멀티 세션 키 생성 프로토콜

박소영[U] 조태남 이상호
이 화 여 자 대 학 교 컴 퓨 터 학 과
{982COG08, tncho, shlee}@ewha.ac.kr

Multi-Session Key Establishment Protocol

So-Young Park[U] Tae-Nam Cho Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

두 명 또는 그 이상의 통신 참가자가 통신 채널을 개설하여 통신을 종료하기까지를 하나의 세션으로 정의하였을 때, 기존의 세션 키 생성 프로토콜은 하나의 세션에서 하나의 비밀 세션 키만을 생성한다. 방대하고 다양한 정보를 빠른 시간에 전송하는 초고속 네트워크 환경에서는 하나의 통신 세션에서 하나의 세션 키만을 사용하는 기존의 방법만으로는 안전한 데이터의 전송이 보장되지 않는다.

본 논문에서는 하나의 세션에서 별도의 키 분배 프로토콜의 수행 없이 서로 다른 다수의 세션 키를 생성하여 사용할 수 있도록 함으로써, 초고속 네트워크 상에서 보다 안전한 데이터의 전송이 이루어질 수 있도록 한다. 이를 위해 키드 해쉬 함수(keyed hash function)를 이용하여 간단하고 효율적인 멀티 세션 키 생성 프로토콜을 제시한다.

I. 서 론

비대칭키 암호 시스템을 이용한 메시지(message)의 암호화 및 복호화는 대칭키 암호 시스템을 이용한 경우보다 통신 참가자들이 보유해야 하는 키의 수가 적고 안전하지만 연산 시간이 길고 통신 오버 헤드가 매우 크다[4][5]. 따라서 모든 통신 참가자가 적은 수의 키만을 보유하되 메시지에 대한 암호화 및 복호화는 보다 효율적으로 수행할 수 있게 하는 방법이 요구되었고 이를 위하여 두 가지 암호화 시스템을 절충하여 사용하는 세션 키(session key)가 대두되었다. 세션 키는 하나의 통신 세션에서만 사용되고 그 통신 세션이 끝나면 함께 제거되는 두 통신 참가자만의 일회성 공유키(shared key)이다. 세션 키는 대칭키로서 이를 키로 하는 대칭키 암호 시스템을 이용하여 전송할 데이터를 빠르게 암호화하고 복호화한다. 이 세션 키는 통신 세션마다 매번 새롭게 생성되어야 하므로 세션 개설 시 두 통신 참가자가 동일한 키를 공유하도록 해야 하며, 세션 키를 생성하여 공유하기 위한 약속된 두 통신 참가자간의 절차를 세션 키 생성 프로토콜(session key establishment protocol)이라고 한다. 세션 키 생성 프로토콜은 세션 키의 안전한 키 분배를 위해 비대칭키 암호 시스템을 사용하며 사용자는 그들만의 고유키 쌍인 공개키와 개인키를 가진다.

기존의 세션 키 생성 프로토콜은 하나의 세션에서 하나의 세션 키를 생성하여 사용하도록 제안하고 있으나 이를 초고속 네트워크 환경에 그대로 적용하면 생성된 세션 키에 대한 정보가 유출될 확률이 높아져서 세션 키의 사용에 따른 안전성이 위협받을 확률이 높아진다. 왜냐하면 공격자는 키에 의해 암호화된 메시지에 대한 의미 있는 정보 혹은 암호화 키를 알아내기 위해서 개방된 네트워크를 통해 전송되는 메시지들을 분석하는데, 초고속 네트워크 환경이 구축됨에 따라 공격자의 입장에서는 분석할 다양한 데이터의 양이 증가하기 때문에 메시지를 암호화하는데 사용된 키에 대한 정보를 얻을 확률이 상대적으로 높아지기 때문이다[1][2].

따라서 본 논문에서는 기존의 세션 키 생성 프로토콜과는 달리 하나의 세션 안에서 다수의 세션 키를 생성하여 사용하되, 별도의 세션 키 생성 및 분배 프로토콜의 수행 과정 없이 간단하고 효율적으로 서로 다른 세션 키를 생성하여 사용할 수 있도록 하는 멀티 세션 키 생성 프로토콜을 제안한다. 제시하는 프로토콜은 안전한 멀티 세션 키의 생성을 위해 다음의 세

조건을 만족한다. (1) 위조 불가능하며, (2) 멀티 세션 키들은 상호 독립적이고, (3) 멀티 세션 키로부터 통신 참가자가 가지는 고유의 키를 유도할 수 없다.

2. 멀티 세션 키 생성 프로토콜의 설계

멀티 세션 키(multi-session key) 생성 프로토콜이란 하나의 세션에서 하나가 아닌 다수의 세션 키를 생성하는 프로토콜을 의미한다. 이 프로토콜은 두 통신 참가자가 멀티 세션 키 생성에 사용되는 초기값을 서로 공유하기 위한 키 분배 프로토콜과 공유한 초기값으로부터 멀티 세션 키를 반복적으로 생성하는 멀티 세션 키 변경 프로토콜로 구성된다.

2.1 키드 해쉬 함수

해쉬 함수란 임의의 길이의 입력값에 대해 짧은 고정된 길이의 출력값을 내는 함수를 말한다. 일반적인 암호학적 해쉬 함수는 일방향성과 충돌 회피성을 만족하며 어떠한 비밀 정보도 포함하지 않기 때문에 누구나 주어진 입력값에 대한 출력값을 얻을 수 있다. 키드 해쉬 함수란 이러한 암호학적 해쉬 함수에 암호학적 키를 부가한 것으로, 키를 모르면 주어진 입력값에 대한 출력값을 계산할 수 없는 형태의 암호학적 해쉬 함수를 의미한다[3].

2.2 멀티 세션 키 생성 프로토콜의 구성

멀티 세션 키 생성 프로토콜의 기본 아이디어는 다음과 같다.

(1) 멀티 세션 키를 생성하기 위해 통신 참가자는 128 bit이상의 랜덤 수 *key*와 150 bit이상의 랜덤 수 *IMSK*를 생성한다. *key*는 키드 해쉬 함수에서 사용될 키 값이고, *IMSK*는 초기 멀티 세션 키를 생성하기 위한 키드 해쉬 함수의 초기 입력 값이다.

(2) 기존의 키 분배 프로토콜을 통해서 두 통신 참가자는 *key*와 *IMSK*를 공유한다.

(3) 키드 해쉬 함수[3]를 이용하여 멀티 세션 키를 생성한다. *key*를 키드 해쉬 함수의 키 값으로 하고 *IMSK*를 초기 입력 값으로 해서, 키드 해쉬 함수에 의해 생성된 결과 값을 초기 멀티 세션 키로 사용한다. 멀티 세션 키의 길이는 160 bit 이다.

(4) 이후에 사용될 멀티 세션 키는 바로 이전에 사용된 멀티 세션 키를 입력 값으로 하고 *key*를 키 값으로 하는 키드 해쉬 함수의 결과 값이다.

두 통신 참가자인 Alice와 Bob이 *key*와 *IMSK*를 공유하는 방법은 사인크립션을 이용할 수 있고[8][9], 대표적인 키 분배 프로토콜인 Diffie-Hellman 방식을 이용할 수도 있다[7].

2.3 멀티 세션 키 변경 프로토콜

두 통신 참가자가 멀티 세션 키 생성을 위한 초기 값을 공유한 다음 더 이상의 키 분배 프로토콜의 수행 없이 두 통신 참가자가 각각 이후에 사용될 멀티 세션 키를 독립적으로 생성하는 구체적인 멀티 세션 키 변경 프로토콜은 다음 [표 2.1]과 같다.

[표 2.1] 멀티 세션 키 변경 프로토콜

Alice	메시지	Bob
$key \in_R \{0,1\}^{lkey}$ $IMSK \in_R \{0,1\}^{lIMSK}$	$E(key, IMSK)$ --->	
초기 멀티 세션 키 : $MSK_0 = KH_{key}(IMSK)$ 이후 멀티 세션 키 : $MSK_p = KH_{key}(MSK_{p-1})$ for $p \geq 1$		초기 멀티 세션 키 : $MSK_0 = KH_{key}(IMSK)$ 이후 멀티 세션 키 : $MSK_p = KH_{key}(MSK_{p-1})$ for $p \geq 1$

※ $lkey = |key| = 128bit$, $lIMSK = |IMSK| = 512bit$
$E()$: 암호화 함수

Alice와 Bob은 각각 키 값을 가지는 동일한 해쉬 함수를 이용하여 서로 다른 멀티 세션 키를 반복적으로 생성한다. *key*를 키로 하는 해쉬 함수를 $KH_{key}()$라고 했을 때, 가장 먼저 사용될 멀티 세션 키 MSK_0 는 $KH_{key}(IMSK)$에 의한 해쉬 결과 값이 되고, p번째 멀티 세션 키 MSK_p는 $KH_{key}(MSK_{p-1})$에 의한 해쉬 결과 값이다. 여기서 MSK_{p-1}은 바로 이전에 사용된 멀티 세션 키를 의미하며 해쉬 함수의 성질에 따라, 생성되는 멀티 세션 키는 동일한 길이를 갖는다. 하나의 세션 내에서의 서로 다른 메시지들은 멀티 세션 키 변경 프로토콜에 의해 생성되는 서로 다른 멀티 세션 키에 의해 암호화되어 전송된다.

3. 멀티 세션 키 생성 프로토콜의 분석

제안된 멀티 세션 키 생성 프로토콜을 통해 생성되는 멀티 세션 키는 한 번만 사용되고 폐기되는 일회성을 가지므로 보다 안전하게 데이터 전송이 이루어지며 멀티 세션 키 변경 과정이 매우 단순하고 효율적이다.

3.1 단순성

일방향 해쉬 함수가 존재한다는 가정 하에서 키드 해쉬 함수를 이용하여 참가자는 서로 다른 멀티 세션 키를 각각 독립적으로 생성하여 동시에 사용한다. 멀티 세션 키 변경을 위해서는 해쉬 함수를 수행하기만 하면 되므로 키 변경을 위한 오버 헤드가 매우 작다.

3.2 안전성

멀티 세션 키 생성 프로토콜은 하나의 세션 내에서 서로 다른 메시지에 대해 서로 다른 멀티 세션 키를 사용하여 암호

화시키므로 하나의 세션 키만을 사용하는 기존의 경우보다 더욱 안전하다는 것은 명백하다. 이것은 대칭키 암호 시스템에서의 데이터의 기밀성에 대한 증대된 안전성을 부여한다. 제시한 멀티 세션 키 생성 프로토콜의 안전성을 평가하기 위하여 다음과 같이 안전성을 정의한다.

[정의 1] 멀티 세션 키 생성 프로토콜에서 안전하다는 것은 공격자가 멀티 세션 키 중에서 하나를 알게 되었다 하더라도 다음에 사용될 멀티 세션 키를 생성해 낼 수 없고 이전에 사용된 멀티 세션 키를 유도할 수 없다는 것을 말한다.

따라서, 멀티 세션 키 생성 프로토콜의 안전성은 암호학적 키드 해쉬 함수가 가지는 안전성에 의존한다. 주어진 멀티 세션 키로부터 이전에 사용된 멀티 세션 키에 대한 정보 유도는 암호학적 해쉬 함수가 가지는 일방향성에 의거하여 불가능하며, 다음에 사용될 유효한 멀티 세션 키로의 유도 또한 키드 해쉬 함수가 가지는 암호학적 기밀성에 의거하여 불가능하다[3]. 따라서 키드 해쉬 함수가 일방향성을 만족하고 안전하다면 제시된 멀티 세션 키 생성 프로토콜은 안전하다.

3.3 효율성

멀티 세션 키를 생성하는 키 변경 프로토콜은 키드 해쉬 함수만으로 구성된다. 따라서, 멀티 세션 키를 바꾸기 위해서는 키드 해쉬 함수를 수행시키는 시간이 부가적으로 필요하다. 그러나 키드 해쉬 함수를 수행하는 데 필요한 시간은 키 분배 프로토콜을 수행하는 데 필요한 지수 연산과 비교해 봤을 때 무시해도 좋을 만큼 작다.

4. 결 론

본 논문에서는 하나의 세션에서 다수의 서로 다른 세션 키를 효율적으로 생성할 수 있는 멀티 세션 키 생성 프로토콜을 제시하였다. 멀티 세션 키 생성 프로토콜은 하나의 세션 내에서 다수의 서로 다른 세션 키를 별도의 키 분배 프로토콜을 수행함 없이 해쉬 함수를 이용하여 간단하고 효율적으로 생성한다. 하나의 세션 안에서 서로 다른 메시지에 대해 서로 다른 세션 키가 사용되므로 메시지의 기밀성이 완전하게 보장되고, 별도의 키 분배 프로토콜의 수행 없이 두 통신 참가자가 각각 독립적으로 키드 해쉬 함수를 이용하여 다음에 사용될 세션 키를 생성하므로 키 생성 방법이 매우 간단하며 효율적이다.

본 논문에서 제시하는 프로토콜은 두 통신 참가자간의 멀티 세션 키 생성을 위한 프로토콜이다. 그러나 많은 응용 분야에서 일대다(one-to-many) 또는 다대다(many-to-many)간 통신을 수행하므로 다자간에도 멀티 세션 키를 생성하여 사용할 수 있는 프로토콜이 필요하다. 본 논문에서 제시된 두 통신 참가자간의 멀티 세션 키 생성 프로토콜의 기본 아이디어를 다자간 통신에서도 쉽게 적용될 수 있을 것으로 예상되며 추후 이를 확장한 다자간 멀티 세션 키 생성을 위한 프로토콜의 설계가 필요하다.

참 고 문 헌

[1] R. Atkinson, "Security Architecture for the Internet Protocol," IETF Network Working Group, RFC 1825, August 1995.

[2] The ATM Forum, "ATM Security Specification, Version 1.0," ATM Forum STR-SEC-01.04, December 1998.

[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Function for Message Authencication," In Advances in Ctyptology - CRYPTO '96, Lecture Notes in Computer Science, Vol. 1109, Springer-Verlag, pp. 1-15, 1996.

[4] W. Diffie, and M. Hellman, "New Directions in Cryptography," IEEE Trans. Info. Theory, Vol. 22, No. 6, pp. 472-492, 1976.

[5] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Advances in Cryptology-CRYPTO '84, Springer-Verlag, pp. 10-18, 1985.

[6] O. Goldreich, and L. Levin, "A Hard Predicate for All One-Way Functions," In Proceedings of the 21st Annual Symposium on Theory of Computing, ACM, 1989.

[7] H. Krawczyk, "SKEME: A Versatile Secure Key Exchange Mechanism for Internet," In Proceedings of the Network and Distributed System Security, IEEE, 1996.

[8] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions," In Information Security - Proceedings of 1997 Information Security Workshop (ISW'97), Lecture Notes in Computer Science, Vol. 1396, Springer-Verlag, pp. 291-312, 1998.

[9] Y. Zheng and H. Imai, "Compact and Unforgeable Session Key Establishment over an ATM Network," In Proceedings of IEEE INFOCOM'98, pp. 411-418, 1998.