휴대용 디지털 오디오 기기에서의 DRM 적용에 관한 연구

조남규* · 이동휘* · 이동춘** · 김귀남* · 박상민***

요 약

인터넷의 보급과 더불어 디지털 콘텐츠도 다양한 경로를 통해 보급 및 사용되고 있다. 그러나 디지털 콘텐츠는 속성상 아날로그 콘텐츠와 달리 쉽고, 빠르게 복사할 수 있으며 복제품은 원본에 비해 질적인 저하가 없으며 더 나아가 사용자들의 무료 선호 인식과 더불어 콘텐츠의 불법 복제 및 비정상적인 유통 문제를 야기시키고 있다. DRM(Digital Right Management)은 이러한 디지털 콘텐츠에 대한 불법 복제 및 불법 유통을 방지 또는 억제하기 위한 기술이라고 할 수 있다.

최근 콘텐츠 저작권 보호를 위한 기술인 DRM(Digital Right Management)은 기존의 PC 환경에서 이루어지던 콘텐츠 활용기술이 휴대용 기기에 기술의 성장으로 휴대용 기기에서의 DRM 적용이 요구되어 왔다 많은 등의 많은 표준화 기구와 많은 DRM 서비스 회사들에 의해서 여러 가지 서비스 모델이 제안되어 왔으며 기존의 PC 환경과 달리 휴대용 디지털 오디오 기기는 프로세스/네트워크 제약으로 기존의 PC DRM의 모델을 그대로 적용하기 어려우며 DRM 적용을 위해 고사양의 H/W사양이 요구되고 있다. 본 논문에서는 현재 많은 디지털 휴대용 오디오 기기에 사용되는 저성능 기기에 적용이 적합하도록 DRM 서비스 모델을 제시하였으며 기기의 내부 메모리 구조 타 DRM 서비스의 호환성을 위해 서비스 변환 서버인 DFCS를 제안하여 저성능 프로세스를 사용한 디지털 휴대용 오디오 기기의 보안성 및 편의성을 증가시켰다.

Study of DRM Application for the Portable Digital Audio Device

Nam Kyu Cho* · Dong Hwi Lee* · Dong Chun Lee** · Kuinam J. Kim* · Sang Min Park***

ABSTRACT

With the introduction of sound source sharing over the high speed internet and portable digital audio, the digitalization of sound source has been rapidly expanded and the sales and distribution of sound sources of the former offline markets are stagnant. Also, the problem of infringement of copyright is being issued seriously through illegal reproduction and distribution of digitalized sound sources. To solve these problems, the DRM technology for protecting contents and copyrights in portable digital audio device began to be introduced. However, since the existing DRM was designed based on the fast processing CPU and network environment, there were many problems in directly applying to the devices with small screen resolution, low processing speed and network function such as digital portable audio devices which the contents are downloadable through the PC. In this study, the DRM structural model which maintains similar security level as PC environment in the limited hardware conditions such as portable digital audio devices is proposed and analyzed. The proposed model chose portable digital audio exclusive device as a target platform which showed much better result in the aspect of security and usability compared to the DRM structure of exiting portable digital audio device.

Key words : DRM, Portable Digital Audio Device

* 경기대학교 정보보호학과
** 광운대학교 산학협력단
*** 인천대학교 산업경영학과

1. 서 론

고속 인터넷 망을 통한 음원 공유 및 휴대용 디지털 오디오 기기의 출현으로 음원의 디지털화는 급속도로 확산되었으며 이에 기존 오프라인을 통해 이루어지던 음원 판매 및 유통 서비스시장이 침체되고 디지털화된 음원의 불법 복제 및 유통으로 저작권에 관한 침해가 심각하게 대두되었다. 이러한 문제점을 해결하기 위해 휴대용 디지털 오디오 기기에서의 콘텐츠와 저작권보호를 위해 DRM 기술이 도입하기 시작하였다.

그러나 기존의 DRM은 빠른 프로세싱의 CPU와 네트워크 환경을 기반으로 설계되었기 때문에 PC를 통해서만 콘텐츠을 다운로드 받는 디지털 휴대용 오디오 기기와 같이 작은 화면의 해상도, 낮은 프로세싱 속도와 네트워크 기능이 없는 기기에 그대로 적용하기에는 많은 문제점을 가지고 있다.

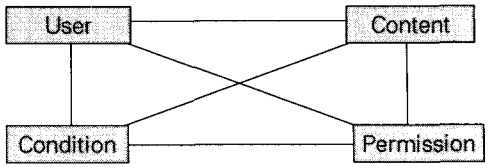
본 논문에서는 휴대용 디지털 오디오 기기와 같은 하드웨어적인 한계 상황에서도 PC 환경에 근접한 보안 강도를 유지하는 DRM 구조 Model을 제안하고 분석한다.

2. DRM 모델 관련 연구

DRM(Digital Rights Management)을 정의하기란 그리 쉽지 않지만, 일반적으로 "디지털 콘텐츠의 불법유통과 복제를 방지하고, 적법한 사용자만이 콘텐츠를 사용케 하며, 과금 서비스 등을 통하여 디지털 콘텐츠 저작권을 관리하는 기술"로 설명할 수 있다[1].

DRM을 구성하는 가장 기본적인 네 가지 핵심 요소는 user, content, permission, condition이며, 이들 구성 요소들간의 연관 관계는 (그림 1)과 같다.

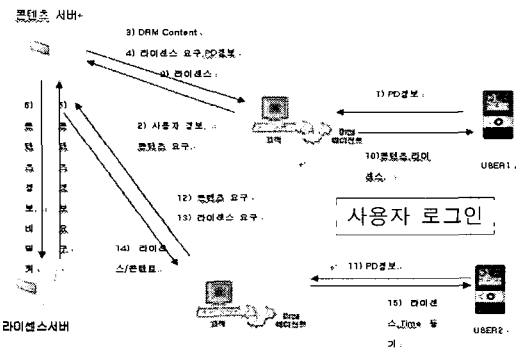
이들 핵심 요소들 간의 연관성은 콘텐츠의 생명주기가 사라지지 않는 한 지속적으로 보호(persistent protection)될 수 있어야 하며, 시스템적으로



(그림 1) DRM 기본 구성 요소들의 연관성

처리 가능하도록 기술(descriptive) 가능하여야 한다. 또한 명시된 권리(rights)에 따라서 콘텐츠가 통제(rights enforcement)될 수 있어야 한다[2].

각 서비스 회사에 따라 구조가 다르지만 일반적으로 DRM을 적용하기 위해 (그림 2)에서와 같은 시스템 구조로 되어 있다.



(그림 2) 휴대용 디지털 오디오 기기(PD)에 적용된 일반적인 DRM 구조

PD에 DRM 서비스 모델 적용을 위해서는 기기 내부의 DRM 관련 프로그램과 기기내부 메모리 의 구조가 DRM 적용을 위해 적합하게 되어 있어야 하며 일반적은 PD는 네트워크 기능이 없고 PC를 통해 DRM 콘텐츠 전송이 이루어짐으로 PC DRM Agent가 필요하다.

소비자가 DRM 콘텐츠 이용시 PC DRM Agent를 통하여 승인 및 과금후 DRM 콘텐츠 요구시 콘텐츠 서버에서 라이센스와 같이 패키징된 콘텐츠를 받아 기기에서 플레이 할 수 있으며 휴대용 디지털 오디오 기기의 내부에서 DRM 콘텐츠 사용을 위해서는 내부 메모리에 DRM을 위해 공간

이 필요하다[6].

기기내부에서 메모리 에서는 DRM Manager와 콘텐츠 와 라이센스 획득시 필요한 정보를 저장하고 있어야 한다.

기기내부의 이러한 영역들은 일반 사용자가 접근할 수 없게 숨김 영역으로 되어 있으며 암호화 기법의 DRM과 워터마킹 기법의 DRM에 따라 메모리 내부구조 및 적용된 하드웨어 성능의 차이가 있다.

또한 위와 같이 휴대용 디지털 오디오 기기의 DRM 적용시 프로세스와 네트워크 제약으로 PC DRM의 모델을 그대로 적용하기 어려우며 강력한 보호를 위한 DRM 적용을 위해 고사양의 하드웨어 사양이 요구되고 있다.

본 논문에서는 현재 많은 디지털 휴대용 오디오 기기에 사용되는 저성능 기기에 적용이 적합하도록 DRM 서비스 모델을 제시하였으며 기기의 내부 메모리 구조 타 DRM 서비스의 호환성을 위해 서비스 변환 서버인 DFCS를 제안 하여 저성능 프로세스를 사용한 디지털 휴대용 오디오 기기의 보안성 및 편의성을 증가시킬 것이다.

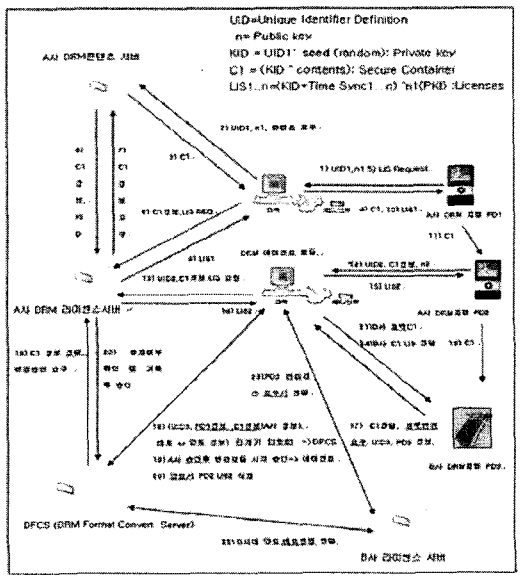
3. 제안된 디지털 휴대용 오디오 기기의 DRM 구조

본 논문에서는 일반적인 휴대용 디지털 오디오 기기의 DRM의 문제점을 해결하기 위한 Model을 제안한다 제안된 Model을 DPAD_DRM라고 명명하기로 한다.

제시한 DRM 모델 구조는 (그림 3)과 같이 구성되어 있다.

콘텐츠 서버에 저작물이 등록되어 있고 PD 사용자는 DRM Agent을 이용하여 콘텐츠 서버에 콘텐츠을 요청한다.

제안된 DRM 모델 에서 사용자의 편의성을 도모하기 위해 사용자의 기기들 중 서로 다른 DRM 서비스 기기를 위해 DRM 콘텐츠 변환 서버(DFCS : DRM Format convert sever) 및 PC DRM Agent에 변환모듈을 제안하였고 이를 이용하여 다른 DRM 서비스를 제공하는 디지털 휴대용 오디오 기기에 콘텐츠 컨테이너(Cn)를 배포시 콘텐츠 변환 후 기존 타기기의 라이센스를 그대로 변환후 양도 및 배포하여 사용할 수 있게 제안하여 진정한 Super Distribution 기능이 가능하도록 제안하였다.



(그림 3) 개선된 DRM 구조

3.1 기기 정보 전달 방식 및 key 생성 방식

콘텐츠 요청시 사용자정보가 전달되지 않고 PC-Agent를 통해 기기의 메모리 내부의 물리적인 Secure 영역에 저장되어 있는 UID와 공개키가 전달된다.

콘텐츠 서버에 전달된 PD-UID(Portable Device Unique Identifier Definition)로 패키징 암호키를 만들며 만들어진 비밀Key는 KID로 표시되며 KID는 비밀키로 Contents를 암호화할 때 사용하며 기기의 공개키는 라이센스를 획득시 라이센스를 암호화하기 위하여 사용한다.

3.2 콘텐츠 패키징

콘텐츠의 패키징 방식은 저 성능 프로세스 솔루션을 위해 암호화 방식을 사용하였으며 패키징된 컨테이너 내부는 제시한 모델에서 표시한

$$Cn = (KID \wedge Content + Info)$$

으로 나타내고 Cn내부는 Content, UID, Metadata, Encrypted Content, Signature, 저작권 소유자 정보, 콘텐츠 배포형식, 콘텐츠 장르, 라이센스 서버 URL, 배포 횟수 제한 등으로 이루어져 있어 콘텐츠 배포시 에는 다른 기기에서 콘텐츠 컨테이너 내부의 Cn정보(Data와 Signature)를 DRM Agent를 통해 라이센스 서버에 전송되고 이 정보를 이용해 라이센스 서버에서는 배포된 콘텐츠의 지속적인 추적이 가능하다.

3.3 라이센스 획득

PC DRM Agent를 통해 패키징된 콘텐츠을 디지털 휴대용 오디오 기기에 내부메모리에 저장하고 라이센스 서버에 라이센스를 획득 후 기기에 전달한다. 기존 디지털 휴대용 오디오기기에서는 DRM 콘텐츠 와키기 한번에 패키징되어 내려 받아 사용하였으나 제안된 시스템은 DRM 콘텐츠 서버에서 기기별 고유의 콘텐츠 컨테이너

$$Cn = (KID \wedge Content + Info)$$

을 기기에 저장 후 PCDRM Agent을 통해 DRM 라이센스 서버에 디지털 휴대용 오디오 기기 내부의 콘텐츠 컨테이너의(Cn) 정보를 전달하고 라이센스를 요구하게 되면 콘텐츠 정보를 보고 요청기기를 확인 후 콘텐츠 서버에서 기기의 공개키을 받아 라이센스를 암호화하여 전달함으로 기존의 평문요청 시스템에서 문제되었던 보안문제와 기기 및 사용자정보가 노출되지 않고 기기고유의 라이센스 획득 및 추후 필요시 라이센스를 따로 획득할 수 있는 안전 및 편의성이 향상된 DRM 모델을 제안하였다.

라이센스 내부는

$$LIS = \{(KID \wedge Timesync) \wedge n(pki)\}$$

크게 공개키로 비밀키와 라이센스로 나누어져 암호화되어 있고 Time Sync는 만료시간설정과 재생 횟수 설정에 있는 타임정보를 전달함으로 기존에 문제되었던 Time 정보 Roll-Back시 콘텐츠의 횟수 및 시간제한을 무력화시킬 수 있는 문제를 보완하고 배포제한 회수정보는 콘텐츠 패키징시 사용자 설정하여 컨테이너(Cn) 안에 같이 다운받음으로써 라이센스 획득없이 사용자의 배포 회수 제한이 가능하며 라이센스는 만료시간 횟수제한을 관리함으로 일반적인 콘텐츠 헤더 공격으로 인한 무력화에 대비하였다.

3.4 DFCS (DRM Format Convert Server)

사용자가 여러 가지의 디지털휴대용 오디오 기기를 사용할 경우 기존에는 A사 DRM 서비스를 제공하는 기기에서 B사 DRM 서비스를 사용하는 기기로의 콘텐츠 배포 및 양도가 불가능하였으나 제안된 시스템은 콘텐츠 호환이 가능하게 PC DRM Agent 통해 DFCS(DRM Format Convert Server)에 패키징된 콘텐츠를 B사 DRM의 포맷으로 파일 변환을 요청하면 UID3, 디지털 휴대용 오디오 기기3정보, 콘테츠 컨테이너(Cn)정보, 양도 및 배포 정보를 DFCS로 전달하고 DFCS는 B사 라이센스 서버에 승인을 얻어 PC DRM Agent 내부에 있는 Tamper resistant module area에 DRM-FCTRM (DRM Format Convert Tamper resistant module)을 다운로드 후 콘텐츠 변환을 수행한다. 변환된 패키징된 Cn을 B사 DRM 지원 기기에 배포 및 양도하고 라이센스 획득시 PC DRM Agent을 통해 B사 지원기기 정보를 B사 라이센스서버에 전달 B사 라이센스 정보를 요청하고 B사 라이센

스 서버는 DFCS로 부터 받은 배포 또는 양도 정보를 분석하여 B사 DRM 기기를 위한 라이센스를 전달 한다. 이와 같이 사용자가 가지고 있는 여러 다른 기기들에서 사용자가 구입한 콘텐츠를 사용 가능한 DRM 구조가 다른 기기간의 콘텐츠 호환성을 가질 수 있는 DRM 구조를 제안하였다.

4. 제안모델 분석

4.1 보안적 측면

4.1.1 사용자 정보 및 기기 정보 보안성 측면

사용자가 콘텐츠 서버에 콘텐츠 요청시 기존에는 사용자 정보와 기기정보를 평문으로 전달하여 네트워크상이나 사용자 PC에 쉽게 노출되어 콘텐츠 보안과 개인 정보 보안에 문제가 발생하였으나 제안된 시스템은 기기의 고유 UID와 공개키, 콘텐츠 요구사항만을 PC Agent를 통하여 전달하여 사용자 개인 정보 유출의 위험이 줄어들며 콘텐츠 서버는 PC Agent을 통해 전달되는 기기정보를 통해 콘텐츠을 패키징함으로 보다 안전한 콘텐츠 요구를 구현하였다.

4.1.2 실험1

Condition :
PD(main chip : Turbo 8051+DSP(MP3 전용)
PC(Pentium4(1.7GB), OS Window XP)
Interface USB port
PD Memory : NAND Flash

- 일반적인 시스템의 콘텐츠와 라이센스 정보의 네트워크나 DRM Agent에서 사용자 정보 전달 과정 해킹시 아래와 같이 사용자 ID와 기본 정보가 오픈된다.

User Name : Simon Cho/
private information
Device information : A Company/
Device Name/ID

- 제안된 시스템의 콘텐츠와 라이센스 정보의 네트워크나 DRM Agent에서 사용자 정보해킹시 아래와 같이 암호화된 상태로 보여줌으로 해킹된 정보 추가 해킹 및 정보이용 용이하지 않는다.

- 콘텐츠 요청
UID : 12345123400123456789
PublicKey : dVBDs1Af1cE05qoPxXIRj482cASM1NSCkAbv7o80a1H1yuQRfOdzZQ =
위와 같이 해킹이 되어도 UID와 공개 Key값만 표시됨으로 사용자 개인 정보의 노출위험과 기기 정보의 확인이 어렵다.

4.2 라이센스 획득 및 지속적 관리 측면

콘텐츠 컨테이너(Cn) 정보만을 라이센스 서버에 전달하여 보안상 문제가 되었던 라이센스 획득시 정보 유출 문제를 보안하였으며 라이센스 서버는 콘텐츠 컨테이너(Cn) 정보를 콘텐츠 서버로부터 확인 및 기기정보를 획득함으로 고유 기기에 대한 라이센스를 PC DRM Agent를 통해 기기에 전달할 수 있으며 같은 DRM 서비스를 지원하는 A기기에서 B기기로 콘텐츠 전달시 B기기에서는 전달된 콘텐츠 컨테이너(Cn)의 정보와 B기기의 UID를 라이센스 서버에 전달하여 다시 라이센스 획득을 함으로 라이센스 서버는 최초 배포자와 전달된 기기의 정보를 모두 획득하여 사용자의 정보 유출없이 지속적인 콘텐츠 의 추적 및 관리가 가능하다.

4.2.1 콘텐츠 컨테이너(Cn)

Cn = (KID ^contents) : Secure Container
KID = UID^ seed : Private Key(UID = Unique Identifier Definition)

4.2.2 라이센스 획득

n = Public Key
LIS1.. n = (KID+Time SynCn … n) ^n1(PKI) : 라이센스

Cn의 최초 Content Container 요구 기기의 UID 가 내포되어 있고 라이센스 요청시 지속적인 기기UID 가 추가되어 콘텐츠 사용의 추적 및 관리 가능하다.

4.3 제안된 내부 메모리 구조의 보안성 측면

제안된 내부 메모리 구조에서는 물리적 시큐어 영역에 UID을 사용함으로 임의로 메모리 Low Format 이나 수정으로 변경할 수 있었던 UID 정보를 원천적으로 불가능하게 하여 고유기기의 저장된 콘텐츠의 불법 사용을 보호하였으며 논리적 히든영역에 시큐어영역을 추가하여 DRM Manager와 비밀키/공개키, Right List, 시큐어타임, 라이센스 정보 등을 두어 메모리 임의 접근하여 헤더 정보 수정으로 횟수/시간 제한 무력화나 키정보 획득 및 타임정보 Roll-Back 등의 문제되었던 부분을 등의 보안강화를 제안하였다.

4.3.1 실험2

Condition :
PD(main chip : Turbo 8051+DSP(MP3)
PC(Pentium4(1.7GB), OS Window XP)
Interface USB port
PD Memory : NAND Flash

- 기존 시스템(임의의 시리얼 번호 생성시켜 객체 식별자 사용 경우) : (그림 14)와 같은 시리얼 번호 (UID) 생성용 TOOL을 사용하여,
  VID : 2735
  PID : 5678
  UID :
  serial0 = 12345
  serial1 = 1234
  serial2 = 00123456789
  TOOL을 이용하여 PD_UID 영역에 저장시 장치 기기 인식후 USB장치 인식 프로그램에서 장치 확인후 ID 확인시 변경된다.

- 제안 시스템(저장 장치의 고유의 UID로 객체 식별자 번호 사용)
  내부메모리 구조가 개선된 시스템에서 동일하게 임의의 PD_UID 영역에 저장한다.
  저장 후 기기 PC 연결후 USB 장치 인식 ID 확인 결과 변경되지 않는다.
  VID : 0402
  PID : 5661
  UID :
  serial0 = 00000
  serial1 = 0000
  serial2 = 00000000000
  로 나타남 변경되지 않는다.

5. 결 론

본 논문에서는 휴대용 디지털 오디오 시스템에 보안 성 및 사용자 편의성을 위해 필요한 DRM 기술을 살펴보고 DRM 기술의 현황과 기존 DRM 서비스 구조와 PC DRM Agent 시스템 및 디지털 휴대용 오디오 기기의 문제점 및 제한사항을 객관적으로 도출하고 문제점을 개선할 수 있는 휴대용 오디오 기기의 환경을 고려한 최적화된 DRM 서비스 구조와 PC Agent 및 기기 내부 메모리 구조를 제안을 하였고 제안된 시스템이 보안성, 사용자 편의성 및 구현 측면에서 분석 및 평가해 보았다.

본 논문에서 제시한 서비스구조 및 시스템은 현재 대다수의 휴대용 디지털 오디오 기기의 환경인 저성능 프로세스와 네트워크 기능을 가지고 있지 않은 기기에서 더 낮은 보안성과 편리성을 가진다.

참 고 문 헌

[1] 오원근, DRM 표준화 및 평가기술 "전자통신 동향분석", 제20권, 제4호, 2005. 8.

[2] 강호갑, "DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구", 소프트웨어진흥원, 2004.

[3] 삼성 UID specification.

[4] 조경옥, DRM 시스템상에서 디지털 콘텐츠 보호를 위한 패키징 기법 설계.

[5] 이승제, OMA 표준화 동향 LG전자 이동통신기술연구소

[6] Markany, http://www.markany.co.kr

[7] Microsoft, http://www.microsoft.com/windows/windowsmedia/forpros/drm/components.aspx

[8] Intertrust, http://www.intertrust.com/main/overview/index.html

[9] intel, "Content Protection in the Digital Home", Vol. 06, No. 04, Intel Technology Journal, 2002. 11.

조 남 규

2000년 동양대학교 정보통신공학과(공학사)

2001년~현재 경기대학교 정보보호학과(공학석사)

2000년~현재 (주)디지털웨이 연구원

이 동 휘

2001년 경기대학교 전자계산학과(이학사)

2003년 경기대학교 정보보호기술공학과(공학석사)

현재 경기대학교 정보보호학과(박사과정)

이 동 춘

연세대학교 컴퓨터과학과 (공학박사)

현재 호원대학교 국방과학기술대학 학장

관심분야 : 이동/무선 통신, USN 및 보안

김 귀 남

미국 캔자스대학 수학과(응용수학사)

미국 콜로라도주립대학 통계학과(통계학석사)

미국 콜로라도주립대학 기계산업공학과(기계·산업공학박사)

현재 경기대학교 정보보호학과 주임교수

박 상 민

1970년 한양대학교(공학사)

1983년 한양대학교(공학석사)

1990년 한양대학교(공학박사)

2002년~현재 동북아전자물류연구센터 소장

현재 인천대학교 산업공학과 교수