ITU-T FG IPTV Security Aspects 표준화 기술 동향

The Standardization Issue for ITU-T FG IPTV Security Aspects

박종열 (J.Y. Park) 유비쿼터스홈서비스연구팀 선임연구원
문진영 (J.Y. Moon) 유비쿼터스홈서비스연구팀 연구원
김정태 (J.T. Kim) 유비쿼터스홈서비스연구팀 연구원
백의현 (E.H. Paik) 유비쿼터스홈서비스연구팀 팀장

목 차

Ⅰ. 서론
Ⅱ. ITU-T 표준화 목적
Ⅲ. ITU-T 표준화 항목
Ⅳ. ITU-T 표준화 기술 동향
Ⅴ. 결론

IPTV 서비스는 IP 환경에서 다양한 콘텐트를 전송하는 기술로 기존의 방송 시스템과 통신 시스템의 장점을 그대로 수용하는 기술이다. 이에 ITU-T SG13에서는 FG IPTV를 통해 요구사항 및 구조 중심의 표준화를 진행하고 있다. ITU-T FG IPTV는 6개의 WG로 구성되어 진행중에 있으며, WG3는 security aspects의 주제를 가지고 보안 기술에 대한 표준화를 진행하고 있다. 본 문서는 2007년 5월과 7월의 4차, 5차 표준화 회의를 중심으로 WG3의 표준화 동향 및 기술적 분석을 정리한다.

Ⅰ. 서론

ITU-T FG IPTV는 SG13(NGN)을 모 그룹으로 하는 프로젝트 그룹이다. 2006년 1월 요구사항 및 서비스 구조 정의를 위해 한시적으로 만들어진 조직으로 현재 5차 회의까지 진행되고 있다. 전반적인 표준화 과정을 진행하면서 특정 기술이나 장치에 종속되지 않고 있다.

본 문서는 Ⅱ장에서 WG3(security aspects) 분야의 표준화 목적 및 대상 범위를 정의하며, Ⅲ장에서는 현재의 작업 문서(Working Document)[1]를 바탕으로 논의되고 있는 쟁점 사항들을 정리한다. Ⅳ장에서는 2007년 5월의 4차 회의 및 2007년 7월의 5차 회의에 걸쳐 집중적으로 논의되고 있는 사항들을 정리하고 결론을 맺는다.

Ⅱ. ITU-T 표준화 목적

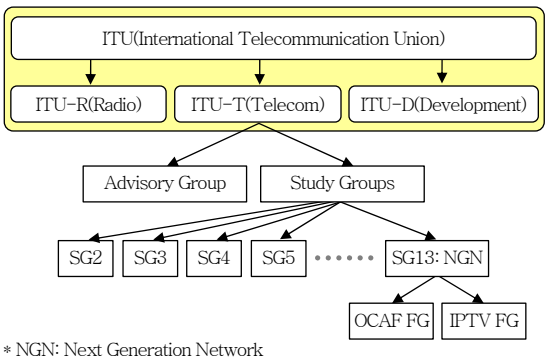
1. FG IPTV 구성

ITU-T의 NGN 표준화 그룹인 SG13은 NGN 활성화 방안으로 IPTV에 대한 표준화 진행을 제안하였다. 이를 받아들여 ITU-TSB는 2004년 4월 consultant meeting을 통해 조직 구성 및 작업 방향에 대한 기본적인 내용을 정의하였다.

이 회의에서 IPTV Focus Group은 2006년 7월 1차 제네바 회의를 시작으로 1년간 요구사항, 서비스 시나리오, 정책 및 표준화 방향, IP 망 기능구조, 시스템 운용/과금/인증, 응용서비스 및 코덱, 구현방법과 QoS에 대한 작업을 마무리할 계획이었다.

(그림 1)은 ITU에서 FG IPTV의 역할에 대한 이해를 돕기 위한 그림이다[2]. IPTV와 관련해서 ITU-R 측면에서의 요구사항과 ITU-T 안의 다른 Study Group과 협력하여 진행중이며, 최종 작업 문서는 SG13의 승인 절차를 통해서 결정된다.

IPTV FG IPTV는 2006년 1차 회의를 통해 "구조 및 서비스 요구사항", "QoS 및 성능", "서비스 보안 및 콘텐트 보호", "네트워크 제어", "단말 시스템", "미들웨어, 애플리케이션, 콘텐트 플랫폼"의 6개 WG을 승인하고 표준화를 진행중에 있다.



* NGN: Next Generation Network
* OCAF: Open Communications Architecture Forum

(그림 1) ITU-T FG IPTV 구조도

2. WG3의 목적 및 표준화 대상 범위

각 WG의 역할에 따라 WG3(security aspects)는 서비스 보안 및 콘텐트 보호를 위한 목적(security goals), 위험 요소(security threats), 요구사항(security requirements), 보안 구조(security architecture), 보안 메커니즘(security mechanism)으로 정리하고 있다.

WG3의 주요 표준화 내용은 IPTV 서비스 접근을 제어하는 service security(예, conditional access system) 분야와 콘텐트 자체에 대한 권한 설정 및 제어를 하는 content security(예, DRM)로 구분하여 연구가 진행중에 있다. 물론 네트워크 보안, 단말 보안, 사용자 보안이 포함되어 있지만, 주 논쟁 분야는 이 두 가지이다.

다음장에서는 WG3의 표준화 항목에 대해서 자세히 알아보고, 현재까지의 표준화 기술 동향 및 관련 기술에 대해서 기술하여 정리한다.

Ⅲ. ITU-T 표준화 항목

WG3의 표준화는 크게 service security와 content security로 양분되어 진행되고 있다. Service security는 전통적인 방송에서 사용하고 있는 CAS

기능으로 IPTV 서비스에 가입된 가입자가 자신의 가입 정보에 따라서 방송 채널을 수신 혹은 수신하지 못하도록 하는 기능을 포괄한다. 반면 content security는 인터넷 및 콘텐트 기반의 접근을 제어하는 기술로 DRM 기술로 대표된다. DRM은 콘텐트의 소유자 혹은 생성자가 콘텐트의 사용 권한을 부여하는 기능을 가지고 있어 콘텐트 혹은 제작자 중심의 콘텐트 보호 기술이다. WG3에서는 특정 기술에 종속되는 것을 피하기 위해서 CAS, DRM과 같은 특정 기술에 관한 단어를 사용하지 않고 있다.

WG3과 관련이 있는 Working Document는 WG1의 security requirement 부분과 WG3의 "Working Document: IPTV Security Aspects"로 구분된다. 본 문서는 5차 회의 Working Document: IPTV security aspects[1]와 4차 회의 Working Document: IPTV security aspects[3] 내용을 위주로 정리한다.

1. 표준화 범위

WG3는 보호해야 하는 대상으로 "콘텐트(content)", "서비스(service)", "네트워크(network)", "단말(terminal devices)"로 정의하고 "위협(threats)", "요구사항(requirements)", "구조(architecture)", "기술(mechanisms)" 4가지 측면에서 각각의 내용을 정리하고 있다.

2. 표준화 목적

WG3의 표준화 문서는 확장성과 보안성을 중심으로 다음의 사항을 만족하는 시스템 구성을 목적으로 한다.

- 성능, 사용성, 확장성, 계정 기반의 과금 지원
- 비인가 콘텐트 혹은 서비스 접근 차단
- 비인가 콘텐트 사용 및 복사, 저장, 재전송 차단
- 콘텐트, 서비스, 네트워크, 단말, 사용자에게 적용된 기득권을 해하지 말 것
- 데이터, 컨트롤, 관리 기능을 분리할 수 있을 만큼 유연하고 확장 가능해야 할 것
- 신호, 컨트롤, 관리, 사용자 데이터 트래픽을 논리적/물리적으로 분리할 것
- 기존에 사용되고 있는 보안 표준 및 설계 명세서를 기반으로 할 것
- 보안 기능은 서비스 성능에 영향을 미치지 말아야 할 것
- 콘텐트 제공자가 정한 허가 및 조건 하에서 콘텐트의 상호 호환성을 막지 말아야 함

위의 내용에서 알 수 있듯이 ITU-T FG IPTV는 새로운 기술을 개발하고 표준화하기 보다는 기존에 확보하고 있는 기술을 기반으로 IPTV 서비스에 적용하는 것을 목적으로 하고 있다.

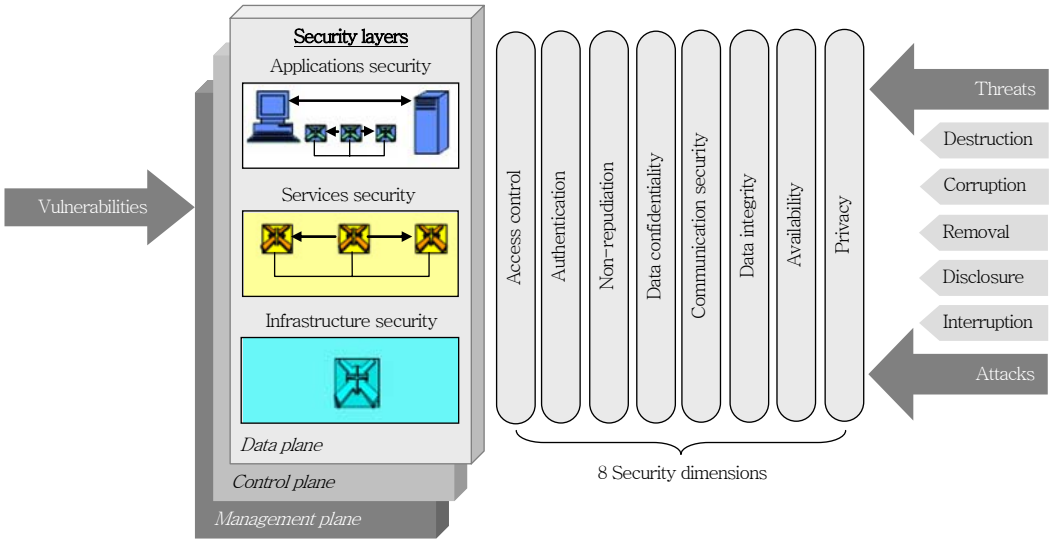
3. 보안 위협(Security threats)

IPTV 서비스에서 고려되는 보안 위협에 대한 내용을 정리하고 있다. 즉 WG3의 보안 서비스의 기능이 대응해야 하는 위협 요소를 정의하고 있다. 이 내용은 ITU-T X.800[4] 및 X.805[5]에서 정의하고 있는 보안 위협 요소 및 이에 대응하는 기술을 기반으로 정의하고 있다. (그림 2)는 X.805[5]에서 정의하고 있는 위협 요소(threats)와 보안 서비스(8 security dimensions)에 대한 그림을 보여 주고 있다.

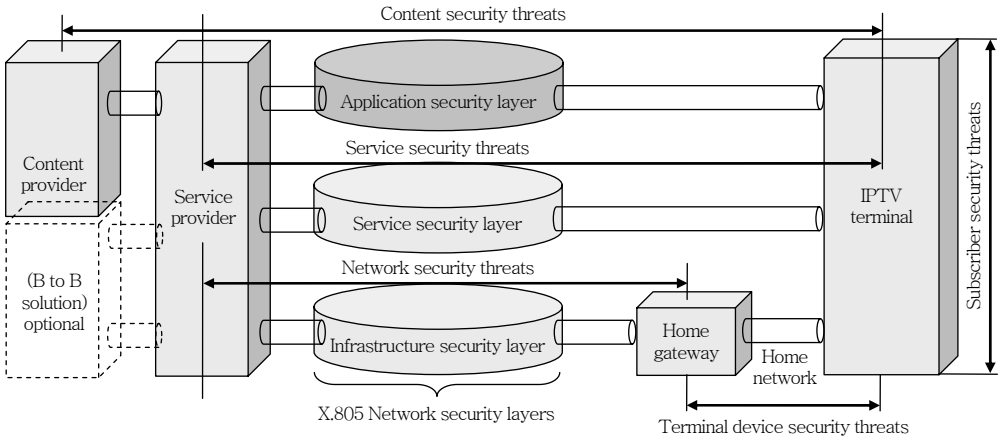
4. 보안 위협 모델(Security threats model)

보안 위협은 5가지 형태의 보안 위협 요소를 가지고 있다. 이러한 보안 위협들 사이의 관계를 모델로 보여주고 있는 것이 (그림 3)이다. WG3에서 주로 담당하게 될 분야로 콘텐트 위협(content security threats), 서비스 위협(service security threats), 네트워크 위협(network security threats), 단말 장치 위협(terminal device security threats), 사용자 위협(subscriber security threats)으로 구분된다.

- 콘텐트 위협(content security threats): 콘텐트 위협으로부터 보호해야 할 대상은 콘텐트 제공



(그림 2) X.805 Security Architecture[5]



(그림 3) IPTV Security Elements and X.805 Network Security Layers[5]

자 혹은 서비스 사업자에게 소속되어 사용자에게 전송되는 콘텐트를 의미하며, 실시간 방송 콘텐트(broadcast TV content), VoD 콘텐트(VoD content), 푸시 VoD 콘텐트(push VoD content), PVR 콘텐트(PVR content), 다운로드 받은 응용 프로그램(downloaded application)을 포함한다. 이들에 대한 잠재적인 위협으로는 "네트워크에서 콘텐트 가로채기(interception)", "무인가 시청(unauthorized viewing)", "무인가 재분배 혹은 재가공(unauthorized reproduction or redistribution)"이 있다.

- 서비스 위협(service security threats): 서비스 위협으로부터 보호해야 할 대상은 서비스 사업자에게 소속되어 있는 자원으로 미디어 서버, AAA 서버, DRM 서버, CDN 서버, 과금 서버, 관리 서버를 포함한다. 이들의 잠재적인 위협으로는 "악의적 저작권 침해(impingement copyrights)", "가면 공격(masquerading/spoofing)", "악의적 공격(hacking, DoS attack)", "가입자 해킹(phishing, Trojan horse)"에 노출되어 있다.
- 네트워크 위협(network security threats): 네트워크 위협으로부터 보호해야 할 대상은 네트

워크 사업자에게 소속되어 있는 자원으로 라우터, 스위치, 네트워크 자원(네트워크 대역폭, 멀티캐스트 주소 등등)을 포함한다. 이들에 대한 잠재적인 위협으로 "내부자 공격(internal threats: malicious attacks)", "멀티캐스트 공격(security threats to multicast)", "악의적 공격(CDN에서의 DoS attack, hacking)"에 노출되어 있다.

- 단말 장치 위협(terminal device security threats): 단말 장치 위협으로부터 보호해야 할 대상은 단말 장치에 소속된 자원으로 최종 사용자가 콘텐트를 소비하는 과정에서 필요한 자원을 대상으로 한다. 이들에 대한 잠재적인 위협으로 "하드웨어 공격(tampering device hardware)", "불법적인 비밀정보 접근(암호화 키 혹은 유사한 비밀 정보)", "하드웨어 장치 수정(DRM 무력화를 위해 시간 정보를 수정)", "비인가된 프로그램의 다운로드 및 실행", "바이러스 공격"에 노출되어 있다.
- 사용자 위협(subscriber security threats): 사용자 위협으로부터 보호해야 할 대상은 가입자의 정보가 되며, 이들에 대한 잠재적인 위협으로 "사용자 정보의 불법적인 복사/유출"이 있을 수 있다.

이상의 위협을 기반으로 WG3는 IPTV 서비스 보안 기술에 대한 요구사항 및 보안 구조 표준안을 작성중에 있다. 보안 위협(threats), 보호 자원(assets), 보안 기법(security mechanism)의 관계 자료는 WG3의 Working Document[1]를 참고하면 된다.

5. 보안 요구사항(Security requirements)

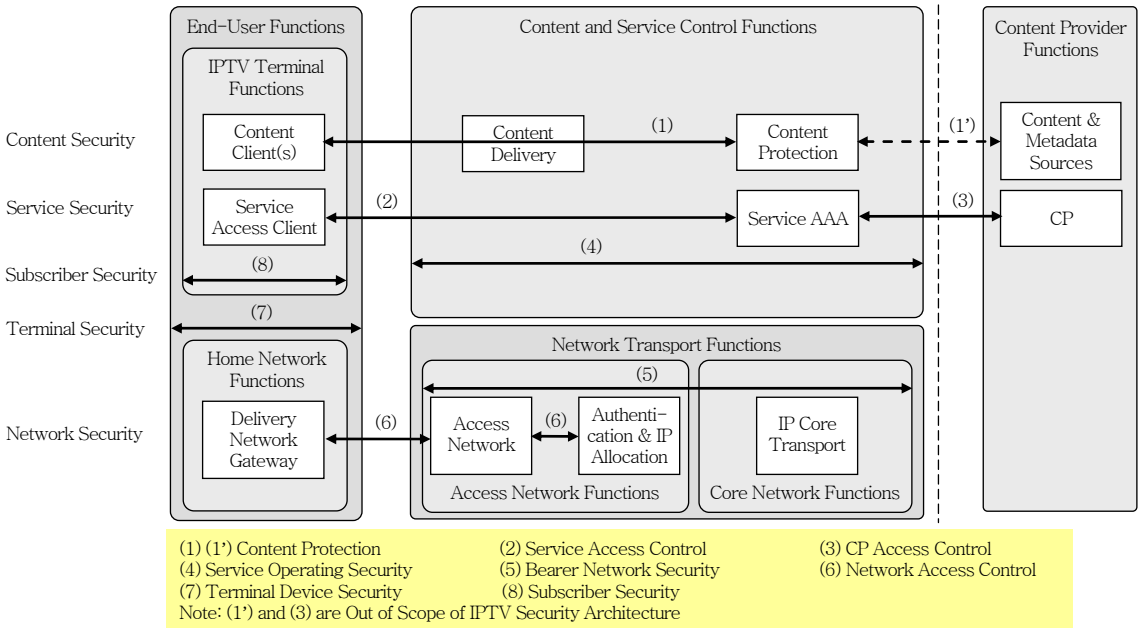
WG3의 보안 측면의 요구사항은 정리하여 WG1의 FG IPTV-DOC-0114[6]에 반영되어 있다. WG3에서의 요구사항은 일반 요구사항(general requirements for IPTV security), 콘텐트 보안(content protection), 서비스 보안(service security), 네트워크 보안(network security), 단말 보안(terminal security), 가입자 보안(subscriber security), 보안 기능 상호호환성(security interoperability)로 구분하여 정리되어 있다. 개별적인 기술 설명은 IV장의 "IPTV Security Aspects 표준화 기술 동향"에서 자세히 다룬다.

6. 보안 구조(Security architecture)

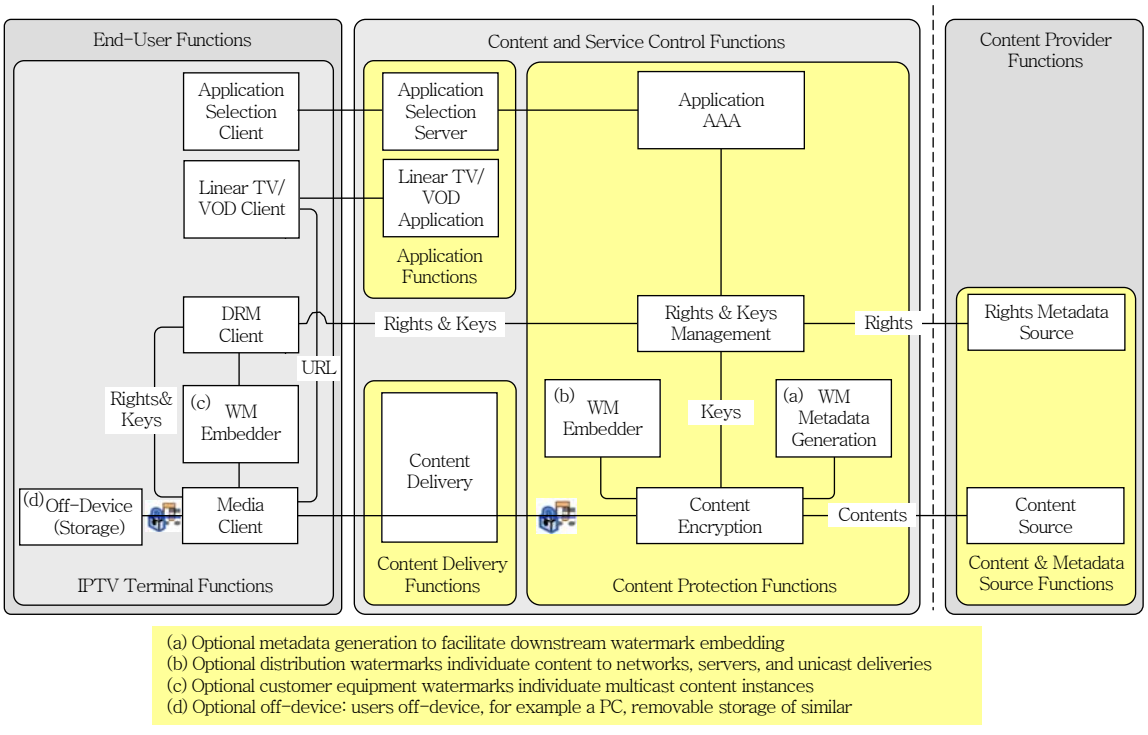
IPTV security architecture는 6차 회의에서부터 본격적으로 다루기로 되어 있으며, 현재는 전체적인 동작과 콘텐트 보안(content security) 관련이 일부 기술되어 있다. 우선 (그림 4)[7]는 콘텐트 제공자, 서비스 제공자, 네트워크 제공자, 사용자로 구분하여 전체적인 기능을 기술하고 있다. 아직 서비스 보안(service security) 측면과 암호화 과정(common scrambling)에 대한 기능이 많이 부족하다. 다음은 그림의 주요 기능에 대한 설명이다.

- 콘텐트 보안(content protection): 콘텐트 보호를 위한 기술들을 포괄하는 기능으로 콘텐트 제어, 저작권 보호, 무결성, 기밀성 등을 포함함
- 서비스 접근 제어(service access control): 불법적인 서비스 접근을 제어하는 기능으로 서비스 보안(service security)을 의미함. 특히 서비스 인증(authentication), 인가(authorization) 기능을 포함함
- 서비스 운영 보안(service operating security): IPTV 서비스를 안전하고 정확하게 사용자에게 제공하기 위한 기능을 정의하는 것으로 서비스 가용성(availibility), 안전성(reliability) 기능을 포함함
- 전송 네트워크 보안(bearer network security): IPTV 네트워크 전송의 보안 기능으로 멀티캐스트 프로토콜 보안에 관련된 기능을 포함함

스위스 제네바에서 개최된 FG IPTV 5차 회의에서는 (그림 4)의 일반적인 보안 구조(general security architecture) 외에 (그림 5)의 콘텐트 보안 구조(content protection architecture)도 승인되었



(그림 4) IPTV General Security Architecture[1]



(그림 5) IPTV Content Protection Architecture[1]

다. 콘텐트 보안 구조는 콘텐트 제공자에 의해서 행해지는 보안 서비스이지만 여기서는 콘텐트 보안이 서비스 영역에서 일부 행해지고 있기 때문에 차기 회의에서 논의가 계속될 예정이다.

7. 보안 기술(Security mechanisms)

아직 명확히 정해지지 않았으며, 진행 순서상 content security mechanisms, service security mechanisms, network security mechanisms, terminal device security mechanisms, subscriber security mechanisms에 대한 내용으로 예정되어 있다.

Ⅳ. ITU-T 표준화 기술 동향

Ⅳ장에서는 ITU-T FG IPTV 4차 회의 및 5차 회의에서 주로 제안된 기술에 대한 소개와 기술적 파급효과에 대해서 정리한다. 특히 댁내 재전송을 포함한 상호호환성 확보를 위한 기술에 대한 부분을 중점적으로 다룬다.

1. IPTV의 댁내 재분배(Re-distribution)

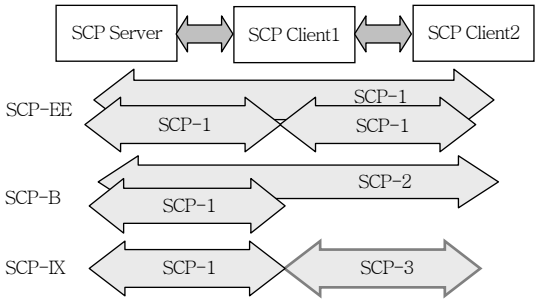
IPTV 서비스는 기존의 방송 서비스와 네트워크 서비스가 결합한 대표적인 기술이다. 기존의 방송이 댁내 단말기에서 최종 실시간 소비되던 것이 개인이 가지고 있는 휴대 단말이나 PVR 장치에 저장하고자 하는 요구사항이 나타나게 되었다.

이와 같은 요구사항은 5차 회의에서 새롭게 대두되었다. 보안 시스템이 적용된 방송 단말에서 방송 콘텐트를 재분배한다는 것은 단말 뒤에 있는 장치가 동일한 보안 시스템을 가지고 있거나 방송 단말에서 다른 단말에서 사용 가능한 형태로 변환해야 한다.

가. 댁내 재분배

방송 콘텐트의 댁내 재분배는 (그림 6)과 같이 3가지의 시나리오에 따라 정리할 수 있다[8]. 방송 서비스 보안 기능과 콘텐트 보호 기술을 통칭하여 SCP라 하고 이들 사이의 변환 과정을 보여준다.

우선 SCP-EE는 SCP Client1과 SCP Client2가 같은 콘텐트 보호 혹은 서비스 보호 기술을 사용하는 경우이다. 콘텐트를 재전송하는 경우에도 별도의



(그림 6) 댁내 재분배에 따른 보안 기능의 변환[1]

가공 없이 수신한 상태 그대로 재분배하는 방식이다. 가장 심플한 방법이지만, 댁내 단말이 전부 동일 보호 기술을 사용해야 하는 제약이 있다.

다음으로 SCP-B 방식은 SCP 서버가 두 단말의 보안 서비스를 동시에 지원하는 방식이다. 즉, SCP 서버는 SCP Client1을 위한 SCP-1 방식으로 보안 서비스를 제공하고, 더불어 SCP Client2를 위해 SCP-2 방식의 보안 서비스도 지원하는 방식이다. 이 방식은 SCP 서버가 모든 서비스 단말을 제어할 수 있는 장점이 있지만, 네트워크 및 전체 IPTV 시스템에 추가적인 부하가 걸리게 된다.

마지막으로 SCP-IX 방식은 SCP 서버가 채용한 보안 서비스는 최소 방송을 수신하는 단말에서만 적용이 되면, 수신 단말은 이를 변환하여 다른 장치에게 전송하는 방식이다. SCP 서버가 직접 댁내의 단말들을 관장하지 않기 때문에 다양한 서비스 보안 기술의 적용이 가능하다. 반면 방송 단말에서 이를 실시간 처리하기 위해서는 방송 단말에 대한 추가적인 성능을 요구하게 된다.

나. 기술적 파급 효과

방송 콘텐트를 댁내로 재분배하는 문제는 홈 네트워크에서 방송 콘텐트를 어떻게 보호할 것인가 하는 부분과 보안 기술들 사이의 상호호환성을 어떻게 보장할 것인가 하는 문제로 귀결된다. 특히 이 두 가지는 산업적으로 미치는 영향이 크기 때문에 단순한 문제가 아니다.

홈 네트워크는 자체적으로 콘텐트를 생성하지 못하기 때문에 대부분의 콘텐트가 외부에서 유입된다.

이중에서 대표적인 콘텐트 공급원은 방송이다. 하지만 지금까지 지상파, 케이블, 위성 방송 콘텐트를 수신하기 위해서는 별도의 단말 장치가 필요했다. 반면 IPTV는 수신기 자체가 디지털 처리를 기반으로 하고 있어 DLNA[9]와 같이 댁내에서 영상 콘텐트를 저장 및 유통하는 것이 쉽다. 무료 콘텐트의 경우는 별 상관이 없지만, 유료 콘텐트의 경우는 상황이 다르다. 사용자는 자신이 수신한 콘텐트를 저장하고 언제든지 원하는 기기에서 보고 싶지만, 콘텐트 사업자의 입장에서는 불법 콘텐트 유통으로 확산될 것을 우려한다. 따라서 댁내에 유입된 유료 콘텐트에 대한 합법적인 유통을 위해서는 홈 네트워크의 보안 서비스에 대한 연구가 필요하다.

홈 네트워크 보안 서비스는 하나의 서비스가 존재하지 않는다. 홈 네트워크에서 지원하는 보안 서비스 혹은 프로토콜을 개발하더라도 휴대 단말이나 가전 기기가 이를 지원하지 않는다면 사용이 어렵다. 특히 기존의 휴대 단말이나 가전 기기들은 저작권 보호 기술을 별도로 채택하여 사용하고 있기 때문에 이들과의 호환성을 보장하기 위한 기술이 필요하다. 이동 단말을 위한 표준 단체인 OMA[10]가 정의한 DRM 기술이 등장했지만, 모든 기기가 이를 채택하고 있는 것이 아니며 홈 네트워크 기기가 아닌 이동 단말을 대상으로 하고 있어 이를 포괄하는 표준화 기술이 필요하다.

현재 홈 네트워크 보안 기술은 DVB IPI의 CPCM [11]이 대표적인 기술이며, DLNA[9]나 ISMA[12]에서도 많은 관심을 가지고 있는 분야이다. 또한 방송 콘텐트의 상호호환성을 위해서는 ATIS[13] IIF의 server side interoperability가 주도적인 역할을 하고 있다.

2. 다중 서비스 보안(Multiple service securities)

서비스 보안(service security)은 콘텐트 보안(content security)과 달리 서비스 사업자에 의해서 제공되는 보안 서비스로 콘텐트의 유통이나 콘텐트의 제한이 아닌 특정 채널에 대한 수신을 제한하는 기술이다. 따라서 사업자에 종속적인 성격이 강했다. 하지만 특정 사업자가 특정 서비스 보안 모델을 채용함으로써 방송 수신 단말기들은 호환성을 확보하는 것이 불가능해졌다.

무료 방송 채널을 제공하는 지상파나 일부 케이블 방송의 경우는 상관이 없지만, 유료 채널의 케이블 방송이나 위성 방송을 수신하는 단말기는 어려움이 크다. 이는 다른 서비스 기술과 달리 보안 서비스 기술이 자세한 기술을 공개하지 않는 구조 때문이기도 하다.

가. 구성

특정 서비스 보안 모델이 전체 시스템을 독점하는 문제를 해결하기 위해서 DVB[14]는 암호화 구조를 통일(common scrambling algorithm)하고 이를 제어하는 메시지를 사업자별로 제공하는 Simul-Crypt 기술을 개발하였다. SimulCrypt는 하나의 암호화된 방송 콘텐트를 여러 사업자가 각기 운영하게 하는 기술이지만, 방송 단말기는 여전히 사업자에 종속적인 특징을 가진다.

반면 케이블 사업자들이 중심이 된 OpenCable 측은 수신 제한 기술의 일부 코드를 다운로드 할 수 있는 DCAS[15] 기술을 개발하였다. 이를 통해 OpenCable 측이 제공하는 SM을 장착한 단말기는 어디서나 필요한 수신 제한 코드를 다운로드 받아 수행할 수 있는 구조를 지원한다.

현재 ITU-T FG IPTV 요구사항에는 이와 관련하여 다중 서비스 보안 모델[16]을 적용하기 위한 내용이 반영되어 있으며, 방송 수신 제한을 위한 코드를 다운로드 하고 검증하는 기술이 포함되어 있다.

나. 기술적 파급 효과

다중 서비스 보안 기술의 적용은 다수의 서비스 보안 모델이 하나의 단말에서 운영 가능하게 하는 기술로 공통 부분에 대한 표준화가 가능하다. 물론 향후의 표준화 진행 방향에 따라서 표준화 수준이 결정되겠지만, 일정 수준의 하드웨어 표준화는 이루

어질 것으로 보인다. 산업적으로 하드웨어 개발 기술과 소프트웨어 개발 기술을 분리하면 각각의 기술이 개별적으로 발전할 수 있기 때문에 빠른 성장이 가능해진다. 특히 각 기능 모듈이 세분화되고 표준 하드웨어를 활용한 새로운 보안 기술의 개발도 가능해진다.

공통 하드웨어가 표준화되고 소프트웨어를 다운로드 받아 실행할 수 있다면 IPTV 단말기는 일반 소매 시장에 판매하는 것이 가능하다. 물론 사업자 기반의 저가 단말기 시장도 형성되지만, 다양한 부가 서비스를 제공하는 고급 IPTV 단말기는 소매 시장에서 판매가 될 것이다. 특히 홈 네트워크의 다양한 서비스와 댁내 콘텐트 분배와 같은 서비스 연계형 제품의 개발이 활발해질 것이다.

3. 보안 서비스 변환(Service security to content security transfer issues)

보안 서비스 변환 문제는 앞의 댁내 콘텐트 재분배 문제와 연결된 것으로 댁내 재분배를 가정하고 있다. 방송 콘텐트가 댁내 재분배되는 경우에 그대로 재분배하면 댁내의 다른 단말기는 IPTV 단말기와 같은 수준의 보안 기능을 가지고 있어야 한다. 동일한 방송 수신 단말기라면 큰 문제가 되지 않지만 이동 단말(PDA, PMP, MP3P, 노트북 등등) 혹은 가전 제품(DVDP, DTV)은 문제가 된다. 보안 서비스가 제공되는 콘텐트는 동일한 보안 코드가 각각의 단말에 내장되어 있어야 하기 때문이다.

DTV와 같이 보안 기능이 전혀 없는 단말기는 방송 수신에서 제외하겠지만 PMP와 같은 단말은 자체적으로 DRM 기술이 적용되어 있다. 이 경우 모든 휴대 단말이 방송용 수신 제한 기술을 적용하는 것이 큰 부담이다. 따라서 서비스 보안 기술을 콘텐트 보안 기술, 즉 DRM 기술로 변환하는 기술이 필요하다.

가. 서비스 보안과 콘텐트 보안 기술

서비스 보안 기술과 콘텐트 보안 기술의 가장 큰 차이점은 암호화 적용 방법에 있다. 서비스 보안 기술은 전통적으로 scrambling 기법을 사용했다. 즉 화면의 주사선 일부를 반전시키는 방법을 말한다. 지금도 일부 아날로그 방송에서 사용하고 있는 방법이다. Scrambling 기술은 디지털 방송으로 전환되면서 암호화 기술을 이용한다. 또한 방송 콘텐트는 실시간 서비스로 프로그램 단위보다는 시간 축을 기준으로 서비스가 이루어진다. 따라서 방송 콘텐트의 암호화에 사용되는 키는 일정 시간을 기준으로 자동 갱신된다. 반면 저작권 보호 기술은 시간 축이 아닌 프로그램 단위의 보호 기술을 적용한다. 즉 하나의 방송 프로그램에 대해서는 동일한 키를 적용하고 이와 관련된 프로파일을 생성하는 것이다.

이 두 기술을 연동하기 위해서는 세 가지 접근 방법이 있다.

- 다중 키를 사용하는 방법: 다중 키를 사용하는 방식으로 저작권 보호 기술에서 다수의 키를 지원하는 방식이다. 즉 방송 수신 제한 기술은 자신이 사용한 키들의 정보를 제공하면 저작권 보호 기술은 이를 기반으로 DRM 프로파일을 생성하고 제공하는 방식이다. 이를 효율적으로 제공하기 위해서는 방송 수신 제한 기술에서 일정한 키의 연관 관계를 포함하면 효율적인 제공이 가능하다.
- 단일 키를 사용하는 방법: 단일 키를 사용하는 방송 수신 제한 기술이 하나의 키를 사용하는 방식이다. 즉 방송 수신 제한 기술에서 시간 단위의 키 갱신이 아닌 프로그램 단위의 키 갱신을 사용하는 것이다. 키의 갱신 주기가 길어지기 때문에 보안 상의 취약점이 증가할 수 있다.
- 다중 키를 단일 키로 변환하는 방법: 다중 키를 사용하는 수신 제한 기술과 단일 키를 사용하는 저작권 보호 기술이 서로 연동하는 방식이다. 방송을 수신하고 재생하는 시점까지는 방송 수신 제한 기술이 담당하고 이를 다시 재분배하기 위해서는 다시 암호화하는 과정을 거치는 방식이다. 암호화 과정은 저작권 보호 기술에 의해서 이루어지며, 이 정보는 서비스 제공자 혹은 콘텐

트 제공자에 의해서 생성된다. 하지만 복호화 후 다시 암호화하는 과정이 있기 때문에 시스템에 추가적인 기능을 요구하는 단점이 있다. 단 여기서 복호화는 IPTV 단말기에서 방송을 재생하기 위해서 반드시 들어가는 기능으로 추가 기능이 암호화 한 번이 된다.

현재 ITU-T FG IPTV에서는 3번째의 "다중 키를 단일 키로 변환하는 방법[16],[17]"에 대한 요구사항이 반영되어 있다.

나. 기술적 파급 효과

보안 서비스 변환 기술은 현존하는 다른 기술과의 인터페이스를 정의하는 것으로 산업적 영향력이 크다. 즉 보안 서비스 변환 기술이 표준화된다면 많은 업체들이 이를 이용한 댁내 콘텐트 분배 및 연계된 응용 서비스 개발이 가능해진다.

4. 상호호환성(Interoperability for service/content securities)

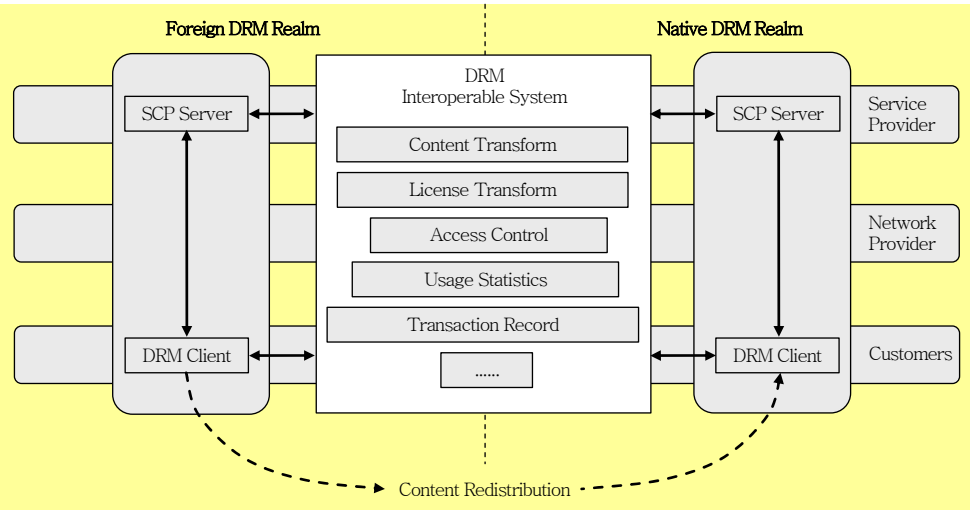
5차 ITU-T FG 회의에서 WG3의 논쟁이 가장 많이 되었던 부분은 댁내 콘텐트 재분배와 이에 따른 상호호환성 문제였다. 상호호환성은 크게 앞에서 언급한 내용들을 모두 포함하지만, 여기서는 상호호환성에 대한 예시 및 시나리오 위주로 설명한다.

먼저 콘텐트 보호 기술은 서비스 보호 기술과 달리 다수의 콘텐트 제공자가 존재한다. 더불어 저작권 보호 기술은 상호호환성 확보를 위한 많은 기술들이 개발되어 있다. ITU-T FG 회의에서도 저작권 보호 기술간의 상호호환성 확보를 위한 기술들이 제안되었다. (그림 7)은 기고서[18]에서 제안하고 있는 DRM 상호호환성 구조이다.

이 구조는 서로 다른 DRM 서버들이 상호 연동하는 모듈과 DRM client들 사이의 콘텐트 재분배 과정을 포함하고 있다. 특히 content transform, license transform 등을 포함하고 있어 상호호환성을 위해서 서로가 모든 정보를 공유하는 형태를 가지고 있다.

그림상으로는 보이지 않지만, 이 기고서는 OMA DRM v2.0을 기반으로 하고 있다. 즉 OMAv2 Marlin Gateway[19]에서 정의하고 있는 내용을 기반으로 하고 있다. 최근 ITU-T FG 회의에서 OMA 기반의 기고서가 늘고 있는 것을 잘 보여주고 있다.

현재 ITU-T 회의에서는 중국, 일본, 한국이 모두 상호호환성의 필요성을 주장하고 있어 충돌이 없지만, 향후 구체적인 구조에서는 각 나라별로 상이



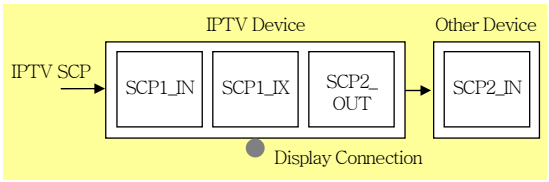
(그림 7) 저작권 보호 기술 상호호환 기술[18]

한 구조를 가져올 것으로 보인다. 특히 중국은 OMA DRM 2.0을 기반으로 하고 있으며 한국은 자체 개발한 기술을 제안하고 있어 6차 회의의 결과가 주목되는 부분이다.

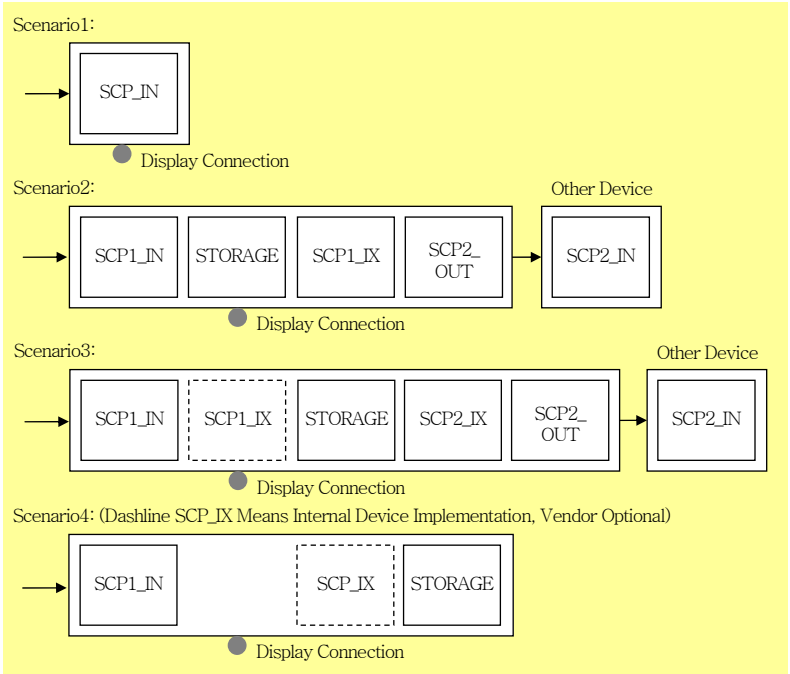
또한 ITU-T FG 5차 회의에서는 댁내 재분배 및 저장 장치를 포함하여 상호호환성 문제를 첨부에서 정의하고 있다. (그림 8)은 보안 모델을 위한 기본적인 서비스 시나리오를 보여주고 있다. 즉 실시간 방송인 IPTV SCP를 방송 단말기가 수신하고 이를 SCP1에서 복호화하여 방송을 보여주고, 이를 다시 SCP2로 변환하여 댁내의 다른 단말에 전송하는 구조이다. 이 (그림 8)을 바탕으로 댁내 저장 장치를 가정하여 확장한 그림은 (그림 9)와 같다.

(그림 9)에서 시나리오1은 외부 연결장치 없이 단순 콘텐트를 소비하는 경우를 보여주며, 시나리오2는 SCP1에 의해서 방송을 재생하면서 저장하고, 그 다음에 SCP2로 변환하여 전송하는 시나리오를 보여 준다. 이는 저장 시점과 변환 시점이 다른 경우를 보여주고 있다. 시나리오3은 방송 콘텐트의 저장과 수신을 분리하여 수신→저장→변환 과정을 보여주고 있다. 저장 앞부분의 SCP1_IX는 SCP1에서 변환이 필요한 경우 옵션으로 변환하는 과정을 포함한다. 그림에서 점선이 옵션으로 행해지는 부분이다. 마지막으로 시나리오4는 변환하지만 외부 장치에 전송하지 않는다. 저장 장치에 저장하기 전에 변환 과정을 거치는 방식이다. 크게 저장 장치를 기준으로 먼저 변환하는 방식과 저장 후 변환하는 방식을 표현하고 있다.

본 그림은 WG3 내부에서 작성하였지만 ITU-T FG 전체 회의에서 승인 받지 못한 것으로 다음 회의에서 논의 후 승인되면 정식으로 문서에 등록될 예정이다. 더불어 본 시나리오가 받아들여진다면, 저장 장치 관련 기능인 PVR, time-shift, place-shift 보안[17]이 활발히 논의될 것으로 예상된다.



(그림 8) SCP 서비스 시나리오[1]



(그림 9) SCP 상호호환 구조(저장 장치)[1]

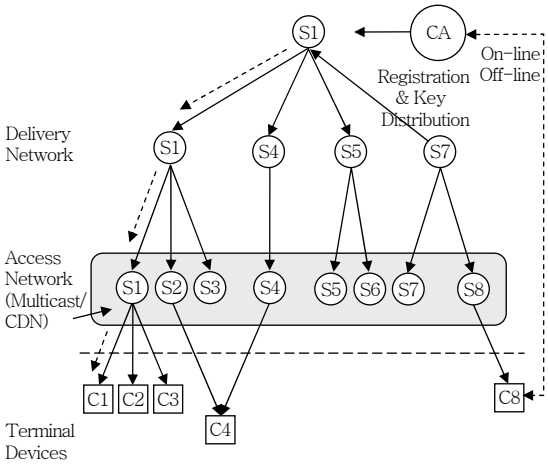
5. 멀티캐스트 보안(Multicasting security: group key management)

멀티캐스트 보안은 중국에서 기고한 기고서[20]로 네트워크 수준의 보안 기능을 포함하고 있다. ITU-T FG IPTV에서는 전체 기능이 문서에 포함되지는 않았지만, 중국 측에서 계속적으로 관련 기고서를 제출하고 있는 실정이다.

우선 멀티캐스트 보안은 기존의 멀티캐스트 프로토콜에 그룹 키 관리 기술을 적용하는 것이다. 그룹 키 관리 기술은 특정 그룹에 소속되어 있는 사용자들이 동일한 키를 사용하도록 하는 그룹 기반의 키 관리 기술이다. 본 기술은 전자 투표 및 그룹 서명과 같은 응용 서비스를 위해서 개발되었지만, 멀티캐스트와 결합한 secure multicast 기술로 발전하였다.

(그림 10)은 그룹 키 관리 기술에 대한 개략적인 그림을 보여주고 있다. 그룹 키는 그룹을 기반으로 하는 서비스이기 때문에 그룹에 대한 가입과 탈퇴를 기반으로 하고 있다. 새로운 그룹에 가입하는 경우 가입자는 서브 그룹에게 요청을 하고 서브 그룹이 가입되어 있다면 승인하고 키를 분배하고 그렇지 않다면 상위 그룹에 본인을 가입하는 절차를 수행한다. 이는 멀티캐스트의 가입과 동일한 구조이다. 하지만 탈퇴의 경우는 전체 그룹의 키를 새로 만들고 분배해야 하기 때문에 멀티캐스트 프로토콜과 다르다.

이와 같이 그룹 키를 이용하는 것은 멀티캐스트



(그림 10) 그룹 키 관리 기술

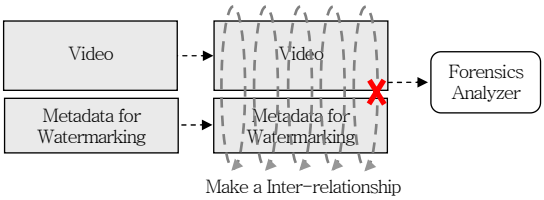
수준에서 안전한 키 분배를 가능하게 하지만, 멀티캐스트 프로토콜 장비를 모두 교체해야 하는 문제점이 있다. 또한 콘텐트 보안, 서비스 보안, 멀티캐스트 보안이 교차되는 특징이 있을 수 있다.

현재 ITU-T FG IPTV에서는 멀티캐스트가 그룹 키를 지원하는 경우에 한해서 지원하는 요구사항이 포함되어 있으며, 더 이상의 표준화 진행은 어려울 것으로 보이지만 다음 회의에서 중국이 어떤 기고서를 가지고 올지 귀추가 주목되는 기술이다.

6. 워터마크(Forensics watermarking)

지난 4차 회의에서 Cinea Inc.에서 제안한 기고서[21]에는 불법적인 콘텐트의 유통을 추적하고 사후 검증할 수 있는 기술에 대한 제안이 있었다. Forensic watermarking이라는 이름을 붙이고 있다. 이 기술을 적용할 수 있는 요구사항을 제출하였고 WG3 문서에 반영되었다. 또 5차 회의에서는 이를 지원하기 위한 메타 데이터를 정의하고 관련 기능을 상세화하는 단계에 접어들었다.

(그림 11)은 Cinea Inc.에서 제안하고 있는 내용을 기반으로 구조를 그린 것이다. 비디오의 저작권이 아닌 사후 검증을 위한 기술 적용을 목적으로 하고 있다. 하지만 5차 회의 이후 제안하고 있는 내용을 보면 DRM 기술과 유사한 기능을 가지고 있다. 향후 DRM과 어떤 차별화를 가지는지 혹은 기능상 융합을 어떻게 할지에 따라 주의가 요구되는 부분이다.



(그림 11) Forensic Watermarking

V. 결론

본 고는 4차 및 5차 ITU-T FG IPTV 회의에서

중점 논의되고 있는 기고서를 중심으로 표준화 문서의 내용을 정리 요약하였다. 더불어 중점 기술인 상호호환성 모델 및 그룹 키 기반의 멀티캐스트 기술에 대한 분석을 포함하여 관련 기술의 기고서를 준비하고 있는 기관에게 도움이 되고자 한다. IPTV 보안 서비스는 콘텐트 보안, 서비스 보안, 네트워크 보안으로 크게 분류가 되며, 이들 하나 하나가 IPTV 보안 모델로 가능하기 때문에 이들의 연동 방식 혹은 주도권 다툼에 대한 연구가 필요하다. 특히 pure IP 기반의 IPTV 서비스에 대한 논의에 따라서 기술의 발전 방향이 달라질 것으로 보이기 때문에 이에 대한 지속적인 관심과 연구가 필요하다. 마지막으로 10월 일본에서 개최 예정인 6차 회의에서는 보안 서비스 구조에 대한 적극적인 논의가 진행될 예정이다.

● 용 어 해 설 ●

피싱(Phishing): 개인정보(private data)와 낚시(fishing)의 합성어로 개인정보를 낚는다는 의미로 사용자에게 신뢰할 수 있는 사람 또는 기업을 사칭하여 사용자의 개인 정보를 얻는 것으로 사회적 공격(social engineering)의 한 형태임

CDN: Content Delivery Networks의 약자로 사용이 빈번한 대용량의 콘텐트를 네트워크의 중간 노드에 저장한 후 병목 구간을 피해 빠르게 전달하는 서비스

약 어 정 리

AAA	Authentication, Authorization and Accounting
ATIS	Alliance for Telecommunications Industry Solutions
CAS	Conditional Access System
CDN	Content Delivery Network
DCAS	Download Conditional Access System
DLNA	Digital Living Network Alliance
DoS	Denial of Service Attack
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
IPTV	Internet Protocol Television
ISMA	Internet Streaming Media Alliance
ITU-R	International Telecommunication Union-Radiocommunication Sector
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
NGN	Next Generation Network
OMA	Open Mobile Alliance
PVR	Personal Video Recoder
QoS	Quality of Service
SCP	Service and Content Protection
SM	Secure Microprocessor
TSB	Telecommunication Standardization Bureau
VoD	Video on Demand
WG	Working Group

참 고 문 헌

[1] ITU-T FG WG3, Working Document: IPTV Security Aspects, FG IPTV-DOC-0122, Geneva: ITU-T FG IPTV, 07 22, 2007.

[2] ITU-TSB, Overview of ITU-T, Geneva: ITU-TSB, 2007.

[3] ITU-T FG WG3, Working Document: IPTV Security Aspects, FG IPTV-DOC-0090Rev.1, Geneva: IUT-T FG IPTV, 07 22, 2007.

[4] ITU-T, Security Architecture for Open Systems Interconnection for ccitt Applications, Recommendation X.800, 1991.

[5] ITU-T, Security Architecture for Systems Providing End-to-end Communications, Recommendation X.805, 2003.

[6] WG1, Working Document: IPTV Service Requirement, FG IPTV-DOC-0114, Geneva: ITU-T FG IPTV, 2007.

[7] CATR/MII, China, Proposed Modifications to Figure 9-1 of FG IPTV-DOC-0090, FG IPTV-C-0657, Geneva: ITU-T FG IPTV, 2007.

[8] NTT Corporation, Proposed Elaboration on FG IPTV-DOC-0090, "X.805 Network Security," - 7 Security Threats, FG IPTV-C-0670, Geneva: ITU-T FG IPTV, 2007.

[9] DLNA, "Digital Living Network Alliance," http://www.dlan.org

[10] OMA, "Open Mobile Alliance," http://www.openmobilealliance.org

[11] DVB, DVB Content Protection & Copy Management. s.l.: DVB, DVB Document A094, 2005.

[12] ISMA, "Internet Streaming Media Alliance," http://www.isma.tv
[13] ATIS, "Alliance for Telecommunications Industry Solutions," http://www.atis.org
[14] DVB, "Digital Video Broadcasting," http://www.dvb.org
[15] OpenCable, "DCAS," http://www.opencable.com/dcas
[16] ETRI, Republic of Korea, Requirements to Support Multiple Service Securities, FG IPTV-C-0743, Geneva: ITU-T FG IPTV, 07 22, 2007.
[17] Korea(Republic of), Proposed Requirements for Interoperability Amongst Multiple IPTV Security Technologies, FG IPTV-C-0810, Geneva: ITU-T FG IPTV, 07 22, 2007.
[18] Huawei Technologies Co., Ltd. A Common DRM Interoperable Architecture, "FG IPTV-C-0793," Geneva: ITU-T FG WG3, 2007.
[19] OMA, Marlin-OMAv2 Gateway Specification, Version 1.1 Final, "Marlin Engineering Workgroup," Sep. 2006.
[20] Huawei Technologies Co., Ltd. Alternative Key Management Algorithm and Effective Group Policy Distribution, FG IPTV-C-0490, Geneva: ITU-T FG IPTV, 05 07, 2007.
[21] Cinea Inc., Proposed Requirements for Forensic Watermarking(a.k.a. Media Serialization), FG IPTV-C-0591, Geneva: ITU-T FG IPTV, 05 07, 2007.