DRM 기술의 상호호환성을 지원하기 위한 방법

최범석 변영배 남제호
한국전자통신연구원
{bschoi, byun, namjho}@etri.re.kr

Advanced Method for Interoperable DRM

Choi, Bum Suk Byun, Young Bae Nam, Je Ho
ETRI

요약

디지털 콘텐츠 서비스 제공자들이 증가함에 따라, 다양한 DRM 시스템들이 상호호환성에 대한 고려 없이 개발되었다. DRM 시스템 간의 상호호환성 부재는 소비자들이 콘텐츠를 다양한 디바이스 환경에서 사용하지 못하도록 하고 있으며 디바이스 제조자들에겐 다양한 DRM을 지원해야 하는 부담을 주고 있다. 본 논문에서는 서로 다른 DRM 시스템 사이에 상호호환성을 지원하기 위한 새로운 방법을 제안한다. '툴팩'이라 불리는 본 기술은 Open Frame Work 기반으로 기존의 Open Frame Work 기반의 DRM 기술이 가지고 있던 약점인 DRM 툴(Tool)의 보안성을 높이는 동시에 새로운 DRM 툴을 추가하기 위한 확장성과 인터페이스의 간략화로 효율성을 증가시키는 효과가 있다.

1. 서론

DRM (Digital Rights Management) 기술의 초기에는 특정 서비스 제공자의 요구사항을 만족시키는 독립적인 형태로 DRM 시스템이 개발되어 왔으며, 보안상의 이유로 인하여 DRM 시스템에 대한 기술적 정보에 접근을 금하였다. 최근 디지털 콘텐츠 서비스 제공자들이 증가되면서 다양한 종류의 DRM 시스템들이 상호운용성에 대한 고려 없이 개발되고 있다. 예를 들어, 이미 잘 알려진 마이크로소프트 DRM 이나 애플 DRM의 경우는 이미 자신의 DRM 시스템을 적용한 시장을 상당부분 독점하고 있으나 이들 두 DRM 시스템은 현재 전혀 호환이 안 되고 있다. 또한 이들은 DRM 시스템의 보안을 유지하기 위하여 시스템 구조를 공개하려 하지도 않는다. 이러한 DRM 시스템 간의 상호호환성 부재는 사용자들이 구매한 정당한 콘텐츠를 자신이 소유한 다른 기기에서도 사용 못하도록 하고 있으며, 디바이스 제조자들에게는 어떤 DRM 시스템을 고려하여 디바이스를 제조해야 하는지에 대한 혼란을 주고 있다. 따라서 DRM 시스템에 관한 표준을 정의하는 것이 디지털 콘텐츠 시장의 성장을 위하여 반드시 필요한 사항이다.

많은 DRM 관련 표준 단체가 상호운용성 문제의 해결을 목표로 2000년 후반부터 활발히 활동하기 시작하였다. IPMP (Intellectual Property Management and Protection)는 MPEG 표준화 기구에 의하여 상호호환적 DRM과 멀티미디어 콘텐츠의 유동적인 배포를 지원하기 위하여 개발된 대표적인 플랫폼 기술이다[1~3]. MPEG-2/4 IPMPX 기술의 기본 개념은 인증, 암호, 워터마킹과 같은 DRM 단위 기능을 하나의 객체 모듈화 (이하 DRM Tool) 하고 이러한 DRM Tool 과 이를 관리하기 위한 디바이스 제어 모듈인 IPMP Terminal 사이의 인터페이스를 정의하고 있다. 또한 콘텐츠에 적용된 DRM Tool에 관한 정보를 표현하는 방법과 이를 전송하는 방법을 역시 정의하고 있다. 이하로부터 이러한 단위 기능을 하는 DRM Tool 기반의 DRM 기술을 Single DRM Tool 방법이라 칭한다[4]. 상호호환성 측면에서 Single DRM Tool 방법은 매우 효율적인 방법이라 할 수 있다. 하지만, 실제 적용의 측면에서 볼 때, 이 방법은 아래와 같은 몇 가지 문제점을 가지고 있다.

1. 일반적으로 DRM Tool은 원형의 미디어 데이터 또는 콘텐츠를 복호화 하기 위한 키 정보와 같은 매우 중요한 데이터를 처리한다. 즉 DRM Tool 자체에 대한 보안이 콘텐츠 보호를 위하여 중요하다. 따라서 DRM 벤더들은 그들의 DRM Tool을 공개된(표준) 인터페이스 형태로 제공하기를 꺼려한다.

2. 콘텐츠를 플레이하기 위해서는 어떠한 DRM Tool들이 필요하며 각 DRM Tool이 어떤 미디어 데이터를 제어하는지에 대한 정보를 IPMP Terminal이 알고 있어야 한다. 따라서 이러한 정보가 콘텐츠 내부에 공개적으로 명시되어야 하므로 악의적 공격에 이용될 수 있다.

3. DRM 시스템은 다양한 종류의 DRM Tool들의 상호 작용에 의하여 동작한다. 이러한 DRM Tool 들은 표준화된 인터페이스 메시지를 통하여 통신하고 모든 메시지들은 IPMP Terminal을 경유하도록 정의되어 있다. IPMP Terminal은 DRM 벤더가 임의로 제어할 수 없고 인터페이스가 공개된 모듈이므로 IPMP Terminal로 입출력되는 메시지를 분석한다면 DRM 메커니즘을 짐작할 수 있다. DRM 벤더들은 이러한 DRM 메커니즘을 외부에 공개하기를 꺼려한다.

4. 만일 새로운 DRM Tool이 이전 DRM Tool과 전혀 다른 기능과 프로토콜을 필요로 한다면, 이를 지원하기 위한 새로운 표준 인터페이스가 정의되어야만 한다. 이는 기존의 IPMP Terminal 역시 변경되어야 함을 의미한다.

이러한 문제점들을 보완하기 위하여 본 논문에서는 툴팩(Tool Pack)이라는 향상된 상호호환적 DRM 방법을 소개한다.

본 논문의 구성은 다음과 같다. 2장에서는 툴팩의 기본 개념을 설명하고, 3장에서는 툴팩 기술을 구성하는 기술 항목들을 설명한다. 마지막으로 4장에서는 결론과 함께 앞으로의 연구과제에 대하여 언급한다.

2. 기본 개념

대부분의 DRM 벤더들은 하나의 DRM 시스템 형태로 운용하고 있으며 이러한 DRM 시스템을 개별적인 DRM Tool 형태로 분리하여 제공하길 원치 않는다. 툴팩은 이러한 개별적인 DRM Tool들을 Tool Group으로 묶고 Tool Group을 운용하기 위한 상위 모듈인 Tool Agent를 생성하여 운용하는 개념이다. 즉 기존의 DRM 시스템에 적용하기가 용이한 구조로 되어 있다. 그림 1은 툴팩의 내부적인 구조와 IPMP Terminal 과의 인터페이스를 나타낸다.

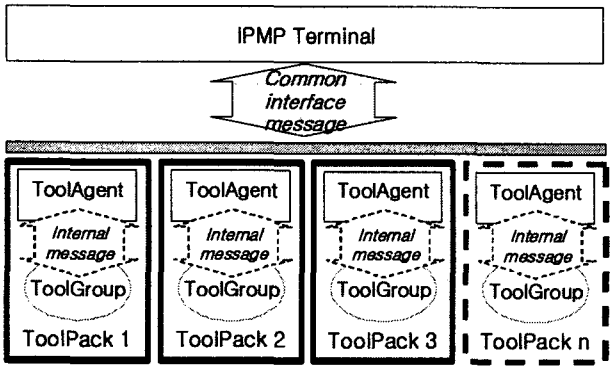

그림 1: 툴팩의 구조와 인터페이스

툴팩은 Tool Group 과Tool Agent를 포함하는 구조로 정의된다. 따라서 DRM 벤더는 그들이 사용하는 DRM Tool들을 Tool Group 안에 포함시키고 Tool Agent와 함께 툴팩 구조로 제공할 수 있다. 여기서 Tool Agent는 Tool Group 안의 개별 툴들을 대신하여 IPMP Terminal 과의 통신을 담당하게 된다. Tool Agent와 Tool Group 사이의 통신은 DRM 벤더가 자체 정의한 프로토콜을 사용하도록 하므로 공통 인터페이스 부분이 간결해진다. 그림 1에서 보듯이, 표준 인터페이스가 필요한 부분은 Tool Agent 와 IPMP Terminal 간의 인터페이스로 상위 레벨의 최소한의 인터페이스만을 정의한다.

Single DRM Tool에 비하여 툴팩은 DRM Tool에 대한 상세한 작동 정보를 내부로 숨길 수 있으며, 표준 인터페이스를 간략화 할 수 있는 장점이 있다. 또한 이러한 최소한의 표준 인터페이스는 어떠한 툴팩에서도 공통적으로 적용될 수 있으므로 새로운 툴에 대한 확장성도 증가된다고 할 수 있다.

3. 기술 항목

툴팩 기술은 IPMP Terminal, 툴팩 구조, 인터페이스 메시지로 구성된다. 본 장에서는 툴팩을 구성하는 각 기술 항목에 대하여 자세히 설명한다.

가. IPMP Terminal

IPMP Terminal은 디바이스 안에서 DRM 관련 기능을 수행하는 모듈이다. IPMP Terminal은 입력되는 콘텐츠로부터 DRM 정보, 툴팩, 키, 그리고 라이센스를 추출한다. 또한 IPMP Terminal은 디바이스 상에서 가용한 콘트롤 포인트(Control Point)를 관리한다. 여기서 콘트롤 포인트란 콘텐츠 디코딩 과정 중에 DRM Tool이 연결되어 작동할 수 있는 위치를 의미한다. 그림 2는 방송셋탑의 구조에서 IPMP Terminal의 역할과 적용 가능한 콘트롤 포인트들을 나타내고 있다(검은 점으로 표시)

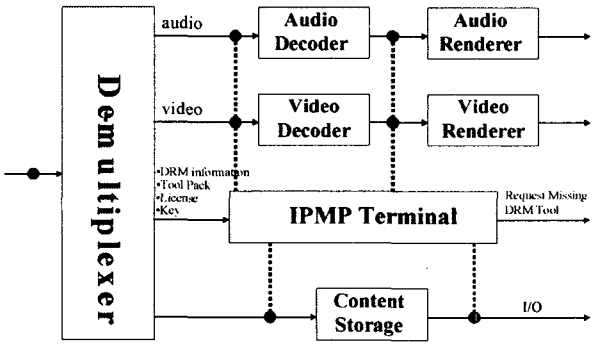

그림 2: 방송셋탑에서의 IPMP Terminal과 콘트롤 포인트

IPMP Terminal은 DRM 정보를 이용하여 필요한 툴팩을 찾고 Tool Agent를 작동시킨다. Tool Agent가 작동되면 IPMP Terminal은 인터페이스 메시지를 사용하여 Tool Agent를 초기화, 인증, 그리고 모니터링하게 된다. 인터페이스 메시지는 콘텐츠가 디코딩 될 때, IPMP Terminal 또는 Tool Agent에 의하여 생성되지만 특정한 경우에는 콘텐츠에 삽입되어 전달되기도 한다(예: 주기적으로 변경될 필요가 있는 키 데이터의 경우). 이러한 경우 IPMP Terminal은 콘텐츠로부터 인터페이스 메시지를 추출하여 Tool Agent에게 전달한다. 만일 디바이스 안에 필요로 하는 툴팩이 존재하지 않으면, IPMP Terminal은 외부서버에 접속하여 필요한 툴팩을 다운로드 하는 역할을 담당한다.

한번 디바이스에서 사용된 툴팩은 디바이스의 안전한 저장소에 저장되어 필요한 경우 재사용 된다.

나. 툴팩 구조

Tool Agent와 Tool Group의 콘테이너로서 툴팩은 그림3과 같은 스키마 구조를 갖는다. 각각의 엘리먼트에 대한 설명은 다음과 같다.

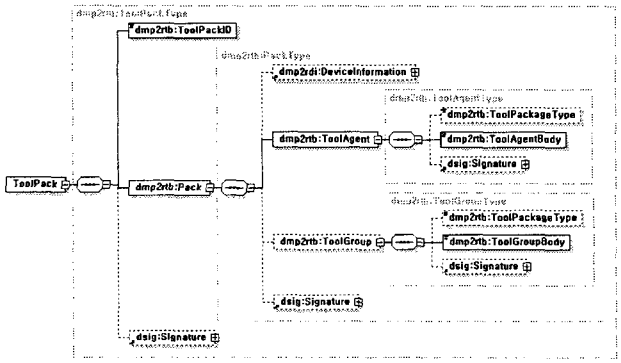

그림 3: 툴팩 스키마 구조

'ToolPack' 엘리먼트는 다음과 같은 하위 엘리먼트로 구성된다:

-Tool Pack ID: 툴팩을 유일하게 구별시켜주는 ID. ID의 유일성을 보장하기 위하여 공인인증기관이 필요하며 이를 통하여 툴팩의 등록과 ID 발급이 이루어져야 함.

-Pack: 유닛 툴팩을 포함하는 엘리먼트. 각 유닛 툴팩은 디바이스 플랫폼 정보, 패키지 포맷 정보, Tool Agent, Tool Group, 그리고 서명을 포함한다. 다양한 디바이스 환경에 따라서 적절한 유닛 툴팩을 적용할 수 있도록 하나 이상의 유닛툴팩이 툴팩 구조 안에 포함될수 있다.

-Device Information: 유닛 툴팩의 Tool Agent 와 Tool Group이 작동할 수 있는 디바이스의 하드웨어 또는 소프트웨어(OS 포함)에 관한 정보를 포함한다.

-Tool Agent: Tool Agent의 바이너리 코드와 패키지 타입을 포함하는 엘리먼트.

-Tool Group: Tool Group의 바이너리 코드와 패키지 타입을 포함하는 엘리먼트. 옵션 엘리먼트로 Tool Agent 내에 필요한 DRM Tool을 모두 포함하도록 구현될 경우 생략 가능함.

-Tool Package Type: 바이너리 코드의 패키지 타입을 나타냄. 예: CAB, Winzip 등. 각 타입에 따른 인덱스 값은 공인기관에서 할당.

-(Tool Agent/Tool Group) Body: Tool Agent (또는 Tool Group)에 대한 바이너리 코드를 포함함.

-Signature: 툴팩 구조에 대한무결성 검사를 위한 디지털 서명.

Tool Pack Data는 Tool Agent를 초기화하기 위한 파라미터 또는 플래그값을 전달하는 데이터 구조이다. Tool Pack Data의 스키마 구조는 그림 4와 같다. Tool Pack Data는 툴팩과 함께 전달될 수도 있고 단독적으로 전달될 수도 있다. 'ToolPackData' 엘리먼트는 다음과 같은 하위 엘리먼트로 구성된다:

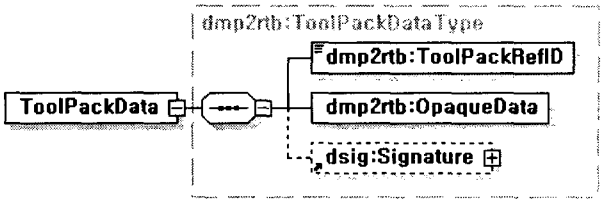

그림 4: Tool Pack Data 스키마 구조

-Tool Pack Ref ID: 툴팩 ID와 매칭되는 ID로 어떤 툴팩에 소속된 Tool Pack Data 인지를 나타낸다.

-Opaque Data: Tool Agent를 초기화하기 위한 정보를 포함한다. 데이터 포맷은 해당Tool Agent 만이 해석할 수 있는 형태로 기술된다.

-Signature: Tool Pack Data 구조에 대한 디지털 서명.

다. 인터페이스 메시지

IPMP Terminal 과 Tool Agent가 작동되면 두 모듈은 인터페이스 메시지를 사용하여 통신하게 된다. 그림 5는 툴팩을 작동시키기 위한 전체적인 인터페이스 메시지의 흐름을 보여준다.

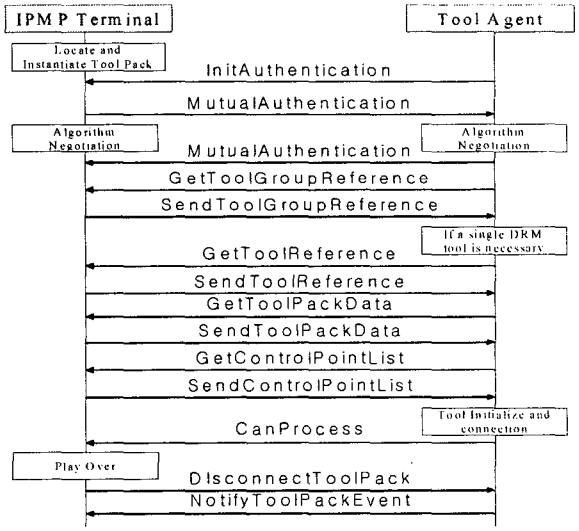

그림 5: 인터페이스 메시지

Init Authentication: IPMP Terminal 과 Tool Agent는 안전한 통신채널을 만들기 위하여 상호인증을 수행한다. 이를 위한 첫 번째 단계가 적절한 인증 타입을 결정하는 단계이다. 인증 타입은MPEG-2/4 IPMPX에서 정의된 4가지 레벨[2~3]을 따른다.

Mutual Authentication: 상호인증의 2번째 단계는 인증에 사용될 알고리즘을 결정하기 위한 조율단계이다. 이 과정은 상호간 적절한 인증 알고리즘이 결정되기까지 반복된다. 일단 인증 알고리즘이 결정되면 결정된 인증 메커니즘에 따라 상호인

증이 수행된다.

Get Tool Group Reference: Tool Agent는 Tool Group을 요구할 수 있다. 이 경우 Tool Agent는 Tool Group이 존재하는 위치 정보를 IPMP Terminal에게 요청한다.

Send Tool Group Reference: IPMP Terminal은 툴팩 구조로부터 Tool Group을 추출하고 그위치 정보를 Tool Agent에게 전달한다.

Get Tool Reference: Tool Agent는 Single DRM Tool을 사용할 수도 있다. 예를 들어 DES 나 AES 같이 일반적으로 사용되는 툴의 경우 Single DRM Tool의 형태로 디바이스에 존재할 수 있다. 이 경우 Tool Agent는 필요로 하는 Single DRM Tool의 ID를 IPMP Terminal에게 요청할수 있다. 만일 하나 이상의 Single DRM Tool이 필요하다면 다수의 Tool ID가 메시지에 포함될 수도 있다

Send Tool Reference: IPMP Terminal은 Single DRM Tool에 대한 위치정보를 Tool Agent에게 전달한다. 만일 하나 이상의 Single DRM Tool을 요청해 왔다면 해당되는 모든 Single DRM Tool에 대한 위치정보를 전달하게 된다.

Get Tool Pack Data: Tool Agent는 경우에 따라 갱신된 파라미터 값들로 초기화 될필요가 있다(예: 좀 더 안전한 콘텐츠 보호를 위하여 주기적으로 암호화 키 값을 변경 적용할 경우). 이 경우 Tool Agent는 IPMP Terminal에게 갱신된 Tool Pack Data를 요청할 수 있다.

Send Tool Pack Data: IPMP Terminal은 툴팩 구조로부터 Tool Pack Data를 추출하여 Tool Agent에게 전달한다.

Get Control Point List: Tool Agent는 IPMP Terminal에게 디바이스 상에서 가용한 콘트롤 포인트 리스트를 요청한다.

Send Control Point List: IPMP Terminal은 디바이스에 적용 가능한 콘트롤 포인트 리스트를 Tool Agent에게 전달한다. 본 메시지에는 콘트롤 포인트 ID들과 각 콘트롤 포인트의 실제 주소 정보가 포함될 수 있다. 표 1은 디바이스에서 적용 가능한 콘트롤 포인트들의 리스트를 보여준다. 디바이스의 환경 또는 기능에 따라 하나 또는 그 이상의 콘트롤 포인트를 적용할 수 있다.

Control Point ID	Description
00	NO_CONTROL_POINT
01	CONTROL_POINT_BEFORE_DEMULTIPLEXING
02	CONTROL_POINT_BEFORE_AUDIO_DECODING
03	CONTROL_POINT_AFTER_AUDIO_DECODING
04	CONTROL_POINT_BEFORE_VIDEO_DECODING
05	CONTROL_POINT_AFTER_VIDEO_DECODING
06	CONTROL_POINT_BEFORE_STORING
07	CONTROL_POINT_BEFORE_PLAYBACK
08	CONTROL_POINT_BEFORE_TRANSFERRING

표 1: Control Point ID list

본 표에 표기된 콘트롤 포인트 리스트는 MPEG-2/4 IPMPX에서 기 정의된 콘트롤 포인트 리스트[2~3]에서 확장된 것이다. 회색음영으로 표기된 부분이 툴팩을 통하여 추가된 콘트롤 포인트이다.

Can Process: 초기화, 인증, DRM Tool의 콘트롤 포인트 연결에 대한 처리가 끝나면, Tool Agent는 IPMP Terminal에게 콘텐츠를 디코딩할 준비가 되었다는 것을 알린다.

Disconnect Tool Pack: IPMP Terminal은 Tool Agent에게 연결되어 있던 DRM Tool들을 콘트롤 포인트에서 제거하라는 명령을 보낼 수 있다(예: 사용자가 임의로 콘텐츠 재생을 멈춘 경우).

Notify Tool Pack Event: Tool Agent는 초기화 처리 또는 콘텐츠 디코딩 처리 중에 일어나는 특정 이벤트에 대하여 IPMP Terminal에게 알릴 수 있다. IPMP Terminal은Tool Agent로부터 전달받은 이벤트의 타입에 따라 적절한 처리를 하게 된다.

만일 IPMP Terminal이 Single DRM Tool을 지원하려면 위에서 열거된 메시지들 이외에 MPEG-2/4 IPMPX에서 정의된 모든 메시지들을 처리할 수 있어야 한다.

4. 결론

본 논문에서는 향상된 상호호환적 DRM 방법에 대하여 설명하였다. 제안된 방법의 특징은 Open Frame Work 구조를 적용하면서도 DRM 벤더들의 DRM Tool 보안성에 대한 요구사항을 만족시키고 있다는 점이다. DRM Tool에 대한 정보와 기능 및 작동 메커니즘에 대한 정보를 외부에 노출시키지 않기 위하여 Tool Group 과 Tool Agent를 정의하였으며, 이를 포함하는 툴팩 구조를 정의하였다. 또한 상호호환적 툴팩의 운용을 위하여 Tool Agent와 IPMP Terminal 사이에 통신을 위한 인터페이스 메시지를 정의하였다. 본 메시지들은 기존의 MPEG-2/4 IPMPX에서 정의한 인터페이스 메시지에 비하여 간단하며 모든 툴팩에서 적용 가능하도록 설계되었다. 향후 연구과제로 본 논문에서 제안한 툴팩을 실제 디바이스에 구현해 보고 이를 다양한 서비스 환경에 적용해 봄으로 그 효과를 증명할 예정이다.

참조

[1]ISO/IEC 21000-4 IPMP Components FDIS, ISO/IEC JTC1/SC29 WG11 MPEG68/N7717, October 2005, Nice, France.

[2]ISO/IEC 13818-1, Information technology — Generic coding of moving pictures and associated audio information — Part 11: IPMP on MPEG-2 systems

[3]ISO/IEC 14496-13, Information technology — Coding of audio-visual objects — Part 13: Intellectual Property Management and Protection (IPMP) extensions