제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

무선환경에서멀티미디어컨텐츠보호를위한DRM설계

곽철용, 조명휘, 소우영
한남대학교 컴퓨터공학과

요 약

인터넷의 발전과 멀티미디어 인프라의 성장으로 방대한 양과, 다양한 종류의 디지털 데이터들이 제작, 유통되고 있다. 디지털 컨텐츠는 기존 아날로그 컨텐츠와 비교 생성, 가공, 유통, 분배 등의 측면에서 많은 장점을 갖는 반면, 원본과 동일한 복사물을 쉽게 생성할 수 있는 특징 때문에 디지털 창작물에 대한 저작권 보호가 중요시된다. 본 논문은 이미 유선 환경에서 디지털 컨텐츠 보호 기술로 각광 받고 있는 DRM(Digital Rights Management)을 토대로 무선 환경에서 디지털 컨텐츠의 보안을 위한 MobileDRM (MDRM) 에 대한 설계를 목적으로 한다. 설계되어진 MDRM은 Mobile 환경을 고려 키 교환 및 컨텐츠 암/복호 시 발생하는 부하를 줄이고 컨텐츠의 불법적인 유포 방지를 위한 SDMS(Secret-Key Distributed Management System : 비밀키 분산 관리 시스템)기술을 이용한다.

Design of DRM for Multimedia Contents Protection in Wireless Environment

Chul-Yong Kwak, Myeong-Hwi Jo, Woo-young Soh

* 본 연구는 과학기술부 지역협력연구사업 (R12-2003-004-01002-0) 지원으로 수행되었음

1. 서 론

DRM(Digital Right Management)이란 디지털 저작권에 대한 관리를 뜻한다. E-Book, Game, 음악,영상, 이미지 등 디지털방식으로 제작된 모든 형태의 저작물을 디지털 컨텐츠라 하고, DRM은 이러한 디지털 컨텐츠의 무단 유통을 방지하는 기술을 의미한다.

2004년 현재 디지털 컨텐츠의 국내 시장규모만도 3조원에 육박할 것으로 예상되고 있지만, 대규모 시장에도 불구하고 제작자의 저작권 및 컨텐츠 사용자 권한 보호 측면에서는 많은 취약성을 갖고 있다. 특히 Forward Lock 방식으로 제공되는 컨텐츠의 경우 사용자에 의한 재배포시엔 DRM이 아무런 실효를 거두지 못하는 문제점을 안고 있다

본 논문은 DRM 특히 무선 인터넷 환경에 적합한 Mobile DRM(MDRM)에 대한 설계를 목표로, 현재 무선 DRM 표준인 OMA(Open Mobile Alliance)Ver 2.0에서 발표한 DRM 솔루션의 문제점에 대하여 조사하고, 조사된 문제점들에 대한 개선을 통해 MDRM의 설계를 제안한다. 이를 위하여 2장에서는 관련연구로 DRM 기술과 OMA Ver2.0의 DRM 솔루션에 대해 알아보고, 3장에서는 기존 DRM에 존재하는 보안 위협들에 대해 조사하며, 4장에서는 이러한 보안 위협

들을 개선한 SDMS를 이용한 MDRM 방식에 대한 설계를 제안하고, 5장에선 향후 연구방안으로 결론 맺는다[1][2][3].

2. 관련연구

DRM 기술이란 컨텐츠를 암호화한 후 배포함으로써 아무나 사용할 수 없도록 보호하는 총체적 기술로, 컨텐츠가 항상 암호화된 상태로 존재한다. 인증된 사용자만이 순간적으로 복호화 하여 사용하도록 하고 무단복제를 하더라도 비인가 사용자는 사용할 수 없도록 제어를 목적으로 하는 기술이다[1][2][7]. 이번 장에서는 DRM의 컨텐츠 저작권 관리기술 및 컨텐츠 보호기술과 무선 환경에서 DRM 표준이 되는 OMA에 대하여 알아본다.

2.1 저작권 보호기술

저작권 관리기술에서 정의하는 일련의 원칙과 시나리오들을 강제화(Enforcement) 하는 기술로서 암호 기술, 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.

②키 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.

2.2 컨텐츠 관리기술

① 디지털콘텐츠 식별 시스템

디지털콘텐츠의 체계적인 관리 및 통제, 접근, 이용효율성을 위해 대상물을 식별할 수 있는 체계 및 변환시스템을 말한다. 디지털콘텐츠에 고유한 코드를 부여하는 기술인 관계로 아직 표준화 단계까지는 시간이 소요될 것으로 예상되며, 이에 따라 대다수의 DRM 솔루션들은 DOI 체계를 미적용 상태에 있다. 따라서 디지털콘텐츠 식별체계와 식별체계 간 상호연동 기술 및 변환 시스템의 개발이 절실히 요구되고 있다.

② 컨텐츠 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.

2.3 OMA

OMA(Open Mobile Alliance)는 무선 DRM의 표준을 제정하는 대표적인 단체로써 구체적인 무선 DRM에 관련된 규격을 제시하고 있다. OMA 에서는 WAP 기반의 무선 통신에 적용되는 application에 의한 무선 DRM 에 대한 규약들을 정의한다[2][3].

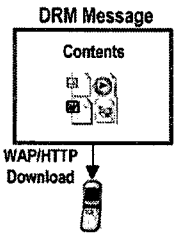
현재까지 DRM 관련 OMA DRM 1.0 버전이 발표된 상태이며 금년 6월경에 2.0 버전이 발표될 예정이다. OMA DRM ver1.0 에서는 DRM 컨텐츠의 형식과, DRM 권한 표현 방법 및 컨텐

츠 다운로드 방식에 대한 규격이 정의되어 있다. OMA DRM에서 규정하는 컨텐츠 분배는 크게 Forward Lock, Combined Delivery, Separate Delivery의 3가지 방식으로 정의한다.

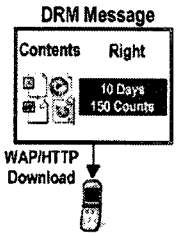
① Forward Lock은 컨텐츠가 인증된 사용자에게 다운로드 될 경우 다운로드한 사용자의 기기에서만 재생 되도록 제한하는 방식으로, 컨텐츠를 포함한 DRM Message 에 사용권한은 삽입하지 않고 단지 다른 사용자의 기기로 전송되지 않게만 설정해준다.

② Combined Delivery 의 경우는 컨텐츠와 함께 Media Object의 사용 제어를 명시한 OMA REL(Rights Expression Language)를 DRM Message로 다운로드 시킨다. Combined Delivery방식의 구현을 위한 요구사항은 Right Object의 포워딩 및 DRM 메시지내의 Media Object의 수정을 제안해야 하는 점이다.

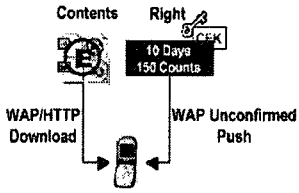
③ Separate Delivery는 컨텐츠를 암호화 시킨 DRM Message와 별도로 클라이언트 측에서 컨텐츠에 대한 복호화및 사용이 가능한 Rights Object가 분리되어 전송된다. Media Object의 경우 DCF 형식으로 다른 클라이언트로의 포워딩이 가능하고 Rights Object의 경우는 포워딩을 제한한다. 이런 기능은 다운로드 받은 사용자는 누구나 Superdistribution을 가능케 하고 재배포 받은 컨텐츠의 사용자는 Rights Object를 컨텐츠 공급자(CP)로부터 다운로드 받아야 사용이 가능하다.



Forward-Lock



Combined Delivery



Separate Delivery

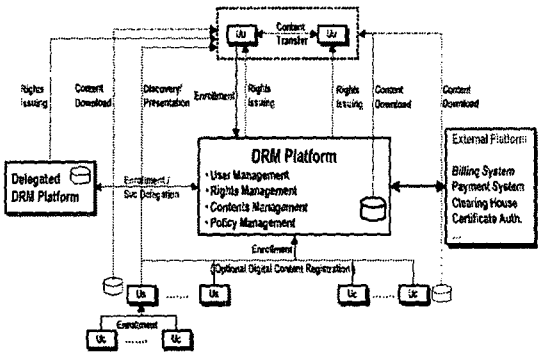
[그림 1] OMA에서 정의하는 컨텐츠 제공 방식

④ Superdistribution 은 DCF 형태의 콘텐츠를 다른 디바이스로 전달하는 것을 허용하며 디바이스를 통해 Superdistributed된 콘텐츠의 사용을 위해 Rights를 발급받을 수 있게 해준다.

디바이스는 DCF 의 Rights-Issuer 필드에 정의된 URL 을 통해 Rights 발급 요청을 하게 된다. 기존 Secure distribution 기술은 사용자에게 종속적인 키를 이용하여 콘텐츠를 암호화함으로써 콘텐츠의 이동을 크게 제한한 반면 Superdistribution 은 콘텐츠의 이동 및 복사는 자유롭게 허락하되 사용 시점에서 사용권한을 획득해야만 콘텐츠의 이용이 가능한 기술적 매커니즘을 포함함으로써, 소프트웨어의 유통을 혁신적으로 활성화한다[5][6].

3. DRM 보안 현황

현재까지 진행된 무선 DRM 기술 표준에서는 보안과 관련하여 여러 가지 취약성을 갖고 있다. 일반적으로 여러 보안 시스템들이 외부의 침입자로부터 내부의 사용자(혹은 데이터)를 보호하는 기능을 갖는다면, DRM의 경우엔 내부의 인가 받은 사용자라 할지라도 경우에 따라선 공격자 자체가 될 수 있기에 이러한 면에서 상당한 취약성을 갖게 된다[4].



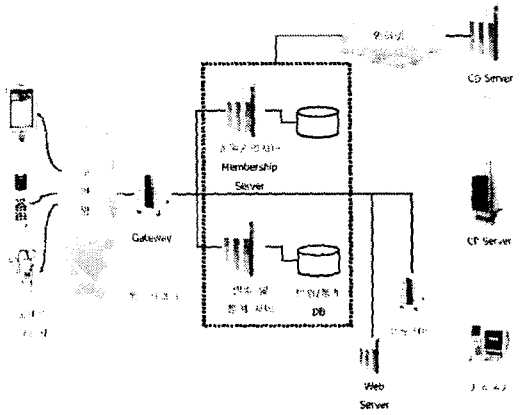
[그림 2] DRM Method

컨텐츠 암호화는 트랜잭션에 쓰이는 비밀키로 암호화하고 이를 다시 사용자의 공개키를 이용해 한 번 더 암호화하는 하이브리드 기법을 사용한다. 여기서 가령 사용자가 비밀키를 고의 혹은 실수에 의해 누출시키게 되면 이를 습득한 누구든 복호화된 컨텐츠를 이용할 수 있는 문제가 발생하게 된다. 이러한 예를 통하여 DRM 이 키 관리부분에 대하여 취약성을 갖고 있음을 알 수 있다. 또한 인가된 사용자의 이용 시 복호화된 컨텐츠를 아무런 제약 없이 가공 혹은 다른 목적으로 이용할 수 있다는 문제가 발생한다. 이는 컨텐츠 저작권 보호 측면의 취약점을 보여준다.

4. MDRM 설계

이번 장에서는 DRM의 취약성을 개선하고, Mobile 환경에 적합한 디지털컨텐츠 암/복호화에 대한 설계를 보여준다. 설계하게될 MDRM 환경은 PDA 와 Mobile-Phone을 대상으로 한다.

4.1 MDRM 구성



[그림 3] MDRM System 구성

컨텐츠 유통 경로를 살펴보면 컨텐츠 제공자(CP)로부터 전달된 컨텐츠는 컨텐츠DRM Packager를 이용 Packing과정을 거치게된다. 이때 컨텐츠는 암호화되고 사용자 쪽에서 복호화할 때 필요한 정보들을 Package 헤더로 구성하고, 컨텐츠 암호화 키(CEK)를 라이선스 안에 첨부하여 사용자에게 전송하기 위한 사전 단계로 라이선스 서버에 CEK 와 DRM Packing 정보를 등록하는 작업도 병행하게 된다.

라이선스 서버에선 사용자에게 발급되는 라이선스에 대한 총괄적인 관리작업을 수행하며, CEK와 컨텐츠 사용자의 권리서명 등이 암호화되어 저장돼있다.

사용자는 다운 받은 컨텐츠를 재생하기 위하여 컨텐츠 라이선스를 이용 사용권리의 범위 내에서 컨텐츠를 복호화후 사용하게 된다.

4.2 SDMS의 개요

앞에서 암호화키 노출에 따른 컨텐츠 불법 접근 및 유포가 유무선 DRM 환경 모두에 해당하는 문제점이라면 Mobile환경에선 여기에 컨텐츠 사용 시 시스템에 걸리는 부하문제가 추가된다.

DRM 암호화의 인코딩 작업은 컨텐츠에 대한 Packaging시 컨텐츠 서버와 라이선스 서버에서

함께 수행되는 구조이고 디코딩의 경우는 사용자의 단말에서 컨텐츠의 이용 시 수행되는 작업이다. 일반적으로 컨텐츠 전체에 대하여 CEK를 사용하여 암호화하고 사용 시에 이를 복호화 하는 방법을 이용하게 되는데, 이는 일반적인 유선 환경에서 쓰인 DRM 방식을 무선 Mobile 환경으로 가져온 것이기 때문에 고용량의 데이터 파일 처리 시에 높은 부하를 유발하게 된다.

이러한 Mobile 환경에서 DRM의 취약성에 대한 해결 방안으로 디지털 컨텐츠의 유통 전반에 참여하는 CP, 라이선스서버, 소비자 등의 모든 구성요소들이 비밀키를 알 수 없도록 관리하는 방법을 들 수 있다. 이는 자신의 키에 접근할 수 없다면 알고리즘의 비밀성이 보장되는 한 컨텐츠의 불법적 사용(불법 복제를 이용한 무단유포)이 불가능하기 때문에 가장 원천적으로 비밀키 노출에 대한 취약성을 해결할 수 있는 방법이 된다.

이번 절에서는 생성된 비밀키에 대해 분산 관리를 통해 키 관리의 취약성을 보완하고 Mobile의 처리능력을 고려한 MDRM의 설계를 위해 다음과 같은 방식을 이용한다.

비밀키 분산 모델은 $1 \le m \le n$인 정수에 대해 m-out-of-n스킴 (또는 (m,n)-threshold 스킴)이라 불린다. 컨텐츠 제공자(CP)와 n개의 비밀키 관리 시스템이 있다고 가정했을 때, CP가 갖고 있는 모든 m으론 비밀키를 복구 할 수 있도록, 그러나 CP 외에 어떠한 m-1부분도 그 비밀키에 대한 정보를 나타낼 수 없도록 비밀키를 n 부분으로 나누고 각 관리 시스템들에 분산시킨다. m과 n값을 다른 값을 선택하면 보안과 신뢰도가 서로 지위를 교환하는데 영향을 미친다. 분산 스킴은 m-1의 어떠한 그룹도 단독적으로 완전한 비밀키에 대하여 예측하지 못하게 함이 기술의 중심사항이다. 이러한 원리를 토대로 DRM의 키 관리 부분에 기술을 적용시켜 기존의 DRM 구조에 SDMS(Secret-Key Distributed Management System : 비밀키 분산관리 시스템)를 도입 비밀키의 누출에 대해 대비책을 세울 수 있다.

4.3 SDMS의 설계

SDMS의 구성은 각각의 분산된 키들을 관리하는 키 분산 서버와 키 분산서버들의 정보 및 총괄적 관리를 수행하는 관리 서버(Management Server)로 구성된다.

제안되는 MDRM 방식은 라이선스 서버에서 CEK를 생성하고 이를 이용 컨텐츠를 Packaging 암호화하는 과정까지는 기존의 DRM 방식과 동일하다. 하지만 CEK의 정보를 n개로 나누고 이를 분배해서 관리한다는 점에서 분명한 차이를 둘 수 있다. 생성된 CEK를 Sk 라 하면 이를 n개로 나누어(Sk1, Sk2,...Skn) 각각의 분배 서버들이 나눠 갖게되고 관리서버에선 분배된 키 값에 대한 Index정보만을 갖고있게 된다. 이렇게 CEK가 생성 분배된 다음 암호화된 컨텐츠가 사용자에게 제공되고, CEK에 대한 Index 정보 갖는 데이터를 PKI를 이용 사용자에게 발송하게 되는데 여기까지를 DRM 서버부분이 수행하게 된다. 사용자는 전송 받은 컨텐츠를 복호화 시켜 이용하게 되는데 이 부분은 DRM 에이전트에서 수행하게 된다. DRM 에이전트는 다운 받은 컨텐츠 라이선스에서 추출한 CEK Index 정보를 가지고 분배된 CEK를 조합하게 된다. 여기서 CEK의 조합과정을 살펴보면 다음과 같다.

전송된 Index 값은 각각의 분배 서버들이 갖고 있는 (Sk1, Sk2,...Skn)들을 요청하게 된다. 이때 각각의 분배 서버들에선 사용자 인증에 필요한 정보를 나누어서 검토하게 된다. 휴대전화를 예로 들면 전화번호를 점검해서 Sk1을 전송하고, 인식 값을 이용해 Sk2을 전송하는 방식으로 Skn 까지를 전송하게 된다. Skn 까지 전송 받게 되면 에이전트는 이를 조합하여 키를 생성하고 이를 이용해 컨텐츠를 사용할 수 있게 한다. 이 경우 사용자가 자신이 갖고 있는 Index 정보를 누출하여도 컨텐츠를 사용 시 인증 및 지불

이 이뤄지지 않은 상태라면 비밀키를 조합할 수 없게 되므로 키 관리에서 야기되는 문제점에 대한 효율적 대응책으로 적용될 수 있다.

5. 결 론

유선기반을 중심으로 개발되어 왔던 DRM 기술은 최근 휴대폰, PDA 등으로 대표되는 Mobile device 의 성능 향상과 네트워크 기술의 빠른 진화로 무선 환경에 적용될 DRM 기술 개발에 대한 수요는 점차 증가하고 있다. 그러나 아직까지 무선 네트워크의 대역폭과 무선 단말기의 CPU 성능 및 메모리 제한이 많은 상황에서 유선기반에서 적용했던 DRM 기술을 그대로 사용하기에는 무리가 따른다. 따라서 모바일 콘텐츠에 적용 가능한 DRM 기술의 소형화, 경량화 노력이 무엇보다 필요한 시점이다.

본 논문은 이러한 추세에 맞추어 무선 환경에서 이용할 수 있는 MDRM 요소기술인 비밀키 분배 관리시스템 (SDMS) 에 대하여 설계를 제안하였다. 유무선 DRM 환경에서 취약점으로 지적되는 키 관리 부분에 효율성과 안전성을 두어 보다 안정적인 디지털 컨텐츠 유통구조를 설계하였다.

향후 연구 방안으론 Mobile 메모리 경량화를 고려한 보다 발전된 형태의 SDMS 개발과 SDMS기술의 효과적인 활용을 위한 비즈니스 모델의 연구가 필요하다.

참고문헌

[1] Open Mobile Alliance, "Generic Content Download Over The Air Specification" V.1.0, 2002.

[2] Open Mobile Alliance, "Rights Expression Language" V.1.0, 2002.

[3] 김진영(실트로닉테크놀로지), "DRM 비즈니스와 기술", Web Business, 2002.

[4] 김원겸, 이선화, 장호욱, "불법 복제 콘텐츠 추적을 위한 핑거프린팅 기술 동향", 전자통신동향분석 제 18 권 204 호, 2003.

[5] http://www.openmobilealliance.org

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

[7] http://www.odrl.net

곽 철 용

2003년 한남대학교 컴퓨터 공학과 (공학사)

2004년 현재 한남대학교 컴퓨터 공학과대학원 석사과정

조 명 휘

2003년 한남대학교 컴퓨터 공학과 (공학사)

1996년 한남대학교 컴퓨터공학과대학 (공학석사)

2004년 현재 한남대학교 컴퓨터공학과대학원 박사과정

2004년 현재 한전 KDN(주) 시스템 사업팀

소 우 영

1979년 중앙대학교 전자계산학과 (이학사)

1981년 서울대학교 전자계산학과 (이학석사)

1991년 미 메릴랜드대 전자계산학과 (이학 박사)

1996년 ETRI 초빙 연구원

2004년 현재 한남대학교 컴퓨터 공학과 교수