韓國컴퓨터情報學會 論文誌
第16卷 第2號, 2011. 2.

2011-16-2-3-9

비대칭 무선랜 환경을 위한 안전한 패스워드 인증 키 교환 프로토콜

양 형 규*

Secure Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks

Hyung Kyu Yang*

요 약

사용자 인증과 비밀키 교환은 암호학의 매우 중요한 응용 분야 가운데 하나로서, 사용자 인증의 경우 일반적으로 패스워드를 이용하고 있지만, 패스워드를 이용한 사용자 인증은 패스워드 추측 공격에 취약한 문제가 있다. 1992년 Bellovin과 Merritt은 패스워드 추측 공격에 안전하면서 비밀키 교환까지 할 수 있는 EKE(Encrypted Key Exchange) 프로토콜을 제안한 바 있으며, 이후 효율성과 안전성을 개선한 많은 논문이 제안되고 있다. 이 가운데 Lo는 Yeh 등이 제안한 패스워드 기반 인증키 교환 프로토콜의 취약점을 지적함과 동시에 개선된 프로토콜을 2006년에 제안하였다. 하지만, Lo의 프로토콜 역시 오프라인 패스워드 추측 공격에 취약함이 Cao와 Lin에 의해 지적되었다. 본 논문에서는 새로운 공격 방법으로 Lo의 프로토콜이 온라인 패스워드 추측공격에도 취약함을 보이고, 온라인 패스워드 추측 공격에도 안전한 개선된 프로토콜을 제안한다. 제안한 프로토콜은 비대칭 무선 네트워크 환경에서 패스워드 기반 인증키 교환 프로토콜로 사용될 수 있다.

▸ Keyword : 패스워드, 인증키 교환, 무선네트워크, 패스워드 추측 공격

Abstract

User authentication and key exchange protocols are the most important cryptographic applications. For user authentication, most protocols are based on the users' secret passwords. However, protocols based on the users' secret passwords are vulnerable to the password guessing attack. In 1992, Bellovin and Merritt proposed an EKE(Encrypted Key Exchange) protocol for user authentication and key exchage that is secure against password guessing attack. After that, many enhanced and secure EKE protocols are proposed so far. In 2006, Lo pointed out that Yeh et al.'s password-based authenticated key exchange protocol has a security weakness and proposed an improved protocol. However, Cao and Lin showed that his protocol is also vulnerable to off-line

• 제1저자 : 양형규
• 투고일 : 2010. 10. 25, 심사일 : 2010. 11. 08, 게재확정일 : 2010. 11. 24.
*강남대학교 컴퓨터미디어정보공학부 교수(Dept. of Computer &media-information Engineering)
※ 본 연구는 2009학년도 강남대학교 교내 연구비 지원에 의해 이루어짐.

www.kci.go.kr

password guessing attack. In this paper, we show his protocol is vulnerable to on-line password guessing attack using new attack method, and propose an improvement of password authenticated key exchange protocol for imbalanced wireless networks secure against password guessing attack.

▸ Keyword : Password, Authenticated Key Exchange, Wireless Network, Password Guessing Attack

Ⅰ. 서 론

DES, SEED, AES 등과 같은 대칭형 암호방식은 RSA와 같은 비대칭형 암호방식보다 암복호화 연산이 빠르다는 장점이 있지만, 비밀키를 사전에 교환해야 하는 키교환 문제가 있다. 이러한 이유로 1976년 Diffie와 Hellman이 공개키를 기반으로 하는 키교환 프로토콜을 제안한 이후 키교환은 암호학에 있어서 주요 연구 과제가 되고 있으며, 많은 연구 결과가 발표되었다[1-8].

1981년에 Lamport는 암호화 기법을 사용하지 않고 단순히 패스워드 기반의 원격 사용자 인증 스킴을 제안하였다[1]. 그 이후 다수의 프로토콜들이 안전성, 또는 효율성을 개선하기 위해서 발표되었다[2].

1992년 Bellovin과 Merritt은 공개키 방식을 기반으로 하는 키교환 방식과는 다른 패스워드 기반 키교환 프로토콜을 제안하였는데[9], 사람이 외우기 쉬운 패스워드를 기반으로 비밀키를 교환한다는 장점으로 인해 이후 많은 패스워드 기반 키교환 프로토콜이 제안되기에 이르렀다[10].

이러한 연구 결과 가운데 2002년에 발표된 Zhu 등의 논문은 대표적 공개키 방식인 RSA를 기반으로 비대칭형 무선 네트워크 환경을 위한 패스워드 기반 인증키 교환 방식[11]으로 RSA를 이용하는 대표적인 패스워드 기반 키교환 방식이지만, 2003년 Yeh 등은 Zhu 등의 프로토콜이 탐지할 수 없는 온라인 패스워드 추측 공격(undetectable on-line password guessing attack)에 취약하며, 명시적인 키인증(explicit key authentication) 기능을 제공하지 못함을 지적하였다[12].

Yeh 등은 이러한 문제점을 해결한 프로토콜을 제안하였지만 이 방식 역시 오프라인 패스워드 추측 공격에 취약함이 Yang 및 Lo에 의해 각각 밝혀졌다[13, 14]. 이 가운데 Lo는 Yeh 등의 방식을 개선한 프로토콜을 2006년에 제안하였지만 Lo의 프로토콜 역시 오프라인 패스워드 추측 공격에 취약함이 Cao와 Lin에 의해 밝혀졌다[15]. 하지만, Cao와 Lin도 개선된 프로토콜을 제안하지 못하면서 RSA를 이용한 패스워드 기반 인증키 교환 프로토콜을 안전하게 설계하기 위한 연구가 현재도 진행되고 있다[16].

본 논문에서는 Lo의 프로토콜이 갖는 취약점인 오프라인 패스워드 추측 공격에 안전한 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서 Lo가 제안한 패스워드 기반 인증키 교환 프로토콜에 대해 설명함과 동시에 Cao와 Lin이 제안한 오프라인 패스워드 추측 공격 방법에 대해 설명한다. 3장에서는 Lo의 프로토콜이 갖는 또다른 취약점인 탐지할 수 없는 온라인 패스워드 추측 공격 방법에 대해 설명하고, 이러한 문제점들을 개선한 패스워드 기반 인증키 교환 프로토콜을 제안한다. 그리고 4장에서 제안한 프로토콜의 안전성 및 효율성을 분석하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. Lo's Protocol

1. 표기법

본 논문에서 사용한 표기법 및 정의는 다음과 같다.

- A : 서버
- B : 저전력 클라이언트
- ID_A, ID_B : 각각 A와 B의 ID
- pw : A와 B가 사전에 교환한 패스워드
- (n,e) : RSA 방식의 공개키
- $E_K(), D_K()$: 각각 비밀키 K를 이용한 대칭형 암호화 및 복호화 함수 ($K \in \{0,1\}^k$)
- $h(), G_1(), G_2()$: 해쉬 함수

2. 프로토콜

본 절에서는 Lo가 제안한 프로토콜에 대해 설명하도록 하며, A와 B는 사전에 패스워드 pw를 공유하고 있다고 가정한다.

- A는 RSA 공개키인 (n,e)를 임의로 생성하고, 난수

www.kci.go.kr

r_A를 이용하여 $R_A = pw \oplus r_A$를 계산한 후 B에게 전송한다.

- B는 대화형 프로토콜을 진행하여 A의 RSA 공개키인 (n, e)의 유효성을 검증한다.
- B는 난수 $s_B \in {}_R Z_n$ 를 선택하여 $\pi = ID_A \| ID_B \| E_{pw}(R_A \oplus pw \oplus s_B)$를 계산한 후, $z = \pi^e \pmod n$을 A에게 전송한다.
- A는 $z^d \pmod n$을 계산하여 $E_{pw}(R_A \oplus pw \oplus s_B)$를 얻고, $D_{pw}(E_{pw}(R_A \oplus pw \oplus s_B)) \oplus r_A$로부터 s_B를 계산한다.
- A는 s_B를 이용하여 $c_B = G_1(s_B)$를 계산한 후, 세션키 $\sigma = G_2(r_A, c_B, ID_A, ID_B)$를 계산하여 B에게 $E_\sigma(ID_B)$를 전송한다.
- 동시에 B는 $c'_B = G_1(s_B)$와 세션키 $\sigma' = G_2(r_A, c'_B, ID_A, ID_B)$을 계산한다. A로부터 $E_\sigma(ID_B)$를 수신하면 $D_{\sigma'}(E_\sigma(ID_B))$를 계산하여 자신의 ID인 ID_B를 확인한다. 만약, 자신의 ID가 맞다면 $h(\sigma')$을 A에게 전달하고, 맞지 않다면 연결을 종료한다.
- A는 $h(\sigma) = h(\sigma')$인지 검증하여 맞지 않다면 연결을 종료한다.

Lo의 프로토콜을 그림으로 표현하면 그림 1과 같다.

3. 기존의 취약점

2006년 Cao와 Lin은 Lo의 프로토콜이 오프라인 패스워드 추측 공격에 취약함을 지적하였다[2]. A와 B는 사전에 패스워드를 교환한 상태이며, 공격자 I는 패스워드를 알지 못한다고 가정했을 때, Cao와 Lin이 제시한 공격 방법은 그림 2와 같으며, 다음과 같다.

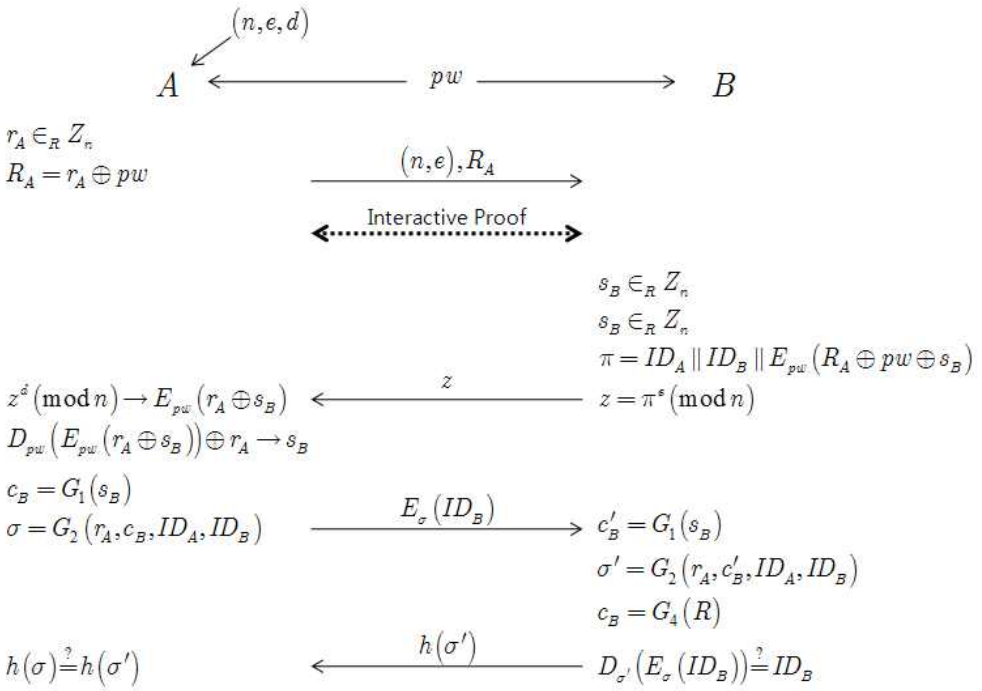

그림 1. Lo의 프로토콜
Figure 1. Lo's protocol

www.kci.go.kr

- A는 RSA 공개키 (n,e)와 $R_A = r_A \oplus pw$(r_A는 난수)를 B에게 전송한다. 이 때 공격자 I는 이를 가로채서 자신이 생성한 RSA 공개키 (n^*,e^*)와 R_A를 B에게 전송한다.
- B는 I와 (n^*,e^*)의 유효성을 검증하기 위한 대화형 프로토콜을 진행하며, I는 A와 (n,e)의 유효성을 검증하기 위한 대화형 프로토콜을 진행한다. 그런 후 B는 난수$s_B \in {}_R Z_n$ 를 선택하여 $\pi = ID_A \| ID_B \| E_{pw}(R_A \oplus pw \oplus s_B)$를 계산한 후, $z = \pi^{e^*} (\mathrm{mod} n^*)$을 A에게 전송한다. 공격자 I는 z를 복호화하여 $\pi = ID_A \| ID_B \| E_{pw}(R_A \oplus pw \oplus s_B)$ $= ID_A \| ID_B \| E_{pw}(r_A \oplus s_B)$로부터 $E_B = E_{pw}(r_A \oplus s_B)$를 획득한다. I는 $z = \pi^e (\mathrm{mod} n)$을 A에게 전송한다.
- A는 $z^d (\mathrm{mod} n)$을 계산하여 $E_{pw}(R_A \oplus pw \oplus s_B)$를 얻고, $D_{pw}(E_{pw}(R_A \oplus pw \oplus s_B)) \oplus r_A$로부터 s_B를 계산한 다음, s_B를 이용하여 $c_B = G_1(s_B)$를 계산하고 세션키 $\sigma = G_2(r_A, c_B, ID_A, ID_B)$를 계산하여 B에게 $E_\sigma(ID_B)$를 전송한다. 공격자 I는 $E_\sigma(ID_B)$를 가로챈다.
- 공격자 I는 자신의 공격을 A,B 양자가 알지 못하도록 $E_\sigma(ID_B)$를 B에게 전송하며, B로부터 전송된 $h(\sigma')$를 A에게 전달하여 프로토콜을 종료한다.

이상의 과정을 마치면 공격자 I는 획득한 정보 ID_A, ID_B, R_A, E_B, 및 $E_\sigma(ID_B)$를 이용하여 오프라인 패스워드 추측 공격을 실행할 수 있다. 먼저 임의의 패스워드를 추측하여 pw^*이라고 한다. 이로부터 $r_A^* = R_A \oplus pw^*$와 $s_B^* = D_{pw^*}(E_B) \oplus r_A^*$를 계산한다. 그리고 $c_B^* = G_1(s_B^*)$와 $\sigma^* = G_2(r_A^*, c_B^*, ID_A, ID_B)$를 계산한 다음 $D_{\sigma^*}(E_\sigma(ID_B))$가 ID_B와 일치하는지 확인한다. 만약 일치한다면 $pw^* = pw$ 즉 패스워드를 정확하게 추측한 경우가 되며 일치하지 않는다면 다른 패스워드를 추측하여 위의 과정을 반복한다.

III. 온라인 패스워드 추측 공격에 안전한 제안 프로토콜

1. Lo 프로토콜의 새로운 취약점

Lo의 프로토콜은 Cao와 Lin이 지적한대로 오프라인 패스워드 추측 공격에 취약하지만, 탐지할 수 없는 온라인 패스워드 추측 공격에도 취약하다. 본 절에서는 그림 3과 같이 탐지할 수 없는 온라인 패스워드 추측 공격 과정을 보이고, 이러한 공격에 취약함을 보인다.

먼저 A와 B는 패스워드 pw를 사전에 공유하고 있으며, 공격자 I는 B의 패스워드를 추측하여 B로 가장하고자 한다. 이 때 공격자 I의 공격 과정은 다음과 같다.

- A는 RSA 공개키 (n,e)와 $R_A = r_A \oplus pw$(r_A는 난수)를 B에게 전송한다. 이 때 공격자 I는 이를 가로채서 A와 대화형 프로토콜을 진행한다.
- 공격자 I는 난수 s_B를 선택하고 임의의 패스워드 pw^*를 추측한다. 그런 다음 $r_A^* = R_A \oplus pw^*$와 $\pi = ID_A \| ID_B \| E_{pw^*}(r_A^* \oplus s_B)$로부터 $z = \pi^e (\mathrm{mod} n)$을 계산하여 A에게 전송한다.
- A는 $c_B^* = G_1(s_B^*)$로부터 세션키 $\sigma = G_2(r_A, c_B^*, ID_A, ID_B)$를 계산한다. 그리고 $E_\sigma(ID_B)$를 I에게 전송한다.
- I는 $\sigma^* = G_2(r_A^*, G_1(s_B), ID_A, ID_B)$로부터 $D_{\sigma^*}(E_\sigma(ID_B))$를 계산하여 ID_B와 일치하는지 확인한다. 만약 일치한다면 I는 B의 패스워드 pw를 정확하게 추측한 것이며, 일치하지 않을 경우 연결을 종료하고 위의 과정을 다시 진행한다.

위의 공격 과정이 의미있는 이유는 A가 정상적인 사용자의 프로토콜 진행과 공격자의 프로토콜 진행을 구별할 수 없기 때문이며, 이런 이유로 공격임을 인지할 수 없게 된다.

www.kci.go.kr

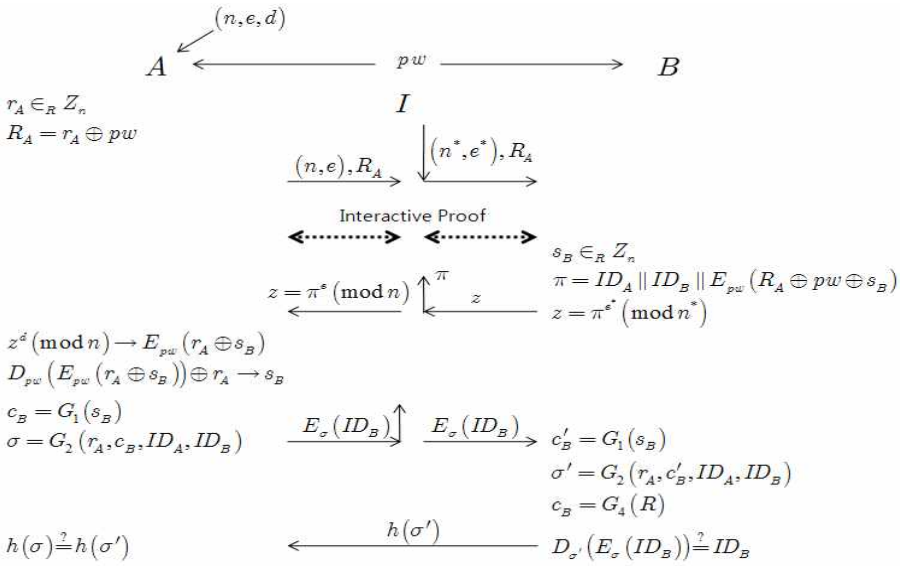

그림 2. Cao와 Lin의 공격 과정

Figure 2. Cao and Lin's attack procedure

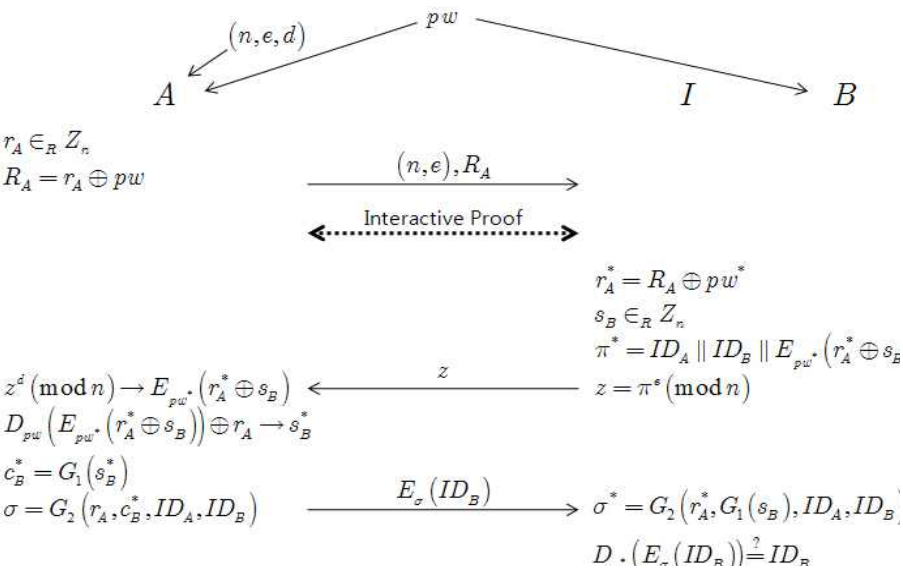

그림 3. Lo 프로토콜의 새로운 취약점

Figure 3. New weakness of Lo's protocol.

www.kci.go.kr

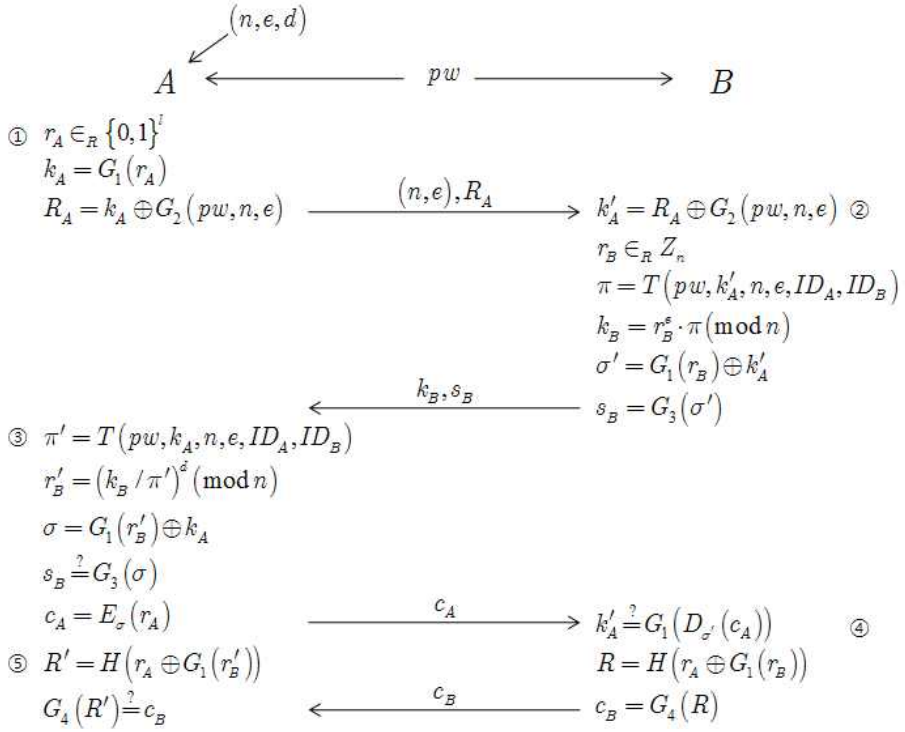

그림 4. 온라인 패스워드 추측 공격에 안전한 제안 프로토콜
Figure 4. Proposed protocol secure against on-line password guessing attack

2. 안전한 제안 프로토콜

Lo의 프로토콜이 오프라인 패스워드 추측 공격에 취약한 이유는 B 입장에서 RSA 공개키 (n,e)가 A로부터 전달되었음을 확인할 수 있는 방법이 없기 때문이다. 이런 이유로 공격자 I는 거짓 RSA 공개키 (n^*,e^*)를 이용하여 손쉽게 E_B를 획득할 수 있다.

제안하는 방식은 공격자 I가 RSA 공개키 (n,e)를 수정하지 못하도록 R_A를 수정하였으며, RSA 공개키를 이용하여 π를 보호하도록 하였다. 이를 통해 RSA 공개키의 유효성을 검증하기 위한 대화형 프로토콜은 더 이상 필요하지 않게 되었으며, 탐지할 수 없는 온라인 패스워드 추측 공격을 방지하기 위하여 그림 4와 같이 A와 B가 서로를 인증하기 전까지는 세션키를 생성하지 않도록 하였다.

먼저, T와 G_1, G_2, G_3, G_4, H를 다음과 같이,

$$T: \{0,1\}^* \rightarrow \{0,1\}^{|n|-1}$$
$$G_1, G_2, G_3, G_4, H: \{0,1\}^* \rightarrow \{0,1\}^l$$

로 정의했을 때, 프로토콜은 다음과 같다.

1) A는 RSA 공개키 (n,e)와 난수 $r_A \in_R \{0,1\}^l$를 선택한다. 그런 다음 $k_A = G_1(r_A)$를 이용하여 $R_A = k_A \oplus G_2(pw,n,e)$를 계산하고, (n,e)와 R_A를 B에게 전송한다.

2) B는 난수 $r_B \in_R Z^n$ 를 선택하여
$k' = R_A \oplus G_2(pw,n,e)$을 이용하여
$\pi = T(pw, k'_A, n, e, ID_A, ID_B)$와
$\sigma' = G_1(r_B) \oplus k'_A$를 계산한다. 그런 다음,
$k_B = r_B^e \pi \pmod n$와 $s_B = G_3(\sigma')$을 A에게 전송한다.

3) A는 $\pi' = T(pw, k_A, n, e)$와
$r'_B = (k_B/\pi')^d \pmod n$을 얻고,
$\sigma = G_1(r'_B) \oplus k_A$를 계산하여 $s_B = G_3(\sigma)$인지를 확인한다. 만약 같다면 A는 $c_A = E_\sigma(r_A)$를 B에게 전송한다.

4) B는 식 $k'_A = G_1(D_{\sigma'}(c_A))$이 만족하는지 검증

www.kci.go.kr

하여 다를 경우 연결을 종료하며, 같을 경우 세션키 $r'_A = D_{\sigma'}(c_A)$를 이용하여
$R = H(r'_A \oplus G_1(r_B))$을 계산한 다음
$c_B = G_4(R)$을 A에게 전송한다.

5) A는 동시에 세션키 $R' = H(r_A \oplus G_1(r'_B))$를 계산한다. 이후 B로부터 c_B를 전송받으면 식 $c_B = G_4(R')$이 성립하는지 검증한다. 만약 다르다면 연결을 종료한다.

IV. 안전성 및 효율성 분석

패스워드 추측 공격은 크게 다음 세가지로 구분할 수 있다.

- 탐지할 수 있는 온라인 패스워드 추측 공격
- 탐지할 수 없는 온라인 패스워드 추측 공격
- 오프라인 패스워드 추측 공격

이 가운데, 반드시 막아야 하는 공격은 탐지할 수 없는 온라인 패스워드 추측 공격과 오프라인 패스워드 추측 공격인데, 탐지할 수 있는 온라인 패스워드 추측 공격은 서버에서 공격 여부를 인지할 수 있고 이에 따라 대응할 수 있기 때문이다.

1. 탐지할 수 없는 온라인 패스워드 추측 공격 방지

제안 방식의 세 번째 과정에서 A는, k_B와 s_B를 이용하여 세션키 생성 이전에 B를 인증하도록 함으로써 pw를 모르는 공격자 I는 정상적인 B로 위장할 수 없도록 하고 있다. 따라서, I는 pw를 정확하게 추측하지 않는 이상 A로부터 c_A를 수신할 수 없기 때문에 패스워드 추측 공격을 실행할 수 없게 된다. 또한 I가 추측한 패스워드인 pw^*를 이용하여 위조된 k_B와 s_B를 전송할 경우 A는 공격 여부를 판단할 수 있기 때문에 이게 대한 대응책을 실행할 수 있게 된다.

2. 오프라인 패스워드 추측 공격 방지

패스워드 기반 인증키 교환 프로토콜은 능동적 또는 수동적 공격자가 실행할 수 있는 오프라인 패스워드 추측 공격에 안전해야 한다. 본 절에서는 제안한 방식을 공격하는 것은 RSA를 공격하는 것과 계산상 동등함을 보임으로써 제안한 방식이 오프라인 패스워드 추측 공격에 안전함을 증명하도록 한다.

먼저, 공격자 I는 n, e, R_A, k_B, s_B, c_A 및 c_B를 획득할 수 있다. 또한, 임의의 패스워드 $pw^* \in_R PW$ (단, PW는 전체 패스워드 집합)를 이용하여 $k_A^* = R_A \oplus (pw^*, n, e)$와 $\pi^* = T(pw^*, k_A^*, n, e, ID_A, ID_B)$를 유추할 수 있다. 하지만, $k_B = r_B^e \pi \pmod n$와 $\sigma = G_1(r_B) \oplus k_A$는 유추할 수 없는데, 왜냐하면 r_B는 B가 정한 난수이기 때문이다. 마찬가지 이유로 c_A와 c_B 역시 유추할 수 없다. 공격자 I가 오프라인 패스워드 추측 공격을 실행하기 위해서는 추측한 패스워드 pw^*의 유효성을 검증할 수 있어야 하는데, 이를 위해서는 k_B로부터 π를 계산하거나, k_B로부터 r_B를 계산하여 식 $s_B = G_3(G_1(r_B^*) \oplus k_A^*)$이 성립하는지 검증해야 한다. 즉, k_B를 해독할 수 있어야 하는데, $k_B = r_B^e \pi \pmod n$을 해독하는 것은 RSA 암호방식을 해독하는 것과 계산상 동등함이 이미 증명되어 있다. 따라서, 제안한 방식은 RSA와 계산상 동등한 안전성을 갖는다고 할 수 있다.

3. 효율성 분석

본 절에서는 계산 효율성 및 전송 효율성을 중심으로 제안한 프로토콜의 효율성을 분석한다. 비대칭 네트워크 환경에서는 서버가 월등히 높은 계산 능력을 갖는다고 가정하기 때문에 가능하면 모든 멱승 연산은 서버에서 수행하도록 하는 것이 바람직하며, 서버의 연산량을 비교하는 것은 의미가 크지 않다. 따라서, 본 절에서는 클라이언트의 연산량을 해쉬 연산, 멱승 연산, 곱셈 연산, 대칭키 암/복호화 연산 그리고 공개키 검증을 위한 대화형 프로토콜을 중심으로 비교하도록 한다.

제안한 프로토콜은 클라이언트 B가 7번의 해쉬 연산, 1번의 멱승 연산, 1번의 대칭키 복호화, 그리고 1번의 곱셈 연산을 표 1에서 보인 것 처럼 실행된다.

제안한 프로토콜은 Lo의 프로토콜과 비교했을 때, 4번의 해쉬 연산과 1번의 곱셈 연산을 추가로 실행해야 하지만, 이보다 연산 시간이 많이 소요되는 암/복호화 연산 횟수가 적으며, 또한 대화형 프로토콜을 필요로 하지 않아 데이터 전송량을 적기 때문에 특히 저전력 클라이언트 단말기를 고려했을 때 보다 효율적이라고 할 수 있다.

www.kci.go.kr

표 1. 효율성 비교
Table 1. Efficiency comparison

	Lo의 프로토콜	제안 프로토콜	차이
Hash	3	7	+4
En/Decryption	2	1	-1 ▲
Exponentiation	1	1	-
Multiplication	-	1	+1
Interactive Proof	Required	None	▲

V. 결론

본 논문에서는 Lo의 프로토콜 및 Cao와 Lin이 제안한 오프라인 패스워드 추측 공격 방법에 대해 설명하고, 이러한 문제를 해결한 안전한 패스워드 인증키 교환 방식을 제안하였다. 제안한 방식은 비대칭 무선 네트워크 환경을 가정하고 있으며 Lo의 프로토콜과 비교하여 대화형 프로토콜을 필요로 하지 않는 장점이 있으며, 클라이언트가 해쉬 연산과 곱셈 연산을 각각 4회 및 1회 많이 실행해야 하지만, 암/복호화 연산 횟수를 줄였기 때문에 전체적인 연산 효율성은 Lo의 프로토콜보다 높다.

참고문헌

[1] L. Lamport, "Password authentication with insecure communication," Communcations of the ACM, 24(11), pp. 770-772, 1981.

[2] D.S. Wong, A.H. Chan, and F. Zhu, "More Efficient Password Authenticated Key Exchange Based on RSA," Indocrypt 2003, LNCS 2904, pp. 375-387, 2003.

[3] Chae, Kang-Suk, and Jung, Sou-Hwan, "SRTP Key Exchange Scheme Using Split Transfer of Divided RSA Public Key," Journal of The Korea Society of Computer and Information, vol. 14, no. 12, pp.147-156, Dec. 2009.

[4] Y. Ding and P. Horster, "Undetectable On-line Password Guessing Attacks," ACM Operating Systems Review, Vol. 29, pp. 77-86, 1995.

[5] T. Wu, "The secure remote password protocol," Proc. of the 1998 Internet Society Network and Distributed System Security Symposium, pp. 97-111, 1998.

[6] M. Bellare, D. Pointcheval and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks," Eurocrypt 2000, LNCS 1807, pp. 139-155, 2000.

[7] V. Boyko, P. MacKenzie and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," Eurocrypt 2000, LNCS 1807, pp. 156-171, 2000.

[8] E. Bresson, O. Chevassut and D. Pointcheval, "Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks," Asiacrypt 2002, LNCS 2501, pp. 603-610, 2002.

[9] S.M. Bellobin and M. Merritt, "Excrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks," IEEE Computer Society Conference on Research in Security and Privacy, pp. 72-84, 1992.

[10] Kim, Hoi-Bok, Shin, Jung-Hoon, and Kim, Hyoung-Jin, "Journal of the Korea Society of Computer and Information," Journal of The Korea Society of Computer and Information, Vol. 14, No. 6, pp.51-57, June. 2009.

[11] F. Zhu, D.S. Wong, A.H. Chan, and R. Ye, "Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks," Information Security Conference 2002(ISC 2002), LNCS 2433, pp. 150-161, 2002.

[12] H.T. Yeh, H.M. Sun, C.T. Yang, B.C. Chen, and S.M. Tseng, "Improvement of Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks," IEICE Trans. on Communications, Vol. E86-B, No. 11, pp. 3278-3282, Nov. 2003.

[13] C.C. Yang and R.C. Wang, "Cryptanalysis of Improvement of Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks," IEICE Trans. on Communications, Vol. E88-B, No. 11, pp. 4370-4372, Nov. 2005.

[14] J.W. Lo, "The Improvement of YSYCT Scheme for Imbalanced Wireless Network," International J. of Network Security, Vol. 3, No. 1, pp. 39-43, Jul. 2006.

www.kci.go.kr

[15] T. Cao and D. Lin, "Cryptanalysis of Two Password Authenticated Key Exchange Protocols Based on RSA," IEEE Communications Letters, Vol. 10, No. 8, pp. 623-625, Aug. 2006.

[16] Jeon, Jeong-Hoon, "An advanced key distribution mechanism and security protocol to reduce a load of the key management system," Journal of The Korea Society of Computer and Information, Vol.11, No.6, pp.35-47, Dec. 2006.

저 자 소 개

양 형 규

1995년 2월 : 성균관대학교 정보공학과 공학박사

1995년 ~ 현재 : 강남대학교 컴퓨터미디어공학부 교수

관심분야 : 암호이론, 정보이론, 정보보호, 디지털 워터마킹

E-mail : hkyang@kangnam.ac.kr

www.kci.go.kr

www.kci.go.kr