[IPTV 보안] ITU-T IPTV 보안 기술의 표준화 완료

IPTV 서비스는 실시간 멀티미디어 서비스를 IP 네트워크를 통해서 제공하는 기술로 VoD 서비스와 실시간 서비스를 포괄하여 정의하고 있다. 하지만 IPTV의 가치는 실시간 전송보다는 다양한 부가 서비스를 제공하는 것이 쉽다는 장점 때문일 것이다. 따라서 IPTV를 둘러싸고 많은 국가에서 표준화에 관심을 가지고 있다. 특히 일본의 경우 자국 내 표준과 ITU-T의 표준을 일치시키는 작업을 진행하고 있고, ITU-T SG16을 중심으로 자국의 서비스를 대거 표준에 반영하고 있다.
본 고는 2013년 4월 17일부터 4월 26일까지 스위스 제네바에서 진행된 ITU-T SG17 표준화 회의에서 논의된 내용을 바탕으로 IPTV 보안 기술 표준화 동향을 소개하고자 한다.

2013년 4월 ITU-T SG17 IPTV 보안 기술 표준화 완료

ITU-T는 FG-IPTV를 통해 IPTV 표준화 요구사항을 도출하고, IPTV-GSI를 거치면서 세부적인 표준화 기술을 정리하여 왔다. 여기서 개발된 요구사항은 각각의 표준 연구반(Study Group)에 전달되어 담당하는 기술의 세부 표준 개발을 진행하였고, SG17은 보안 기술에 대한 표준을 진행하여 마지막 승인 절차에 들어간 X.iptvsec-8을 포함하여 총 8개의 권고안을 제정하였다.
SG17 연구반에서 IPTV 보안 이슈는 Q6/17에서 담당을 하였으며, X.iptvsec-1 (X.1191) 문서는 FG-IPTV 결과물은 인계 받아서 기본 요구사항 문서로 승인하였고 X.iptvsec-2 ~ X.iptvsec-8까지 총 7개의 추가 권고안을 만들게 되었다.
모든 문서는 X.iptvsec-1 (X.1191)의 요구사항 및 구조에 정의되고 있는 내용을 바탕으로 하며, SG13 / SG16 / SG17이 협력하여 표준을 개발하였다. 최근 SG17에서는 작업 진행 중에 있던 8번째 권고안을 채택하여 최종 승인 절차에 돌입하였다. 이로써 5년간 지속되어 온 표준화 작업에 완성을 이루었다고 할 수 있다. 특히 마지막 권고안인 X.iptvsec-8 (X.1198) 권고안은 국내 iCAS 표준안과 맥을 같이하는 표준으로 국내 기술의 국제 표준 반영 및 관련 기술의 국내 특허 확보라는 2가지 장점을 모두 가지고 있다. 다음은 표준화 회의에서 승인된 8개의 문서에 대해서 살펴보고자 한다.

X.1191: IPTV 요구사항 및 구조

X.1191 권고안은 IPTV 보안에 대한 요구사항과 보안 구조를 정의하고 있는 문서로 “콘텐츠”, “서비스”, “네트워크”, “단말”, “사용자” 구분하여 요구사항을 정리하고 있다. 이 중에서 표준화 대상은 콘텐츠와 서비스로 한정하고 있으며 네트워크 보안 기능은 네트워크의 고유 기능을 확장하는 것으로 IPTV 표준화의 대상이 되지 않는다. 단말 및 사용자 보호 기술은 다른 보안 기술과 연동하여 제공하는 기술로 IPTV 서비스 혹은 콘텐츠 보호를 위한 대상이 아니기 때문에 X.1191에서는 표준화 대상으로 선정하지 않았다

X.1192: 트랜스코딩 가능한 보안 기술

X.1192는 별도의 복호화 과정을 거치지 않고 트랜스코딩이 가능한 기술을 표준화하고 있다. 모바일 단말기를 위해 별도의 스트림을 제작하지 않고, 기존의 스트림을 암호화된 상태로 다운 사이징하는 기술이다. 트랜스코더에서 SCP(Service and Content Protection)가 변하지 않고 PDA용으로 다운사이징하는 경우와 완전 다른 SCP로 변환하는 경우를 모두 포함하고 있다.

X.1193: 키 관리 기술

IPTV 서비스를 위한 키 관리 기술을 정의하고 있는 문서로 3단계인 TEK, SEK, URK의 키를 정의한다. 수신제한 시스템에서 사용하는 다단계 키 관리 시스템과 비교하여 CW, AK, DK로 매칭되는 내용이며 IETF의 MIKEY 문서를 기반으로 IPTV 시스템에 맞도록 확장하여 정한 표준 문서이다.

X.1194: 복호화 선택 기술

방송 서비스에서 사용자의 단말이 특정 사업자에게 종속되는 가장 큰 이유는 암호 알고리즘 및 이를 지원하는 알고리즘들이 특정 사업의 제품을 사용하기 때문이다. 기존에 SimulCrypt 등의 다중 암호화 방식이 사용되기도 하였으나 실제 제품 적용에는 어려움이 있었다. 본 표준은 이를 해결하기 위해서 사업자가 임의로 암호 알고리즘을 변경할 수 있고 이를 단말이 지원하는 방식을 제안하고 있다. 특히 이미 잘 알려진 암호 알고리즘의 경우 별도의 추가 설치 없이 바로 적용이 가능한 기능을 제공한다.

X.1195: 보안 기술 상호호환 기술

X.1195 표준은 실시간 혹은 비실시간 서비스에서 서로 다른 보안 기술을 적용하는 시스템이 상호 호환성을 갖도록 하는 표준이다. 특히 PVR 및 Service Roaming과 같이 서로 다른 보안 서비스를 변환해야 하는 경우에 대해서 표준 형식을 정의하고 있어 보안 기술 간에 상호호환이 가능하다.

X.1196: 모바일 IPTV에서의 다운로드 기반 보안 기술

X.1196 표준은 모바일 단말에서 IPTV 서비스를 시청하는 경우 별도의 하드웨어 혹은 장치 없이 콘텐츠 및 응용서비스 등을 소프트웨어적으로 다운로드 받아서 실행할 수 있는 표준을 정의하고 있다. 즉, IPTV 콘텐츠 제공자들이 생성한 응용서비스들을 서비스 제공자들을 통해 사용자 모바일 단말에 안전하게 전달되는 방식(개별전달 방식, 중계서버 방식)을 규정하는 표준이다.

X.1197: IPTV 서비스에서 암호 알고리즘을 선택하는 가이드라인

X.1197 표준은 다양한 IPTV 서비스 및 응용 서비스에서 암호 알고리즘 및 관련 기능을 선택하는데 있어서 선택과 적용을 위한 가이드라인을 제공하고 있다. 서비스의 성격에 따라서 제공하는 보안 강도를 고려하고 현재 상태에서 안전한 알고리즘을 정리 및 권고하고 있다. 또한, 본 표준의 궁극적인 목적은 대부분의 IPTV 서비스에서 암호 알고리즘이 미국 AES가 사용되고 있어, 국

내 SEED, HIGHT 등의 암호 알고리즘을 국제표준에 추가하는 데 그 의의가 있는 표준이다.

X.1198: 가상 머신 기반의 보안 시스템

국내 iCAS 기술인 가상 머신 기반의 보안 시스템 기술을 국제 표준에 반영한 표준안으로 가상 머신의 세부 동작, 호환성 확보를 위한 구조, 메시지 형식, 단말 인증 방식을 포함하고 있으며, 중복 및 복제 단말을 검출하기 위한 일회용 단말 인증 기술을 포함하고 있다.

주요 이슈 및 쟁점사항

X.1191을 시작으로 X.1198까지 8개의 권고안이 최종 승인되어서 IPTV 서비스 보안을 위한 표준이 완성되었다고 볼 수 있다. 특히 X.1198 표준은 국내의 표준을 국제 표준에 반영한 것으로 그 의미가 크다고 할 수 있다. 지금까지 표준이 진행된 문서는 IPTV 1.0을 가정하고 있고 또한 다양한 응용 서비스 보다는 IPTV 서비스 자체에 대한 보안 기술을 표준 적용한 것으로 향후 IPTV 2.0 및 다양한 응용 서비스에서의 표준화가 추가되어야 할 것이다. 또한 이러한 일련의 표준은 1세대의 표준이 아닌 2세대의 표준으로 새롭게 자리매김할 것으로 판단한다.

박종열 (ETRI 실장, ITU-T SG17 에디터, ISO/IEC JTC1 에디터, jongyoul@etri.re.kr)