IPTV를 위한 콘텐츠보호 기술

이 선 영*

◈ 목 차 ◈

1. 서 론

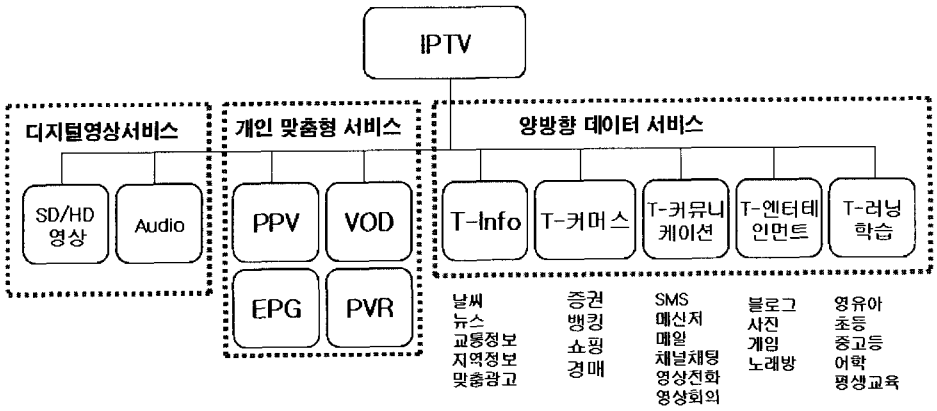
IPTV(Internet Protocol TV)란 IP망을 통해 방송이나 정보 등을 TV로 제공하는 통신과 방송이 융합된 서비스를 말한다. IPTV 서비스는 디지털 영상서비스, 양방향 데이터 서비스 및 다양한 개인 맞춤형 서비스를 제공하는 서비스로서, 기존 방송 콘텐츠와 인터넷의 풍부한 콘텐츠를 TV에 맞게 재구성할 수 있다. 현재 공중파 방송은 방송된 콘텐츠의 재사용에 제약을 두지 않고 있으며, 케이블 방송도 방송 가입자에게 안전하게 콘텐츠를 전송하기 위한 방법은 사용하고 있으나 방송된 후의 콘텐츠의 사용은 개인에게 모두 맡기고 있는 상황이다. 그러나, 디지털화된 콘텐츠는 누구나 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있고, 복제품은 원본과 질적으로 동일하며 확산 속도가 빠른 특성을 가지고 있다. 따라서, 디지털 콘텐츠에 대한 불법복제, 저작권 침해, 기밀 누출이 상대적으로 용이한 실정이다. 다양한 디지털 콘텐츠를 사용하는 IPTV에서는 방송과 인터넷이 융합함으로서 오히려 저작권 침해 문제가 더욱 심각해 질 수 있으므로 저작권 보호 및 콘텐츠의 불법 복제/배포를 방지하기 위한 기술이 필요하다. 콘텐츠 보호를 위해 현재 케이블 방송에서는 콘텐츠를 가입자에게만 전송하기 위한 방법으로 수신제한방법(CAS)를 도입하여 이용하고 있고, 컴퓨터를 기반으로 한 인터넷 상에서는 디지털 콘텐츠에 대한 저작권 보호 기술로서 다양한 DRM(Digital Right Management) 기술들을 사용하고 있다. DRM은 디지털 콘텐츠의 생산, 분배, 거래규칙, 과금, 거래내역의 관리, 정산 등 디지털 콘텐츠의 전체 라이프 사이클에 걸쳐 투명성과 신뢰성을 보장하는 유통 체계 전반을 통칭하는 서비스를 말한다. 이에 비해 CAS는 인가된 사용자가 암호화된 콘텐츠를 복호하여 원본 콘텐츠를 획득한 후의 사용에 대해서는 관여하지 않으므로 사용자가 획득한 콘텐츠를 불법 복제 및 불법 유통할 경우에는 콘텐츠에 대한 지속적인 보호가 이루어지지 않는다. 따라서, 통신과 방송의 특성을 함께 가지는 IPTV에서는 CAS만으로 콘텐츠를 보호할 수 없고 DRM을 병용하여야 한다. 본 논문에서는 CAS와 DRM 기술을 표준화된 기술을 중심으로 살펴보기로 한다.

본 논문은 제2장 IPTV의 개념, 제3장 DRM의 개요, 제4장 수신제한시스템, 제5장 방송 표준을 위한 DRM 및 복제방지 기술, 제6장 결론으로 구성된다.

2. IPTV의 개념

IPTV는 IP 방식의 인터넷 망을 통해 방송 콘텐츠가 제공되는 서비스로서 통신의 속성과 방송 프로그램의 전송과 다수 가입자라는 방송의 속성을 모두 갖고 있는, 통신과 방송이 융합된 서비스라 할 수 있다.

* 순천향대학교 정보보호학과 조교수



〔그림1〕 IPTV 서비스

즉, IPTV는 인터넷 프로토콜을 이용한 패킷 방식으로 멀티미디어 콘텐츠를 제공하고, PC가 아닌 TV 단말기를 통하여 다양한 서비스를 제공한다[1]. [그림 1]은 IPTV가 통신기능과 방송기능이 통합된 서비스 개념이라는 점과 VoD, EPG, T-커머스 등과 같은 양방향 콘텐츠를 제공하는 통신과 방송기능이 모두 녹아있는 융합 서비스임을 나타내고 있다[2].

[그림 1]에서 알 수 있듯이 IPTV를 통하여 이용자가 획득할 수 있는 콘텐츠의 종류는 매우 다양하며, 홈네트워크가 발달함에 따라 IPTV를 통하여 얻어진 콘텐츠는 PC, PMP, 모바일 기기 등 이용자가 사용하고 있는 다양한 기기에서 재사용될 수 있다. IPTV를 이용하면 현재 PC를 통하여 얻을 수 있는 것보다도 다양한 콘텐츠를 획득할 수 있고, 더 많은 기기 및 사용자에게 재사용, 복제, 배포할 수 있게 된다. 이 점 때문에 IPTV에서는 콘텐츠에 대한 제어를 위하여 기존의 방송에서 사용하고 있는 기술뿐 아니라, 통신에서 사용되는 콘텐츠 보호 기술을 병용할 필요가 있다.

3. DRM의 개요

DRM이란 디지털 콘텐츠의 생산, 분배, 거래규칙, 과금, 거래내역의 관리, 정산 등 디지털 콘텐츠의 전체 라이프 사이클에 걸쳐 투명성과 신뢰성을 보장하는 유통 체계 전반을 통칭하는 서비스를 말한다. 이러한 서비스를 위하여 DRM 시스템은 DRM을 적용한 콘텐츠를 만들고 공급하는 DRM 패키저와 라이센스를 발급하고 관리하는 클리어링 하우스, 라이센스에 따라 사용을 통제하는 DRM 클라이언트로 구성된다.

DRM 기술은 접근제어(Access Control) 방식, 사용제어(Use Control) 방식, 복제방지(Copy Protection) 방식으로 구분할 수 있다[3,4]. 접근제어 방식은 사용자 또는 장치가 특정 디지털 콘텐츠에 대해 접근 권한이 있을 때에만 해당 콘텐츠의 사용을 인가하는 기술로서 방송 콘텐츠의 유료 채널을 보호하는데 사용되는 CAS(Conditional Access System : 수신제한시스템)가 있다. 그러나 이 방식은 정당한 사용자의 부정한 행위에 대해서는 콘텐츠를 보호할 수 없다. 사용제어 방식은 사용 권한이 있는 사용자라 하더라도 부여된 권한에 따라 디지털 콘텐츠의 사용 권한을 지속적으로 통제하는 방식이다. 이 방식은 콘텐츠의 생명 주기 전체에 걸쳐 원본 추출이 보장되기 때문에 현재 많은 디지털 콘텐츠들이 이 기술을 이용하고 있다.

복제방지 방식은 저장 매체 또는 장치에 유일하게 부여된 정보를 키로 사용하여 디지털 콘텐츠를 암호화함으로써 다른 매체나 장치로 복제되더라도 의미없는 데이터가 되게 하는 기술이다. 복제방지 기술은 단독으로 사용되기도 하지만 CAS 또는 DRM 기술과 연동하여 최종 사용자가 디지털 콘텐츠의 장점인 복제를 할 수 없게 한다. 복제방지 기술의 대표적인 예로는 4C의 CPPM/CPRM[5], 5C의 DTCP[6], Intel의 HDCP[7] 등이 있다.

〔표 1〕 DRM 관련 국제 표준단체 현황

기술분야	표준단체	기술내용	현재 상태
DRM	MPEG-21	범용적으로 사용될 수 있는 DRM 프레임워크의 표준 기술 개발	진행
	OMA	모바일 환경에서 사용될 수 있는 DRM 기술 사양 개발	진행
	CORAL	디지털 콘텐츠의 상호호환성을 보장하는 DRM 기술 개발	진행
	CRF	DRM의 상호호환성을 위한 표준	진행
	ISMA	MPEG-4 기반의 DRM 기술 개발	진행
	DLNA	디지털 홈 환경에서 사용될 수 있는 DRM 기술 사양 개발	보류
	DMP	DRM의 정책 및 기술 사양 정립을 위한 프로젝트 형태의 포럼	진행
	TCG	하드웨어 및 OS의 보안성 강화를 위한 기술 사양 개발	진행
	DVB CPCM	유럽의 방송 표준에서 사용될 수 있는 DRM의 기술 사양 개발	진행
	TV Anytime	PVR에서의 디지털 콘텐츠 보호를 위한 DRM 기술 사양 개발	진행
	SDMI	온라인 음악 콘텐츠의 지적재산권 보호 기술 개발	중단
	OeBF	e-Book에서 사용될 수 있는 DRM 표준 개발	침체
REL	XrML	XML 기반의 권리표현기술 사양	완료
	ODRL	XML 기반의 권리표현기술 사양	완료
Metadata	IMPRIMATUR	디지털 콘텐츠 유통의 비즈니스 프레임워크 연구 프로젝트	완료
	Indecs	디지털 콘텐츠 유통에서 사용되는 메타데이터 표준 개발	완료
Copy Protection	CPTWG	DVD, 디지털방송 콘텐츠의 복제방지기술 표준화 포럼	진행
	4C CPPM/ CPRM	광디스크의 복제방지기술 표준	완료
	5C DTCP	디바이스간에 전송되는 디지털 콘텐츠의 복제방지기술	완료
	HDCP	디바이스간에 전송되는 디지털 콘텐츠의 복제방지기술	완료
	SmartRight	디지털 홈 환경에서의 디지털 콘텐츠 복제방지 기술	진행
	SVP	디지털 홈 환경에서의 디지털 콘텐츠 복제방지 기술	진행
	DVD CCA	DVD의 복제방지 기술	완료
	AACP	HD DVD의 복제방지 기술	진행
CAS	DVB CA	디지털 방송 콘텐츠의 보호를 위한 수신권한제어(CA) 기술	완료
	OpenCable CPT	케이블 방송의 복제방지기술 표준	완료
	ATSC CAS	지상파 디지털방송 콘텐츠의 수신권한제어(CA) 기술	완료

DRM의 표준을 만들기 위해 SDMI, AAP, OeBF, DVD Forum, IRTF의 IDRM, MPEG- 21등 다양한 표준화 단체들이 각자 독자적인 DRM 표준 기술을 준비해 왔다. 표 1은 국제적인 DRM 표준화를 진행하고 있는 단체들의 현황을 보여주고 있다.

여러 표준화 단체들 중에서 DRM 표준 기술의 개발을 위해 OMA, MPEG-21, DMP, Coral, DVB CPCM 등이 현재 가장 활발한 활동을 보이고 있으며, 4C Entity, 5C등의 산업표준단체들은 매우 구체적인 기술 규격을 마련하고 있다.

4. 제한수신 시스템(CAS : Conditional Access System)

CAS는 암호화된 방송 콘텐츠를 유선이나 위성, 인터넷을 통하여 수신자에게 보내고, 시청료를 지불한 수신자에게만 암호를 복호할 수 있는 권한을 부여함으로써 유료 서비스를 가능하게 한다. 그러나, 이 방식은 정당한 사용자의 부정한 행위에 대해서는 콘텐츠를 보호할 수 없다. 즉, 인가된 사용자가 암호화된 콘텐츠를 복호하여 원본 콘텐츠를 획득한 후 이를 불법 복제 및 불법 유통할 경우에는 콘텐츠에 대한 지속적인 보호가 이루어지지 않는다. CAS의 주요 기능은 스크램블링/디스크램블링(srcambling /descrambling) 기능, 자격제어(Entitlement Control) 기능, 자격관리(Entitlement Management) 기능으로 나눌 수 있다[8].

(1) 스크램블링/디스크램블링(Scrambling /Descrambling) 기능

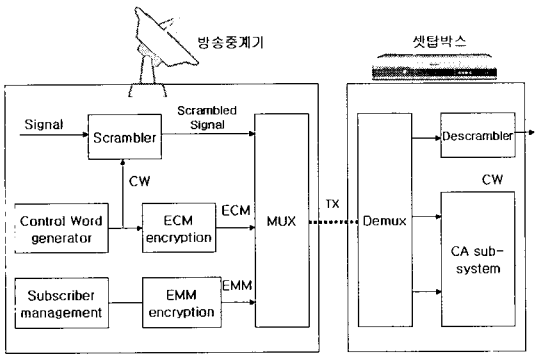
수신자격이 없는 수신자는 시청이 불가능하도록 콘텐츠를 암호화하여 보내며, 암호화된 방송 콘텐츠의 제어는 제어단어(Control Word)를 이용하여 수행된다.

(2) 자격제어(Entitlement Control) 기능

CW를 인증키로 암호화하여 ECM (Entitlement Control Message)에 실어 수신자에게 전송한다. CW는 주기적으로 전송되며, 그 때마다 새로운 CW가 생성되고 암호화되어 전달된다. ECM에는 암호화된 CW외에 제어수(Control parameter)가 포함되며, 모든 수신기

는 수신된 제어변수와 수신기의 인증변수(authentication parameter)를 비교하여 정당한 사용자로 판단될 경우에만 스마트 카드내의 비밀키를 이용하여 CW를 복호하고, 수신된 콘텐츠를 디스크램블링 한다.

(3) 자격관리(Entitlement Management) 기능



〔그림 2〕 CAS의 시스템 모델

수신기에 자격을 부여/갱신/관리 하는 기능으로, 인증키를 분배키로 암호화하여 EMM(Entitlement Management Message)을 생성하고 암호화하여 수신측으로 전송한다. EMM은 수신기의 보안 장치인 스마트 카드에 자격을 부여하거나 갱신하는 기능을 한다.

CAS의 시스템 모델은 [그림 2]와 같다. CAS 기술을 사용하기 위해서는 디지털 방송 표준인 DVB(Digital Video Broadcasting), ATSC(Advanced Television System Committee), OpenCable에서 정한 인터페이스 및 콘텐츠 보호 규격을 만족해야 한다. 각 방송 규격에서 요구하는 CAS에 대하여 간략하게 살펴보도록 한다.

4.1 ATSC 제한수신시스템

ATSC에서는 하나의 프로그램에 여러개의 CAS가 동시에 적용될 수 있는 simulcrypt방식을 채택하고 있다, 콘텐츠를 암호화하는데 사용되는 스크램블링 알고리즘은 168비트의 키를 가진 CBC(Cipher Block Chaining) 모드의 Triple-DES가 규격화 되어 있다. 수신부에서 사용되는 보안 인터페이스 모듈에 대한 규격은 스마트카드 타입의 NRSS(National Renewable Security Standard)-A, PCMCIA 타입의 NRSS-B 두 가지가 허용되고 있다. 수신기와 보안 모듈간의 통신 규정은 없지만 NRSS 사용을 의무화하고 있다[9].

4.2 DVB 제한수신시스템

DVB에서 규격화된 제한수신시스템은 simulcrypt 기술을 표준화하여 가입자의 수신기에서 디스크램블링과 암호화 기능을 분리하였다[10]. 디스크램블링 방식은 DVB-CSA(Common Scrambling Algorithm)를 사용하도록 하고, 암호화 방법은 각 제한수신시스템마다 다르게 사용할 수 있도록 하여 가입자 수신기는 서로 다른 제한수신시스템을 갖는 보안 인터페이스 모듈을 수용할 수 있도록 하였다.

4.3 OpenCable 제한수신시스템

OpenCable의 제한수신시스템은 송신부의 시스템과 수신부의 호스와 분리된 POD(Point Of Deployment)로 구성되어 있다. 기존의 디지털 방송 수신장치 시스템에서는 암호화된 콘텐츠를 수신하여 복원하는 기능이 수신 장치 내부에 내장되어 있었으나 POD에서는 수신 장치로부터 분리한 별도의 보안 모듈로 정의하고 있다. OpenCable에서는 DVB나 ATSC와 같이 특정 암호 알고리즘을 표준으로 규정하지 않고, 수신기와 보안 모듈 간의 인터페이스만을 규정하고 있다[11].

5. 방송 표준을 위한 DRM 기술 및 복제 방지 기술

[표 1]에서 보인 표준화 단체 중 방송 표준과 관련된 DRM 기술과 획득한 콘텐츠에 대한복제를 방지하는 기술에 대하여 살펴본다.

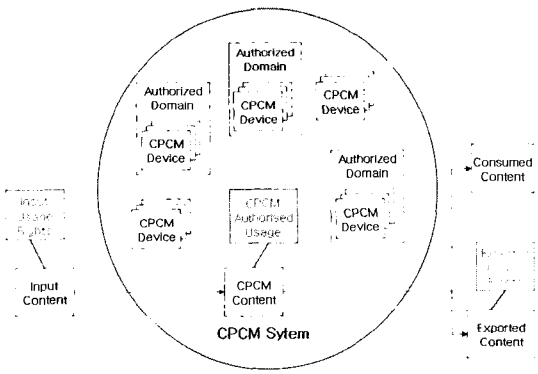
5.1 DVB CPCM

CPCM(Content Protection & Copy Management) 시스템은 상업적인 콘텐츠의 보호와 관리를 위하여 상호호환적 플랫폼을 제공한다. 그리고, CPCM 시스템은 불법복제를 방지하기 위한 방법이 아니라 사용자가 콘텐츠를 복사하여 어떻게 사용하는지를 제어한다

[11]. 사용자가 획득한 콘텐츠는 브로드캐스트, 케이블, 위성, 인터넷 등 다양한 방법으로 인가된 도메인 내의 각 장치에 전송되어 사용될 수 있다. [그림 3]은 CPCM 시스템의 개념을 나타내고 있다.

입력 콘텐츠가 CPCM 시스템에 입력되면 CPCM 디바이스에 의해 구현되는 포착 지점(Aquistion Point)에서 CPCM 콘텐츠로 된다. CPCM 콘텐츠는 저장, 처리될 수 있으며, 사용자에 의해 사용되거나 다른 시스템으로 수출되어 CPCM 시스템을 떠날 수 있다. CPCM 시스템의 구성 요소는 다음과 같다.

(1) CPCM Device
CPCM 함수를 수행하는 장치
(2) CPCM Authorised Domain
한 가정내에 속하는 모든 CPCM 디바이스의 국소적 그룹
(3) CPCM Content Usage Rules
콘텐츠, 서비스 제공자에 의해 정해짐
(4) CPCM Content
CPCM 시스템에 의해 관리되는 콘텐츠



〔그림 3〕 CPCM의 개념도

5.2 TV Anytime

TV Anytime 포럼은 EBU(European Broadcasting Uniton), BBC, Phillips, 마이크로소프트, 디즈니 등을 중심으로 구성된 통신 기능 및 대용량 기억 장치를 가진 DVR(Digital Video Recorder)을 위한 새로운 방송 서비스를 위해 표준화를 진행하고 있는 국제 표준 단체이다[13]. TV Anytime에서는 권리의 표현, 권리 보호, 콘텐츠 이용의 제한 등 권리에 대한 문제가 중요한 과제이며 이를 RMP(Rights Management and Protection)에서 다룬다. 보호할 권리가 무엇인지, 콘텐츠에 대한 시청자의 권리는 무엇인지 등에 대한 정보를 RMPI(Rights Management and Protection Information)라고 한다. RMP는 콘텐츠가 아닌 콘텐츠의 이용을 관리하는데 중점을 둔다. RMP 및 RMPI는 다음의 요구 조건을 만족하여야 한다.

(1) 콘텐츠 소유자 정보와 이용규칙을 제공
(2) 콘텐츠, 권리 정보 및 그 이용 규칙을 완전한 형태로 영속적으로 보호할 것
(3) 적절한 법규정에 따라 시청자의 이용권을 보호할 것
(4) 적절한 법규정에 따라 시청자의 기본적 법률상의 권리(개인 이용 범위 내에서의 복제권, 개인정보 보호 등)를 보호할 것

여기에 RMPI는 다양한 과금 방법 및 가격 설정 방법을 구현하기 위해 다음 정보를 포함할 필요가 있다.

(1) 콘텐츠 식별 정보
(2) 저작권자
(3) 저작권자에 의해 주장될 수 있는 권리
(4) 콘텐츠를 이용하기 위한 조건
(5) 사용되고 있는 정보보호 기술에 대한 정보

RMPI의 중요한 개념은 도메인(Domain)으로, 이것은 보호될 콘텐츠를 사용할 수 있는 기기의 집합을 의미한다.

5.3 CPPM/CPRM

CPPM(Content Protection for Prerecorded Media)과 CPRM(Content Protection for Recordable Media)은 모두 DVD 규격에서 채용되고 있는 복제방지기술로써 CPPM은 재생전용 매체용, CPRM은 기록 가능한 매체용으로 개발되었다[5]. 두 가지 기술 모두 매체(Media)에 MKB(Media Key Block)라는 키 묶음을 기록해 두

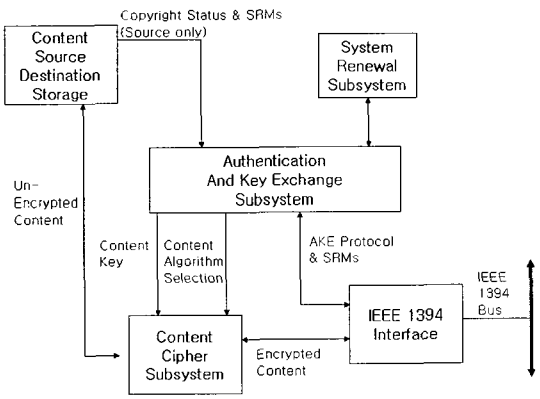
고, 기기에 준비되어 있는 장치키(Device key)와 MKB를 이용하여 불법복제방지를 실현한다.

CPPM/CPRM은 매체와 기기 양쪽에 고유의 정보를 삽입하여, 둘 사이에서 키가 생성되지 않으면 재생이 되지 않는다. 또, MKB와 장치키는 매체나 기기를 설계하는 회사가 자유롭게 사용할 수 있는 것이 아니고 모두 라이센스 회사에 의해 관리 된다.

5.4 DTCP(Digital Transmission Content Protection)

DTCP는 5C(Hitach, Intel, Matsushita, Sony, Toshiba)가 개발한 기술로 오디오/비디오의 콘텐츠를 IEEE 1394, USB 표준 및 IP 기반 홈네트워크와 같은 디지털 인터페이스로 전송할 때 불법복제, 가로채기 등으로부터 보호하기 위한 암호화 기반의 프로토콜이다[6]. DTCP에서 복제방지를 위한 4가지 기본 요소는 다음과 같고, [그림 4]는 DTCP의 콤포넌트 구조를 나타낸다.

- 인증과 키 교환(Authentication and Key Exchange)
- 콘텐츠 암호화(Content Encryption)
- 복제제어 정보(Copy Control Information)
- 시스템 갱신능력(System Renewability)



〔그림 4〕 DTCP 상호호환시스템의 콤포넌트 구조

PC, DVD 플레이어, 디지털 TV, 그리고 디지털 셋탑박스 수신기를 포함한 많은 새로운 기술들이 데이터 전송을 위해 IEEE 1394 및 USB 인터페이스를 지원함에 따라 이 기술이 향후 많이 적용될 것으로 예상된다.

5.5 HDCP(High-bandwidth Digital Content Protection)

HDCP는 1999년 Intel Developer Forum에서 처음 소개된 기술로서, DVI 또는 HDMI 등 디지털 버스를 통해 전송되는 오디오/비디오 콘텐츠의 전송을 보호하기 위해 사용되는 기술이다[7]. HDCP에서는 출력측과 입력측 양쪽에 DPK(Device Private Keys)가 삽입되어 있다. DPK는 HDCP의 사양을 결정하는 Digital Content Protection LLC.로부터 공급되고, HDCP의 사양을 만족하지 않는 벤더에는 공급되지 않는다. 각각의 장치가 DPK를 교환, 인증함으로써 출력측으로부터 입력측으로 콘텐츠가 넘어가는 구조이다.

5.6 SmartRight

SmartRight[14]는 Thomson Multimedia 기술을 기반으로 한 디지털 홈 네트워크 환경에서의 복제방지 기술로서 스마트 카드 기반 콘텐츠 보호 기술이다. SmartRight는 CAS 또는 DRM 시스템과의 연동을 통해 디지털 콘텐츠를 보호하는 솔루션을 제공하는 것을 목적으로 하고 있으며, 이를 위해 타 보호 시스템과의 연동을 위한 사용 규칙에 대해서 정의하고 있다.

6. 결론

본 논문에서는 현재 표준화가 완료되었거나 진행중인 DRM 기술 중에서 IPTV에서 콘텐츠 보호를 위해 사용될 수 있는 DRM을 중심으로 살펴보았다.

DRM은 PC를 중심으로 하여 발전되었으나 이제는 IPTV, 디지털 방송 및 디지털 홈 네트워크를 통하여 모바일 기기, 가전 기기에서도 다양한 디지털 콘텐츠를 이용할 수 있는 환경이 확산되고 있으며, 이러한 콘텐츠를 보호하기 위하여 다양한 플랫폼에서 사용할 수 있는 다양한 콘텐츠 보호 기술이 개발되고 있다.

통신과 방송의 융합된 서비스를 제공하는 IPTV에서 콘텐츠를 보호하기 위해서는 현재 방송과 통신에서 각기 사용되고 있는 수신제한시스템, DRM, 불법복

제 방지 기술 등과 같은 콘텐츠 보호기술도 융합되어 사용될 필요가 있다. IPTV를 위한 콘텐츠 보호 기술로는 현재 유료 방송 시스템에서 많이 사용되고 있는 CAS와 DRM을 융합하여 사용하는 방법이 가장 유력시되고 있으나, CAS와 DRM을 어떻게 조합, 연동하여 사용할 것인지 대해서는 아직 많은 논의가 필요하다.

참 고 문 헌

[1] ITU-T Focus Group on IPTV, http://www.itu.int /ITU-T/IPTV, 2006.

[2] 장길수, "IPTV 서비스 기술 및 시장 동향", 전자정보센터, 2006.8.

[3] 강호갑, "국제 DRM표준화 동향 분석 및 대응 전략", 정보과학회지, 제23권 8호, pp.15-24, 2005,9

[4] 이선영, "홈네트워크를 위한 DRM 기술", 한국정보보호학회지, 제16권 6호, pp.46-53, 2006, 12

[5] 4C Entity, "Content Protection System Architecture Revision 0.81," 2000/02 /17. (CPRM)

[6] 5C, "5C Digital Transmission Content Protection White Paper," 1998/07/14.

[7] Digital Content Protection LLC, "High- bandwidth Digital Content Protection System Revision 1.1," 2003/06/09

[8] EBU, Functional Model of Conditional Access system, EBU Project Group B/CA, October, 1995.

[9] ATSC, Draft Conditional Access System for Terrestrial Broadcasst, A/70A, May, 2004.

[10] ETSI, DVB Head-end Implementation of DVB Simulcrypt, ETSI TS 103 197 V1.4.1, December, 2004

[11] CableLabs, CableCARD Copy Protection system. Interface Specification, OC-SP-CCCP-IF- C01 - 050331, March, 2005.

[12] DVB, Digital Video Broadcasting (DVB); Content Protection & Copy Management, DVB Document A094, November 2005

[13] The TV-Anytime Forum, http://www.tv-anytime.org

[14] SmartRight, "SmartRight :Technical White Paper Version 1.7", 2003

◐ 저 자 소 개 ◑

이 선 영(Sun-Young Lee)

1993년 부경대학교 전자계산학과 졸업(이학사)
1995년 부경대학교 대학원 전자계산학과 졸업(이학석사)
2001년 일본 동경대학교 대학원 전자정보공학과 졸업(공학박사)
2001년 순천향대학교 강사
2004년~현재 순천향대학교 정보보호학과 조교수
관심분야 : 암호이론, 정보이론, 인터넷 보안, DRM
E-mail : sunlee@sch.ac.kr