중앙분배방식의 그룹키 관리 기법에 관한 안전성 모델

김현정, 황정연, 이수미, 이동훈*

*고려대학교, 정보보호기술연구센터

Security Model for Centralized Group Key Management Scheme

Hyun Jeong Kim, Jung Yeon Hwang, Su Mi Lee, Dong Hoon Lee

*Center for Information Security Technologies(CIST) Korea Univ.

요 약

본 논문에서는 멀티캐스트기법에 기반한 중앙분배방식의 그룹키 관리 기법에 대한 안전성 모델을 제시하고자 한다. 지금까지 키 관리 기법과 관련한 안전성 모델 연구는 주로 두 사용자간에 안전한 키 교환이 이루어지는 환경에 집중되어 왔다. 이와 달리 본 논문에서 다루는 환경은 특정 그룹에 속한 다수의 사용자가 안전하게 키를 공유하는 것을 목적으로 하며 이때 키 생성, 키 분배 등의 그룹키 관리를 위해 신뢰기관인 그룹 관리자가 존재한다. 이러한 중앙분배방식의 그룹키 관리가 안전하게 이루어지기 위해 반드시 요구되어지는 안전성 조건을 분석하고 이를 기반으로 구체적인 안전성 모델을 제시한다.

I. 서론

지금까지 중앙집중방식의 그룹키 관리 기법들이 다양하게 제안되어 왔다[3,5,6]. 중앙집중방식의 그룹키 관리 기법에서는 신뢰할 수 있는 그룹 관리자가 존재하며 이 관리자가 그룹키 생성/분배 및 그룹 구성원 관리를 담당함으로써 그룹에 속한 구성원들간의 안전한 그룹키 공유가 이루어질 수 있도록 하는 것을 그 목적으로 한다.

중앙집중방식의 그룹키 관리를 위해 지금까지 제안된 기법들의 안전성은 구체적인 안전성 모델을 기반으로 증명된 것은 아니다. 다만 제안된 각 기법들에 적용된 암호학적 도구들의 안전성에 의존하여 전체적인 그룹키 관리 기법들이 안전할 것이라 추측되어지고 있는 것이다. 그러나 안전성이 증명되지 않은 프로토콜의 경우 이후에 그 안전성에 문제점이 발생하는 경우가 종종 있어 왔다. 따라서 안전할 것으로 추측되는 기법을 제시하는 것도 중요하지만 이러한 기법들의 안전성 증명을 위해 일반적인 안전성 모델을 설계하는 것이 더욱 중요하다.

본 논문에서는 기존의 두 사용자간의 안전한 키 교환을 위해 연구되었던 안전성 증명기법[1,2]에 기반하여 중앙집중방식의 그룹키 관리 기법에 대한 안전성 모델을 제시하고자 한다.

II. 본문

1. 요구되는 안전성

안전한 그룹키 관리 기법을 위해서 가장 중요한 사항은 그룹 구성원 이외의 다른 사람들은 그룹내부의 통신사항—메시지나 컨텐츠 등—을 알 수 없어야 한다는 것이다. 즉, 그룹키를 소유한 허가된 사용자들만이 그룹 통신에 참여할 수 있어야 한다. 또한, 그룹 구성원들이 유동적이어서 구성원 가입/탈퇴가 수시로 발생하는 특성을 지니는 그룹의 경우 추가적으로 요구되어지는 안전성은 그룹에 새로 가입한 신규 가입자는 가입 이전에 자신이 속하지 않았던 그룹의 키에 관한 정보를 알 수 없어야 하며(*전방보호*), 그룹을 탈퇴해서 그룹 구성원 자격이 박탈된 사람의 경우 탈퇴와 동시에 더 이상 그룹 통신에 필요한 정보를 알 수 없어야

한다(*후방보호*)는 것이다.

신규 가입자는 자신이 신규로 받은 그룹키를 이용하여 과거의 그룹키 정보를 얻을 수 없어야 하고, 탈퇴한 사용자는 과거의 그룹키를 이용하여 탈퇴후의 그룹키 정보를 얻을 수 없어야 하기 때문에 전방보호와 후방보호는 그룹키의 독립성[4]도 만족해야 함을 알 수 있다. 특히, 지금까지는 안전한 그룹키 관리를 위해서 전방보호와 후방보호가 동시에 요구되어져 왔다. 그러나 넓은 의미의 전방보호 개념이 후방보호 개념을 포함하고 있음을 알 수 있다. 즉, 그룹을 탈퇴한 사용자는 그 이후에 다시 그룹에 가입할 수 있으며, 이 경우 새로 가입한 이 사용자에 대해서도 전방보호가 만족되어야 한다. 이때 이 사용자에 대해 전방보호가 만족되려면 반드시 후방보호도 만족되어야 한다. 즉, 전방보호를 만족하면 동시에 후방보호도 만족되어짐을 알 수 있다.(넓은 의미의 전방보호 개념을 *전후방보호*라 칭하도록 한다.) 따라서 안전한 그룹키 관리 기법을 위한 요구 사항은 다음과 같다.

— **접근통제**: 그룹 구성원 이외에는 그룹 데이터에 접근하는 것이 쉽지 않다.

— **전후방보호**: 그룹의 신규 가입자와 그 이전의 그룹 탈퇴자가 공모하여 공모자들이 속하지 않은 특정 그룹의 그룹키를 얻는 것이 쉽지 않다.

2. 안전성 모델

그룹키 관리 기법의 참여자들은 그룹 관리자 GC와 사용자 집합 U 이다. U에 속하는 사용자들 u_i은 누구나 그룹에 가입할 수 있다. 먼저, 중앙집중방식의 그룹키 관리 기법을 위해 필요한 알고리즘들을 살펴보면 다음과 같다.

1) 알고리즘

— **키생성 알고리즘** : 안전성 매개변수 k에 대해 입력값 1^k를 이용하여 사용자들의 개인키를 생성하는 확률적인 다항식 알고리즘으로써 사용자의 개인키는 기법에 따라 대칭키 형태이거나 또는 비대칭키 형태이다.

— **셋업 알고리즘** : GC는 새로운 그룹 통신을 위한 특정 그룹을 생성하고 그룹 매개변수를 결정한다.

— **가입 알고리즘** : 새로운 사용자가 그룹에 가입하기 위한 알고리즘으로 GC는 전후방보호를 위해 새로운 그룹키를 생성하여 기존의 그룹 구성원들에게 안전하게 전송하고 신규 가입자에게는 그 사용자의 개인키를 이용하여 생성된 그룹키를 전송한다.

— **탈퇴 알고리즘** : 기존의 그룹 구성원이 탈퇴할 수 있도록 하기 위한 알고리즘으로 구성원 탈퇴시 전후방보호를 위해 GC는 새로운 그룹키를 생성하여 다른 그룹 구성원들에게 안전하게 전송한다.

위의 알고리즘을 통해 사용자 가입/탈퇴에 따라 그룹 구성원 집합이 새롭게 형성되고 그룹키도 갱신됨을 알 수 있다. 이때 사용자 가입/탈퇴에 따라 생성되는 각 그룹을 G_j 라하고 해당 그룹키를 K_j라 표시하도록 한다. 또한 GC가 사용자 u_i에게 가입 알고리즘이나 탈퇴 알고리즘을 통하여 생성된 새로운 그룹키 K_j를 전송하는 경우 형성되는 세션은 $SID(u_i, G_j)$로 표시하도록 한다.

2) 안전성 모델

중앙집중방식의 그룹키 관리 기법의 안전성 모델은 공격자의 공격 능력을 분석함으로써 정의될 수 있다. 즉, 중앙집중방식의 그룹키 관리 기법이 적용되는 환경내에서 존재 가능한 공격자의 공격이 무엇인지 분석하고 이러한 공격에 대해서 안전한지를 테스트함으로써 그 안전성이 증명될 수 있다. 다음은 중앙집중방식의 그룹키 관리 기법에서 수행되는 공격자의 공격유형을 질의형태로 정의함으로써 안전성 모델을 제시한 것이다.

— Setup (GC): 공격자는 GC로 하여금 새로운 그룹 통신을 위한 셋업 알고리즘 과정을 수행하도록 할 수 있다.

— Send (u_i, m): 공격자는 사용자 u_i로 하여금 그룹 가입/탈퇴 요청 메시지 m을 GC에게 전송하도록 할 수 있다. 이때 공격자는 메시지를 수정하거나 변조할 수 없다. 공격자가 메시지를 수정하거나 변조할 수 있는 능력이 있을지라도 그룹키 분배를 위한 메시지 전송은 GC에 의해 이루어지므로 사용자 u_i의 메시지를 위·변조하는 행위가 공격자의 공격에 도움이 되지 않는다. 따라서 중앙집중방식의 그룹키 관리 기법의 안전성 모델에서는 공격자의 메시지 변조능력을 포함시킬 필요가 없다.

— Join (J): J는 그룹 가입을 원하는 사용자들의 집합이다. 이때, 공격자는 J에 속하는 사용자들의 그룹 가입을 위해 GC로 하여금 가입 알고리즘을 실행하도록 한다.

— Leave (R): R은 그룹 탈퇴를 원하는 그룹 구성원들의 집합이다. 이때, 공격자는 R에 속하는 구성원들의 그룹 탈퇴를 위해 GC로 하여금 탈퇴 알고리즘을 실행하도록 한다.

— Reavel (u_i, G_j): 공격자는 이 질의를 수행함으로써 세션 $SID(u_i, G_j)$를 통하여 전송된 그룹키 K_j를 획득할 수 있다. 이때 공격자는 사용자 u_i의 비밀키와 해당 세션의 사용자 내부정보는 알 수는 없다.

— Corrupt (u_i, G_j): 공격자는 이 질의를 수행함으로써 세션 $SID(u_i, G_j)$를 통하여 전송된 그룹키 K_j를 획득할 수 있고 또한 사용자 u_i의 비밀키와 해당 세션의 사용자 내부정보를 모두 알 수 있다. 이 공격의 경우 사용자 비밀키는 얻을 수 있지만 내부 정보는 알 수 없는 약한 공격 유형과 사용자의 내부 정보까지 모두 얻을 수 있는 강한 공격 유형[7]이 있는데 중앙집중방식의 그룹키 관기 기법에서는 강한 공격 유형에 대해서도 안전해야 한다.

— Test (G_j): 공격자는 특정 기법에 대해 공격을 수행하는 동안 이 질의는 단 한번만 실행할 수 있으며 실행 시점에는 제한이 없다. 공격자가 그룹 G_j에 대해 이 질의를 실행하는 경우 공격자는 알지 못하는 상태에서 한 비트값 b가 임의로 선택되어 진다. 만일 $b=1$인 경우 공격자는 정당한 그룹키 K_j를 받고, $b=0$인 경우는 랜덤한 값을 받게 된다. 이 값을 받은 후 공격자는 최종적으로 한 비트값 d를 출력한다. $b \neq d$이면 공격자가 공격에 실패한 것이다. 즉, 해당 기법은 의미론적 안전성(Semantic Security)을 만족한다.

Test 질의는 일종의 게임(Game)으로 고려되어 질 수 있으며 중앙집중방식의 그룹키 관리 기법에 대한 공격자의 최종 목표는 이 게임에서 이기는 것이다. 즉, Reveal이나 Corrupt을 통하여 얻은 정보를 이용하여 Test 질의에서 받은 값이 G_j의 그룹키인지 랜덤한 값인지를 정확히 판단하는 것이다. 이때 Test 질의를 수행하기 위해서는 해당 그룹 G_j에 대해 Reavel이나 Corrupt질의가 실행되어서는 안된다.

Ⅲ. 결론

본 논문에서는 중앙집중방식의 그룹키 관리 기법을 위해 필요한 안전성 요구사항을 분석하고 구체적인 안전성 모델을 제시하였다. 제시된 안전성 모델에 기반하여 증명 가능한 안전성을 제공하는 중앙집중방식의 그룹키 관리 기법이 제시될 수 있을 것으로 기대된다.

참고문헌

[1] M. Bellare, R. Canetti and H. Krawczyk, "A Modular Approach to The Design and Analysis of Authentication and Key-Excahnge Protocols", *30th STOC*, 1998.

[2] M. Bellare, D. Pointcheval, P. Rogaway, "Authenticated Key Exchange Secure Aginst Dictionary Attack", *Proc. of Eurocrypt'00*, LNCS 1807, Springer-Berlag, pp.139-154, 2000.

[3] R. Canetti, J. Garay, G. Itkis, K. Micciancio, M. Naorr, and B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Construcions", *Proc. of INFOCOM'99*, 1999.

[4] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Group", *7th ACM Conference on Computer and Communications Security*, pp.235-244, Athens, Greece, Nov. 2000.

[5] D. Naor, M. Naor and J. Lotspech, "Revocation and Tracing Schemes for Stateless Receivers", *Proc. of CRYPTO2001*, LNCS 2139, Springer-Verlag, pp.41-62, 2002.

[6] A. Perrig, D. Song, and J. D. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Kistribution", *2001 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2001.

[7] V. Shoup. "On Formal models for Secure Key Exchange.", *Technical Report RZ 3120*, IBM Zurich Research Lab., 1999.