Diffie-Hellman을 이용한 패스워드 기반의 사용자 인증 및 키 교환 프로토콜†

최재덕*, 정수환*

*숭실대학교, 정보통신전자공학부

A password-based user authentication and key-agreement protocol using Diffie-Hellman†

Jaeduck Choi*, Souhwan Jung*

*School of Electronics Engineering Soongsil Univ.

요 약

본 논문에서는 DH(Diffie-Hellman) 기반의 사용자 인증 및 키 교환 프로토콜인 SAK(Simple Authentication and Key-agreement)를 제안하고자 한다. 제안 프로토콜 SAK는 단순하고 사용하기 쉬운 패스워드와 이산 대수 문제의 어려움을 이용하여 안전하고 효율적이다. 패스워드 기반 프로토콜의 취약점인 사전 공격(Dictionary attack)과 알려진 공격으로부터 안전하고 DH 기반의 기존 프로토콜보다 적은 지수 계산량을 요구한다.

I. 서론

안전하지 못한 환경에서 서버에 접속하고자 하는 경우 사용자 인증 및 암호화 통신은 반드시 필요하다. 대표적으로 사용되는 것이 패스워드로 인증 및 키 교환 프로토콜에서는 안전성과 효율성을 고려하여야 한다. 패스워드는 사람이 기억할 수 있는 범주 내에서 사용되어야 한다는 한계 때문에 사전 공격에 매우 취약하다. 이러한 문제점을 해결하기 위해서 패스워드를 이용한 프로토콜은 DH 알고리즘 또는 공개키 암호 알고리즘을 사용하여 사전 공격, Replay attack, Man-in-the-middle attack 등과 같이 알려진 공격에 대하여 안전을 강화한다.

사용자 인증 및 키 교환 프로토콜의 효율적인 측면은 프로토콜에서 요구되는 계산량에 따른다. 프로토콜에서는 해쉬 함수, Random 함수, 지수 계산 등이 사용되는데 지수 계산이 가장 많은 계산량을 요구한다. DH 알고리즘 또는 공개키 알고리즘을 사용하는 인증 및 키 교환 프로토콜에서는 이러한 지수 계산을 얼마나 최소화하는 것이 관건이다.

본 논문에서는 DH과 패스워드 식별자 기반(verified-based)으로 사전 공격 등과 같은 알려진 공격으로부터 안전하고 기존의 DH 기반의 프로토콜보다 적은 계산량을 요구하는 사용자 인증 및 키 교환 프로토콜을 설계한다.

II장에서는 기존의 DH 기반의 사용자 인증 및 키 교환 프로토콜에 대해서 간략히 정리를 하고, III장에서는 제안 프로토콜에 대해서 설명을 하고, IV장에서는 제안 프로토콜의 안전성 분석 및 특징에 대해서 알아보고 V장에서 결론을 맺고자 한다

II. 관련 기술

인증 및 키 교환 프로토콜은 패스워드와 공개키 암호 알고리즘 또는 DH 알고리즘을 사용하여 메시지 송·수신을 위한 암호화 키 생성 및 사용자 인증을 수행한다.

공개키 암호 알고리즘은 RSA를 이용하는 방법이 대표적이며 A-EKE[7], OKE[8], SNAPI-X[9] 등이 있으나 많은 연산량을 요구하는 단점이 있다.

키 교환 알고리즘으로 가장 널리 알려진 DH 알

† 본 연구는 학술진흥재단 협동연구과제(과제번호 2001-042-E00045) 지원으로 수행하였습니다.

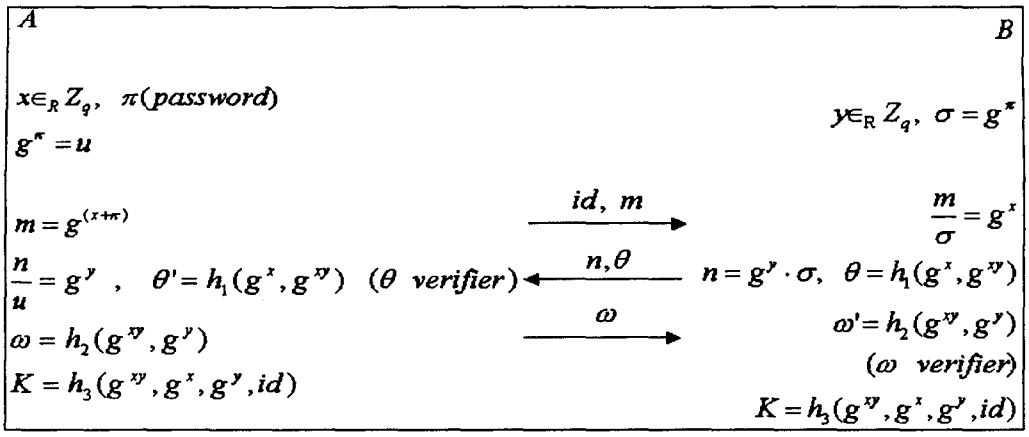

그림 1: SAK.

고리즘은 DLP(Discrete Logarithm Problem)를 기반으로 하고 있다. 대표적인 프로토콜로는 B-SPEKE[2], SRP[3], AMP[4], PAK-X[5] 등이 있으며 이들은 DH에 패스워드를 추가하여 사용자 인증 및 세션키를 생성한다. 각각의 프로토콜은 통신회수 및 연산량에 따라 장단점을 갖는다. B-SPEKE는 4회의 통신회수와 사용자와 서버간의 각각 3회, 4회의 지수 연산량을 요구한다. SRP는 사용자와 서버사이의 패스워드 정보를 비대칭으로 저장하여 패스워드가 직접 노출되지 않게 하고 4회의 통신회수와 각각 3회씩의 지수 연산량을 요구한다. AMP 프로토콜은 사용자와 서버에서 각각 2회씩의 지수 연산량을 요구하지만 통신 회수는 4회를 갖는다. PAK-X 프로토콜은 패스워드를 공유하여 사용자와 서버사이에 유일한 식별자를 생성한다. 통신회수 3회와 지수 연산량 각각 4회씩의 연산량을 요구한다. 각 프로토콜 비교는 IV장의 표 1에 따로 정리하였다.

III. 제안 프로토콜

이번 장에서는 제안 프로토콜 SAK에 대해서 설명한다. SAK는 패스워드 식별자 기반으로 이산대수 문제의 어려움을 이용하여 상호 인증 및 세션키를 생성한다. 통신회수는 3회로 그림 1과 같이 전체적인 구조를 갖는다. Step 1에서 서버 B에 전송되는 메시지는 DH 파라미터 g^x 와 패스워드 식별자의 값으로 구성되어 있다. Step 2에서는 서버가 갖고 있는 식별자 σ와 사용자로부터 받은 메시지 m을 이용하여 서버 인증을 위한 비밀 정보 g^{xy} 값과 θ 값을 계산하여 A에게 전송한다. Step 3에서도 g^{xy}값과 사용자의 정상적인 패스워드 식별자와 서버로부터 받은 메시지 n을 이용하여 비밀정보 g^{xy}와 사용자 인증 정보 ω를 생성한다.

● Notation

A, B : 통신자 (사용자, 서버)

π : 공유한 패스워드

g, q : 공개 파라미터 생성자(g) , 소수(q)

x, y : A와 B의 임의의 값

h_1, h_2, h_3 : 일 방향 해쉬 함수

K : 세션키

σ : 패스워드 식별자

● 설정단계

A와 B는 공개 파라미터 g, q를 공유하며 사용자 패스워드 π를 이용하여 식별자 g^{π} 를 생성한다. 서버 B는 식별자 $\sigma = g^{\pi}$를 패스워드 파일로 저장한다.

● 실행단계

① A는 패스워드 π를 이용하여 식별자 g^{π}를 생성하고 $x \in_R Z_q$를 만족하는 값을 선택하여 메시지 $m = g^{(x+\pi)} \bmod q$를 id와 함께 서버 B에 전송한다.

② ①의 메시지를 받은 B는 $y \in_R Z_q$를 만족하는 값을 선택하여 $n = g^y \cdot \sigma \bmod q$를 계산하

고 A로부터 받은 메시지 m을 식별자 σ로 나누어 g^x값을 계산한다. B는 g^{xy}를 계산한 후 서버 인증 정보 $\theta = h_1(g^x, g^{xy})$를 계산하고 이들 결과 값 n, θ를 A에게 전송한다.

③ ②의 메시지를 받은 A는 $\frac{n}{u} = g^y$를 계산하여 g^{xy}를 구한다. A는 자신이 보내준 g^x값이 B의 식별자에 의해 정상적으로 구해졌는지를 $\theta = h_1(g^x, g^{xy})$값을 통해서 서버 인증을 한다. 서버 인증이 정상적으로 이루어지면 A는 자신의 인증 값 $\omega = h_2(g^{xy}, g^y)$를 생성한다. ω는 g^{xy}값과 서버의 g^y값이 A의 패스워드 정보 (u)를 통해 정상적으로 구해진 값이다.

④ ③의 메시지를 받은 B는 자신이 생성한 g^y값을 사용하여 A와 같이 계산된 ω를 검증하여 A를 인증 한다. 상호 인증 후 생성된 세션키는 $K = h(g^{xy}, g^x, g^y, id)$이다.

IV. 안전성 분석

이번 장에서는 SAK의 안전성 분석과 기존 프로토콜과 비교하여 갖는 특징에 대해서 논한다.

1. SAK의 안전성

1) Dictionary attack

사전 공격은 인증 및 키 교환 프로토콜에서 가장 주의해야 할 공격 유형이다. 공격자는 사용자나 서버로 위장하여 패스워드 추측에 필요한 정보를 획득한 후 임의의 패스워드를 대입하여 획득한 정보와 비교하여 패스워드를 추측해 낸다.

먼저 SAK에서 공격자가 사용자로 위장하였을 경우 임의의 패스워드 π'을 사용하여 $m' = g^{x+\pi'}$를 서버 B에 전송한다. 서버 B는 메시지 m'과 식별자 σ를 이용하여 $\frac{m'}{\sigma} = g^{x+\pi'-\pi}$를 계산하고 서버쪽 DH 파라미터 n은 식별자를 이용하여 $g^y \cdot \sigma = g^y \cdot g^{\pi}$와 같이 계산한다. B는 서버 인증 정보 θ를 $\theta = h_1(g^{x+\pi'-\pi}, g^{xy} \cdot g^{(\pi'-\pi)y})$과 같이 계산하여 메시지 n과 함께 사용자 A에 전송한다. 공격자 A는 임의의 패스워드 정보 $g^{\pi'}$ 을 이용하여 서버의 DH 파라미터를 $g^{y+\pi-\pi'}$과 같이 구한다. 서버의 인증 정보 θ를 검증하기 위해 공격자 A가 계산한 θ'은 $\theta' = h_1(g^x, g^{xy} \cdot g^{(\pi-\pi')x})$가 되나 서버의 y값을 모르기 때문에 공격자 A는 패스워드 추측을 통한 사전 공격을 할 수 없다.

공격자가 서버로 위장하였을 경우 Step 1에서 받은 m메시지 만으로는 공격이 불가능 하다. Step 2에서 공격자 B는 DH 파라미터 n'을 $n' = g^y \cdot \sigma' = g^y \cdot g^{\pi'}$과 같이 계산하고 공격자의 인증정보 θ'을 $\theta' = h_1(g^{x+\pi-\pi'}, g^{xy} \cdot g^{(\pi-\pi')y})$와 같이 생성하여 사용자 A에게 메시지 n'과 함께 전송한다. 사용자는 θ' 검증 과정에서 공격자가 임의의 패스워드를 사용하여 보냈기 때문에 사용자 A의 $\theta = h_1(g^x, g^{xy} \cdot g^{(\pi'-\pi)x})$값과 틀리므로 서버 인증에 실패한다. 이 후 공격자 B는 사용자 A로부터 공격에 필요한 추가 정보 획득을 할 수 없으므로 패스워드 추측을 통한 사전 공격은 불가능하다.

2) Replay attack

Replay attack은 공격자가 사용자와 서버 사이에 이미 주고받은 메시지를 통해 공격하는 유형이다. SAK는 매 세션마다 DH 임의의 값 g^x와 g^y를 사용하기 때문에 메시지를 재 사용하여 공격한다는 것은 불가능하다.

3) PFS(Perfect Forward Secrecy)

PFS는 현재의 세션키를 알고 있어도 이전의 세션키를 알 수 없다는 것이다. SAK는 세션키 생성 시 매 세션마다 임의의 값 g^x와 g^y를 사용하여 생성하고 이전의 키 생성과 독립적으로 생성이 되기 때문에 PFS를 제공한다.

4) Denning-Sacco attack

Denning-Sacco attack은 이전의 세션키를 알고 있을 때 패스워드 추측이 가능한 공격 유형이다. SAK는 DLP 기반의 세션값 g^{xy}값과 사용자와 서버에서 각각 패스워드 식별자를 이용하여 얻은 g^x, g^y 을 사용하여 세션키를 생성하기 때문에 키가 노출되어도 패스워드 추측은 불가능하다.

5) MITM(Man-In-The-Middle) attack

MITM attack은 공격자가 사용자와 서버 사이에서 둘 간에 메시지를 가로채어 "사용자-공격자-서버"와 같이 두 세션을 생성해 공격하는 유형이다. SAK는 패스워드 정보를 사용하기 때문에

MITM으로부터 안전하다.

SAK는 위에서 살펴본 것과 같이 기존의 프로토콜과 같이 사전 공격 및 알려진 공격에 대해서 안전하다.

2. SAK의 특징

이번 절에서는 DH 기반의 기존 프로토콜 B-SPEKE, SRP, AMP, PAK-R, PAK-RY, PAK-X와 SAK을 비교하여 장점을 알아본다. 표 1은 DH 기반의 기존 프로토콜과 SAK의 통신회수 및 계산량을 비교한 것이다. B-SPEKE, SRP, AMP는 통신회수 4회를 요구하지만 SAK는 3회의 통신회수를 갖는 장점이 있다. 같은 통신회수를 갖는 PAK 계열 프로토콜과 연산량을 비교했을 때 SAK는 사용자와 서버에서 각각 3회와 2회를 요구하기 때문에 계산량에 있어서 보다 효율적이다. PAK-R 프로토콜도 지수 계산량 3회씩으로 SAK와 같지만 PAK-R은 패스워드 식별자 기반의 프로토콜이 아닌 패스워드 자체를 사용하고 있는 단점이 있다. PAK-X는 사용자와 서버 사이에서 실제 통신 중일 때 사용자측에서 3회의 지수 연산을 수행하지만 SAK는 사용자측에서 프로토콜 동작 전에 2회의 지수 계산을 미리 실시하기 때문에 실제 서버와 통신시에는 1회의 지수 계산만을 한다. SAK는 PAK-X 프로토콜의 지수 계산량 각각 4회씩을 사용자와 서버에서 각 3회와 2회로 줄여 보다 간단하게 설계하였다.

표 1: DH 기반의 프로토콜 비교.
(C : Client, S : Server)

프로토콜	통신회수	Hash 함수		지수 연산		Random 생성	
		C	S	C	S	C	S
B-SPEKE	4	1	1	3	4	1	2
SRP	4	3	2	3	3	1	1
AMP	4	4	4	2	2	1	1
PAK-R	3	3	3	3	3	2	1
PAK-RY	3	3	3	4	5	3	1
PAK-X	3	4	4	4	4	1	2
SAK	3	3	3	3	2	1	1

V. 결론

본 논문에서는 DH을 이용하여 안전하고 효율성이 높은 패스워드 기반의 사용자 인증 및 키 교환 프로토콜을 설계하였다. 제안 프로토콜 SAK는 패스워드 식별자 기반으로 이산 대수 문제의 어려움을 이용하여 사전 공격 등과 같은 알려진 공격으로부터 안전하고 기존의 프로토콜보다 사용자 측면에서 지수 계산량을 4회에서 3회로 줄여 효율성을 높였다.

SAK는 기존의 프로토콜보다 지수 계산량을 줄여 효율적이지만 앞으로 현재의 지수 계산량보다 적은 프로토콜 설계가 필요하다.

참고문헌

[1] 손기욱, 서인석, 원동호, "패스워드 기반 키 분배 프로토콜 표준화 동향," 정보보호학회지, pp 46-55, 2002년 8월.

[2] D. P. Jablon, "Extended Password Key exchange Protocols Immune to Dictionary Attack," In WETICE '97 Enterprise Security Workshop. Cambridge. MA, June 1997.

[3] T. Wu, "The SRP Authentication and Key Exchange System," Internet Society Symposium on Network and Distributed System Security, pp. 97-111, Mar 1998.

[4] T. Kwon, "Authentication and Key Agreement via Memorable Passwords," NDSS 2001 Symposium Conference Proceedings, February 7-9. 2001.

[5] V. Boyko and P. MacKenzie and S. Patel, "Provably Secure Password Authenticated Key Exchange Using Diffie-Hellma," Advances in Cryptology - EUROCRYPT 2000, May 14-18. 2000.

[6] 박호상, 정수환, "패스워드 기반의 상호 인증 및 키 교환 프로토콜", 정보보호학회논문지, pp 37-43, 2002년 10월.

[7] Steven M. Bellovin. Michael Merritt, "Augmented Encrypted Key Exchange : a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise," Proceedings of the First ACM Conference on Computer and Communications Security, 1993.

[8] S. Lucks, "Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys," The Security Protocol Workshop '97, Ecole Normale Sperieure, April 7-9, 1997.

[9] P. MacKenzie and R. Swaminathan, "Secure Network Authentication with Password Identification," Presented to IEEE P1363a, August, 1999.