제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

DRM 기반 유통시스템을 위한 컨텐츠 패키저 설계

박지현*, 윤기송*, 박창순*
*한국전자통신연구원 컴퓨터소프트웨어연구소
e-mail : juhyun@etri.re.kr

Design of the Content Packager for DRM-based Distribution System

Ji-Hyun Park*, Ki-Song Yoon*, Chang-Soon Park*
*Computer&Software Research Laboratory, ETRI

요 약

DRM 을 통한 저작권 보호는 대부분 컨텐츠를 암호화하여 보호하고, 요금을 지불한 사용자에게 컨텐츠를 복호화할 수 있는 암호화 키를 포함한 라이센스를 발급하여 컨텐츠를 사용할 수 있도록 하는 방법을 사용한다. 암호화된 컨텐츠는 내부 정보를 보호할 수 있도록 설계된 secure container 라는 구조체에 컨텐츠에 대한 메타데이터 및 컨텐츠 사용에 관한 비즈니스 룰과 함께 패키징되어 구매자에게 배포된다.

현재 개발된 DRM 시스템들은 컨텐츠 유통업자와 구매자 사이의 단순한 유통 모델을 지원하도록 설계되어 있으므로 패키징 작업 또한 유통업자에서만 수행된다. DRM 을 통한 컨텐츠 유통이 활성화되면 컨텐츠 제작자에서부터 제공자, 유통업자, 구매자에 이르는 모든 컨텐츠 유통 채널에서 컨텐츠가 보호되어야 하며, 이런 경우 각 유통주체에서 컨텐츠의 패키징이 발생할 수 있다. 이처럼 다양한 유통 모델에서의 컨텐츠 보호를 위해서는 각 유통 모델을 지원할 수 있도록 유연한 구조로 secure container 를 설계하고 이를 지원하는 도구로써 컨텐츠 패키저를 설계하여야 한다.

본 논문에서는 유연성 있는 컨텐츠 패키저의 구조를 기술하고 컨텐츠 창조자, 유통업자, 구매자가 참여하는 유통모델에서 이를 적용하여 보고자 한다.

1. 서론

저작권 보호에 대한 요구가 커짐에 따라 암호화, 워터마킹, 식별자 시스템과 같은 여러가지 방법의 저작권 보호 기술이 연구되고 있다. 특히 컨텐츠 암호화를 통하여 컨텐츠를 보호하려는 DRM 관련 기술은 현재 몇가지 제품이 상용화 되어 서비스 되고 있는 상황이다. 하지만 현재의 기술은 최종 사용자로부터의 컨텐츠 보호에 중점을 두고 있어, 컨텐츠 제작자, 제공자, 분배자 등 컨텐츠 유통에 참여하는 주체들에게 호환성 문제, 저작권의 보호 및 관리 문제, 올바른 유통 체계 확립 문제 등을 효과적으로 해결할 수 있는 수단을 제공하지 못하고 있다.

복잡하고 다양한 유통모델에서 DRM 유통시스템을 적용하기 위해서는 다양한 유통모델을 분석하고, 이를 뒷받침할 수 있도록 메타데이터, secure container, 라이센스 발급 구조 등을 설계하는 것이 필수적이다. 특히, secure container 를 다루는 패키징의 경우 각 유통단계에서 패키징을 할 때 이전단계의 메타데이터 및 비즈니스 룰을 어기지 않게 할 수 있도록 설계되어야 한다.

본 논문에서는 창조자, 유통업자, 구매자, 클리어링 하우스가 참여하는 유통모델에서 창조자와 유통업자가 각각 컨텐츠를 패키징할 수 있도록 secure container 와 컨텐츠 패키저의 구조를 설계하고, 이를 이용한 컨텐츠 유통 방법에 대하여 기술한다.

2. Secure Container

Secure container 는 디지털 컨텐츠를 외부의 불법 침해로부터 방지할 뿐만 아니라 인터넷을 통해 손쉽

게 이동할 수 있는 기술적 정보 구조체를 말한다[1]. 이는 기존의 정보보호가 네트워크 전송 채널에서의 보호를 목적으로 한데 반해, 정보의 실사용자까지도 방어의 대상으로 하여 정보보호가 가능하도록 하는 개념이다.

InterTrust 는 DigiBox[5] 또는 Rights Pack[6]이라 불리는 secure container 기술을 사용하고 있으며, IBM 은 Cryptolopes[4]라는 secure container 기술을 사용하고 있다. InterTrust 의 경우 DigiBox Container 에 대한 생성 및 접근을 InterRights Point 소프트웨어를 통해서만 가능하도록 하여 보안성을 높이고 있다. 그림 1 은 InterTrust 의 secure container 인 DigiBox 의 구조를 간략히 나타낸 그림이다[2].

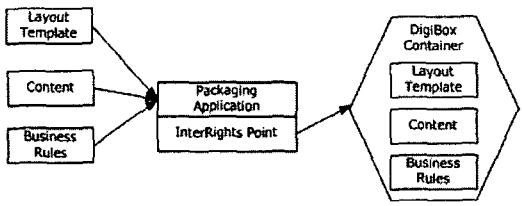

그림 1. DigiBox Container 의 구조

이러한 정보 구조체는 컨텐츠를 암호화할 뿐만 아니라, 컨텐츠 사용에 대한 비즈니스 모델 정보까지 포함하며 다음과 같은 특성을 갖는다[1].

- 기밀성(Confidentiality) : Secure container 에 포함된 정보에 대한 보안성 유지. 즉, 허락된 사용자에 대해서만 정보 접근을 허락하도록 함. 디지털 컨텐츠는 비즈니스 룰에서 정의한 조건에 따라 컨텐츠 사용이 허락됨. 대칭키 또는 비대칭키 암호화 기술 이용
- 무결성(Integrity) : Secure container 에 포함된 내용이 변경되지 않았음을 보장, 주로 해쉬(hash) 함수를 이용한 암호화 기술 이용

컨텐츠 패키징(Content Packaging)은 컨텐츠, 메타데이터, 비즈니스 룰 등 컨텐츠 보호와 유통에 관련되는 정보들로써 secure container 를 구성하는 작업이며 컨텐츠 패키저(Content Packager)를 통하여 수행된다.

3. 컨텐츠 유통시스템 구조

3.1. 컨텐츠 유통 모델

본 논문에서의 컨텐츠 유통 모델은 그림 2 와 같이 창조자, 컨텐츠 유통업자, 클리어링하우스, 구매자로 구성되며 각각의 역할은 표 1 과 같다.

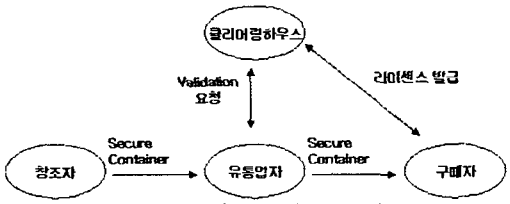

그림 2. 컨텐츠 유통 모델

주체	역 할
창조자	컨텐츠 제작, 컨텐츠 패키징
유통업자	컨텐츠 패키징, 컨텐츠 판매
클리어링 하우스	컨텐츠 위변조 검사, 결제, 라이센스 발급, 리포팅
구매자	컨텐츠 사용

표 1. 각 유통주체의 역할

3.2. 패키징 과정

3.2.1. 창조자의 컨텐츠 패키징

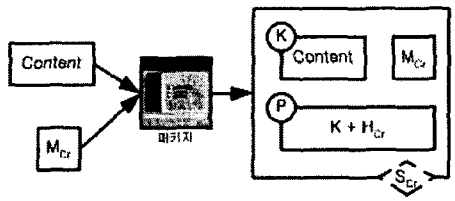

그림 3. 창조자의 패키징

컨텐츠 창조자에서의 컨텐츠 패키징의 결과로 생성되는 secure container 는 다음과 같은 요소를 가진다.

- 대칭키로 암호화된 컨텐츠
- 메타데이터 및 비즈니스 룰
- 컨텐츠 암호화 키와 메타데이터의 해쉬값을 클리어링하우스의 공개키로 암호화한 값
- secure container 에 대한 전자서명

그림 3 은 창조자에서 패키징한 결과로 생성된 secure container 의 구조를 보여준다.

3.2.2. 유통업자의 컨텐츠 패키징

유통업자가 컨텐츠를 패키징하기 위해서 먼저 창조자에게서 받은 컨텐츠의 위변조 여부를 검사한다. 이는 클리어링하우스를 통해서 이루어진다.

유통업자는 창조자에게서 받은 secure container 에서 일부 데이터와 메타데이터의 해쉬값을 계산하여 클리어링하우스에 validation 검사를 요청한다. 클리어링하우스는 자신의 비밀키로 복호화한 값과 해쉬값을 비교하여 위변조 여부를 판단하여 유통업자에 알려준다. 그림 4 와 그림 5 는 이 과정을 나타낸 것이다.

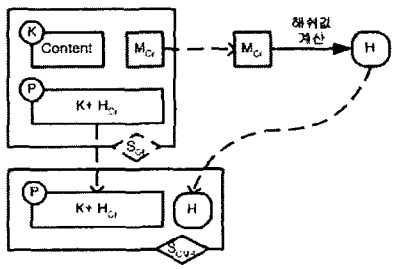

그림 4. 유통업자에서의 컨텐츠 Validation 요청

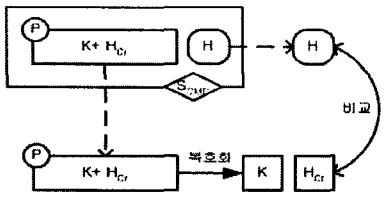

그림 5. 클리어링센터에서의 컨텐츠 Validation

창조자로부터 받은 secure container 의 무결성이 검사되면 유통업자는 자신의 메타데이터와 비즈니스 룰을 첨가하여 secure container 를 수정한다. 그림 6 은 유통업자에서 패키징한 결과로 생성된 secure container 의 구조를 보여준다.

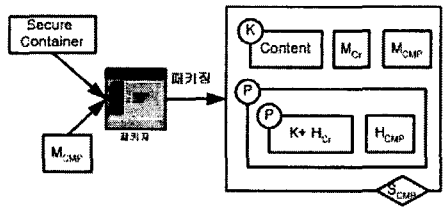

그림 6. 유통업자의 패키징

표 2 는 그림 3 ~ 6 에서 사용된 기호에 대한 설명이다.

기호	설 명
K	컨텐츠를 암호화하는데 사용하는 대칭키
P	클리어링하우스의 공개키
M_{Cr}	창조자가 작성하는 메타데이터
M_{CMP}	유통업자가 작성하는 메타데이터
H_{Cr}	M_{Cr} 의 해쉬값
H_{CMP}	M_{CMP} 의 해쉬값
S_{Cr}	창조자의 전자서명
S_{CMP}	유통업자의 전자서명

표 2. 기호 설명

4. 패키저 구조

4.1. 설계 고려사항

패키징은 Secure container 의 형식을 정의하고 그 형식에 따라 데이터를 채워 넣는 방법과 절차를 정의하는 것이다. 패키징을 위한 secure container 설계시 고려해야 할 사항은 다음과 같다.

- 내부 데이터에 대한 계층적인 구조
- 데이터 무결성
- 암복호화 방법 정의
- 내부데이터 인코딩/디코딩 방법 설계

또한 패키저 설계시 고려해야 할 사항은 다음과 같다.

- 패키저 실행 환경
- 패키징을 지원하는 도구
- 패키징의 결과물
- 무결성 보장
- 일괄 처리

여기에서 무결성 보장은 메타데이터가 추가될 때 앞 유통주체의 권한을 어기지 않았는지, 그리고 클라이언트에서 메타데이터로써 권한을 확인할 때 컨텐츠에 대한 올바른 사용 권한을 가지고 있는지를 검사하는 것이다. 본 논문에서는 rule engine 을 통하여 무결성을 검사하도록 하였다.

4.2. 구성 요소

패키저를 구성하기 위한 내부 구성요소와 외부 구성요소는 다음과 같다.

1) 메타데이터 작성기

사용자가 메타데이터를 입력하기 위한 도구이다. 필요에 따라 메타데이터의 일부분을 암호화하거나 전자서명을 추가 할 수 있다. 작성된 메타데이터는 일반적인 XML 문서이거나 인코딩된 문서이다.

2) 메타데이터 템플릿 에디터

패키징하려는 컨텐츠의 종류에 따라 사용자는 메타데이터로부터 자신이 필요로 하는 요소들만을 선택할 수 있다. 메타데이터 템플릿 에디터는 이러한 작업을 위한 도구이다.

3) 사용자 인터페이스

메타데이터 입력을 위한 사용자 인터페이스이다. 메타데이터 템플릿에 따라 사용자가 입력해야 하는 요소들이 다르므로 사용자 인터페이스 또한 달라져야 한다. 따라서 메타데이터 템플릿의 내용에 맞는 사용자 인터페이스가 자동적으로 생성 가능해야 한다.

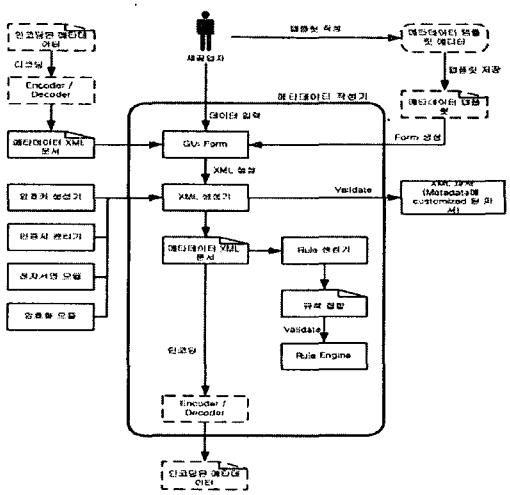

그림 7. 메타데이터 작성기

4) XML 생성기

사용자가 입력한 내용을 바탕으로 XML 형태의 메타데이터 문서를 생성한다.

5) Encoder/Decoder

메타데이터 XML 을 미리 정의된 규칙에 의하여 인

코딩, 디코딩한다.

6) Secure Container 생성기

메타데이터와 컨텐츠를 하나의 secure container 에 바인딩하는 도구이다. 컨텐츠는 필요에 따라 암호화될 수 있다.

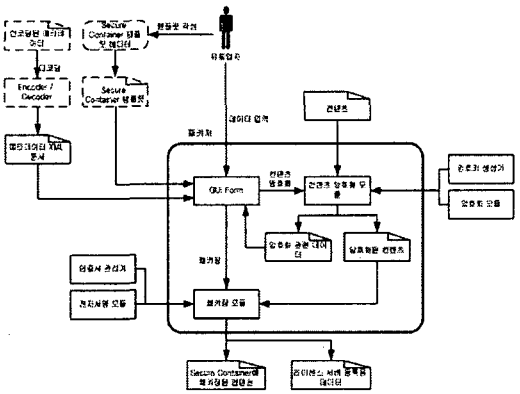

그림 8. Secure Container 생성기

7) Secure Container 템플릿 해석기

Secure container 템플릿의 정보를 읽어 secure container 내부 데이터들을 구조화시킨다.

8) Secure Container 해석기

패키징된 secure container 로부터 메타데이터와 컨텐츠를 분리한다

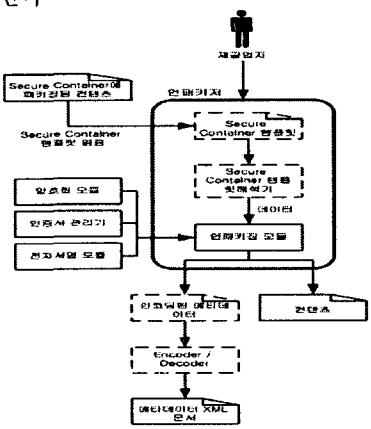

그림 9. Secure Container 해석기

9) Rule 생성기

메타데이터의 정보를 읽어 rule engine 을 위한 규칙 집합을 생성해낸다.

10) Rule Engine

규칙 집합들을 입력으로 받아서 규칙들의 무결성을 검사한다.

11) 컨텐츠 암호화 모듈

대칭키를 사용하여 컨텐츠를 암호화한다. 컨텐츠를 여러 개의 블록으로 나누고 각각 다른 키를 사용하여 암호화 가능하다.

12)메타데이터 템플릿

사용자가 선택한 메타데이터 요소들에 대한 정보를 담고 있는 데이터이다.

13)Secure Container 템플릿

secure container 의 내부 구조를 정의한 데이터이다.

5. 결론 및 향후 연구

본 논문에서는 창조자, 유통업자, 구매자, 클리어링하우스가 참여하는 유통모델에서 창조자와 유통업자가 각각 컨텐츠를 패키징할 수 있도록 secure container 와 컨텐츠 패키저의 구조를 설계하고, 이를 이용한 컨텐츠 유통 방법에 대하여 설명하였다.

본 논문에서 설계한 컨텐츠 패키저는 현재 서비스되고 있는 DRM 유통 모델보다는 복잡한 유통모델을 지원할 수 있지만, 다양한 컨텐츠 유통모델을 지원하기 위한 패키저의 모델로는 부족한 점이 있다. 클리어링하우스에 의존적이므로 여러개의 클리어링하우스를 사용하는 컨텐츠 유통 모델에서는 적용하기가 어렵다.

향후에는 이 같은 문제를 해결할 수 있도록 secure container 의 구조와 패키저의 구조를 개선해 나가는 방향으로 연구를 진행할 것이다.

참고문헌

[1] 강호갑, "DRM 기술동향", 계간저작권, 2001.

[2] InterTrust SDK

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

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

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

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