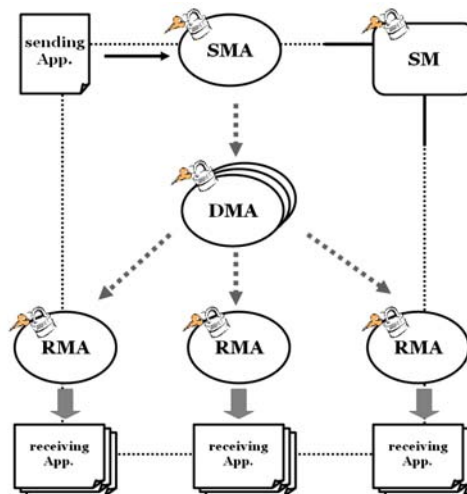


[공통기반] 멀티캐스트 전송 및 보안 기술 표준화 동향

멀티캐스트 기술은 IPTV 서비스에서 콘텐츠를 전송하기 위한 핵심기술로, 현재 ITU-T SG11과 SG17에서 멀티캐스트 전송 및 보안에 관련된 표준화를 진행 중에 있다. 최근 9월 아르헨티나에서 개최된 SG11회의에서는 멀티캐스트 보안 규격(ITU-T X.603.1|ISO/IEC 16512-2-Amendment1)에 대한 최종 표준안 검토가 이루어졌으며, 최종승인을 진행하기로 결의되었다. 또한, 다-대-다 멀티캐스트 전송 프로토콜 표준(안)에 대한 논의가 이루어졌으며, 메시지 포맷 표현 등 기술적 이슈를 중점적으로 다루었다. 본 표준(안)은 차기 1월 회의에서 최종승인을 추진할 예정으로 보인다. 또한, 모바일 환경에서의 멀티캐스트 전송을 위한 MMC-3에 대한 논의도 이루어졌으며, 본 표준안에서는 오버레이 멀티캐스트 환경에서 이동 사용자를 위한 끊김 없는 전송을 지원하는 규격을 정의하고 있다. 이와 함께, IP-멀티캐스트 환경에서의 이동 사용자를 위한 전송 규격인 X.MMC-2는 이번 회의에서는 논의가 이루어지지 않았으나, 내년 1월 차기 회의에서 최종 승인을 추진할 예정으로 보인다. 이 밖에, SG17에서 추진하고 있는 다양한 멀티캐스트 통신 환경에서의 보안 요구사항 및 기능, 프레임워크를 정의하는 X.mcsec-1에 대해서는 차기 회의에서 최종 승인을 추진하기로 하였다.

멀티캐스트 보안 규격 표준화 진행현황

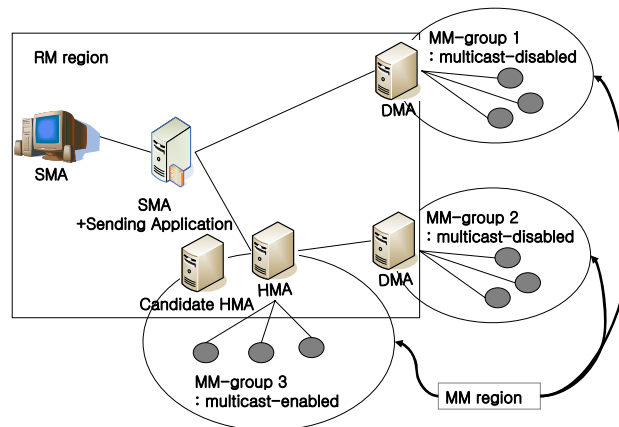
이번 회의에서 최종승인단계에 진입한 중계기반 멀티캐스트 보안 규격(ITU-T X.603.1 |ISO/IEC 16512-2 - Amendment1) 표준안 내용을 간략히 소개하도록 하고자 한다. <그림 1>은 본 보안프로토콜에서 구성하는 보안 서비스 모델이다. SM은 멀티캐스트 서비스를 위한 전체 세션에 대한 관리 및 하위 보안 에이전트에 대한 관리를 담당한다. SMA는 멀티캐스트 콘텐츠에 대한 보호를 담당하며, RMA는 보안 클라이언트 프로그램이다. DMA는 멀티캐스트 그룹키 관리, 멤버십 인증, 서비스 권한검증 등의 중추적인 역할을 담당한다.



<그림 1> 중계기반 멀티캐스트 보안 규격 표준(안) 관련 보안 서비스 모델

(출처: ITU-T X.603.1|IS 16512-2/draft Amd.1: Final draft Recommendation for Consent(T09-SG11-090902-TD-GEN-0311!R1!MSW-E))

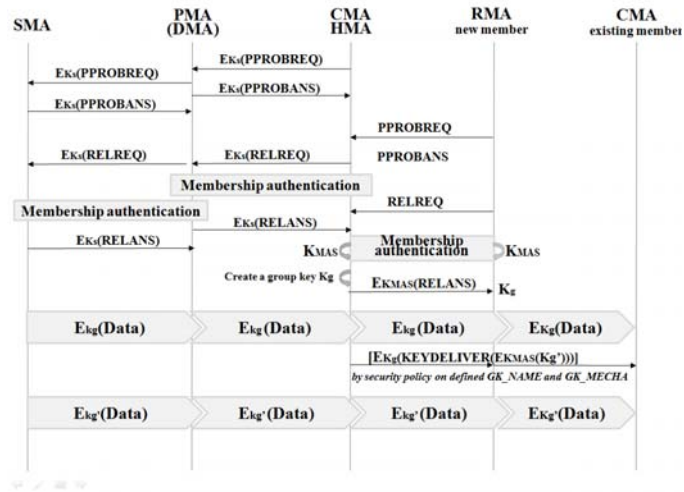
좀 더 구체적으로 설명하면, SM은 보안 정책관리, 세션 가입 관리, 보안 에이전트 간에 공유되는 세션키 관리, 접근제어 리스트 관리, 멀티캐스트 그룹 및 세션 멤버십 관리와 기본적인 데이터 암호화를 수행한다. DMA는 RMA 그룹과 공유되는 그룹키 관리, 콘텐츠 암호키 관리, 안전한 멀티캐스트 전송 트리 구성, 수신자에 대한 멤버십 관리를 수행한다.



<그림 2> 멀티캐스트 보안영역 정의

(출처: ITU-T X.603.1|IS 16512-2/draft Amd.1: Final draft Recommendation for Consent(T09-SG11-090902-TD-GEN-0311!R1!MSW-E))

<그림 2>는 안전한 멀티캐스트 보안 관리를 위해 2개의 영역으로 분산하여 보안영역을 정의한 것으로 나타낸다. 송신자 보안 에이전트인 SMA와 SM, DMA로 구성된 RM 영역과, DMA와 수신자 보안 에이전트인 RMA들로 구성되는 MM 영역이 있다. 또한 MM 영역은 각 DMA와 수신 그룹을 구성하는 RMA들로 구성되는 MM 그룹으로 구성되어 분산시켜서 보안 관리를 수행함으로써 안전성을 높이고, 일부의 변화가 전체에 영향을 미치는 범위를 최소화 했다.



<그림 3> 안전한 멀티캐스트 트리 구성을 위한 절차

(출처: ITU-T X.603.1|IS 16512-2/draft Amd.1: Final draft Recommendation for Consent(T09-SG11-090902-TD-GEN-0311!R1!MSW-E))

<그림 3>은 안전하게 멀티캐스트 트리를 구성하기 위한 절차를 나타낸 것으로, RM 영역에 교환되는 모든 메시지는 세션키(Ks)로 암호화하여 보호하며, 멤버십 인증을 통해 멀티캐스트 세션에 가입된 노드 인지를 검증한 후, 트리 가입을 허용한다.

멀티캐스트 데이터의 보호는 SMA에 의해 생성되는 암호키를 통해 보호되며, SMA가 생성한 암호키를 RM영역에서는 세션키로, MM 영역의 각 하위 그룹들은 각자가 소유한 그룹키로 보호하여 전달함으로써 대용량의 멀티캐스트 데이터에 대한 암호복호화에 따른 효율성을 높였다. 본 표준에서의 그룹키 관리 방식은 기존의 IETF에서 제정한 많은 키관리 방식을 도입하여 사용할 수 있도록 표준 간의 상호호환성도 고려하였다.

이외에, 멀티캐스트 표준에 대해서 간단히 소개하자면, X.RMCP-3는 효율적인 다-대-다 그룹통신을 지원하기 위해 메쉬 또는 링구조의 코어의 집합을 가지며, 코어에 하부 트리가 구성됨으로써, 다-대-다 통신에서의 멀티캐스트 구성에 따른 효율성 및 안정성을 제공하였다. X. MMC-1은 이동 환경에서의 끊임 없는 멀티캐스트 전송을 제공하기 위한 기본 요구사항 및 기능 프레임워크를 정의하고 있으며, X.MMC-2에서는 IP 멀티캐스트를 이용해서 데이터를 수신하는 환경에서 이동 노드를 지원하기 위한 멀티캐스트 핸드오프 및 제어를 위한 프로토콜을 정의한다. X.MMC-3에서는 오버레이 환경에서 이동성 지원을 위한 핸드오프 및 제어 절차 등의 전송 규격을 정의하고 있다. 또한 SG17에서 추진되고 있는 X.mcsec-1에서는 앞에서 소개된 다양한 환경에서의 멀티캐스트 전송시 지원해야 할 멀티캐스트 보안 요구사항과 기능, 프레임워크를 정의하고 있으며, 각 다양한 멀티캐스트 전송시에 보안 적용 시나리오를 제안하고 있다.

결언

향후 멀티캐스트 기술 표준화는 차세대 네트워크인 NGN 환경에서 적합한 멀티캐스트, 그리고 IPTV 서비스에서의 멀티캐스트 관련된 부분에서 중점적으로 다루어질 것으로 전망되며, 연구로만 진행되어 오던 멀티캐스트 기술이 직접 활용되는 IPTV 서비스, IPv6 인프라, 그린 IT의 첫걸음으로서의 원격 화상회의 활성화 등에 힘입어 실제 환경을 고려한 멀티캐스트 기술에 대한 표준화에 박차를 가해야 할 것이다.

윤미연 (한국인터넷진흥원 정보보호본부 보호기술팀 선임연구원, myyoon@kisa.or.kr)