홈 도메인에서 안전한 콘텐츠 전송을 위한 DRM 시스템의 설계

이 창 보[†] · 김 정 재[††] · 문 주 영[†††] · 이 경 석[††††] · 전 문 석[†††††]

요 약

오늘날 DRM 벤더별 독자적인 기술규격 사용으로 디지털 콘텐츠 및 디지털 기기의 상호호환성이 보장되고 있지 않으며, 디지털 콘텐츠의 권리를 보호할 수 있지만 사용자는 많은 제한과 불편을 감수해야 한다. InterTrust사가 제안한 Superdistribution은 콘텐츠 획득에 상관없이 오직 라이선스와 사용자 인증에 의해 콘텐츠 사용이 가능한 콘텐츠 분배 기술이다. 그러나 원래 콘텐츠가 사용자 소유의 디바이스로부터 다른 디바이스로 이동되어야 할 때 DRM 서버로부터 재 인증과 함께 추가적인 라이선스를 필요로 한다. 이 논문에서는 재 인증과 라이선스 재발급 절차의 불편함을 줄이고 오프라인 상에서 지속적인 콘텐츠 권리의 보호를 위해, 홈 디바이스 간에 도메인을 생성하고 사용자가 도메인 안에서 자유로운 콘텐츠 이동 가능한 DRM 시스템을 제안한다.

키워드 : 저작권보호, 홈 도메인, 디바이스 인증, 라이선스 이동

Design of DRM System for Secure Contents Transfer in Home Domain

Chang-bo Lee[†] · Jung-jae Kim[††] · Ju-young Moon[†††] · Kyung-seok Lee[††††] · Moon-seog Jun[†††††]

ABSTRACT

For the usage of the different standard technology among DRM vendors, the DRM technologies in today could not guarantee the interoperability between the digital contents and digital devices. While users have been guaranteed the protection of contents, they have to put up with the limitation and inconvenience. The Superdistribution methods that InterTrust has proposed is the content distribution technology which is possible to use the content only by the user authentication with the license regardless of the acquisition of the DRM contents. However, it need a additional license with re-authentication from DRM server when the original contents need to be moved to other devices from the own device. In this paper, to reduce the inconveniences of re-authentication and re-issue procedures of the license and continually to protect the rights of contents on the offline, we propose the DRM system that creates domain between home devices and enable users to freely transfer contents with the domain.

Key Words : DRM, Home Domain, Device Authentication, License Move

1. 서 론

최근 정보통신기술의 발전에 따라 초고속 인터넷, 무선 인터넷, 디지털 방송 등 다양한 인프라를 바탕으로 동영상, 이미지, 음악, e-Book등과 같은 디지털 콘텐츠의 유통이 활발하게 이루어지고 있다. 디지털 콘텐츠는 그 특성상 무한히 반복하여 사용해도 품질의 저하가 발생하지 않고, 수정과 복사가 편리하며, 통신망을 통해 대용량의 콘텐츠를 짧은 시간에 전송 및 배포가 가능하다. 이러한 특성은 디지털 콘텐츠의 손쉬운 배포 및 접근 환경을 제공함으로써 누구든지 편리하게 콘텐츠를 이용할 수 있는 순기능을 제공하기도 하지만, 불법복제와 같은 저작권자의 권익을 위협하는 역기능의 원인이 되기도 한다. 이러한 디지털 콘텐츠의 역기능을 막기 위해 암호화 기술을 기반으로 한 디지털 저작권 관리(DRM : Digital Rights Management) 기술이 등장하였다[1].

현재 디지털 콘텐츠의 불법복제방지 및 저작권보호를 위해 다양한 DRM 기술 및 제품들이 출시되고 있으나, DRM 업체별 독자적인 기술규격 사용으로 디지털 콘텐츠 및 디지털 기기의 상호호환성이 보장되지 않고 있다. DRM의 상호호환성 보장을 위해 MPEG-21(Moving Picture Experts Group-21), OMA(Open Mobile Alliance), DMP(Digital Media Project) 등 많은 국제표준단체에서 DRM 표준기술을

† 준 회 원 : 숭실대학교 대학원 컴퓨터학과 박사과정
†† 정 회 원 : (주)RetailTech 수석연구원
††† 정 회 원 : 부천대학 전산정보처리과 조교수
†††† 종신회원 : 산업연구원 연구위원
††††† 종신회원 : 숭실대학교 컴퓨터학부 교수
논문접수 : 2007년 1월 4일, 심사완료 : 2007년 4월 17일

개발하고 있으나, 이들 단체 간에도 독자적인 기술규격 개발로 상호호환성이 보장되지 않고 있다. 한편, 통방융합, 디지털 홈, 디지털기기의 다기능화 등 디지털 기술의 컨버전스 가속화가 이루어지고 있으나 도메인별, 디지털 기기별 사업자별 상이한 기술규격의 사용으로 호환성이 결여되어 디지털 콘텐츠 및 디지털기기의 보급 확산에 장애요소로 대두되고 있다. 만일 자신이 소유하고 있는 여러 장치들 사이에 DRM 기술의 상호 호환성이 보장되지 않는다면 콘텐츠를 이용하는 사용자는 불편함을 감수해야 한다. 미국의 InterTrust 사는 Superdistribution 기술이라 불리는 콘텐츠 분배기술을 제안하였는데, 사용자가 콘텐츠를 입수하더라도 인증된 사용자만이 콘텐츠의 라이선스를 받아 사용할 수 있는 기술이다[2]. 하지만 자신이 소유한 디바이스들 사이에서 콘텐츠가 이동할 때 마다 DRM 서버로부터 새롭게 인증 받아야 하는 문제점이 발생한다.

본 논문에서는 불법복제로부터 디지털 콘텐츠에 대한 지적재산권을 지속적으로 보호하면서, 사용자들이 소유하고 있는 여러 장치들 간에 콘텐츠 이동을 자유롭게 하는 프레임 워크를 제안하였다. 이를 위해 도메인을 생성하고 각각의 장치들은 도메인에 등록을 마친 뒤 상호 인증을 통하여 콘텐츠와 라이선스를 안전하게 이동시킨다. 또한 각 장치들이 도메인 등록 시에 디바이스들이 사용하게 될 Device Key Set을 미리 알려 줌으로써 오프라인 상에서도 지속적인 저작권 보호가 가능하다.

2. 관련 연구

2.1 DRM 시스템의 구성

DRM 시스템은 (그림 1)과 같이 출판업자와 콘텐츠 공급업자, 사용자, 그리고 클리어링하우스(Clearing house)등으로 구성되고 세부 기능은 다음과 같다.

전체 DRM 시스템의 참여자들은 DRM CA로부터 공개키를 등록하고 인증서를 발급 받는다. 콘텐츠 출판업자는 콘텐츠 제공자에게 보호조건, 저작권, 사용조건, 인증 정보, 사용 비용, 사용 추적 조건 등을 명시하고 분배 업자에게 전송한다.

콘텐츠 분배 업자는 출판업자가 제공한 보호조건에 맞도록 암호화 하여 암호화된 콘텐츠를 생성한 후에, 암호화된 콘텐츠는 콘텐츠를 이용하고자 하는 사용자에게 온라인 혹은 오프라인을 통하여 배포된다. 또한 분배 업자는 콘텐츠에 대한 가격, 결제 처리 방법 등을 정한 후 해당 정보를 데이터베이스에 저장하고 클리어링하우스에 전송하여 사용자에 대한 결제 정보를 처리 할 수 있도록 한다. 사용자는 온라인이나 오프라인을 통해 다운로드 받은 콘텐츠는 암호화되어 있기 때문에, 콘텐츠를 이용하기 위해서 라이선스 에이전트를 통해 클리어링하우스로부터 라이선스를 발급받고 해당 라이선스를 클리어링하우스를 통하여 인증한 후 결제 정보를 제공하면 라이선스 에이전트가 콘텐츠를 사용이 가능하도록 한다[3].

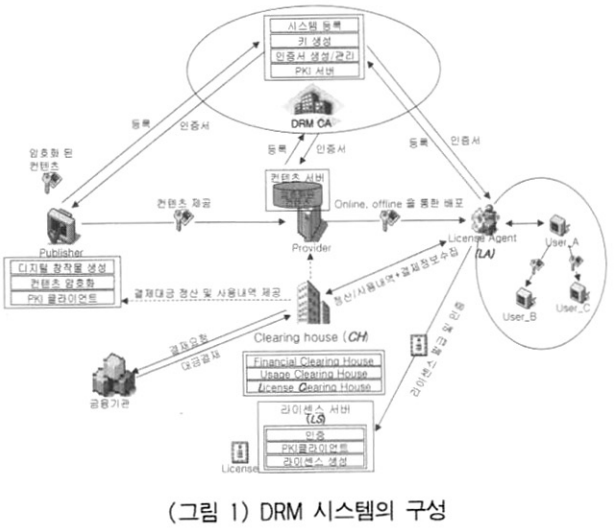
2.2 라이선스 구조

라이선스는 라이선스 일련 번호 sn, 라이선스 발행시간 *date*, 사용규칙 *Usage rule*, 라이선스 하드웨어 바인딩 정보인 *KID* = *H(DID||LSID)*와 기타 필요한 정보를 포함한 *Other_data*를 포함한다. 여기서 *DID*는 사용자의 하드웨어 장치 ID를, *LSID*는 라이선스 서버의 ID를 의미하는 것으로 지정된 디바이스가 아닌 경우에 콘텐츠를 사용 할 수 없게 된다. 그리고 무결성, 부인방지를 위해 이러한 파라미터들을 해쉬 함수로 처리하고 라이선스 서버의 개인키로 암호화 하여 서명을 한다[4].

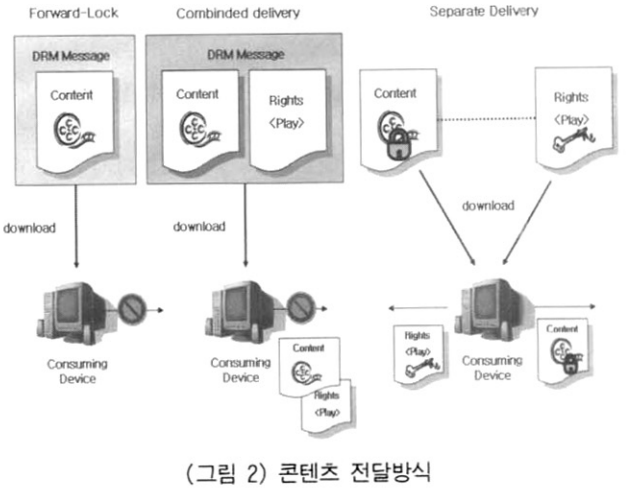
$$License = \{sn,\ KID,\ date,\ Usage\ rule,\ Other\_data,\ SigLS(H(sn,\ KID, date,\ Usage\ rule,\ Other\_data))\}$$

2.3 콘텐츠 전달 방식

콘텐츠 전달 방식에는 (그림 2)와 같이 3가지 방법이 있다.



(그림 1) DRM 시스템의 구성



(그림 2) 콘텐츠 전달방식

- 지정 전달(Forward-lock) : 디바이스에 전달된 콘텐츠가 다른 디바이스로 전송되지 않도록 하는 방식이다. Rights가 존재하지 않으며 사용자는 기본 사용 방침에 따라 콘텐츠를 이용한다.
- 혼합 전달(Combined delivery) : Rights object와 원본 콘텐츠가 함께 DRM Message의 형태로 패키징 된다. Rights object는 사용권한에 대해 정의하며 CP/SP(Contents Provider/Service Provider)는 play, display, print, execute의 권한을 설정할 수 있다. 다운로드 된 콘텐츠 및 Rights object는 다른 디바이스에 전달될 수 없으며 최종 사용자는 DRM Content의 저장, 설치, 삭제 등을 할 수 있어야 한다.
- 분리형 전달(Separate delivery) : 콘텐츠와 Rights object가 서로 다른 채널을 통해 디바이스에 전달된다. Rights는 Push 서비스를 통해 단말기에 전달된다. 콘텐츠는 AES (Advanced Encryption Strandard) 알고리즘을 이용하여 암호화되며 CEK(Content Encryption Key) 없이는 복호화 될 수 없으며, CEK는 Rights에 포함되어 사용자에게 전달된다. 암호화된 콘텐츠는 다른 디바이스로 전달될 수 있지만 Rights의 전달은 불가능하며 콘텐츠를 전달받은 다른 디바이스의 사용자는 새로운 Rights를 발급받아야 한다. Separate delivery 방식은 콘텐츠를 구입한 사용자가 해당 콘텐츠를 제 3자에게 자유롭게 배포할 수 있게 함으로써 다양한 유통 채널을 제공하는 Superdistribution기술을 가능하게 한다. PC 기반의 DRM 기술과는 달리 무선 단말기 플랫폼과 같은 폐쇄된 환경에서는 지정 전달 방식과 혼합 전달 방식만으로도 콘텐츠의 외부 유출로 인한 불법복제를 방지할 수 있었으나, 전체적인 디바이스의 성능 향상과 디바이스 간 통신이 가능해짐에 따라 분리형 전달 방식을 통해 콘텐츠의 기밀성을 증가시키려는 요구가 점차 증가하고 있다.

3. 제안 시스템 구조

집에서 각종 디바이스를 소유하고 있는 사용자는 도메인을 설정한다[5]. 그리고 디바이스를 도메인에 등록 시켜야 한다. 같은 도메인 안에 존재하는 디바이스들은 콘텐츠 이동시 자동으로 같은 도메인에 포함된 디바이스인지 인증을 거쳐 라이선스를 재패키징(re-packaging) 하여 콘텐츠와 라이선스를 보내주어야 한다.

3.1 시스템 요구사항

제안하는 시스템에 필요한 요구사항은 다음과 같다.

- 각각의 디바이스는 디바이스에 인증기관으로부터 발급 받은 디바이스 인증서와 개인키를 디바이스에 탑재한다[6].
- 각각의 디바이스는 DRM 서버로부터 자신의 특성에 맞는 DRM Agent가 설치되어 있다.
- 디바이스에는 유일하게 식별 가능한 디바이스 ID(Identification)가 부여 된다.
- 인증서 및 키는 Temper Resistant Memory에 저장하여 물리적인 공격으로 인한 인증서 및 키 유출을 방지하도록 한다.
- 제안하는 시스템은 모든 장치가 온라인으로 연결되지 않았다고 가정한다.

디바이스가 인증기관으로부터 디바이스 인증서를 부여 받는 과정은 (그림 3)과 같으며 세부내용은 다음과 같다.

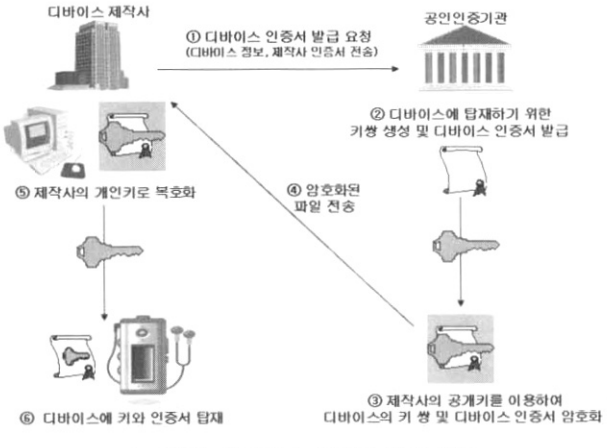
①,② 디바이스 제작사는 디바이스 인증서를 디바이스에 탑재하기 위해 공인 인증기관에 디바이스 정보 및 제작사의 인증서를 전송한다. 그리고 공인인증기관은 디바이스에 탑재 할 공개키와 개인키 쌍과 인증서를 발급한다.

③,④ 디바이스를 위한 키 쌍 및 디바이스 인증서는 보안상의 이유로 제작사의 공개키로 암호화 하여 다시 디바이스 제작사에게 전송한다.

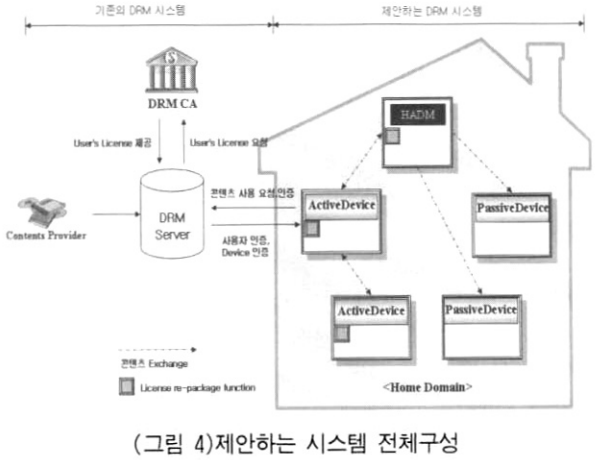
⑤,⑥ 디바이스 제작사는 암호화된 키 쌍 과 디바이스 인증서를 제작사의 개인키로 복호화한 후에 최종적으로 디바이스에 키 와 인증서를 탑재한다.

3.2 제안하는 시스템

제안하는 DRM 시스템의 구성요소는 다음과 같이 크게 3가지로 나뉘며 전체 구조는 (그림 4)와 같다.



(그림 3) 디바이스 인증서 발급 과정



(그림 4)제안하는 시스템 전체구성

- HADM(Home Authorized Domain Manager) : 홈 디바이스의 전체 도메인을 관리하는 장치로 새로운 디바이스를 도메인에 추가하거나, 혹은 디바이스를 제거한다. 사용자는 홈 디바이스들 중 성능이 가장 좋은 디바이스를 선택한다.
- Active 디바이스 : DRM 서버로부터 직접 콘텐츠를 다운로드 받을 수 있는 장치로, 라이선스를 재패키징 할 수 있는 모듈을 가지고 있으며, 비교적 높은 처리능력을 가진 PC, PDA와 같은 디바이스이다.
- Passive 디바이스 : DRM 서버로부터 직접 콘텐츠를 다운 받을 수 없으며, 비교적 제한된 처리능력을 가진 디바이스로 MP3 player, 자동차 오디오등이다.

본 논문에서 제안하는 시스템은 집에서 콘텐츠 이용이 가능한 각종 디바이스를 소유하고 있는 사용자가 여러 디바이스들 중에 성능이 가장 좋은 디바이스를 HADM(Home Authorized Domain Manager)이라 불리는 도메인 관리자로 지정하고, HADM을 통해 도메인을 생성한 뒤에 나머지 각각의 디바이스들을 차례로 도메인에 등록시킨다. 도메인 안에 Active 디바이스는 DRM 서버로부터 사용자 인증과 디바이스 인증 후에 콘텐츠 사용요청을 통하여, 콘텐츠와 라이선스를 다운로드 받아 콘텐츠를 사용할 수 있게 된다. 제안한 시스템의 특징은 디바이스 자신이 소유하고 있는 콘텐츠와 라이선스를 도메인 안에 존재하는 다른 디바이스들에게 전달해야 하는 경우가 발생하면, 디바이스는 같은 도메인에 속한 디바이스인지 자동으로 인증과정을 거쳐 이동하려는 디바이스의 환경에 맞게끔 라이선스를 재패키징 한다. 그리고 한번 라이선스의 이동이 발생하면 원래 라이선스를 가지고 있던 디바이스에는 라이선스가 더 이상 존재하지 않는다. 라이선스는 완전히 이동하게 되고 결국 홈 도메인에 중복된 라이선스가 존재 하지 않으므로 라이선스 관리는 그만큼 쉬워지고, 또한 DRM 서버로부터 다시 라이선스를 발급 받아야 하는 불편함 또한 제거할 수 있다.

3.3 시스템 동작과정

제안하는 시스템의 동작과정은 도메인의 생성, 도메인으로 디바이스 등록, 그리고 디바이스 인증을 통한 콘텐츠 이동으로 구분되어지며, 도메인 안에 디바이스가 추가되거나 제거 되었을 때와, 라이선스 이동에 관하여 기술한다.

3.3.1 도메인 생성

사용자는 최초에, 자신이 소유하고 있는 디바이스들 중에 전체 도메인을 관리하기 위한 도메인 관리자인 HADM을 선택해야 한다. HADM 장치는 키를 생성할 수 있고 DRM 서버와 온라인으로 연결되어 있어야 하며, 라이선스를 재패키징 할 수 있어야 한다. 사용자가 HADM이 될 장치를 선택하였다면, DRM 서버로부터 HADM을 수행하기 위한 HADM Agent를 다운로드 받아 설치한다. HADM Agent는 최초에 도메인 ID를 생성하는데, 도메인 ID는 디바이스 ID(DID)와 TimeStamp를 연접한 값을 해쉬 하여 얻는다 (Domain ID = H(DID || TimeStamp)). 여기서 TimeStamp 값은 시간에 따라 항상 변하기 때문에 DID 값과 연접하여 해쉬를 하면 유일한 값이 보장된다. HADM은 자신에게 등록할 디바이스들이 사용할 Device Key를 미리 생성한다. 키의 개수는 DRM 서버와 사전에 미리 그 수를 정할 수 있지만, 집에서 사용하는 콘텐츠 사용이 가능한 디바이스 개수와 앞으로 도메인에 추가되거나 제거될 디바이스를 개수를 고려하여 AES 암호화 알고리즘으로 128bit Key를 20개 생성한다. 그리고 각 키마다 Domain Device Index(DDI)을 0~19를 부여하여 나머지 각각의 디바이스들이 HADM에 등록을 할 경우, 각 디바이스가 사용하게 될 Key의 DDI와 전체 Device Key Set을 전송한다. HADM은 등록되는 순서에 따라 차례대로 DDI값을 1씩 증가 시킨다.

각 디바이스들이 HADM에 자신을 등록과정을 마치면 HADM Agent는 각각의 디바이스 정보를 수집하여 DRM 서버에게 보고한다. 그리고 도메인 안에 디바이스들이 새로이 추가 되거나 제거되는 경우에도 DRM Agent는 수시로 DRM 서버에게 보고할 수 있다.

3.3.2 디바이스 등록

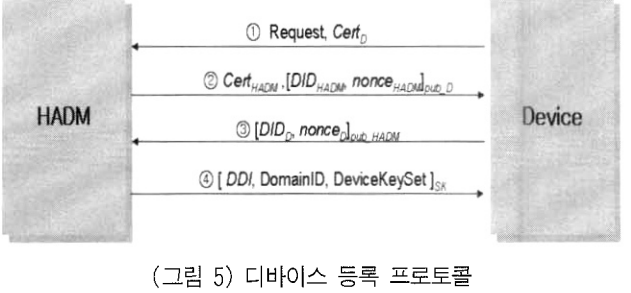
도메인을 생성한 뒤에 각각의 디바이스들은 도메인에 등록을 해야 하며, Active 디바이스와 Passive 디바이스가 HADM에 자신을 등록하는 과정은 (그림 5)와 같으며 세부과정은 다음과 같다.

①,② 디바이스는 HADM에게 자신의 인증서 $Cert_D$와 함께 등록 요청 메시지를 보낸다. 그리고 HADM은 자신의 인증서 $Cert_{HADM}$와 함께 DID(Device ID), 난수 $nonce_{HADM}$를 디바이스의 공개키 pub_D로 암호화 하여 보낸다.

③ 디바이스는 자신의 DID와 난수 $nonce_D$를 HADM의 공개키 pub_HADM으로 암호화하여 보낸다. HADM과 디바이스는 $nonce_{HADM}$와 $nonce_D$를 연접하고 해쉬하여 비밀키 SK를 생성한다(Secret Key = H($nonce_{HADM}$|| $nonce_D$)).

④ HADM은 디바이스에게 디바이스의 DDI(Domain Device Index)와 DomainID 그리고 Device Key Set를 비밀키 SK로 암호화 하여 전송한다.

디바이스의 모든 등록 과정을 마치게 되면 HADM에는 Domain ID와 각 장치에 해당하는 DID, DDI, DeviceKey가

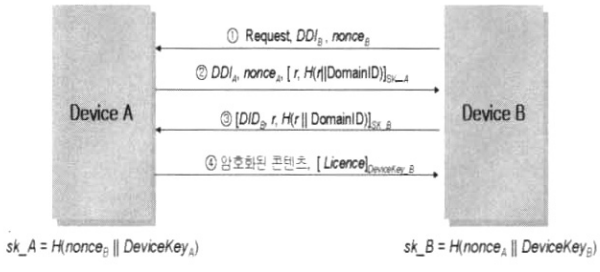


(그림 5) 디바이스 등록 프로토콜

저장되고, 최종적으로 DRM 서버에게 자신의 도메인 정보를 알린다.

3.3.3 디바이스 인증

DRM 서버로부터 콘텐츠를 다운로드 받은 디바이스가 도메인 안에 있는 다른 디바이스에게 콘텐츠를 전송하고자 할 때, 실제 자신의 도메인에 있는 디바이스인지 인증해야만 한다.



(그림 6) 디바이스 인증 프로토콜

디바이스 A와 B가 상호 인증 과정은 (그림 6)과 같으며 세부 내용은 다음과 같다.

① 디바이스 B는 디바이스 A에게 콘텐츠를 요청 메시지와 자신의 Domain Device Index 번호 DDI_B 그리고 난수 $nonce_B$를 보낸다.

② 디바이스 A는 $nonce_B$와 자신의 Device Key를 연접하고 해쉬하여 비밀키 SK_A를 생성한다. 그리고 자신의 Domain Device Index 번호 DDI_A, 난수 $nonce_A$와 r, H(r||DomainID)을 비밀키 SK_A로 암호화 하여 디바이스 B에게 보낸다.

③ 디바이스 B는 [r, H(r||DomainID)]$_{SK\_A}$ 를 복호화하여 디바이스 A가 같은 도메인 안에 있는 디바이스인지 검증을 한다. 만일 같은 도메인 안의 디바이스라면 $nonce_A$와 자신의 Device Key를 연접하고 해쉬하여 비밀키 SK_B를 생성한 후에 DID_B, r, H(r||DomainID)을 비밀키 SK_B로 암호화 하여 디바이스 A에게 보낸다.

④ 디바이스 A는 [DID_B, r, H(r||DomainID)]$_{SK_B}$를 복호화하여 디바이스 B가 같은 도메인의 안에 있는 디바이스 인지 검증을 한다. 같은 도메인의 디바이스라면, 디바이스 사이에 상호인증 과정을 성공적으로 마치게 된다. 디바이스 A는 디바이스 B에게 DRM 서버로부터 받은 암호화된 콘텐츠와 디바이스 B의 DID정보에 맞게 재패키징된 라이선스를 디바이스 B의 Device Key로 암호화 하여 보낸다[7].

상호 인증과정을 마친 후에 디바이스 B는 디바이스 A로부터 받은 콘텐츠와 라이선스로 콘텐츠를 사용할 수 있다.

3.3.4 라이선스 이동

Active 디바이스와는 달리 Passive 디바이스는 라이선스를 재패킹하거나 DRM 서버로부터 직접 콘텐츠를 다운로드를 받을 수 없는 제한된 디바이스가 도메인 안에 존재하므로 제안한 시스템에서 라이선스의 이동가능 여부는 [표 1]과 같다.

〈표 1〉 라이선스의 이동 방향

라이선스 이동방향	가능 여부
Active → Active	○
Active → Passive	○
Passive → Active	×
Passive → Passive	×

Passive 디바이스에서 Active 디바이스로, Passive 디바이스에서 Passive 디바이스는 라이선스를 직접 이동 할 수 없으므로 Passive 디바이스는 HADM으로부터 직접 콘텐츠와 라이선스를 다운로드 받아 사용한다. 그 이유는 Passive 디바이스로 한번 이동한 라이선스는 다시 다른 디바이스로 이동하는데 제한이 있기 때문에, 전체 도메인 관리자인 HADM이 직접 라이선스 사용 기간에 제한을 두고 Passive 디바이스에게 발급을 하고 라이선스에 관한 모든 것을 관리함으로써 Passive 디바이스에서도 안전하게 콘텐츠 이용이 가능하다[8].

3.3.5 디바이스 추가

새로운 디바이스가 도메인 안에 추가되면 3.3.2절에서 기술한 등록 프로토콜을 통해 HADM에 등록한다. 새로운 디바이스가 추가 되어도 특별히 다른 디바이스에게 알릴 필요는 없다. 왜냐하면 도메인 생성 시 도메인의 구성하는 디바이스들에게 미리 Device Key Set를 알려 주었기 때문에, 추가된 디바이스는 등록 시 부여 받은 DDI에 해당하는 키를 사용한다. 나머지 디바이스들도 추가적인 정보를 받지 않고 디바이스 인증 시 Device Key Set에 키를 사용한다. 만일 사용하지 않는 DDI의 키가 없는 경우에는 불가피하게 도메인을 재구성해야 한다.

3.3.6 디바이스 제거

사용자는 디바이스가 다른 도메인으로 이동되거나 디바이스의 물리적인 손상, 도난, 해킹 등 여러가지 이유로 인하여 도메인에서 제거 될 시에 HADM Agent를 통해 DRM 서버에 제거된 장치를 보고하여야 한다. 그리고 장치가 도메인 안에서 제거되었다는 사실을 다른 디바이스에게도 알려야 하는데, 이것은 이미 제거된 장치에 다시 콘텐츠가 전송되는 것을 막기 위해서다.

각각의 디바이스에게 장치가 제거 되었다는 사실을 알리기 위해서 DRM 서버는 콘텐츠 안에다 ADL(Access Device List)라고 불리는 접근 가능한 디바이스 리스트를 함께 패키징 한다. 디바이스 DRM Agent는 자신이 가지고 있는 ADL과 콘텐츠 내에 포함된 ADL을 비교하여 도메인 내의 디바이스 변경 사항을 판단하고 최신의 ADL으로 갱신하다. 뿐만 아니라 HADM은 도메인에 가입된 디바이스들과 연결이 이루어질 때마다, ADL을 갱신하여 도메인 안의 구성원은

항상 최신의 ADL을 유지하여, 불법적인 디바이스에 콘텐츠가 전송되는 것을 막을 수 있다.

만일 HADM은 도메인을 구성하는 가장 핵심적인 장치로 새로운 디바이스로 교체되거나 공격자에 의해 시스템이 붕괴된 경우 DRM 서버에 이 사실을 알리고 3.3.1에 기술한 도메인 생성과 3.3.2의 디바이스 등록과정을 거쳐 도메인을 재구성해야 한다.

4. 제안한 시스템의 분석 및 보안성 평가

4.1 기존의 DRM 시스템과 비교 분석

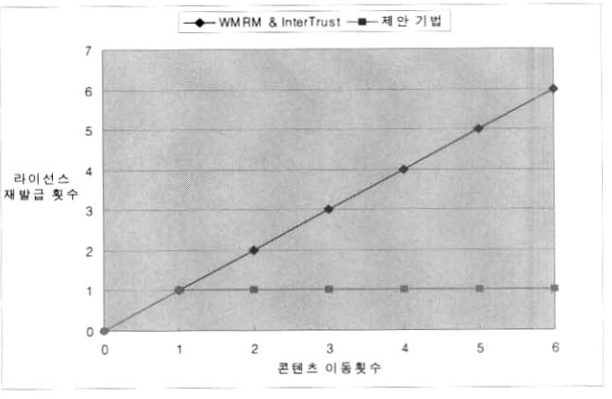
MS사의 DRM인 WMRM과 InterTrust사의 DRM, 그리고 제안한 시스템의 프로토콜을 비교 분석 하면 [표 2]와 같다 [9][10].

〈표 2〉 기존의 DRM 시스템과의 특성 비교

	WMRM	InterTrust	제안 시스템
사용자 설치 모듈	N	Y	Y
적용 가능한 응용 프로그램	동영상 /음악	다양함	다양함
저작권 보호	Y	Y	Y
동적권한변경	제한적임	Y	Y
네트워크 의존성	높음	매우 높음	낮음
라이선스 이동	N	N	Y

WMRM은 별도의 DRM 모듈의 필요 없이 윈도우 미디어 플레이가 DRM 기능을 지원한다. 하지만 윈도우 미디어 플레이어에서만 동작 되므로 다양한 응용 프로그램을 지원하지 못하고 있다, 이에 반해 InterTrust사와 제안한 시스템은 사용자 전용 모듈을 설치하여야 하는 불편함이 있지만 DRM Agent 프로그램을 설치하여 다른 콘텐츠 응용 프로그램과 상호 작용하여 다양한 파일과 응용 프로그램을 지원할 수 있는 장점이 있다. 그리고 제안한 시스템은 기존의 시스템과 마찬가지로 TRM(Temper Resistant Memory)을 지원하여 중요한 키 정보 및 인증 정보의 유출을 방지를 방지하고 있다. WMRM의 경우 라이선스 획득 시에만 인증을 하고 그 이후에는 사용자 장치에 저장되어 구동되므로, 라이선스 사용 규칙과 변경 등에서 제한적이나 InterTrust와 제안한 시스템은 언제든지 라이선스 서버와 연결만 가능하다면 실시간으로 사용 내역을 보고하거나 동적인 콘텐츠 권한 변경이 가능하다.

또한 기존의 DRM 시스템이 지속적인 콘텐츠 저작권 보호를 위해 항상 온라인으로 연결되어 있어야 하나, HADM를 제외하고는 계속적인 온라인 연결을 필요로 하지 않으므로 네트워크 의존다가 다른 시스템에 비해 낮고, 라이선스의 이동성 측면에서도 라이선스에는 DID가 포함되어 라이선스의 이동 자체가 제한되어 있으나, 제안한 시스템은 라이선스 이동이 가능하다는 장점을 가지고 있다.



(그림 7) 기존의 시스템과 제안한 시스템의 라이선스 재발급 횟수

(그림 7)은 콘텐츠 이동 회수에 따른 라이선스 재발급 회수를 나타내고 있다. 기존의 시스템들이 콘텐츠가 이동이 발생할 때마다 콘텐츠를 사용하기 위해 라이선스를 DRM 서버로부터 재발급 받아야 하지만 제안한 시스템은 DRM 서버로부터 한번 발급 받은 라이선스는 라이선스 권한 변경이 없는 한 다시 재발급 받지 않아도 된다.

라이선스 서버는 라이선스를 발급하는 부담을 덜어 과부하를 방지하고, 사용자는 라이선스로부터 새로이 인증 받아야 하는 불편함이 없어진다는 것을 확인할 수 있다.

4.2 안전성 평가

제안한 기법은 기존의 DRM 시스템이 제공하였던 라이선스의 분배권한을 사용자에게도 일부 넘겨주었다. 그러므로 그에 따르는 보안상에 문제점의 발생을 최소화 하고, 기존이 DRM 시스템이 제공한 콘텐츠 보호 기능을 제안한 시스템에서도 계속적으로 유지 할 수 있어야 한다. 제안한 기법에서는 디바이스의 인증을 위해 디바이스에 인증서를 탑재하였다. 이에 수반되는 문제가 없는지 분석해 보고, 악의적인 사용자들에 의한 스니핑(Sniffing), 스푸핑(Spoofing), 재전송(Replay Attack)등의 공격들에 대해서도 안전한지 평가하였다.

4.2.1 디바이스 인증

본 논문에서 제안한 시스템은 도메인에 디바이스 등록 시, 인증을 위해 디바이스 제조 과정부터 디바이스에 인증서의 탑재를 가정하고 있다. 인증서를 사용하는 이유는 불법적인 디바이스의 사용을 막고, 완벽하게 디바이스를 식별하기 위해서이다. 그리고 인증서를 사용한 공개키 암호화 방식은 현재까지 알려진 어떠한 공격에 대해서도 안전하며, 공개키와 개인키로 나누워져 있기 때문에 키 교환을 하는데 있어서도 편리하다.

3.3.2절에서 기술한 디바이스 등록 프로토콜 과정에서 HADM과 디바이스는 서로의 인증서를 교환한다. 인증서를 검증하는 과정은 실시간으로 이루어져야 하기 때문에 인증서를 검증할 처리 능력이 없는 Passive 디바이스에 경우에는

일부 제한이 따를 수 있다. 그러나 HADM은 도메인의 생성 과정부터 사용자와 DRM 서버가 신뢰하는 장치이므로, 도메인에 가입하려는 디바이스가 HADM의 인증서를 검증하는 것은 반드시 필요한 과정은 아니며 보다 중요한 것은 도메인에 가입하려는 장치를 명확하게 식별하여 콘텐츠의 불법적인 도용을 막는 것이다. 만일 제한된 능력을 가진 Passive 디바이스가 도메인에 가입하려할 때, HADM은 Passive 디바이스의 인증서를 OCSP(Online Certificate Status Protocol)를 이용하여 실시간으로 인증서의 유효성을 검증한다.

4.2.2 스니핑 공격에 대한 안정성

집에서 사용하는 기기는 장치에 따라 콘텐츠와 라이선스를 분배하는 방식이 다양하므로, 케이블을 이용하거나 기존의 유선망 혹은 무선망을 통해 콘텐츠와 라이선스의 분배가 가능하다. 제안하는 방식은 어떠한 방식으로 데이터가 전송되던 간에 데이터는 항상 암호화 되어 전송되므로 불법적인 장치가 키를 가지고 있지 않는 한 디바이스 정보가 노출될 위험은 없다. 실제로 디바이스 인증과 등록과정에 있어서, 비밀키 SK는 난수 *nonce*값에 의해 발생되고 세션이 이루어질 때마다 키 값은 항상 변하기 때문에, 키를 유추하는 것이 어렵다. 또한 인증서 교환으로 인해 공개키가 노출되더라도 복호화 하기위해서는 개인키 없이는 *nonce*값을 유추할 수 없기 때문에 안전하다.

4.2.3 스푸핑 및 재전송 공격에 대한 안전성

기존의 DRM 프로토콜의 경우에 데이터의 암호화로 인하여 Sniffing 공격에는 강하나 스푸핑, 재전송 공격에는 매우 취약하다. 제안한 프로토콜은 스푸핑 및 재전송 공격으로부터 안전하기 위하여 디바이스 사이에 전송되는 데이터는 난수를 이용하여 불법적인 장치의 인증을 방지하고 있다. 3.3.3절에서 기술한 디바이스 인증 프로토콜에서 중요한 인증 정보인 Domain ID는 난수 r과 함께 연접하여 해쉬한 값으로 전송하기 때문에, 중간에서 메시지를 가로채더라도 실제 메시지의 내용을 알 수 없을 뿐 아니라 인증이 이루어질 때마다 값이 매번 변하기 때문에 값을 유추하는 것은 불가능하다. 그러므로 실제 Domain ID를 가지고 있지 않은 디바이스가 중간에 메시지를 가로채어 재전송 하여도 인증 받을 수 없다.

5. 결 론

본 논문에서는 디지털 콘텐츠의 지속적인 저작권 보호가 이루어지면서도 집에서 사용하는 디지털 기기 간에 자유로운 콘텐츠 이동을 위한 프레임 워크를 제안 하였다. 사용자는 디지털 기기들의 관리를 위해 도메인 관리자인 HADM을 선별하여 도메인을 생성하고, 나머지 기기들을 도메인에 등록한다. 등록과정에 있어 오프라인 상에서도 지속적인 콘텐츠 저작권 보호를 위해 디바이스들이 사용할 키들을 미리 만들어 안전하게 기기들에게 전송함으로써, 나중에 도메인에 장치들이 추가 되거나 제거 됐을 시에 추가적인 비용이 없이 도메인 유지가 가능하다. 등록된 디바이스들은 도메인 안에서 콘텐츠를 안전하게 다른 디바이스로 이동시키기 위해 상호 인증과정을 통해 라이선스를 재패키징하여 콘텐츠와 라이선스를 보냄으로써 콘텐츠의 저작권 보호는 지속적으로 가능하다.

향후 연구 과제로는 연산 능력이 현저히 떨어지는 디바이스들을 위해 인증 방식에 있어 보다 경량화된 프로토콜이 필요하며, 많은 가정에 제안한 시스템을 적용하기 위해 디바이스들에 적합한 DRM 모듈과 미들웨어의 개발이 필요하다.

참 고 문 헌

[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] 김정재, 박재표, 전문석, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM 시스템," 한국정보처리학회 논문지 C, Vol. 12-C No.02 pp.0183-0190 2005.04.

[4] 박복녕, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜," 한국정보과학회논문지 Vol.30 No.02, pp.189-198, 2003.04.

[5] Natali Helberger, Nicole Dufft, Margreet Groenenboom, 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.

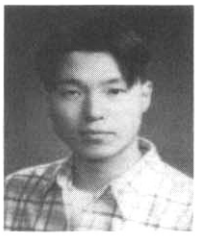
[6] Bogdan C. Popescu, Bruno Crispo, Frank L.A.J. Kamperman, Andrew S. Tanenbaum, "A DRM Security Architecture for Home Networks," Proc. 4th ACM Workshop on DRM, pp. 1-10, 2004.

[7] Iwata T., Abe T., Ueda K., Sunaga H.,"A DRM system suitable for P2P content delivery and the study on its implementation," Proceeding of the 9th Asia-Pacific Conference on Communications (APCC 2003), Vol.2, pp. 806-811, 2003.

[8] Kwok S. H., Lui S. M., "A license Management Model to Support B2C and C2C Music Sharing," 10th International World Wide Web Conference, 2001.

[9] "InterTrust" http://www.intertrust.com/main/overview/drm.html

[10] "Microsoft" http://www.microsoft.com/windo ws/win dowsmedia/drm.asp



이 창 보

e-mail : onsmile79@nate.com
2005년 숭실대학교 컴퓨터학과 공학사
2007년 숭실대학교 대학원 컴퓨터학과 공학석사
2007년~현 재 숭실대학교 대학원 컴퓨터 학과 박사과정
관심분야 : DRM, RFID, 네트워크 보안

김 정 재

e-mail : argniss@nate.com
1995년 영동대학교 컴퓨터공학과 공학사
1999년 숭실대학교 컴퓨터학과 공학석사
2005년 숭실대학교 컴퓨터학과 공학박사
2006~현 재 (주)RetailTech 수석연구원
관심분야 : 멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID

문 주 영

e-mail : jym@bc.ac.kr
1989년 경희대학교 물리학과 학사
1995년 동경농공대학교 전자정보공학과 석사
2004년 숭실대학교 컴퓨터학과 박사수료
2000~현 재 부천대학 전산정보처리과 조교수
관심분야 : 멀티미디어 보안, 전자상거래, DRM, RFID

이 경 석

e-mail : kslee@kiet.re.kr
1978년 숭실대학교 학사
1981년 성균관대학교 석사
1983년~1986년 Univ. Paris 7 연구소(ITODYS) 연구원
1986년 University Paris 7, 박사
1987년~현 재 산업연구원 연구위원
2001년~2006년 건국대 정보통신대학원 겸임교수
관심분야 : 데이터베이스, 네트워크보안, 정보보안표준, 정보보안알고리즘

전 문 석

e-mail : mjun@computing.ssu.ac.kr
1981년 숭실대학교 전자계산학과 공학사
1986년 University of Maryland Computer Science 공학석사
1989년 University of Maryland Computer Science 공학박사
1989년 3월~7월 Morgan State University 조교수
1989년~1991년 New Mexico State University Physical Science Lab 책임 연구원
1991년~현 재 숭실대학교 컴퓨터학부 교수
관심분야 : 전자상거래 보안, 인터넷 보안, 멀티미디어 보안, 인증시스템