강한 서버/사용자 가장 공격, 서비스 거부 공격, 제한된 재전송 공격, 사용자 익명성에 대해 분석한다.

2.1 Bindu et al. 프로토콜의 구조

Bindu et al. 프로토콜은 등록절차, 로그인 절차, 인증절차로 구성되어 있다. 본 논문에서는 [표 1]과 같은 표기법을 사용한다.

[표 1] 파라미터 표기법

기호	설 명
U	사용자
E	공격자
PW	사용자의 패스워드
ID	사용자의 식별자
S	원격 시스템
h( )	일방향 해쉬함수
x	S의 강한 비밀키
⊕	XOR 비트연산자
Ek[x]	키 k를 이용하여 x를 암호화
p, g	Diffie-Hellman의 공개 파라미터

[등록절차]

사용자가 원격 시스템에 등록을 하고자 할 때 다음과 같이 수행 한다.

Step 1. U는 등록을 위해 ID와 h(PW)를 S에게 전달한다.

Step 2. S는 $m = h(ID \oplus x) \oplus h(x) \oplus h(PW)$과 $I=h(ID \oplus x) \oplus x$을 계산한다.

Step 3. S는 U에게 스마트카드를 발행한다. 스마트카드에는 m, I 그리고 공개 파라미터인 h( )와 p를 포함한다.

[로그인 절차]

사용자 U가 원격시스템에 로그인을 원할 때, U는 자신의 스마트카드를 리더기에 삽입하고, ID와 PW를 입력한다.

Step 1. 스마트카드는 난수인 $r_u=g^a \bmod p$를 생성한다.

Step 2. $M=m \oplus h(PW)$을 계산한다.

Step 3. $C=M \oplus r_u$를 계산한다.

Step 4. $R=I \oplus r_u=h(ID \oplus x) \oplus x \oplus r_u$를 계산한다.

Step 5. U는 S에게 $\{C, T, E_R[r_u, ID, T]\}$ 메시지를 보낸다. 여기서 T는 타임스탬프이고, $E_R[r_u, ID, T]$은 비밀키 R을 이용하여 암호화한 암호문이다.

[인증절차]

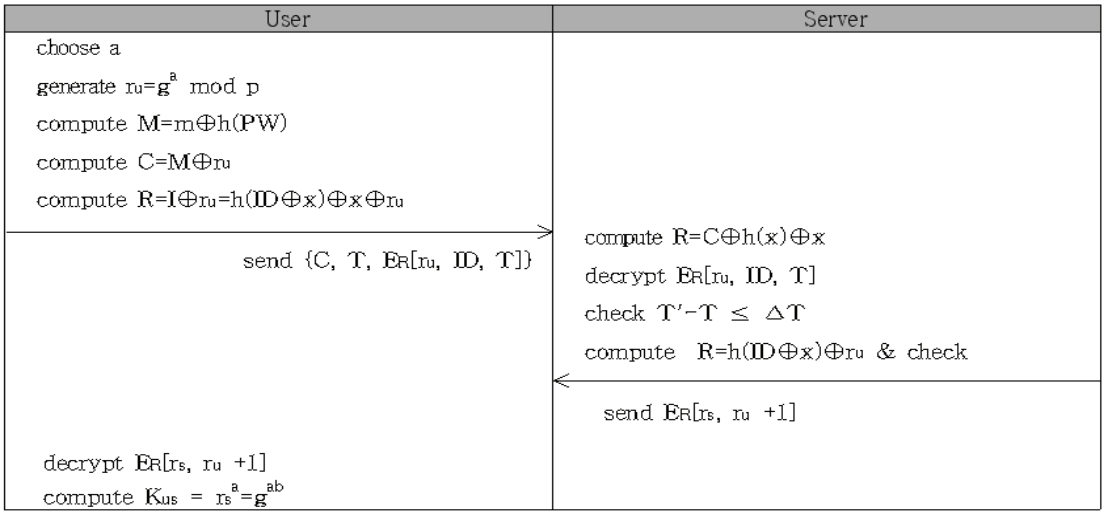
원격시스템은 사용자로부터 메시지를 받고 다음과 같이 수행하여 사용자에 대한 인증을 할 수 있다.

Step 1. S는 메시지를 받은 후, S의 비밀키 x를 이용하여 $R=C \oplus h(x) \oplus x$을 계산한다. 그리고 $E_R[r_u, ID, T]$ 메시지를 복호화한다.

Step 2. T와 T'과의 시간 간격의 유효성을 테스트한다. 여기서, T'은 S가 메시지를 받았을 때의 타임스탬프이다.

Step 3. 복호화된 $E_R[r_u, ID, T, N]$ 메시지의 값들을 이용하여 $R=h(ID \oplus x) \oplus r_u$을 계산하고, 받은 R값이 맞는지 검증한다.

Step 4. 서버는 U에게 $E_R[r_s, r_u +1]$ 메시지를 보낸다. 여기서 $r_s =g^b \bmod p$이다.



[그림 1] Bindu et al. 프로토콜 구조

Step 5. $E_R[r_s, r_u+1]$ 메시지를 받자마자, U는 복호화하여 r_u+1값이 포함이 되었는지 검사한다. 만약에 포함되었다면, U는 세션키 $K_{us} = r_s^a=g^{ab}$ 만들고, 세션키를 이용하여 S에게 서비스를 요청할 수 있다.

2.2 Bindu et al. 프로토콜의 취약성 분석

Bindu et al.은 Chien과 Chen 프로토콜[5]이 내부자 공격과 중간자 공격에 대해 취약하다고 지적하였고, 새로운 프로토콜을 제안하였다. 이 장에서는 Bindu et al. 프로토콜에서 발생하는 강한 서버/사용자 가장 공격, 서비스 거부 공격, 제한된 재전송 공격, 사용자 익명성과 같은 문제점에 대해 분석한다.

2.2.1 강한 서버/사용자 가장 공격

정당한 사용자인 공격자는 h(x)⊕x를 얻을 수 있고, 또한 공격자는 서버/사용자 가장 공격이 가능하다.

공격자 E를 정당한 사용자라고 가정하면, 다른 사용자의 스마트카드를 훔칠 필요가 없다. 왜냐하면 공격자 자신은 스마트카드의 h(x)⊕x=C⊕R또는 h(x)⊕x=M⊕I=m⊕h(PW)⊕I를 통해서 h(x)⊕x를 얻을 수 있기 때문이다. 다음으로 공격자는 네트워크를 통해서 사용자 U의 로그인 메시지 { C, T, $E_R[r_u, ID, T]$ }를 가로챌 수 있다. 그리고 E는 R=C⊕h(x)⊕x를 계산하고 $E_R[r_u, ID, T]$를 복호화할 수 있다.

만약에 E가 U의 {C, T, $E_R[r_u, ID, T]$ }의 통신을 가로챈다면, E는 위와 같은 계산 방법으로 U의 정확한 R과 r_u를 취득할 수 있기 때문에 S로 위장할 수 있고, E가 위조한 $E_R[r_s, r_u+1]$를 사용자에게 보낼 수 있다.

만약에 E가 U의 로그인 메시지 {C, T, $E_R[r_u, ID, T]$ } 가로 챈다면, E는 U의 확실한 R, ID, r_u를 위와 같은 방법으로 취득할 수 있기 때문에 S에 로그인하기 위해 U로 성공적으로 위장 할 수 있다.

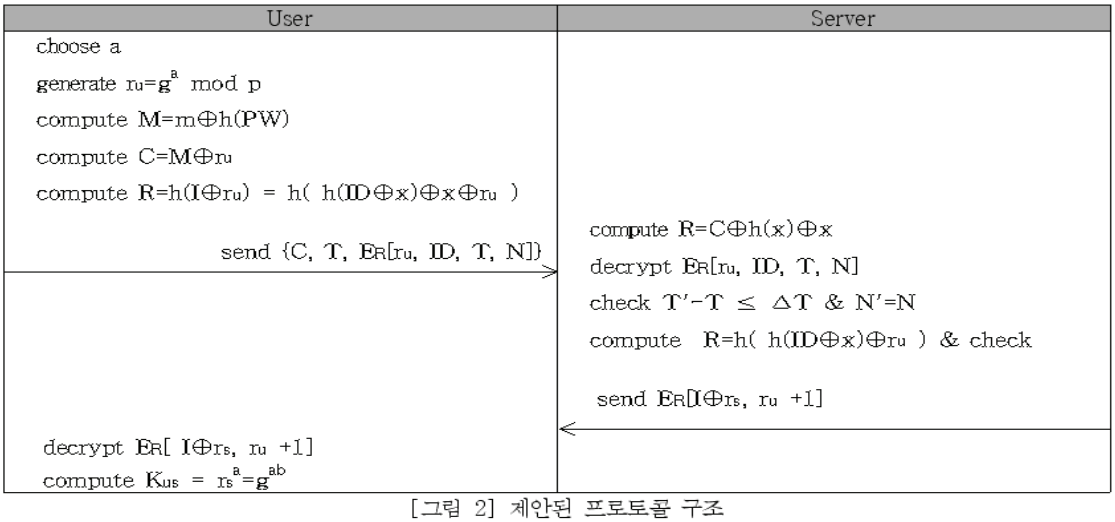
Bindu et al. 프로토콜은 정당한 사용자의 스마트카드에 저장된 비밀정보 또는 계산과정을 알아낼 경우 서버/사용자 가장 공격에 취약하다.

2.2.2 서비스 거부 공격

Bindu et al. 프로토콜은 요청 메시지의 유효성을 보장하기 위해 타임스탬프를 사용한다. 그리고 2.2.1절과 같이 Bindu et al 프로토콜에서는 공격자가 정당한 사용자라면 비밀키 R을 구할 수 있다. 그리고 공격자는 $E_R[r_u, ID, T]$를 네트워크로부터 얻을 수 있으며, 복호화 할 수 있다. 정당한 사용자인 공격자는 복호화된 타임스탬프 T 값을 바꾸고 서버에게 보낸다면, S가 인증 Step 2에서 타임스탬프 T에 대한 메시지를 검증할 수 없다. 서비스를 거부당한 실제 사용자 U가 다시 원격시스템에 접속을 시도하려 할 때, 공격자는 위와 같은 과정을 반복하여 계속적으로 원격시스템이 사용자에 대한 서비스를 거부하게 할 수 있다.

2.2.3 제한된 재전송 공격

Bindu et al. 프로토콜에서는 재전송 공격을 막기 위해서 타임스탬프 T를 이용한다. 타임스탬프 T는 인증 Step 2에서 검증되며, 일반적으로 타임스탬프를 이용하는 프



[그림 2] 제안된 프로토콜 구조

로토콜에서는 보낸 시간 T와 서버가 받은 시간 T' 간의 오차를 인정하기 위한 허용윈도우 ΔT 가 존재한다. 그리고 공격자는 허용윈도우 ΔT보다 짧은 시간 안에서 언제든지 같은 메시지를 재전송할 수 있으며, T' - T ≦ ΔT를 만족하는 T내에 모든 메시지는 인증 Step 2를 통과할 수 있다. 따라서 타임스탬프를 이용하는 프로토콜에서는 제한적인 시간이내에서 언제든지 재전송 공격이 가능하다[7].

2.2.4 사용자 익명성

익명성이란 사용자가 자신의 신원을 드러내지 않고 서비스나 리소스를 사용하는 것을 말한다[8]. 사용자 익명성을 제공하는 스마트카드 기반 프로토콜은 Das et al.에 의해서 제기되었으며, Bindu et al. 프로토콜도 사용자 익명성을 제공하기 위한 프로토콜 중 하나이다. 그러나 Bindu et al. 프로토콜에서는 비밀키 R값을 구할 수 있으며 비밀키 R값을 얻어낼 수 있는 정당한 공격자는 누구든지 사용자의 ID를 알 수 있으므로, Bindu et al. 프로토콜은 서버뿐만이 아니라 다른 참여자들에게도 사용자의 신원이 노출된다. 따라서 Bindu et al. 프로토콜은 사용자의 익명성을 보장하지 못한다.

3. 제안한 프로토콜

본 논문에서는 Bindu et al. 프로토콜의 문제점 중에서 강한 서버/사용자 가장 공격과 제한된 재전송 공격을 해결하기 위한 새로운 프로토콜을 제안한다. 제안한 프로토콜은 등록절차, 로그인절차, 인증절차로 구성된다.

[등록절차]

사용자가 원격시스템에 등록 또는 재등록하기를 원할 때 다음과 같이 수행한다.

Step 1. U는 등록을 위해 ID와 h(PW)를 S에게 전달한다.

Step 2. S는 $m=h(ID\oplus x)\oplus h(x)\oplus h(PW)$과 $I=h(ID\oplus x)\oplus x$을 계산한다.

Step 3. S는 U에게 스마트카드를 발행한다. 스마트카드에는 m, I 그리고 공개 파라미터인 h( )와 p를 포함한다.

[로그인절차]

사용자가 원격시스템에 로그인하고자 할 때, U 는 자신의 스마트카드를 리더기에 삽입하고, ID와 PW를 입력한다.

Step 1. 스마트카드는 난수인 $r_u=g^a \bmod p$를 생성한다.

Step 2. $M=m\oplus h(PW)$을 계산한다.

Step 3. $C=M\oplus r_u$를 계산한다.

Step 4. $R=h(I\oplus r_u) = h(h(ID\oplus x)\oplus x\oplus r_u)$를 계산한다.

Step 5. U는 S에게 {C, T, E_R[r_u, ID, T, N]} 메시지를 보낸다. 여기서 T는 타임스탬프이고, N은 타임스탬프를 일정한 카운터로 나눈 계수기의 값이다. E_R[r_u, ID, T, N]은 비밀키 R을 이용하여 암호화한 암호문이다. 이 때, 사용자는 이전 메시지와 현재 메시지가 허용윈도우 시간내의 범위를 초과한다면 계수기의 값을 0으로

한다.

로그인 절차에서 제안한 프로토콜은 강한 서버/사용자 가장 공격을 해결하기 위해 한 번의 해시 연산을 더 사용하여 R을 계산한다.

[인증절차]

사용자로부터 메시지를 받은 후 원격시스템은 다음과 같은 단계를 통하여 사용자가 정당한 사용자인지 인증하는 절차이다.

Step 1. S는 메시지를 받은 후, S의 비밀키 x를 이용하여 $R=C\oplus h(x)\oplus x$을 계산한다. 그리고 $E_R[r_u$, ID, T, N] 메시지를 복호화한다.

Step 2. T와 T'과의 시간 간격의 유효성을 테스트한다. 여기서, T'은 S가 메시지를 받았을 때의 타임스탬프이다. 그리고 U가 보낸 N값과 S의 N'값을 비교하여 두 값이 같으면 메시지를 허용한다.

Step 3. 복호화된 $E_R[r_u$, ID, T] 메시지내의 값들을 이용하여 $R=h(\ h(ID\oplus x)\oplus r_u\ )$을 계산하고, 받은 R값이 맞는지 검증한다. 검증에 실패하면, 서비스 요청을 거절한다.

Step 4. 서버는 U에게 $E_R[I\oplus r_s$, r_u +1] 메시지를 보낸다. 여기서 $r_s = g^b \bmod p$이다.

Step 5. $E_R[\ I\oplus r_s$, r_u +1] 메시지를 받자마자, U는 복호화하여 ru +1값이 포함이 되었는지 아닌지를 검사한다. 만약에 포함되었다면, U는 세션키 $K_{us} = r_s^a = g^{ab}$ 만들고, 세션키를 이용하여 S에게 서비스를 요청한다.

Step 6. U와 S는 허용윈도우 내의 계수기 값 N을 N+1로 초기화 한다.

공격자가 서버로 가장하는 것을 해결하기 위해 ru +1을 암호화하여 인증을 수행한다.

4. 안전성 평가 및 비교분석

본 장에서는 제안한 프로토콜의 안전성을 분석하고, 최근에 지속적인 문제로 제기되고 있는 강한 서버/사용자 가장 공격을 포함하여 내부자 공격, 제한된 재전송 공격, 전방향 안전성, 은밀한 검증자 공격과 같은 문제점에 대해서 분석한다. 그리고 제안한 프로토콜과 Bindu et al. 프로토콜을 기능적인 측면과 성능적인 측면에서 비교분석하였다.

4.1 제안 프로토콜의 안전성 평가

본 논문에서 제안한 프로토콜에 대한 강한서버/사용자 공격, 내부자공격, 제한된 재전송 공격, 전방향 안전성, 은밀한 검증자 공격 등에 대하여 안전성을 평가한다.

4.1.1 강한 서버/사용자 가장 공격

정당한 사용자인 공격자 E는 $h(x)\oplus x = C\oplus R$ 또는 $h(x)\oplus x=M\oplus I=m\oplus h(PW)\oplus I$를 계산할 수 있다. 또한 공격자는 U의 로그인 요청 메시지 {C, T, $E_R[r_u$, ID, T, N]}를 가로챌 수 있고, $R = C\oplus h(x)\oplus x$을 계산할 수 있다. 그리고 $E_R[r_u$, ID, T, N]를 복호화 할 수 있게 된다. 공격자는 U의 ID와 r_u를 알아내서 서버에게 사용자로 가장할 수 있다. 그러나 공격자는 사용자의 I값을 알지 못하므로 인증 Step 4의 $E_R[I\oplus r_s$, r_u +1]을 만들 수 없기 때문에 사용자에게 서버로 가장할 수 없다. 따라서 제안한 프로토콜은 강한 사용자/서버 가장 공격에 안전하다.

4.1.2 내부자 공격

내부자 공격이란 올바른 경로로 서버에 등록된 사용자가 공격하는 것을 말한다[9]. 제안한 프로토콜에서는 사용자의 PW를 해시함수를 통해 해시한 값만을 서버에 등록하기 때문에 서버의 내부자라 할지라도 사용자의 PW를 알 수 없으므로 내부자 공격을 막을 수 있다.

4.1.3 제한된 재전송 공격

타임스탬프를 이용한 방법은 허용윈도우 △T의 시간 동안에 공격시도가 가능하다[10]. 그래서 제안한 프로토콜에서는 허용윈도우 △T를 다시 계수기 N값으로 나누어 재전송 공격을 막을 수 있다. 만약 공격자가 사용자의 메시지를 가로채어 허용윈도우 △T 내에 메시지를 재전송하더라도 서버와 사용자는 허용윈도우 내의 같은 계수기 값을 알고 있기 때문에 재전송 공격에 성공할 수 없다. 이 때 서버는 계수기 N값을 허용윈도우 △T 내의 시간동안만 사용하며, △T 시간이 바뀌면 계수기 N값은 소멸하게 된다. 즉, 검증테이블이 존재하지 않을 시에는 N값이 0임을 의미한다.

4.1.4 전방향 안전성

공격자가 U의 개인키나 패스워드를 알아냈다고 해도 이전에 U가 사용했던 어떠한 세션의 키도 알 수 없을 경우 프로토콜이 전방향 안전성을 만족한다고 한다[9]. 제안한 프로토콜에서는 Bindu et al 프로토콜과 마찬가지로 Diffie-Hellman 키 교환 프로토콜[11]에 의존하여 키를 교환하기 때문에 전방향 안전성을 만족한다.

4.1.5 은밀한 검증자 공격

은밀한 검증자 공격은 서버로부터 사용자에 대한 정보를 얻을 수 없을 때 만족하게 된다[12]. 제안한 프로토콜에서는 계수기 값을 사용하여 허용윈도우 시간 내에서만 해당 사용자의 검증테이블을 사용한다. 그러나 사용되는 검증테이블의 정보를 알아내더라도 허용윈도우 시간을 초과하면 이 정보는 사용할 수 없는 정보이기 때문에 이 공격에 안전하다.

4.2 기존 프로토콜과의 비교분석

본 논문에서 제안한 프로토콜과 Bindu et al. 프로토콜의 강한 서버/사용자 가장 공격, 제한된 재전송 공격 등에 대한 효율성과 안전성에 대해 비교분석하였다.

4.2.1 효율성

효율적인 측면에서, Bindu et. al 프로토콜은 등록절차에서 해시연산 3번과 XOR 연산 4번이 필요하고, 로그인 절차는 암호연산 1번, XOR연산 3번, 해시연산 1번, 지수연산 1번과 인증절차에서 해시연산 2번, XOR연산 3번, 암호연산 1번, 지수연산 2번이 필요하다. 제안프로토콜의 등록절차와 인증절차는 Bindu et. al 프로토콜과 마찬가지로 등록절차에서 해시연산 3번과 XOR 연산 4번이 필요하고, 인증절차에서 해시연산 2번, XOR연산 3번, 암호연산 1번, 지수연산 2번이 필요하지만, 로그인 절차는 암호연산 1번, XOR연산 3번, 해시연산 2번, 지수연산 1번이 필요하다. 이와같이 제안한 프로토콜이 로그인 절차에서 Bindu et. al 프로토콜에 비해 1번의 해시 연산을 더 수행한다. 하지만 로그인 절차는 사용자가 계산하는 절차이고, 서비스거부공격 등과 같은 공격의 대상이 되는 서버가 계산하지 않으므로, 서버에 과부하를 주지 않는다. 그리고 해시연산은 비트연산으로 구성되기 때문에 현대 컴퓨팅 기술에 비추어 볼 때, 연산 수행 속도에는 전혀 영향을 미치지 않는다. 다음 [표 2]는 제안한 프로토콜과 Bindu et al. 프로토콜과의 효율성을 비교했다.

[표 2] Bindu et al 프로토콜과의 효율성 비교

	Bindu et al	제안 프로토콜
등 록	3h, 4⊕	3h, 4⊕
로그인	1E, 3⊕, 1h, 1p	1E, 3⊕, 2h, 1p
인 증	2h, 3⊕, 1E, 2p	2h, 3⊕, 1E, 2p

h : 해시함수 수행 연산, E : 암호화 수행,
⊕ : 비트연산자 XOR, p : 지수승 연산

4.2.2 안전성

이 절에서는 위장공격, 내부자공격, 재전송공격, 전방향안전성, 은밀한 검증자에 대한 안전성을 비교분석한다. 기존 프로토콜인 Bindu et al. 프로토콜은 강한 서버/사용자 가장 공격, 제한된 재전송 공격에 대해 취약하지만, 제안된 프로토콜은 이러한 공격에 대해 안전성이 뛰어나다. 따라서 제안한 프로토콜은 로그인 단계에서 한 번의 해시 연산을 더 수행하여 Bindu et al. 프로토콜에서 제기된 강한 서버/사용자 가장 공격, 제한된 재전송 공격에 대한 문제점에 대해 안전하다. 기존 프로토콜과 제안한 프로토콜에 대한 안전성 비교는 다음 [표 3]과 같다.

[표 3] Bindu et al 프로토콜과의 안전성 비교

	Bindu et al	제안프로토콜
위장공격	X	O
내부자 공격	O	O
재전송 공격	X	O
전방향 안전성	O	O
은밀한 검증자	O	O

X : 공격에 안전하지 않음, O : 공격에 대해 안전함

5. 결론

Bindu et al.은 Chien et al. 프로토콜에 대하여 안전성을 평가하고, 강한 서버/사용자 공격에 취약하다는 것을 보였다. 그리고 Bindu et al.은 새로운 프로토콜을 제안하였다. Bindu et. al 프로토콜은 서버에 등록된 정당한 사용자라면 모든 정보를 알 수 있고 중간자 공격이 가능하다. 따라서 인증을 할 때 공격자가 세션을 가로챌 수 있다.

본 논문에서는 Bindu et al.이 제안한 프로토콜 또한 강한 서버/사용자 가장 공격과 제한된 재전송 공격에 취약하다는 것을 보이고 강한 서버/사용자 가장 공격과 제한된 재전송 공격에 대해 안전한 프로토콜을 제안하였다. 제안한 프로토콜은 Bindu et al. 프로토콜보다 한 번의 연산이 추가되지만, 이 연산은 현대 컴퓨팅 기술을 생각할 때 많은 영향을 주지 않을 정도로 가벼운 연산이다. 따라서 제안한 프로토콜은 강한 서버/사용자 가장 공격, 내부자 공격, 제한된 재전송 공격, 전방향 안전성, 은밀한 검증자 공격에 대한 기능성이 뛰어나다. 본 논문에서 제안한 프로토콜은 스마트카드를 이용한 키 교환 및 다양한 응용 분야에서 사용될 수 있을 것으로 예상된다.

참고문헌

[1] Behrouz A. Forouzan, “암호학과 네트워크 보안”, McGraw-Hill Korea, pp. 433-455, 2008.1.

[2] C.Shoba Bindu, P. Chandra Sekhar Reddy, and B.Satyanarayana, "Imporoved Remote User Authentication Scheme Preserving User Anonymity," IJCSNS, Vol.8, No.3, 2008.3.
[3] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.
[4] Manik Lal Das, Ashutosh Sacena, and Ved P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme," IEEE Trans. on Consumer Electronics, Vol.50, No.2, pp. 629-631, 2004.
[5] H.Y. Chien and C.H. Chen, "A remote authentication scheme preserving user," IEEE AINA'05, Vol.2, pp. 245-248, 2005.
[6] Lanlan Hu, Yixian Yang, and Xinxin Niu, "Improved Remote User Authentication Scheme Preserving User Anonymity," IEEE CNSR'07, pp. 323-328, 2007.
[7] L.Gong, "A security risk of depending on synchronized clocks," Operating System Review, Vol.26, No.1, pp. 49-53, 1992.
[8] 김세일, 천지영, 이동훈, "추적이 가능한 스마트카드 사용자 인증 기법", 한국정보보호학회, 제18권, 제5호, pp. 31-39, 2008.10.
[9] 김용훈, 윤택영, 박영호, "서버의 개입이 없는 스마트카드 기반의 3자간 키 교환 프로토콜", 한국정보보호학회, 제18권, 제2호, 2008.4.
[10] 정연오, 김주배, 김현석, 최진영, "안전성과 효율성을 고려한 스마트카드 기반 사용자 인증 프로토콜 분석", 한국정보과학회, 제35권, 제2호, 2008.10.
[11] W.Diffie, M.E.Hellman, "New directions in cryptography," IEEE Trans, Vol.IT-22, No.6, pp. 644-654, 1976.
[12] 유혜정, 이현숙, "스마트카드를 이용한 속성기반 사용자 인증 스킴", 한국정보보호학회, 제18권, 제5호, pp. 41-47, 2008.10.

정 민 경(Min-Kyoung Jeong) **[준회원]**

- 2006년 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 컴퓨터공학과 (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

오 상 영(Sang-Young Oh) **[종신회원]**

- 2001년 2월 : 충북대학교 경영학과 (경영학박사)
- 2006년 3월 ~ 현재 : 청주대학교 경영학부 교수

<관심분야>
KMS, 혁신이론, System Thinking, e-Biz, BSC, EC