컨텐츠 보호를 위한 스트리밍 서비스 방안 연구

박 지 현*, 윤 기 송*, 전 경 표*
한국전자통신연구원*

A Study on Streaming Service for Content Protection

Park Ji-Hyun*, Yoon Ki-Song*, Jeon Kyung-Pyo*
Electronics and Telecommuications Research Institute*
E-mail : juhyun@etri.re.kr

요 약

인터넷 및 네트웍의 환경 변화는 고품질, 고용량의 컨텐츠의 실시간 서비스를 가능하게 만들었다. 디지털 콘텐츠의 편리성은 콘텐츠에 대한 수요를 증가시키고 있지만, 자유로운 복제가 가능한 디지털 콘텐츠의 특성 때문에 보안과 저작권 문제가 중요한 문제로 대두되고 있다. 스트리밍 서비스는 콘텐츠의 저장을 막음으로써 이같은 문제를 해결하여 왔다. 하지만 스트리밍되는 콘텐츠를 저장할 수 있는 몇가지 툴이 등장하면서 스트리밍 컨텐츠도 더 이상 불법사용 문제로부터 자유롭지 못하게 되었다. 따라서 접근제어 위주의 보안대책과 함께 콘텐츠의 사용권한 제어 및 통제를 지속적으로 보호 관리할 수 있는 새로운 기술이 요구되며, 그 해결책의 하나가 DRM 시스템이다. 본 논문에서는 스트리밍 컨텐츠로 가장 널리 사용되고 있는 Microsoft의 멀티미디어 파일 포맷인 ASF를 기반으로한 스트리밍 시스템에 DRM을 적용하는 방안에 대하여 설명한다..

Abstract

Changes in internet and network environment make it possible to provide high-quality content services in real time. As demand for digital content is increased, problems related to intellectual property rights are getting more important. Streaming service like video-on-demand solved this problem by preventing content from being saved. But, as the advent of several tools able to save streamed content, the streamed content is not free from these problems any more. So, with security countermeasure like access control, new technologies to control and manage rights for content are needed. One of the solutions is DRM In this paper, we describe a DRM-based streaming service that can send the ASF stream which is the multimedia file format of Microsoft.

I. 서론

스트리밍(Streaming)이란 인터넷을 통하여 영상, 음악 등 디지털 멀티미디어 데이터를 실시간으로 전송하여 재생할 수 있는 기술이다. 사용자의 PC에 저장된 컨텐츠는 복사가 자유로웁기 때문에 저작권에 관한 문제가 발생하였으나, 스트리밍 컨텐츠는 몇가지 방법을 통하여 이용자의 PC에 저장할 수 없도록 하여 불법 복사에 관한 문제를 해결하였다. 하지만 스트리밍 컨텐츠를 저장할 수 있는 프로그램이 나타나면서 스트리밍 컨텐츠

도 불법 복사가 가능하게 되었다. 이 같은 문제를 해결하기 위한 방법중 하나는 스트리밍 시스템에 DRM을 도입하는 것이다.

본 논문에서는 현재 스트리밍 컨텐츠로 가장 많이 사용되고 있는 Microsoft의 ASF(Advanced Systems Format) 파일을 기반으로 스트리밍 컨텐츠의 보호 방법에 관하여 설명한다.

II. 컨텐츠 보호

스트리밍 시스템에서 DRM 적용을 하기 위해서 서버측에는 보호된 컨텐츠를 생성하기 위한 패키징 프로그램[1]이, 클라이언트측에는 보호된 컨텐츠를 재생할 수 있도록 하는 몇가지 모듈이 필요하다. 스트리밍 시스템과 DRM 시스템이 효과적으로 연동되기 위해서는 기존의 스트리밍 서버를 전혀 수정하지 않고 스트리밍 컨텐츠에 대한 DRM을 구현하여야 한다. 즉, 컨텐츠 파일과 클라이언트 재생기에 대한 작업만으로 DRM이 가능하도록 구현되어야 한다.

1. ASF

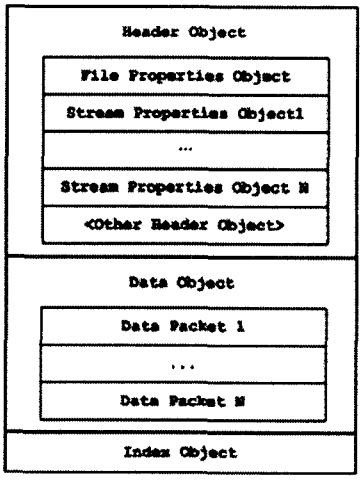

그림1. ASF 구조

Microsoft사가 1996년에 멀티미디어 스트리밍용으로 고안한 파일 포맷인 ASF는 상당히 유연한 포맷으로 같은 시간으로 동기화 된 오디오, 비디오, 텍스트(캡션), 이벤트의 압축된 디지털 버전을 포함하고 있다. 즉, ASF는 동기화된 멀티미디어 데이터를 저장할 수 있도록 설계된 확장 가능한 파일 포맷으로 로컬 재생에 적합하면서도 다양한 네트워크와 프로토콜 상에서의 데이터 전송을 지원한다. ASF는 확장 가능 미디어 유형, 저작자 지정, 스트리밍 우선순위 부여, 다중 언어 지원, 문서 및 콘텐트 관리를 비롯한 광범위한 서지 기능 등 고급 멀티미디어 기능을 지원한다[2].

ASF는 기능에 따라 다양한 객체들로 구성되어 있으며 사용자의 의도에 따라 객체의 확장이 가능하기 때문에 유연한 구조를 가진다. ASF의 전체 구조와 각 객체의 구조는 각각 그림 1, 2와 같다[3]. 그림 1에서와 같이 ASF의 가장 상위 객체는 헤더객체, 데이터 객체, 인덱스 객체이다. 헤더객체는 일반적인 파일정보와 스트림 정보로 구성되며 미디어 재생기가 프레젠테이션을 올바로 렌더링하는 데 필요한 정보를 포함한다. 데이터 객체는 실제적인 미디어 데이터를 가진다. 이들 데이터는 스트리밍시 보내질 패킷단위로 저장되어 있다. 인덱스 객체는 미디어 데이터의 시간단위의 전후 탐색이 가능하도록 하는 인덱스 정보를 가진다.

Object GUID (16 bytes)
Object Size (8 bytes)
Object Data (N bytes)

그림2. ASF 객체 구조

2. ASF 암호화 방법

기존의 DRM은 컨텐츠의 포맷에 관계없이 동일한 암호화 방법을 사용한다[4]. 즉, 컨텐츠의 전체 데이터를 암호화하여 보호한다. 하지만 스트리밍 시스템에 이와같은 암호화 방법을 적용할 수 없다. 컨텐츠의 전체 데이터를 암호화하면 컨텐츠 자체의 포맷이 변경되므로 스트리밍 서버가 컨텐츠를 올바르게 스트리밍할 수 없게된다. 따라서 스트리밍 서버를 수정하지 않고 ASF 파일의 보호가 가능하게 하기 위해서는 ASF 파일의 포맷을 변경하지 않는 방안이 필요하다.

<table>
<tr><td colspan="2">error correction data</td></tr>
<tr><td colspan="2">payload Parsing information</td></tr>
<tr><td rowspan="3">payload data</td><td>payload 1</td></tr>
<tr><td>...</td></tr>
<tr><td>payload n</td></tr>
<tr><td colspan="2">padding data</td></tr>
</table>

그림3. 데이터 패킷 구조

본 논문에서는 데이터 패킷에서 실제 데이터에 해당하는 부분만을 암호화하여 파일의 포맷을 변경하지 않도록 하였다. 그림 3은 데이터 패킷의 내부 구조를 나타낸 것이다. 그림에서 payload에 해당하는 부분만을 암호화하면 스트리밍에 아무런

영향을 주지 않게 된다. 클라이언트에서 재생할 때 암호화된 데이터를 복호화하여 재생하면 DRM을 쉽게 적용할 수 있다.

III. 클라이언트 설계

1. DirectShow 기술

DirectShow는 Microsoft에서 개발한 멀티미디어 처리 기술이다. DirectShow는 멀티미디어가 갖는 다양한 입력, 다양한 포맷, 다양한 출력에 대한 문제를 해결하기 위해 컴포넌트 구조를 도입하였다. 컴포넌트 구조가 갖는 유연성을 활용하여 다양한 환경에 대해 컴포넌트를 적절히 조합함으로써 필요한 상황에 다양한 형태로 멀티미디어 데이터를 처리할 수 있도록 하였다[5,6].

DirectShow는 필터(filter)라는 구조의 컴포넌트를 도입하고 이들을 조합하여 다양한 멀티미디어 환경에 대응할 수 있도록 설계되었다. 필터는 Microsoft의 COM(Component Objet Model)의 기술을 기반으로 제작되어 컴포넌트의 장점을 가질 수 있도록 하였다. Windows에서 사용되는 멀티미디어 재생기는 대부분 이 기술을 이용하여 개발되며 사용자의 의도에 맞는 필터를 쉽게 개발하고 적용시킬 수 있으므로 본 논문은 DirectShow를 기반으로 DRM을 적용하도록 하였다.

2 복호화 필터 설계

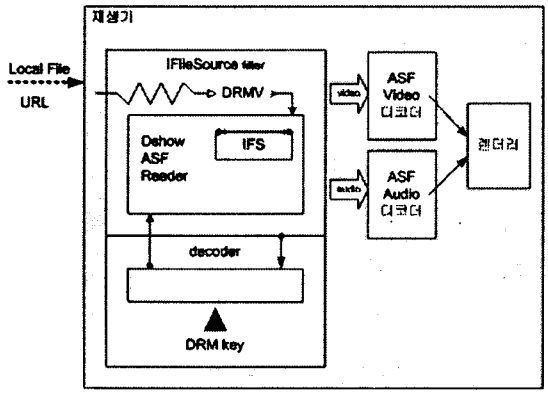

그림4. 소스 필터 구조

기존의 윈도우 미디어 플레이어를 지원하기 위해서는 DirectShow기반의 소스 필터[5]를 개발해야 다. 이 필터는 기존의 소스 필터와 유사하면서 인크립트된 스트리밍 동영상이나 로컬 동영상 파일을 처리해야 한다. 그림 4는 DRM 처리를 위한 소스필터의 구조를 나타낸 것이다.

재생되는 파일 타입은 다음과 같이 처리된다. 먼저, 소스 필터는 자체 파일 포맷 정보를 갖는 형태로 등록되어야 한다. 파일 포맷에 대한 모든 정보와 핸들러는 레지스트리에 등록된다. 파일 이름이 ":"을 포함하면 필터 그래프 관리기는 ":"앞을 프로토콜명으로 사용한다. 예를 들어, 파일 이름이 "myprot://myfile.ext"일 경우 레지스트리를 통해 "myprot"키 값을 검색한다. 이 키 값이 등록되어 있고 하위 값으로 Extensions 서브키 값이 있다면 필터 그래프 관리자는 파일 확장명과 일치되는 값을 서브키 값에서 검색한다. 만약 Extensions 서브키 값에 일치되는 키 값이 없다면 Source Filter 서브키 값에서 검색한다. 일치되는 키값이 있다면 필터 그래프 매니저는 소스 필터의 CLSID값으로 검색해서 나온 GUID값을 사용한 후 이 값으로 등록된 필터를 로드한다. 일치되는 키 값이 없다면 파일 소스 필터를 이용해서 파일 값을 URL로 인식해서 처리한다.

```
HKEY_CLASSES_ROOT
  <protocol>
     Source Filter = <Source Filter CLSID>
     Extensions
        <.ext1>=<Source Filter CLSID>
        <.ext2>=<Source Filter CLSID>
```

그림 5. 레지스트리 설정

3 DRM 클라이언트와의 연동

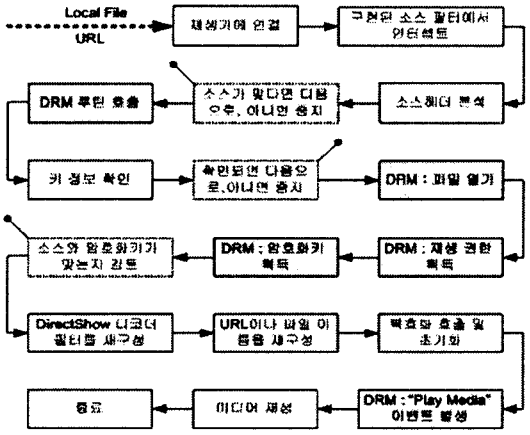

그림 6. 클라이언트 흐름도

DRM 클라이언트는 DRM 서버와의 통신을 통하여 DRM 관련 정보들을 주고 받으며, 중요한 데

이터들을 관리한다. 또한 컨텐츠 재생기를 제어하여 사용자가 획득한 권리에 따라 올바르게 컨텐츠가 사용될 수 있도록 한다. 특히, 사용자로부터 발생할 수 있는 원본 컨텐츠의 누출을 방지할 수 있도록 고도의 보안 메커니즘이 적용되어야 한다.

스트리밍 시스템과 DRM 시스템이 연동하기 위해서 소스필터는 DRM이 제공하는 API에 맞추어 개발되어야 하며, 이 인터페이스를 통하여 원하는 정보를 주고 받으며 서로 연동하게 된다. 그림 6은 클라이언트에서 DRM 모듈과 DirectShow 필터가 서로 연동하여 스트리밍 컨텐츠를 재생하는 흐름을 보여준다.

IV. 전체 시스템 구성

DRM 기반 스트리밍 서비스를 위한 전체 시스템은 스트리밍 서버, DRM 서버, 클라이언트 응용 프로그램, DRM 클라이언트로 구성된다. 컨텐츠에 대한 정보는 컨텐츠 메타데이터로 정의되고, 컨텐츠에 대한 사용권한은 라이센스를 통하여 발급된다. 표 1은 전체 시스템 구성요소를 나타내며, 그림 7은 시스템간의 흐름도를 나타낸다.

표 1. 전체 시스템 구성 요소

스트리밍 서버	동영상 파일을 스트리밍할 수 있는 서버 (Microsoft의 경우는 Windows Media Server가 이에 해당한다)
DRM server	라이센스와 키 정보가 저장된 서버
Client application	로컬 및 스트리밍용 동영상을 재생할 수 있는 클라인언트 재생 프로그램
DRM Core	라이센스 정보와 암호화된 파일을 관리하는 클라이언트 프로그램
라이센스	암호화된 동영상 컨텐츠를 복호화하는데 필요한 정보를 가지는 문서
메타데이터	컨텐츠 자체에 대한 정보와 DRM을 적용하기 위한 정보를 기술하는 데이터

V. 결론

본 논문은 ASF 파일 포맷의 분석을 통해서, 파일 구조를 변경시키지 않고 ASF 데이터 자체를 보호하는 방안과 이를 클라이언트에서 재생하기 위한 구조를 설계하고 구현하였다. 복호화에 필요한 정보는 컨텐츠의 암호화와 동시에 DRM 서버로 전송되며, DRM 서버는 암호화 메타데이터에 복호화키를 포함한 DRM 정보를 추가하여 인증된 사용자에게 전송하면, 사용자는 복호화 키를 이용 데이터를 복호화한 후 서비스를 이용한다.

본 연구의 결과를 토대로 다양한 스트리밍용 매체에 대한 연구와 높은 성능을 제공하기 위한 연구가 가능하다. 향후에는 스트리밍 서비스의 성능을 증가시키기 위하여, 암/복호화 기술의 부하 방지, 결함 감지, 복구 및 보다 안전하고 효율적인 분산 키 관리 시스템 연구가 수행될 것이다.

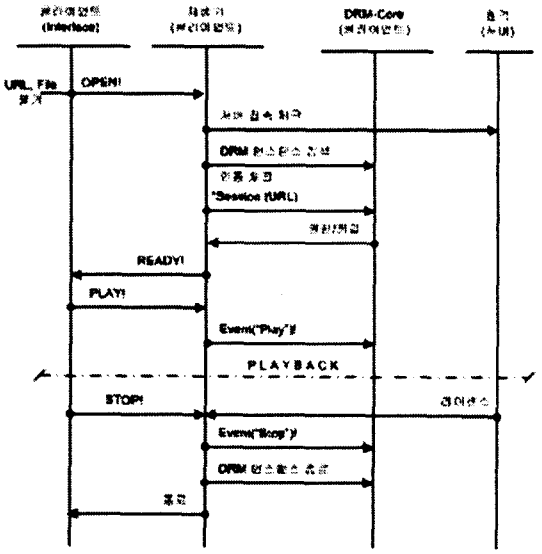

그림 7. 전체 시스템 흐름도

참 고 문 헌

[1] Kenneth Louis Milsted, Automated Method and Appara-tus to Package Digital Content for Electronic Distribution using the Identity of the Source Content, United States Patent 6,345,256.

[2] http://www.microsfot.com/windows/windows media

[3] ASF Specification, Microsoft.

[4] Olin Sibert, DigiBox: A Self-Protecting Container for Information Commerce, 1st USENIX Workshop on Electronic Commerce, 1995.

[5] 신화선, DirectShow 멀티미디어 프로그래밍, 한빛미디어, 2002.

[6] DirectX SDK, http://www.microsoft.com/directx