情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

홈네트워크를 위한 DRM 기술

이 선 영*

요 약

홈네트워크는 가전 기기와 유무선 인터넷, 모바일 기기 등을 연결하여 가정 내의 시스템을 제어하거나 데이터를 서로 전송하며 다양한 분야에서 이용될 수 있다. 그 중에서 홈 엔터테인먼트, 디지털 홈 등과 같이 콘텐츠가 가치를 가지는 경우에 있어서는 콘텐츠의 불법적인 복제나 유통을 방지하여 콘텐츠 제공자 또는 콘텐츠 저작자의 권리를 보호하기 위한 DRM 기술이 필요하다. 본 논문에서는 DRM 기술을 소개하고, 홈네트워크를 위한 DRM 기술 및 표준화 활동에 대하여 알아본다.

Ⅰ. 서 론

오늘날 인터넷과 관련 기술의 발달로 문서, 오디오, 비디오, 소프트웨어 등의 디지털 콘텐츠의 생성 및 분배가 용이하게 되었다. 디지털 콘텐츠는 무한히 반복하여 사용해도 품질이 저하되지 않고, 수정과 복사가 편리하며, 네트워크를 통해 대용량의 콘텐츠를 짧은 시간에 전송 및 배포할 수 있다. 이러한 특성은 디지털 콘텐츠의 장점이지만 지적재산권자의 권리를 위협하는 원인이 되기도 한다.

디지털 콘텐츠의 불법복제방지와 저작권 보호를 위하여 다양한 기술들이 제안되었는데 그 중에서 DRM이 최적의 기술로 평가되고 있으며, 이미 디지털 음악, 영화, 문서보안 등 다양한 분야에서 사용되고 있다. 향후 DRM이 이용될 분야 중 주목받고 있는 것이 홈네트워크이다.

홈네트워크는 가정 내의 가전 기기 및 시스템을 상호 또는 외부 인터넷 상의 정보 기기와 연결하여 각각의 기기 및 시스템에 대한 원격 접근과 제어가 가능하고, 음악, 비디오, 데이터 등과 같은 콘텐츠를 사용할 수 있도록 양방향 통신 서비스를 구현하는 기술을 말한다. 홈네트워크는 디지털 TV, 휴대폰, 영화, 반도체, PC, 콘텐츠 등 거의 모든 사업과 연관되어 있고, 많은 이용자들이 음악, 영화 등과 같은 상업용 콘텐츠를 홈네트워크 상의 다양한 기기에서 사용하게 된다. 그러므로 홈네트워크에서 디지털 콘텐츠는 현재 우리가 PC를 기반으로 이용하고 있는 것보다 훨씬 더 다양하게 이용될 것이고, 이러한 홈네트워크 환경에서 콘텐츠에 대한 보호가 이루어지지 않는다면 콘텐츠 제공자는 PC를 기반으로 한 환경에서보다 훨씬 더 막대한 경제적 피해를 입게 될 것이다. 이와 같은 피해를 막기 위해서는 DRM 기술을 이용하여 디지털 콘텐츠의 불법복제 및 유통을 방지해야만 한다.

그러나, 현재 DRM 기술은 콘텐츠와 플랫폼의 종류에 따라 적용되는 보호 기술이 다르고, 비즈니스 및 도메인별로 별도의 표준이 존재하고 있어 현재의 DRM 기술들을 그대로 홈네트워크에 적용하기는 어렵다. 다양한 플랫폼과 디지털 TV, 인터넷, 휴대단말기, 셋톱박스 등 다양한 기기를 사용하는 홈네트워크에서 DRM을 적용하기 위해서는 DRM간의 상호호환성이 보장되어야 한다.

본 논문에서는 DRM기술 동향과 홈네트워크를 위한 DRM 기술 및 표준화 동향에 대하여 소개한다.

본 논문의 구성은 다음과 같다. 2장에서 DRM에 대해 알아보고, 3장에서는 홈네트워크에서의 DRM 표준화 동향에 대하여 알아본다. 4장에서는 홈네트워크를 위한 DRM 표준 기술 규격들에 대하여 살펴보고, 마지막 5장에서 결론을 내리고자 한다.

* 순천향대학교 정보보호학과 (sunlee@sch.ac.kr)

Ⅱ. DRM(Digital Right Management)

2.1 DRM 기술 개요

DRM이란 디지털 콘텐츠의 생산, 분배, 거래규칙, 과금, 거래내역의 관리, 정산 등 디지털 콘텐츠의 전체 라이프사이클에 걸쳐 투명성과 신뢰성을 보장하는 유통체계 전반을 통칭하며, 디지털 콘텐츠의 유통에 참여하는 모든 참여주체들에게 투명성과 신뢰성을 제공해주는 기반 서비스를 말한다.

디지털 콘텐츠에 대한 불법적인 사용이나 복제를 방지하기 위한 기술적인 접근은 크게 두 가지로 구분되며, 허가되지 않은 사용자에게 디지털 콘텐츠의 사용은 허가하되 스스로 불법적인 행동을 자제하게 만드는 효과를 기대하는 소극적인 보호기술(Passive Protection Technology)과 사용이 허가되지 않는 사용자에게는 디지털 콘텐츠의 접근을 차단하는 강력한 불법복제방지 기술을 사용하는 적극적인 보호기술(Active Protection Technology)이 있다[1].

2.1.1 소극적 보호 기술

소극적 보호 기술에는 저작권 정보 표시(Copy right information), 디지털 워터마킹(Digital watermarking)[2, 3], 디지털 핑거프린팅(Digital fingerprinting)이 있다[4~6]. 저작권 정보 표시방식은 영화 앞부분의 저작권 공지, 전자문서 표지처럼 디지털 콘텐츠를 사용하기 전에 사용자가 저작권에 대한 정보를 볼 수 있도록 하여 사용자로 하여금 무단 도용 혹은 복제 및 배포에 대한 행위를 자제하는 역할을 한다.

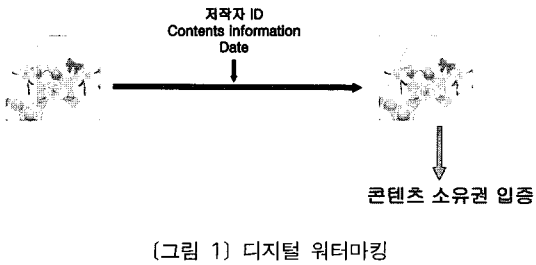
디지털 워터마킹 방식은 저작권 정보를 담고 있는 워터마크 정보를 원본의 내용을 왜곡하지 않는 범위에서 또는 사용자가 인식하지 못하도록 디지털 콘텐츠에 삽입하는 기술이다. 저작권에 대한 침해가 발생했을 경우, 불법복제 및 불법 유통된 디지털 콘텐츠로부터 저작권 정보를 추출하여 증거 자료로 활용할 수 있다. 디지털 워터마킹의 처리과정은 [그림 1]과 같다.

디지털 핑거프린팅은 워터마킹 기술을 기반으로 하는 콘텐츠 보호 기술로서 저작권자의 정보가 아닌 사용자에 대한 정보인 핑거프린트를 삽입하여 사후에 발생하게 될 콘텐츠의 불법복제자를 추적하는데 사용하는 기술이다[4~6]. 디지털 핑거프린팅 방식은 사용자의 고유 정보를 포함하는 핑거프린트가 삽입되므로 정당한 사용자들은 서로 다른 핑거프린트를 가진 콘텐츠를 사용한다. 디지털 핑거프린팅 방식에서는 서로 다른 핑거프린트를 구성하는 방법이 중요한데, 핑거프린트의 구성방법에 따라 결탁 공격 등의 공격에 강인성을 가질 수 있기 때문이다. [그림 2]는 디지털 핑거프린팅 방법을 나타내고 있다.

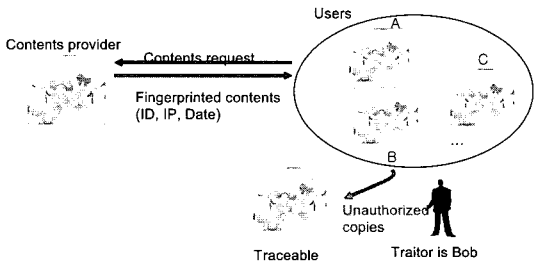
2.1.2 적극적 보호 기술

소극적인 보호 기술이 허가되지 않은 사용자에게도 디지털 콘텐츠의 접근을 허용하는데 비해 적극적인 보호 기술은 허가되지 않은 사용자로부터의 접근을 차단함으로써 콘텐츠를 보호하는 기술이다. 적극적인 보호 기술은 접근제어(Access Control) 방식, 사용제어(Use Control) 방식, 그리고 복제방지(Copy Protection) 방식으로 크게 구분할 수 있다.

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. 즉, 인가된 사용자가 암호화된 콘텐츠를 복호하여 원본 콘텐츠를 획득한 후 이를 불법복제 및 불법 유통할 경우에는 콘텐츠에 대한 지속적인 보호가 이루어지지 않는다.



[그림 1] 디지털 워터마킹



[그림 2] 디지털 핑거프린팅

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 의미 없는 데이터가 되게 하는 기술이다. 복제 방지 기술은 단독으로 사용되기도 하지만 CAS 또는 DRM 기술과 연동하여 최종 사용자가 디지털 콘텐츠의 장점인 복제를 할 수 없게 한다[7]. 복제방지 기술의 대표적인 예로는 4C의 CPPM/CPRM[8], 5C의 DTCP[9], Intel의 HDCP[10] 등이 있다.

2.2 DRM 핵심 기술 요소

DRM 시스템은 여러 가지 기술들이 조합되어 구성된다. DRM 시스템의 기본 구조와 대표적인 DRM의 핵심 기술을 살펴본다.

2.2.1 DRM 구조

DRM 시스템의 기본적인 구조는 크게 원본 디지털 콘텐츠에 DRM을 적용하여 보호된 콘텐츠를 만들고 이를 공급하는 **DRM 패키저**와 라이센스를 발급하고 관리하는 **클리어링 하우스**, 라이센스에 따라 사용을 통제하는 **DRM 클라이언트**로 구성된다.

2.2.2 DRM의 핵심 기술 요소

DRM은 콘텐츠 보호를 위한 소극적 보호 기술 및 적극적 보호 기술, 암호화 기술, 인터페이스 기술 등 여러 가지 기술들이 복합적으로 사용되어 구현된다. DRM의 대표적인 핵심 기술은 다음과 같다[11, 12].

(1) 암호화 기술(Cryptography)

DRM에서 암호화 기술은 콘텐츠의 기밀성과 무결성 보장을 위하여 사용된다. 기밀성 보장을 위하여 DES/3-DES, AES-128 등의 대칭키 암호 알고리즘이 사용되며, 무결성 및 인증 처리를 위하여 PKI 인증서 기반의 전자 서명 기술을 이용한다.

(2) 키 관리 기술(Key Management)

콘텐츠의 암호화를 위해 사용된 키를 안전하게 관리하는 기술이다. 콘텐츠의 암호화는 랜덤하게 생성된 암호화 키를 이용하며, 암호화 키는 라이센스에 권리 정보와 함께 콘텐츠의 이용자에게 전달되어 콘텐츠를 복호할 때 사용된다. 콘텐츠를 암호화할 때 사용된 비밀키를 클리어링 하우스에 보관하고 라이센스를 발급할 때 이를 이용하는 중앙 집중식 분배 방식과 암호화 키를 암호화된 콘텐츠에 동봉(envelope)하여 관리하는 방식이 있다.

(3) DRM 패키징 포맷(Secure Container)

디지털 콘텐츠의 보호 및 신뢰성 있는 유통을 위해 디지털 콘텐츠를 암호화하고, 메타데이터를 추가하여 하나의 전자적 정보구조체(Secure Container)로 구성하는 기술이다.

(4) 디지털 콘텐츠 식별체계(Identification)

디지털 콘텐츠의 식별을 가능케 함으로써 콘텐츠 유통 과정에서의 콘텐츠 관리를 용이하게 하는 기술이다.

(5) 메타데이터(Metadata)

디지털 콘텐츠에 대한 식별 정보, 내용 정보, 특성 정보 등을 표현하는 기술로써 디지털 콘텐츠의 체계적인 관리 및 원활한 검색에 활용된다.

(6) 권리 표현 기술(Rights Expression)

디지털 콘텐츠에 대한 사용 권한과 조건을 표현하는 기술이다. 일반적으로 디지털 콘텐츠의 사용 권한은 디지털 콘텐츠 배포자로부터 허가된 사용자에게 제공되는 라이센스에 명시되어 전달되며, 이러한 라이센스는 기계가 해독할 수 있는 형태의 권리 표현 기술을 이용하여 생성되고 전달된다. 대표적인 권리 표현 기술로는 XrML을 기반으로 한 MPEG-21 REL과 OMA의 ODRL이 있다.

(7) 권리 통제 기술(Rights Enforcement)

디지털 콘텐츠를 라이센스에 명시된 사용 권한과 사용 조건의 범위에서만 사용될 수 있도록 지속적으로 통제하는 기술이다.

(8) 인증 기술(Authentication)

허가된 사용자 또는 장치에서만 사용 권한이 유효하도록 통제하기 위해 사용되는 기술이다. 사용자 인증을 위하여 사용되는 기술로는 ID/Password, 공인인증서, 생체 인식 등이 있고, 장치 인증을 위해서는 CPU 고유번호, MAC address, HDD 일련번호,

X.509 기반의 디바이스 인증서 등이 사용된다.

(9) 도메인 권한 관리 기술(Domain Rights Management)

사적 복제권이 허락되는 장비에 한하여 콘텐츠의 자유로운 전송 및 편집 작업이 가능하도록 DRM이 지원하는 것을 목표한 기술이다. 디바이스 인증처리 기술, 가상 도메인(Virtual domain) 구성 기술 및 디바이스의 도메인 합류/탈퇴 처리를 위한 기술이 필요하다.

2.3 DRM 기술 개발 현황

초기의 DRM 기술은 주로 인터넷을 기반으로 한 디지털 음악 및 동영상 등의 유료 콘텐츠 보호를 위해 사용되었다. 그러나, 표 1에서 나타난 것처럼 최근에는 기업의 문서 보안이나 모바일 콘텐츠 보호를 위해 DRM의 활용 범위가 확산되고 있는 추세이며, 디지털 방송 및 디지털 홈 환경에서의 활용이 모색되고 있다[1].

DRM 기술은 초기에는 DRM 기술 벤처에 의해 주도 되었으나, 현재는 운영 체제 또는 미디어 플레이어를 가진 Microsoft, Sony 등의 기업으로 DRM 기술 개발의 주체가 이동되고 있다. 그리고 현재 많은 DRM 기술이 개발되고 있으나 디지털 콘텐츠를 이용하는 플랫폼의 종류 및 콘텐츠를 이용하는 서비스의 종류에 따라 서로 다른 DRM 기술이 개발되어 사용되고 있는 실정이다. 즉, 휴대폰, 컴퓨터, 디지털 홈, MP3 플레이어 등 다양한 기기를 이용하는 사용자는 자신이 사용 권한을 가진 디지털 콘텐츠를 자신의 모든 장치에서 사용하기를 원하지만 각 장치에서 사용되는 DRM 기술이 다르기 때문에 모든 장치에서 콘텐츠를 사용하는 것은 현재로서는 불가능하다. 그러나, 콘텐츠의 기기간 이동에 대한 수요는 점점 더 증가하고 있는 추세이므로, 이를 해결하는 것이 시급한 문제라고 할 수 있다. 이 문제를 해결하기 위해서 DRM 간의 상호호환성을 보장하는 기술에 대한 연구가 계속되고 있고, DRM 표준화를 통하여 상호호환성 문제를 해결하려고 노력하고 있다.

2.4. DRM 기술의 표준화 동향

DRM의 표준을 만들기 위해 SDMI, AAP, OeBF, DVD Forum, IRTF의 IDRM, MPEG-21등 다양한 표준화 단체들이 각자 독자적인 DRM 표준 기술을 준비해 왔다. 표 2는 국제적인 DRM 표준화를 진행하고 있는 단체들의 현황을 보여주고 있다.

〔표 1〕 단계별 DRM 기술 개발 현황 및 전망

단 계	내 용
1단계(99-02)	- 인터넷을 기반으로 한 디지털 콘텐츠의 저작권 보호
2단계(03-06)	- 기업 문서 보안, 의료 정보 보안 등 정보의 기밀성 보호 - 모바일 환경의 유료 콘텐츠 보호
3단계(07-10)	- 디지털 방송 콘텐츠의 보호
4단계(11-15)	- 디지털 홈 환경에서의 디지털 콘텐츠 보호

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[13], 5C[14]등의 산업표준단체들은 매우 구체적인 기술 규격을 마련하고 있다.

Ⅲ. 홈네트워크를 위한 DRM 표준화 동향

네트워크와 디지털 기기의 발달로 사용자는 보다 많은 디지털 콘텐츠를 사용하게 되고 콘텐츠에 대한 보호의 필요성 역시 증가하게 되었다. 다양한 디지털 기기를 이용하는 사용자들은 콘텐츠를 컴퓨터, DVD 플레이어, 셋탑박스, 디지털 TV 등의 개인용 기기 사이에서 이동시키기를 원한다. 그러나, 2장에서 살펴본 바와 같이 장치들은 각각 독자적인 DRM 기술을 사용하고 있어, 이와 같은 사용자의 요구를 실현하는 것은 쉽지 않다. 기기간 콘텐츠의 이동이 많을 것으로 예상되는 홈네트워크에서 이 문제가 해결되지 않는다면 디지털 콘텐츠 제공자들은 홈네트워크에 참여하기를 주저하게 될 것이고, 이는 홈네트워크의 활성화에 많은 지장을 초래하게 될 것이다. 따라서 홈네트워크 DRM에서 가장 중요한 것은 DRM의 상호호환성이라고 할 수 있다. 이와 같은 홈네트워크에서의 요구를 만족하기 위하여 많은 표준화 활동이 이루어지고 있다(표 2 참조).

3.1 DLNA(Digital Living Network Alliance)

DLNA은 2003년에 설립된 디지털 홈네트워킹 분야의 국제산업단체로 삼성전자, Fujitsu, HP, IBM, Intel, Kenwood, Microsoft, NEC, Nokia, Panasonic, Philips, Sony 등 국제적인 가전업체와 소프트웨어 업체들이 대거 참여하고 있다. 여기에서도 디지털 콘텐츠 보호 기술의 표준화가 중요한 분

〔표 2〕 DRM 관련 국제 표준단체 현황

기술분야	표준단체	기술내용	현재상태
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

야로 인식되어 이에 대한 기술 표준 마련을 위한 작업을 진행하였다. 그러나 Microsoft의 소극적 참여로 인하여 DRM의 표준화 활동은 진척을 보지 못하였고, DRM의 표준화를 위해 삼성전자, Sony, Philips, HP, InterTrust, Matsushita, Fox film 등 7개사는 Coral이라는 단체를 별도로 구성하여 이에 대한 표준화 작업을 진행하고 있다.

3.2 Coral

Coral 컨소시엄은 미디어 및 기술 기업 7개사, 삼성전자, Sony, Philips, HP, InterTrust, Matsushita, Fox film이 DRM의 상호호환성 확립을 위해 구성한 단체로서 서비스 제공자(Service provider)나 장치에 상관없이 사용자가 디지털 콘텐츠에 쉽게 접근할 수 있는 환경을 실현하는 것을 목표로 하며, 서로 다른 DRM 기술이 공존할 수 있는 새로운 기술개발에 초점을 두고 있다. Coral은 공통의 DRM 기술을 정의하는 것이 아니라 서로 다른 DRM 간에 상호 작용이 가능하도록 각종 사양을 책정하며, 상호호환성을 실현하는 기술층은 복수개의 서로 다른 DRM 기술을 지원한다. Coral의 사양은 Web이나 홈네트워크를 통한 안전한 콘텐츠 배송 서비스 및 디바이스에서의 채용을 가정하고 있다.

3.3 마린공동개발연합(Marlin Joint Development Association)

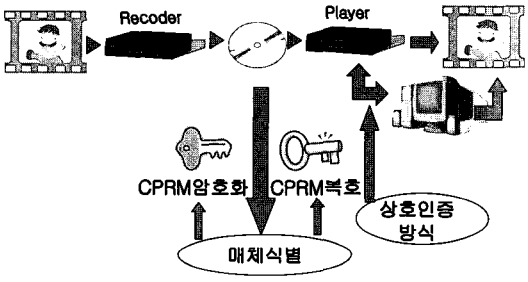
마린공동개발연합은 음악이나 비디오 등 저작권이 보호된 콘텐츠를 모든 가전 제품에서 재생할 수 있도록 하는 것을 목표로 한다. 이 단체에는 Coral에 참여하고 있는 삼성전자, Sony, Philips, HP, InterTrust, Matsushita, Fox film이 참가하고 있다. 마린공동개발연합에서는 먼저 결성된 Coral의 작업 성과를 활용하는데, Coral과는 달리 애플, MS의 독자적인 DRM 규격에 대응되는 새로운 DRM 표준을 마련하기로 하였다. 마린공동개발연합은 최종적으로는 참가 기업과 다른 기업이 호환성을 갖는 시스템을 개발할 수 있도록 하기 위한 각종 사양을 정리할 예정이다.

Ⅳ. 홈네트워크를 위한 주요 DRM 기술 규격

홈네트워크에서 사용되고 있거나 향후 사용될 수 있는 DRM 기술들을 살펴본다.

4.1 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[8]. 두 가지 기술 모두 매체(Media)에 MKB(Media Key Block)라는 키 묶음을 기록해 두고, 기기에 준비되어 있는 장치키(Device key)와 MKB를 이용하여 불법복제방지를 실현한다. [그림 3]은 CPRM의 기본 구조를 도식화한 것이다.



[그림 3] CPRM의 기본구조

재생전용인 CPPM에서는 매체키, 앨범단위로 다른 앨범ID, CCI(Copy Control Information)로부터 작성되는 키를 이용하여 기록 콘텐츠에 대한 암호화가 수행된다. 매체키는 장치키와 MKB를 사용하여 작성할 수 있다. 앨범 ID와 MKB는 리드인 영역에 기록되어 복제할 수 없고, MKB는 라이센스 회사가 제조업체에 배포한다. MKB는 항상 고유한 것이 사용되는 것이 아니라 일정 수까지 도달하면 새로운 것으로 갱신된다. CCI는 복제에 대한 정보로서 복제가 가능한지에 대한 정보뿐만 아니라 복제를 인정할 경우에도 몇 번까지 복제할 수 있는지에 대한 정보를 기록하고 있다. 기기에 준비되어 있는 장치키는 라이센스 회사로부터 기기제조업체에게 부여된 키로서 각 기기에는 반드시 서로 다른 키가 사용된다. PC를 사용할 경우에는 재생에 사용되는 소프트웨어가 기기에 해당된다.

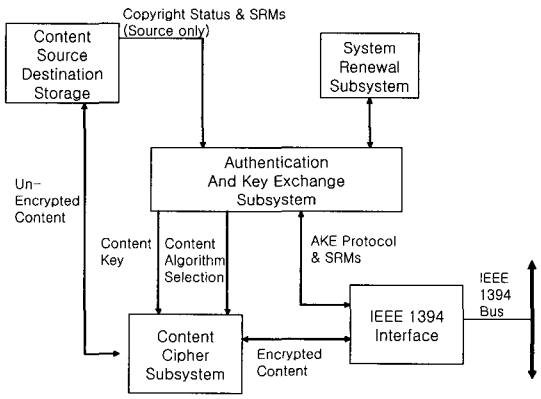
이와 같이 CPPM에서는 MKB, 앨범ID, CCI, 장치키라는 4개의 정보를 이용한다. 실제 콘텐츠 재생은 MKB와 장치키를 사용하여 매체키를 생성한 후, 앨범 *ID*와 *CCI*를 사용하여 암호화에 사용하는 키를 생성하여 재생이 이루어진다. 따라서, 4개의 정보 중 하나라도 이상이 있다면 콘텐츠를 복원할 수 없다. CPRM은 기본적으로 CPPM의 기록 가능한 매체버전이라고 할 수 있다.

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.

4.2 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[9]. 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 호환시스템의 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.

4.3 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[10]. 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.

4.4. SmartRight

SmartRight[15]는 Thomson Multimedia 기술을 기반으로 한 디지털 홈 네트워크 환경에서의 복제 방지 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.

V. 결 론

본 논문에서는 저작권 보호를 위한 기본이 되는 기술인 DRM에 관련된 기술을 살펴보았다. DRM 기술은 초기의 인터넷 PC 기반의 DRM 플랫폼에서 모바일, 디지털 방송, 디지털 홈 엔터테인먼트 등 다양한 분야로 응용이 확산되고 있는 추세이다. 홈네트워크에서의 콘텐츠 유통은 지금까지의 디지털 콘텐츠 유통 및 서비스와는 비교될 수 없을 정도의 큰 시장 규모를 가지고 있기 때문에, 홈네트워크 환경에서 DRM 기술이 순조롭게 이용될 수 있다면 홈네트워크의 활성화는 보다 쉬울 것이다.

그러나 현재의 DRM 기술을 홈네트워크에서 이용하기 위해서는 무엇보다도 먼저 상이한 DRM 기술 간의 호환성을 보장해야만 한다. DRM 기술 간의 상호호환성 보장을 위해 현재 여러 표준화 단체에서 표준화 작업을 진행하고 있으나, 기술적인 문제보다는 기업 또는 국가 간의 정치 또는 비즈니스적인 문제로 인하여 상호호환성을 보장하는 문제는 여전히 어렵다.

기술적인 면에서는 향후 상호호환성 보장과 더불어 미래의 홈네트워크 시장에서 필요로 하는 DRM의 안정적 기반 제공을 위해서 아직 드러나지 않은 많은 요소 기술들을 발굴하고 개발하는 것이 필요할 것이다.

참 고 문 헌

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

[2] I.Cox, J.Kilian, F.Leighton, T.Shamoon, "Secure spread spectrum watermarking for multimedia, " IEEE Trans. Image Processing, vol.6, pp.1673-1687, 1997, Dec.

[3] M.Barni, F.Bartolini, V.Cappellini, A.Piva, "A DCT domain system for robust image watermarking," Signal Processing, vol.66, pp.357-372, 1998.

[4] B.Chor, A.Fiat, M.Naor, B.Pinkas, "Tracing traitors," IEEE Trans. Inform. Theory, vol.46, pp.893-910, 2000, May.

[5] W.Trappe, M.Wu, Zhen Wang, K.J.R. Liu, "Anti-Collusion Fingerprinting for multimedia," IEEE Trans. On Signal Processing, vol.51, pp. 1069-1087, 2003.

[6] 강인구, 이홍규, "콘텐츠 불법 사용자 추적을 위한 디지털 비디오 핑거프린팅", 정보과학회지, 제23권 8호, pp. 71-77, 2005년 9월.

[7] M.Ripley, C.Brendan, S.Balogh, M.Reed, "Content Protection in the Digital Home," Intel Technology Journal, vol.6, Issue 4, 2002.

[8] 4C Entity, "Content Protection System Architecture Revision 0.81," 2000/02/17. (CPRM)

[9] 5C, "5C Digital Transmission Content Protection White Paper," 1998/07/14.

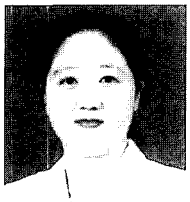
[10] Digital Content Protection LLC, "High-bandwidth Digital Content Protection System Revision 1.1," 2003/06/09

[11] 강호갑, "2005, 최신 DRM 기술 동향", 전자공학회지, 제32권11호, pp.1337-1356, 2005년 11월.

[12] ETRI, 오원근, "DRM 표준화 및 평가 기술". 전자통신동향분석, 제20권, 제4호, 2005년 8월

[13] [4C Entity] http://www.4centity.com
[14] [5C DTLA] http://www.dtcp.com
[15] SmartRight, "SmartRight : Technical white paper Version 1.7."2003.

〈 著 者 紹 介 〉



이 선 영(SunYoung Lee)
종신회원
1993년 2월 ~ 1995년 2월 : 부경대학교 전자계산학과(학사, 석사)
1996년 ~ 20001년 : 일본 동경대학교 대학원 전자정보공학과 공학박사
2004년 ~ 현재 : 순천향대학교 정보보호학과 교수
〈관심분야〉 암호이론, 정보이론, DRM, 정보보호