간단한 패스워드 기반 키 교환 프로토콜

이성운*, 김우헌*, 김현성**, 유기영*

*경북대학교 컴퓨터공학과, **경일대학교 컴퓨터공학과

Simple Password-based Key Agreement Protocol

Sung-Woon Lee*, Woo-Hun Kim*, Hyun-Sung Kim**, Kee-Young Yoo*

*Department of Computer Engineering Kyungpook Univ.
**Department of Computer Engineering Kyungil Univ.

요 약

Seo와 Sweeney가 패스워드 기반의 키 교환 프로토콜인 SAKA (Simple Authenticated Key Agreement)를 제안한 이래로 몇몇 변형 프로토콜들이 제안되었다. 그러나 그 프로토콜들은 중간 침입자 공격 또는 패스워드 추측 공격에 취약하거나 완전한 전방향 보안성을 제공하지 못한다. 본 논문에서는 중간 침입자 공격과 패스워드 추측공격에 대하여 안전하며 완전한 전방향 보안성을 제공할 수 있는 새로운 키 교환 프로토콜을 제안한다. 여러 가지 알려진 공격에 강한 프로토콜을 제안하기 위해서 먼저 SAKA 변형 프로토콜들에 대한 기존에 분석되지 못한 추가적인 취약점들을 분석한다. 그리고 기존에 알려진 취약점 및 본 논문에서 분석한 추가적인 취약점에 강한 새로운 패스워드 기반 키 교환 프로토콜을 제안한다.

Ⅰ. 서론

인터넷과 같은 공개된 통신망을 통하여 안전한 통신을 위해서는 전송되는 정보가 암호화되어야 한다. 이를 위해서 통신 참여자들 간에 공통으로 사용할 키의 공유와 통신하고 있는 상대가 정확한지를 확인할 수 있는 인증 방법이 함께 요구된다. 따라서 참여자들이 서로를 인증하면서 그들 사이에 키를 공유할 수 있는 키 교환 프로토콜의 개발이 필요하다.

Diffie-Hellman 키 교환 프로토콜은 안전하지 않은 통신상에서 안전하게 세션키를 공유하기 위한 가장 잘 알려진 방법이다[6]. 이 프로토콜은 유한 필드 상에서 이산대수 문제와 Diffie-Hellman문제의 어려움을 이용하여 참여자들간에 세션키를 공유한다. 하지만 이 프로토콜은 참여자들을 인증하는 방법을 제공하지 못하기 때문에 중간 침입자 공격(man-in-the-middle attack)에 대하여 안전하지 못하다.

Seo와 Sweeney는 Diffie-Hellman 키 교환 프로토콜을 토대로 하여 간단한 방법으로 참여자들 간에 키를 공유하고 서로를 인증할 수 있는 SAKA (Simple Authenticated Key Agreement) 프로토콜을 제안하였다[1]. 그러나 Tseng은 SAKA의 키 검증에 문제가 있음을 지적하고 SAKA의 키 검증 단계를 개선하였다[2]. 그 후에 Ku와 Wang은 Tseng의 프로토콜이 두 종류의 공격에 취약하다는 것을 보이고, SAKA의 키 검증 단계를 재 수정하였다[3]. 한편, Sun은 SAKA가 세 종류의 취약점을 가지고 있음을 지적하였다[7]. Lin 등은 Sun이 지적한 이 문제들을 해결하기 위하여 SAKA의 키 검증 단계를 개선하였다[4]. 그러나 Hsieh 등은 Lin 등의 프로토콜마저도 여전히 패스워드 추측 공격(password guessing attack)에 안전하지 않음을 보여주었다[5].

본 논문은 SAKA의 두 변형 프로토콜, 즉 Tseng의 프로토콜과 Ku와 Wang의 프로토콜들에 대한 기존에 알려지지 않은 추가적인 취약성을 분석한다. 그리고 중간 침입자 공격과 패스워드 추측공격에 안전하고 완전한 전방향 보안성을 제공할 수 있는 새로운 패스워드 기반의 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 구성이 무척 간단하기 때문에 하드웨어나 소프트웨어로 구현하기에 무척 용이할 것이다.

Ⅱ. 관련연구

1. 용어 정의

본 절에서는 앞으로의 여러 프로토콜들에서 동일하게 사용될 용어와 표기법, 그리고 가정들을 정의한다.

A, B	두 참여자
g	곱셈군 Z_p^*의 생성자(generator)
n	큰 소수
P	두 참여자간에 미리 공유된 패스워드
Q	패스워드 P로부터 계산된 정수
Q^{-1}	Q의 역수
a, b	참여자 A와 B에 의하여 각각 선택된 임의의 정수 ($a,b \in_R [1,n-1]$)
K_A, K_B	참여자 A와 B에 의하여 생성된 세션키
X_Y	참여자 Y에 의하여 계산된 데이터

그림 1: 프로토콜들을 위한 수학적 표기

프로토콜의 참여자인 A와 B는 합법적인 사용자들이라 가정한다. 또한 A와 B는 안전하게 패스워드 P와 Z_p^*상의 생성자인 g, 그리고 큰 소수인 n을 미리 공유하고 있다고 가정한다. A와 B는 프로토콜이 시작하기 전에 패스워드 P로부터 두 정수 Q와 Q^{-1}을 구한다. 미리 결정된 방법에 의해서 패스워드 P로부터 Q를 계산하고, Z_p^*상의 Q의 역수인 Q^{-1}를 구한다. Q는 n-1과는 서로 소이어야 하고 서로 다른 패스워드 P로부터 같은 Q가 계산될 확률이 아주 낮아야 하는 특성을 가져야 한다. 예를 들어 간단한 방법은 패스워드 P보다 더 큰 소수들 중에서 가장 작은 소수를 취하면 된다.

여기에 정의된 용어, 표기법, 가정, 그리고 Q와 Q^{-1}의 계산은 아래의 모든 프로토콜들과 제안된 프로토콜에 동일하게 적용된다. 그리고 앞으로의 모든 연산들은 mod n 연산 하에서 계산이 이루어진다고 본다.

2. SAKA와 SAKA 변형 프로토콜

본 절에서는 SAKA 관련 프로토콜들에 대하여 살펴보고 이들에 대하여 기존의 논문들에서 제기되었던 취약점들을 기술한다. 특히 SAKA와 본 논문에서 안전성을 분석하고자 하는 Tseng의 프로토콜 및 Ku와 Wang의 프로토콜에 대해서 자세히 살펴본다.

SAKA는 Diffie-Hellman의 키 교환 프로토콜에 사용자의 인증성을 제공하기 위한 목적으로 제안되었다. SAKA에서는 키 교환을 위해 미리 공유된 패스워드를 필요로 한다. 두 참여자는 패스워드 P로부터 Q와 Q^{-1}를 앞 절과 같이 계산하고, 이 값들을 세션키 생성과 검증에 이용한다. SAKA는 다음과 같이 수행된다.

SAKA의 세션키 생성:

■1단계. A는 임의의 정수 a을 선택하고 $X_A(=g^{aQ})$를 계산하여 B에게 전송한다.

■2단계. B는 임의의 정수 b를 선택하고 $X_B(=g^{bQ})$를 계산하여 A에게 전송한다.

■3단계. A는 Y_A와 세션키 K_A를 다음과 같이 계산한다.

$$Y_A = (X_B)^{Q^{-1}} = g^b$$
$$K_A = (Y_A)^a = g^{ab}$$

■4단계. B는 Y_B와 세션키 K_B를 다음과 같이 계산한다.

$$Y_B = (X_A)^{Q^{-1}} = g^a$$
$$K_B = (Y_B)^b = g^{ab}$$

SAKA의 세션키 검증:

■5단계. A는 $V_A(=(K_A)^Q = g^{ab,Q})$를 계산하여 B에게 전송한다.

■6단계. B는 $V_B(=(K_B)^Q = g^{ab,Q})$를 계산하여 A에게 전송한다.

■7단계. A는 $(V_B)^{Q^{-1}} \stackrel{?}{=} K_A$ 이 만족되는지를, B는 $(V_A)^{Q^{-1}} \stackrel{?}{=} K_B$ 이 만족되는지를 각각 검사한다.

그러나 Tseng은 SAKA가 후방향 재전송 공격(backward replay attack)에 의해 공격당할 수 있음을 지적하였다. 즉, 공격자는 1단계에서 X_A를 가로채 A에게 재전송하고 5단계에서 V_A를 가로채 A에게 재전송한다. 반대로 2단계와 6단계에서 B에 대해서도 동일하게 할 수 있다. 결국, A와 B는 공격자의 존재를 알지 못한 채 잘못된 세션키를 적법한 키로 검증하게 된다. 이러한 문제점을 해결하기 위해서 Tseng은 다음과 같이 새로운 검증 단계를 제안하였다[2].

Tseng의 세션키 검증:

■5단계. A는 $Y_A(=g^b)$를 B에게 전송한다.

■6단계. B는 $Y_B(=g^a)$를 A에게 전송한다.

■7단계. A는 $Y_B \stackrel{?}{=} g^a$ 이 만족되는지를, B는 $Y_A \stackrel{?}{=} g^b$ 이 만족되는지를 각각 검사한다.

그러나 Ku와 Wang은 Tseng의 프로토콜 또한 SAKA와 마찬가지로 후방향 재전송 공격에 취약하고, 공격자가 중간 메시지를 수정하여 공격한다면 참여자들 중에 한쪽은 잘못된 세션키를 신뢰하게 되는 문제점을 지적하였다. 그래서 그들은 다음과 같은 새로운 키 검증 단계를 제안하였다[3].

Ku와 Wang의 세션키 검증:

■5단계. A는 $V_A(=(K_A)^Q=g^{ab,Q})$를 계산하여 B에게 전송한다.

■6단계. B는 $(V_A)^{Q^{-1}} \stackrel{?}{=} K_B$ 이 만족되는지를 검사한다. 그리고 B는 Y_B를 A에게 전송한다.

■7단계. A는 $Y_B \stackrel{?}{=} g^a$ 이 만족되는지를 검사한다.

한편, Sun은 논문[7]에서 SAKA에 다음과 같은 3가지 문제점이 있음을 지적했다: ㉠사용자의 신원(identity)을 확인할 수 없다, ㉡패스워드 추측 공격에 취약하다, ㉢완전한 전방향 보안성을 제공하지 못한다. Lin 등은 이 문제점들을 해결하기

위해 새로운 세션키 검증단계를 제안하였다[4]. 그러나 Hsich 등은 Lin 등에 의해 개선된 프로토콜 역시 패스워드 추측 공격이 가능함을 밝혔다[5].

III. 보안 요구사항과 취약성 분석

1. 보안 요구사항

본 절에서는 패스워드 기반의 키 교환 프로토콜들의 보안 요구사항을 기술한다. 패스워드 기반의 키 교환 프로토콜은 다음과 같은 보안 요구사항을 만족해야한다[8].

1) 중간 침입자 공격(man-in-the-middle attack)에 안전해야 한다.

키 교환 프로토콜은 안전하지 않은 통신상에서 메시지 교환을 통해 세션키를 공유하고 세션키의 정확성을 검증한다. 그래서 공격자는 통신 선로 중간에서 키 교환을 위한 전송 메시지들을 도청(eavesdropping)하여 패스워드나 세션키의 정보를 알아내려고 할 수 있다. 그리고 전송 메시지를 변경(modification), 반송(reflection), 또는 이전 세션의 메시지를 저장해 두었다가 후에 재전송(replay)하는 방법 등으로 참여자들이 알지 못한 상태에서 잘못된 세션키를 생성하도록 유도할 수도 있다. 또한 공격자는 참여자로 위장하여 정상적인 방법으로 합법적인 참여자와 키를 공유하려고 하거나 패스워드에 관한 정보를 얻으려고 할 수 있다. 키 교환 프로토콜은 이러한 공격들에도 패스워드나 세션키에 관한 정보를 노출시켜서는 안되며 잘못된 세션키의 생성을 탐지할 수 있어야 한다.

2) 패스워드 추측 공격(password guessing attack)에 안전해야 한다.

패스워드 추측 공격은 온라인 패스워드 추측 공격과 오프라인 패스워드 추측 공격으로 나뉠 수 있다. 온라인 패스워드 추측 공격은 패스워드 인증 실패 횟수를 셈으로써 쉽게 탐지되고 실패 횟수를 제한함으로서 쉽게 조치될 수 있다. 그러나 공격자는 안전하지 않은 통신상의 메시지를 가로채거나 정당한 사용자로 가장하여 다른 사용자와 키 교환 시에 발생하는 정보들을 모아 오프라인으로 패스워드에 관한 정보를 알아내려고 한다. 이러한 오프라인 패스워드 추측 공격은 사용자에 의해 사용되는 패스워드의 낮은 엔트로피 때문에 패스워드 기반의 키 교환 프로토콜들에는 아주 큰 위협이다. 그러므로 패스워드 기반 키 교환 프로토콜은 패스워드 추측 공격에 안전해야 한다.

3) 완전한 전방향 보안성(perfect forward secrecy)을 제공해야 한다.

공격자가 참여자의 패스워드를 알아내었다 할지라도 이전에 사용된 세션키에 관한 정보는 알 수 없어야 한다. 이러한 성질을 완전한 전방향 보안성이라 한다. 패스워드 기반 키 교환 프로토콜은 이러한 성질을 만족해야 한다.

2. 암호학적 취약성 분석

본 절에서는 2장에서 살펴보았던 Tseng의 프로토콜과 Ku와 Wang의 프로토콜에 대한 기존에 알려지지 않은 추가적인 취약점을 분석한다.

Tseng의 프로토콜은 Ku와 Wang이 지적한 두 공격에 취약한 문제 이외에도 추가적인 취약점을 가지고 있다. Tseng의 프로토콜은 패스워드 추측 공격을 막을 수 없다. Tseng의 프로토콜에서 공격자가 1, 2, 5, 그리고 6단계의 메시지들인 X_A, X_B, Y_A, 그리고 Y_B를 가로채어 저장해 둔다면 공격자는 그 자료들을 이용하여 패스워드 P를 추측할 수 있다. 즉 공격자는 임의의 P'를 선택하여 미리 결정된 방법에 의해 Q'를 계산하고, Y_B에 Q'를 지수승한 값과 X_A의 값이 같은지를 비교하거나, Y_A에 Q'를 지수승한 값이 X_B의 값과 같은지를 비교함으로써 선택된 P'가 참여자들이 사용하고 있는 P인지를 결정할 수 있다.

Ku와 Wang은 Tseng의 프로토콜에 대하여 문제점들을 지적하고 새로운 프로토콜을 제안하였지만 이 프로토콜 또한 패스워드 추측 공격에 취약하다. Ku와 Wang의 프로토콜에서 공격자는 2단계의 X_A와 6단계의 Y_B를 가로채고 패스워드 P'를 추측하여 Q'와 Q'^{-1}을 계산한다. 이 Q'^{-1}을 X_A에 지수승하여 Y_B와 같은지를 비교함으로 패스워드 P'가 정확한 패스워드인지를 결정할 수 있다. 또한, Ku와 Wang의 프로토콜은 완전한 전방향 보안성도 제공하지 못한다. 패스워드 P가 공격자에게 노출되었다면 이 패스워드 P를 알아낸 공격자는 Q와 Q^{-1}을 계산하고 5단계의 V_A를 가로채 이 값에 Q^{-1}을 지수승하여 이전에 사용된 세션키를 쉽게 구할 수 있다.

그러므로 SAKA를 포함한 SAKA 변형 프로토콜들은 중간 침입자 공격 또는 패스워드 추측 공격에 안전하지 못하거나 완전한 전방향 보안성을 제공하지 못한다. 표1은 SAKA 관련 프로토콜들의 특징을 보여준다.

표 1: SAKA 관련 프로토콜들의 특징
S:안전, NS:안전하지 않음, P:제공, NP:제공하지 않음

프로토콜 / 분석	SAKA [1]	Tseng [2]	Ku와 Wang[3]	Lin 등 [4]
중간 침입자 공격	NS	NS	S	S
패스워드 추측 공격	NS	NS	NS	NS
완전한전방향 보안성	NP	P	NP	P

IV. SPKA (Simple Password-based Key Agreement)

본 장에서는 SAKA 및 SAKA 변형 프로토콜의 기존에 알려진 보안상 취약점과 본 논문에서 추가로 제시한 보안상 취약점들을 해결 할 수 있는 새롭고 간단한 패스워드 기반 키 교환 프로토콜(SPKA)을 제안한다. SPKA 프로토콜에 대한 용어와 표기법, 가정, Q와 Q^{-1}의 계산은 2장에 기술된 것과 동일하다. 제안된 프로토콜은 다음과 같이 수행한다.

세션키 생성:

■1단계. A는 임의의 정수 a를 선택하고 Q를 사용함으로 $X_A(=g^{aQ})$를 계산하여 B에게 전송한다.

■2단계. B는 임의의 정수 b를 선택하고 Q^{-1}를 사용함으로 $X_B(= g^{bQ^{-1}})$를 계산하여 A에게 전송한다.

■3단계. A는 다음과 같이 B로부터 받은 X_B에 Q를 지수승하여 Y_A를 계산하고, 세션키 K_A를 계산한다.

$$Y_A = (X_B)^Q = g^b$$
$$K_A = (Y_A)^a = g^{ab}$$

■4단계. B는 다음과 같이 A로부터 받은 X_A에 Q^{-1}를 지수승하여 Y_B를 계산하고, 세션키 K_B를 계산한다.

$$Y_B = (X_A)^{Q^{-1}} = g^a$$
$$K_B = (Y_B)^b = g^{ab}$$

세션키 검증:

■5단계. A는 Y_A에 K_A를 지수승함으로 $V_A(= (Y_A)^{K_A} = g^{bK_A})$를 계산하여 B에게 전송한다.

■6단계. B는 A로부터 받은 V_A를 $(g^b)^{K_B}$와 비교하여 세션키를 검증한다. 그리고 B는 Y_B에 K_B를 지수승함으로 $V_B(= (Y_B)^{K_B} = g^{aK_B})$를 계산하여 A에게 전송한다.

■7단계. A는 B로부터 받은 V_B를 $(g^a)^{K_A}$와 같은지를 비교하여 세션키를 검증한다.

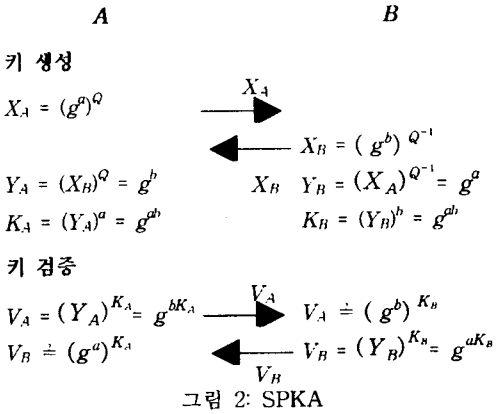

그림 2: SPKA

V. 안전성 분석

본 장에서는 본 논문에서 제안한 프로토콜인 SPKA가 앞에 제시한 보안 요구사항을 만족하는지를 분석한다. SPKA는 Diffie-Hellman 키 교환 프로토콜과 같이 이산대수 문제와 Diffie-Hellman 문제의 어려움에 기반하여 설계되었다.

1. 중간 침입자 공격

SPKA에서 참여자들간에 전송되는 메시지들인 X_A, X_B, V_A, V_B를 공격자는 중간에서 가로채거나 수정하여 참여자에게 전송할 수 있다. 그러나 공격자 X_A, X_B, V_A, V_B 값을 획득하더라도 a, b, Q, Q^{-1}, g^a, g^b, K_A, K_B 값은 이산대수 문제와 Diffie-Hellman 문제의 어려움에 근거하기에 안전하다. 공격자는 a, b, Q, Q^{-1}에 관한 지식 없이는 X_A와 X_B로부터 Y_A와 Y_B를 계산할 수 없고, K_A와 K_B를 계산할 수 없다.

A는 Q를 사용하여 X_A와 Y_A를 계산하고 B는 Q^{-1}을 사용하여 X_B와 Y_B를 계산한다. 이러한 비대칭적인 속성은 기존의 프로토콜의 문제점인 후방향 재전송 공격을 막을 수 있다.

그리고 공격자가 X_A와 X_B를 중간에서 위조하여 각각 A와 B에게 전송한다면, 이 위조된 값들은 A와 B에 의해 세션키 K_A와 K_B를 생성하는데 사용되게 된다. A는 a를 사용하여 K_A를 계산하고 B는 b를 사용하여 K_B를 계산하기 때문에 K_A와 K_B의 값이 같게 될 확률이 거의 없다. 혹시 K_A와 K_B의 값이 같게 계산된다 할지라도 SPKA는 이러한 중간 침입자 공격을 탐지할 수 있다. 즉, 세션키 검증단계에서 A와 B는 각각 V_A와 V_B를 주고받고 A는 V_B를, B는 V_A를 검사하게 되는데, 이는 자신들이 보냈던 Y_A와 Y_B의 정확성뿐만 아니라 K_A와 K_B의 동일성까지 검사하기 때문이다.

또한 공격자는 참여자로 위장하여 정상적인 방법으로 합법적인 참여자와 키를 공유하려고 하거나 패스워드에 관한 정보를 얻으려고 할 수 있다.

그러나 이러한 위장 공격은 상대에게 패스워드에 관한 정보를 제공하지 못하므로 키 검증단계에서 모두 탐지될 것이다.

2. 패스워드 추측 공격

공격자는 과거에 전송되었던 메시지나 패스워드 사전을 이용하여 패스워드 추측 공격을 수행할 수 있다. 그러나 전송 메시지인 X_A, X_B, V_A, V_B는 각각 이산대수 문제의 어려움에 근거하고 있어서 공격자는 패스워드 추측에 필요한 충분한 정보를 얻을 수 없다. 그러므로 제안된 프로토콜은 패스워드 추측 공격에 안전하다.

3. 완전한 전방향 보안성

SPKA에서 Q값을 구하는 방법이 알려져 있다는 가정 하에 공격자가 패스워드 P를 알아내었다면 공격자는 Q와 Q^{-1}값을 구할 수 있다. 공격자가 Q와 Q^{-1}을 안다면 1단계와 2단계의 X_A와 X_B를 가로채 Q와 Q^{-1}를 지수승하여 g^a와 g^b도 구할 수 있을 것이다. 그렇지만 g^a와 g^b이 드러난다 할지라도 V_A와 V_B로부터 g^{ab}을 구하는 것은 Diffie-Hellman 문제의 어려움 때문에 불가능하다. 결국, 오랫동안 사용되는 사용자의 패스워드가 공격자에게 노출되어도 과거에 사용되었던 세션키 정보는 알 수 없다.

VI. 결론

본 논문에서는 새롭고 간단한 패스워드 기반의 키 교환 프로토콜을 제안하였다. 먼저, Tseng의 프로토콜과 Ku와 Wang의 프로토콜에 대한 새로운 취약점을 분석하였다. 결국, SAKA를 포함한 SAKA의 변형 프로토콜들은 중간 침입자 공격이나 패스워드 추측 공격에 안전하지 못하거나 완전한 전방향 보안성을 제공하지 못하였다. 그리고, 기존의 프로토콜들이 가진 문제점들을 해결하기 위해서 새로운 키 교환 프로토콜을 제안하였다. 제안한 프로토콜은 구성이 무척 간단하기 때문에 하드웨어나 소프트웨어로 구현하기에 무척 용이할 것으로 기대된다.

참고문헌

[1] Seo D.H., and Sweeney P., "Simple authenticated key agreement algorithm," *IEE Electronics Letter*, 1999, 35, (13), pp. 1073-1074

[2] Tseng Y.M., "Weakness in simple authenticated key agreement protocol," *IEE Electronics Letter*, 2000, 36, (1), pp. 48-49

[3] Ku W.C., and Wang S.D., "Cryptanalysis of modified authenticated key agreement protocol," *IEE Electronics Letter*, 2000, 36, (21), pp. 1770-1771

[4] Lin I.C., Chang C.C., and Hwang M.S., "Security Enhancement for the Simple Authentication Key Agreement Algorithm," *24th Ann. Int. Computer Software and Applications Conf.*, 2000, pp. 113-115

[5] Hsieh B.T., Sun H.M., and Hwang T., "Cryptanalysis of enhancement for simple authentication key agreement algorithm," *IEE Electronics Letter*, 2002, 38, (1), pp. 20-21

[6] Diffie W., and Hellman M.E., "New directions in cryptography," *IEEE Trans., IT-22*, 1976, (6), pp. 644-654

[7] Sun H., "On the security of simple authenticated key agreement algorithm," *Proceedings of the Management Theory Workshop* 2000, 2000

[8] Simon B.W. and Alfred M., "Authenticated Diffie-Hellman Key Agreement Protocols," *Proceedings of SAC 98, LNCS*, 1998