The Journal of Korean
Institute of CALS/EC
Vol. 7, No. 1, April 2002

확장 멀티캐스트를 이용한 다중레벨 전자상거래 보안에 관한 연구

서장원*

A Study on the Multilevel Electronic Commerce Security using Scalable Multicast

Jang-Won Suh

Abstract

Through the increment of requirement for EC(Electronic Commerce) oriented communication services, security multicast communications is becoming more important. However, multicast to EC environment is much different from unicast concept most network security protocols. On the network security, using mandatory access control of multilevel architecture which assigns a specific meaning to each subject, so we accomplish access control. In this way, access control security based on the information security level is proposed.

A security protocol based on the architecture proposed in this paper would be utilized in security multicast communications, group key management service and leveled security service through multilevel EC security policy. Also we discuss and propose the security level scaleability and key management method on the network.

Key Word *: security multicast, multilevel architecture, EC security policy*

* 동서울대학 전자계산과

1. 서론

인터넷이 급속히 확산되면서 그 동안 오프라인 환경 하에서만 가능했던 많은 작업들이 사이버 상에서도 가능하게 된 반면에, 해킹이나 바이러스, 보안 시스템 위협 등의 새로운 문제점들도 증가하게 되었다. 이러한 보안 위협은 현재와 같은 다중레벨 네트워크 통신상에서 그 문제점과 이에 대한 대응책을 필요로 하게 된다. 아울러 전자상거래와 같은 가상 공간에서의 모든 거래에 있어서는 네트워크 보안에 관한 문제를 선결해야함은 재고의 여지가 없다 하겠다. 이와 같은 관점에서 본 논문은 기존의 유니캐스트(unicast) 보안 개념과는 근본적으로 다른 멀티캐스트(multicast) 보안에 관한 연구에 초점을 맞추었다.

멀티캐스트는 한 송신자가 여러 수신자들에게 데이터를 전송하는 효율성을 제공하게 되며[1], 송신자 전송 오버헤드나 네트워크 대역폭 요구사항 그리고 수신자 측면에서의 지연시간을 줄여준다. 멀티캐스트가 큰 그룹 통신에서 효율적이고 최선의 데이터 전송 서비스를 제공하는데 있어 매우 성공적이라고 볼 수 있지만, 반면에 멀티캐스트의 신뢰성, 흐름제어 그리고 혼잡 제어 등과 같은 부분에 확장성(scalability)을 갖도록 하는 데에는 많은 어려움이 있다고 알려져 있다[2]. S. Mitrra가 제안한 구조에서는 이러한 확장성의 문제를 서브 그룹으로 나눔으로써 해결하려는 시도를 보여주고 있으므로[3], 본 논문에서는 이러한 점을 근거로 하여 다중레벨 보안을 설명하였다.

그리고, S. Mitrra의 구조상에서의 네트워크 다중레벨 보안을 지원하는 확장된 멀티캐스트를 제안한다. 이것은 보안 분배 트리(secure distribution tree)에 기반을 두고, 여기에 강제적 접근(mandatory access) 방식을 추가한 확장 보안 멀티캐스트에 대한 형태이다.

2. 유니캐스트와 멀티캐스트 보안

일반적으로 네트워크 보안 프로토콜의 기본적인 역할은 불안전한 개방형 네트워크 상에서 외부의 공격자가 최초의 원문을 읽고 이것을 변경하거나 삭제할 수 없도록 해서 인증된 주체들 간에 안전하게 통신하도록 하는 것이다. 인증(authentication)이란 사용자나 호스트와 같은 실체를 인식하는 과정을 일컫는 것으로써, 이것은 전자상거래 보안 네트워크 시스템에서는 매우 중요한 부분이다.

인증 과정은 자주 키 분배와 결부되며[4], 보안 연관(security association)은 인증된 주체들간에 의해서만 공유되는 키의 집합을 정의하고, 인증, 기밀성(confidentiality), 무결성(integrity) 등과 같은 다양한 보안 목적을 위해 사용될 수 있다. 키 분배 문제에 따라 유니캐스트와 멀티캐스트로 분류하는데, 일대일(point-to-point) 유니캐스트의 보안 연관 개념은 쉽게 이해되는 반면, 다대다(multipoint-to-multipoint) 멀티캐스트 모델에서의 보안 연관 개념은 근원적으로 다소 차이가 있다.

유니캐스트의 경우를 보면, 두 주체가 통신하기를 결정하고 유니캐스트 네트워크 보안 프로토콜로 하여금 그들 사이의 보안 연관을 설정하도록 한다. 이 연관이 쌍을 이루어 안전하게 통신하도록 한다. 여기서, 보안 연관은 완전히 정적(static)이며, 두 주체가 통신을 시작할 때 생성되고 통신을 끝낼 때 소멸된다. 멀티캐스트에서도 유사하게 진행되나, 두 주체가 쌍

을 이루는 것이 아니라 임의 수의 주체들이 한 그룹을 형성한다. 그리고, 유니캐스트의 보안 연관이 정적인 반면에 멀티캐스트의 보안 연관은 그룹의 멤버쉽이 상황에 따라 변하기 때문에 반드시 동적(dynamic)이여야 한다.

또한, 멀티캐스트 보안 프로토콜은 반드시 한 주체가 매 번 동적인 시기마다 인증되어 있음을 확인해야만 한다. 실제적인 멀티캐스트 동작에서 보면, 이 시간의 구분은 멤버들이 만나고(join) 떠나는(leave) 것에 대응된다. 따라서, 보안 연관과 키는 반드시 만남과 떠남마다 변화되어야 한다. 이러한 변화로 인해 새로이 만난 주체는 이전 멀티캐스트 데이터에 접근할 수 없고, 떠난 주체는 그룹을 떠난 후에는 계속해서 멀티캐스트 데이터에 접근할 수 없게 된다. 그러므로, 매 번 만남과 떠남마다 키가 변해야하는 것이 반드시 필요하지는 않지만, 멀티캐스트 보안 프로토콜은 반드시 각 만남과 떠남이 있을 때마다 현재 그룹의 무결성을 보호하기 위해서 키를 변경할 준비를 하고 있어야만 한다.

3. 다중레벨 보안

다중레벨 보안에 있어서, 강제적 접근 제어(mandatory access control)는 주체 및 객체의 보안 레벨에 근거하여 주체와 객체에 대한 접근을 제어하는 방법이다. 이 때, 주체 및 객체의 중요도에 따라 보안 레벨을 설정하고, 주체가 객체에 접근하고자 할 때 주체 및 객체의 보안 레벨에 따라 접근 제어를 한다.

주체 및 객체는 먼저 멀티캐스트 환경에서 적합한 정의가 되어 있어야 한다. 다중레벨 보안에서의 주체는 전송되는 데이터를 매체를 통해 받는 응용이며, 객체는 이것의 접근을 받게 되는 통신상의 데이터이다.

주체 및 객체와 더불어 보안 레벨에 대한 정의도 있어야 한다. 보안 레벨은 주체 및 객체의 중요도를 나타내는 정보로써 여러 형태가 가능하다. 일반적인 보안 레벨의 형태는 계층 구조를 갖는 보안 등급(security level)과 데이터를 취급 분야별로 나누는 보안 범주(security category)로 구성된다.

그리고, 보안 레벨의 비교를 통해 접근 제어를 하게 되는데, 일반적으로 $SL(o) \leq SL(s)$ 라고 표현한다. 이것은 "주체 보안 레벨 SL(s)가 객체 보안 레벨 SL(o)를 지배한다."라고 표현하며, 접근 제어 규칙은 "주체 보안 레벨이 객체 보안 레벨을 지배할 때 접근이 가능하다."라는 것을 적용하게 된다.

또한, 보안 레벨은 강제적 접근 제어의 근거가 되는 정보로써, 인가된 관리자에 의해 설정 및 변경이 되어야 하는데, 이는 멀티캐스트에서 멤버가 만나는 서버에 접근 제어 목록(access control list)을 갖는 데이터베이스의 구축 책임이 된다. 따라서, 본 논문에서는 일반적인 보안 등급을 통한 계층적 접근 내용을 다룬다.

4. 다중레벨 보안을 지원하는 확장 멀티캐스트

보안 레벨은 암호키(encryption key)로 할당되는데, 이 때, 멤버는 자기 보다 상위 레벨의 키로는 접근할 수 없지만, 하위 레벨의 키에는 접근할 수 있다. 따라서, 하나의 멤버가 하위 레벨에 접근하기 위해서는 자기와 동일

하거나 자기 보다 하위인 레벨의 키들을 갖고 있어야 한다.

다중레벨 보안에서는 두 가지 방법을 사용하는데, 하나는 하위 레벨의 정보는 상위 레벨 그룹 멤버들이 접근할 수 있도록 하는 것이다. 이렇게 함으로써 하위 레벨 그룹 멤버들이 상위 레벨의 그룹에게 멀티캐스트 메시지를 보낼 수 있어야 한다. 그러나, 송신자는 상위 레벨의 암호키를 가질 수 없기 때문에 하위 레벨 키들이 상위 레벨 멤버들에게 사용 가능하도록 되어 있어야 한다.

또 다른 하나는 게이트웨이(gateway)를 두어서 들어오는 메시지를 하위 레벨 암호키로 복호화(decryption)한 후 상위 레벨 키로 다시 암호화(encryption)하여 메시지를 전달할 수도 있고, 또는 하위 레벨 사용자가 상위 레벨 공용키(public key)를 사용해서 전송할 수도 있다.

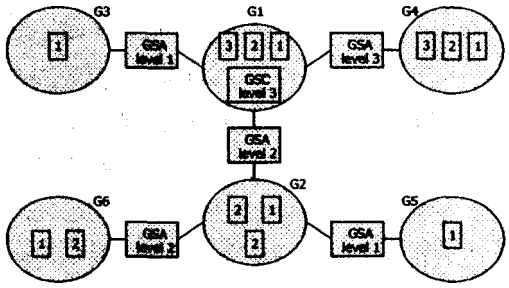
그러나, 게이트웨이를 두어서 암/복호화하는 과정은 몇 가지 단점을 지니고 있다.

- 게이트웨이로 하여금 동일한 데이터의 전송을 레벨 수만큼 반복하게 한다.
- 게이트웨이를 거칠 때마다 시간이 소비되는 암/복호화 과정을 거쳐야만 한다.
- 게이트웨이는 동일한 레벨의 사용자들 집합을 묶고 있어야 하는데, 사실상 보안레벨은 유동적이기 때문에 유연성이 부족하다.

본 논문에서는 상위 레벨의 멤버가 하위 레벨의 키에 접근 가능하도록 하는 방법에 대해서만 서술한다. 이를 위해 다중레벨 보안을 지원하는 확장 멀티캐스트 개념을 제안한다.

확장성을 확보하기 위해서는 서브 그룹(sub group)을 사용한다. 그리고, 보안 분배 트리는 하나의 가상 보안 멀티캐스트 그룹(virtual security multicast group)을 계층적으로 구성하기 위해 많은 수의 작은 멀티캐스트 서브 그룹들로 구성된다. 이때, GSC (Group Security Controller)는 상위레벨 서브 그룹을 관리하고, GSA(Group Security Agent)는 각 서브 그룹들을 관리한다.

다음에 표현한 <그림 1>은 이것의 간단한 구축 예를 나타낸 것이다.



<그림 1> 다중레벨 보안을 지원하는 확장 멀티캐스트의 구축 예

확장성은 각 서브 그룹이 상대적으로 독립이 유지될 때 얻을 수 있으며, 보안 분배 트리 안의 각 서브 그룹은 자신만의 고유 주소로 자신만의 멀티캐스트 그룹을 갖는다. 또한, 각 그룹은 자신만의 서브 그룹 키 K_{SGR}을 가지며 전역(global) K_{GRP}는 갖지 않는다. 따라서, 하나의 멤버가 만나거나 떠날 때, 단지 지역(local) 서브 그룹에만 만나거나 떠나는 것이 된다. 궁극적으로, 오직 지역 K_{SGR}만 변경될 필요성을 갖게 되므로 확장성 문제는 감소하게 된다.

GSC는 보안 분배 트리의 루트에서 상위 레벨 서브 그룹의 제어를 관리하며, 전체 그룹의 보안에 대한 책임을 맡는다. GSA는 GSC나 그들의 부모 GSA의 프록시 서버 역할을

하도록 인증된 신뢰할 수 있는 서버이고, 지역 서브 그룹의 제어를 담당한다. GSA는 보안 분배 트리에서의 레벨에 따라 그룹화 되어져 있으며, 특정 레벨에서의 GSA는 바로 위 레벨이나 GSC의 서브 그룹에 있는 GSA의 서브 그룹에 만남을 시도한다. 이 때, 하위 GSA는 상위 GSC나 GSA 보다 높은 보안 레벨을 가질 수 없다.

다음 단락에서부터는 본 논문에서 제안한 확장 멀티캐스트 구조를 단계별로 살펴보도록 하겠다.

4.1 만남(join)

멀티캐스트 보안 그룹(multicast security group)에 만남을 수행하기 위해, 송/수신자는 지정 GSA의 위치를 알아내고 JOIN 요청을 유니캐스트 보안 채널(unicast security channel)을 통해서 전송한다. 여기서, 유니캐스트 보안 채널이란 상호 인증을 제공하는 유니캐스트 보안 프로토콜 중 어떤 것이라도 무관하다.

JOIN 요구를 받은 GSA는 데이터베이스를 조사해서 이 요구를 허용할 것인지 아니면 거부할 것인지를 결정한다. 만일 요구가 허용된다면 다음과 같은 절차를 거친다.

(1) 새로운 멤버와만 공유되는 $K_{GSA\text{-}MB}$를 생성하고,
(2) 개별적인 데이터베이스 안에 새로운 멤버에 관련되는 다른 연관 정보를 이 키와 함께 저장하고 난 다음,
(3) $K_{GSA\ MB}$를 안전한 채널을 통해 새 멤버에게 전달한다.

앞에서 기술한 바와 같이, GSA는 K_{SGR}을 변경하고 K_{SGR}'을 현재의 멤버들과 만난 멤버에게 알려야 한다. 이를 위해서, GSA는 K_{SGR}로 암호화된 K_{SGR}'을 현재의 멀티캐스트 서브 그룹에게 GRP_KEY_UPDATE 안에 포함해 멀티캐스트 한다. 이 때, 각 레벨마다 다른 키를 사용하므로, level 2의 멤버가 만남을 수행했다면 다음의 <그림 2>와 같은 메시지가 멀티캐스트 되어 같거나 낮은 레벨의 키를 갱신하게 된다.

HD	$\{K_{SGR1}'\}K_{SGR1}$	$\{K_{SGR2}'\}K_{SGR2}$

<그림 2> <그림 1>의 G2에서 보안 level 2인 멤버의 JOIN으로 인한GRP_KEY_UPDATE의 예

그런 후에, K_{SGR}'을 다른 유니캐스트 보안 채널을 통해서 만난 멤버에게 전달한다. GSA는 접근 제어 목록이나 JOIN을 처리하는데 사용되는 다른 데이터베이스를 제공받는다.

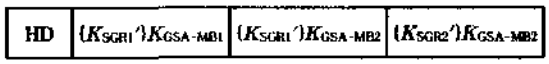
4.2 떠남(leave)

떠남은 다음과 같은 두 가지 조건하에서 발생된다.

(1) 멤버가 자율적으로 서브 그룹을 떠나려고 LEAVE 요구를 GSA에게 보내거나,
(2) GSA가 멤버를 서브 그룹에서 쫓아내려고 멤버에게 통보하는 경우.

어느 경우든 K_{SGR}은 변경되어서 떠나는 멤버의 참여를 더 이상 허용하지 않도록 해야 한다. 또한, 떠난 멤버가 갖고 있는 키들 모두를 변경해야 하므로, GSA는 떠나는 멤버의 레벨 이하의 키들을 생성해야만 한다.

K_{SGR}'의 복사본을 각 멤버에게 그 멤버의 K_{GSA-MB}로 암호화해서 보내는 방법이 있다. <그림 3>에서처럼 GSA는 하나의 메시지 안에 K_{SGR}'의 복사본을 각각 다른 멤버의 K_{GSA-MB}로 암호화한다.



<그림 3> <그림 1>의 G2에서 보안 level 2인 멤버의 LEAVE로 인한 GRP_KEY_UPDATE의 예

여기서, K_{SGR}'은 해당 멤버 레벨 이하의 키들을 포함한다. 이렇게 하면 하나의 메시지에 모든 멤버의 키를 보낼 수 있게 된다.

그룹 키 분배 방법은 Differ-Hellman 그룹 키 확장 교환[5], 중국인 나머지 정리[6], 다항식 보간법[7] 등과 같은 많은 문헌에서 기술되었다. 본 논문에서는 암/복호화를 위한 키 분배를 사용하는데, 이것은 위의 문헌들에서 기술된 여러 방법들이 $O(n)$의 계산을 요하는 방법들이므로, 성능면에서 비교해도 감소하지 않는다. 또한, 하나의 메시지를 이용함으로써 네트워크 상에서의 부하도 덜 차지하게 된다.

JOIN과 LEAVE 시에는 인증 정보를 포함하지 않는데, 이것은 실제적인 키 분배의 경우이기 때문이다. 물론, GSA와 멤버와의 인증을 포함할 수는 있지만, 그렇게 하지 않는다고 해서 치명적인 데이터의 유출이 일어나지는 않고, 단지 데이터 수신자가 수신하지 못하는 경우만 발생하게 된다. 재생 공격으로 멤버를 속인다고 한다면, 재생 공격자는 현재의 그룹 키를 알고 있어야 하므로, 재생 공격으로 인해 데이터가 하위 레벨로 누출되는 일은 없다. 또한, 멤버는 정상적인 데이터를 받을 수 없게 되어 즉각 키의 재분배를 요구하게 된다.

4.3 만남과 떠남 시의 키 분배에 관한 확장성 고찰

어느 멤버의 만남과 떠남은 그 멤버가 속한 서브 그룹에서만 키를 재분배하도록 하는 구조를 갖고 있다. 만일 서브 그룹에 없다면, 키의 재분배에 전체 멤버들이 관련되어야만 한다. 다음의 경우를 예로 살펴보자.

c_{sh} : 가장 먼 서브 그룹까지의 hop 수
c_{sn} : 전체 서브 그룹의 수
T_{KU} : 키가 갱신되는데 걸리는 시간
T_{RK} : 어느 멤버에서 GSA로 키 생성 요구 메시지의 전달 시간
T_{GK} : GSA의 키 생성 시간
T_{SK} : GSA가 서브 그룹 내에 키 분배 메시지를 전달하는 시간

• 하나의 전체 그룹인 경우

$$T_{KU} = T_{RK} + T_{GK} + c_{sh} \times T_{SK}$$

• 서브 그룹에 키의 분배가 제한되는 경우

$$T_{KU} = T_{RK} + T_{GK} + T_{SK}$$

갱신 시간에 있어서, 서브 그룹에 키의 분배가 제한되는 경우에는 $(c_{sh}-1)T_{SK}$ 만큼의 시간이 감소하게 된다. 멀티캐스트 서브 그룹들의 증가 추이를 예상하고 있다면, 전체 그룹에 키 분배를 한다는 것은 확장성 문제에 봉착하게 됨을 알 수 있다.

고려될 수 있는 또 다른 관점은 GSA의 부하 문제이다. GSA가 서브 그룹에 속하지 않은 멤버의 키 생성 요구에 의해서 키를 생성하게 되면, 전체 GSA로는 $(c_{sn}-1)T_{GK}$ 만큼의 시간이 증가하게 된다.

4.4 데이터 전이

제안한 확장 멀티캐스트 구조에서, 멀티캐스트 전송은 단지 지역 서브 그룹에만 도달하게 된다. 멀티캐스트의 계층 구조가 고려되어 전송을 받기 위해서는 전체 보안 멀티캐스트 그룹에 대한 메카니즘이 있어야만 한다.

송신자가 직접 그룹에 멀티캐스팅하지 않고, GSA에게 $K_{GSA\ MB}$로 암호화된 데이터를 유니캐스트 한다. 그러면, GSA는 데이터를 복호화하고 K_{SGR}로 다시 암호화하여 서명한 다음 그의 부모 서브 그룹뿐만 아니라 자신의 그룹에게도 이를 멀티캐스트 한다.

보다 효율적인 방법으로, 송신자가 데이터를 K_{SGR}로 직접 암호화하지 않고 전송할 때마다 임의의 키 K_{RD}를 생성해서 데이터를 암호화하고, 이 키를 K_{SGR}로 암호화하여 데이터에 포함시키는 방법이 있다.

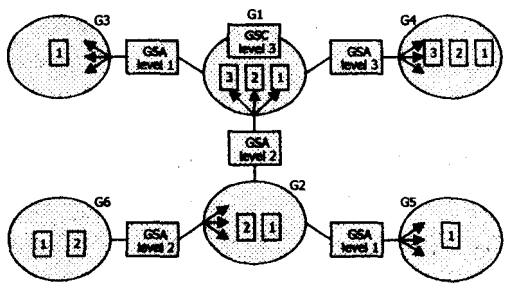
이러한 방법을 이용하면 패킷의 복호화와 재암호화는 간단하게 임의의 키 K_{RD}의 복호화와 재암호화로 감소하게 된다. 이 때, <그림 4>와 같이 수신자들은 이 메시지가 유효한 원본에서 참조되었는지를 확인하기 위해 GSA의 서명을 확인해야만 한다.

HD	{DATA, S_{GSA}}K_{RD1}, {K_{RD1}}K_{SGR1}

<그림 4> K_{RD}를 이용한 간접 암호화 패킷

서명은 RSA나 MD5를 사용하여 DATA의 내용을 가지고 서명 값을 얻을 수 있으며, DATA와 함께 암호키에 의해 기밀성을 보장받게 된다.

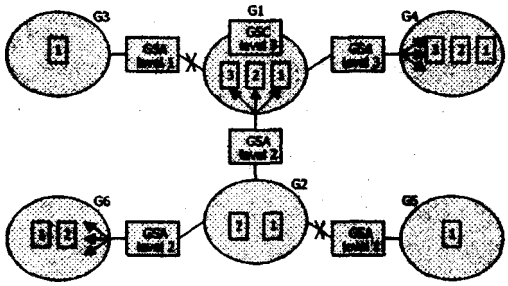
부모 GSA는 멀티캐스트 전송을 받아서, 이를 복호화하고 그 서브 그룹의 K_{SGR}로 암호화해서 다시 멀티캐스트 한다. 유사한 방법으로, 서브 그룹의 자식 GSA는 멀티캐스트 전송을 받아서 복호화하고 이들을 자식 서브 그룹의 K_{SGR}로 암호화해서 자식 서브 그룹에 다시 멀티캐스드 한다. 이러한 처리는 데이터가 다시 멀티캐스트 되는 서브 그룹에서도 반복할 것이므로, 그 데이터는 결국 모든 서브 그룹에 도착하게 된다. 이 과정은 다음의 <그림 5>에서 나타냈다.



<그림 5> G6에서 level 1인 송신자의 멀티캐스트 전송

하지만, 보안 레벨이 높은 송신자가 보낸 데이터는 그 데이터의 보안 레벨 보다 낮은 레벨을 갖는 GSA와 멤버에서는 판독을 할 수 없게 되지만, 같거나 높은 보안 레벨의 GSA와 멤버는 판독할 수 있다. <그림 6>은 이러한 과정을 나타낸 것이다.

- level 3 GSA의 처리 Traffic = level 1 Traffic + level 2 Traffic + level 3 Traffic
- level 2 GSA의 처리 Traffic = level 1 Traffic + level 2 Traffic
- level 1 GSA의 처리 Traffic = level 1 Traffic



<그림 6> G2에서 level 2인 송신자의 멀티캐스트 전송

따라서, 데이터 패킷이 자기 자신 보다 낮은 보안 레벨의 GSA는 통과하지 못하게 되므로, GSA는 패킷을 필터링하여 보안 레벨에 맞게 전체 네트워크의 부하를 줄이는 역할까지 담당하게 된다.

전체 트래픽을 산출하는 공식은 다음과 같이 적용했다.

$$\text{전체 트래픽} = \frac{1}{n}\sum_{i=1}^{n}\frac{i}{n} = \frac{1}{n^2}\sum_{i=1}^{n} i$$

$$= \frac{n+1}{2n}$$

여기서, n은 레벨의 수를 의미하며, 데이터 전송 레벨, 보안 레벨의 분포가 균등하고 동일 레벨의 네트워크 규모가 비슷하다는 가정 하에서 산출하였다.

4.5 GSA의 문제점과 대책

(1) 만남과 떠남시의 키 분배 역할

GSA는 세션 리더(session leader)와 인증 서버의 기능을 모두 갖고 있다. 멤버가 등록이 되면 세션 리더는 키를 보관하게 되고, 등록하기 전에 GSA는 세션 정책을 검사하여 세션을 열 것인가를 결정한다. 새로운 멤버가 세션에 받아들여지면, 그 멤버는 GSA로부터 그룹 키를 받게 되므로 GSA를 그룹 리더로도 볼 수 있다. 또한, 시스템의 안전도가 GSA에 의존하여 공격의 대상이 되거나 내부 범죄에 취약하여 만일의 사태시 피해가 예상될 수 있다.

GSA가 다운된다면, 다른 서버가 동작할 수 있도록 예비 프로토콜이 정의되어야만 한다. 이것을 위해 GSA 백업 서버를 구성하여 신뢰성을 높일 수 있다. 궁극적으로, GSA 백업 서버는 GSA 주 서버와 일정 간격으로 신호를 주고 받으며 다운되었는지 상태를 점검할 수 있다. 만일 GSA 주 서버가 다운된다면, 백업 서버는 자신이 주 서버의 IP 주소를 인계 받고 ARP(Address Resolution Protocol) 테이블의 내용을 갱신해서 주 서버의 역할을 이어나갈 수 있다.

(2) 내부 공격자에 대한 대응

멤버 중에 악의를 가진 자가 있을 수도 있다. 모든 멤버는 그룹 키를 가지고 있으므로 이것의 오용을 차단할 수 있는 메카니즘이 포함되어야 한다. 특히, 위장 공격과 재생 공격에 주의해야 하는데, 그 이유는 두 공격은 멀티캐스트에서 키를 알고 있으면 쉽게 시도될 수 있기 때문이다. 이 두 가지 공격에 관해 좀 더 살펴보면 다음과 같다.

- 위장 공격은 그룹 키만으로는 메시지의 발신처를 알아내지 못한다. 따라서, 이 문제는 각 멤버가 그의 메시지에 디지털 서명 기술을 사용해 서명을 하도록 함으로써 해결할 수 있다. 물론 디지털 서명 기술을 포함하기 위해선 이미 서로의 공개키를 가지고 있다고 가정하는데, 여기에서는 PKI(Public Key Infrastructure)를 사용한다고 가정한다. 인증 서버는 모두 의 공개키를 보관하고 있고 필요한 호스트에게 상대의 공개키를 제공한다고 가정한다.
- 멀티캐스트에서는 참여한 어느 멤버든지 간에 송신자의 메시지를 받았다가 나중에 이를 똑같이 재전송할 수 있다. 수신자는 이전의 메시지들과 키들을 보관하고 있지 않는 한 이러한 재생을 탐지해 낼 수 없다. 만일 수신자가 이러한 기록을 유지하지 않는다고 한다면, 메시지의 선명성(freshness)을 확보하는 것은 꼭 필요하다. 이를 위해 먼저 클럭이 안전하게 동기화 되었다고 가정하면, 가장 일반적 인 방법으로는 메시지 m에 타임 스탬프 (time stamp) t를 붙이는 것이다. 여기서, t는 메시지 생성 시간을 가리킨다. 그러므로, m 대신에 (m, t)로 대처하는 것이다. 선명성을 얻기 위한 또 다른 방법으로는 challenge and response 방법이 있다.

그 외 외부 공격자는 그룹 키를 모르기 때문에 트래픽의 양에 따라 추측하는 수동적인 공격만이 가능하다. 이것마저도 차단하고자 한다면, GSA가 주기적으로 무의미한 패킷을 전송함으로써 외부 공격을 피할 수 있다.

5. 결론

본 논문에서 제안한 내용은 S. Mitrra가 고안한 멀티캐스트 확장성 구조에 다중레벨 보안성을 이루는 방법을 제시한 것이다. 이것은 여러 서브 그룹들로 나누어서 각 서브 그룹에게 멤버들의 키 관리를 위임하면서 전체적인 가상 멀티캐스트 네트워크를 유지하는 것이다.

서브 그룹에서, 각 멤버의 인증 및 만남, 떠남, 데이터 전송, 키 관리 등은 GSA가 맡아서 하도록 하였다. GSA가 맡아서 하는 만큼 위험성도 내재하는데, 그 안정도에 따라서 GSA의 보안 레벨이 주어지도록 보안 정책을 세워야 한다. 이에 따라, 높은 보안 레벨을 얻기 위해서는 얼마나 서버가 안전한가를 먼저 공인 받는 일련의 객관적인 기준과 절차가 있어야 하고, 위협이 될 수 있는 보안 공격에 대한 대응책을 준비하는 것도 빠뜨려서는 안될 중요한 부분이다. 또한, 각 서브 그룹과 멤버는 보안 레벨을 갖고 있어서 차별화된 각종 서비스를 제공할 수 있다.

제안한 다중레벨 보안 구조는 다자 간의 네트워크 통신을 이용한 전자상거래 시스템 상에서의 신뢰성을 보장하기 위한 목적으로 연구하였으며, 특히, 금융 네트워크에서의 정보보호나 위성 방송사업과 연계된 CAS (Conditional Access System) 등에 유용하게 사용될 수 있을 것으로 예측된다.

참고문헌

[1] T. Ballardie, P. Francis, J. Crowcroft, "Core Based Trees - An Architecture for Scalable, Inter-Domain Multicast Routing", In Proceedings of ACM SIGCOMM '93, Sep. 1993.
[2] S. Deering, "Host Extensions for IP Multicasting", Request for Comments 1112, Inetrnet Network Working Group, Aug. 1989.
[3] S. Mitrra, "A Framework for Scalable Secure Multicasting", ACM SIGCOMM, Sep. 1997.
[4] M. Burrows, M. Abadi, R. Needham, "A Logic for Authentication", ACM Transaction on Computer Systems, Feb. 1990.
[5] M. Steiner, G. Tsudik, M. Waidner, "Differ-Hallman Key Distribution Extended to Group Communication", In Proceedings of the 3rd ACM Conference on Computer and Communications Security, Mar. 1996.
[6] G. Chiou, W. Chen, "Secure Broadcasting Using the Secure Lock", IEEE Transaction on Software Engineering, Aug. 1989.
[7] L. Gong, N. Shacham, "Multicast Security and its extension to a mobile environment ", ACM Baltzer Journal of Wireless Networks, 1(3):281-295, Oct. 1995.
[8] N. Heintze, D. Tygar, "Model Checking Electronic Commerce Protocol", ARP contract F33615-93-1-1330, Nov. 1995.
[9] J. Daeman, "Cipher and Hash Function Design", Ph.D. thesis, Katholieke Universiteit Leuven, Mar. 1995.
[10] M. Green, "Role of Certificate Authrity in Internet Commerce", 1997.
[11] H. Sun, "Computer and Network Security", Lecture by Rivest of MIT. http://theory.lcs.mit.edu/~rosario/6.915/lecture6.
[12] CCITT X.500, "The Directory: Overview of concepts, Models and Services", CCITT, 1992.

저자소개

서장원(e-mail : jwsuh@haksan.dsc.ac.kr)
1992년 : 서울산업대학교 전자계산학과(공학사)
1996년 : 숭실대학교 정보과학대학원 소프트웨어공학과(공학석사)
2000년 : 숭실대학교 대학원 컴퓨터학과(공학박사)
1992년~1998년 : 서울산업대학교 전자계산소
1998년~2001년 : 서울산업대학교 공동실험실습센터
2001년~현재 : 동서울대학 전자계산과 전임강사
관심분야 : 암호시스템, 네트워크 보안, 전자상거래 보안 솔루션