해쉬체인을 이용한 효율적인 그룹키 관리 프로토콜

이광식, 한승철
명지대학교 컴퓨터공학과
e-mail: saetian@mju.ac.kr bongbong@mju.ac.kr

An Efficient Group Key Management using Hash Chain

Kwang-Sik Lee, Seung Chul Han
Dept of Computer Engineering, Myongji University

요 약

그룹키란 그룹 내의 사용자들이 암호화와 복호화를 위하여 공유하는 비밀키를 의미하며, 그룹키는 Backward secrecy와 Forward secrecy를 모두 제공하여야 한다. Backward secrecy는 새로운 그룹 사용자가 과거의 데이터를 읽지 못하도록 하는 것이고, Forward secrecy는 탈퇴한 사용자가 이후의 데이터를 읽지 못하도록 하는 것이다. 본 연구에서는 해쉬체인을 사용하여 네트워크 환경에서 Backward secrecy와 Forward secrecy를 효율적으로 제공하는 기법을 제안한다.

1. 서론

현재 인터넷상의 여러 사용자가 그룹으로 참여하는 응용 프로그램(예를 들면, 화상회의, 화이트보드, 파일공유 등)의 수요가 폭발적으로 증가하고 있다. 이에 따라 그룹 내의 사용자들이 신뢰성과 보안성을 위해서 같은 키를 공유하고자하는 필요성이 대두되고 있다. 그룹키(Group key)란, 그룹 내의 사용자들이 암호화와 복호화를 위하여 공유하는 비밀키를 의미한다. 여기에서 비밀키는 대칭키 암호화 방식의 키를 의미한다. 통상 RSA와 같은 공개키 암호화 방식의 키는 속도상의 효율성 문제 때문에 많은 경우에 사용에 제한이 있기 때문이다[4].

그룹 내에서 공유되고 있는 비밀키는 Backward secrecy와 Forward secrecy를 만족시키기 위하여, 새로운 사용자들이 그룹에 참여하거나 기존의 사용자가 그룹을 탈퇴할 때마나 계속 새로운 그룹키로 갱신되어 재분배되어야 한다. 즉 Backward secrecy를 만족시키기 위해서 그룹에 새로 가입한 사용자들은 자신의 가입이전의 데이터들을 복호화 할 수 없어야 하고, Forward secrecy를 만족시키기 위해서는 그룹을 탈퇴하는 사용자들이 탈퇴이후의 데이터를 복호화 할 수 없어야 한다. 위 조건을 만족시키기 위해서 새로운 사용자의 가입과 기존 사용자의 탈퇴 때마다 현재의 그룹키를 새로운 그룹키로 갱신하여 분배하는 작업이 이루어져야 하지만, 그룹의 크기가 크거나 가입과 탈퇴가 매우 자주 발생하는 경우에는 심각한 과부하를 가져올 수 있다.

기존의 대표적인 그룹키 관리방법으로는 Nave방식[1], Iolus방식[2], Nortel방식[3] 등이 제안되었지만, 대부분 그룹키를 갱신하고 분배하는 과정에서 과다한 데이터 전송, 불필요한 암복호화의 반복으로 인해서 그룹키를 관리하는 비용이 크다.

따라서, 본 연구에서는 해쉬체인(Hash chain)을 사용하여 네트워크상의 여러 사용자들로 구성된 그룹의 공유되는 비밀키를 효율적이고 안전하게 생성, 갱신, 분배하는 기법을 제안한다.

2. 해쉬체인을 이용한 그룹키 관리 기법

본 연구에서 제안하는 그룹키 관리기법은 서버, 사용자, 사용자 그룹, 그룹키의 4가지 컴포넌트로 구성되며, 각 컴포넌트에 대한 설명은 다음과 같다.

- 서버: 그룹 내 그룹키 생성 및 갱신, 분배에 대한 역할을 수행한다.
- 사용자: 사용자는 서버에 가입요청을 해서 원하는 그룹에 가입할 수도 있고, 현재 속해 있는 그룹에서 탈퇴할 수도 있다.
- 그룹: 현재 그룹에 속해있는 사용자가 탈퇴할 수도 있고, 새로운 사용자가 가입할 수도 있기 때문에 그룹의 크기는 유동적이다.
- 그룹키: 하나의 그룹 내에서 공유되는 비밀키이다. 그룹이 처음 만들어 질 때, 서버에 의해서 그룹키가 생성이 되며, 이후 사용자의 가입 또는 탈퇴에 따라서 갱신이 된다.

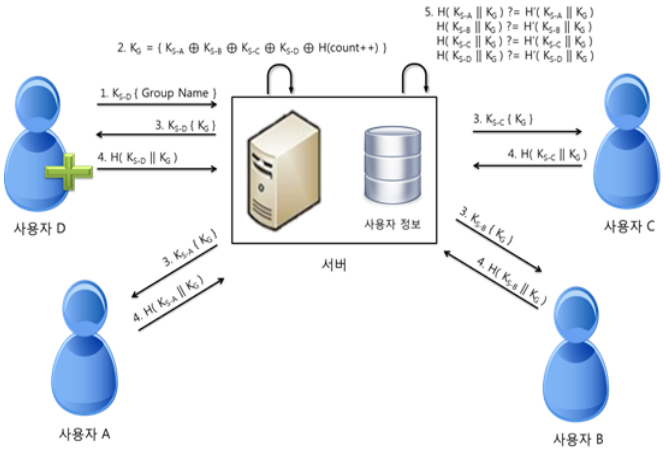
본 연구에서 제안하는 그룹키 관리기법은 Backward secrecy와 Forward secrecy 제공을 위해, 새로운 사용자가 그룹에 가입하는 경우와 기존 사용자가 그룹에서 탈퇴하는 2가지 경우로 구분된다. 설명에 사용되는 주요 기호들은 <표 1>과 같다.

<표 1> 주요기호 정리

기호	설명
S	서버
KS-A	서버와 사용자 A의 대칭키
KG	그룹키
H( )	해쉬함수
count	count 값

2.1 그룹에 새로 가입하는 경우 (Backward secrecy)

새로운 사용자가 그룹에 가입하는 경우는, 이전의 데이터들을 보호하기 위해서 그룹키를 갱신하여야 한다. (그림 1)은 기존에 사용자 A, B, C가 이미 그룹에 가입되어 있고 사용자 D가 그룹에 새로 가입하려고 하는 경우를 나타낸다. D가 서버에 가입요청을 하면, 서버는 D와 공유하고 있는 대칭키를 이용하여 새로운 그룹키를 생성한다. 그리고 서버는 생성된 그룹키를 기존에 그룹에 속해있던 사용자 A, B, C와 새로 가입한 D에게 모두 전송한다. (그림 1)의 step 1, step 3에서 전달되는 메시지는 각 사용자와 서버가 공유하고 있는 대칭키로 암호화 및 복호화 된다.



(그림 1) 사용자가 그룹에 새로 가입하는 경우

① 그룹에 새로 가입하려고 하는 사용자 D는 서버에 가입요청을 한다. 이때, D는 가입하려고 하는 그룹의 이름을 D와 서버가 공유하고 있는 대칭키를 이용해서 암호화하여 서버에 전송한다.

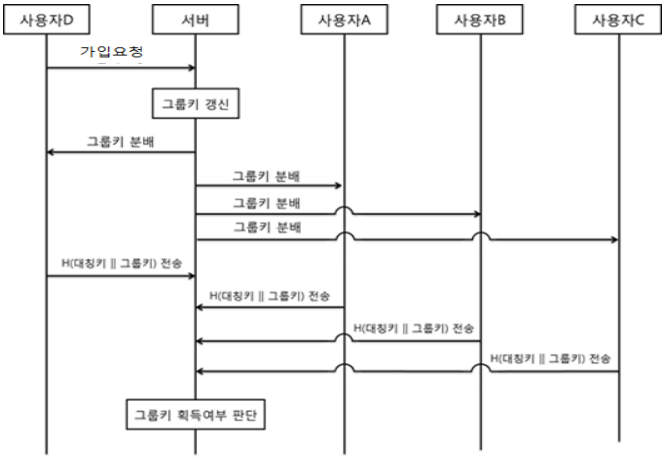
② 서버는 가입요청 메시지를 복호화하고, 그룹의 이름을 확인한다. 그리고 해당 그룹에 현재 속해있는 사용자(A, B, C)들의 대칭키와 가입을 요청하는 사용자 D의 대칭키와 현재 count값을 1 증가시킨 값의 해시값을 XOR 연산하여 그룹키를 갱신한다.

③ 서버는 갱신된 그룹키를 각 사용자들과의 대칭키로 각각 암호화하여 전송한다.

④ 각 사용자는 갱신된 그룹키를 획득하고, 자신의 대칭키와 획득한 그룹키를 OR 연산한 결과의 해시값을 서버에게 전송한다.

⑤ 서버는 갱신된 그룹키와 각 사용자의 대칭키를 OR연산을 한 해시값과 각 사용자로부터 전달받은 값이 같은지 검사를 해서 갱신여부를 확인한다. 만약, 이상이 있으면 step 3, step 4, step 5의 과정이 반복된다.

(그림 2)는 step 1부터 step 5까지의 그룹 가입 프로토콜의 제어 흐름을 나타낸다.



(그림 2) 그룹 가입 프로토콜 흐름

2.2 그룹에서 탈퇴하는 경우 (Forward secrecy)

사용자가 그룹에서 탈퇴하는 경우, 탈퇴이후의 데이터의 보호를 위해서 그룹키를 갱신하여야 한다. (그림 3)에서는 사용자 A, B, C, D가 그룹에 가입되어있고, D가 그룹에서 탈퇴하는 경우를 나타낸다. D가 서버에 탈퇴요청을 하면, 서버는 탈퇴요청을 한 사용자의 대칭키를 제외하고 그룹에 남아있는 사용자들의 대칭키만을 이용하여 새로운 그룹키를 생성한다. 서버는 새로운 그룹키를 그룹에 남아있는 사용자 A, B, C에게 전송한다.

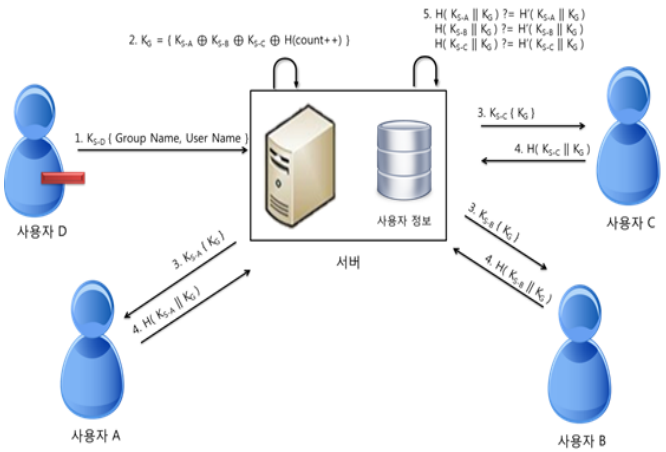
① 사용자 D가 탈퇴요청을 서버에 전송한다.

② 서버는 탈퇴요청 메시지를 복호화하고, 탈퇴를 요청한 사용자를 제외하고 현재 그룹에 남아있는 사용자들의 대칭키와 count값을 1증가시킨 값의 해시값을 XOR 연산하여 그룹키를 갱신한다.

③ 서버는 갱신된 그룹키를 현재 사용자들과의 대칭키로 각각 암호화하여 사용자들에게 전송한다.

④ 갱신된 그룹키를 전달받은 각 사용자는 갱신된 그룹키를 획득하고 자신의 대칭키와 획득한 그룹키를 OR연산한 결과의 해시값을 서버에게 전송한다.

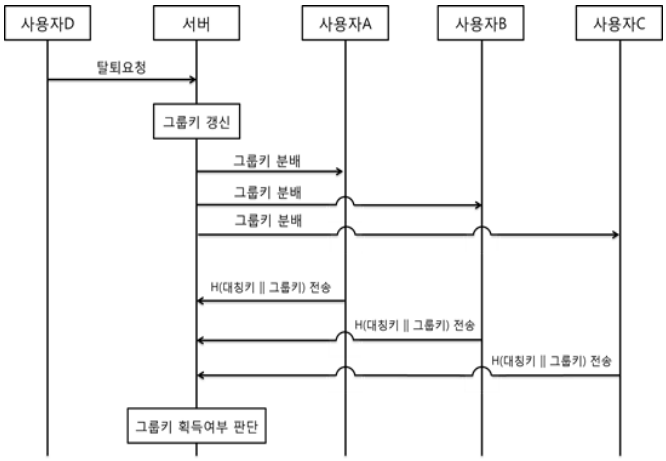
⑤ 서버는 갱신된 그룹키와 각 사용자의 대칭키를 OR



(그림 3) 사용자가 그룹에서 탈퇴하는 경우

연산을 한 해시값과 각 사용자로부터 전달받은 값이 같은지 검사를 해서 갱신 여부를 판단한다. 만약, 이상이 있으면 step 3, step 4, step 5의 과정이 반복된다.

(그림 4)는 설명한 step 1부터 step 5까지의 그룹 탈퇴 프로토콜의 제어 흐름을 나타낸다.



(그림 4) 그룹 탈퇴 프로토콜의 흐름

3. 보안성 분석

본 연구의 프로토콜에서 제공하는 보안적 요소는 크게 기밀성(confidentiality), 사용자 인증(user authentication)으로 나누어 분석할 수 있다.

- 기밀성: 기밀성은 정보를 인가된 대상에게만 공개하는 것으로 네트워크를 통해 주고받는 데이터의 내용을 비 인가된 자에게 공개하지 않는 것을 말한다. 본 방법에서 제안하는 프로토콜에서 고려해야 할 주요 요소로는 그룹키이다. 본 보안 프로토콜에서 사용자와 서버가 주고 받는 모든 메시지는 사용자와 서버가 공유하고 있는 대칭키로 암호화 및 복호화 과정을 거치게 된다. 그리고 사용자가 그룹에 가입하는 경우와 그룹에서 탈퇴하는 경우의 step 4 단계에서는 대칭키와 그룹키를 OR 연산한 결과의 해시값을 전달한다. 해시함수의 일방향성 때문에 원래 메시지를 알아내는 것은 불가능하다. 따라서 본 기법에서 제안하는 프로토콜에서 발생하는 모든 통신 메시지는 암호화된 메시지 또는 해시함수의 결과값이기 때문에 서버와 사용자 사이에서 전달되는 그룹키의 기밀성이 보장된다.
- 사용자 인증: 사용자 인증이란 누가 어떤 기록에 어떤 조치를 취할 수 있는가를 미리 정한 바에 따라, 어떤 시스템에 접근하는 사용자의 접근 자격을 확인하는 절차를 말한다. 본 기법에서 제안하는 보안 프로토콜에서는 메시지 암호화 및 복호화 과정에 대칭키 암호화 방식을 사용한다. 대칭키 암호화 방식은 메시지를 암호화 할 때 쓰는 키와 메시지를 복호화 할 때 쓰는 키가 같다. 즉, 메시지를 주고받는 사용자와 서버가 같은 키를 공유하면서 암호화 및 복호화 하는 것이다. 그리고 다른 사용자는 그 키를 공유하거나 알지 못한다. 따라서, 서버가 전달받은 메시지를 어떤 대칭키를 이용해서 복호화 할 수 있다는 것은 그 대칭키를 공유하고 있는 사용자가 보낸 메시지라는 것을 확신할 수 있다. 따라서 사용자 인증성이 보장된다.

4. 결론

그룹키 관리는 그룹을 구성하는 다수의 참여자들이 인터넷망을 통하여 안전하고 효율적으로 비밀키를 생성, 분배, 갱신하는 방법이다. 하지만 기존의 제안되었던 그룹키 관리기법들은 대부분 그룹키를 갱신하고 분배하는 과정에서 과다한 데이터 전송, 불필요한 암복호화의 반복으로 인해서 그룹키를 관리하는 비용이 큰 단점이 있었다. 본 연구에서는 해쉬체인을 사용하여 그룹의 비밀키를 효율적이고 안전하게 생성, 갱신, 분배하는 기법을 제안한다. 본 연구의 결과는 스마트 그리드, 화상회의 등에서 활용될 수 있다.

참고문헌

[1] Thomas Hardjono, Brad Cain, N.Doraswamy, "A Framework for Group Key Management for Multicast Security" IETF Feb. 2000

[2] Suvo Mittra, "Iolus: A framework for scalable secure multicasting", ACM SIGCOMM Sep.1997

[3] Thomas Hardjono, Brad Cain, Indermohan Monga, "Intra-domain group key management protocol" IETF Feb. 2000

[4] 김창오, 강경란, 조영종, "계층적 네트워크를 위한 분산 멀티캐스트 그룹 키 관리 기법" 정보과학회논문지 38(11) 2011