디지털 컨텐츠 통합 DRM을 위한 PDMS 적용

성경*, 곽철용**, 소우영**
한남대학교 컴퓨터공학과

Applying PDMS for Integrated DRM Digital Contents

Kyung Sung*, Chul-Yong Kwak**, Woo-Young Soh**
*Dept. of Computer Engineering Donghae University
**Dept. of Computer Engineering Hannam University

요 약

컴퓨터 보급 증가와 인터넷 발전으로 다양한 종류와 다량의 디지털 데이터들이 제작, 유포되고 있다. 디지털 컨텐츠는 기존 아날로그 컨텐츠와 비교할 때 생성, 가공, 유통, 분배 등의 측면에서 많은 장점을 갖는 반면, 원본과 동일한 복사본을 쉽게 생성할 수 있는 특징 때문에 디지털 창작물에 대한 저작권 보호가 중요시 된다. 본 논문에서는 디지털 컨텐츠 보호 기술로 각광 받고 있는 DRM(Digital Rights Management)기술에서 컨텐츠 유통 시 개인키가 노출될 경우 비인가자에 의한 컨텐츠 불법접근이 가능해지는 취약성에 대한 개선책으로 PDMS (Public-Key Distributed Management System : 개인키 분산관리 시스템)를 확장 적용하는 방안에 대하여 논한다.

1. 서론

전 세계적으로 연결된 인터넷 망과 사회전반에 보급된 컴퓨터의 발전으로 디지털 데이터의 제작과 사용 율이 증가되었다. 또한 기존의 정보에 대한 개념이 영리 추구를 목적으로 하는 디지털 정보로 변화됨에 따라 인터넷상에서 디지털 정보에 대한 안전성 확보는 디지털 정보의 생성만큼이나 중요한 문제가 된다. 이는 많은 시간과 노력을 투자하여 제작한 디지털 데이터가 제작자의 허가 또는 적절한 대가의 지불 없이 불법적으로 복사됨에 따라 저작권이 보호받지 못하는 경우가 발생하게 되고, 복제된 컨텐츠의 불법적 이용으로 기업과 제작자 모두 많은 피해를 입어 디지털 컨텐츠 제작 산업을 위축시키는 결과를 가져왔다. 디지털컨텐츠 보호의 중요성이 부각되는 가운데 DRM을 이용한 여러 보호 기법들이 제안되고 있다[1]. 본 논문 2장에서는 현재 컨텐츠 보호 관련 기술에 대하여 분석하고, 3장에서는 통합 DRM 모델에 대한 분석 및 문제점을 제시하며, 4장에서 분석된 취약점에 대한 보완책에 대하여 논하고, 5장에서 결론을 맺는다.

2. DRM(Digital Rights Management)

DRM 기술이란 컨텐츠를 암호화한 후 배포함으로써 아무나 사용할 수 없도록 보호하는 총체적 기술로, 컨텐츠가 항상 암호화된 상태로 존재한다. 이는 인증된 사용자만이 순간적으로 복호화 하여 사용하도록 하고 무단복제를 하더라도 인증되지 않은 사용자는 사용할 수 없도록 제어하기 때문에 불법적인 접근을 방지하는 기술이다[1][2][7]. DRM은 여러 가지 기술들이 조합되어 이루어지는 개념이며 다음과 같이 컨텐츠 저작권 관리기술과 컨텐츠 저작권 보호기술로 구별한다.

2-1.저작권 관리기술

①컨텐츠 식별자(DOI: Digital Object Identifier): IDF(International DOI Foundation)에 의해 추진되고 있는 디지털 컨텐츠 식별체계 표준화 작업이다. 등록되는 모든 디지털 저작물에 유일한 식별자를 부여하기 위한 식별 및 등록 체계를 정의하고, 부여된 식별자에 의한 접근의 용이성을 보장하기 위한 검색기능, DOI-IP 자동 변환기능 등을 제공한다.

②컨텐츠 메타데이터(INDECS, Interoperability of Data in ECommerce Systems): 유럽을 중심으로 한 저작권 단체들이 주도하는 디지털 컨텐츠의 메타데이터를 정의하는 표준화 작업으로, 저작물정보, 저작자

정보, 저작권자 정보, 권리운용 정보로 구별하여 컨텐츠의 메타데이터를 정의한다.

③컨텐츠 권리명세언어: 컨텐츠의 메타데이터를 표현하는 권리명세언어는 ContentsGuard사가 개발한 XrML (Extensible Rights Markup Language) [3]을 비롯하여 ODRL(Open Digital Rights Language), XACML (Extensible Access Control Markup Language) 등이 있으며, 모두 확장성을 제공하는 XML 형식이다.

2-2. 저작권 보호기술

저작권 관리기술에서 정의하는 일련의 원칙과 시나리오들을 강제화(Enforcement) 하는 기술로서 암호기술, TRM(Tamper Resistant Module) 및 키 분배 및 관리 기술 등이 있다.

①암호 요소기술: 컨텐츠 인증, 컨텐츠 사용자 인증, 거래 및 사용규칙 강제화, 거래 및 사용내용 확인(부인방지) 기능 등을 위하여 암호화, 전자서명, 그리고 이에 필요한 인증 및 키 분배 기술 등 다양한 암호 요소기술들이 사용된다.

②TRM: 컨텐츠 보호를 어렵게 하는 요인은 컨텐츠가 사용되는 어떤 순간에 반드시 복호화 되어야 한다는 점이다. 컨텐츠를 가공하거나 사용하는 과정에서 컨텐츠 복호화키 또는 복호화된 컨텐츠가 사용자에게 노출될 수 있다면, 암호기술을 깨지 않고도 보호되지 않은 컨텐츠를 얻어낼 수 있게 된다. TRM은 마치 블랙박스와 같이 세부동작 과정이 드러나지 않도록 숨기고, 변형을 가하면 동작하지 않도록 제작된 소프트웨어 또는 하드웨어 모듈을 의미한다. DRM에서는 컨텐츠의 권리 정보, 키 정보, 복호화된 컨텐츠 등을 다루는 모듈에 TRM 기술을 적용하여, 디버깅 도구를 사용한 소프트웨어 역분석을 방지한다.

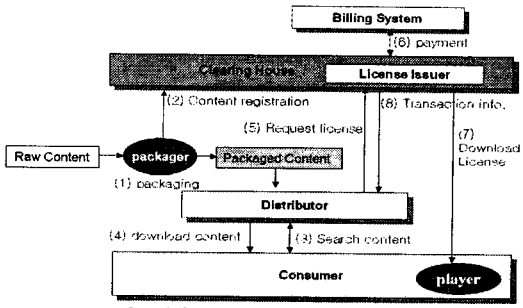
③키 분배 및 관리: DRM 키 분배 방법은 대칭키 방식과 공개키 방식으로 구별될 수 있다. 대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 컨텐츠 거래에 키 분배 서버가 관여해야 한다. 반면 공개키 방식을 사용할 경우 분산성, 확장성, 상호 운용성 등에서 많은 장점을 갖게 되나, 공개키 기반구조(PKI)가 필요하다는 부담이 있다. 현재 제안되고 있는 방식은 두 암호 시스템이 갖는 장점만을 이용하여 실제 데이터의 암호에는 대칭키 방식을, 대칭키 방식에 이용되는 비밀키의 암호에는 공개키 방식을 이용하는 하이브리드 암호 시스템(Hybrid cryptosystem)이 주로 이용된다.

3.컨텐츠 유통을 위한 통합 DRM 분석

DRM 시스템은 컨텐츠 저작권자, 컨텐츠 저작권 관리단체, 컨텐츠 공급자, 컨텐츠 신디케이터(유통자), 컨텐츠 분배자, 컨텐츠 소비자에 이르기까지 다양한 거래주체들 간에 '가치 고리(Value Chain)'를 형성할 수 있도록 지원해야 하는 기반구조의 성격을 갖는다. 따라서, 컨텐츠 식별자(예: DOI), 컨텐츠 메타데이터(예:INDECS), 권리명세언어(예:XrML, ODRL, XACML, RMI) 등의 저작권 관리 표준들, 저작권 보호기술에 적용되는 PKI(X.509, PKCS 등) 표준들, 그리고 전자책 관련 표준 OEBF의 EBX, 동영상 관련 표준 MPEG, 인터넷 관련 표준 W3C, 디지털 방송표준 DVB 등 관련 응용분야의 국제표준들과 밀접한 관련이 있다.

3-1. 통합 DRM 분석

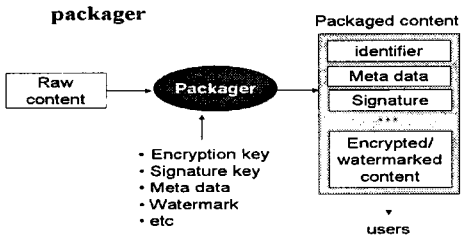
디지털 컨텐츠 유통 체계에 DRM 기술이 접목된 모델에 대해 설명해 보면 우선 다음과 같은 절차를 통해 컨텐츠 교환이 이루어진다.



[그림1]. DRM Architecture Model

(1) 순수 컨텐츠를 패키저를 사용하여 패키징 (2) 패키징 정보를 클리어링하우스에 등록 (3) 소비자가 쇼핑몰을 검색 후 컨텐츠 선택 (4) 패키징된 컨텐츠를 소비자에게 제공(다운로드) (5) 소비자가 컨텐츠를 작동시(컨텐츠 속에 기록된 권리관리정보로부터 Player가 쇼핑몰에 대한 정보를 추출하여 쇼핑몰에 요청), 쇼핑몰이 클리어링하우스에게 라이선스 발급을 요청 (6) 만약 컨텐츠 사용에 대한 금액(유료)이 있으면, 빌링 시스템을 통하여 요금 정산 처리 (7) 라이선스를 만들어 소비자에게 제공 (8) 클리어링하우스가 주기적으로 쇼핑몰에 거래내역 정산에 대한 보고서 발송을 끝으로 하나의 트랜잭션이 완료된다.[그림2]는 Packager방법에 대한 분석을 보여준다. Packager과정을 거치게 되면서 컨텐츠는 암호화 및 메타 데이터에 대한 관리 등의 저작권 보호기술들이 적용(Mata data, Watermarking)

되어 불법적 재배포 및 변경에 대한 적극적인 대비책을 갖게 한다. 다음으로(5)~(8) 라이선스 관리 부분 및 과금등을 담당하는 클리어링 하우스의 구조[그림3]를 살펴보면 첫째 컨텐츠 사용허가 시스템, 둘째 유통 정보처리 시스템 셋째, 결제 시스템의 세부분으로 나누어진다. 컨텐츠 사용허가 시스템의 경우 유통업자로



[그림2].Packaging 과정

부터 요청된 컨텐츠를 등록하고 구매자에게 라이선스를 발급하는 역할을 하며 유통 정보처리 시스템은 컨텐츠 거래내역 관리와 컨텐츠 제작자, 제공업자, 유통업자등에게 로열티를 분배내역을 리포팅하고, 결제 시

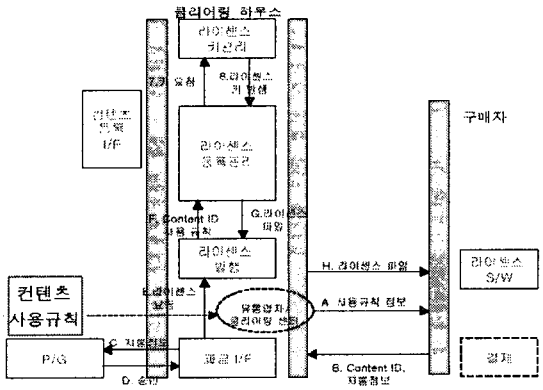


그림3].클리어링 하우스의 내부 구조

스템은 로열티 분배의 역할을 한다. 이상의 절차를 통해 시스템은 지불여부, 회원여부 등을 확인해 사용자를 인증한 후, 인증된 사용자만이 주어진 사용권한에 준하여 컨텐츠를 사용하도록 집행(Enforce)하게 된다. 또, 사용자는 컨텐츠의 출처, 저작자 등을 인증할 수 있도록 하였으며, 오디오/비디오의 경우 스트리밍 서비스를 지원한다.

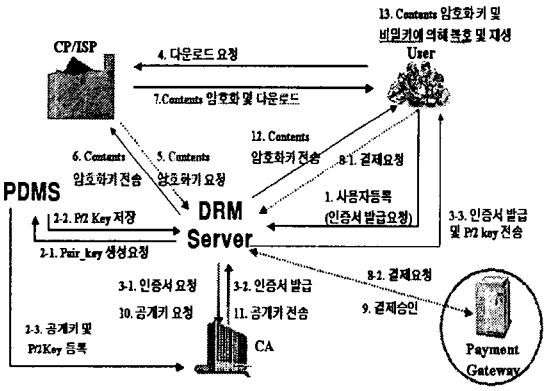
3-2. 취약점 분석

위에서 분석된 구조를 토대로 DRM 시스템이 갖고 있는 취약점을 진단해 보면 Packager는 컨텐츠를 트랜잭션에 쓰이는 비밀키를 이용해 암호화 하고 이를 다시 사용자의 공개키를 통해 한 번 더 암호화 하는 과정인 하이브리드 기법[8]에 의한 암호화를 구현한다. 여기서 가령 사용자가 개인키를 고의 혹은 실수에 의해 누출시키게 되면 이를 습득한 비인가자는 대칭키 암호문 블록에 대하여 일련에 분석을 통해 비밀키와 복호된 컨텐츠를 습득할 수 있는 문제가 발생하게 된다. 이러한 예를 통하여 DRM이 키 관리부분에 대하여 취약성을 갖고 있음을 알 수 있다. 다음으론 인가된 사용자가 이용 시 복호화된 컨텐츠를 다운로드 한 후 사용하게 될 경우 아무런 제약 없이 컨텐츠를 가공 혹은 다른 목적으로 이용할 수 있는 문제가 발생한다. 이는 컨텐츠 저작권 보호 측면의 취약점을 보여준다.

4. DRM 취약성에 대한 보완책 연구

본 논문에서는 키 관리 부분에 대한 취약점을 중점적으로 다루기로 한다. 개인키 노출에 따른 비밀키 및 컨텐츠 불법 접근에 대한 해결책으로 가장 이상적인 방법은 컨텐츠 전달과정에 참여하는 유통업자, 분배자, 소비자 등 모든 사용자가 자신도 자신의 키를 알 수 없도록 관리하는 방법이다. 원천적으로 자신의 키에 접근할 수 없다면 알고리즘의 비밀성이 보장되는 한 컨텐츠의 불법적 접근이 불가능해지기 때문이다. 하지만 자신의 개인키에 대한인지가 없다면 키 생성과 관리가 불가능하다는 더 큰 문제점이 야기된다. 여기서 개인키 관리에 대한 다른 방식의 접근을 시도하여 생성된 개인키에 대해 분산 관리를 통해 키 관리 문제의 보완에 대하여 논한다. 개인키 분산의 일반적인 모델은 $1 \le m \le n$인 정수에 대해 m-out-of-n스킴 (또는 (m,n)-threshold 스킴)이라 불린다. 스킴에서, 발신자 그리고 n명의 관리자가 있다. 발신자는 어떠한 m 부분이 모여도 개인키를 복구 할 수 있도록, 그러나 발신자 외에 어떠한 m-1부분도 그 개인키에 대한 정보를 나타낼 수 없도록 개인키를 n 부분으로 나누고 각 관리 시스템에게 한 부분씩 분산시킨다. m과 n값을 다른 값을 선택하면 보안과 신뢰도가 서로 지위를 교환하는데 영향을 미친다. 분산 스킴은 m-1의 어떠한 그룹도 단독적으로 완전한 개인키에 대하여 예측하지 못하게 함이 기술의 요체이다. 이러한 원리를 토대로 DRM의 키 관리 부분에 기술을 적용시켜 보면 [그림4]와 같은 구조를 갖게 된다. 기존의 DRM 구조에 PDMS(Publlic-Key Distributed Management System : 개인키 분산관리 시스템)를 도입해 개인키의 누출에

대해 대비책을 세웠다. 여기서 사용자가 Pair_Key를 생성 자신의 공개키를 인증기관에 등록시키는 형태의 공개키 교환 방식대신 PDMS에서 직접 키 쌍을 생성하는 방식으로 개인키를 Pk 라 하면 이를 2개로 나누어(Pk1, Pk2) 각각 사용자와 DRM서버가 나눠 갖게끔 만들었다. 그 다음 절차에 의해 암호화된 컨텐츠가 제공되고 이를 복호화 시킬 수 있는 비밀키가 공개키를 이용하여 암호화되어 전송시 사용자와 DRM Server가 갖고 있는 개인키(Pk)를 조합(Pk1+Pk2)하여 비밀키를 얻어내는 방식으로 키 관리 메커니즘을 구성하였다. 사용자가 자신이 갖고 있는 개인키를 누출하여도 컨텐츠를 사용할 때 인증 및 지불이 이뤄지지 않은 상태라면 비밀키를 복호화 낼 수 없게 되므로 키 관리에서 야기되는 문제점에 대한 효율적 대응책으로



적용될 수 있다.

[그림4] PDMS 에 의해 보완된 DRM 시스템

5. 결론 및 향후 연구 방안

최근 디지털 컨텐츠의 제작과 사용이 증가하며 보다 신속하고 효율적으로 양질의 컨텐츠를 배포시킬 수 있는 기술이 요구되고 있으며 컨텐츠의 안전한 보호 기술 역시 병행해서 발전 돼야할 중요한 과제이다. 이러한 요구에 따라 DRM의 요소 기술들에 대한 표준화가 현재 활발하게 연구되고 있다. 본 연구에서는 PKI 기반의 하이브리드 암호 알고리즘을 통해 암호화되는 컨텐츠에서 개인키 누출에 의해 암호문 판독, 비밀키와 메시지가 누출될 수 있는 문제점에 대한 대응책으로 PDMS의 구조와 방식에 대하여 논하였다. 앞으로 PDMS가 Pair-key의 생성 및 분배에서 발생하는 트래픽을 효과적으로 해소 할 수 있는 방안과 개인키의 분산 및 키 조합에 대한 알고리즘 이 연구되어야 할 것이다.

[참고문헌]

[1] http://www.drm.or.kr DRM Forum

[2] Trafford, Proposal for the Formation of a Digital Rights Management Working Group, March 28, 2000

[3] AAP, Digital Rights Management for Ebooks: Publisher Requirements version 1.0,November, 2000

[4] 이창열 "디지털 정보에 대한 식별자 부여 및 전자상거래용 메타데이타 모델에 관한 연구" 한국교육 학술정보원, RR-1999-2

[5] 이응효 "Digital Content Management",DRM Working Group workshop March 30, 2001

[6] Mark Baugher "Digital Rights Management on Internet Protocol" March 1, 2001

[7] Henning Schulzrinne, Jonathan Rosenberg, "The Session Initiation Protocol : Internet-Centric Signaling", IEEE Communication Magazine, 134p-141p, October 2000

[8] "DRM Forum" http://www.drm.or.kr/~contents/index.html

[9]ANSI X9.42, "Agreement of symmetric Key on Using Diffie-Hellman Cryptography".

[10] http://crypto.jmi.co.kr "암호화 연구소"