익명성을 보장하는 그룹키 합의 프로토콜

임재열, 김우헌, 류은경, 윤은준, 유기영
경북대학교 컴퓨터공학과 정보보호연구실
{tenheat, whkim, ekryu, ejyoon}@infosec.knu.ac.kr yook@knu.ac.kr

A conference key agreement protocol with user anonymity

Jae-yuel Im, Woo-hun Kim, Eun-kyung Ryu, Eun-jun Yoon, Kee-young Yoo
Department of Computer Engineering, Kyungpook National University, Daegu, Korea

요 약

최근에 Tseng은 사용자의 익명성을 제공할 수 있는 두 종류의 그룹키 전송 프로토콜을 제안하였다. 본 논문에서는 Tseng이 제안한 프로토콜 중 서명을 이용한 그룹키 전송 프로토콜의 문제점을 지적하고 그 해결책을 제시한다. 또한 라그랑지 보간법을 사용하여 사용자의 익명성을 제공하는 새로운 그룹키 합의 프로토콜을 제안한다. 제안된 프로토콜은 사용자의 추가적인 연산 없이 안전한 그룹키를 생성할 수 있으므로, 사용자의 익명성 및 키 합의 프로토콜이 요구되는 애플리케이션에 적합하다.

1. 서 론

서로 통신하고자 하는 두 사용자는 보안상 취약한 채널을 통해서 안전한 통신을 하기 위해 세션키를 공유할 필요가 있다. 1976년 Diffie와 Hellman [1] 은 두 사용자가 세션키를 설정하기 위한 안전한 키 설정 시스템을 제안하였다. 하지만 Diffie와 Hellman의 시스템은 세 명 이상의 사용자들이 기밀성을 요하는 통신을 하고자 하는 경우에는 비효율적이었다. 다수간에 효율적이고 안전한 통신을 위해서는 공통의 그룹키를 설정할 필요가 있었다. 이런 이유로 그룹키 교환을 위한 몇몇 프로토콜들이 제안되었다.

현재까지 제안된 대부분의 그룹키 설정 프로토콜들은 참가자들에 대한 프라이버시을 제공하지 못하였다. 예를 들어 비밀투표의 경우, 외부의 영향력을 배제하기 위해 참가자의 신원를 알 수 없도록 익명성을 제공할 필요가 있다. Wu [2] 는 대수적인 접근을 통해서 익명성을 제공하는 그룹키 전송 프로토콜을 제안하였고, Tseng [3] 은 Wu가 제안한 프로토콜을 개선하여, 다항식을 이용한 보다 효율적인 그룹키 전송 프로토콜을 제안하였다. Tseng은 해쉬함수를 이용한 방식과 서명을 이용한 방식의 두 가지 프로토콜을 제안하였다.

본 논문은 *Tseng*의 서명을 이용한 그룹키 전송 프로토콜의 문제점을 지적하고, 그 해결책을 제시한다. 또한 라그랑지 보간법을 이용한 사용자의 익명성을 제공하는 새로운 그룹키 합의 프로토콜을 제안한다.

2. Tseng의 프로토콜

Tseng은 사용자의 익명성을 보장하기 위해서 해쉬함수를 이용한 그룹키 전송 프로토콜(프로토콜 A)과 서명을 이용한 그룹키 전송 프로토콜(프로토콜 B)를 제안하였다. 각각의 프로토콜은 다음과 같다.

2.1 프로토콜 A

프로토콜은 3단계(시스템 설정, 키 전송, 그리고 키 복구 단계)로 구성된다. 각각의 단계를 설명하면 다음과 같다.

■ 시스템 설정 단계

m은 사용자의 수, ID_i는 사용자 U_i의 아이디이고, $H()$는 일방향 해수 함수이다. 시스템은 $q|(p-1)$를 만족하는 충분히 큰 소수 $p>2^{512}$, $q>2^{|H()|+|m|}$ 및 위수가 q인 $GF(p)$의 생성자 g를 선택한다. 그리고 $x_i \in Z_q^*$는 각 사용자 U_i의 비밀값이고 $y_i = g^{x_i} \bmod p$를 공개값으로 한다.

■ 키 전송 단계

그룹키를 생성, 검증하는 의장을 U_c, 참가자들의 집합을 $A=\{U_i | i=1,...,n,\ n<m\}$이라고 두자. U_c는 세션키 전송을 위해 다음 과정을 수행한다.

단계1, 모든 참가자 $U_i \in A(1 \le i \le n)$와 공유하는 비밀키 $k_{ci} = y_i^{x_c} \bmod p$ 를 구한다.

단계2, 타임스탬프 T를 이용해서 다음을 구한다.
$h_i = H(k_{ci} || ID_c || ID_i || T) || m,\ 1 \le i \le n$

단계3, 그룹키 $CK \in Z_q^*$를 랜덤하게 선택하고, n개의 포인트 (h_i, CK)를 사용하여 n차 다항식을 만든다.

$$P(x)=\sum_{i=1}^{n}(x-h_i)+CK \bmod q$$

$$=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0 \bmod q$$

여기서, $c_{n-1},c_{n-2},...,c_1,c_0 \in Z_q$ 이다.

단계4, $V=H(CK||ID_c||T)$를 계산한다.

단계5, U_c는 $M=\{ID_c,V,T,c_{n-1},c_{n-2},...,c_1,c_0\}$를 브로드캐스트 한다.

■ 키 복구 단계

각 사용자 U_i는 메시지 M을 받은 후, 다음의 과정을 통해 그룹키 CK를 계산한다.

단계1, 먼저 타임스탬프 T의 유효성을 검사한다.

단계2, U_c와 공유하는 비밀값 $k_{ic}=y_c^{x_i} \bmod p$를 구한다.

단계3, $h_i=H(k_{ic}||ID_c||ID_i||T)||m$를 구하고 전달받은 함수 $P(x)$에 대입하여 다음과 같이 그룹키 CK를 구한다.

$$P(h_i)=(h_i)^n+c_{n-1}(h_i)^{n-1}+\cdots+c_1h_i+c_0 \bmod q$$

$$=CK \bmod q$$

단계4, U_i는 위에서 계산된 CK값을 이용하여 구한 해쉬값과 U_c로부터 받은 V값을 비교하여 회의 참가 여부를 알아낸다.

$H(CK||ID_c||T)$ =? V

2.2 프로토콜 B

U_c는 $V=H(CK||ID_c||T)$의 해쉬 값을 대신하여 서명 a, b를 생성하여 참가자들에게 전달한다.

■ 키 전송 단계

단계1, 임의의 정수 $r \in Z_q^*$ 을 선택하고 다음과 같이 a와 b값을 구한다.

$a=g^r \bmod p$,

$b=r+H(T||a)x_c \bmod q$

단계2, $U_i \in A$에 대해 다음을 계산한다.

$k_{ci}=y_i^r \bmod p$, $1 \le i \le n$

단계3, 그룹키 $CK \in Z_q^*$을 생성한다.

단계4, n개의 포인트 (k_{ci},CK)를 이용하여 n차 다항식을 만든다.

$$P(X)=\sum_{i=1}^{n}(x-k_{ci})+CK \bmod q$$

$$=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0 \bmod q$$

단계5, U_c는 $M=\{a,b,T,c_{n-1},c_{n-2},...,c_1,c_0\}$를 브로드캐스트 한다.

■ 키 복구 단계

단계1, 타임스탬프 T의 유효성을 검증한다.

단계2, $H(T||a)$를 계산하여 전달받은 a, b에 대한 서명을 검증한다. $g^b=a \cdot y_c^{H(T||a)} (\bmod p)$

단계3, U_i는 U_c와 공유하는 비밀 값을 구한다.

$k_{ic}=a^{x_i} \bmod p$

단계4, 단계3에서 구한 k_{ic}값을 전달받은 함수 $P(x)$에 대입하여 그룹키 CK를 구한다.

$$P(k_{ic})=(k_{ic})^n+c_{n-1}(k_{ic})^{n-1}+\cdots+c_1k_{ic}+c_0 \bmod q$$

$$=CK \bmod q$$

2.3 Tseng이 제안한 프로토콜의 문제점 및 개선책

프로토콜 A에서 U_c는 단독으로 그룹키 CK를 결정하므로, 사용자 U_i들은 그룹키 CK에 기여하는 부분 없이 오직 U_c에만 의존하게 되는 단점이 있다.

또한, 프로토콜 B의 단계1에서 U_c는 서명 a, b를 생성하고 이를 사용자들에게 전달하고 U_i는 키 복구 단계2에서 받은 a, b값을 검증하여 U_c를 인증한다. 하지만 기존의 $V=H(CK||ID_c||T)$ 값에서처럼 계산된 그룹키인 CK의 값이 유효한 값인지 확인할 수 없는 문제점이 있다. 즉, U_i는 자신이 계산한 CK값으로 회의에 참석 여부 및 계산된 키의 유효성 여부를 알 수 없게 된다. U_i가 계산한 CK값이 유효한 값인가를 검증하여 자신이 회의에 참석하는가 여부를 판단하기 위해서는 검증식에 그룹키 CK값이 추가되어야 한다.

이를 해결하기 위해서 프로토콜 B의 키 전송 단계1을 다음과 같이 수정할 수 있다.

$a=g^r \bmod p$

$b=r+H(T||a)x_cCK \bmod q$

키 복구 단계2를

$g^b=a \cdot y_c^{H(T||a)CK} (\bmod p)$ 로 바꾸고,

단계2를 단계4의 그룹키 CK를 계산 뒤의 단계로 바꾼다. 이와 같은 방식으로 CK의 검증으로 회의 참가 여부를 알 수 있으며 U_c를 인증할 수 있게 된다.

3. 제안한 프로토콜

제안하는 프로토콜은 3단계(시스템 설정, 키 전송, 그리고 키 복구 단계)로 구성된다. 각각의 단계를 설명하면 다음과 같다.

■ 시스템 설정 단계

m은 사용자의 수, ID_i는 사용자 U_i의 아이디이고, $H()$는 일방향 해수 함수이다. 시스템은 $q|(p-1)$를 만족하는 충분히 큰 소수 $p>2^{512}$, $q>2^{|H()|+|m|}$ 및 위수가 q인 $GF(p)$

의 생성자 g를 선택한다. 그리고 $x_i \in Z_q^*$는 각 사용자 U_i의 비밀값이고 $y_i = g^{x_i} \bmod p$를 공개값으로 한다.

■ **키 전송 단계**

키 전송 단계에서, U_c는 키 전송을 위해 다음과 같은 과정을 수행한다.

단계1, 모든 참가자 $U_i \in A(1 \le i \le n)$와 공유하는 비밀키 $k_{ci} = y_i^{x_c} \bmod p$ 를 구한다.

단계2, 타임스탬프 T를 이용해서 다음을 구한다.
$h_i = H(k_{ci} || ID_c || ID_i || T) || m,\ 1 \le i \le n$

단계3, U_c는 h_i의 해쉬 값인 $H(h_i)$를 계산한다. 그리고 라그랑지 보간법을 이용, 다음과 같은 n개의 포인트 $(h_i, H(h_i))$, $1 \le i \le n$를 지나는 n-1차 함수를 구한다.

$$f(x) = \sum_{k=1}^{n} H(h_k) L_k(x),\quad L_k(x) = \frac{\prod_{j=1, j \neq k}^{n} (x - h_j)}{\prod_{j=1, j \neq k}^{n} (h_k - h_j)}$$

$$f(x) = c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \bmod q$$

여기서, $c_{n-1}, c_{n-2}, \ldots, c_1, c_0 \in Z_q$ 이고

그룹키 CK는 상수항 c_0가 된다.

단계4, $V = H(CK || ID_c || T)$를 계산한다.

단계5, U_c는 $M = \{ID_c, V, T, c_{n-1}, c_{n-2}, \ldots, c_1\}$를 브로드캐스트 한다.

■ **키 복구 단계**

키 복구 단계에서, 각각의 사용자 $U_i \in A(1 \le i \le n)$는 키 전송을 위해 다음과 같은 과정을 수행한다.

단계1, 먼저 타임스탬프 T의 유효성을 검사한다.

단계2, U_c와 공유하는 비밀값 $k_{ic} = y_c^{x_i} \bmod p$를 구한다.

단계3, $h_i = H(k_{ic} || ID_c || ID_i || T) || m$를 구하고, 그 값을 해쉬해서 함수 $f(x)$위에 한 점$(h_i, H(h_i))$을 구한다. 구한 값을 함수에 대입하여 다음과 같이 그룹키 CK를 구한다.

$$f(h_i) = c_{n-1}(h_i)^{n-1} + \cdots + c_1 h_i + CK = H(h_i) \bmod q$$

$$CK = H(h_i) - c_{n-1}(h_i)^{n-1} - \cdots - c_1 h_i \bmod q$$

단계4, U_i는 위에서 계산된 CK값을 이용하여 V값을 검증하여 회의 참가 여부를 알아낸다.
$H(CK || ID_c || T) = V$

U_c는 라그랑지 보간법을 이용하여 다항식을 구하고, 그 다항식의 상수항을 그룹키 CK로 사용한다. 이로써 U_c는 임의로 CK를 선택할 수 없게 되고 참가자들의 기여한 값으로 CK가 결정되게 된다.

4. 안전성 분석 및 효율성 비교

U_c는 각 사용자들과 공유하고 있는 비밀 값인 k_{ci}를 이용하여 $h_i = H(k_{ci} || ID_c || ID_i || T) || m$를 구한 후, 서로 다른 n개의 포인트 $(h_i, H(h_i))$를 생성한다. U_c는 생성한 n개의 포인트를 라그랑지 보간법을 이용하여 n개의 포인터를 지나는 유일한 n-1차 다항식을 구하게 되고, 그 상수항을 그룹키 CK로 사용한다. 이 때 U_c는 임의로 자신이 원하는 그룹키 CK로 조작할 수 없다. 즉, 그룹키 CK는 n명의 참가자들이 U_c와 공유하고 있는 비밀 값 k_{ci}로부터 계산되어 키 합의를 이루게된다.

제안된 프로토콜은 전송단계에서 U_c가 n개의 포인트를 이용, 라그랑지 보간법으로 다항식을 계산하여야 하므로 Tseng의 프로토콜에 비해 많은 연산을 필요로 한다. 하지만 전송되는 메시지의 형식과 그룹키 복구 과정은 Tseng의 프로토콜과 동일하므로 사용자 U_i는 같은 연산량이 요구된다. 따라서 그룹키 설정을 주도하는 U_c의 연산 능력이 각 사용자 U_i의 경우 보다 우수하고 상대적으로 U_i의 연산능력에 제한이 있는 환경에서, 각 사용자U_i들은 별도의 추가적인 연산 없이 계산 능력이 뛰어난 U_c의 추가 연산만으로도 키 합의 프로토콜 구현이 가능해진다.

5. 결론

본 논문에서는 Tseng이 제안한 사용자 익명성을 제공하는 그룹키 전송 프로토콜의 문제점을 지적하고 그 해결책을 제시하였다. 또한 라그랑지 보간법을 기반으로 사용자 익명성을 제공할 수 있는 새로운 그룹키 합의 프로토콜을 제안하였다. 제안된 프로토콜은 사용자의 추가적인 연산 없이 안전한 그룹키를 생성할 수 있으므로, 사용자의 익명성 및 키 합의 프로토콜이 요구되는 응용 도메인에 적합하다.

참고 문헌

[1] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Info. Theory 22 (6) (1976) 644-654

[2] T.C. Wu, Conference key distribution system with user anonymity based on algebraic approach, IEE Proc. Comput. Digit. Tech. 144(2) (1997)145-148

[3] Y.-M.Tseng, J.-K.Jan, Anonymous conference key distribution systems based on discrete logarithm problem, Computer Communications 22 (1999) 749-754