사례 발표

Portable Device 환경에서 디지털 콘텐츠의 저작권 보호를 위한 임베디드 소프트웨어의 설계와 구현

신 동 환* 유 세 근** 최 종 욱***

목 차

1. 서 론

최근의 IT 기술은 마이크로프로세서의 가격이 낮아지고 소형화 및 고성능화가 진행됨에 따라 제품 경쟁력의 핵심이 하드웨어 생산 기술에서 소프트웨어 최적화 기술로 이동하는 변혁기를 맞이하여 임베디드 소프트웨어가 탑재된 상품의 가치가 하드웨어보다는 소프트웨어에 의해 좌우되는 기술 집약적 고부가가치 산업으로 발전하고 있다. 초창기 임베디드 소프트웨어는 간단한 제어 프로그램만으로 산업용 기기를 제어하는데 그쳤으나, 최근에는 멀티미디어 처리와 같은 점차 복잡한 기능을 위해 멀티태스크 및 네트워크 기능을 제공하는 임베디드 OS(Operating System)를 이용하고 있다[1][5].

이와 같이 임베디드 시스템의 발전으로 PD(Portable Device, 이동형 재생기)가 등장하여 디지털 콘텐츠를 이동하면서 이용할 수 있게 되었으며 고정된 플랫폼에서보다 이동하면서 디지털 콘텐츠를 소비하는 시간이 증가하게 되었다. 인터넷 기술의 발전과 초고속 인터넷 망의 확산에 따라서 누구나 손쉽게 디지털 콘텐츠를 인터넷을 통하여 얻을 수 있게 되었다. 디지털 음악인 경우 컴퓨터를 통해서도 음악을 듣지만 많은 사람들이 MP3P(MP3 Player)와 같은 전용 재생기기를 이용하고 있다. 본 고에서는 PD의 범위를 스스로 네트웍에 접속할 수 없으며 이동하면서 디지털 콘텐츠를 사용할 수 있는 장치로 한정한다. 최근의 MP3P는 단지 MP3 압축방식 외에 마이크로소프트사의 WMA압축방식, 공개소스 진영의 오디오 압축 코덱방식인 OGG도 모두 재생할 수 있는 구조로 변화되고 있다. 따라서 이동형 재생장치에서 소비될 수 있는 디지털 콘텐츠의 불법복제 및 재생을 막을 수 있는 기술에 대한 요구가 점증하고 있다. 콘텐츠 제공자가 안심하고 일반 사용자들에게 콘텐츠를 암호화하여 배포하고 정식으로 구매한 사용자만이 해당 콘텐츠를 이용할 수 있도록 하는 DRM(Digital Rights Management) 기술이 발전하게 되었다. 무선 이동통신 분야에서는 OMA(Open Mobile Alliance)를 중심으로 무선 DRM에 대한 표준 스펙 작업을 진행하고 있으며, 현재 Ver 2.0이 나와있다.

* ㈜마크텍 연구소장
** ㈜마크애니 컨텐츠사업실 실장
*** 상명대학교 소프트웨어학부 교수

본 고에서는 세계적으로 표준화가 진행되고 있는 OMA DRM의 구조를 살펴보고 DRM의 일반적인 특징을 제시한다. 또한 이와 환경이 유사한 PD를 위한 DRM 구조를 설명하고 현재 가장 대표적인 MP3 재생기를 대상으로 DRM 구현사례를 제시한다.

2. OMA DRM 구조

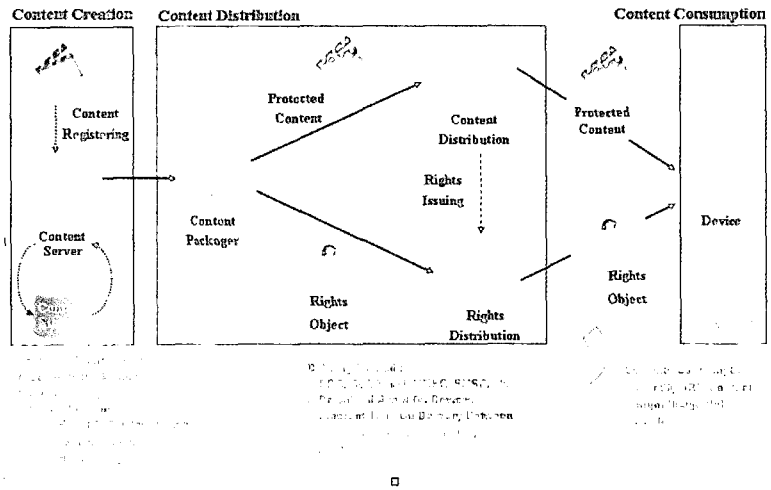
OMA DRM 1.0이 처음 논의가 된 시기는 2002년 1월이었으며, 최초 OMA DRM 1.0의 구조는 단순한 대칭키 구조의 단순한 보안 레벨에서 시작하여, 제한적인 모바일 단말기 환경에서 적합한 DRM 기술의 핵심적인 뼈대를 만들어 가는 과정을 중점적으로 고민해왔었다[3]. 그러나, OMA DRM Working Group 은 향후 Strong-End-to-End 의 보안 레벨 및 Streaming 과 같은 다양한 콘텐츠에 대해 DRM이 적용될 수 있는 환경을 이미 OMA DRM 1.0부터 고민해왔으며, 향후 OMA DRM 2.0의 전환에 필수적인 방법론에 대해 기본적인 요소를 구축해 왔다.

(그림 1)에서 보는 바와 같이 OMA DRM은 소비자가 구입한 콘텐츠를 적법하게 사용하기 위해서, 소비자는 Rights Issuer에 접속하여 사용권한(Rights Object)을 획득/구입해야 하는 기본적인 아키텍처를 제시한다[4]. 콘텐츠는 소비자에게 배포될 때 암호화되어 보호된 형태 (Protected Content)로 배포되며, 소비자는 암호화된 콘텐츠에 대한 적절한 사용 권한이 없으면 이 암호화된 콘텐츠를 사용할 수 없는 구조가 OMA DRM의 핵심이다.

OMA DRM 1.0에서 지원하는 콘텐츠 다운로드 방식은 Forward-Lock, Combined Delivery, Separate Delivery 세 가지로 분류한다. 여기에 Separate Delivery를 이용하여 만들어지는 Super-Distribution방식을 설명한다.

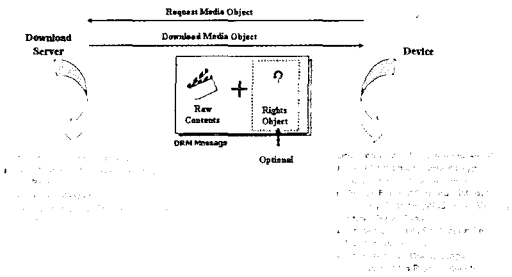
2.1 Forward-Lock 다운로드

Forward-Lock 전달 방식은 서비스 시스템 운영자에 의해 결정되며, 이 전달 방식 단말기로 다운로드된 원본 콘텐츠가 다른 단말기로 전달되지 않는다는 가정 하에 DRM 클라이언트에서 보호가 불필요하다. 또한 사용 권한은 선택적으로 전달되며, 사용 권한이 전달되지 않을 경우는 콘텐츠의 사용 제한이 없다. 여기서 네트워크 상의 원본 콘텐츠의 전달에 있어, 콘텐츠의 불법적 후킹(Message Hooking)은 단말기와 서버 사이 강한 신뢰관계를



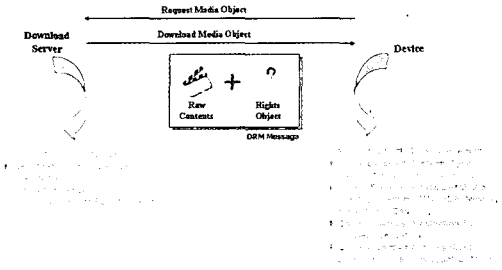
(그림 1) 콘텐츠 배포과정

유지하고 있기 때문에 불가능하다는 가정도 포함한다.



(그림 2) Forward-Lock의 콘텐츠 다운로드 방식

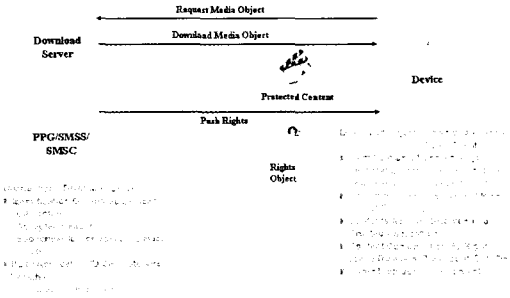
2.2 Combined Delivery 다운로드



(그림 3) Combined Delivery의 콘텐츠 다운로드 방식

Combined Delivery 전달 방식은 서비스 시스템 운영자에 의해 결정되며, 암호화 되지 않은 원본 콘텐츠와 콘텐츠의 사용 권한 정보가 포함되어 있는 Rights Object가 HTTP Multipart 로 구성되어 전달된다. Combined Delivery에서도 역시 원본 콘텐츠가 전달되기 때문에 콘텐츠는 외부 단말기로 전달되는 것은 허용하지 않는다. 사용 권한은 콘텐츠의 사용회수의 제한, 사용기간의 제한, 그리고 일정한 주기 내에서 사용을 허용하는 다양한 Constraint 정보를 포함하고 있으며, 또한 콘텐츠를 미리 다운로드 받고, 1회 미리 보기를 허용을 위해 1회 사용회수를 가지는 사용 권한을 같이 다운로드 받을 수 있다. 미리 보기가 끝나고, 다시 콘텐츠를 사용하고자 할 경우는 사용 권한은 사용정보가 없기 때문에 사용 권한을 다시 구매하는 과정을 거치게 된다.

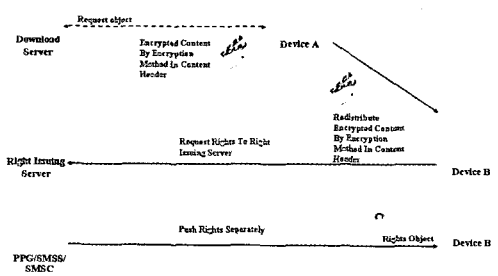
2.3 Separate Delivery



(그림 4) Separate Delivery의 콘텐츠 다운로드 방식

Separate Delivery는 서버에서 암호화되고 DCF 형태로 패키징된 콘텐츠와, 해당 콘텐츠의 사용 권한 정보를 담고 있는 사용 권한을 단말기로 다운로드 받기 위해 서로 다른 시간 또는 다른 채널을 통해 전달되는 방식을 의미한다. 콘텐츠 자체는 암호화되어 있기 때문에 콘텐츠를 복호화 하기 위한 CEK(Content Encryption Key)가 존재하지 않으면 단말기에서 사용되지 않기 때문에 반드시 소비자는 CEK가 담겨 있는 사용 권한의 구매를 통해서만 콘텐츠를 사용할 수 있다. 이에, 암호화되어 보호된 콘텐츠는 어떠한 채널을 통해서도 단말기로 전달되어도 무방하나, 사용 권한은 반드시 서버와 단말기 사이 신뢰된 채널(WAP/ HTTP Push)을 통해서만 전달되어야 한다. 또한 Combined Delivery와 마찬가지로 콘텐츠의 사용권한 정보에 따라 콘텐츠를 제어할 수 있고, 콘텐츠는 암호화되어 있어 다른 단말기로 전달될 수 있다. 이러한 콘텐츠에 대해 소비자는 미리 보기도 가능하며, 그리고 다른 단말기로 전달 받은 콘텐츠에 대해 DRM 클라이언트는 소비자로 하여금 사용 권한을 서버로부터 발급받을 수 있도록 유도할 수 있다.

2.4 Super-Distribution



(그림 5) Super-Distribution의 콘텐츠 다운로드 방식

Separate Delivery를 통해 전달된 암호화된 콘텐츠는 다른 단말기로 전달될 수 있는데 이를 DRM에서는 Super-Distribution이라 정의한다. 다른 단말기로부터 전달 받은 콘텐츠에 대한 사용 권한을 발급받기 위해서는 DCF Header 내 'RightsIssuer URL' 정보를 통해 Rights Issuing Server 로 접속하여, 해당 콘텐츠의 Content ID를 전달함으로써 사용 권한을 발급받을 수 있다. 발급된 사용 권한은 단말기와 서버사이의 신뢰된 통신채널을 통해 전달받으며, 대표적으로 Push Service를 통해 전달받게 된다.

3. PD DRM 구조 설계

3.1 임베디드 프로세서의 발전

PD DRM을 설계하기 위해서는 대상이 되는 PD의 시스템 사양을 이해하는 것이 중요하다. PD의 시스템 성능은 임베디드 소프트웨어가 탑재되는 임베디드 프로세서의 성능에 따라 좌우 된다. 초기에 PD에 내장된 임베디드 프로세서는 단순히 장치 내에 내장되어 주로 제어와 계산을 담당하며 주로 마이크로 컨트롤러의 기능을 수행하였다. 우선, 임베디드 프로세서를 비트수에 따라 분류해 보면 몇 년 전까지만 해도 8비트나 16비트가 주요 제품이었는데 최근 들어 32비트 이상되는 프로세서를 채택하는 고성능 시스템이 늘어가고 있는 추세다. 또한 프로세서에 메모리와 각종 보조회로들을 한 개의 칩에 탑재시켜 모든 기능을 제공할 수 있는 시스템 온 칩(SOC : System On a Chip) 기술이 발달하여 임베디드 시스템의 확산을 더욱 가속화시키고 있다. 특히 32비트 프로세서가 50% 이상 시장 점유을 기록하고 있다.

현재 PD의 대표적인 MP3재생기의 경우에도 50% 이상이 ARM코어를 기반으로 하는 임베디드 프로세서를 탑재하고 있다. 대부분의 경우 메모리, ADC(Analog Digital Converter), DAC(Digital-Analog Converter), USB 컨트롤러 등을 단일 칩 안에 내장하고 있는 형태로 공급되고 있다. 국내 MP3P에서 사용되고 있는 임베디드 프로세서는 모토롤러 코어를 갖고 있는 Sigmatel, ARM 코어를 내장하고 있는 Telechips, Phillips, Cirrus logic사에서 만든 프로세서가 주류를 형성하고 있다.

3.2 PD 시스템의 특성

초기의 오디오 PD는 디지털 압축된 음원 소스를 하드웨어적으로 디코딩할 수 있는 하드웨어 코덱을 갖고 있었다. 임베디드 프로세서의 기능이 낮고 MP3와 같이 단지 하나의 압축 형식만 지원해도 시장에서 환영받을 수 있었기 때문에 가능했다. 그러나 최근에는 다양한 압축형식의 지원을 소비자가 원하고 있다. 인터넷에서 서비스되고 있는 디지털 오디오의 경우 다양한 압축형식으로 제공되고 있기 때문이다. 이러한 욕구를 수용하기 위해서 하드웨어 압축코덱을 지양하고 소프트웨어 압축코덱을 선호하게 되었으며 고성능의 임베디드 프로세서를 PD에서 사용하게 되었다.

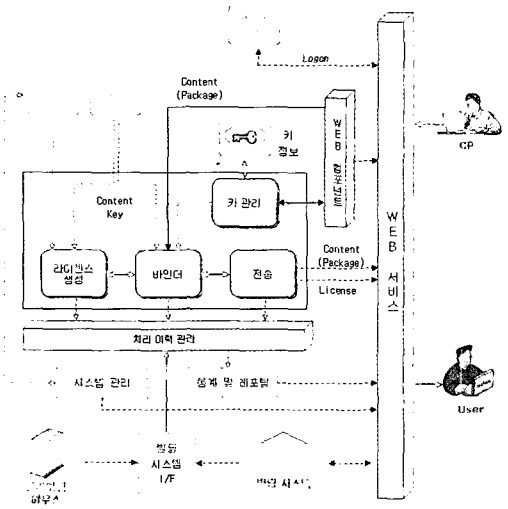
임베디드 프로세서의 고성능화는 DRM을 PD에 구현하는 것을 용이하게 하였다.

3.3 PD DRM 구성

전체 시스템은 크게 서버와 클라이언트부로 구분되어 있으며 클라이언트부는 적용 단말기기의 구분에 따라 PDA와 핸드폰 혹은 PC에 연결된 MP3P로 나뉘게 된다. 서버부는 라이센스(컨텐츠를 이용할 수 있는 권리를 정의)의 생성 및 Key관리를 담당하며, 클라이언트부는 DRM으로 보호된 컨텐츠를 사용 Application 상에서 복호화시켜 보안성이 보장된 자료를 제공하는 시스템을 구축한다.

2.3.1 서버

서버부는 다음과 같은 기능을 담당한다. (그림 6)은 PD DRM의 서버부를 나타낸다.



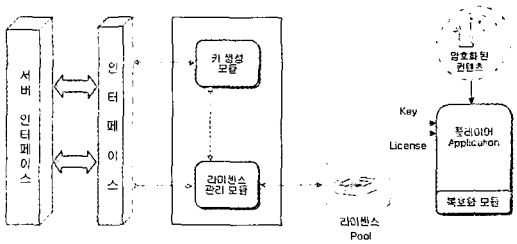
(그림 6) 서버 구성도

- 컨텐츠를 등록한다.
- 결제 시스템과 연계하여 결제 정보를 전달한다.
- 사용자에게 컨텐츠를 제공한다.
- Rule정보 및 컨텐츠의 정보 등을 담는 라이센스를 사용자별로 발급한다.
- 라이센스를 발급할 때 Cracking으로부터 보호하기 위해 라이센스를 암호화 한다.
- Virtual Key 재원이 없는 Player를 위해 Virtual Key 생성을 한다. 이 Virtual Key는 라이센스를 복호화하여 콘텐츠 키를 얻기 위해서 사용한다.
- 처리 이력 관리가 있어야 한다.

2.3.2 클라이언트

(그림 7)는 클라이언트 구조도를 나타내고 있다. 클라이언트 상에서 라이센스 갖어와서 해당되는 암호화된 콘텐츠의 복호화 키를 획득, 관리하는 기능을 수행한다.

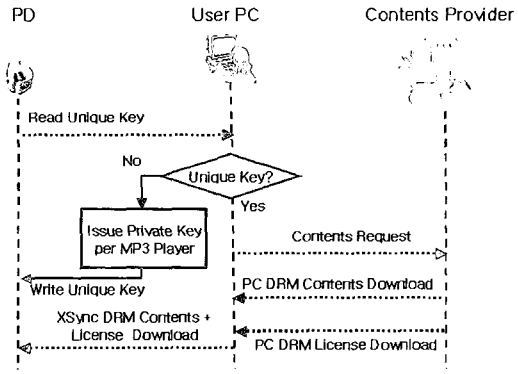
- 라이센스 획득 기능
- 라이센스 관리 기능
- 라이센스 디코더 기능
- 콘텐츠복호화 기능



(그림 7) 클라이언트 구조도

4. PD DRM 구현

(그림 8)은 구현된 PD DRM의 디지털 콘텐츠의 다운로드 과정을 나타내고 있다. PD를 이용하여 디지털 콘텐츠를 이용하려면 우선 PD의 고유한 키가 있어야 한다. 이 고유한 키가 없다면 고객 정보 등을 이용하여 고유한 키를 PC에서 생성하여 PD에 발급한다. PD의 고유한 키의 역할은 디지털콘텐츠의 라이센스를 복호화 하는 데 사용한다. 다운로드되는 라이센스 정보는 사용자 PC의 하드웨어 고유정보를 이용하여 암호화된다. PD에 다운로드하기 위해서 이미 콘텐츠 키로 암호화되어 있는 디지털콘텐츠와 PD 고유키를 이용하여 암호화된 라이센스 정보를 PD에 다운로드하여 디지털콘텐츠를 PD에서 재생, 사용하게 된다. PD의 하드웨어적인 성능을 고려하여 라이센스 정보를 콘텐츠에 결합하여 함께 다운로드했다.



(그림 8) 구현된 PD DRM의 콘텐츠 다운로드

5. 결 론

휴대폰이나 PDA와 같은 무선 단말기인 경우에 내장되어 있는 임베디드 프로세서의 성능이 우수하기 때문에 무선 모바일 장비를 타깃으로 만들어진 OMA DRM이 포팅이 되어 사용되고 있다. 그러나 MP3P와 같이 스스로 네트워크에 접속할 수 없는 PD의 경우에는 단지 디지털콘텐츠를 재생만 하면 되고 시장에서의 가격 경쟁력을 위하여 고성능의 임베디드 프로세서를 사용할 필요가 없었다. 현재 상용되고 있는 PD의 하드웨어 조건에서 DRM을 구현하기 위해서 암호화 및 복호화 알고리듬은 대칭키 방식의 스트리밍 암호화 기법을 사용하였고 콘텐츠를 부분적으로 암호화하여 하드웨어적인 부담을 줄였다.

향후 PD에 적용되는 임베디드 프로세서의 성능과 관련 하드웨어의 환경이 개선되면 모바일 환경에서 사용되고 있는 표준화된 OMA DRM을 적용할 수 있을 것이다.

참고문헌

[1] 임채덕, "임베디드 소프트웨어 기술동향 및 산업발전 전망," 정보통신연구진흥 제4권 제3호, 정보통신연구진흥원, 2002. 9.

[2] 윤범진, "임베디드 프로세서 산업동향," 정보처리학회지 제10권 4호, 2003. 7.

[3] Open Mobile AllianceTM, OMA-Download-DRM-v1_0, http://www.openmobilealliance.org/

[4] Open Mobile AllianceTM, OMA-Download-ARCH-V2_0, http://openmobilealliance.org/documents.html

[5] 남상엽, 조상엽, 이영무, 임베디드 시스템 설계와 응용, 상학당, 2004. 7.

저자약력

신 동 환

1992년 서울시립대학교 전자공학과 (학사)
1996년 서울시립대학교 전자공학과 (석사)
2002년 서울시립대학교 전자공학과 (박사)
1992년~1994년 LG전자 비디오사업부 연구원
1996년~2000년 체육과학연구원 시스템공학실 선임연구원
2000년~2001년 ㈜마크애니 연구소 선임연구원
2002년 - 현재 ㈜마크텍 연구소 연구소장
관심분야 : 디지털워터마크, 임베디드시스템, DRM, 디지털신호처리
이 메 일 : dhshin@marktek.co.kr

유 세 근

1992년 연세대학교 의용공학과(학사)
1994년 서울시립대학교 전자공학과 (석사)
2004년 서울시립대학교 전자공학과 (박사)
2002년 - 현재 ㈜마크애니 콘텐츠사업실 실장
관심분야 : DSP, Commercial Digital Rights Management
이 메 일 : samyoo@markany.com

최 종 욱

1982년 아주대학교 산업공학과(학사)
1988년 University of South Carolina 인공지능 (박사)
1988년~1991년 KIST 시스템공학센터 인공지능실장
1991년 - 현재 상명대학교 소프트웨어학부 교수
2000년 - 현재 ㈜마크애니 대표이사
관심분야 : digital watermarking, digital rights management, and computer forensics
이 메 일 : juchoi@markany.com