情報保護學會論文誌
第16卷 第2號, 2006. 4

OMA 구조를 이용한 안전한 전자문서 관리를 위한 DRM 시스템 구현*

신 영 찬[1†], 최 효 식[1], 김 용 구[1], 최 석 진[2], 류 재 철[1‡],
[1]충남대학교, [2]국가보안기술연구소

Implementation of Digital Document Management DRM System with OMA Structure*

Young-Chan Shin,[1†] Hyo-Sik Choi,[1] Yong-Goo Kim[1],
Seoko-jin Choi[2], Jae-Cheol Ryou[1‡]
[1]Chungnam National University, [2]National Security Research Institute

요 약

얼마 전, 국가 주요기관에 해커가 침입하는 사건이 발생하였다. 이러한 사고의 경우 기관 혹은 기업의 기밀문서에 해당되는 전자문서들의 유출이 발생할 수 있으며, 이에 따른 금전적 혹은 이미지 손상 등에 대한 피해를 발생시킬 수 있다. 이러한 전자문서 유출에 대한 피해를 줄이기 위해서는 안전하고 다양한 전자문서 규격을 제공하는 전자문서 관리 시스템이 필요하다. 하지만 전자문서의 특성상 이용하는 어플리케이션에서 종속되어 보안기능이 제공되고 있어 통일된 보안정책의 수립이 어려울 실정이다. 본 논문은 안전하고 호환성 있는 전자문서의 이용을 위하여 오픈 소스인 OpenOffice와 DRM 표준중 하나인 OMA의 규격을 기반으로 하는 전자문서 관리에 이용에 사용될 DRM 시스템의 구조를 제안하였다. 더불어 권한관리자를 통하여 문서의 권한을 분배, 이용하는 방식으로 DRM 시스템 구성 요소들 사이의 프로토콜을 제안하고 설계 구현하였다.

ABSTRACT

As widespread of using digital documents in various fields, control the usage of digital document is needed. So, Digital Rights Management(DRM) will become a key component of digital document system, but absence of proper digital document DRM system, there is a real risk to lose important information when a hacker achieved intrusion in important system. This paper designs and implements digital document DRM system based on OMA(Open Mobile Alliance) DRM model and OpenOffice. We considered being a digital document DRM system to contain appropriate solution of security and document compatibility.

Keywords : *DRM, 전자문서 보안, 문서 관리*

Ⅰ. 서 론

컴퓨터 기술이 발전하고 대중화됨에 따라, 아날로그 형태로 생산, 보관, 관리되던 일반 상거래의 저작물들이 대부분 디지털화 되어가고 있다. 더불어 이러한 디지털 저작물들의 유통환경이 인터넷을 통하여 발달됨에 따라 원저작자에 대한 권익을 보호하기 위한 DRM(Digital Rights Management)기술이 저작물 유통시스템에 적용되어지고 있고 이러한 저작물보호를 위한 기술들은 대부분

접수일: 2005년 11월 10일: 채택일: 2006년 2월 27일
* 본 연구는 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음.
† 주저자 : badbabu@home.cnu.ac.kr
‡ 교신저자 : jcryou@home.cnu.ac.kr

상업성을 위한 미디어 콘텐츠 중심으로 개발되어지고 있다[1,2,4,10]. 하지만 흔히 접하는 전자문서의 보안과 유통에 대한 연구는 따로 진행되고 있지 않은 실정이다.

대부분의 기업과 정부기관들은 인가된 주체나 권한이 있는 사용자들에게만 특정 데이터 또는 자원들이 제공되는 것을 보장하기 위해 접근제어 또는 권한부여 기술을 적용하고 있다. 접근제어 또는 권한부여 기술은 일반적으로 어떤 사용자 또는 사용자 집단이 자원에 대해서 조회, 변경 등 연산의 수행 여부를 제한할 수 있는 수단이다. 하지만 권한을 부여받은 사용자에 대해서는 문서에 대한 제한사항을 부여하지 않고 있다. 이와 같이 부분적인 제안수단을 동원하는 경우는 조직에서 문서 유출의 빈도가 조직내 구성원에 의해 이루어지는 비율을 감안한다면 문서 보안의 측면에서 바람직한 방법이 아니다. 이와 같은 문제를 극복하기 위해서는 문서에 특정한 권한을 부여하기 위한 DRM의 도입이 절실히 필요하다.

하지만 문서관리가 가능한 DRM 시스템의 개발은 전용 어플리케이션을 개발하는 멀티미디어 분야와는 달리 기존의 응용프로그램을 유지하는 상태에서 동작하여야 하는 제약 사항이 존재한다. 이와 더불어 DRM 문서의 다양한 공유를 위한 호환성 문제가 존재한다.

본 논문에서는 워드프로세스, 스프레드쉬트, 프리젠테이션등의 오피스 제품기능과 다양한 운영체제와 문서 형식을 제공하는 소스코드 공개버전인 오픈오피스(OpenOffice)를 이용하여 문서 호환성 문제를 해결한다. 그리고 DRM 문서의 유통을 위해 현재 가장 활발히 진행되고 있는 DRM 표준중 하나인 OMA DRM v2.0에 준수하는 시스템의 구조를 통해 상호 호환문제를 해결하는 안전한 전자문서 관리 시스템을 제안하고 이를 설계 구현하였다.

본 논문에서는 OMA DRM v2.0에 준수하는 문서 형태의 유통을 통해 안전한 전자문서 관리시스템을 제안하고 이를 설계 구현하였다.

본 논문은 2장에서 DRM 관련 동향을 알아보고 3장에서 제안한 시스템의 구성에 대하여 설명한다. 그리고 4장에서 본 논문에서 제안한 전자문서 관리 시스템의 설계 및 구현 내용에 대하여 설명하고, 5장에서 구현 및 시험 결과를 기술하였다. 마지막으로 6장에서 결론을 기술하였다.

Ⅱ. DRM 관련 연구

본 장에서는 제안 시스템에서 이용하는 DRM 표준인 OMA와 문서 어플리케이션에 적용된 DRM의 기능과 특징에 대하여 기술한다.

1. OMA(Open Mobile Alliance)

OMA DRM의 표준은 현재 2.0버전까지 발표되었다[12,13]. OMA DRM 기술은 웹등을 통한 유료 콘텐츠의 불법 배포를 방지하기 위해 개발된 솔루션으로 윈도우, 리눅스 등 다양한 환경에 모두 적용할 수 있는 특징이 있다. 또 오디오와 비디오, 스트리밍 콘텐츠에 대한 지원을 향상시켰으며 다양한 기기를 통해 전송되는 콘텐츠의 불법복제 및 저작권 침해방지 기능이 포함되어 있다. 또한, ISO/IEC, 3GPP, w3c등과 같은 기존의 표준 기구들의 표준을 많이 원용하고 채택하여 기술의 적용 범위가 넓다.

2. 주요 문서 어플리케이션 보호기술

1) Microsoft Office

MS 오피스는 RMS(Rights Management Services) 및 IRM(Information Rights Management)을 이용하여 DRM을 위한 정보 보호 기술을 반영하고 있다.

① RMS(Rights Management Services) : RMS는 온라인 및 오프라인, 그리고 방화벽 내부 및 외부에서 디지털 정보를 무단으로 사용하지 못하도록 막아주는 정보 보호 기술이다. RMS를 이용하면 MS Windows Server, 개발자 도구 그리고 암호화, XML 기반 인증서, 인증 등을 포함한 보안 기술을 결합해 정보가 어디로 전달되건 관계없이 지속적인 보안 정책을 적용할 수 있다.

② IRM(Information Rights Management) : IRM은 RMS를 확장한 정보 보호 기술이다. 정보 제공자는 문서를 열람할 수 있는 사용자를 규정하고 수신자가 해당 문서를 사용할 수 있는 방법의 기술이 가능하다. 즉, 문서를 열고 이를 변경, 출력, 전송하거나 기타 작업을 할 수 있는 권한을 세부적으로 제어할 수 있다.

2) Adobe Acrobat Professional

Acrobat은 기본적으로 암호기능이 제공되어지며

파일에 대한 다양한 접근을 제어한다. 파일에 대한 출력이나 문서내의 자료에 대한 복사와 수정 기능 등에 대한 보안기능들이 아래의 3가지 방법에 의해 제공된다.

① 문서 암호화(Document Encryption) : 정보 권한 관리와 공유 패스워드 암호화 및 사용자 지정 암호화를 통해 문서의 기밀성을 보장한다. 암호화 방법은 두 가지로 공유 패스워드 암호화와 사용자 지정 암호화가 있다. 공유 패스워드 암호화는 문서에 하나의 암호를 설정하여 일괄적인 제어 가능하도록 하는 것이고, 사용자 지정 암호화는 문서의 이용자별로 암호를 달리 설정하여 개별적인 제어 가능하도록 한다.

② 전자서명(Digital Signature) : PKI의 특징을 이용한 전자 서명은 내용의 무결성, 인증 및 부인방지의 부가적인 문서보호를 보장한다.

③ 문서 제어(Document Control) : 문서의 열람, 수정, 인쇄 등의 특정 기능을 제한하여 특정 사용자의 문서에 대한 접근제어를 보장한다. 이러한 제어는 암호화 방법에 따라 모든 사용자 또는 개별 사용자로 나누어 적용할 수 있다.

III. 전자문서 DRM 시스템 구성

본 논문에서 이용하는 OMA 모델에서 제안하는 환경의 경우 콘텐츠가 모바일 디바이스에 종속되고 이를 이용하여 사용자의 인증이 가능한 모바일 환경이다. 하지만 일반적인 컴퓨팅 환경의 경우 사용자의 이동이 빈번히 일어며 사용자의 인증에 시스템을 이용할 수 없기 때문에 전자문서 유통을 위한 DRM 모델의 경우 시스템을 이용하여 인증을 확인하고 권한을 저장하는 것은 제약이 따른다. 때문에 본 논문에서 설계·구현한 시스템은 각 사용자의 권한을 권한 관리자(Right Manager)에서 관리함으로 기존 OMA의 각 디바이스에 종속되어 권한이 이용되는 것과는 다르다. 본 장에서는 OMA DRM에서 제안하고 있는 두가지 모델인 Separate Delivery와 Superdistribution을 적용한 문서 분배방식의 흐름과 제안하는 시스템 모델에서 적용한 전체적인 흐름 및 구성 요소들에 대해 설명한다.

1. 문서 분배방식에 따른 흐름

1) Separate Delivery

Separate Delivery는 관용 암호화 방식을 이용하여 안전하게 보호되어지는 DRM Content Format(DCF) 과 이를 이용하기 위한 사용권한을 분리하여 클라이언트 시스템에 전송해주는 방식이다[13]. 사용권한에 포함된 Content Encryption Key (CEK)를 소유하지 않은 사용자는 전자문서를 이용할 수 없으므로 전자문서를 안전하게 보호할 수 있다.

본 논문에서 Separate Delivery의 경우, DCF는 사용자의 시스템으로 전송하지만, 사용권한은 Right Manager(RM)로 전송하여 안전하게 관리가 된다.

2) Superdistribution

Superdistribution은 전자문서에 대한 추가적인 권한을 허용하는 진보된 Separate Delivery 방식이다[3,8,9]. 클라이언트 시스템 사이에서는 자유롭게 DRM 전자문서가 유통되고, 다른 클라이언트로부터 DRM 전자문서를 제공받은 시스템은 DRM 전자문서에 명시된 사용권 발행자를 통하여 사용권 요청을 통하여 이용이 가능하다. 일반적인 전자문서 이용 시스템의 경우, 이동과 복사가 간단하기 때문에, 이 방식을 통하여 자유로운 전자문서의 이동이 가능하다.

2. DRM 시스템 모델

안전한 전자문서 관리 시스템은 패키징 관리자(Packaging Manager), 문서 분배자(Document Distributor), 권한 관리자(Right Manager)의 서버와 Linux, Windows를 이용하는 클라이언트로 구성된다. 문서 분배자는 문서 유통이 필요한 도메인에 존재하는 중개 서버이며, 권한 관리자는 사용권한 발행 및 관리를 중개해 주는 역할을 한다. 본 논문에서 구현한 전체적인 전자문서 관리 DRM 시스템의 모델은 [그림 1] 과 같다.

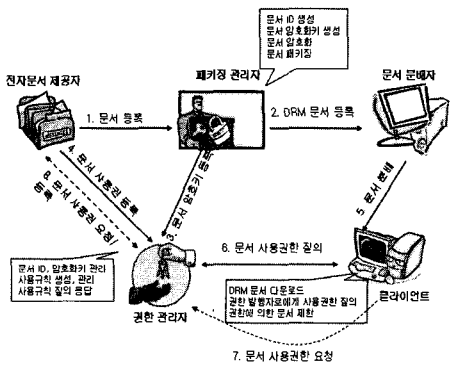


그림 1. 전자문서 관리 DRM 시스템 모델

⊙ 전자문서 제공자 : 원본 전자문서에 대한 저작권을 가지고 있으며 패키징 관리자를 통해 전자문서를 등록한다. 등록된 DRM 전자문서에 대한 사용권한을 등록, 삭제한다.
⊙ 패키징 관리자 : DRM 전자문서 생성을 위하여 문서 ID를 생성하며, 이에 이용된 암호화키를 권한 관리자에 등록한다. 가공되어진 DRM 전자문서는 문서 분배자에 등록한다.
⊙ 권한 관리자 : 클라이언트에 대한 전자문서 권한을 발행, 관리 해주는 서버이다. 클라이언트 시스템은 권한 관리자를 통하여 권한을 확인 후 문서 분배자로부터 다운받은 전자문서를 이용할 수 있다. 또한, 전자문서에 대한 권한이 필요한 경우, 전자문서 제공자에 대한 요구를 통하여 권한 등록을 중개해 주는 역할을 한다.
⊙ 문서 분배자 : 패키징 관리자로부터 제공받은 가공된 전자문서에 대한 정보를 알려주며, 이를 보관하고 있는 서버이다. 클라이언트는 문서 분배자에 접근을 통하여 가공된 전자문서를 받는다.
⊙ 클라이언트 : 전자문서를 이용할 수 있는 Linux, Windows를 이용하는 시스템을 의미한다.

Ⅳ. 전자문서 DRM 시스템 설계 및 구현

본 장에서는 제안하고자 하는 전자문서 DRM 시스템에 대해 기술한다. 본 논문에서 설계·구현한 시스템은 다음과 같은 몇가지 가정을 도입한다.

⊙ 각 참여자는 CA로부터 발급되어진 공개키-개인키 쌍과 공개키 인증서를 가지고 있으며, 이를 통하여 서로간의 인증이 가능하다.
⊙ 패키징 관리자와 문서 분배자, 권한 관리자는 문서 유통이 필요한 도메인에 속해 있으며, 사용자의 정보는 도메인의 서버에 ID와 Password를 통하여 저장되어 진다.
⊙ 클라이언트는 항상 네트워크를 통하여 각 서버에 접근이 가능하다.

1. 주요 데이터 형식

1) Secure Document Format(SDF)

전자문서를 DRM 형태로 가공을 위하여 SDF 형식을 정의하여 사용하였다. SDF 형식은 OMA DRM v2.0에서 정의한 DCF 형식을 따르며 이중 Discrete Media Profile만을 이용한다. OMA DRM v1.0의 DCF에서는 Superdistribution 제공을 위한 추가적인 필드의 정의가 필요하였지만 v2.0에서 부터는 이를 위한 필드 및 좀더 자세한 정보의 기술이 가능하다. SDF는 아래와 같은 정보로 구성된다.

⊙ 문서 식별자(Content ID)
⊙ 문서 암호화 정보(암호 알고리즘, 패딩 방법)
⊙ 문서 정보(길이, 타입 등)
⊙ 권한 발급자 정보(RightIssuerURL)

2) Right

DRM 문서의 사용을 위하여 부여된 사용권한 및 사용조건에 관한 정보 표현하기 위해 ODRL(Open Digital Rights Language)와 OMA REL(Rights Expression Language)를 확장 이용하여 정의하였다[14]. Right는 아래와 같은 정보로 구성된다.

⊙ Content ID, version 등과 같은 DCF 정보
⊙ 사용 권한 및 암호화 정보
  ▷ 사용 규칙(Display, Print, Copy) 및 제약사항
  ▷ 암호화키(Content Encryption Key)

2. 권한 전송 프로토콜

전자문서 DRM 시스템에 있어서 권한 요청·응답을 위한 권한 관리자와 클라이언트 간의 프로토콜을 살펴보기로 한다.

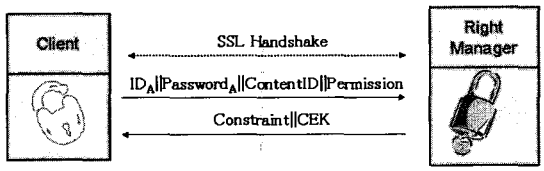


그림 2. SSL 전송 프로토콜

권한 전송 방식은 두가지 방법으로 구분된다. 하나는 PKI를 통한 공개키 이용 방법과 ID/Password를 확장시킨 방법이다.

우선 첫 번째 방법은 공개키를 이용하는 것으로, [그림 2]와 같이 SSL을 이용한 안전한 채널을 통한 메시지 통신 방법이다[11,15].

클라이언트는 SSL을 이용하여 서버와 안전한 채널을 생성후 권한을 요청·응답 받는다. 이와 같은 경우 SSL을 이용하기 때문에 안전한 방법이긴 하지만, 권한 요청·응답이 많아 채널의 설정이 많은 경

우 클라이언트와 서버에 오버헤드가 생기게 된다.

두 번째 프로토콜은 미리 등록된 사용자의 Password를 이용하는 [그림 3]과 같은 방법이다.

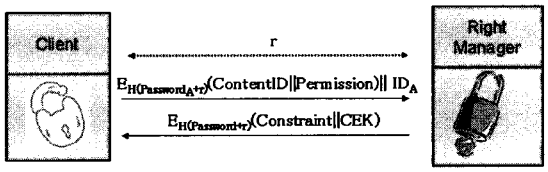


그림 3. Password 이용 전송 프로토콜

권한 관리자는 클라이언트에게 세션키 생성에 사용할 난수 r을 전송한다.

클라이언트는 자신이 속한 도메인에 등록된 PasswordA와 전송받은 난수 r을 함수 h로 처리하여 세션키를 생성하고, 이를 이용하여 ContentID(CID)와 Permission을 암호화한 후, IDA와 함께 권한 관리자에 전송한다.

권한 관리자는 IDA를 이용하여 PasswordA를 찾은 후 세션키 H(PasswordA+r)을 생성하여 메시지를 복호화 하여, ContentID, Permission을 확인한다. 마지막으로 세션키를 이용하여 제약사항과 CEK를 암호화 하여 전송한다.

이 방법의 경우, 권한 관리자와 클라이언트간의 응답·요청이 많을 경우 오버헤드를 줄이며 안전한 통신을 제공한다.

3. 패키징 관리자(Packaging Manager)

패키징 관리자는 전자문서 제공자로부터 받은 문서를 암호화 하여 DRM 문서로 패키징 하고 생성된 전자문서와 CEK를 등록하는 역할을 한다. 웹 브라우저를 통하여 패키징에 필요한 정보를 입력 받아 문서 패키징 모듈에 패키징을 요청한다. 문서 패키징 모듈은 CID 생성기에서 고유한 ID를 생성하고 CEK 생성기를 통해 문서 암호화에 이용할 키인 CEK를 생성한다. 그리고 전달받은 문서를 CEK로 암호화 한 후 DRM 문서(SDF)으로 패키징 한다. 이때 생성된 DRM 문서와 CEK는 각각 문서 분배자와 권한 관리자에게 등록된다. 패키징 관리자의 전체 처리 흐름은 [그림 4]와 같다.

4. 권한 관리자(Right Manager)

권한 관리자는 클라이언트가 이용할 권한을 등록해주는 역할과 등록된 권한을 관리해 주는 역할을 하는 서버이다. 권한 관리자는 [그림 5]와 같은 순서로 클라이언트가 이용할 권한등록을 처리한다.

전자문서 제공자는 자신이 등록한 DRM 문서를 이용할 사용자와 permission, constraint를 등록한다. 이와 같은 권한등록 과정은 전자문서 제공자가 직접 클라이언트를 선택하여 등록이 되어 지거나 혹은, 사용자가 DRM 문서를 문서 분배자 혹은 Superdistribution을 통해 전달받거나 자신이 가진 권한이 만료되었을 경우 클라이언트는 DRM 문서에 명시된 RightIssuer정보를 이용하여 권한 관리자에게 권한 요청을 할 수 있다[7].

클라이언트는 권한 관리자에게 자신이 가진 권한 정보의 확인을 통하여 위의 [그림 6]과 같이 DRM 문서를 사용할 수 있는 권한의 획득이 가능하다. 권한 확인을 위하여 4-2장에서의 사용자 인증을 통과한 후, CID와 확인하고자 하는 Permission을 권한 관리자에 요청한다. 사용권한 확인모듈은 Permission과 Constraint확인 모듈에 사용자에 적합한 권한이 있는지를 확인 후, 사용권한 발행모듈에 권한 발급을 요청한다. 사용권한 발행모듈은 CEK

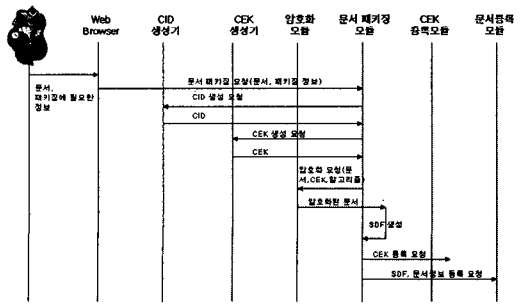


그림 4. 문서 패키징 흐름

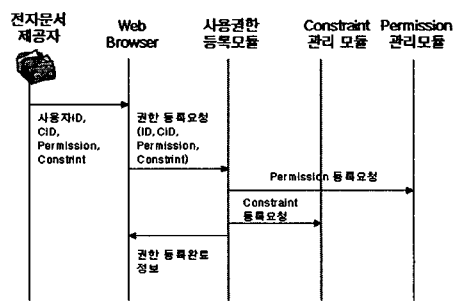


그림 5. 권한등록 흐름

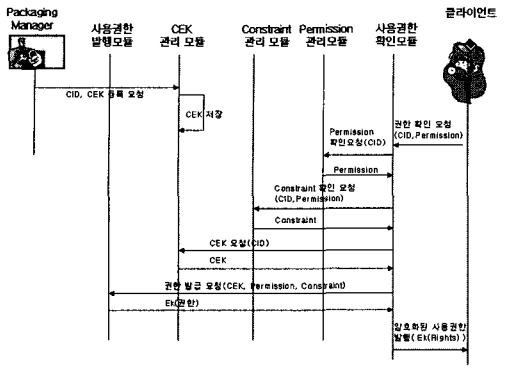


그림 6. 권한 확인 흐름

와 사용자가 이용 가능한 Constraint등의 정보를 암호화 하여 사용권한 확인모듈에 전달하고, 다시 클라이언트에게 전달한다.

5. 문서 분배자(Document Distributor)

문서 분배자는 [그림 7]과 같이 DRM 문서와 정보를 관리하는 서버이다. 우선 패키징 관리자로부터 받아진 정보를 저장하는 문서 등록모듈과 문서정보를 저장하고 관리, 사용자로부터 HTTP 요청을 받아 문서정보를 보여주는 문서정보 관리모듈이 있다.

그리고 DRM 문서를 저장하고 관리하며 문서제공 요청을 받으면 DRM 문서를 검색하여 클라이언트 시스템에 전송하는 역학을 하는 DRM 문서 관리모듈이 있다.

6. 클라이언트 시스템

1) 구성 요소

전자문서 관리를 위한 DRM 시스템의 클라이언트 구성요소는 [그림 8]과 같다.

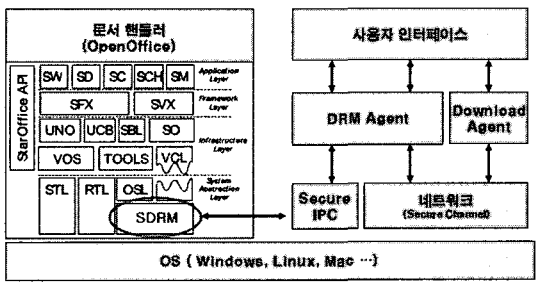


그림 8. 클라이언트 구성요소

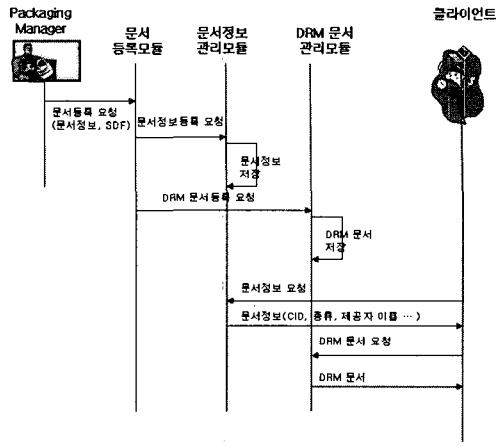


그림 7. 문서 분배 흐름

⊙ 문서 핸들러(Document Handler) : DRM 문서를 이용하기 위한 응용프로그램이다. DRM 문서의 경우 SDRM(Secure DRM Module)을 통해서만 이용이 가능하다.

⊙ 문서 관리자(Secure DRM Module) : 사용자에 할당된 권한정보를 DRM 에이전트로부터 얻어 문서 사용을 제어한다. 사용권한이 있는 경우에만 복호화를 통해 사용 가능하게 한다.

⊙ DRM 에이전트(DRM Agent) : 문서 관리자로부터 요구받은 권한 확인요청을 권한 관리자에게 요청, 응답을 받는 역할을 한다. 또한 클라이언트 시스템 전반에 관한 사용자와 자원 관리기능과 API와 메시지 후킹을 통하여 시스템 상에서의 원활한 DRM 클라이언트 진행을 관리한다.

2) DRM 문서 설치

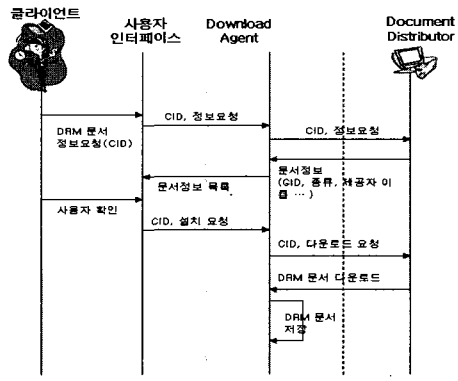


그림 9. DRM 문서 다운로드 흐름

다운로드 에이전트는 [그림 9]와 같은 과정을 거쳐 클라이언트에 DRM 문서를 설치한다.

3) DRM 문서 사용

문서 핸들러가 DRM 문서를 사용하는 과정은 [그림 10]과 같다.

사용자가 DRM 문서를 이용하는 경우, 문서 핸들러는 문서 관리자를 통해 평문 문서를 요청하게 된다. 문서 관리자는 DRM 에이전트에게 사용권한 확인 요청을 하며, DRM 에이전트는 문서를 사용하고자 하는 사용자의 정보를 획득한 후, 권한 관리자에게 안전한 채널을 통해 권한 확인 요청을 한다. 권한 관리자는 요청한 사용자와 ContenetID에 부합되는 권한의 존재를 확인 후, CEK와 제약사항을 포함하는 권한을 전달한다. 얻어진 CEK와 제약사항을 확인하여 문서 관리자는 DRM 문서의 복호화를 통해 평문 문서를 추출하고, 이를 이용하여 사용자에게 적당한 제약사항을 적용하여 제공한다.

[그림 11]은 만약 사용자가 해당 DRM 문서에 대한 적절한 권한이 존재하지 않는 경우 DRM 문서에 존재하는 RightIssuer 정보를 이용하여 Superdistribution에서 사용권한을 발급받는 과정을 보여준다.

DRM 에이전트는 사용자에게 문서의 권한이 없음을 알리고 사용자로부터 이용하고자 하는 문서의 CID와 권한 정보를 입력받아 권한 관리자에게 권한 발급 승인요청을 한다. 전자문서 제공자는 이 정보는 판단하여 권한 관리자에 사용자에 대한 권한을 추가하게 된다. 이후의 처리 과정은 DRM 문서 사용흐름과 동일하게 처리된다.

V. 구현 및 평가

1. 실험 환경

본 논문에서 구현한 시스템의 개발환경은 [표 1]과 같다.

표 1. 개발 환경

구 성 요 소	개 발 환 경
패키징 관리자	운영체제 : Windows Server 2003 개발언어 : JSP, C/C++ Web Server : IIS User Interface : Web Browser
문서 분배자	운영체제 : Windows Server 2003 개발언어 : JSP, PHP Web Server : IIS Data Base : My SQL User Interface : Web Browser
권한 관리자	운영체제 : Windows Server 2003 개발언어 : JAVA Data Base : My SQL Network : TCP/IP Socket
DRM 에이전트	운영체제 : Windows XP 개발언어 : JAVA, C/C++ Network : TCP/IP Socket User Interface : Web Browser
문서 관리자	운영체제 : Windows XP 개발언어 : C/C++ 문서 핸들러 : OpenOffice

2. 시험 결과

전자문서 제공자는 [그림 12]와 같은 사용자 인터페이스를 이용하여 전자문서를 등록한다. 전자문

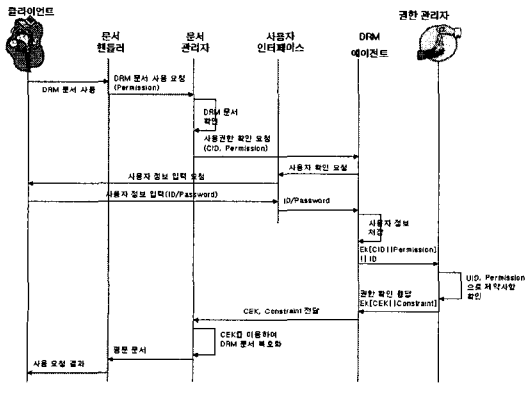


그림 10. DRM 문서 사용 흐름

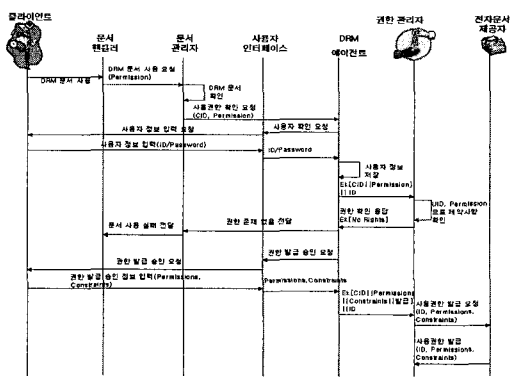


그림 11. 클라이언트 권한 요청 흐름

서가 DRM 문서로 패키징 되면 자동으로 문서 분배자에 등록되고, 이때 이용된 CEK는 권한 관리자에 등록된다. 이후, 전자문서 제공자는 등록된 DRM 문서에 대한 권한을 [그림 13]과 같이 추가할 수 있다.

클라이언트 사용자가 사용하고자 하는 DRM 문서는 문서 배분자를 통하여 클라이언트 시스템에 설치가 가능하다. DRM 문서를 문서 핸들러를 통해 처음 이용할 경우 [그림 14]와 같이 사용자의 기본 정보를 입력하게 되고, 이 정보는 DRM 에이전트를 통해 권한 관리자로 전달되어 권한 확인이 이루어진다.

만약, 사용자가 요청한 DRM 문서에 대한 권한이 적합하지 않은 경우, 사용자는 [그림 15]와 같이, 원하는 권한을 요청·획득함으로써 이용 가능하다.

3. 제안시스템 고찰

본 시스템에서 구현한 문서 DRM 시스템은 기본적으로 OMA DRM v2.0에서 정의한 DCF 형태의 문서 구조를 유지하며 OMA DRM에서는 정의하지 않은 일반적인 컴퓨팅 환경에서의 보안구조와 추가적으로 문서 콘텐츠 타입을 포함하는 모델을 제시하였다. 현재 일반적으로 이용하는 DRM 시스템의 경우 문서의 암호화에 단순히 키를 이용하고 권한 정보 역시나 암호화된 문서에 추가하는 "Forward Lock" 혹은 "Combined Delivery" 를 제공하는 수준에 머무르고 있을 뿐, 좀 더 진보된 "Separate Delivery" 혹은 "Superdistribution"등을 이용한 문서를 임시적으로 이용하게 하는 사용권한 발급 기능 등은 제공하지 않고 있다.

[표 2]는 제안 시스템과 일반 문서 어플리케이션에서 제공하는 DRM 기능을 비교한 것이다.

제안 시스템의 경우 Windows, Mac, Linux등 운영체제에 유동적으로 대처가 가능하다. 또한 일반적으로 라이센스(권한)를 암호화된 콘텐츠에 삽입시키는 것에 반해 제안 시스템에서는 권한을 따로 관리함으로써 Superdistribution이 가능한 메커니즘을 제공한다. 더불어 OMA의 표준 포맷을 준수하였기 때문에 유선환경 뿐 아니라 무선 환경에서 역시나 적용 가능 하고 다양한 문서 형태를 지원함으로 문서 유통에 유동적으로 대처할 수 있다.

Ⅳ. 결 론

본 논문에서는 안전한 전자문서 관리를 위한 DRM 시스템을 설계 및 구현하였다. 본 시스템의 설계 및 구현시 우선사항은 현존하는 다양한 문서 형태를 그대로 유지하며, 안전한 문서 유통 및 이용을 위한 모델의 제안이었다. 이를 위하여 현재 가장 활발히 표준화가 이루어지고 있는 OMA DRM v2.0 표준을 유선 환경과 문서 관리로 확장하여 시스템을 구현하였다.

표 2. DRM 시스템 비교

	Microsoft Office	Acrobat	아래아 한글	제안 시스템
다양한 운영체제 지원	Windows	Windows, Mac, Linux	Windows	Windows, Mac, Linux
권한 관리	콘텐츠에 삽입	콘텐츠에 삽입	콘텐츠에 삽입	독립적 권한 관리
Superdistribution 지원	No	No	No	지원
문서 암호화 메카니즘	128 bit AES	40/128 bit RC4	압축기술	128 bit AES
유·무선 연동	No	No	No	고려
DRM 문서 핸들러	Microsoft Office	Acrobat Reader	한글과 컴퓨터	공통 Viewer를 통한 문서 제어 (Office, 한글 등 지원)

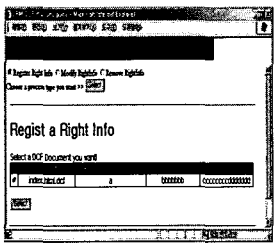


그림 12. 권한 발급

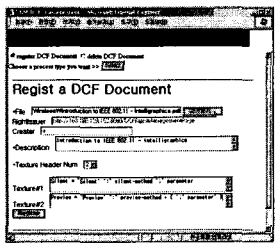


그림 13. 전자문서 패키징

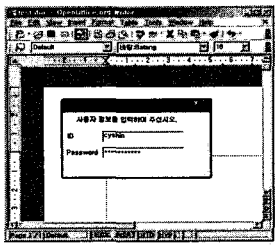


그림 14. 사용자 정보 입력

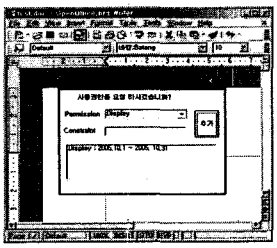


그림 15. 사용권한 요청

본 논문에서 제시한 DRM 시스템에서는 클라이언트가 문서 분배자로부터 DRM문서를 제공받고, 해당 문서에 대한 사용권한은 전자문서 제공자로부터 발급되어진다. 또한 발급되어진 권한정보는 권한 관리자에서 저장되어져 서비스되어 각 클라이언트 시스템에서 권한 저장을 위한 추가적인 장비가 불필요하게 되는 장점을 가진다. 특히나 일반적으로 권한이 삽입된 암호화된 콘텐츠의 경우 콘텐츠의 복사본, 혹은 디스크 자체의 복사본을 이용하여 복원할 경우와 같은 불법 사용을 방지할 수 없다는 점이다. 시큐어 데이터베이스 혹은 IC Card등의 저장장치를 이용한다 하더라도 불법적인 데이터 변조가 가능하다면 마찬가지로 방어가 불가능하다. 하지만 제안 시스템에서는 중앙의 권한 관리자가 권한의 추가·갱신·요청·응답의 역할을 대신함 으로써, 사용자가 하나의 시스템에 종속되지 않고 다양한 장소에서 이용이 가능하며 불법적인 권한의 변조가 불가능하다는 장점을 지닌다. 하지만 DRM 문서를 이용하기 위해서는 무선 혹은 유선을 이용하여 권한 관리자에게 접속해야 하며, 문서의 권한확인 요청이 증가하게 되면 클라이언트와 서버에 약간의 오버헤드가 발생하게 된다.

본 논문에서는 권한의 사용을 하나의 문서사용 도메인으로 가정하여 설계하였다. 문서를 사용하기 위한 도메인과 다른 도메인 사이에서는 권한을 표현하기위한 언어와 DRM 문서의 표준이 서로 다를 수 있다. 이를 중개하기 위해서는 OMA의 표준 뿐 아니라 그밖의 XrML(eXtensible rights markup Language)이나 ODRL(Open Digital Rights Language), XMCL(eXtensible Media Commerce Language)등에 문서사용을 위한 형태로의 확장을 통해 호환성의 문제를 해결하기 위한 방안의 연구가 필요할 것이다[5,6].

참 고 문 헌

[1] Bill Rosenblatt, Bill Trippe, Stephen Mooney, "Digital Rights Management, Business and Technology", Published by M&T Books, pp79-102, 200

[2] U. Kohl, "Secure Container Technology as a Basis for Cryptographically Secured Multimedia Communication, "Proc. Multimedia and Security Workshop at ACM Multimedia '98, Sep. 1998

[3] M. arc, A. Kaplan, IBM Cryptolopes TM, "SuperDistribution and Digital Rights Management", http://www.research.ibm.comm/people/k/kaplan, Dec., 1996

[4] F. Hartung, F. Ramme, Digital rights management, and watermarking of multimedia content for m-commerce applications, IEEE Communications Magazine, Vol.38, No.11, pp.78-84, Nov., 2000.

[5] http://www.odrl.net, ODRL

[6] http://www.XrML.org, XrML

[7] T. Berners-Lee, U.C., Irvine,L., Masinter, Aug, 1998, "Uniform Resource Identifiers(URI): Generic Syntax", RFC2396

[8] R. Mori, M.Kawahara, "Superdistribution : The concept and Architecture", Transactions on the IEICE, Vols.E 73, No.7 July, 1990

[9] J. Jeon, S.Park, "DRM Security Framework:ID-Based Approach for Content Super-Distribution," SCI, 2001

[10] W. Shaprio, R. Vingralek, "How to Manage Persistent State in DRM Systems," LNCS 2320, pp176

[11] V. Gupta, S. Gupta, S. Chang, "Performance Analysis of Elliptic Curve Cryptography for SSL", Proc. of the ACM Workshop on Wireless Security, ACM Press, 2002, Atlanta (GA), USA.

[12] http://www.openmobilealliance.org/release_program/drm_v20.html, Open Mobile Alliance. DRM

[13] http://www.openmobilealliance.org/release_program/drm_v20.html, Open Mobile Alliance. DRM Specification V2.0. Candidate Version 2.0. December 2004. OMA-DRM-DRM-V2_0-20041210-C.

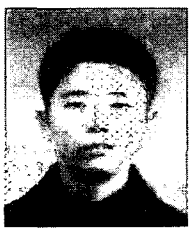
[14] http://www.openmobilealliance.org/release_program/drm_v20.html, Open Mobile Alliance. DRM Rights Expression Language V2.0, Candidate Version 2.0, December 2004. OMA-DRM-REL-V2_0-20041210-C.

[15] M. Meyers et al., ""X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"", RFC 2560, The Internet Society, 1999.

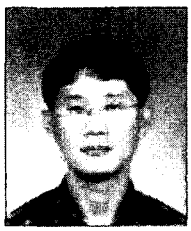
〈著者紹介〉

신 영 찬 (Young-chan Shin) 학생회원
2003년 2월: 충남대학교 컴퓨터과학과 졸업
2005년 2월: 충남대학교 컴퓨터과학과 석사
2005년 3월~현재: 충남대학교 컴퓨터공학과 박사과정
〈관심분야〉 디지털 콘텐츠 보안, 인증시스템, 유·무선 인터넷 보안

최 효 식 (Hyo-sik Choi) 학생회원
2005년 2월: 충남대학교 컴퓨터공학과 졸업
2005년 3월~현재: 충남대학교 컴퓨터공학과 석사과정
〈관심분야〉 무선 인터넷 보안, 디지털 콘텐츠 보안, 네트워크 포렌식무선 인터넷 보안



김 용 구 (Yong-goo Kim) 학생회원
2005년 8월: 충남대학교 컴퓨터공학과 졸업
2005년 9월~현재: 충남대학교 컴퓨터공학과 석사과정
〈관심분야〉 디지털 콘텐츠 보안, 인증시스템, 유·무선 인터넷 보안



최 석 진 (Seok-jin Choi) 정회원
1995년 8월: 경북대학교 전자공학과 졸업
1998년 2월: 한국과학기술연구원 전자공학과 석사
2005년 3월~현재: 고려대학교 정보보호대학원 박사과정
1998년 5월~ 2000년 9월 : 하이닉스 반도체 연구원
2000.10~현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 디지털 콘텐츠 보안, 인증시스템, 유·무선 인터넷 보안

류 재 철 (Jae-cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학과 석사
1990년 12월: Northwestern University 전산학과 박사
1991년~현재: 충남대학교 정보통신공학부 교수
1993년~1995년: JTC1/SC27 보안기술 전문위원회 위원
1995년~1996년: 시스템공학연구소 초빙연구원
1997년~현재: 한국정보보호학회 이사
2001년~현재: 국가정보원 정보보호시스템 인증위원회 위원
2003년~현재: 인터넷침해대응기술연구센터 센터장
〈관심분야〉 스마트 카드 보안, 인증이론 및 시스템, 유·무선 인터넷 보안, 저작권 보호