韓國컴퓨터情報學會 論文誌
第15卷 第12號, 2010. 12.

2010-15-12-3-8

상호 호환성을 위한 홈 도메인 DRM 설계

문 주 영*

Design of Interoperable DRM System in Home Domain

Ju-Young Moon*

요 약

본 논문에서는 홈 도메인에서 상이한 DRM 규격의 콘텐츠 재배포가 안전하게 이루어질 수 있도록 홈 도메인 기반의 상호 호환성을 위한 DRM 시스템을 제안하였다. DRM 규격이 다른 디바이스간의 콘텐츠 재배포에 대한 어려움을 해결함으로서, 사용자의 콘텐츠 사용상의 제약과 불편을 해소하고 동시에 콘텐츠 제작자 및 제공자의 권익을 보호할 수 있는 홈 도메인 내의 콘텐츠 재배포를 위한 DRM 시스템을 제안하였다. 사용자가 구입한 콘텐츠를 자신이 소유한 다른 디지털 디바이스에서도 자유롭게 사용할 수 있도록, 디바이스들을 하나의 홈 도메인으로 묶어 상호 호환성있는 DRM을 위한 홈 도메인을 구축했다. 이로서 엑스포트 및 임포트 디바이스 각각 HADM에 의하여 홈 도메인에서 인증되면, DIM을 이용하여 엑스포트 디바이스의 콘텐츠 및 라이선스를 임포트 디바이스의 DRM 규격에 맞게 변환한 후 재패키징하여 임포트 디바이스에게 재배포할 수 있게 된다.

Abstract

In this paper, we proposed the interoperable DRM(Digital Rights Management) system that allows to redistribute contents safely based on home domain. We tried to solve the problem about contents redistribution between devices under different DRM regime so that we suggested a interoperable DRM system that allow end users to redistribute contents within home domain can solve the restriction and the inconvenience occuring in using contents and at the same time protect the right of contents producer and provider as well. In order that end users can use freely their contents using home digital device without additional payment, we must build a home domain for interoperable DRM system for contents redistribution among devices. If both of exporting device and importing device are authenticated in home domain by HADM(Home Authorized Domain Manager), then the exporting device can redistribute packaged contents under importing DRM regime to the importing device by DIM(DRM Interoperability Manager).

▸ Keyword : 저작권 보호(DRM), 홈 도메인(Home Domain), 상호 호환성 (Interoperability), 디바이스 인증(Device Authentication), 콘텐츠 재배포 (Contents Redistribution), 라이선스 재패키징 (License Repackaging)

• 제1저자 : 문주영
• 투고일 : 2010. 10. 25, 심사일 : 2010. 11. 08, 게재확정일 : 2010. 11. 15.
* 부천대학 전산정보처리과 부교수
※ 본 연구는 2009학년도 부천대학의 연구년 실시로 수행된 것임.

Ⅰ. 서 론

초고속 인터넷, 무선 인터넷, 디지털 방송 등 컴퓨터 네트워크의 가용성 증대, 멀티미디어 데이터 압축 기술의 발달, 온라인 쇼핑몰과 같은 구매 방식의 다양화, 그리고 휴대가 간편한 다양한 멀티미디어 재생 장치의 보급 등에 힘입어 음악, 이미지, 동영상, 게임, 출판물 등의 디지털 콘텐츠의 제작과 유통이 매우 활발하게 이루어지고 있다. 한편, 홈 네트워킹과 같은 새로운 디지털 콘텐츠의 사용 환경은 디지털 콘텐츠 관련 산업의 확장을 더욱 가속화시키고 있다. 이에 따라, 디지털 콘텐츠에 대한 제공자의 권리와 이익을 안전하게 보호하며 불법 복제와 유통을 막고 체계적으로 콘텐츠를 관리할 수 있는 메커니즘이 필요하게 되었고, 이를 위한 것이 암호화 기술을 기반으로 한 디지털 저작권 관리 (DRM : Digital Rights Management) 기술이다[1]. 한편, 사용자가 디지털 콘텐츠를 구매하여 자신이 소유하고 있는 여러 장치에서 호환하여 사용하고자 할 때 불편이 따르게 되는 데, 이는 DRM 기술이 업체별 독자적인 기술 규격과 서비스를 실시함에 따라 DRM 상호 호환성이 보장되지 못하기 때문이다. 이와 같이 DRM 분야는 개발업체의 기술간 상호 연관성을 갖지 못한 채 플랫폼 별로 독자적인 양상으로 전개되고 있다. 또한 미국의 InterTrust 사에서 제안한 재분배(Superdistribution) 기술은 콘텐츠의 사용을 위하여 콘텐츠 뿐 아니라 콘텐츠의 라이선스를 함께 필요로 한다[2]. 이에 따라 사용자가 자신이 소유한 여러 장치에서 콘텐츠를 사용하기 위해서는 각 장치마다 별도로 라이선스 발급을 위한 인증 철차를 받아야 한다는 문제점이 발생한다. 이러한 문제를 해결하기 위하여, 서비스별, 기기별, 업체별로 상이한 DRM 기술 규격을 사용함에 따라 다양한 표준들이 혼재되어 있고 DMR 상호 호환성을 위한 표준화 노력이 활발하게 이루어지고 있다[3].

본 논문에서는 등록된 장치들 상호간의 콘텐츠 전송이 가능한 홈 도메인을 제안한다. 특히, 각 장치간의 DRM 규격의 상이한 경우에도 콘텐츠 전송과 사용이 가능하도록 상호 호환성을 가진 홈 도메인내의 DRM 프레임워크를 제안한다. 이는 콘텐츠의 재배포 범위를 도메인 내로 제한하여 불법 재배포를 방지하고, 도메인에 등록된 장치간의 타협에 대한 공격을 차단하는 방식이다.

Ⅱ. 관련 연구

본 장에서는 홈 도메인 기반의 DRM 시스템의 기존 연구에 대해 살펴본다. 또한 DRM의 상호 호환성을 위한 접근 방식에 대해 살펴본다.

1. 홈 도메인 기반의 DRM 시스템

홈 도메인은 가정이나 소집단의 콘텐츠 이용이 가능한 각종 디바이스를 하나의 단위로 묶어 관리하여 디바이스 상호간의 콘텐츠와 재패키징한 라이선스를 주고 받음으로서 상호간의 콘텐츠 재배포가 가능하도록 구성한다[4]. 홈 도메인의 구축으로 사용자는 도메인 내의 여러 디바이스에서 동일한 콘텐츠를 사용하려 할 때마다 각 디바이스마다 별도로 라이선스를 발급받아야 하는 불편을 해소할 수 있게 된다. 홈 도메인 구축은 사용자의 편의성을 증대시킬 뿐 아니라 디지털 콘텐츠의 불법적인 사용과 유통으로부터 디지털 콘텐츠를 보호하여 안전성을 여전히 유지시켜야 한다. 따라서 홈 도메인 기반의 DRM 시스템은 도메인에 등록된 디바이스의 등록과 인증과정을 거쳐 콘텐츠와 재패키징한 라이선스를 전달함으로서 홈 도메인 내의 콘텐츠 재배포에 따른 안전성을 확보할 수 있다. 홈 도메인 시스템은 HADM(Home Authorized Domain Manager), Active 디바이스 그리고 Passive 디바이스로 구성된다[5].

HADM은 홈 도메인의 디바이스를 관리하는 장치로서 홈 도메인에 새로운 디바이스를 추가하거나 홈 도메인으로부터 특정 디바이스를 제거한다. 디바이스 키를 생성할 수 있고 라이선스를 재패키징할 수 있는 능력을 갖춘 디바이스를 HADM으로 선택하여 HADM Agent를 장착한다. HADM은 도메인 ID를 생성하고 도메인에 새로 등록될 디바이스를 위한 최대 등록 가능한 디바이스 수만큼의 Device Key를 미리 생성하여 Device Key Set을 구한다. Device Key는 새로 등록된 디바이스에게 도메인내의 디바이스 번호 DDI와 함께 전송한다. 이와 같이, HADM은 도메인 내의 디바이스의 추가, 삭제 등의 변경사항을 처리한다[6].

Active 디바이스는 DRM 서버로부터 직접 콘텐츠를 다운로드 받을 수 있는 디바이스로서 라이선스를 재패키징할 수 있는 모듈을 가지고 있기 때문에 도메인 내의 다른 디바이스에게 상호 인증 과정을 거쳐 콘텐츠와 재패키징된 라이선스를 재배포한다.

Passive 디바이스는 비교적 제한된 처리능력을 가진 MP3 플레이어, 자동차 오디오와 같은 디바이스가 이에 해당되며, Active 디바이스와 달리 라이선스를 재패키징할 수 있는 모듈을 가지고 있지 않기 때문에 다른 디바이스에게 콘텐츠를 재배포할 수 없다.

홈 도메인내에서 디바이스간의 콘텐츠 재배포는 <그림 1>[7]과 같이 디바이스간의 상호 인증 과정을 거쳐 이루어진

다. 디바이스의 상호 인증 과정은 Device A가 Device B에게 콘텐츠를 전송하고자 할 때, Device A는 Device B와 같은 도메인 내에 속하는지 확인하기 위하여 Device B의 Domain ID를 받고, Device A는 Device B가 자신과 같은 도메인에 속해 있음을 확인하여 Device B에게 Device B의 DID 정보에 맞게 재패키징된 라이선스와 콘텐츠를 보낸다. 콘텐츠 재배포가 완료되면 Device B는 Device A로부터 받은 콘텐츠를 사용할 수 있게 된다.

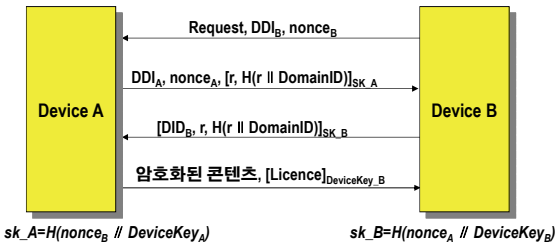

그림 1. 디바이스 인증 프로토콜
Fig 1. Protocol process for device authentication

2. DRM의 상호 호환성을 위한 접근 방식

DRM이 제한하는 상호작용성의 문제는 사용자의 선택을 불필요하게 제한한다. DRM의 기본적인 목적과 디지털 기기 플랫폼의 다양성을 고려한다면 DRM을 통한 모든 디지털 콘텐츠 서비스가 각기 완벽한 호환성을 갖추는 것은 실제로 어려운 일이다[8]. DRM의 적정한 디지털 콘텐츠 보호 기능과 더불어 최대한의 호환성을 고려하기 위한 방식에는 완전 포맷(full-format) 방식, 연결형(connected) 방식 그리고 환경 구성 중심(configuration-driven) 방식이 있다[9].

완전 포맷 방식은 콘텐츠 제공자 모두가 같은 DRM 플랫폼을 채택하는 방식이다. 이 방식은 사용자의 편의성 측면에서는 가장 우수하다고 할 수 있으나 어플리케이션이나 비즈니스 모델 측면에서는 매우 실현하기 어려운 방식이다.

연결형 방식은 해당 DRM 규격에 맞게 온라인 변환 서비스를 제공하는 방식으로서, 콘텐츠 제공자에게는 가장 손쉬운 방식이지만 사용자에게는 이와 같은 서비스를 제공받기 위하여 온라인 상태로 접속되어 있어야 하는 제약점이 있다. 즉, 다른 디바이스에서 콘텐츠를 사용하기 위해서 사용자는 서비스를 제공하는 서버와 온라인 상태이어야 한다는 것을 의미한다. 이 방식은 서비스를 제공하는 DRM 서버가 개인 사용자를 모니터링 할 수 있으므로 개인 정보 보호에 있어서도 문제가 될 수 있다.

한편, 환경 구성 중심 방식은 앞의 두 방식의 중간적인 형태로서, 최종 사용자가 콘텐츠 제공자로부터 받은 변환 도구를 사용하여 콘텐츠를 변환하여 사용할 수 있도록 하는 방식이다[10]. 콘텐츠와 라이선스 변환 모듈을 통하여 콘텐츠 제공자 A로부터 공급된 디바이스에서 콘텐츠 제공자 B의 디바이스에게 맞도록 콘텐츠와 라이선스를 변환시키도록 한다. 즉, 변환 모듈은 엑스포트 DRM 시스템(DRM_A)하에 패키징된 디지털 콘텐츠를 임포트 DRM 시스템(DRM_B)에서 사용 가능하도록 변환시켜준다. 이 방식을 실현하기 위해서는 상이한 시스템 구성에 따르는 다양한 프로토콜이 필요하다.

3. 홈 도메인에서의 DRM 상호 호환성

콘텐츠 재배포가 가능한 홈 도메인에서 서로 다른 규격의 DRM에 의한 디바이스의 상호 호환성을 문제를 해결하기 위한 방안이 필요하다. 본 연구에서는 홈 도메인에서의 DRM의 상호 호환성을 위하여 앞에서 서술한 3가지 접근 방식 중 환경 구성 중심 방식을 채택하였다. 완전 포맷 방식과 같이 모든 콘텐츠 제공자가 동일한 DRM 플랫폼을 채택하기에는 실현하기 어려운 점이 많을 뿐 아니라 연결형 방식은 모든 디바이스가 온라인으로 연결되어 중앙 집중식 서비스를 제공받게 되므로 유연성이 매우 적으며 사용자의 변환 내역에 관한 정보를 불필요하게 서버가 다룰 수 있게 되는 단점이 있기 때문이다. 환경 구성 중심 방식을 채택함으로서 도메인 단위의 상호 호환성을 지원하는 DRM 시스템을 구축하여 상이한 DRM 규격을 갖는 디바이스 상호간의 콘텐츠 재배포가 가능하도록 하여 시스템의 유연성을 확보한다. 또한 사용자의 서비스 사용 내역 즉 변환 내역이 도메인 내에서 관리될 수 있는 장점을 가질 수 있다.

III. 상호 호환성을 위한 홈 도메인 DRM 시스템

II장에서 소개한 홈 도메인 기반의 DRM 시스템에 대하여 상이한 DRM 규격의 디바이스 상호간의 콘텐츠 재배포가 가능하도록 개선함으로서 사용자의 편의성을 최대화할 수 있도록 상호 호환성을 가진 DRM 시스템을 제안하고자 한다. 저작권 보호에 관한 안전성을 유지하면서 상호 호환성이 지원되는 홈 도메인 DRM 시스템 모델을 제안한다.

1. 시스템 요구사항

본 논문에서 제안하는 시스템에 필요한 요구사항은 다음과

같으며, 콘텐츠 제공자는 고유한 DRM 규격을 갖지만 상호 호환성을 위한 본 DRM 시스템의 수용을 전제로 한다.

- 각 디바이스는 디바이스 인증기관으로부터 발급받은 디바이스 인증서와 개인키를 디바이스에 탑재한다[11][12].
- 홈 도메인 서버로 사용될 디바이스는 DRM 서버로부터 다운로드한 HADM Agent, DIM(Domain Interoperability Manager) Agent가 설치되어 있다.
- 각 디바이스는 DRM 서버로부터 다운로드한 DRM Agent가 설치되어 있다.
- 각 디바이스에는 고유한 디바이스 ID가 부여되어 있다.
- 인증서 및 키는 TRS(Tamper Resistant Memory)로 보호하여 물리적인 공격으로 인한 인증서 및 키 유출을 방지하도록 한다.
- 제안하는 시스템에서는 홈 도메인 서버로 사용될 디바이스를 제외한 모든 디바이스는 반드시 온라인으로 항상 연결되어 있어야 하는 것은 아니다.

2. 시스템 모델

본 논문에서 제안하는 상호 호환성을 위한 DRM 시스템은 홈 도메인 기반의 DRM 시스템에서 상이한 DRM 규격의 디바이스 상호간에 콘텐츠 재배포가 가능한 모델로서, DRM 시스템 구성도는 <그림2>와 같다.

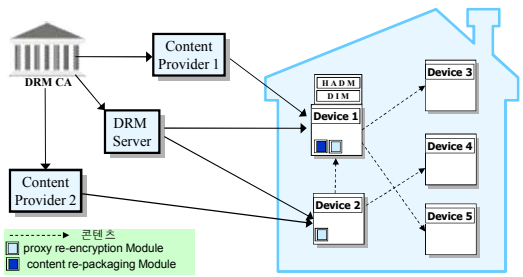

그림 2. 홈 도메인 기반의 상호 호환성을 위한 DRM 시스템 구성도
Fig 2. Block diagram of interoperable DRM system based in home domain

DRM 시스템의 주요 구성 요소는 다음과 같다.

- DRM 서버 : DRM 서버는 콘텐츠 제공자로부터 공급된 콘텐츠 재패키징을 위한 변환 도구인 라이선스 발급자 모듈을 DIM에게 제공한다. 또한 해당 서비스 사용 내역 즉 변환 내역을 관리한다.
- HADM (Home Authorized Domain Manager) : 홈 도메인의 디바이스를 관리하는 장치로서, 새로운 디바이스를 도메인에 추가하거나 특정 디바이스를 도메인으로부터 제거하는 등 도메인에 속한 디바이스를 관리한다. 또한 주기적으로 DRM 서버와 온라인으로 연결하여 도메인의 사용 내역 즉 변환 내역을 DRM 서버에게 송신한다.
- DIM : 도메인에 속한 상이한 DRM 규격을 가진 디바이스간의 콘텐츠 재배포가 가능하도록 도메인의 DRM 규격에 대한 상호 호환성을 제공하기 위한 장치이다. 엑스포트 DRM 규격에 의하여 패키징된 디지털 콘텐츠를 임포트 DRM 규격에 맞게 변환하여 패키징하기 위하여 라이선스 발급 모듈이 설치된다. 이는 호환성있는 DRM 시스템 구축을 위해 동의한 콘텐츠 제공자로부터 위임받음으로서 가능하다. 예를 들면, 호환가능한 DRM 시스템 구축에 참여하기로 계약한 콘텐츠 제공자 P_A와 P_B는 라이선스 발급 모듈을 위한 정보를 제공하게 된다. DIM 또한 주기적으로 DRM 서버를 통하여 콘텐츠 제공자와 온라인으로 연결해야 하며, 이에 따라 동일한 디바이스에 HADM과 같이 장착되는 것이 편리하다.
- 디바이스 : 도메인 내에 속하며 콘텐츠 제공자로부터 직접 콘텐츠와 라이선스를 받거나, 도메인 내의 다른 디바이스로부터 재배포 받을 수 있다. 또한, 콘텐츠 재배포가 가능한 Active 디바이스는 콘텐츠를 proxy re-encryption 모듈을 통해서 콘텐츠와 라이선스를 재패키징하여 다른 디바이스에게 재배포 할 수 있다. 한편, 엑스포트 디바이스가 상이한 DRM 규격의 임포트 디바이스에 재배포할 경우, DIM의 content re-packaging 모듈을 통하여 임포트 DRM 규격으로 변환하여 재패키징한 콘텐츠를 재배포할 수 있다.

3. 시스템 동작

상호 호환성을 제공하는 홈 도메인 기반의 DRM 시스템 모델에서 디바이스간의 콘텐츠 재배포는 다음의 2가지 경우로 구분하여 처리한다. 하나는 동일한 DRM 규격의 디바이스간의 콘텐츠 재배포, 다른 하나는 상이한 DRM 규격을 가지는 디바이스 간의 콘텐츠 재배포이다. 이는 상이한 DRM 규격을 가지는 디바이스 간에는 DIM의 도움으로 엑스포트 DRM 규격을 따르는 콘텐츠와 라이선스가 임포트 DRM 규격을 따르는 콘텐츠와 라이선스로 변환되어야 하기 때문이다.

본 시스템에서는 proxy re-encryption 모듈을 사용한다. proxy re-encryption 모듈을 통해 프록시는 앨리스의 공개키(C_{PKA})로 암호화 된 암호문을 밥의 비밀키(C_{PKB})로 복호화 할 수 있도록 변환시켜준다[13][14]. 여기서 프록시가 평문의 어떤 정보도 얻을 수 없다는 것이 특징이며, 보안성 측면에서 큰 장점이 된다. 이와 같이 proxy re-encryption은 프

록시 역할을 하는 DIM이나 임포트 디바이스가 콘텐츠와 라이선스에 관한 평문이나 어떤 디바이스의 비밀키도 획득하지 못하도록 한다. 이로서 DIM은 보호되지 않은 콘텐츠에 접근하지 못하게 된다. 다른 임포트 디바이스 역시 비밀키를 가질 수 없으므로 보호되지 않은 콘텐츠에 접근할 수 없게 된다.

3.1 동종 DRM 규격의 디바이스간 콘텐츠 재배포

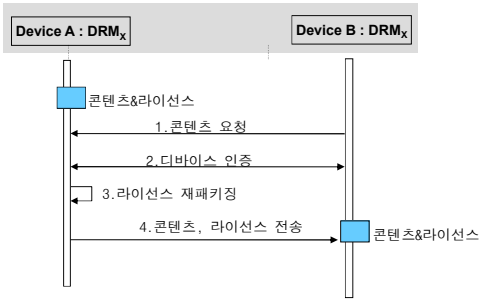

그림 3. 동종 DRM 규격의 디바이스간의 콘텐츠 재배포 과정
Fig 3. Redistribution process of contents between same DRM regime devices

M	콘텐츠
CEK	콘텐츠 암호키
R	콘텐츠 M의 사용 권한
$[M]_k$	키 K로 암호화 한 암호문
$KeyGen_A(\cdot)$	디바이스A를 위한 CEK 생성 모듈
$SEnc_k(\cdot)$	키k를 이용한 대칭키 암호화 모듈
$PEnc_k(\cdot)$	키k를 이용한 공개키 암호화 모듈
$DomainID$	도메인 식별자
DID_A	디바이스 A의 식별자
DDI_A	도메인내에서의 디바이스 A의 식별자
SK_A	디바이스A가 다른 디바이스와의 통신을 위한 세션키

그림 4. 표기법
Fig 4. Notation

홈 도메인에 등록된 디바이스간의 콘텐츠 재배포 과정은 <그림3>와 같다. 디바이스 B의 콘텐츠 및 라이선스의 요청에 따라 디바이스 A는 <그림5>의 프로톨콜 (1)~(3)과 같이 디바이스의 상호 인증 프로토콜을 통하여 디바이스 B가 동일 도메인에 속함을 확인한 후, 디바이스 A의 proxy re-encryption 모듈을 사용하여 라이선스를 디바이스 B의 공개키로 암호화하여 콘텐츠와 함께 디바이스 B로 전송한다.

(1) $D_B \rightarrow D_A$: $request, Cert_B, DDI_B, nonce_B$
(2) $D_A \rightarrow D_B$: $DDI_A, nonce_A, [r, H(r \,//\, DomainID)]_{SK_A}$
(3) $D_B \rightarrow D_A$: $[DID_B, r, H(r \,//\, DomainID)]_{SK_B}$
(4) D_A: $[CEK, R]_{PK_B} = Re\text{-}Enc(rek_{A \rightarrow B}, [CEK, R]_{PK_A})$
(5) $D_A \rightarrow D_B$: $[M]_{CEK}, [CEK, R]_{PK_B}$

그림 5. 프로토콜 1 - 동종 DRM 규격의 디바이스간의 콘텐츠 재배포
Fig 5. Protocol 1 - for redistribution process of contents between same DRM regime devices

3.2 이종 DRM 규격의 디바이스간 콘텐츠 재배포

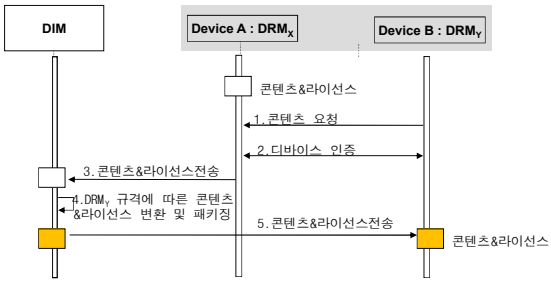

그림 6. 이종 DRM 규격의 디바이스간의 콘텐츠 재배포 과정
Fig 6. Redistribution process of contents between different DRM regime devices

상이한 DRM 규격의 디바이스간의 콘텐츠 재배포과정은 <그림6>과 같다. 상호간의 인증을 마친 후, <그림7>의 프로토콜에서 (5)와 같이 콘텐츠(M)와 사용 권한(R)을 임포트 DRM 규격에 따라 변환시킨다. 이는 DIM이 DRM 프레임워크에 동의한 콘텐츠 제공자로부터 위임받은 사항이다. 변환된 콘텐츠는 키 생성자에 의해 생성된 디바이스 B의 대칭키로 암호화되고, 사용 권한으로 재패키징된 라이선스는 디바이스 B의 공개키로 암호화되어 디바이스 B에게 전송된다.

(1) $D_B \rightarrow D_A$: $request, Cert_B, DDI_B, nonce_B$
(2) $D_A \rightarrow D_B$: $DDI_A, nonce_A, [r, H(r \,//\, DomainID)]_{SK_A}$
(3) $D_B \rightarrow D_A$: $[DID_B, r, H(r \,//\, DomainID)]_{SK_B}$
(4) $D_A \rightarrow DIM$: $[M]_{CEK_A}, [CEK_A, R]_k$,
(5) DIM : Transcode M', Translate R'
(6) DIM : $CEK_B \leftarrow KeyGen_A(1^k)$
(7) DIM : $[M']_{CEK_B} \leftarrow SEnc_{CEK_B}(M')$
(8) DIM : $[CEK_B, R']_{PK_B} = PEnc_{PK_B}(CEK_B, R')$
(9) $DIM \rightarrow D_B$: $[M']_{CEK_B}, [CEK_B, R']_k$,

그림 7. 프로토콜 2 - 이종 DRM 규격의 디바이스간의 콘텐츠 재배포
Fig 7. Protocol 2 - for redistribution process of contents between same DRM regime devices

Ⅳ. 제안 시스템의 분석 및 평가

1. 제안 시스템의 특성 분석

[6]에서 제안된 기존의 홈 도메인 기반의 DRM 시스템과 본 논문에서 제안한 상호 호환성을 위한 홈 도메인 DRM 시스템의 특성을 비교 분석하면 <표1>과 같다. 본 시스템은 기존 시스템과 마찬가지로 도메인내의 디바이스 인증을 위한 프로토콜에서 인증서와 세션키를 이용하도록 하여 도메인내의 불법적인 디바이스의 사용을 막고 완벽하게 디바이스를 식별함으로서 저작권을 보호한다.

또한 도메인 서버로 이용되는 장치는 디바이스의 인증 및 콘텐츠와 라이선스의 재배포를 위해, 도메인 관리에만 초점을 둔 기존의 시스템은 HDAM Agent을 설치하지만, 본 시스템은 HADM Agent 외에 DIM Agent를 설치하여 상이한 DRM 규격의 디바이스간의 콘텐츠 및 라이선스 재배포를 가능하게 하였다.

한편, 기존 시스템에서는 라이선스의 이동이 동일한 DRM 규격의 디바이스에 한해서만 가능하였으나, 본 시스템에서는 DIM Agent가 콘텐츠와 사용 권한을 재패키징함으로서 상이한 DRM 규격의 디바이스에게도 라이선스가 이동될 수 있도록 하여 기존 시스템의 제한적인 라이선스 이동 문제를 개선하고 DRM 규격에 따른 상호 호환성을 제공하였다.

마지막으로, 기존 시스템은 콘텐츠 및 라이선스를 재배포할 때마다 도메인 서버에 재배포 내역인 RDL(Re-Distribution List)을 전송하는데, 이는 RDL에 의한 콘텐츠 사용료 산정을 위한 것으로 데이터 전송량 및 디바이스의 네트워크 의존성이 증가되어 시스템에 부담을 가중시키는 단점이 있다. 본 시스템에서는 이러한 문제를 보완하기 위하여 사용자가 콘텐츠 및 라이선스 재배포를 전제로 책정된 콘텐츠 구매가로 콘텐츠를 구입하는 Usage Rule 방식을 도입함으로서 RDL을 DRM 서버에 보고하지 않아도 되므로 콘텐츠 재배포를 위한 프로토콜이 경량화되었다.

표 1. 기존 시스템과의 특성 비교
Table 1. The comparison of specific characters between DRM systems

비교항목	기존 시스템	제안 시스템
저작권 보호	Y	Y
도메인서버 설치 모듈	HADM	HADM, DIM
라이선스 이동	제한적	Y
DRM 규격에 따른 상호 호환성	N	Y
콘텐츠 재사용료 산정	RDL	Usage Rule

2. 안전성 분석

디바이스 인증 프로토콜을 이용한 제안 시스템은 불법적인 디바이스의 행위를 차단하고 완벽하게 디바이스 식별이 가능하다. 특히, 디바이스 인증 과정에서 난수값을 이용한 비밀키 생성으로 세션이 이루어질 때마다 가변적인 키값을 사용하기 때문에 스니핑 공격과 재전송 공격으로부터 안전성을 확보하였다.

또한, 제안하는 방식은 콘텐츠와 라이선스를 변환하여 재패키징하기 위해 proxy 알고리즘을 사용한다. 이때 DIM이 re-encryption key를 가지지만 콘텐츠 제공자 PA, PB와 디바이스 DA, DB의 비밀키를 알 수 없기 때문에 만약 DIM이 어떤 악의적 사용자와 타협을 한다고 해도 콘텐츠와 라이선스 변환 및 재패키징 과정에서 보호되지 않은 어떤 정보도 악의적인 사용자에게 노출시키지 않을 수 있다. 이로서 상이한 DRM 규격의 디바이스 간의 콘텐츠 재배포가 안전하게 이루어질 수 있다.

Ⅴ. 결론

본 논문에서는 가정과 같은 소집단에서 상호 호환성을 지원하는 디지털 디바이스간의 콘텐츠 공유가 가능한 홈 도메인을 위한 프레임 워크를 제안하였다. 특히 도메인 기반 시스템에서도 지속적으로 콘텐츠 저작권이 안전하게 보호될 수 있도록 콘텐츠의 불법 배포를 막을 수 있는 시스템을 제안하였다. 특히 상이한 규격의 DRM 하의 디바이스간의 콘텐츠 재배포를 위한 콘텐츠 및 라이선스의 변환 및 재패키징을 안전하게 처리하기 위한 프로토콜을 제안하였다.

향후 과제로는 HADM이 디바이스 간의 상호 작용에 관한 정보를 체계적으로 관리하고 활용할 수 있는 방안이 필요하며, 악의적 사용자의 다양한 공격에 대응하기 위한 검토가 필요하다.

참고문헌

[1] Joshua Duhl, "Digital Rights Management : A Definition," IDC 2001.

[2] Brad Cox, Superdistribution: Objects As Property on the Electronic Frontier, Addision-Wesley, May. 1996.

[3] Carlos Serrão, Victor Torres, Jaime Delgado,

Miguel Dias, "Interoperability Mechanisms for registration and authentication on different Open DRM platform", IJCSNS International Journal of Computer Science and Network Security, VOL. 6 NO.12, Dec. 2006.

[4] Natali. Helberger, Nicole, Dufft, Margreet Groene nboom, Kristóf Kerényi, Carsten, Orwat, Ulrich Riehm, "Digital rights management and consumer acceptability," A multi-disciplinary discussion of consumer concerns and expectations, State-of-the-art report, Amsterdam, pp.104 et seq..., 2004.

[5] 이창보, 김정재, 문주영, 이경석, 전문석, "홈 도메인에서 안전한 콘텐츠 전송을 위한 DRM 시스템의 설계," 한국정보처리학회 논문지 C, VOL. 14-C NO. 03, 2007년 4월.

[6] 문주영, 이창보, 김정재, 전문석, "홈 도메인에서 콘텐츠 재배포를 위한 DRM 시스템 설계", 한국컴퓨터정보학회 논문지, VOL. 12 NO. 3, 2007년 7월.

[7] 이창보, "홈 도메인에서 안전한 콘텐츠 전송을 위한 DRM 시스템의 설계," 숭실대학교 석사논문, 2007년 2월.

[8] 성만규, "디지털 저작권 관리(Digital Rights Management) 현황 분석", 동향과 분석, 통권 240호, 2006년.

[9] R. H. Koenen, J. Lacy, M. Mackey, D. Mitchell, "The Long March to Interoperable Digital Rights Management," Proceedings of the IEEE, VOL. 92(6), Jun. 2004.

[10] D. W. Kravitz, T. S. Messerges, "Achieving Media Portability through Local Content Translation and End-to-End Rights Management," Proceedings of the ACM Digital Rights Management workshop DRM'05, pp 27~36, Nov. 2005.

[11] Bogdan C. Popescu, Bruno Crispo, Frank L.A.J. Kamperman, Andrew S. Tanenbaum "A DRM Security Architecture for Home Networks," Proc. 4th ACM Workshop on DRM, pp. 1-10, 2004.

[12] 김정재, 박재표, 전문석, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템," 한국정보처리학회 논문지 C, VOL. 12-C NO. 02 pp. 0183~0190 2005년 4월.

[13] M. Blaze, G. Bleumer, M. Strauss. "Divertible Protocols and Atomic Proxy Cryptography," In EUROCRYPT, pp. 127~144, 1998.

[14] Benoît Libert, Damien Vergnaud, "Multi-Use Unidirectional Proxy Re-Signatures," CCS '08: Proceedings of the 15th ACM conference on Computer and communications security, pp 511~520, Oct. 2008.

저 자 소 개

문 주 영

1995 : 일본 동경농공대학교 공학석사
2008 : 숭실대학교 공학박사
2000 - 현재 :
부천대학 전산정보처리과 부교수
관심분야 : 정보 보호, 멀티미디어 보안, DRM