[정보보호] ITU-T의 IPTV 보안기술 표준화 현황

IPTV 분야의 국제표준 개발을 추진하고 있는 ITU-T IPTV-GSI 회의가 2010년 7월 19일부터 23일까지 스위스 제네바에서 개최되었다. 본 회의에 보안 분야의 표준을 리드하고 있는 연구반 17의 연구과제 6&7 그룹이 참가하였으며, 보안 이슈 회의에서는 다양한 크기를 갖는 모바일 단말에 적용가능한 종단간 보안 요구사항과 메커니즘을 다루는 IPTV 트랜스코더블 보안 기법(X.iptvsec-2), 유니캐스트 및 멀티캐스트 환경에서 IPTV 스트림과 다운로더불 SCP(service and content protection) 을 위한 키관리 기법(X.iptvsec-3), 모바일 IPTV 환경에서 다운로더블 SCP(서비스 콘텐츠 보안) 기법(X.iptvsec-6), IPTV 암호알고리즘 선택 기준(X.iptvsec-7) 등의 기존 권고안들에 대한 기고서들이 다뤄졌다. 본 고에서는 IPTV 보안 표준화 동향을 개관하고, 7월 회의에서 논의된 쟁점사항을 중심으로 기술하며, 향후 추진방향을 제시하고자 한다.

주요 이슈 및 쟁점사항

현재 ITU-T 연구반 17 연구과제 6에서 개발 중이거나 완료된 권고 또는 권고안은 <표 1>과 같으며, 표준화가 완료된 권고의 경우 2009년 2월 채택된 “IPTV 보안 기능요구사항과 구조(X.1191)”가 있으며, 현재 개발중인 권고의 경우 “안전한 IPTV 트린스코더블 기법(X.iptvsec-2)", "IPTV 키관리 기법(X.iptvsec-3)", "IPTV 단말에서 디스크림블링 알고리즘 선택 기법(X.iptvsec-4)", "서로 다른 IPTV SCP 시스템의 상호연동(X.iptvsec-5)", "모바일 IPTV 환경에서 다운로더블 서비스 콘텐츠 기법(X.iptvsec-6)", "IPTV 표준 암호알고리즘 선택 기준(X.iptvsec-7)" 등 6건의 권고가 있다. .

7월에 개최된 IPTV-GSI 회의에서는 X.iptvsec-2에 관한 3건, X.iptvsec-3에 관한 1건, X.iptvsec-6에 관한 1건, X.iptvsec-7 에 관한 2건 등 모두 7건의 기고서가 다뤄졌다.

X.iptvsec-2(안전한 트랜스코더블 기법)와 X.iptvsec-3(키관리)의 경우, 별다른 쟁점사항은 없었고, 한국 제안 내용이 대부분 이견없이 반영되었으며, 주로 권고안의 완성도를 높이는 작업이 이뤄졌다. 또한 지난 4월 연구반 17 회의에서 신설된 바 있는 X.iptvsec-6(다운로더블 SCP 기법)의 경우, TTA 단체 표준인 iCAS (interchangeable conditional access system)표준과 연계추진이 가능한 권고로서 한국 제안이 큰 쟁점 없이 채택되었으며, 이를 통해 권고의 문서 구조와 일반 요구사항이 합의되었다. 한편, 연구반 13 연구과제 3에서 “모바일 IPTV를 위한 요구사항” 권고안이 지난 5월 신설된 바 있어, X.iptvsec-6 개발시 연구반 13과 긴밀하게 협력해 개발키로 합의했다. 또한 “모바일 IPTV 보안 요구사항”에 관한 신규 워크아이템을 신설할 지와 시기에 대한 논의가 이뤄졌고, 논의 결과 향후 연구반 13에서 모바일 IPTV를 위한 기능 구조와 유스 케이스가 개발되는 시점에 모바일 IPTV 보안 요구사항과 기능구조에 대한 표준의 신설 여부를 결정키로 했다.

<표 1> 현재 개발 중 또는 개발 완료된 ITU-T IPTV 보안 권고 (2010 년 8 월 현재)

표준약어	표준 제목	표준 에디터	승인 추진일시
X.1191 (X.iptvsec-1)	Functional requirements and architecture for IPTV security aspects	염흥열(순천향대), Nhut Nguyen (미국), Ishii. Shinji(일본), Xie Wei(중국)	2009.2
X.iptvsec-2	Functional requirements and mechanisms for secure transcodable scheme of IPTV	나재훈(ETRI)	2011.4
X.iptvsec-3	Key management framework for secure IPTV services	염흥열(순천향대)	2011.4
X.iptvsec-4	Algorithm selection scheme for service and content protection (SCP) descrambling	박종열(ETRI), Nhut Nguyen (미국)	2011.4
X.iptvsec-5	Service and content protection (SCP) interoperability scheme	윤기송(ETRI), Dong Wang (중국)	2010.12
X.iptvsec-6	Framework for the downloadable service and content protection (SCP) system in mobile IPTV environment	염흥열 (순천향대)	2012.3
X.iptvsec-7	Guidelines on criteria for selecting cyptographic algorthms for the IPTV service and content protection (SCP)	윤석웅(KISA), 염흥열(순천향대)	2012.3

X.iptvsec-7(IPTV 보안 알고리즘 선택 기준)의 경우 두 가지 쟁점사항이 제기되었다. 하나는 알고리즘 선택 기준을 개발 시 각 나라나 지역의 규제도 고려해야 하느냐 하는 문제이고 다른 하나는 기존 권고와의 관계의 구체화에 대한 문제였다. 지난 4월 권고안 신설 시 X.iptvsec-7은 알고리즘의 기술적 선택 기준만을 개발하고, 현재 주요 표준화 기구나 국가에 의해 표준화된 암호알고리즘 중 이 기준을 만족하는 암호 알고리즘을 IPTV 암호 알고리즘 후보 목록으로 선정키로 합의한 바 있다. 그러나 이번 7월 회의에서 독일이 암호 알고리즘 선정 기준 개발 시 각 지역과 국가의 알고리즘 선정 관련 규제도 중요하게 고려해야 한다고 주장하면서 EU의 두 가지 directive인 “Universal service directive”와 “Access control directive”, 그리고 연관 부록 등에 제시된 한정수신시스템(CAS, conditional access system) 관련 규제 항목을 권고안 본문에 넣자고 제안하였다. 토론 동안 한국은 규제까지 다룬다면 권고안 개발 과정과 승인과정에서 어려움이 예상되며 기술적인 선정 기준만을 다루는 것이 타당하므로, 암호알고리즘 규제는 정보만을 다루는 appendix로 넣자고 주장했다. 일본은 규제관련 구체 내용은 권고 본문과 동일한 조건을 갖는 annex에 넣자고 주장했다. 토론 후 타협이 이뤄져, 권고 본문에는 EU 규제의 개요를 간단히 기술하고, 규제 세부 내용은 appendix에 간단히 넣는 것으로 합의했다. 또 다른 쟁점은 X.iptvsec-4와 X.iptvsec-7 과의 범위를 분명히 하자는 것이었는데, 토론 후, X.iptvsec-4는 제한수신시스템에 대한 선택을 다루고, X.iptvsec-7은 암호알고리즘 선택 기준을 다루는 것으로 합의했다.

향후 추진 전망

이번 회의를 통해 지난 4월 연구반 17 회의에서 IPTV 보안 분야 두 가지 새로운 워크아이템으로 신설된 X.iptvsec-6(다운로더블 SCP 기법)과 X.iptvsec-7(암호알고리즘 선정 기준)에 대한

권고안의 구조와 내용이 합의되었다. 이 두 가지 권고는 현재 권고개발 초기 상태에 있으므로, 앞으로 권고 내용 구체화가 필요하다. X.iptvsec-6 권고안은 방송통신위원회의 IPTV 한전수신제한 기술에 대한 기술기준(분리가능, 교체가능, 상호연동가능, 다운로드 가능 서비스 콘텐츠 보호기술 적용)과 연관되므로 향후 세심한 관찰이 필요하며, X.iptvsec-7는 국산 암호알고리즘(SEED 등)이 탑재될 수 있도록 암호 알고리즘 선정 기준을 결정해야 할 것이다. 현재 연구반 17에서 개발 중인 IPTV 보안 표준은 국내 산업에 미치는 파급효과가 클 것으로 예측되므로, 국내 산업체와 보안 기관들의 관찰과 대응이 요구된다.

염흥열 (순천향대 교수, ITU-T SG17 부의장, WP2/SG17 의장, hyyoum@sch.ac.kr)