네트워크 계층에서의 다단계 멀티캐스트 접근통제

신동명[0]* 박희운* 최용락**
*한국정보보호진흥원, **대전대학교
{dmshin[0], hupark}@kisa.or.kr, yrchoi@dragon.dju.ac.kr

A Multi-Level Multicast Access Control Scheme on Network Layer

Dong-Myung Shin[0]*, Hee-Un Park*, Yong-Rak Choi**
*Korea Infomation Security Agency, **Daejeon University

요 약

안전한 멀티캐스트 아키텍처, 키분배, 송신자 인증 등에 대한 연구가 활발히 이루어지고 있지만 서비스 거부 공격이나 권한없는 멤버에 대한 멀티캐스트 서비스 접근을 통제할 수 있는 접근통제 기술에 대한 연구는 극히 미진한 상태이다. 멀티캐스트 그룹의 경우, 그룹의 일부 멤버는 다른 멤버보다 높은 보안 레벨의 메시지를 교환할 수 있다. 또한 대규모의 멀티캐스트 통신 환경에서 트리의 깊이가 깊어짐에 따라 루트노드에 대한 접근통제 정보가 폭증하고, 서비스 거부 공격 또는 서비스 폭증으로 인한 루트노드의 서비스 장애시 멀티캐스트 서비스의 중단을 가져올 수 있는 취약한 구조를 갖고 있다. 기존의 송신자 기반 멀티캐스트 접근통제 방식이 멀티캐스트 라우터의 서브넷에 하나의 멤버만이 가능한 한계를 갖고 있고 다중 접속 네트워크 환경에서의 불법접근을 효율적으로 막지 못하는 단점이 있다. 본 논문에서는 이 문제점을 분석하여 해결방안을 제시하고 기존 접근통제 모델을 확장하여 네트워크 계층에서의 효율적인 다단계 송신자 기반 접근통제 구조를 제시한다.

1. 서 론

멀티캐스트는 그룹에 참가한 멤버들 사이에서 한 송신자가 다수의 참여자에게 메시지를 효율적으로 전송하는 메커니즘을 제공한다. 기존 TCP/IP 프로토콜을 이용한 연결중심의 전송 방식에 비해 그룹에 참가한 송신자의 전송 오버헤드, 네트워크 대역폭 및 지연을 감소시키는 장점을 갖는다.

멀티캐스트는 음성 및 영상회의, 중복된 데이터베이스 검색 및 수정, 소프트웨어 수정본의 배포, 분산 대화형 모의실험, 원격회의 등 여러 분야에서 사용될 수 있는 중요한 통신 메커니즘이다. 현재, 국제적으로 인터넷관련 사실표준을 개발하고 있는 표준화기구인 IETF (Internet Engineering Task Force)에서는 멀티캐스트에 대한 표준화 논의가 활발히 진행되고 있다[1].

멀티캐스트 서비스는 인터넷과 같은 공개된 네트워크를 이용하므로 많은 부분에서 안전성과 관련하여 취약성에 노출되어 있으며, 이러한 취약성으로부터 안전성과 신뢰성을 확보하기 위한 방안으로 암호 시스템이 이용되고 있다. 암호시스템에서의 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄지고 있으며, 키 정보를 안전하고 효율적으로 분배하는 기법과 멀티캐스트 멤버의 가입 및 탈퇴에 따른 키갱신 기법 등이 활발히 연구되어 왔다[2,3,4,5].

그러나, 멀티캐스트 그룹관리가 기본적으로 공개전략을 채택하고 있어 송신자와 수신자 모두를 통제하는데 충분하지 않다. 따라서 어떤 송신자라도 어느 때나 모든 그룹 멤버에게 데이터를 전송할 수 있다.
IGMPv2는 멤버들이 멀티캐스트 세션을 가입하거나 탈퇴할 때 그룹멤버들을 관리하는데 사용된다. 그러나, 그룹 멤버들이 특정한 정보 출처로부터 데이터 수신을 막거나 민감한 정보의 수신으로부터 특정한 호스트들을 막는 통제 메커니즘이 없다[6].

멀티캐스트 데이터가 권한없는 호스트 또는 사용자들에 의해 접근되는 것을 막는 방법에 대해 많은 연구가 진행되어 왔으나 해법들의 대부분은 응용레벨의 암/복호화에 기초하고 있다. 그러나, 응용레벨 메커니즘은 플러딩 공격과 같은 서비스 거부 공격에 대해 라우팅 인프라를 보호할 수 없다. 멀티캐스트 데이터가 수신자들에게 전송되는 선상에 있는 멀티캐스트 라우터들에게 계속 복제될 수 있기 때문에 이러한 공격들은 멀티캐스트 서비스에 치명적인 영향을 줄 수 있다. 따라서 서비스 거부 공격을 막기 위한 메커니즘은 응용계층 보다는 네트워크 계층에서 제공되어야 한다.

CBT[2]와 같이 양방향성을 지원하면서, 중앙집중화된 그룹 멤버관리 형태는 서비스 거부 공격에 대해 특히 취약한 구조를 갖게된다. 악의적인 호스트가 서비스 거부 공격을 수행하고자 한다면 양방향 멀티캐스트 트리의 어떤 위치에서도 가짜 데이터로 폭주시키는 것이 가능하다.

이러한 취약성을 해결하기 위한 라우터 기반의 접근통제 기법이 몇몇 제안되었다[6,7]. 본 논문에서는 네트워크 계층에서의 접근통제를 수행하여 서비스 거부 공격을 최소화하고, 네트워크 트래픽의 효율성을 향상시키기 위한 기존의 연구를 살펴보고, 문제점을 보완하면서 다단계 접근통제를 지원하는 구조를 제시하고자 한다. 멀티캐스트에서의 다단계 접근통제는 비밀 원격회의나 다양한 등급을 갖는 고객에 대한 차별된 멀티미디어 서비스 제공 등에 활용될 수 있다.

2. DSAC(Dynamic Sender Access Control) 방식[6] 분석

트리상에 있는 각각의 라우터들은 가입절차에서 지역 송신자 접근통제 목록(SACL)을 다운스트림 송신자들에게만 추가한다. 그리고 접근목록에 있는 송신자들은 코어로부터 통지를 수신할 때 활성화된다. 코어만이 출처들을 수용할지 안할지를 결정하는 권한을 갖고 있다. 그리고 코어는 현재 인가된 모든 송신자들에 대한 전체 SACL을 유지한다. 인가되지 않은 호스트로부터 오는 패킷은 트리상에 전송되더라도 임의의 트리상의 라우터에 도달하자마자 즉시 취소된다. 이를 위해, 모든 송신자들은 그룹에 데이터를 송신하기 전에 코어에 먼저 등록한다. 등록 패킷이 트리상의 라우터를 통과할 때, 송신자의 유니캐스트 주소는 가는 길목에 있는 각각의 라우터의 SACL에 추가된다. 특별한 송신자에 대한 접근 정책은 코어 라우터를 따라 등록이 수신된 첫 번째 트리상의 라우터로부터의 분기점에서 시작된다. 여기에서 라우터의 다운스트림 인터페이스로써 등록 패킷이 수신되는 네트워크 인터페이스와 업스트림 인터페이스로써 유니캐스트 데이터를 코어로 절달하는데 사용하는 인터페이스를 정의한다. SACL 엔트리의 형식은 (G, S, I)이고 G는 멀티캐스트 그룹 주소를 S는 송신자를 I 는 등록패킷이 수신된 경로인 다운스트림 인터페이스를 가리킨다. 만일 코어가 가입을 승인했다면 "전송 승인" 패킷을 송신자쪽으로 거꾸로 보낸다. 그리고, 트리상의 라우터가 이 패킷을 일단 수신하면 그때부터 양방향 트리상에 데이터를 송신할 수 있게 하기 위해 라우터의 SACL에서 해당 송신자의 엔트리 정보를 활성화시킨다.

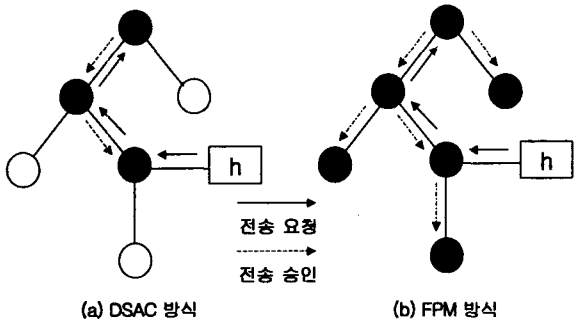

그림 1 DSAC 방식과 FPM 방식 비교

그림 1에서 노드 C가 코어 라우터이고, 노드 A에 속한 호스트 h가 코어 라우터에 가입신청을 한다. FPM(Full Policy Maintenance) 방식은 멀티캐스트 트리상의 모든 라우터에게 전체 송신자 접근 목록을 주기적으로 전달하는 방식이다. 따라서, 노드 C와 노드 A간의 연결노드 외의 노드에 대해서도 송신자 접근 목록이 배포되며 메시지 전송시에는 트리상의 모든 노드에 전송하게 된다. 그에 반해, DSAC방식은 노드 A가 노드 C에 전송 요청한 경로를 기억하였다가 동일한 경로를 따라 송신자 접근 목록을 배포한다. DSAC방식은 FPM방식에 비해 송신자 접근 목록을 저장하고 배포해야할 수를 줄일 수 있다.

DSAC방식에서 라우터가 다운스트림 네트워크 인터페이스로부터 데이터 패킷을 수신할 때, 자신의 SACL에서 데이터 송신자에 대한 엔트리 정보가 존재하는지 먼저 검사한다. 만약, 라우터가 송신자의 유니캐스트 주소를 포함하는 엔트리 정보를 찾지 못하면 그 데이터 패킷은 즉시 폐기된다. 반대로, 엔트리를 발견한 경우는 동일한 인터페이스로부터 패킷이 왔는지 검사한후, 업스트림 인터페이스로 전달한다. 서브넷으로의 메시지 전달은 코어 라우터에서부터 업스트림 인터페이스를 통해 하부 라우터 및 서브넷의 호스트까지 전달된다. 데이터 패킷이 업스트림 인터페이스로부터 온 경우, 라우터는 패킷을 모든 다른 인터페이스에 항상 전달한다.

DSAC방식에서는 멤버를 송수신 가능 멤버, 송신 전용 멤버, 수신 전용 멤버, 비멤버 송신자로 나누어 접근권한을 분류하고 있다. 아래의 제안방식에서는 이를 좀 더 세분화한 다단계 접근통제 방식을 제안한다.

3. 제안방식

DSAC방식은 라우터의 인터페이스 하나에 하나의 호스트 또는 사용자가 연결된 경우를 가정하고 있으며, 하나의 서브넷에 서로다른 접근권한을 갖는 멤버가 존재하는 경우에는 적용되지 않는다. 또한 허브와 같은 네트워크 연결장치를 이용하여 랜환경에서 다중 접속이 허용되는 일반적인 네트워크환경에서의 불법접근을 막지 못한다. 업스트림 인터페이스로부터 오는 모든 패킷은 모두 전달을 허용하기 때문에, 다중 접속 랜환경에서 신뢰된 라우터 사이에 불법접속하는 경우를 원천적으로 막지 못한다. 그러나, 일반적인 네트워크 환경에서는 하나의 네트워크 인터페이스에 하나의 서브넷이 연결되어 있는 경우가 대부분이고, 하나의 서브넷에는 다수의 멀티캐스트 멤버들이 연결될 수 있다. 제안방식에서는 멀티캐스트 그룹에 참여하고자 하는 모든 호스트는 IGMP 프로토콜을 이용하여 지정된 라우터에 가입을 요청하고. 가입요청에 따른 인증과 접근통제 권한부여는 DSAC에서와 마찬가지로 코어에서 담당한다.

DSAC방식은 서브넷 내에 다수의 멤버가 존재하는 경우에 적합하지 않다. 또한 DSAC방식에서는 동일한 서브넷에 있는 멤버들은 동일한 접근통제 규칙을 적용받는다. 따라서, 네트워크 세그먼트내에 동일한 그룹에 가입한 멤버가 여럿 있는 경우에 대한 방안이 마련되어야 한다. 이를 해결하기 위하여, 제안방식에서는 지정된 라우터간의 데이터 전송은 네트워크 레벨의 접근통제를 수행하고, 동일한 세그먼트내에서의 멤버별 접근통제는 어플리케이션 계층의 암/복호화 기법을 사용하여 수행한다. 먼저 네트워크 레벨의 다단계 접근통제를 수행하기 위하여 접근과 거부 2가지의 접근요소에서 확장하여 다단계의 비밀성 레벨을 고려한 접근통제 기법을 제안한다.

긴급을 요하는 메시지는 코어(접근통제 관리자)에 위임하여 접근통제 레벨을 상향시킬 수 있는 동적인 환경제공이 가능하다. 업스트림 인터페이스로의 전송은 모두 허용되므로, 접근통제 레벨을 상향조정하기 위해서는 코어 라우터에 유니캐스트 한 후, 코어의 권한에 의해 접근통제 레벨을 조정할 수 있다. 그림 2에서 S는 멤버의 접근 레벨을 나타내고 EmaxR과 EmaxL은 각각 우측,좌측 서브노드에 대한 접근레벨의 최대값을 나타낸다. 본

문에서는 인증절차 및 최대값 등록, 접근통제 활성화 단계, 서브넷 키교환단계는 지면상 생략하고, 멀티캐스트 라우터에 의한 네트워크 계층에서의 효율적인 다단계 접근통제에 대해서 기술한다. EmaxR과 EmaxL을 통칭하여 Emax라하면 Emax는 자신의 하위 노드 전체에 대한 최대값이고 Imax는 자신의 노드 안쪽에 대해서만 최대값을 나타낸다. Emax ≥ (하위노드 Imax 와 하위노드 Emax)가 성립한다. Emax는 하위노드의 모든 Emax와 Imax의 최대값을 가져야 한다. 또한 Imax는 자신노드의 최대값을 가져야 한다. 단, 자신의 Emax와 자신의 Imax와는 상관관계가 없다. 임의의 호스트 또는 멤버는 자신의 접근통제 레벨에 상응하는 암호화된 메시지를 생성한다. 접근통제를 위한 계층형 키구조에서 각 멤버들은 해당 접근권한에 해당하는 키목록을 라우터와 공유했다고 가정한다. 암호화된 메시지는 멀티캐스트 라우터에서 상위노드 인터페이스와 우측, 좌측 하위 인터페이스로 전달할지를 결정한다. 이때, 상위노드로의 전달은 항상 이루어지고, 하위노드에 대한 전달은 각각의 최대값과 비교하여 결정한다.

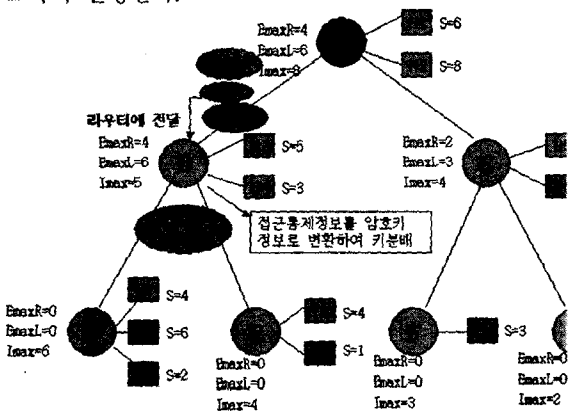

그림 2 다단계 멀티캐스트 접근통제 구조 예

본 방식에서는 멀티캐스트 트리상에서 하위 레벨로 내려가면서 사전에 하위 노드에 대한 접근통제 레벨을 파악하여 불필요한 접근통제 연산과 전체 네트워크 트래픽을 줄일 수 있다. 접근통제 레벨에 따른 연결노드의 최적화가 이루어지면, 각 노드당 메시지 전달 확률은 더욱 낮아지며, 최악의 경우에도 서브넷내에서의 접근통제에 의해 1이하의 확률을 갖는다. 일반적인 환경에서는 높은 접근권한을 갖는 멤버가 낮은 권한을 갖는 멤버보다 적기 때문에, 트리의 깊이가 커질수록 메시지 전달 확률은 낮아진다.

어플리케이션 계층(Layer)의 계층형(Hierarchical) 암복호화는 서브넷 내의 멤버의 접근권한에 따라 다른 암호키를 분배하는 방식이다. 상위 권한을 갖는 키는 하위 권한을 갖는 키를 즉시 유도해낼 수 있으나 그 역은 계산상의 어려움을 갖는다. 이러한 계층형 암호키에 대한 연구는 꾸준히 진행되어 왔으나, 멀티캐스트의 동적환경에 따른 FS(Forward Secrecy)와 BS(Backward Secrecy)를 모두 만족시키지 못하고 있다. 따라서, 본 논문에서는 계층형 키생성은 해쉬함수를 재귀적으로 이용함으로써 경량화된 계층형 암호키를 생성하고, 접근권한 레벨에 따른 다수의 암호키를 효과적으로 갱신할 수 있는 방법에 대한 연구가 필요하리라 생각된다. 현재 모듈러 연산을 이용한 효율적인 키갱신 방식을 완료하고 검토중에 있다.

4. 결론

본 논문에서는 멀티캐스트에서의 다단계 접근통제를 네트워크 계층과 어플리케이션 계층으로 나누어 제시하였다. 서브넷 내에 다수의 멤버가 존재하는 경우의 문제점과 다단계 접근통제를 어플리케이션 레벨의 계층형 암호키를 이용한 해결방안을 제시하였다. 동일한 그룹에 가입한 멤버간에는 접근권한에 맞는 암/복호화 키를 사용하여 메시지의 열람 및 기록에 대해 적절한 제한을 가할 수 있도록 하였다.

네트워크 계층에서의 다단계 접근통제는 멤버가 코어에 등록하는 과정에서 자신이 속한 서브넷의 최대 접근레벨과 하위 노드 각각에 대한 최대 접근레벨을 등록함으로써, 접근권한이 높은 메시지의 불필요한 전달을 사전에 차단하여 전체적인 네트워크 효율성을 제공한다.

다단계 접근통제 레벨은 멀티미디어 서비스 제공시 멤버별로 멀티캐스트 서비스에 대한 제공범위를 제한하는데 응용할 수 있다. 예를들어 프리미엄 사용자는 일반사용자가 수신할 수 있는 메시지를 모두 포함하여 보다 더 많은 메시지를 수신하여 볼 수 있다. 실제로 멀티캐스트 네트워크를 각각의 보안등급에 따라 서로 다른 가상 네트워크를 구성하게 된다.

현재, 멀티캐스트상에서의 접근통제에 대한 전문적인 연구는 극히 미진한 상태이며, 향후 멀티캐스트 서비스의 활성화 및 활용범위 확대와 함께 활발한 연구가 진행되리라 예상된다.

5. 참고문헌

[1] IETF magma, bgmp, idmr, msdp, pim, ssm, msec, malloc, rmt working-group, http://www.ietf.org

[2] Ballardie, "Core Based trees(CBT) Multicast Routing Architecture", IETF RFC 2201, 1997.

[3] Hardjono, Cain and Monga, "Intra-Domain Group Key Management Protocol", Internet Draft, 2001.

[4] Valdvogel, Caronni, Sun, Weiler and Plattner, "The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, 1999.

[5] Sato, Tanaka, "A push-based key distribution and rekeying protocol for secure multicasting", ICPADS 2001.

[6] Ning Wang & George Pavlou, "Towards Dynamic Sender Access Control for Bi-directional Multicast Trees", GLOBECOM 2001.

[7] Thomas Hardjono, "Router-Assistance for Receiver Access Control in PIM-SM", Proceedings. ISCC 2000.