MTI 기반의 새로운 PAK 프로토콜 제안

김락현, 염흥열

순천향대학교 정보보호학과

New Password-Authenticated Key Exchange Protocol based on MTI

Rack-Hyun Kim, Heung-Houl Youm

Department of Information Security SoonChunHyang Univ.

요 약

본 논문에서는 PAK(Password-Authenticated Key Exchange)와 PAK-R 프로토콜 기반으로 세가지 형태의 MTI(Matsumoto, Takashima, Imai) 키 일치 프로토콜을 적용하여, 안전한 보안성 요구 조건을 만족하면서 다양한 시스템에 적용할 수 있는, 패스워드-인증 키 분배 프로토콜을 소개하고자 한다. PAK 패스워드-인증 키 프로토콜은 통신 주체의 짧은 길이의 패스워드를 이용하여 통신 주체의 식별 및 상호 인증 후, 크기가 긴 세션키를 분배하기 위한 프로토콜이다. 또한 PAK는 이미 안전한 보안성이 증명되었고,[8,9,10] 이를 이용한 많은 패스워드 기반의 인증 키 분배 프로토콜이 소개되었다. 본 논문은 이미 안정성 검증이 된 키 분배 프로토콜을 이용하여 새로운 PAK 프로토콜을 제안하며, credential의 이용성을 보장하기 위한 다양한 응용에 적용될 수 있다.

I. 서론

통신 및 네트워크 기술의 발전으로 인터넷, 전자 상거래, 원격 사용자간의 통신, 응용서버와 클라이언트의 통신 등 많은 서비스가 확대되고 있다. 특히 인터넷 통신을 이용한 원격 사용자간의 통신과 응용서버와 클라이언트의 통신에서 사용자간에 안전한 통신 서비스를 제공하기 위하여 여러가지 방법으로 보안 서비스를 제공하고 있는데, 통신 정보의 암호화를 통한 보안 서비스는 대표적인 방법이다. 이때 정보의 암호화 서비스를 위해서는 통신 주체간에 통신에 사용될 키가 공유되어야 하고, 통신 주체는 상호 인증을 통해 통신을 하고 있는 주체가 정당한 주체인지를 확인하여야 한다. 이에 정보의 암호화 서비스에서 키 분배와 상호 인증은 반드시 필요한 기능이며, 이를 위해서는 보다 효율적이고 다양한 시스템에 적용할 수 있는 프로토콜 개발이 필요하다.

PAK 프로토콜은 통신 주체간에 사전에 공유한 패스워드를 기반으로 상호 인증과 안전한 통신을 위해 세션키를 분배하는 프로토콜이다.[1,2] 이때 두 통신 주체가 공유한 짧은 길이의 패스워드는 식별 및 상호 인증과 통신에 필요한 큰 길이의 세션키를 만드는데 중요한 요소가 된다. 그리고 PAK는 두 사용자간의 통신, 응용 서버와 클라이언트 역할에 따라 변형된 프로토콜이 제안되고 있다. 이에 기본 구조의 PAK와 MTI 키 일치 프로토콜을 결합하여 다양한 환경에서의 세션키 분배를 제공하고자 한다.[3]

본 논문에서는 PAK 프로토콜의 사전 전제와 환경에서 PAK와 PAK-R 프로토콜에 MTI((1),변형(1),(2)) 프로토콜을 적용하여 일반적인 원격 사용자간의 통신과 응용 서버와 클라이언트의 통신에 적용 가능하게 하였고, PAK와 MTI(1) 결합 프로토콜에 EC(Elliptic Curve)를 적용함으로써 모바일 클라이언트에 적용할 수 있는 프로토콜을 제안하였다. 이에 PAK 프로토콜에서의 연산 부하량을 유지하면서, 다양한 환경에 적용 가능한 프로토콜 설계가 본 논문의 목적이다.

II. 개요

이 장에서는 본 논문에서 사용되는 PAK 프로토콜과 MTI 프로토콜에서 사용되는 보안 요구 사항과 용어와 파라미터를 정의한다.

1. PAK 프로토콜 용어 정리

1) 보안 요구 사항

패스워드 기반의 키 교환 프로토콜을 이용하여 사용자간 세션키를 분배하는 과정에서 필요로 하는 보안 요구 사항은 다음과 같다.[7]

- 도청 공격(eavesdropping) :

공격자가 통신 주체 사이에서 통신 내용을 도청하여 통신 주체의 개인 정보, 통신 내용 그리고 세션키의 정보를 알아내는 공격이다.

- 재전송 공격(replay attack) :

공격자는 이전에 사용했던 통신 주체의 정보를 재사용하여 정당한 사용자처럼 통신에 접근하는 공격이다.

- 중간자 공격(man-in-the-middle attack) :

통신 주체의 중간에 위치하여 두 사용자 사이에 전송되는 정보를 도청, 변조, 위조하여 두 사용자의 정보 및 세션키를 알아내는 공격이다.

- 사전공격(Dictionary attack) :

두 사용자 사이에서 전송된 정보의 내용을 사전공격(Dictionary Attack)으로 알아내는 공격이다.

- PFS(Perfect Forward Secrecy)의 만족 :

공격자가 두 사용자 사이에서 패스워드나 패스워드 검증자를 알아냈다 할 지라도, 이전에 사용되었던 세션키에 대한 정보는 알아낼 수 없는 성질이다.

2) 용어 정리

PAK protocol에서 사용되는 용어와 기호들을 다음에 설명하고 있다. 또한 이 기호들은 본 논문에서 사용되는 PAK와 PAK-R 프로토콜에 모두 적용된다.

- A : 사용자 A (또는 클라이언트)
- B : 사용자 B (또는 서버)
- π : 사용자 A, B의 공유 패스워드
- $p = rq + 1, \gcd(r, q) = 1$
  - p는 1024 비트의 소수
  - q는 160 비트의 소수
  - g는 Z_p^*의 서브그룹의 생성자, q의 원시근
- H_1, H_{2a}, H_{2b}, H_3 : 해쉬 기능의 함수
  - H_1: 1024 + 160=1184 비트의 출력
  - H_{2a}, H_{2b}, H_3 : 160 비트의 출력
- K : 공유된 세션키

3) PAK 프로토콜

A
lice(A) Step 1 : $x \in_R Z_q$ 을 선택

$m \equiv g^x \cdot H_1(A, B, \pi)^r$ 계산

m : 전송

Bob(B) Step 2 : $m \stackrel{?}{=} 0 \mod p$ 검사

$y \in_R Z_q$ 을 선택하여 $\mu = g^y$ 계산,

$\sigma = (\frac{m}{H_1(A, B, \pi)^r})^y = g^{xy}$ 계산,

$k = H_{2a}(A, B, m, \mu, \sigma, \pi)$ 을 계산

μ, k : 전송

Alice(A) Step 3 : $\sigma = \mu^x$ 계산

$k \stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(A, B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 4 : $k' \stackrel{?}{=} H_{2b}(A, B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = H_3(A, B, m, \mu, \sigma, \pi)$: 세션키

이로써 PAK 프로토콜은 두 사용자의 공유 패스워드 π 와 σ , k 그리고 k' 로써 사용자 식별과 상호 인증을 하고 마지막으로 안전한 보안 통신을 위한 세션키 K 를 생성한다. [1,2]

세션키 : $K = H_3(A, B, m, \mu, \sigma, \pi)$

4) PAK-R 프로토콜

Alice(A) Step 1 : $x \in_R Z_q$, $h \in_R Z_q^*$ 을 선택

$m \equiv g^x \cdot h^q \cdot H_1(A, B, \pi)$ 계산

m : 전송

Bob(B) Step 2 :

$y \in_R Z_q$ 을 선택하여 $\mu = g^y$ 계산,

$\sigma = ((\frac{m}{H_1(A, B, \pi)})^r)^{yr^{-1}} = g^{xy}$ 계산,

$k = H_{2a}(A, B, m, \mu, \sigma, \pi)$ 을 계산

μ, k : 전송

Alice(A) Step 3 : $\sigma = \mu^x$ 계산

$k \stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(A, B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 4 : $k' \stackrel{?}{=} H_{2b}(A, B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = H_3(A, B, m, \mu, \sigma, \pi)$: 세션키

PAK-R 프로토콜은 기본 PAK 프로토콜에서 사용자 A 를 클라이언트로 사용자 B 를 서버로 가정하고, 클라이언트 측면에서 계산 부하량을 감소시키는데 목적이 있다. 이로써 클라이언트에서 사용할 수 있는 장치(매우 작은, 느린 디바이스, 오래된 PC, 스마트카드, 휴대용 PDA 등)에 유용하다.[1,2]

세션키 : $K = H_3(A, B, m, \mu, \sigma, \pi)$

2. MTI 프로토콜 용어 정리

1) 용어 정리

MTI 프로토콜에서 사용되는 용어와 기호들을 다음에 설명하고 있다. 또한 이 기호들은 본 논문에서 사용되는 MTI(1)과 MTI(2)프로토콜에서 사용된다.

- A : 사용자 A (또는 클라이언트)
- B : 사용자 B (또는 서버)
- $p = rq + 1, \gcd(r, q) = 1$
  - p는 1024 비트의 소수
  - q는 160 비트의 소수
- 개인키 파라미터
  - X_A, X_B : 사용자 A, B 의 고정 개인키
  - r_A, r_B : 사용자 A, B 의 임시 개인키
- 공개키 파라미터
  - y_A, y_B : 사용자 A, B 의 고정 공개키
  - T_A, T_B : 사용자 A, B 의 임시 공개키

2) MTI(1) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

$r_A \in_R Z_q$ 선택,

$T_A \equiv g^{r_A} \bmod p$ 계산

T_A : 전송

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

$r_B \in_R Z_q$ 선택,

$T_B \equiv g^{r_B} \bmod p$ 계산

T_B : 전송

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_A X_B + r_B X_A} \bmod p$

MTI(1) 프로토콜은 개인키와 공개키 정보 $r_A X_B + r_B X_A$ 를 이용하여 세션키 K 를 생성한다.[3]

세션키 : $K = g^{r_A X_B + r_B X_A} \bmod p$

3) MTI(2) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

$r_A \in_R Z_q$ 선택,

$T_A \equiv y_B^{r_A X_A} \bmod p$ 계산

T_A : 전송

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

$r_B \in_R Z_q$ 선택,

$T_B \equiv y_A^{r_B X_B} \bmod p$ 계산

T_B : 전송

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_B X_A r_A X_B} \bmod p$

MTI(2) 프로토콜은 개인키와 공개키 정보 $r_B \cdot X_A \cdot r_A \cdot X_B$ 를 이용하여 세션키 K 를 생성한다.[3]

세션키 : $K = g^{r_B X_A r_A X_B} \bmod p$

III. 제안 프로토콜

이 장에서는 2장에서 설명한 PAK와 PAK-R 프로토콜에 MTI(1)과 MTI(2) 프로토콜을 적용하여 다양한 시스템에 적용 가능한 프로토콜을 제안하고자 한다. 그리고 MTI(1) 프로토콜은 기본과 변형 프로토콜로 나누어 PAK의 σ 의 계산량 차

이에 관점을 두고 두 가지 프로토콜을 설계하였다.

1. PAK+MTI(1) 프로토콜

1) PAK+MTI(1) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

Alice(A) Step 2 : $r_A \in_R Z_q$ 선택,

$m \equiv g^{r_A} \cdot H_1(A,B,\pi)^r$ 계산

m : 전송

Bob(B) Step 3 : $m \stackrel{?}{=} 0 \bmod p$ 검사

$\mu = g^{r_B}$ 계산

$\sigma = (\frac{m_A}{H_1(A,B,\pi)^r})^{r_B} = g^{r_A r_B}$ 계산

$k = H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = (\mu)^{r_A} = g^{r_A r_B}$ 계산

$k \stackrel{?}{=} H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 :

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_B X_A + X_B r_A} \bmod p$

2) PAK+변형 MTI(1) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

Alice(A) Step 2 : $r_A \in_R Z_p$ 선택,

$m \equiv g^{r_A} \cdot H_1(A,B,\pi)^r$ 계산

m : 전송

Bob(B) Step 3 : $m_A \stackrel{?}{=} 0 \bmod p$ 검사

$\mu = g^{r_B}$ 계산

$\sigma = (\frac{m}{H_1(A,B,\pi)^r})^{X_B} \cdot y_A^{r_B}$

$= g^{r_A X_B} \cdot g^{r_B X_A}$ 계산

$k = H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = (\mu)^{X_A} \cdot y_B^{r_A}$

$= g^{r_B X_A} \cdot g^{r_A X_B}$ 계산

$k \stackrel{?}{=} H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 :

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_A X_B + X_A r_B} \bmod p$

2. PAK+MTI(2) 프로토콜

1) PAK+MTI(2) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

Alice(A) Step 2 : $r_A \in_R Z_q$ 선택,

$m \equiv y_B^{r_A X_A} \cdot H_1(A,B,\pi)^r$ 계산

m : 전송

Bob(B) Step 3 : $m \stackrel{?}{=} 0 \bmod p$ 검사

$\mu = y_B^{r_B}$ 계산

$\sigma = (\frac{m}{H_1(A,B,\pi)^r})^{r_B} = g^{X_A X_B r_A r_B}$ 계산

$k = H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = (\mu)^{r_A X_A} = g^{X_A X_B r_A r_B}$ 계산

$k \stackrel{?}{=} H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 :

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{X_A r_B X_B r_A} \bmod p$

PAK+MTI(1) 프로토콜은 PAK 프로토콜 기반

에 MTI의 공개키 일치 프로토콜을 적용한 것으로 PAK 프로토콜의 σ ($\sigma = g^{r_A r_B}$)값을 유지하면서 결과로 분배된 세션키는 MTI 프로토콜 세션키 파라미터 형태의 키를 분배하게 된다. 그러나 PAK+MTI(1) 변형 프로토콜은 PAK 프로토콜 기반에 MTI(1)의 공개키 일치 프로토콜을 적용한 것으로 PAK 프로토콜의 σ ($\sigma = g^{r_A r_B}$)값과는 상이한 σ ($\sigma = g^{r_B X_A} \cdot g^{r_A X_B}$)을 이용하여 상호 인증을 하게 된다. 이때 σ 의 형태는 세션키와 동일한 형태를 갖게 된다. [6]

3. PAK-R+MTI(1) 프로토콜

1) PAK-R+MTI(1) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

Alice(A) Step 2 : $r_A \in_R Z_q$, $h \in_R Z_q^*$ 선택,

$m \equiv g^{r_A} \cdot h^q \cdot H_1(A, B, \pi)$ 계산

m : 전송

Bob(B) Step 3 : $m \stackrel{?}{=} 0 \bmod p$ 검사

$\mu = g^{r_B}$ 계산

$\sigma = (((\frac{m_A}{H_1(A,B,\pi)})^{r_B})^{r^{-1}} = g^{r_A r_B}$ 계산

$k = H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = (\mu^{r_A}) = g^{r_A r_B}$ 계산

$k \stackrel{?}{=} H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 :

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_B X_A + X_B r_A} \bmod p$

2) PAK-R+변형 MTI(1) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

Alice(A) Step 2 : $r_A \in_R Z_q$, $h \in_R Z_q^*$ 선택,

$m \equiv g^{r_A} \cdot h^q \cdot H_1(A, B, \pi)$ 계산

m : 전송

Bob(B) Step 3 : $m \stackrel{?}{=} 0 \bmod p$ 검사

$\mu = g^{r_B}$ 계산

$\sigma = (((\frac{m}{H_1(A,B,\pi)})^{r})^{X_B})^{r^{-1}} \cdot y_A^{r_B} = g^{r_A X_B} \cdot g^{r_B X_A}$ 계산

$k = H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = (\mu)^{X_A} \cdot y_B^{r_A} = g^{r_B X_A} \cdot g^{r_A X_B}$ 계산

$k \stackrel{?}{=} H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 : 계산

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_B X_A + X_B r_A} \bmod p$

4. PAK-R+MTI(2) 프로토콜

1) PAK-R+MTI(2) 프로토콜

Alice(A) Step 1 : $y_A \equiv g^{X_A} \bmod p$ 계산 [공개]

Bob(B) Step 1 : $y_B \equiv g^{X_B} \bmod p$ 계산 [공개]

Alice(A) Step 2 : $r_A \in_R Z_q$, $h \in_R Z_q^*$ 선택,

$m \equiv y_B^{r_A X_A} \cdot h^q \cdot H_1(A, B, \pi)$ 계산

m : 전송

Bob(B) Step 3 : $m \stackrel{?}{=} 0 \bmod p$ 검사

$\mu = y_B^{r_B}$ 계산

$\sigma = (((\frac{m_A}{H_1(A,B,\pi)})^{r_B})^{r^{-1}} = g^{r_A X_A r_B X_B}$ 계산

$k = H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = (\mu)^{r_A X_A} = g^{X_A X_B r_A r_B}$ 계산

$k \stackrel{?}{=} H_{2a}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 :

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = g^{r_A X_A r_B X_B} \bmod p$

PAK-R+MTI(1), PAK-R+MTI(1) 변형, PAK-R+MTI(2) 프로토콜은 서버와 클라이언트의 통신 모델에 적용 가능한 프로토콜로서 PAK에서의 클라이언트의 멱승 계산량을 감소시킨 PAK-R 프로토콜의 특성을 유지하기 때문에 클라이언트에 적용 가능한 프로토콜이다.

5. PAK-R+MTI(2)+EC 프로토콜

이 절에서는 이전에 제안한 PAK+MTI(2) 프로토콜에 EC(Elliptic Curve) 기법을 적용하였다. 이 프로토콜은 클라이언트와 서버의 계산 복잡도를 현저히 감소 시킬수 있는 하나의 방법이다.[2,5]

1) PAK-R+MTI(2)+EC 프로토콜

Alice(A) Step 1 :

$y_A \equiv X_A G \bmod p$ 계산 [공개]

Bob(B) Step 1 :

$y_B \equiv X_B G \bmod p$ 계산 [공개]

Alice(A) Step 2 :

$R_A \in_R Z_q$ 선택

$m \equiv G(X_B + R_A + X_A) + r(f(A, B, \pi))$ 계산

m : 전송

Bob(B) Step 3 :

$R_B \in_R Z_q$ 선택

$\sigma = (m - r(f(A, B, \pi)) + G \cdot R_B$
$= G(X_A + R_B + X_B + R_A)$ 계산

$\mu = G(X_B + R_B)$ 계산

$k = H_{2a}(A, B, m, \mu, \sigma, \pi)$ 계산

μ, k : 전송

Alice(A) Step 4 :

$\sigma = \mu + G(X_A + R_A)$
$= G(X_A + R_B + X_B + R_A)$ 계산

$k \stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi)$ 검사

$k' = H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 계산

k' : 전송

Bob(B) Step 5 :

$k' \stackrel{?}{=} H_{2b}(y_A, y_B, m, \mu, \sigma, \pi)$ 검사

Alice(A) 와 Bob(B) 세션키 계산

$K = H_3(y_A, y_B, m, \mu, \sigma, \pi)$

IV. 프로토콜 분석

1. 안전성 분석

1) 도청 공격

• 메시지는 임의의 난수를 근거로 생성하고, 인증을 위한 σ 와 해쉬값은 사용자가 각각 계산에 의해 산출한다.

2) 재전송 공격

• 단계별로 전송되는 메시지가 연속적으로 전송되지 않고, 인증을 위해 기본적으로 3개의 서로 다른 해쉬 함수가 사용된다.

3) 중간자 공격

• Diffie-Hellman 문제의 어려움에 근거하여 설계하였다.[4]

4) 사전 공격

• 3개의 해쉬 함수로 인증을 위한 해쉬값을 생성하고 해쉬 함수내의 비밀정보는 이산대수 문제로 보호하여 공격 불가능하도록 설계 하였다.

5) PFS(perfect forward secrecy)의 만족

• 세션키의 생성은 두 사용자의 비밀 정보와 난수를 이용하여 세션마다 갱신되므로 사용자의 패스워드가 공개되더라도 이전 세션의 세션키 값을 알수 없다

2. 효율성 검사

본 논문에서 제안된 프로토콜들은 PAK 프로토콜의 기본 연산 부하량과 동일한 부하량을 유지한다. 기본적인 곱셈 연산과 덧셈연산에서 부하량 증가가 발생하지만, 시스템의 지연을 발생하는 멱승 연산의 동일수에 의하여 기존의 PAK 프로토콜 적용 시스템에 교체 적용 가능하다.

V. 결론

본 논문에서는 PAK 프로토콜과 PAK-R 프로토콜을 기반으로 MTI 키 분배 프로토콜을 적용하여 다양한 시스템에서 적용 가능한 세션키 분배 프로토콜을 제안하였다. 제안한 프로토콜은 두 사용자간 패스워드를 기반으로 세션키를 분배할 수 있는 PAK 프로토콜과 MTI 프로토콜의 보안 특성을 유지하면서 공개키 정보와 개인키 정보를 이용하여 키를 분배하는 프로토콜을 설계하였다. 그리고 응용서버와 클라이언트 환경에서 사용가능하도록, 클라이언트 측면의 계산량 감소를 고려하여 설계된 PAK-R 프로토콜에 MTI 프로토콜과 EC를 적용하여 모바일 통신에 적용 가능한 프로토콜을 제안하였다.

참고문헌

[1] V. Boyko and S. Patel, "Provably Secure Password Authentication and key Exchange Using Hiffie-Hellman" *EuroCrypt 2000*, pp. 156-171, 2000.

[2] P. MacKenziie, "More Efficient Password-Authenticated Key Exchange", RSA Conference, Cryptographer's Track, pp. 361-377, 2001.

[3] T. Matsmoto, Y. Takashima and H. Imai, "On seeking smart public-key distribution systems", *The Transaction of the IECE of Japan*, E69, pp. 99-106, 1986.

[4] S.Blake-Wilson, and A. Menezes, "Authenticated Diffie-Hellman key agreement protocol", *Selected Areas in Cryptography-SAC '98 Proceeding*, pp. 339-361, 1999.

[5] IEEE. IEEE 1363, *"standard Specifications for Public Key Cryptography"*, 2000.

[6] M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols". *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pp. 419-428. 1998.

[7] Seung-Hyun Seo, Tae-Nam Cho and Sang-Ho Lee, "OTP-EKE: A New Key Exchange Protocol based on One-Time Password," *Proceeding of the 3rd Joint Forum of Ewha Womans University, Japan Women's University and Ochanomizu University, Tokyo, Japan*, Nov. 2001.

[8] S. M. Bellovin and M. Merritt. "Encrypted key exchange: Password-based protocols secure against dictionary attacks." *In Proceedings of IEEE Security and Privacy*, pp. 72-84, 1992.

[9] D. Jablon. "Strong password-only authenticated key exchange." *ACM Computer Communication Review. ACM SIGCOMM*, 26(5):5-20, 1996

[10] D. Jablon. "Extended password key exchange protocols immune to dictionary attack." *In WETICE'97 Workshop on Enterprise Security*, 1997.