신뢰 도메인이 다른 사용자간의 ID기반 키합의 프로토콜

이병천*

*중부대학교 정보보호학과

ID-based Key Agreement Protocol Between Users in Different Trust Domain

Byoungcheon Lee*

*Department of Information Security, Joongbu University.

요 약

ID기반 암호를 사용하는 시스템에서 사용자는 자신의 ID를 공개키로 사용하며 키생성기관이 생성해서 보내준 비밀키를 이용하게 된다. 이런 환경에서 ID기반 키합의 프로토콜에 대해 많은 연구가 이루어져 왔으나 대부분 하나의 신뢰도메인 내부 사용자간의 키합의 프로토콜에 관한 연구였다. 이 논문에서는 신뢰도메인이 다른, 즉 소속된 키생성기관이 서로 다른, 두 사용자간의 ID기반 키합의 프로토콜을 제시한다.

I. 서론

ID기반 암호를 사용하는 시스템에서 사용자는 자신의 ID정보를 공개키로 사용하게 되며 그와 짝이 되는 비밀키는 키생성기관(KGC, Key generation center)이 생성하여 보내준 것을 사용하게 된다[3,4]. 이런 환경에서 사용자간의 ID기반 키합의 프로토콜에 대해 많은 연구가 이루어져 왔으나[1,2] 대부분 키생성 기관이 동일한 하나의 신뢰도메인 내부 사용자간의 키합의 프로토콜에 관한 것이었다.

그런데 인터넷 환경에서 하나의 키생성기관이 모든 사용자들에게 키생성 서비스를 제공하기 어려우므로 사용자들은 조직 환경에 따라 서로 다른 키생성기관에 소속되어 ID기반 암호 시스템을 사용하게 되는 것이 일반적일 것이다. 이렇게 신뢰도메인이 서로 다른 사용자간의 ID기반 공개키암호, ID기반 전자서명 등은 상대방의 키생성기관에 대한 신뢰 문제만 확인된다면 아무 문제없이 사용될 수 있을 것이다. 그렇다면 이렇게 서로 다른 신뢰 도메인에 속한 사용자들간에도 ID기반 키합의가 가능할까?

키합의 프로토콜은 SSL/TLS[5] 등에서와 같이 양자간의 비밀통신을 시작하기 전에 공격자에게 노출되지 않고 비밀키를 공유할 수 있도록 하기 때문에 매우 중요한 요소기술이다. 신뢰도메인이 서로 다른 경우 ID기반 암호 시스템에서 키합의가 가능한지의 여부는 ID기반 암호의 유용성을 확인하기 위해 반드시 필요하다.

이 논문에서는 Smart의 ID기반 키합의 프로토콜[1]을 변형하여 신뢰도메인이 서로 다른 사용자간에도 ID기반 키합의가 가능함을 보이고자 한다.

II. 관련 연구

2.1 겹선형 암호시스템

이 논문에서는 겹선형성에 기반한 암호시스

템을 사용한다. G_1은 위수 q를 갖는 덧셈군이라 하고 G_2는 같은 위수 q를 갖는 곱셈군이라 하자. P는 G_1의 생성자이며 겹선형쌍은 $e: G_1 \times G_1 \rightarrow G_2$로 표시된다고 하자. 여기에서는 다음과 같은 해쉬함수를 사용한다.

$H: \{0,1\}^* \rightarrow G_1$ (ID 정보로부터 타원곡선상의 포인트를 추출하는데 사용)

2.2 Smart의 인증된 키합의 프로토콜

사용자 A와 B가 같은 키생성기관(KGC)의 신뢰도메인에 속한 사용자라고 하자. KGC는 마스터 비밀키 $s \in Z_q^*$를 선택하고 공개키 $P_{KGC} = sP$를 계산하여 공개한다.

사용자 A와 B가 비밀키 발급을 요청하면 KGC는 다음과 같이 사용자의 ID비밀키를 생성하여 발급한다.

$KGC \rightarrow A: \ Q_A = H(A), \ d_A = sQ_A$
$KGC \rightarrow B: \ Q_B = H(B), \ d_B = sQ_B$

사용자A와 B는 인증된 키합의를 이루기 위하여 다음의 프로토콜을 수행한다. A와 B는 각각 임시비밀키 a, b를 선택하고 임시공개키 T_A, T_B를 계산하여 교환한다.

$A: \ a \in Z_q^*, \ T_A = aP$
$B: \ b \in Z_q^*, \ T_B = bP$
$A \rightarrow B: \ T_A$
$A \leftarrow B: \ T_B$

그러면 A와 B는 다음과 같이 공유된 비밀정보를 계산할 수 있다.

$k_A = e(aQ_B, P_{KGC}) \bullet e(d_A, T_B)$
$k_B = e(bQ_A, P_{KGC}) \bullet e(d_B, T_A)$

이 두가지 비밀정보는 같다는 것을 다음과 같이 보일 수 있다.

$$\begin{aligned} k_A &= e(aQ_B, P_{KGC}) \bullet e(d_A, T_B) \\ &= e(sQ_B, aP) \bullet e(sQ_A, bP) \\ &= e(aQ_B + bQ_A, P_{KGC}) \\ &= e(d_B, T_A) \bullet e(bQ_A, P_{KGC}) \\ &= k_B \end{aligned}$$

그러면 A와 B는 키유도함수 V를 이용하여 합의된 키 K를 계산할 수 있다.

$K = V(k_A) = V(k_B)$

III. 제안 키합의 방식

이제 두 사용자 A, B가 서로 다른 신뢰도메인에 있다고 가정하자. 편의상 사용자 A는 KGC_A에게 속해있고 사용자 B는 KGC_B에 속해있다고 하자. 디피헬만 기반의 키합의 프로토콜이 가능하도록 하기 위해 두 개의 신뢰도메인은 같은 시스템 파라메터 P, q, G_1, G_2, H를 사용하고 있으며 마스터비밀키만 서로 다르다고 가정하자.

3.1 아이디키 발급

먼저 KGC_A와 KGC_B는 다음과 같이 마스터키를 생성하여 가지고 있다.

$KGC_A: \ s_A \in Z_q^*, P_A = s_A P$
$KGC_B: \ s_B \in Z_q^*, P_B = s_B P$

KGC_A는 사용자 A에게, KGC_A는 사용자 B에게 다음과 같이 아이디키를 발급한다.

$KGC_A \rightarrow A: \ Q_A = H(A), d_A = s_A Q_A$
$KGC_B \rightarrow B: \ Q_B = H(B), d_B = s_B Q_B$

3.2 인증된 키합의 프로토콜

사용자A와 B는 인증된 키합의를 이루기 위하여 다음의 프로토콜을 수행한다. A와 B는 각각 임시비밀키 a, b를 선택하고 임시공개키 T_A, T_B를 계산하여 교환한다.

$A: \ a \in Z_q^*, \ T_A = aP$
$B: \ b \in Z_q^*, \ T_B = bP$
$A \rightarrow B: \ T_A$
$A \leftarrow B: \ T_B$

그러면 A와 B는 다음과 같이 공유된 비밀정보를 계산할 수 있다.

$k_A = e(aQ_B, P_B) \bullet e(d_A, T_B)$
$k_B = e(bQ_A, P_A) \bullet e(d_B, T_A)$

이 두가지 비밀정보는 같다는 것을 다음과 같이 보일 수 있다.

$$\begin{aligned} k_A &= e(aQ_B, P_B) \cdot e(d_A, T_B) \\ &= e(s_B Q_B, aP) \cdot e(s_A Q_A, bP) \\ &= e(d_B, T_A) \cdot e(bQ_A, P_A) \\ &= k_B \end{aligned}$$

그러면 A와 B는 키유도함수 V를 이용하여 합의된 키 K를 계산할 수 있다.

$$K = V(k_A) = V(k_B)$$

3.3 프로토콜의 보안성 분석

제안된 키합의 프로토콜은 알려진 키에 대한 안전성, 전방향 보안성, 키관리 측면에서 안전성을 가진다.

1) 알려진 키에 대한 안전성(known key security): 매 세션마다 새로운 키를 생성하므로 지나간 세션의 키가 공격자에게 노출되더라도 프로토콜의 안전성이 보장된다.

2) 전방향 보안성(forward secrecy): 양 당사자가 생성하여 교환한 임시키를 이용하여 세션키가 계산되므로 장기 비밀키 d_A, d_B가 공개되더라도 이전에 사용한 세션키들의 안전성이 보장된다.

3) 키관리(key control): 양 당사자가 모두 키생성에 간여하므로 어느 일방이 키를 특정한 방식으로 만들 수 없다.

IV. 결론

인터넷 환경에서 사용자들은 복잡한 조직구조 및 신뢰구조 속에서 통신을 이용하고 있으므로 키합의를 원하는 두 사용자가 서로 다른 신뢰도메인에 속해있는 것은 매우 일반적인 상황이다. 이 논문에서는 아이디기반 암호를 사용하는 두개의 신뢰도메인이 동일한 시스템 파라메터를 공유하고 KGC의 마스터키비밀키만 서로 다른 환경인 경우를 고려하였으며 Smart의 인증된 키합의 프로토콜을 변형하여 신뢰도메인이 서로 다른 사용자 사이에서도 인증된 키합의가 가능함을 보였다.

[참고문헌]

[1] N. P. Smart, An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing, Electronics Letters, 38, 630 - 632, 2002.

[2] L. Chen, Z. Cheng, and N.P. Smart, “Identity-based Key Agreement Protocols From Pairings”, Cryptology ePrint Archive: Report 2006/199.

[3] D. Boneh, and M. Franklin, “Identity-based encryption from the Weil pairing”, Advances in Cryptology - Crypto'2001, LNCS 2139, Springer-Verlag, pp. 213-229, 2001.

[4] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure Key Issuing in ID-Based Cryptography", In ACSW Frontiers 2004 - Second Australasian Information Security Workshop (AISW2004), volume 26 of Australian Computer Science Communications, pp. 66-74. Australian Computer Society, January 2004.

[5] The Transport Layer Security (TLS) Protocol, http://tools.ietf.org/html/rfc5246