공개키 기반의 디지털 콘텐츠 및 인스턴트 플레이어 보호방법연구

류 석†

요 약

인터넷 기술의 발전에 따라 많은 사람들이 인터넷을 통하여 다양한 디지털 콘텐츠를 액세스할 수 있게 되었으나 이러한 접근은 저작권과 소유권 침해를 일으킬 수 있다. 디지털 콘텐츠가 다운로드 된 이후에 디지털 콘텐츠를 보호할 수 있는 방안으로 디지털 콘텐츠에 대한 저작권을 보호하기 위해 DRM(Digital Rights Management)기술이 연구되고 있는 상태이다. 본 논문에서는 콘텐츠의 생성에서부터 사용자가 사용하는 Player를 사용자의 공개키로 암호화 하고 Player 내부에 디지털 콘텐츠에 대한 저적권을 보호할 수 있는 일정기간 사용이 가능한 대칭키와 CCI(Copy Control Information)을 넣는 시스템을 제안한다.

키워드 : 인스턴트 플레이어, 디지털 콘텐츠 보호,DRM

Protect Digital Contents and Instant Player using PKI

Seok Ryu†

ABSTRACT

According to the development of the internet technology, many people can access many kind of digital contents. This approach can infringe the copyright and right owner-ship. Currently many people research the DRM(Digital Rights Management) for protect digital content after digital content downloaded. This paper propose the system that client player witch encrypted using PKI have symmetric key and CCI (copy control information), decrypt digital content witch encrypted when digital content created.

Key Words : Instant Player, Digital Contents, DRM

1. 서 론

정보통신기술의 발전으로 기존의 아날로그 중심의 콘텐츠들이 디지털 콘텐츠들로 빠르게 변화하고 있다. 디지털 콘텐츠는 그 특성상 빈번한 사용이나 복사함으로 인하여 콘텐츠의 품질이 저하되지 않는 특징을 가지고 있다. 또한 그 복사가 용이하다는 장점이 있다. 이에 따라 새로 등장하는 콘텐츠와 기존의 아날로그 콘텐츠들도 디지털 콘텐츠로 제작 되거나 변환되고 있다[1].

디지털 콘텐츠는 인터넷의 확산에 힘입어 많은 사람들이 디지털 콘텐츠를 쉽게 이용할 수 있게 되었다. 그러나 콘텐츠를 제작하는 저작권자의 입장에서는 자신의 콘텐츠가 자신의 동의 없이 자신의 콘텐츠가 도용될 수 있다는 문제점을 낳게 되었다. 이러한 문제를 해결하기 위하여 암호화, 워터마킹, 식별자 시스템 및 이유 유사한 여러가지 방법의 저작권 보호 기술이 연구되고 있다[2].

† 정 회 원 : 국가보안기술연구소 연구원
논문접수 : 2006년 10월 2일, 심사완료 : 2006년 10월 23일

현재 디지털 콘텐츠가 가장 많이 사용되는 분야 중 하나는 디지털 방송, VOD, IPTV등의 실시간 방송 분야이다. 이러한 실시간 방송 분야 에서도 저작권을 보호하기 위하여 CAS/DRM(Conditional Access System/Digital Right Management)를 사용하는데 이러한 기술이 해킹 등의 이유로 인하여 암호가 해독되는 경우 새로운 시스템을 도입하기 전까지는 해결할 수 없는 문제가 있다[2, 3].

따라서 본 논문에서는 디지털 콘텐츠 및 인스턴트 플레이어를 암호화하여 실시간 방송시에 저작권이 보호될 수 있는 방안을 연구하였다.

본 논문은 제2장에서 기존의 디지털 콘텐츠 보호방법에 대한 기술동향을 알아보고, 제3장에서는 제안되는 방법에 대한 설명 및 기존기술과 비교분석을, 하고 제4장에서 결론을 맺는다.

2. 디지털 콘텐츠 보호 기술 동향

디지털 콘텐츠는 사용목적에 따라 그 기술이 특화되는

것이 특징이다. 본 논문에서는 그 기술을콘텐츠 저장기술, 콘텐츠 전송 하드웨어/소프트웨어 기술, 디지털 콘텐츠 보호 기술의 적용 예로CPPM/CPRM(Contents Protection for Prerecorded Media/Content Protection for Recordable Media), DTCP(Digital Transmission Content Protection), HDCP(High-bandwidth Digital Content Protection), MS-DRM을 들어 현재 디지털 콘텐츠 기술동향을 살펴 보도록 한다.

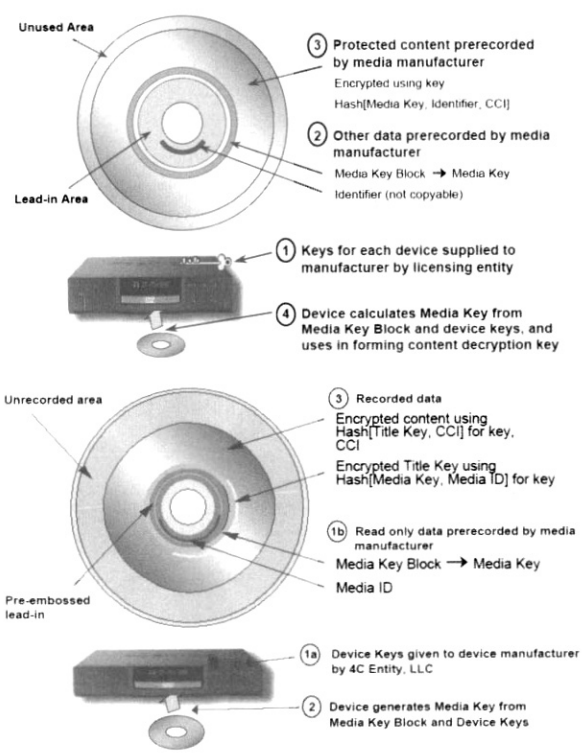
2.1 CPPM/CPRM

IBM, Intel, Matsushita, Toshiba는 4C Entity를 구성하고 1998년 CPPM/CPRM Spec을 발표 하였다. 4C Entity의 목적은 Portable/removable media로 저장되는 콘텐츠의 보호 기술을 위해 조직 되었으며 아래와 같은 핵심 기술을 가지고 있다[4, 5].

- C2 Block Cipher : C2-CBC 모드
- C2 One-way Function : 일방함 함수의 암호 기술

4CEntity, LLC에 라이센트 관리에 의하여 Secret Device Key, Media Identifier, Media Key Block의 배포 관리가 이루어 지고 있다. 각 콘텐츠 들은 Media Key Block이라는 4Entity LLC에서 생성해 주는 키블럭의 특정 키를 가지고 암호화 된다. CPPM의 경우 Media Key Block에서 특정 Media Key를 선택하여 Media Identifier, CCI(copy control information)을 Hash한 값을 Key로 사용하여 콘텐츠를 암호화 한다. CPRM의 경우 Media Key Block, Media ID를 Hash한 값으로 Title Key를 생성하고 Title Key와 CCI을 Hash하여 그 값을 키로 전체 콘텐츠를 암호화 한다. 따라서 Media Key Block,과 Media ID가 키생성의 시작이 된다.

4CEntity는 현재 Network의 전송시의 콘텐츠 암호화와 SD메모리에 콘텐츠를 저장할 경우 암호화 방식에 대하여 Specification을 내놓고 활동 중이다.



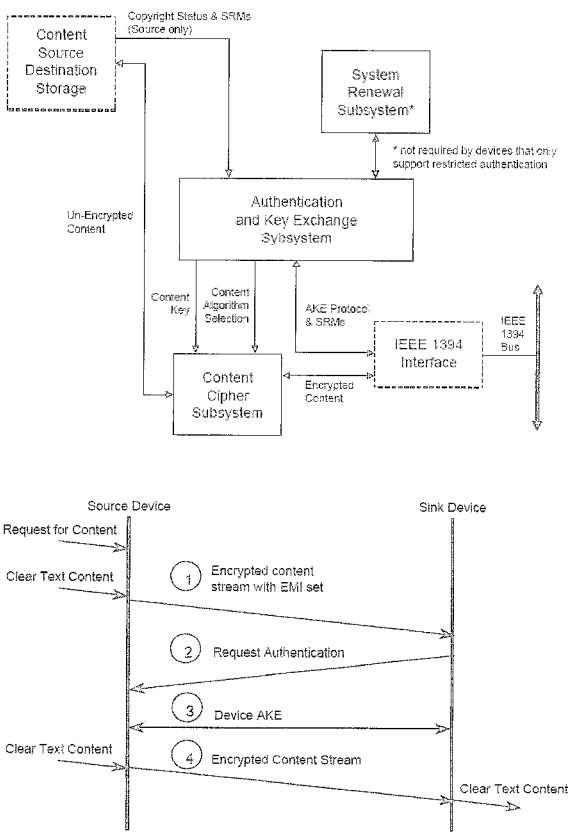
(그림 1) CPPM/CPRM 예제

2.2 DTCP

DTCP(Digital Transmission Content Protection)는 Matsushita, Intel, Hitachi, Sony, Toshiba의 5개 회사가 IEEE 1394/USB를 통하여 전송되는 audio/video Content의 복제를 방지하기 위해 구성된 단체이다. 1998년 조직되었으며 1999년 DTCP1.0, 2003년 DTCP v1.3을 발표하면서 기존의 1394/USB가 아닌 IP환경에서도 불법복제를 방지하는 규격을 발표하였다[6].

이 규격은 DTLA(Digital Transmission Licensing Administrator)에서 라이센스를 관리하는데 규격의 주요 내용은 아래와 같다.

- Device Authentication & Key Exchange
- Copy control Information
- Content Encryption
- System Renewability Message



(그림 2) DTCP 디바이스 구성도 및 콘텐츠 보호방법

DTLA는 2003년 DTCP-IP에 대한 규격을 작성한 뒤 IEEE1394/USB 외에도 인터넷에 연결되는 Device에 대한 Contents보호 방안을 만들고 업체들을 중심으로 활동중이며 UPnP 및 DLNA그룹에서도 A/V Data의 전송보호 대책으로 DTCP-IP를 선택하고 있다[7][8].

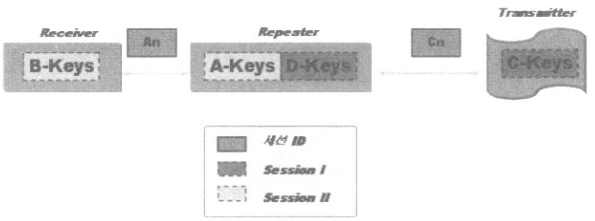
2.3 HDCP

HDCP(High-bandwidth Digital Content Protection)는 DVI/HDMI와 같은 High-bandwidth interface를 통해 Digital Display로 전달되는 audio/video content의 복제를 방지하기 위하여 Intel이 발표한 기술이다. DCP (Digital Content Protection) LLC에서 라이센스를 관리하고 있으며, 2003년 1.1 Revision을 발표한 상태이다[9].

HDCP 규격의 주요 내용은 아래와 같다.

- 장치 인증 프로토콜
- Revocation
- HDCP Encryption (ESSS for HDMI/DVI, OESS for DVI, SHA-1, HDCP Cipher)

HDCP는 Receiver, Transmitter와 이 둘을 동시에 가지고 있는 Repeater가 존재한다. Receiver와 Transmitter사이에 repeater가 존재할 수 있는데 각각의 송신/수신 모듈은 Session ID와 DCP LLC에서 할당해 주는 Key Selection Vector를 기반으로 장비가 Binding 될때 키교환을 통하여 장비들끼리 서로 인증 및 통신용 키를 생성하고 HDCP Encryption 방식에 의하여 암호통신을 하게 된다[9].

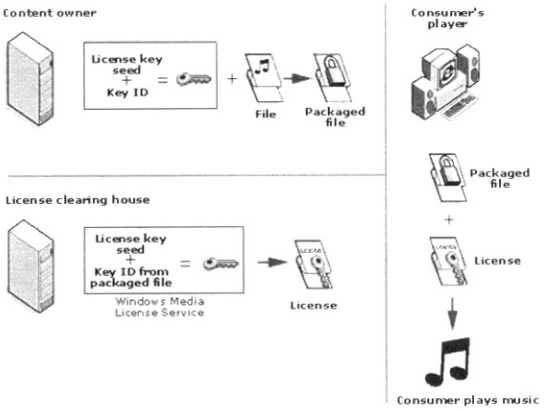


(그림 3) HDCP의 구조

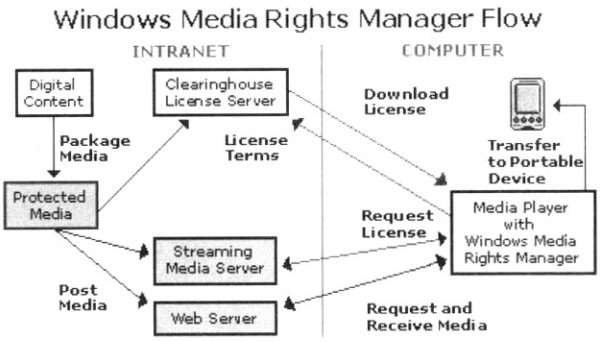
2.4 Microsoft's Windows Media DRM

Microsoft's windows Media DRM은 아래 그림과 같이, 콘텐츠 소유주, 라이센스 발행자, 소비자 세주체의 상호작용에 관여한다. Windows Media Right Manager는 Microsoft DRM에서 가장 핵심적인 기능을 담당하는데, 기본적으로 패키징(Packaging), 유통, 라이센스 발급, 라이센스 획득, 콘텐츠 사용의 순서에 따라 프로세스가 진행된다[10].

Microsoft DRM에서는 라이센스가 Media가 각각 분리되어 배포되면, 라이센스의 변경이 쉽고, 대여 혹은 회원제 형태의 모델을 적용하거나, 프리뷰(Preview)의 제한, 투명한 라이센스 발급, 휴대용 SDMI장치에 대한 전송 통제들의 세부기능이 있다.



(그림 4) MicroSoft DRM개요



(그림 5) MicroSoft DRM Process

Microsoft DRM은 개별 프로그램이나 PC혹은 단말기와 같은 장치위주로 구성되어 있고, DRM을 구성하는 여러 가지 프로세스 중에서 '패키징-라이센스 발급 사용'에 초점을 두고 있다. 하드웨어 ID를 이용한 유일한 DLL을 사용하여 사용자의 컴퓨터와 바인딩하는 개별화(Individualization)나, 운영체제, 사운드 카드, 드라이버를 통해서 음악파일을 관리하는 SAP, 운영체제의 커널 수준에서 작동하는 Protected Content Manager Exclusion등의 요소는 Microsoft DRM기술이 운영체제와 컴퓨터, 단말기 등의 장치 위주의 관리에 집중하고 있음을 보여준다. Microsoft DRM은 콘텐츠의 소유주가 패키징을 하여 유통시킨 후, 이에 대한 라이센스 발급과 소비자 사용에 대한 기술로만 구성되어 있다. 그러나 2006년 9월 MS-DRM에 "FairUse4WM"과 같은 프로그램으로 MS-DRM으로 만들어진 디지털 미디어 콘텐츠가 Crack한 사례가 언론에 크게 보도 되기도 하였다.

3. 디지털 콘텐츠 및 플레이어 보호방식 제안

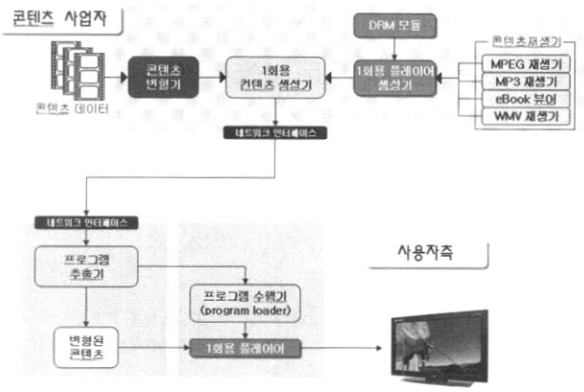
디지털 콘텐츠의 저작권 보호를 위한 시스템들의 주 관심분야는 콘텐츠 자체를 암호화 하는 방식과 콘텐츠의 내용을 보호하면서 전송하는 방식, 플레이가 가능한 장치의 인증에 대한 부분으로 크게 나눌 수 있다.

본 논문에서는 콘텐츠와 플레이가 될 장치에 대한 규격을

두어서 디지털 콘텐츠의 저작권을 보호할 수 있는 방법에 대하여 연구 하였다.

3.1 시스템 개념 및 구조

시스템의 구성요소는 아래 그림과 같다.



(그림 6) 시스템 주요 구성 요소

- 콘텐츠 생성기
- 콘텐츠를 대칭키를 통하여 암호화한다.
- 인스턴스 플레이어 생성기
- 사용자의 운영체제와 재생할 디지털 콘텐츠의 종류를 고려하여 플레이가 가능한 인스턴스 플레이어를 생성하고 사용자의 공개키를 이용하여 암호화 한다.
- 프로그램 수행기
- 네트워크를 통하여 전송받은 인스턴스 플레이어와 콘텐츠에 대하여 먼저 사용자의 개인키로 인스턴스 플레이어를 복호하고 플레이어에 내장되어 있는 대칭키를 사용하여 암호화된 디지털 콘텐츠를 복호화 한다. 복호된 인스턴스 플레이어는 DRM의 정보에 따라 동작한다. DRM 권한이 만료가 되면 인스턴스 플레이어기는 자동으로 시스템에서 삭제된다.

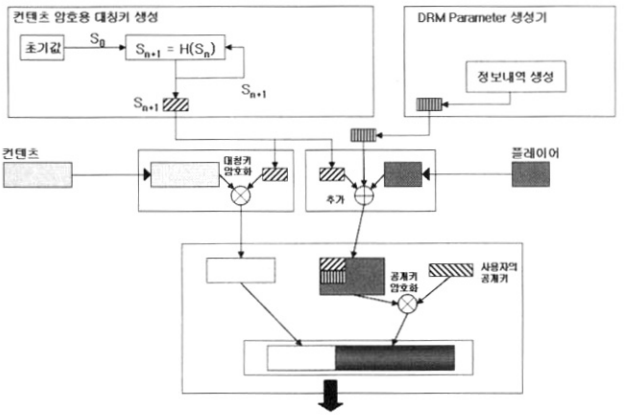
3.2 콘텐츠 보호 및 인스턴스 플레이어 설계

콘텐츠의 암호화는 VOD나 실시간 서비스를 하고자 하는 시스템에서 초기 Random Number(S_0)를 생성하여 그 값을 Hash Function을 사용하여 Sn+1을 생성하며 Sn+1을 다음 생성할 Sn+2의 Hash Function의 인자로 사용한다.

$$Sn + 1 = HashFunction(Sn)$$
$$EC = DE(Sn+1)$$

Sn : Hash Function의 인자
Sn+1 : Hash Function의 결과물
EC : 암호화된 Content
DE : 대칭키 암호화 함수

인스턴스 플레이어 생성기에는 DRM Parameter 생성기에서 생성한 DRM정보, 콘텐츠 암호화에 사용했던 Sn+1 과



(그림 7) 시스템 기능 구성도

그리고 실제 Binary Code로 되어 있는 플레이어를 붙여서 인스턴스 플레이어를 생성한다. 생성된 인스턴스 플레이어는 사용자의 공개키를 가지고 암호화 되어 네트워크를 통하여 소비자에게 전송한다.

이때 플레이어는 공개키로 암호화 되지만 디지털 콘텐츠는 대칭키로 암호화 된다. 이것은 공개키로 암호화하는 플레이어는 사람이 콘텐츠를 전송 받기 이전이므로 일정 수준의 생성지연이 있을 수 있지만, 한번 전송이 시작된 콘텐츠에 대해 복호지연이 있을 경우 플레이어의 성능에 문제가 될 수 있기 때문에 콘텐츠 자체는 대칭키로 암호화 한다. 일반적은 대칭키로 암호화 하는 것이 공개키로 암호화 하는 것보다 성능상으로 적은 지연이 발생하기 때문이다[12].

$$EPlayer = Pub_{user}(Dp|| Sn+1||Player)$$

EPlayer : 암호화된 1회용 플레이어
Pub_{user} : 사용자의 공개키를 이용한 함수
Dp : DRM Parameter
Sn+1 : Hash Function의 결과물
Player : 해당 콘텐츠를 플레이 할 수 있는 플레이어

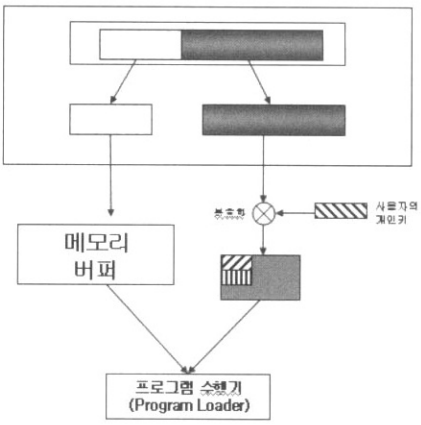
이러한 방식은 DTCP나 HDCP에서 하는 것과 같이 통신 세션이 형성 되었을 경우 동적인 키교환이 필요 없기 때문에 키교환 시 도청당해도 별도의 보안대책 없이 운영이 용이하게 된다.

3.3 Player 복호 및 프로그램 수행기 설계

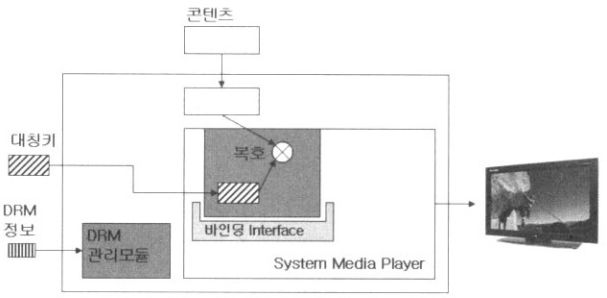
전송받은 콘텐츠는 EC부분과 EPlayer부분으로 분리하여 EC는 메모리 버퍼로 옮기고 EPlayer는 사용자의 개인키로 복호화 하여 프로그램 수행기(Program Loader) 로 전송하게 된다.

프로그램 수행기에서는 아래와 같은 역할을 한다.

- DRM 정보에 대한 처리
- 사용자의 개인키를 이용하여 복호화된 인스턴스 플레이어에서 추출한 대칭키로 콘텐츠를 복호화



(그림 8) 콘텐츠 플레이 방식



(그림 9) 프로그램 수행기 구조

- 인스턴스 프로그램이 만약 온전한 Player를 내장하고 있으면 Player를 구동하여 콘텐츠를 Play하지만 MS-Windows와 같이 Direct Show Filter들을 지원하는 플랫폼에 대해서는 Direct Show Filter에 Binding 할 수 있는 Interface가 제공되어야 한다.

위와 같은 방식으로 플레이를 마친 플레이어는 DRM의 정보에 따라 자신이 Expire될 시점에서 자동으로 삭제되게 된다. 만약 콘텐츠를 1회만 시청하게 권한 설정이 되었다면 1회 시청 이후에는 플레이어가 자동으로 삭제되게 된다.

3.4 제안된 기술의 분석

CPPM/CPRM은 콘텐츠를 암호화 함으로써, DTCP는 전송시 키교환을 통하여 전송되는 콘텐츠를 보고하는 것으로, HDCP는 특정 하드웨어서 전송되는 콘텐츠를 보호하기 위하여 제안된 기술들이다. MS-DRM은 콘텐츠를 공개키로 암호화하고 CCI나 암복호의 모든 과정은 운영체제와 밀접하게 연결되어 동작한다. 그러나 위의 기술들은 아래와 같은 문제가 있다.

- CPPM/CPRM나 HDCP의 경우에 Key Vector를 알고 있는 경우에는 모든 Media가 Crack당할 수 있다.
- DTCP의 경우 Key Exchange를 도청 당할 경우 Media전체를 도청하여 Crack할 수 있다.
- MS-DRM의 경우 License confirm중에 DRM정보가 유출되는 것이 실제 문제가 되었다

본 논문에서는 Player자체를 암호화 함으로써 사용자가 자신의 의지대로 Player를 수정하여 디지털 콘텐츠의 암호화를 무력하게 하는 것을 방지하는 효과가 있다.

<표 1>에서 보이는 것과 마찬가지로 제안된 기술은 아래와 같은 장점이 있다.

- 콘텐츠를 암호화 할 때 Hash의 결과로 나온 값을 키로 사용하기 때문에 동일 콘텐츠라 하더라도 같은 플레이어로 플레이를 할 수 없다.
- DTCP와 같이 키가 콘텐츠 전송시에 결정되는 것이 아니기 때문에 키를 도청당하지 않는다.
- 플레이어의 수명이 다하면 자동으로 삭제 되기 때문에 사용자가 콘텐츠를 암호화하는 대칭키를 capture할 수 없다.
- CCI및 플레이어의 모습이 Loader에 의하여 은닉되므로 외부 공격으로부터 CCI및 플레이어를 보호 할 수 있다.

4. 결 론

본 본문에서는 VOD나 인터넷 방송과 같은 서비스 환경에서 디지털 콘텐츠의 저작권을 보호하기 위하여 콘텐츠를 암호화 하고 암호에 사용된 키를 플레이어 및 DRM과 합성하여 사용자의 공개키를 이용하여 암호화 하고, 콘텐츠 및 합성된 인스턴트 플레이어를 다운로드 받아 사용자의 개인키로 복호화 하고 각 요소를 추출한 뒤 시스템 플레이어 환경에 맞게 바인딩하여 플레이하는 방법을 제안한다. 이러한 디지털 콘텐츠 들은 각 콘텐츠의 제작사, 콘텐츠를 서비스하기 원하는 사업자의 비즈니스 모델과 밀접한 연관이 있기 때문에, 실제 상용화하여 사용하기 위해서는 전체 구성이 간단하고 사용자에게 쉽게 서비스할 수 있는 방안이 있어야 하는데, 본 논문의 방법은 특별한 하드웨어 장치 없이 기존의 공개키 기반 시스템에 연동되어서 서비스가 가능하기 때

〈표 1〉 각 기술별 콘텐츠 암호 및 플레이어 보호 비교

기술명칭	콘텐츠 재전송시	Player 구성	Player보호 방안
CPPM/CPRM	매번 같은 키 사용	H/W Player	별도의 보안대책 없음
DTCP	매번 다른 키	H/W, S/W Player	별도의 보안대책 없음
HDCP	매번 같은 키 사용	H/W Player	별도의 보안대책 없음
MS-DRM	사용자의 공개키	S/W Player	OS에 의하여 보호됨
제안기술	매번 다른키	S/W Player	공개키 및 프로그램 수행기에 의하여 보호됨

문에 그 의의가 있다고 할 수 있다. 향후 이러한 서비스를 하기 위해서는 DRM 관리 모듈, 사용자 관리 등의 시스템들이 같이 연동되어서 운영되어야 실제로 완벽한 서비스가 가능할 것으로 보인다.

본 논문의 기술은 MS-DRM과 같이 PKI내용 중 키 분배 관련된 내용만 존재하는 형태가 아닌 키의 생성 및 소멸까지의 생명주기를 가지는 PKI 시스템과의 연동되는 것이 바람직하다. 그리고 현재는 S/W구성이 되어 있는데 이것을 H/W Player를 사용하는 경우에 H/W Player의 일정부분을 S/W로 변경하여 공개키로 암호화 하는 것에 대한 연구가 이루어져야 한다.

참 고 문 헌

[1] Frank Hartung, Friedhelm Ramme, "Degital Rights Management and Watermarking of Multimedia Content for M-Commerce Application," IEEE Communications Magazine, pp.78-83, November, 2000.

[2] Marc. A. Kaplan,"IBM Cyptolopes, SuperDistribution and Digital Rights Management", http://www.research.ibm/com/people/k/kaplan/cryptolop-docs.crypap.html

[3] Olin Sibert, "DigiBox: A Self-Protecting Container for Information commerce," 1st USENIX Workshop On Electronic Commerce, 1995.

[4] http://www.4centity.com/tech/cprm

[5] http://www.4centity.com/docs/version.html

[6] http://www.dtcp.com

[7] http://www.dlna.org

[8] http://www.upnp.org

[9] http://www.digitial-cp.com

[10] http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx

[11] Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria," DOD 5200.28-STD, December, 1985.

[12] 강주성, 박상우 외, "현대암호학", 한국전자통신연구원, 2000.

류 석

e-mail : ryusk@etri.re.kr

1998년 충남대학교 컴퓨터공학교육학과(학사)

2000년 충남대학교 컴퓨터공학과(석사)

2000년~2002년 ㈜해동정보통신 선임연구원

2003년~2004년 ㈜삼성전자 선임연구원

2005년~현재 국가보안기술연구소 연구원

관심분야 : 컴퓨터통신보안, Embedded System, 실시간 운영체제