안전성이 향상된 스마트카드 기반 원격 사용자 인증 프로토콜

박대식*, 곽 진**

요약

원격 사용자 인증 기술은 1981년 Lamport 에 의해 제안된 이래로 다양한 연구를 통해 지속적으로 발전되어 왔다. 2008년 Bindu 등은 Chien 등의 프로토콜이 중간자 공격과 내부자 공격에 취약하다는 문제점을 제기하고 새로운 프로토콜을 제안하였다. 그러나 Bindu 등의 인증 프로토콜은 강한 서버/사용자 위장 공격, 서비스 거부 공격, 제한적 재전송 공격 등에 취약하다. 따라서 본 논문에서는 Bindu 등의 인증 프로토콜이 가지는 취약점을 해결할 수 있는 안전성이 향상된 스마트카드 기반 원격 사용자 인증 프로토콜을 제안한다.

Smartcard-based Remote User Authentication Protocol with Improved Security

Dae-Sik Park*, Jin Kwak**

ABSTRACT

Remote user authentication methods has been continuously developed on the basis of the various researches. In 2008, Bindu et al. pointed out that Chien et al.'s protocol has security weaknesses in the man-in-the-middle attack and the insider attack. And then Bindu et al. proposed new protocol. However Bindu et al.'s protocol was found some weaknesses about strong masquerading user/server attack, DoS attack and restricted reply attack. In this paper, we propose an smartcard-based remote user authentication protocol with improved security functions which can remove vulnerabilities of Bindu et al.'s protocol.

Keywords : Remote User Authentication, Strong Masquerading Attack, DoS Attack, Reply Attack, Authentication Protocol

* 순천향대학교 정보보호학과(✉ dspark@sch.ac.kr)
· 제1저자(First Author) : 박대식 · 교신저자(Correspondent Author) : 곽 진
· 접수일(2011년 6월 24일), 수정일(1차 : 2011년 7월 22일), 게재확정일(2011년 7월 25일)

Ⅰ. 서 론

최근 컴퓨터 네트워크의 발전에 따라 분산된 컴퓨팅 환경에서 원격 서버로 접속하는 일이 빈번히 이루어지고 있으며 이러한 원격 서버로 접속하기 위해서는 안전한 원격 사용자 인증 기술이 요구된다. 원격 사용자 인증 기술이 적용되지 않은 원격 접속 방식은 악의적인 공격자에 의한 데이터 도청, 위변조 등과 같은 공격에 쉽게 노출될 수 있기 때문에 이러한 문제점들을 해결하기 위해 원격 사용자 인증 기술에 대한 다양한 연구가 진행되어 왔다.

원격 사용자 인증 기술은 1981년 Lamport에 의해 처음으로 제안되었으며 이를 시작으로 인증 기술의 효율성 및 안전성을 향상시키기 위해 지속적으로 연구가 수행되었다[1].

초기에 제안된 스마트카드 기반 원격 사용자 인증 기술은 서버에서 검증 테이블을 기반으로 사용자를 검증하는 방식이었다[2, 3]. 그러나 이러한 방식은 공격자가 검증 테이블에 대한 정보를 취득하게 되는 경우, 시스템의 취약점을 이용한 공격이 가능하다는 것이 밝혀짐에 따라 서버에서 검증 테이블을 저장하지 않는 형태로 발전되었다[4-7].

이후 1991년 Chang과 Wu에 의해 제안된 패스워드와 스마트카드를 이용한 원격 사용자 인증 기술을 바탕으로 지속적으로 연구가 진행되어 왔으며[8] 2004년 Das 등은 사용자 익명성을 제공하기 위해 동적 아이디 기반 인증 기술을 제안하였다[9]. 그러나 Chien 등은 Das 등의 인증 프로토콜이 로그인 단계에서 서버로 전송되는 데이터를 통해 사용자의 익명성을 제공하지 못함을 지적하였고 이를 개선한 프로토콜을 제안하였다[10]. 2007년에는 Hu 등은 Chien 등의 프로토콜이 강한 서버/사용자 위장 공격, 내부자 공격 등에 취약하다는 문제점을 제기하고 새로운 프로토콜을 제안하였다[11]. 2008년 Bindu 등은 Chien 등의 프로토콜이 중간자 공격과 내부자 공격에 대해 취약하다는 문제점을 제기하고 새로운 프로토콜을 제안하였다[12]. 그러나 Bindu 등의 프로토콜은 강한 서버/사용자 위장 공격, 서비스 거부 공격, 제한적 재전송 공격에 취약하다.

따라서 본 논문에서는 Bindu 등의 프로토콜의 문제점을 해결하기 위해 안전성이 향상된 스마트카드 기반 원격 사용자 인증 프로토콜을 제안한다.

Ⅱ. Bindu 등의 인증 프로토콜 및 안전성 분석

본 장에서는 Bindu 등의 인증 프로토콜 및 안전성을 분석한다.

본 논문에서 사용되는 표기법은 Bindu 등의 인증 프로토콜에서 사용한 표기법을 적용하며 이는 다음과 같다.

2.1 용어 정의

본 논문에서 사용되는 표기법은 Bindu 등의 인증 프로토콜에서 사용한 표기법을 적용하며 이는 다음과 같다.

- U : 사용자
- PW : 사용자의 패스워드
- ID : 사용자의 아이디
- S : 원격 서버
- $h(\cdot)$: 일방향 해쉬 함수
- $\oplus$: XOR 연산
- $E_k[x]$: 대칭키 k를 이용하여 x를 암호화
- $D_k[x]$: 대칭키 k를 이용하여 x를 복호화
- x : 서버의 비밀키
- N : 랜덤 넌스
- T : 타임스탬프(time stamp)
- r_u, r_s : 난수
- g : 순환군 Z_p의 생성자

- p : 1024-bit 소수
- SK_{us} : 세션키

2.2 Bindu 등의 인증 프로토콜

Bindu 등의 인증 프로토콜은 등록 단계, 로그인 단계, 인증 단계로 구성되어 있다. 등록 단계는 사용자 등록 시, 안전한 통신을 위해 최초 1회만 수행되며 로그인 단계 및 인증 단계는 시스템에 접근할 때마다 수행된다.

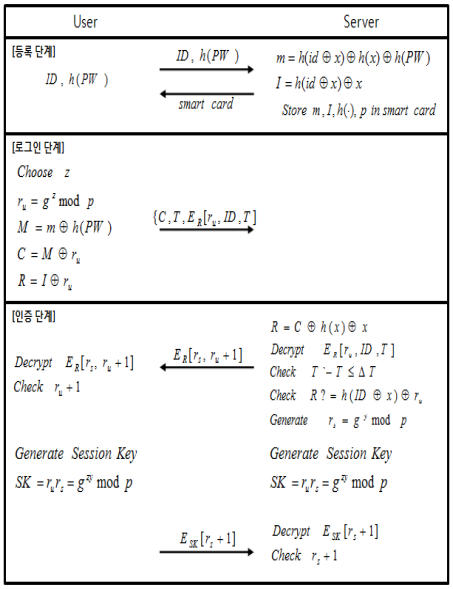


그림 1. Bindu 등의 인증 프로토콜
Fig 1. Bindu et al.'s authentication protocol

2.2.1 등록 단계

본 단계에서는 원격 서버에 사용자를 등록하는 단계이며 이는 다음과 같다.

① 사용자는 등록을 위해 ID와 h(PW)를 서버로 전송한다.
② 서버는 m=h(ID⊕x)⊕h(x)⊕h(PW)와 I=h(ID⊕x)⊕x를 계산한다.
③ 서버는 m, I, 공개 파라미터 h(), P 값이 저장된 스마트카드를 사용자에게 발행한다.

2.2.2 로그인 단계

본 단계에서는 등록이 완료된 사용자가 원격 서버에 로그인하는 단계이며 로그인은 사용자가 발급받은 스마트카드를 리더기에 삽입하고 ID 및 패스워드 입력하면 스마트카드는 다음과 같은 연산을 수행한다.

① 스마트카드는 난수를 r_u를 생성한다.
$$r_u=g^z \bmod p$$
② M=m⊕h(PW)를 계산한다.
③ C=M⊕r_u를 계산한다.
④ R=I⊕r_u를 계산하고 사용자의 로그인 메시지 {C, T, E_R[r_u, ID, T]}를 서버에 전송한다.

2.2.3 인증 단계

본 단계에서는 사용자의 로그인 메시지를 전송받은 원격 서버에서 사용자에 대한 인증을 수행하는 단계이며 이는 아래와 같다.

① 서버는 로그인 메시지를 복호화하기 위해 서버의 비밀키 x를 이용해 R=C⊕h(x)⊕x를 계산하고 E_R[r_u, ID, T]를 복호화한다.
② 서버는 ⊿T≥T'-T를 계산하여 타임스탬프를 확인한다. T'은 서버가 로그인 메시지를 전송받았을 때의 타임스탬프이며 ⊿T는 로그인 메시지 전송시간을 고려한 최소 인증시간이다.
③ 복호화된 로그인 메시지 E_R[r_u, ID, T]를 이용해 R=h(ID⊕x)⊕x⊕r_u을 계산하고 검증한다.
④ 서버는 난수 r_s를 생성하고 사용자에게 메시지 {E_R[r_s, r_u+1]}을 전송한다.
$$r_s=g^y \bmod p$$
⑤ 사용자는 메시지 {E_R[r_s, r_u+1]}을 복호화하여

r_u+1이 메시지에 포함되어 있는지 확인한다.

⑥ 사용자는 서버와 통신한 세션키를 생성하고 서버에 $E_{Kus}[r_s+1]$을 전송한다.

$$K_{us}=r_s^{z}=g^{yz} \bmod p$$

⑦ 서버는 메시지 $E_{Kus}[r_s+1]$을 복호화하여 r_s+1을 확인하고 서비스를 제공한다.

2.3 Bindu 등의 인증 프로토콜의 안전성 분석

Bindu 등의 인증 프로토콜은 강한 서버/사용자 위장 공격, 서비스 거부 공격, 제한적 재전송 공격과 같은 취약점들을 내포하고 있으며 본 장에서는 이러한 취약점들을 분석한다.

2.3.1 강한 서버/사용자 위장 공격

공격자가 정당한 사용자로써 스마트카드를 발급 받는다면 공격자는 자신의 스마트카드를 통해 $h(x)\oplus x=C\oplus R$ 혹은 $h(x)\oplus x=M\oplus I$를 계산하여 $h(x)\oplus x$를 얻을 수 있다. 이를 통해 공격자는 사용자 위장 공격 및 서버 위장 공격이 가능하다.

- 사용자 위장 공격

공격자는 다음과 같이 사용자 위장 공격을 수행할 수 있다.

① 공격자는 사용자의 로그인 요청 메시지 {C, T, $E_R[r_u, ID, T]$}를 획득한다.

② 공격자는 사전에 획득한 $h(x)\oplus x$를 이용하여 $R=C\oplus h(x)\oplus x$를 계산한다.

③ R을 이용해 $E_R[r_u, ID, T]$를 복호화하여 사용자의 ID를 추출하여 사용자로 위장하여 서버에 로그인할 수 있다.

- 서버 위장 공격

공격자는 다음과 같이 서버 위장 공격을 수행할 수 있다.

① 공격자는 사용자의 로그인 요청 메시지 {C, T, $E_R[r_u, ID, T]$}를 획득한다.

② 공격자는 사전에 획득한 $h(x)\oplus x$를 이용하여 $R=C\oplus h(x)\oplus x$를 계산한다.

③ 공격자는 서버의 메시지 {$E_R[r_s, r_u+1]$}을 복호화하여 이를 통해 서버로 위장할 수 있다.

2.3.2 서비스 거부 공격

Bindu 등의 인증 프로토콜은 타임스탬프를 사용하여 요청 메시지의 유효성을 보장하고 있다. 그러나 앞서 분석한 바와 같이 공격자가 정당한 사용자의 경우 암호화키 값인 R을 연산할 수 있다. 이를 통해 공격자는 사용자의 로그인 메시지 {C, T, $E_R[r_u, ID, T]$}를 획득한 후, 임의의 타임스탬프 T′을 삽입하여 서버에 전송한다. 서버에서는 타임스탬프 T에 대한 메시지를 검증할 수 없기 때문에 서비스를 거부하게 된다.

2.3.3 제한적 재전송 공격

Bindu 등의 인증 프로토콜은 타임스탬프를 사용하여 요청 메시지의 유효성을 보장하고 있다. 그러나 공격자가 로그인 요청 메시지 {C, T, $E_R[r_u, ID, T]$}를 획득한 후 사용자로 위장하여 서버에 재전송을 하게 되면 서버는 $\Delta T \geq T'-T$가 허용되는 한 로그인 요청을 무조건 받아들일 수 있다. 따라서 공격자는 ΔT시간 이내에서는 재전송 공격이 가능하다.

III. 제안 인증 프로토콜

본 논문에서 제안하는 인증 프로토콜은 Bindu 등의 인증 프로토콜의 취약점을 해결할 수 있는 인증 프로토콜을 제안한다.

제안 프로토콜은 Bindu 등의 인증 프로토콜과 동일하게 등록 단계, 로그인 단계, 인증 단계로 동작한다.

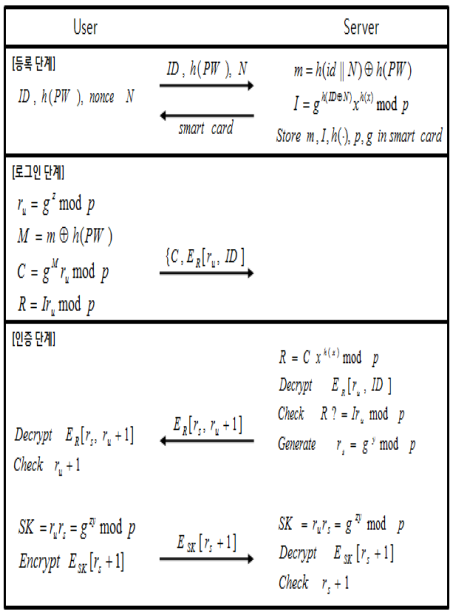


그림 2. 제안하는 인증 프로토콜
Fig 2. Proposed authentication protocol

3.1 등록 단계

본 단계에서는 원격 서버에 사용자를 등록하는 단계이며 이는 다음과 같다.

① 사용자는 등록을 위해 ID, h(PW)를 선택하고 N을 생성하여 서버로 전송한다.
② 서버는 아래와 같이 m과 I를 계산한다.

$$m=h(ID||N)\oplus h(PW)$$
$$I=g^{h(ID\oplus N)}x^{h(x)} \bmod p$$

③ 서버는 m, I, 공개 파라미터 h(·), p, g 값이 저장된 스마트카드를 사용자에게 발행한다.

3.2 로그인 단계

본 단계에서는 등록이 완료된 사용자가 원격 서버에 로그인하는 단계이며 로그인은 사용자가 발급받은 스마트카드를 리더기에 삽입하고 ID 및 패스워드를 입력하면 스마트카드는 다음과 같은 연산을 수행한다.

① 스마트카드는 난수를 r_u를 생성한다.

$$r_u=g^z \bmod p$$

② M=m⊕h(PW)를 계산한다.
③ $C=g^M r_u \bmod p$를 계산한다.
④ $R=Ir_u \bmod p$를 계산하고 사용자의 로그인 메시지 {C, $E_R[r_u, ID]$}를 서버에 전송한다.

3.3 인증 단계

본 단계에서는 사용자의 로그인 메시지를 전송받은 원격 서버에서 사용자에 대한 인증을 수행하는 단계이며 이는 아래와 같다.

① 서버는 로그인 메시지를 복호화하기 위해 서버의 비밀키 x를 이용해 R을 계산하고 $E_R[r_u, ID]$를 복호화하여 이를 검증한다.

$$R=C\,x^{h(x)} \bmod p$$

② 서버는 난수 r_s를 생성하고 사용자에게 메시지 {$E_R[r_s, r_u+1]$}을 전송한다.

$$r_s=g^y \bmod p$$

③ 사용자는 메시지 {$E_R[r_s, r_u+1]$}을 복호화하여 r_u+1이 메시지에 포함되어 있는지 확인한다.
④ 사용자는 서버와 통신할 세션키 K_{us}를 생성하고 서버에 $EK_{us}[r_s+1]$을 전송한다.

$$K_{us}=r_u r_s=g^{zy} \bmod p$$

⑤ 서버는 메시지 $E_{Kus}[r_s+1]$을 복호화하여 r_s+1을 확인하고 서비스를 제공한다.

Ⅳ. 안전성 분석

4.1 강한 서버/사용자 위장 공격

기존의 Bindu 등의 인증 프로토콜은 정당한 사용자로써 공격을 시도하는 공격자가 자신의 스마트카드의 정보를 통해 h(x)⊕x를 획득할 수 있기 때문에 강한 서버/사용자 위장 공격에 취약하였다.

본 논문에서 제안한 프로토콜은 $R=Ir_u \bmod p$를 통해 암호화를 수행하며 $R=C\,x^{h(x)} \bmod p$를 통해 복호화를 수행한다. 또한 암호화에 사용되는 r_u는 스마트카드에서 생성하는 임의의 난수로써 각각의 세션마다 다른 난수가 사용된다.

이를 통해 공격자가 정당한 사용자로써 자신의 스마트카드를 이용하여 내부 정보를 획득하여도 매 세션마다 새로운 난수가 생성되고 이를 통해 모듈러 연산이 수행되기 때문에 공격자는 r_u 및 $h(x)$ 값을 취득할 수 없다. 따라서 제안된 프로토콜은 강한 서버/사용자 위장 공격에 안전하다.

4.2 서비스 거부 공격

제안 프로토콜에서는 타임스탬프를 사용하지 않으므로 Bindu 등의 프로토콜에서 적용되었던 타임스탬프를 이용한 서비스 거부 공격에 안전하다.

제안 방식은 타임스탬프를 사용하지 않기 때문에 일정 시간의 지체가 있다 하더라도 합법적인 사용자에 대한 서비스를 순차적으로 처리해 줄 수 있다.

4.3 재전송 공격

제안 프로토콜에서는 매 로그인마다 난수 r_u, r_s를 생성하므로 공격자가 이전 세션에서 사용된 메시지를 이용하여 재전송 공격이 불가능하다.

만약 공격자가 로그인 요청 메시지 $\{C, E_R[r_u, ID]\}$를 획득하여 재전송하더라도 공격자는 난수 r_u, r_s를 알 수 없기 때문에 검증 단계에서 사용자 인증 메시지인 $E_R[r_s+1]$을 계산할 수 없으므로 인증 과정을 통과할 수 없다. 또한 제안 프로토콜에서는 타임스탬프를 사용하지 않으므로 Bindu 등의 프로토콜에서 취약한 제한적 재전송 공격에 대해서도 안전하다.

표 1. 안전성 분석
Table 1. Security Analysis

구분	Bindu 등의 프로토콜	제안 프로토콜
강한 사용자/서버 위장 공격	X	O
서비스 거부 공격	X	O
재전송 공격	X	O

O : 공격에 안전함
X : 공격에 안전하지 않음

Ⅴ. 효율성 분석

표 2.는 Bindu 등의 인증 프로토콜과 본 논문에서 제안한 인증 프로토콜의 효율성을 비교 분석한 것이다.

표 2. 효율성 분석
Table 2. Efficiency Analysis

구분		Bindu 등의 프로토콜	제안 프로토콜
로그인 단계	사용자	1M, 1H, 1S, 3X	3M, 1H, 1S, 1X
	서버	-	-
인증 단계	사용자	1M, 2S	1M, 2S
	서버	2M, 3S, 2X	4M, 1H, 3S

M : 지수 연산
H : 해쉬 연산
S : 대칭키 암호화/복호화
X : XOR 연산

표 2.에서 볼 수 있듯이 본 논문에서 제안한 프로토콜은 로그인 단계에서 3번의 지수 연산, 1번의 해쉬 연산, 1번의 암호화 연산이 필요하며 인증 단계에서는 사용자가 1번의 지수 연산, 2번의 암호화/복호화 연산이 필요하며 서버는 4번의 지수 연산, 1번의 해쉬 연산, 3번의 암호화/복호화 연산이 필요하다.

XOR 연산은 지수 연산에 비해 연산 속도가 매우 빠르기 때문에 지수 연산을 수행하지 않는 Bindu 등의 프로토콜은 제안 프로토콜에 비해 연산 속도는 매우

빠르지만 앞서 분석한 바와 같이 안전성 부분에서는 매우 취약한 것으로 나타났다.

기존의 Bindu 등의 프로토콜은 로그인 정보를 암호화하는데 XOR 연산을 통해 수행하였으나 XOR 연산의 특성으로 인해 강한 사용자/서버 위장 공격 등에 취약하다. 따라서 본 논문에서는 XOR 연산이 아닌 지수 연산을 사용함으로써 이러한 취약점들을 해결하였다.

지수 연산은 XOR 연산에 비해 처리 속도에 따른 효율성은 떨어지지만 지속적으로 발전하는 스마트카드 및 서버의 성능을 고려한다면 충분히 수행될 수 있다.

Ⅵ. 결 론

본 논문에서는 Bindu 등이 제안한 프로토콜이 강한 사용자/서버 공격, 서비스 거부 공격과 제한적 재전송 공격에 취약하다는 것을 분석하고 이를 해결할 수 있는 스마트카드 기반 원격 사용자 인증 프로토콜을 제안하였다.

제안한 기법은 Bindu 등의 제안 프로토콜과 달리 XOR 연산을 최소화하고 타임스탬프를 사용하지 않아 기존 Bindu 등의 제안 프로토콜이 가진 취약점들을 해결하여 안전성을 보다 향상시켰다.

본 논문에서 제안한 프로토콜은 스마트카드를 이용한 키 교환 및 다양한 응용 분야에서 사용될 수 있을 것으로 예상된다.

참고문헌

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

[2] T. Y. Hwang, "Passwords Authentication Using Public-Key Encryption," *Proc. of international Carnahan Conference on Security Technology*, pp. 35-38, 1983.

[3] C. S. Laih, L. Harn,and D. Huang, "Password authentication using quadratic residues," *Proceedings of International Computer Symposium*, pp. 1478-1483, 1988.

[4] T. Hwang, Y. Chen, and C.S. Laih, "Non-interactive password authentications without password tables," *IEEE Region 10 Conference on Computer and Communication Systems, IEEE Computer Society*, pp. 429-431, 1990.

[5] S. J. Wang, and J. F. Chang, "Smart card based secure password authentication scheme," *Computers and Security*, Vol. 15 No. 3 pp. 231-237, 1996.

[6] W. H. Yang, and S. P. Shieh, "Password authentication schemes with smart cards," *Computers and Security,* Vol. 18 No. 8, pp. 727-733, 1999.

[7] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, Vol. 36 No. 4 pp. 23-29, 2002.

[8] C. C. Chang, and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings Computers and Digital Techniques*, Vol. 138 No. 3, pp. 165-168, 1991.

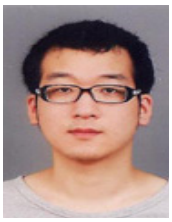
[9] M. L Das, A. Saxena, and V. P Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 629-631, May 2004.

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

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

[12] 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.

저자소개



박대식(Dae-Sik Park)

2010년 순천향대학교
정보보호학과 학사

2010년~현재 순천향대학교 정보보호학과 석사과정
※ 관심분야 : 정보보호, 클라우드 컴퓨팅 보안 등

곽진(Jin Kwak)

2003년 성균관대학교 컴퓨터공학과
(공학석사)
2006년 성균관대학교 컴퓨터공학과
(공학박사)

2007년~현재 순천향대학교 정보보호학과 교수
※ 관심분야 : 암호 프로토콜, 개인정보보호 등