안전한 그룹 키 분산 기법에 관한 연구

정성은° 염희운
동덕여자대학교 전자계산학과
iyaho@hanmir.com

A Study on Secure Group key distribution

Sung-Eun Jung° Hee-Woon Yum
Dept. of Computer Science, Dongduk Women's University

요 약

최근 인터넷을 통한 네트워크 응용들의 확산은 unicast에서 multicast로 넓혀가고 있는 추세이다. 그러나 공개키 쌍을 사용하는 PKI 키 관리 및 인증기법에 반해 그룹 키 관리 및 인증기법에 대한 연구는 아직 미비한 상태이다. 따라서 본 논문에서는 동일한 보안등급을 갖는 다중 사용자들이 보다 안전하게 키를 공유하고 인증할 수 있도록 하는 그룹 키 분산 기법에서, 즉, 그룹 키를 관리함에 있어서 필요한 정보보호에 대한 고찰 및 그룹 키 관리에서의 주요 처리인 join/leave 함수 처리, 다양한 그룹 키 분산 기법에 관하여 연구하고 보다 안전한 키 관리 및 객체가 갖는 장점들을 포함하는 안전한 그룹 키 분산기법에 관하여 논하도록 한다.

1. 서 론

개별 사용자의 신분을 인증하거나 안전한 정보의 교환을 위한 사용자의 키 관리 등에 사용되는 공개 키 기법에 반해 특정 그룹의 가입자들, 즉, 그룹의 멤버간의 키 공유 및 그룹 인증에 필요한 것이 그룹 키 관리 기법이다. 그룹 키를 관리하기 위해서는 그룹의 멤버의 가입이나 탈퇴에 따른 join/leave 연산을 고려한 rekeying 방법, 즉, 각 연산마다 현재 사용되고 있는 그룹 키를 새로운 키로 대체하는 안전한 방법이 필요하다.

본 논문에서는 그룹 멤버의 가입이나 탈퇴 등 멤버의 변화에 따라 그룹 멤버들이 공유하고 있는 키를, 그룹의 상태 변화에 따라 멤버 간의 키 관련 정보를 안전하게 유지하면서 분산하고 관리하는 방식들 가운데 그룹 전자서명 기법, 확장된 Diffie-Hellman 키 분산 기법, 이산로그를 사용한 키 분산 기법 및 키 그래프를 사용한 키 분산 기법에 대하여 다루고자 한다.

2. 본 론

가. 그룹 키와 공개 키의 비교

그룹 키는 그룹 멤버의 키 공유 및 인증이 필수적이며, 멀티캐스트 등의 실시간 응용에 사용되어진다. 따라서 다수의 멤버에게 키를 전달하는 키 분산(key distribution), 즉 멤버의 join, leave 연산을 고려한 rekeying 방법 및 공유하는 키에 대한 인증이 필요하다. 이에 반해 공개 키는 안전한 정보 교환을 원하는 개별 사용자의 키 관리 및 개별인증 또는 키의 일대일 분배 및 키 교환에 사용되어진다.

나. 그룹 사용자를 갖는 멀티캐스트에서의 정보보호

a. 전향적 보안성과 후향적 보안성(Backward and forward secrecy) : 그룹을 떠나는 사용자는 그룹을 떠난 이 후의 메시지를 복호화 할 수 없어야 하며, 동시에 그룹에 새로 가입한 사용자는 가입하기 전의 메시지를 복호화 할 수 없어야 한다.

b. 알려진 키에 대한 보장성(known-key security): 이전의 다른 세션 키가 공격자에게 노출되었을 경우에도 프로토콜의 안전성이 보장되어질 수 있어야 한다.

c. 키 노출에 의한 위장(key-compromise impersonation) 방지 : 멤버 A 가 갖고 있는 그룹 공유 키가 공격자에게 노출되었을 경우 공격자는 A 로 위장하여 그룹의 권한을 취할 수 없어야 한다.

d. 미지의 키 공유(Unknown key-share)에 대한 안전성 : 실체 B 는 실체 C 와 키를 공유하고 있다고 믿었지만 자신도 모르는 사이에 실체 A 와 키를 공유하게 되며 실체 A 는 B 와 키를 공유하고 있다고 믿는 경우에 대한 안정성을 가져야 한다.

e. 그룹 환경 하에서의 메시지 인증(authentication of group members) : 개별 인증이 특정한 사용자가

해당 메시지를 전송하였다는 것을 인증하는 것인 반면, 그룹 인증(group authentication)은 메시지가 동일한 그룹 내에서 전송 되었음을 인증하는 것이다.

f. 데이터 기밀성 및 무결성(data confidentiality and integrity)의 만족

다. 일반적인 그룹키 관리 알고리즘

그룹키를 관리하는 일반적인 알고리즘의 유형은 크게 중앙 집중 방식, 분산 환경 방식, 복합 방식의 세가지로 구분된다. 중앙 집중 방식은 트리 구조를 바탕으로 이루어 지며 키 그래프를 이용한 알고리즘을 사용하며, 분산 환경 방식은 복수개의 키 서버들을 사용하는 방식이며 키 서버들이, 키 분산자(key distributor)들이 유일 키를 알고 있다는 보안상의 취약점을 가지나, 보안이 심각하게 요구되지 않는 응용들에서는 적합한 알고리즘이다. 아래에서는 분산환경방식의 그룹 전자서명 기법과 복합 방식의 확장된 DH 기법, 이산로그를 사용한 기법 및 중앙집중방식의 키 그래프 기법에 관하여 간략히 서술한다.

(ㄱ) 그룹 전자서명(Group Signature)[1]

그룹의 멤버는 자신의 신분을 드러내지 않고 자원을 사용할 수 있으며, 필요 시에만 사용자의 신분을 확인하도록 하였다. 제한 조건으로는 멤버만이 서명을 할 수 있으며, 검증자는 그룹의 서명임을 확인할 수는 있으나, 서명자의 신분은 알 수 없다는 것이다. 즉, 조직 내부 구조 등을 외부에 숨길 수 있으며, 분쟁 발생 시, 누구에 의한 서명인가를 확인할 수 있다는 장점을 갖는다.

이 서명은 아래 5 단계로 구성된다.

a. Setup : 그룹의 공개 키와 그룹 관리자 간의 관리 키를 생성한다.
b. Join : 새로운 그룹 멤버와 그룹 관리자 간의 프로토콜로 멤버의 비밀 키와 멤버임을 증명하는 인증서를 생성한다.
c. Sign : 메시지와 그룹 멤버의 비밀 키를 사용하여 서명을 생성한다.
d. Verify : 메시지, 서명, 그룹 공개 키를 사용하여 서명의 유효성을 검증한다.
e. Open : 서명과 그룹 관리자의 관리 키를 사용하여 서명을 생성한 멤버의 신분 및 증거(Proof)를 확인하여, 서명의 주인이 누구인가를 . 확인할 수 있는 장점을 갖는다.

TTP(Trusted Third Party)를 이용한 그룹 전자 서명 방식은 공개 키와 비밀키로 이루어진 여러 개의 키 쌍 목록을 생성하여, 그룹 멤버에게 비밀 키 목록을 나누어 주고, 공개 키의 목록은 공개한다. (여기서 공개 키의 소요자는 TTP 가 비밀리에 간직한다.) 이 목록 내의 비밀 키를 이용하여 서명을 생성하며, 공개된 공개 키를 이용하여 서명을 검증한다.

(ㄴ) 확장된 Diffie-Hellman(DH) 키 분산 기법[2][4]

2-party DH 키 분산은 그룹 멤버들 간의 멤버 수에 따른 메시지의 지수 승 계산을 통해 키를 생성하고 broadcast 하는 기법이다. 3 단계로 구성된 일반적 DH 키 분산 프로토콜을 사용하여 멤버간의 키 생성 및 분배, 멤버의 신규 가입 및 삭제 등의 변동에 따른 이상적 연산 방식이다. 또한 양자간 키 교환 알고리즘을 확장하여 효율적 그룹 키 분산기법이 되도록 하였다. 기초적 분산 알고리즘은 upflow 와 downflow 의 두 단계로 구성된다. upflow 단계는 모든 그룹 멤버들로부터 contribution 을 모은다. 멤버 Mi 는 모아진 중간 값들을 수신하고, upflow 상의 각각의 Mi 가 하는 일은 모아진 중간값의 가장 큰 값인 $\alpha^{N1...Ni-1}$ 을 사용하여 $\alpha^{N1...Ni}$ 를 계산한다. 흐름은 아래와 같다.:

$M_i \xrightarrow{\{\alpha^{\prod\{Nk\in[1,j]\}} | j\in[1,i]\},\alpha N1\neq\ldots\neq Ni} M_{i+1}$

단계 1: (Upflow) : Round i; i∈[1,n-1]

$M_i \xleftarrow{\{\alpha^{\prod\{Nk\in[i,j]\}} | i\in[1,i]\}} M_{n-i+1}$

단계 2: (Downflow) : Round (n-1+i); i∈ [1,n-1]

그림 1. 그룹키 분산의 흐름

(ㄷ) 이산 로그 기법을 사용하는 키 분산[5][6]

El Gamal 암호시스템에 사용되어지는 이산로그 문제가 RPSf(Reverse Parametic Sequence)라고 하는 함수를 생성하는데 사용되어 진다. 여기서 p를 큰 소수라고 하고, f를 노드 연산, $f(x,a) = x^a \bmod p$ 라고 한다. $y = f(u,v)$ 가 (u,v) 로 부터 v 를 연산하는 것이 계산상으로 불가능하다고 가정하며, 이에 따른 이산로그 기법을 사용하는 간단한 키 분산의 예는 아래와 같다.:

키 K를 분산하고자 하는 source는 아래의 초기 값을 자신의 자식 노드들에게 전송한다.

초기 값 $S_1 = (S_0)^{a_1} \bmod p$ 이고, $T = K \oplus S_0$ 이다.

트리의 중간 노드들은 입력 $S_{i_{k-1}}$ 상에서 함수 f를 수행하며, T에 따라 자신의 자식 노드들에게 S_{i_k} 를 전송하며, 그 식은 아래와 같다. :

$$S_{i_k} = f(S_{(i_k-1)}, a_{i_k}) = (S_{(i_k-1)})^{a_{i_k}} \bmod p$$

(ㄹ) 키 그래프를 사용한 키 분산 기법[7]

각각의 secure group은 그룹의 사용자에게 K에 있는

키를 생성하고 안전하게 분산하는 책임을 갖는 신뢰할 수 있는 그룹 서버를 갖는다. 특히, 그룹 서버는 사용자 집합 U와 키 집합 K를 알고 있으며, 사용자-키 관계 R을 유지한다. U안의 모든 사용자는 K내의 키를 갖는다. 이 키는 오로지 그룹 서버와 만 공유되어지고 그룹 서버와 동등한 기밀 통신을 위해 사용된다. K 내에 그룹키 k가 있고 이 키는 그룹서버와 U내의 모든 사용자에 의해 공유된다. 그룹키는 각각의 사용자에 의해 전체 그룹에 기밀로 메시지를 전송하는데 사용되어진다. 이 방법의 속성은 사용자나 서버가 계층 구조가 아닌 키의 트리 구조를 가진다는 것이다. . join/leave마다 다중 rekey 메세지를 사용하는 경우, 단일 전자서명으로 다중 rekey 메세지들을 서명하는 기법이다. 여기서 rekey전략 및 프로토콜은 그룹 서버에 구축되어 진다.

주어진 키 그래프 G에서, secure group (U,K,R)을 아래와 같이 명시한다.

- U와 G내의 u-노드 집합 사이에는 일대일 대응이 있다.
- K와 G내의 k-노드 집합 사이에는 일대일 대응이 있다.
- 만약 G가 u에 대응하는 u-노드로부터 k에 대응하는 k-노드로의 직접경로를 갖는다면,(u,k)는 R에 있다.

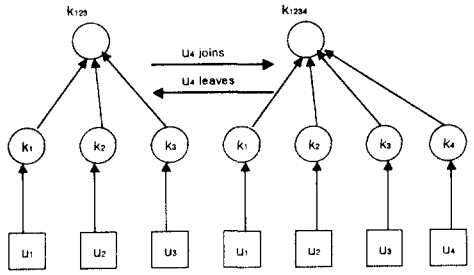

그림 2. join/leave 전 후의 키 그래프

3. 결 론

그룹키는 화상회의나 유료TV같은 기존의 멀티캐스트 등 실시간 응용 및 그룹 웨어 응용기반에서 사용된다. 따라서, 정보 보호의 기능이 실시간 개념을 해치지 않는 범위 내에서 관리되어야 한다. 그룹 단위의 업무는 단일정보를 다중 사용자에게 전달하는 것이므로 많은 수의 사용자들이 메시지를 암,복호화 하기 위해서는 항상 한 개의 비밀키를 멤버쉽을 가진 다수가 공유하여야 한다. 여기서의 키는 RSA 등의 비대칭 키 암호 알고리즘에 사용되는 키와 같이 소수연산을 처리하는 방식의 기법은 그 느린 처리 속도 때문에 그룹 키로 사용되어질 수 없다. 일반적인 그룹 키 분산 알고리즘에 대해 아래와 같은 결론을 얻는다.

그룹 서명 방식은 TTP가 그룹 소속원의 비밀 키를 알고 있어 보안상의 취약점을 가지며, 그룹의 크기가 고정되어있어 확장성에 문제를 갖는다. 또한 그룹의 공개키가 멤버의 수에 비례하여 대단히 큰 그룹의 응용에는 많은 부하를 갖는다는 단점을 갖는다.

키 그래프 방식은 rekeying은 했으나, 조건마다 효율성이 다르고 제약조건 들을 갖는다. 즉 정형화가 어려우며 rekeying 조건마다 다른 기법을 사용해야 한다는 단점을 갖는다. 키 트리를 사용하는 rekey 전략은 그룹 키 관리 서비스가 특히 그룹사이즈의 로그 값에 선형적으로 증가하는 join/leave당 평균 서버 처리 시간에 확장성이 있다는 것을 보여준다.

확장된 DH 키 분산 방식은 일반적 n-party 통신 프로토콜을 제안하였다. 그러나 이들의 프로토콜은 그룹 통신을 위한 multicast의 개념이 아닌 일대일 통신의 연속으로 구성된 n-party통신의 개념이다.

이산로그를 사용하는 방식은 대규모의 동적 멀티캐스트 그룹 내에서의 데이터 기밀성을 지원하는 것이 초점을 맞추고 있으며, 확장성에 대한 고려는 되어있지 않다. RPS라는 개념을 소개하였으며, 이를 동기적 암호 알고리즘 및 비동기적 암호 알고리즘에 적용하여 키 분산 기법을 구현하였다. 트리라는 개념을 적용한 키 분산 기법이며, 아주 규모가 큰 그룹에서의 적용은 고려하지 않고 있다.

결과적으로 안전한 그룹 통신을 위한 키의 분배에서는 키의 초기 생성 및 분배에서 보다는 멤버의 join/leave 시에 rekeying 된 키 값을 얼마나 효과적으로 안전하게 사용자 그룹의 멤버들에게 분산하는 가에 달려 있다. 따라서 그룹키의 보안 상의 제약 조건을 만족하는 적절한 알고리즘의 구현이 요구된다.

4. 참 고 문 헌

[1] D. Chaum and E. van Heyst, "Group signatures", in proc. Eurocrypt '91, pp. 257-265.

[2] M. Steiner, G. Tsudik and M. Waidner. "Diffie-Hellman Key Distribution Extended to Group Communication" in CCS/ACM '96, pp. 31-37

[3] M. K. Just, "Methods of Multi-party Cryptographic Key Establishment.", Master's thesis, OCI for CS, Caleton University, Otawa,Ontario, Aug.'94

[4] M. Steiner, G.Studik and M. Waidner, "Refinement and Extension Of Encrypted Key Exchange", OS Review /ACM Jul '95

[5] R. Molva and A. Pannetrat. "Scalable Multicast Security in Dynamic Groups" in CCS/ACM '99, pp. 101-112

[6] T. Ballardie, "Scalable Multicast Key Distribution" in RFC 1949, '9

[7] C. K. Wong, M. Gouda and S. S. Lam, "Secure Group Communications Using Key Graphs" in SIGCOMM/ACM '98, pp. 68-7