공유 패스워드를 이용한 클라이언트/서버 인증 키 교환 프로토콜

(A Client/Sever Authenticated Key Exchange Protocol using Shared Password)

류 은 경 † 윤 은 준 †† 유 기 영 †††

(Eun-Kyung Ryu) (Eun-Jun Yoon) (Kee-Young Yoo)

요 약 본 논문에서는 사용자와 서버가 사전에 공유한 패스워드 정보를 이용하여 안전하게 세션키를 생성하는 인증 키 교환 프로토콜을 제안한다. 제안된 프로토콜은 디피헬만 스킴을 기반으로 하며, 인증 키 교환 프로토콜 설계시 요구되는 여러 암호학적 안전성에 대한 요구조건을 만족한다. 제안된 프로토콜은 수동적 또는 능동적 공격자에 의한 오프라인 사전공격에 안전하고, 전방향 안전성을 가진다. 특히, 기존의 연구된 인증 키 교환 프로토콜들과는 달리 제안된 프로토콜은 서버의 패스워드 파일과 같은 사용자 인증파일이 공격자에게 유출되었을 때 공격자의 사용자 또는 서버 위장공격에 안전하다는 장점이 있다. 또한, 제안된 프로토콜은 성능면에서 기존의 주요 프로토콜들과 비교해서 보다 효율적이다.

키워드 : 패스워드, 인증, 키 교환/합의 프로토콜, 디피헬만

Abstract In this paper, we propose a new authenticated key exchange protocol in which client and sever can mutually authenticate and establish a session key over an insecure channel using only a human memorable password. The proposed protocol is based on Diffie-Hellman scheme and has many of desirable security attributes: It resists off-line dictionary attacks mounted by either passive or active adversaries over network, allowing low-entropy passwords to be used safely. It also offers perfect forward secrecy, which protects past sessions when passwords are compromised. In particular, the advantage of our scheme is that it is secure against an impersonation attack, even if a server's password file is exposed to an adversary. The proposed scheme here shows that it has better performance when compared to the previous notable password-based key exchange methods.

Key words : Password, Authentication, Key Exchange/Agreement, Diffie-Hellman

1. 서 론

인증 키 교환 프로토콜은 통신을 원하는 통신 당사자 각각이 제공하는 정보에 의해 상호인증 및 세션키를 공유하는 과정으로, 이때 생성된 키는 기밀성, 무결성과 같은 암호학적인 목적을 달성하기 위해 사용된다. 안전한 인증 키 교환 프로토콜은 쇼핑몰, 인터넷 뱅킹과 같이 인증, 기밀성, 무결성 등과 같은 보안 서비스를 필요로 하는 전자상거래에서 아주 중요하다. 현재까지 연구된 인증 키 교환 프로토콜은 통신 당사자가 공유키를 생성하는데 제공하는 정보에 따라 크게 두 종류, 대칭적 프로토콜과 비대칭적 프로토콜로 분류할 수 있다[1].

대칭적 프로토콜에서, 두 통신 당사자는 미리 공유한 비밀 값을 이용하는 반면, 비대칭적 프로토콜에서는 사전에 인증된 공개된 암호학적 키 정보를 이용한다. 이때, 사용되는 키는 알고리즘과 안전성의 정도에 따라 약 100 비트에서부터 수천 비트에 이르기까지 랜덤하게 선택된다. 그러나, 사용자들은 암호학적인 키의 길이가 너무 길고, 키들을 저장하기 위해 스마트카드, 메모리와 같은 안전한 저장 공간이 따로 필요하거나, 인증서 또는 키서버와 같은 제 3의 신뢰기관 등이 요구됨으로 암호시스템의 사용에 부담을 가지고 있다. 이에 반하여, 미리 공유된 비밀 값만을 이용하는 대칭적 프로토콜은 암호학적 키를 저장하기위한 어떤 부가적인 장치 또는 인

· 본 논문은 2003년도 두뇌한국21사업에 의하여 지원되었음
† 비 회 원 : 경북대학교 컴퓨터공학과
ekryu@infosec.knu.ac.kr
†† 학생회원 : 경북대학교 컴퓨터공학과
ejyoon@infosec.knu.ac.kr
††† 종신회원 : 경북대학교 컴퓨터공학과 교수
yook@knu.ac.kr
논문접수 : 2003년 10월 7일
심사완료 : 2004년 2월 10일

증서 등을 요구하지 않고 패스워드와 같이 비교적 짧은 길이의 비밀값만을 이용한다는 장점 때문에 현재 많은 연구가 이루어지고 있다. 본 논문은 대칭적 프로토콜인 패스워드 기반의 인증 키 교환 프로토콜에 초점을 둔다.

패스워드 기반의 인증 키 교환 프로토콜은 다시 대칭구조와 비대칭구조로 분류될 수 있다. 대칭구조 프로토콜은 사용자와 서버가 각각 같은 값을 이용하여 서로 적법한 사용자 그리고 적법한 서버라는 것을 검증하는 프로토콜이고, 비대칭 구조를 갖는 프로토콜은 사용자는 자신의 패스워드를, 서버는 사용자의 패스워드로부터 유도된 검증자를 가지며 각각 패스워드, 검증자를 이용하여 상호 검증한다. 대칭구조의 경우 서버가 저장하고 있는 사용자 패스워드 파일을 공격자가 얻게 되면 그 공격자는 항상 사용자 또는 서버 위장공격을 할 수 있다. 이러한 대칭구조를 갖는 패스워드 기반 인증 키 교환 프로토콜에는 EKE[2], SPEKE[3] 등이 있다. 이러한 문제점을 개선하기 위해 제시된 프로토콜이 비대칭구조 프로토콜이며, 비대칭구조를 갖는 주요 프로토콜에는 B-SPEKE[4], SRP[5], AMP[6], PAK-RY[7] 등이 있다. 비대칭구조 프로토콜에서 공격자는 서버가 저장하는 사용자 패스워드 파일을 공격자가 얻더라도 곧바로 사용자 위장공격을 할 수 없다. 그러나 비대칭구조를 갖는 프로토콜 역시 서버의 사용자 패스워드 파일 유출시 공격자는 오프라인 사전공격을 통해 사용자 또는 서버 위장공격이 가능하다. 다시 말해서, 기존의 패스워드 기반의 인증 키 교환 프로토콜은 대칭, 비대칭구조 구분 없이 서버의 사용자 패스워드 파일이 유출될 경우 공격자의 위장공격에 취약하다는 문제점이 있다.

본 논문에서는 사용자와 서버가 서로 공유한 패스워드 정보를 이용해서 서로 안전한 통신을 할 수 있는 보다 안전하고 효율적인 인증 키 교환 프로토콜을 제안한다. 제안된 프로토콜의 안전성은 잘 알려진 두 가지 가정, 이산대수 및 디피헬만(Diffie-Hellman) 가정을 기반으로 하며, 인증 키 교환 프로토콜 설계시 요구되는 여러 요구사항들을 만족한다. 제안된 프로토콜은 엔트로피가 낮은 패스워드를 안전하게 사용할 수 있으며, 네트워상에서 수동적 공격자 또는 능동적 공격자에 의한 오프라인 사전공격에 대응할 수 있다. 또한 어떤 경로를 통해서 패스워드가 유출된다 하더라도 공격자가 과거 통신내용을 복호화 할 수 없는 전방향 보안성을 갖는다. 특히, 기존의 패스워드 기반의 인증 키 교환 프로토콜과는 달리 제안된 프로토콜은 서버의 패스워드 파일과 같은 사용자 인증파일 유출시, 공격자의 사용자 또는 서버 위장공격에 안전하다는 장점을 갖는다. 제안된 프로토콜은 기존의 주요 패스워드 기반 인증 키 교환 프로토콜들과 비교했을 때 보다 안전할 뿐 아니라 성능 면에서도 보다 나은 효율성을 보인다.

본 논문의 구성은 다음과 같다. 2장에서 인증 키 교환 프로토콜 설계시 고려해야 할 암호학적 안전성 및 성능에 대해서 간략히 논의한다. 3장에서는 본 논문에서 제안하는 공유 패스워드를 이용한 클라이언트/서버 인증 키 프로토콜에 대해서 기술하며 4장에서는 제안된 프로토콜에 대한 암호학적 안전성 분석과 기존에 연구된 프로토콜들과의 효율성을 비교분석한다. 마지막으로 5장에서는 결론을 맺는다.

2. 인증 키 교환 프로토콜 설계시 요구사항

2.1 공격유형 및 안전성 요구사항

안전한 인증 키 교환 프로토콜은 공격자가 적법한 사용자와 서버의 통신내용을 엿봄으로써 공격할 수 있는 수동적 공격뿐만 아니라, 공격자가 사용자와 서버 중간에서 전송되는 메시지에 추가적인 정보를 삽입, 삭제함으로써 공격할 수 있는 능동적 공격에 안전해야 한다[8, 9]. 본 논문에서 제안하는 프로토콜은 공격자의 수동적 또는 능동적 공격뿐만 아니라 다음과 같은 인증 키 교환 프로토콜 설계시 요구되는 여러 암호학적 안전성에 대한 요구조건들을 만족한다.

데닝사코(Denning Sacco) 공격: 사용자와 서버간의 키 교환 프로토콜에서 프로토콜의 각 인스턴스는 유일한 키를 생성하며, 이때 생성되는 키를 세션키라고 부른다. 만일 공격자가 어떤 경로를 통해 특정 세션에 사용된 세션키를 알았을 경우, 공격자가 알고 있는 세션키를 이용하여 이후 세션의 세션키를 생성하거나, 오프라인 사전공격을 통해 패스워드를 계산하는 공격이 데닝사코 공격이다. 따라서, 인증 키 교환 프로토콜은 공격자에게 세션키가 노출되더라도 패스워드에 대한 어떤 정보도 노출되지 않아야 하며 이후에 사용될 세션키에 대한 안전성도 보장되어야 한다.

전방향 보안성: 사용자와 서버간에 공유된 패스워드가 어떤 경로를 통해 유출 되었을 때 유출된 패스워드의 영향을 최소화하여야 한다. 다시 말해서, 전방향 보안성을 보장한다는 것은 패스워드가 유출된 상황에서 그 패스워드를 이용하여 이전에 사용된 세션키들을 계산할 수 없음을 의미한다.

서버의 사용자 패스워드 파일 유출에 대한 대응: 일반적으로 서버는 사용자의 패스워드를 검증할 수 있는 검증인자를 저장한 패스워드 파일을 가진다. 사용자가 안전하게 자신의 패스워드를 가지고 있다 하더라도 서버가 노출될 위험은 여전히 존재한다. 서버가 노출되었을 때 공격자가 정당한 서버인 것처럼 속이는 공격에 대해 보호할 수 없다. 그러나, 서버의 패스워드 파일이 유출된 경우 공격자의 추가적인 사전공격 없이 행하는

공격자의 사용자 위장공격에 대응할 수 있어야 한다.

2.2 프로토콜의 성능 요구사항

인증 키 교환 프로토콜의 성능은 다음과 같은 인수들에 의존한다[9].

- 전송되는 메시지 교환 횟수
- 메시지의 크기
- 산술적 연산량

따라서, 인증 키교환 프로토콜 설계를 위해서는 전송되는 메시지 교환 횟수, 메시지의 크기, 산술 연산량과 같은 효율성에 관한 성질을 고려해야한다.

3. 제안한 프로토콜

본 장에서는 앞에서 기술한 인증 키교환 프로토콜 설계시 요구사항들을 만족하는 보다 안전하고 효율적인 클라이언트/서버 인증 키교환 프로토콜을 제안한다.

3.1 가정 및 시스템 파라미터

본 논문에서 제안하는 프로토콜은 수학적인 가정과 계산적인 가정에 기반하고 있다. p와 q는 $p=2q+1$를 만족하는 충분히 큰 소수이고, G는 위수가 q인 Z_p^*의 서브그룹이라 하자. 프로토콜 수행이 시작되기 전에 시스템의 공개 파라미터인 생성자 $g \in G$ 와 함수 H_1, H는 미리 정의되었다고 가정한다. 이때, H_1은 $\{0,1\}^* \rightarrow Z_p^*$ 이고 H는 안전한 일방향 해쉬 함수이다. 제안하는 프로토콜은 대부분의 암호 프로토콜들의 암호학적 안전성에 근간을 이루는 이산대수 및 디피헬만(Diffie-Hellman) 가정에 기반을 둔다. 이 가정들은 다음과 같다.

이산대수 가정(Discrete Logarithm Assumption: DLA) : 이산대수 문제는 $g^a = y$ 및 g가 주어질 때 $a = \log_g y$를 계산하는 것이다. 이때 $g \in G$이고 $a \in Z_q$, $a \in 0, 1, \ldots, q-1$ 이다. 이산대수 가정은 그룹 G의 위수가 q이고, q 가 충분히 큰 소수라면, $g, y \in G$가 주어질때 $a = \log_g y$ 를 구하는 것은 계산적으로 어렵다는 것이다.

계산적 디피헬만 가정(Computational Diffie-Hellman Assumption: CDHA)

계산적 디피헬만 문제는 g^a와 g^b로부터 g^{ab}를 계산하는 것이다. 이때 $g \in G$이고, $a, b \in Z_q$ $a, b \in 0, 1, \ldots, q-1$ 이다. 계산적 디피헬만 가정은 g, g^a, g^b가 주어져도 g^{ab}를 구하는 것은 계산적으로 어렵다는 것이다.

프로토콜에서 두 통신 당사자 사용자 및 서버를 각각 A와 B라고 지칭한다. A는 기억 가능한 패스워드 π를 가지고 B는 패스워드를 검증할 수 있는 패스워드 검증자 I를 저장한다. 이때 검증자 I를 유도하는데 사용되는 서버의 마스터키 s는 안전하게 저장된다고 가정한다. 패스워드 π로부터 I를 유도하는 과정은 3.2절에서 설명할 것이다. 안전한 비트 크기를 나타내는 변수 k는 사전공격에 안전하도록 충분히 커야 한다. 일반적으로 k는 해쉬함수 출력 값의 비트 수와 같이 생각될 수 있다. 프로토콜에서 덧셈, 뺄셈 그리고 지수 연산에서 mod p 표기는 생략한다. 본 논문에서 사용되는 표기는 다음과 같다

표 1 프로토콜에서 사용되는 표기

표 기	의 미
A, B	사용자, 서버
π	사용자의 패스워드
P	π로부터 유도된 정수
s	서버의 마스터키
I	s와 P로부터 유도된 패스워드 검증자
p, q	$p=2q+1$를 만족하는 큰 소수
G	위수가 q인 유한군
g	군 G의 생성자
a, b	A와 B가 각각 선택하는 랜덤 정수
Z_{AB}	A와 B에 의해 계산되는 공유 비밀값
k	안전한 비트크기를 나타내는 변수
H_1	패스워드 π를 Z_p^*의 정수로 변환하는 함수
H	안전한 일방향 해쉬 함수
$F(\cdot)$	세션키 유도함수
K_{AB}	세션키

3.2 프로토콜

3.2.1 시스템 초기화

A는 자신의 패스워드 π를 선택한 후 안전한 채널을 통해 π를 B에게 전송한다. B는 먼저, $P = H_1(\pi)^2$를 계산한 후, P와 자신의 마스터 키 $s \in_R Z_q^*$를 사용하여 패스워드 검증자 $I = P^s$를 계산하여 사용자 패스워드 파일에 저장한다.

3.2.2 프로토콜 수행

A와 B의 세션키 교환을 위한 프로토콜 수행과정은 그림 1과 같다. 프로토콜 수행과정에서 각각의 단계를 설명하면 다음과 같다.

① $A \Rightarrow B$: T_A

A는 랜덤 정수 a를 선택하고, $T_B = g^a + P$를 계산한다. 이때 $P = H_1(\pi)^2$는 자신의 패스워드로부터 유도되는 정수이다. A는 계산한 T_A를 B에게 보낸다.

② $A \Leftarrow B$: T_B, V_B

B는 T_A를 받은 후, 자신의 랜덤 정수 b를 선택하여 먼저 $T_B = g^b$를 계산하고, $V_B = H(T_A, T_B, Z_{AB})$를 계산한다. 여기서 $Z_{AB} = (T_A - P)^b$는 A로부터 받은 T_A

와 패스워드 검증자 I, 그리고 B의 마스터키 s로부터 유도된 $P=I^{1/s}$로부터 계산된다. 계산한 T_B와 V_B를 A에게 다시 전송한다.

③ $A \Rightarrow B$: V_A

A는 B로부터 받은 T_B로부터 $Z_{AB}=(T_B)^a$를 계산한 후, V_B의 값이 $H(T_A, T_B, Z_{AB})$와 같은지를 비교한다. 이때 두 값이 같다면 A는 B를 인증하고, $V_A=H(T_B, V_B, Z_{AB})$를 계산하여, V_A를 B에게 전송한다.

B는 A로부터 받은 V_A와 $H(T_B, V_B, Z_{AB})$의 값이 같은지를 확인한다. 만약, 두 값이 같다면 B는 A를 인증한다.

위의 단계들이 성공적으로 끝났다면 A와 B는 세션키 $K_{AB}=F(Z_{AB})$를 계산한다. 이때 F는 세션키 유도 함수이다.

본 논문의 목적은 스마트카드 혹은 기타 하드웨어와 같은 부가적인 장치, 또는 공개키 암호 시스템의 인프라를 이용하지 않고 사용자와 서버가 공유한 패스워드를 이용하여 보다 안전하고 효율적인 클라이언트/서버 인증 키 교환 프로토콜 제안하는 것이다. 특히 제안하는 프로토콜에서 사용자 패스워드가 서버의 마스터키로 암호화된 후 서버에 저장되기 때문에 서버의 패스워드 파일이 유출될 경우 공격자가 패스워드 파일로부터 사용자의 패스워드를 계산하기 위해서는 패스워드 추측과 이산대수(Discrete Logarithm) 문제를 동시에 풀어야 할 것이다. 그러므로 제안하는 프로토콜은 기존의 인증 키 교환 프로토콜들과 비교해서 서버의 사용자 패스워드 파일 유출시 공격자의 사용자 위장 공격에 안전하다는 주요 장점이 있다.

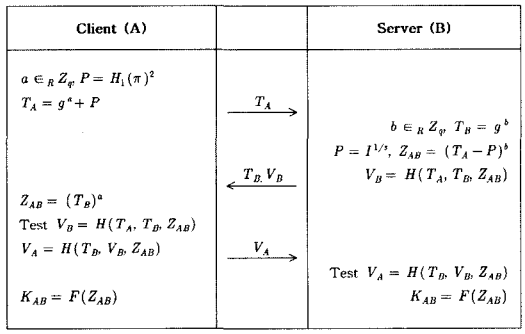
4. 제안한 프로토콜의 안전성 분석 및 효율성

본 장에서는 제안한 프로토콜에 대해서 앞서 기술한 인증 키 교환 프로토콜의 암호학적 안전성 요구사항에 대해서 만족여부를 분석하고, 패스워드를 기반으로 하는 기존의 주요 연구와 효율성을 비교한다.

4.1 안전성 분석

① 수동적 공격: 수동적 공격은 공격자가 통신내용을 엿봄으로써 얻을 수 있는 정보를 이용하여 세션키 생성에 사용되는 공유 키 값에 대한 정보 또는 사용자의 패스워드 정보 와 같은 유용한 정보를 얻는 공격을 말한다. 제안된 프로토콜에서 공격자가 수동적 공격을 통해 의미 있는 정보를 얻는다는 것은 앞서 기술된 디피헬만 가정을 깰 수 있음을 의미한다. 다시 말해서, 제안된 프로토콜에서 수동적 공격은 공격자가 네트웍 상에 전송되는 정보 T_A, T_B, V_A, V_B 로부터 g^{ab}를 계산하는 것이다. 이는 공격자가 먼저 올바른 패스워드 π'를 추측하여 $P'=H_1(\pi')^2$을 계산한 다음 $g^a=T_A-P'$와 g^b로부터 g^{ab}를 계산한다는 것이다. 이것은 공격자가 올바른 패스워드를 추측한다고 가정하더라도 명백히 디피헬만 문제이다. 따라서, 제안된 프로토콜은 디피헬만 가정을 기반으로 공격자의 수동적 공격으로부터 안전하다.

그림 1 제안된 키 교환 프로토콜



② 능동적 공격: 능동적 공격은 공격자가 가지고 있는 정보가 무엇인가에 따라 여러 가지 형태로 나타날 수 있다. 만약 공격자가 사용자의 패스워드를 안다면, 공격자가 서버에 접근시 적법한 사용자로 위장할 수 있다. 마찬가지로, 패스워드 정보를 가진 공격자는 사용자가 서버에 접근할 때 서버를 가장할 수 있다. 이것은 패스워드를 기반으로 인증 서비스를 제공하는 모든 프로토콜에 해당된다. 제안된 프로토콜은 위장공격, 중간자공격 그리고 재전송 공격과 같은 능동적 공격에 안전하다.

- 위장 공격: 위장 공격은 공격자가 사용자를 가장하는 경우와 서버를 가장하는 경우를 생각할 수 있다. 먼저, 공격자가 서버에게 자신이 적법한 사용자인체 가장하기를 원한다고 가정해보자. 이때 공격자는 $X'=g^e+H_1(\pi')^2$를 계산하여 서버에게 전송할 수 있다. 여기서, e는 공격자가 선택한 랜덤 정수이고, π'는 사용자의 패스워드를 추측한 값이다. 서버는 X'를 받은 후 $T_B=g^b$와 $V_B=H(X', T_B, Z_{A'B})$를 계산해서 공격자에게 T_B와 V_B를 전송한다. 사용자를 가장하는 공격자가 서버로부터 T_B와 V_B 값을 받은 후 서버의 사용자 검증 과정을 통과하기 위해서는 $V_E=H(T_B, V_B, Z_{A'B})$를 계산하여 서버에게 전송해야 한다. 이때 $Z_{A'B}=(g^e+H_1(\pi')^2-H_1(\pi)^2)^b$이다. 공격자가 $Z_{A'B}=(g^e+H_1(\pi')^2-H_1(\pi)^2)^b$를 계산하기 위해서는 올바른 패스워드 추측 및 서버로부터 받

은 T_B로부터 $b = \log_g T_B$를 유도해야 한다. 따라서 제안된 스킴은 이산대수 가정을 기반으로 공격자의 사용자 위장 공격에 안전하다. 공격자가 서버를 가장하는 경우 역시, 같은 방법으로 패스워드 정보를 갖지 않은 공격자는 서버 위장공격을 할 수 없음을 알 수 있다.

- 중간자 공격: 중간자 공격은 공격자가 사용자와 서버의 중간 위치에서 두 개체 모두를 속일 수 있음을 의미한다. 그러므로 중간자 공격은 앞서 기술한 서버 혹은 사용자 한쪽을 속이는 위장 공격보다 더 어렵다고 할 수 있다. 프로토콜 수행시 전송되는 모든 메시지를 이용하더라도 패스워드 정보를 가지지 않은 공격자는 사용자 또는 서버 검증 과정을 통과하지 못한다. 제안된 프로토콜에서 사용자 및 서버를 가장하기 위해서는 패스워드 정보를 아는 공격자만이 가능하다.
- 재전송 공격: 재 전송 공격은 과거 세션에서 교환되었던 메시지를 기록하였다가 이를 다음 세션에 사용하여 성공적으로 사용자를 가장하거나, 키 확인 과정을 통과하는 공격을 의미한다. 그러나 프로토콜에서 모든 메시지들은 매 세션마다 랜덤하게 생성되므로, 재전송 공격은 중간자 공격과 마찬가지로 패스워드 정보를 알고 있는 공격자만이 가능하다.

③ 데닝 사코(Denning-Sacco) 공격: 데닝사코 공격은 공격자에게 어떤 특정 세션에 사용된 하나의 세션키가 노출되었을 경우, 공격자가 획득한 세션키를 이용하여 이후 세션의 세션키를 유도하거나, 또는 오프라인 사전공격을 통해 패스워드를 유도할 수 있음을 의미한다. 그러나 제안된 프로토콜에서 공격자는 획득한 세션키와 네트워상에 전송되는 정보들을 결합하여 사용자의 패스워드 정보를 얻지 못한다. 즉, 제안된 프로토콜에서 공격자가 Z_{AB}, V_A, V_B를 결합함으로써 얻을 수 있는 새로운 정보는 없다. 또한 제안된 프로토콜에서 세션키는 매 세션마다 선택되는 랜덤 값에 따라 새로운 키가 생성된다. 따라서 제안된 프로토콜은 데닝 사코 공격으로부터 안전하다.

④ 전방향 보안성: 전방향 보안성을 제공한다는 것은 패스워드가 노출된 경우 이것이 과거에 사용된 세션키의 안전성에 영향을 주지 않음을 의미한다. 사용자의 패스워드가 어떤 경로를 통해서 공격자에게 노출되었다고 가정할 때, 이것은 제안된 프로토콜에서 생성된 과거의 세션키의 안전성에 영향을 미치지 않는다. 제안된 프로토콜에서 세션키는 매 세션마다 선택되는 랜덤 값에 따라 새로운 키가 생성되기 때문에 공격자가 패스워드 정보를 가진다 하더라도 과거 세션에 사용된 키를 계산할 수 없다. 왜냐하면, 세션키를 계산하기 위해서 공격자는 디피헬만 가정을 깨어야 하기 때문이다. 그러므로 제안된 프로토콜은 공격자가 사용자의 패스워드 정보를 알더라도 사용자와 서버 간에 과거의 통신 내용을 복호화할 수 없는 전방향 보안성을 제공한다.

⑤ 서버의 패스워드 파일 유출에 대한 대응: 제안된 프로토콜에서 사용자의 패스워드 π는 서버의 마스터키 s로 암호화되어 패스워드 검증자 $I = P^s$ 형태로 저장되며, 이때 $P = H_1(\pi)^2$이다. 그러므로 서버의 패스워드 파일이 유출되었다고 가정할 때, 제안된 프로토콜에서 공격자가 서버의 사용자 패스워드 파일로부터 사용자의 패스워드 정보를 알기위해서는 다음과 같은 작업이 요구된다. 첫째, 공격자는 먼저 패스워드 π'을 추측하여 P'를 유도한 후 P'와 I을 이용하여 서버의 마스터키 $s' = \log_{P'} I$ 을 계산한다. 둘째, 첫 번째 과정으로부터 얻은 값 s'을 이용하여 $I' = P'^{s'}$을 계산하여, I와 I'의 값이 같은지 비교해서 같다면 추측한 패스워드 P'가 사용자의 패스워드임을 확신하고, I와 I'의 값이 다르다면 위의 과정을 반복 수행한다. 그러나 첫 번째 과정에서 서버의 마스터키 s'값을 구하는 것은 논문 3.1절에서 기술된 이산대수 문제이다. 따라서 제안된 프로토콜은 서버의 패스워드 파일 유출의 경우 이산대수 가정을 기반으로 공격자의 사용자 또는 서버 가장공격에 안전하다.

4.2 효율성

앞 절에서 살펴본 바와 같이, 인증 키 교환 프로토콜의 성능에 영향을 미치는 주요 요소에는 프로토콜 수행시 교환되는 메시지 수, 전송되는 메시지의 크기, 그리고 연산량 등이 있다. 이 절에서는 기존의 연구된 주요 프로토콜들과 제안된 프로토콜의 효율성을 비교하기 위해 프로토콜 수행시 교환되는 메시지의 수(프로토콜 수행 단계) 및 교환되는 메시지의 크기를 통해 통신 오버헤드를 측정하고, 연산량 비교를 위해서는 실행시간이 가장 많이 소요되는 모듈러 지수승의 횟수를 고려한다.

인증을 제공하지 않는 전통적인 디피헬만 키 교환 스킴[10]에서 통신을 원하는 두 통신 당사자 A와 B가 세션키 $K_{AB} = (g^a)^b = (g^b)^a$를 계산하기 위해서는 A와 B는 각각 한번의 메시지 전송과 2번의 모듈러 지수승을 필요로 한다. 통신 당사자간의 인증 기능을 제공하는 디피헬만 스킴은 세션키 교환을 위해 프로토콜 수행시 최소한 2번의 메시지 전송과 4번의 모듈러 지수승이 요구된다. 따라서 키 교환뿐만 아니라 인증 및 키 확인 기능을 제공하기 위해서는 더 많은 메시지 교환 및 연산이 필요하다.

표 2는 사용자와 서버가 공유 패스워드 정보를 이용하여 인증 및 세션키를 생성하는 기존의 주요 인증 키 교환 프로토콜들과 제안된 프로토콜의 효율성을 보여준다. 표에서 보는 바와 같이 B-SPEKE, SRP, 그리고

표 2 공유 패스워드를 이용한 인증 키 교환 프로토콜의 효율성 비교

프로토콜	통신 오버헤드		연산량(모듈러 지수승 횟수)		
	단계	메시지 크기	사용자	서 버	합 계
B-SPEKE	4	$3\|p\|+2k$	3	4	7
SRP	4	$2\|p\|+2k+\|q\|$	3	3	6
AMP	4	$2\|p\|+2k$	2	3	5
PAK-RY	3	$2\|p\|+2k+\|q\|$	5	4	9
제안된 프로토콜	3	$2\|p\|+2k$	2	3	5

AMP는 4번의 메시지 교환이 요구되는 반면 PAK-RY과 제안된 프로토콜은 3번의 메시지 교환 횟수를 갖는다. 그러나, PAK-RY는 메시지 교환 횟수를 줄이는 대신에 더 많은 지수승이 요구되는 반면, 본 논문에서 제안하는 프로토콜은 추가적인 지수승없이 3번의 메시지 교환으로 프로토콜을 안전하게 수행할 수 있다. 따라서 제안하는 프로토콜은 2장에서 기술한 안전성에 대한 요구조건을 만족하면서 최소의 통신량과 연산량을 가진다는 것을 알 수 있다.

5. 결 론

본 논문에서는 사용자와 서버가 사전에 공유한 패스워드 정보를 이용하여 안전하게 세션키를 교환할 수 있는 인증 키 교환 프로토콜을 제안하였다. 제안된 프로토콜의 안전성은 잘 알려진 두 가지 가정, DLA, CDHA를 기반으로 하며, 인증 키 교환 프로토콜 설계시 요구되는 여러 암호학적 안전성에 대한 요구조건을 만족한다. 특히, 제안된 프로토콜은 기존의 인증 프로토콜들과는 달리 서버에 저장된 사용자 패스워드 파일이 어떤 경로를 통해 공격자에게 유출되었을 때 공격자의 사용자 또는 서버 위장공격에 안전하다는 장점이 있다. 또한, 기존에 연구된 주요 프로토콜들과 효율성을 비교한 결과 제안된 프로토콜의 수행은 3번의 메시지 교환과 5번의 모듈러 지수승이 요구됨으로 제안된 프로토콜이 보다 효율적임을 알 수 있었다.

참 고 문 헌

[1] S. Blake-Wilson, A. Menezes, Authenticated Diffie-Hellman key agreement protocols, Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98), LNCS Vol. 1556, pp.339-361, 1999.

[2] S. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocols secure aganist dictionary attacks, In IEEE Symposium on Research in Security and Privacy, pp.72-84, 1992.

[3] D. Jablon, Strong Password-Only Authenticated Key Exchange,Computer Communication Review, ACM SIGCOMM, vol. 26, no. 5, pp.5-26, 1996.

[4] D. Jablon, Extended password key exchange protocols immune to dictionary attack, WETICE Workshop, pp.248-255, 1997.

[5] T. Wu, Secure remote password protocol, Internet Society Symposium on Network and Distributed System Security, 1998.

[6] T. Kwon, Ultimate solution to authentication via memorable password, Contri- bution to the IEEE P1363 study group for Future PKC Standards, available from http://grouper.ieee.org/groups/1363/passwdPK/contributions.html 2000.

[7] P. MacKenzie, More Efficient Password-Authenticated Key Exchange, CT-RSA, LNCS Vol. 2020, pp.361-377, 2001.

[8] D. Johnson and S. Blake-Wilson and A. Menezes, Key agreement protocols and their security analysis, Proceedings of the Sixth IMA International Conference on Cryptography and Coding, LNCS Vol. 1355 pp. 30-45, 1997.

[9] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, An efficient protocol for authenticated key agreement, Designs, Codes and Cryptography, pp. 119-134, 2003.

[10] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transaction on Information Theory, IT-22, pp.644-654, 1976.

[11] M. Bellare and P. Rogaway, Entity Authentication and Key Distribution, In Proc. of Crypto '93, LNCS Vol. 773, pp. 232-249, 1993.

[12] V. Boyko, P. MacKenzie and S. Patel, Provably secure password authenticated key exchange using Diffie-Hellman, In Proc. of EuroCrypt 2000, pp.156-171, 2000.

[13] D. Denning and G. Sacco, Timestamps in key distribution systems, Communications of the ACM, 1981.

[14] L. Gong, M. Lomas, R. Needham, and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, IEEE Journal on Selected Areas in Communications, pp 648-656, 1993.

류 은 경

1995년 2월 경일대학교 컴퓨터공학과 학사. 1999년 8월 계명대학교 정보통신공학과 석사. 2001년 3월~현재 경북대학교 컴퓨터공학과 박사과정. 관심분야는 암호이론, 암호 응용기술

윤 은 준

1995년 2월 경일대학교 섬유패션학과 학사. 2003년 2월 경일대학교 컴퓨터공학과 석사. 2003년 3월~현재 경북대학교 컴퓨터공학과 박사과정. 관심분야는 암호 프로토콜, 네트워크 보안

유 기 영

1976년 경북대학교 이과대학 수학교육과(이학사). 1978년 한국 과학 기술원 컴퓨터공학과(공학석사). 1993년 New York Rensselaer Polytechnic Institute 컴퓨터과학과(이학박사). 1978년~현재 경북대학교 공과대학 컴퓨터공학과 교수. 관심분야는 암호연산, 병렬처리, 암호화 프로토콜, 정보보호