Journal of Digital Contents Society Vol. 12 No. 2 Jun. 2011(pp. 165 -176)

스마트카드 기반의 강한 보안을 갖는 DRM 모델의 설계 및 평가

박종용*, 김영학**, 최태영***

요 약

최근에 IT 산업이 발달하면서 디지털 콘텐츠를 보호하기 위한 DRM 기술에 관한 연구가 광범위하게 진행되고 있다. 이러한 기술을 사용하여 디지털 콘텐츠의 불법유통 및 복제를 방지함으로써 저작권자의 이익과 권리를 보호해 준다. 본 논문에서는 스마트카드 인증을 기반으로 하여 보안 기능이 강화되고 효과적인 프로토콜을 갖는 새로운 DRM 모델을 제안한다. 본 논문에서 제안한 모델은 기존의 WCDRM 모델에 비해 다음과 같은 장점을 갖는다. 첫째, 사용자의 고유정보를 보안기능이 강화된 스마트카드에 저장함으로서 공격자가 고유정보를 알 수 없도록 하여 복제방지를 강화한다. 둘째, 저작권자, 배포권자, 인증기관, 사용자 간의 프로토콜을 명확하게 하여 콘텐츠 암호화에 대한 서버의 부담을 줄인다. 셋째, 오프라인환경에서도 동작하며 스마트카드에 사용자의 고유정보를 저장하여 핵심적인 정보가 노출되는 것을 최소화한다. 또한 임의의 공격자에 대해 여러 가지 공격 매개변수에 대해 두 시스템을 비교하여 제안된 시스템이 우위에 있음을 보인다.

Design and Evaluation of DRM Model with Strong Security Based on Smart Card

Jong Yong Park*, Young Hak Kim**, Tae Young Choe***

Abstract

Recently, digital rights management (DRM) related researches are widely spreading with prosperity of IT industries. The DRM technology protects proprietor of copyright by preventing mischanneling and illegal copy. In this paper, we propose a new DRM model that has an enhanced and efficient protocol based on certificate using smart card. The proposed model overcomes weaknesses of WCDRM model and has following additional advantages: first, copy protection is enhanced by hiding user's specific information from attacker by storing the information within smart card; second, server load for contents encryption is reduced by making clear protocols among author, distributer, certificate authority, and users; third, offline user authentication is guaranteed by combining partial secret values in media players and smart card. Exposure of core information also is minimized by storing them in smart card. In addition, we show that the proposed system is more secure than WCDRM model by comparing various factors of anonymous attackers.

Keywords : Smart card, Security, Digital Contents, Digital right management

1. 서론

최근에 다양한 분야의 콘텐츠들이 디지털 매체로 제작되고 있으며 이들을 보호하기 위한 복제방지 기술이 개발되고 있다. 디지털 매체로 제작된 콘텐츠는 기존의 책과 달리 복제 및 복사가 훨씬 간편하며 인터넷 등 각종 매체들을 통

※ 제일저자(First Author) : 박종용
접수일:2011년 04월 20일, 수정일:2011년 05월 19일
완료일:2011년 06월 07일
* 금오공과대학교 컴퓨터공학과
** 금오공과대학교 컴퓨터공학과(교신저자)
*** 금오공과대학교 컴퓨터공학과
▣ 본 연구는 2009년도 금오공과대학교 학술연구비 지원을 받아 수행되었습니다.

하여 빠르고 광범위하게 일어날 수 있다. 그러나 복제방지 기술의 발달에도 불구하고 익명의 사용자들에 의해 불법 복제가 빈번하게 일어나고 있다. 저작권보호협회의 자료에 따르면 불법복제 적발건수는 오프라인(25.7%)보다 온라인(74.3%)에서 훨씬 많이 발생하지만 금액규모에서는 오프라인(78.7%)이 온라인(21.3%)보다 훨씬 큰 것을 보여준다[1].

디지털 콘텐츠를 보호하기 위한 대표적인 방법으로는 DRM(Digital Right Management) 기술이 있다. 이 방법은 디지털 콘텐츠의 저작권을 보호하고 디지털 콘텐츠의 불법유통 및 복제를 방지함으로써 저작권자의 이익과 권리를 보호해 준다[2]. Jiaming He 등은 디지털 콘텐츠의 암호화와 워터마크를 사용하여 콘텐츠를 보호하는 WCDRM(Watermark & Cryptography DRM) 모델을 제안하였다[3]. 이 모델에서 콘텐츠를 등록할 때 CA(Certificate Authority)가 저작권자와 배포권자의 워터마크를 삽입하고 사용자의 라이선스 키를 생성하기 위해 휴대용기기의 핑거프린트와 같은 고유정보를 이용한다. 이러한 방법을 개선한 연구가 [4]에서 진행되었다. 여기서 휴대용기기는 MP3 재생기, 스마트폰 등 휴대가 간편하지만 제한된 하드웨어 성능을 가지고 있는 장비를 말한다. 현재 스마트폰과 같은 휴대용기기는 USIM과 같은 스마트카드에 접근할 수 있다.

Jiaming He 등이 제안한 방법을 사용함으로써 저작권 분쟁이 일어났을 때 내부에 삽입된 워터마크와 암호화된 콘텐츠를 이용하여 저작권자의 이익과 불법복제를 보호할 수 있다. 그러나 이 방법은 다음과 같은 문제가 있을 수 있다. 먼저 이 모델은 추상적인 프로토콜 정의로 인증과정을 명확하게 설명하지 못하였으며 같은 콘텐츠에 대해 중복된 암호화 루틴을 수행하여 서버에 과중한 부담을 준다. 또한 불법복제가 일어나는 여부를 파악할 수 없으며 휴대용기기의 핑거프린트를 사용하여 라이선스 키를 생성하기 때문에 이 정보를 입수한 공격자에게 공격을 당할 수 있다는 약점을 가진다.

DRM 기술을 활용한 스트리밍서비스의 예로 마이크로소프트사의 WMDRM (Windows Media Right Management System)이 있으며 이를 구현한 실버라이트(Silverlight)의 경우는 암호화된 콘텐츠를 재생할 때 라이선스를 요구한다[5]. 이 시스템은 사용자가 서버에 접속하면 클라이언트는 내부에 DRM 소프트웨어가 설치되어 있는지 확인하는 작업을 거친다. 그러나 스트리밍서비스는 온라인 환경에서 가능하며 이 시스템은 장치기반의 DRM을 구현하고 있기 때문에 장치가 바뀌면 라이선스를 중복으로 구매해야 하는 단점이 있을 수 있다[6].

본 논문에서는 Jiaming He 등[3]이 제안한 방법의 문제점들을 개선하여 휴대용기기가 변경되거나 오프라인 환경에서도 활용 가능한 스마트카드를 사용한 새로운 형태의 DRM 모델을 제안하고 이를 기존의 시스템과 비교한다. 스마트카드란 자체 연산이 가능하고, 메모리 공간에 IC 기억소자를 장착하여 대용량의 정보를 저장할 수 있는 플라스틱 카드로서 일반 저장매체와는 여러 가지 차이점을 가지게 된다. 내부에 저장공간이 있어 인증서 등을 저장할 수 있는 것은 일반 메모리와 동일하지만, 비밀번호가 존재하여 비밀번호 인증을 통하여 권한을 획득하여야 내부의 정보를 사용할 수 있다. 스마트카드는 보안성이 뛰어나 전자인증 기반기술을 기반으로 하는 금융거래, 모바일 인증 등의 분야에 널리 사용되고 있다[7]. 스마트카드를 사용하여 리모트 사용자를 인증하는 방법과 이와 유사한 결과들이 이전에 [8,9]에서 연구되었다.

본 논문에서 제안한 모델은 Jiaming He 등의 방법을 근간으로 하나 다음과 같은 차이점을 갖는다. 첫째, 사용자의 고유정보를 보안기능이 강화된 스마트카드에 저장함으로서 공격자가 고유정보를 알 수 없도록 하여 복제방지를 강화한다. 둘째, 저작권자, 배포권자, 인증기관, 사용자 간의 프로토콜을 명확하게 하여 콘텐츠 암호화에 대한 서버의 부담을 줄인다. 셋째, 오프라인환경에서도 동작하며 스마트카드에 사용자의 고유정보를 저장하여 핵심적인 정보가 노출되는 것을 최소화한다. 또한 등록과정에서 해시 알고리즘을 적용하여 휴대용기기내의 재생프로그램이 복제방지 여부를 판단하도록 함으로써 저작권자의 권리를 보장한다. 본 논문에서는 이러한 방법을 통하여 시스템이 공격받더라도 스마트카드 내의 정보를 보호하여 보다 신뢰성이 보장된 콘텐츠 관리기법을 제시한다.

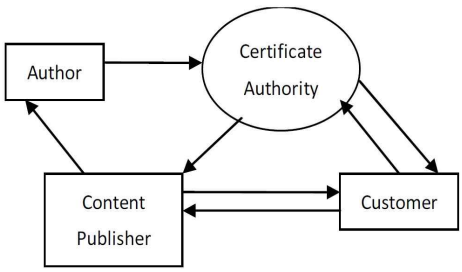
본 논문의 2장에서는 Jiaming He 등이 제안

한 WCDRM 모델 및 디지털 콘텐츠 복제방지를 위한 방법들을 설명한다. 3장에서는 본 논문에서 제안한 스마트카드를 사용한 새로운 DRM 시스템을 설명한다. 4장에서는 제안된 모델과 기존의 모델에 대해 비교를 하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 WCDRM

이 모델은 2008년에 Jiaming He 등에 의해 제안되었으며 그 구성은 (그림 1)과 같다[3]. 구성요소는 콘텐츠의 암호화 및 라이선스 발급을 담당하는 CA와 콘텐츠의 저작권자(Author), 그리고 저작권자로부터 판권을 구입하여 암호화된 콘텐츠를 CA로부터 사용자에게 전송하는 배포권자(Contents Publisher)가 있다. 마지막으로 배포권자에게 콘텐츠를 요청하여 암호화된 콘텐츠를 다운로드하고, CA에 인증을 시도하여 라이선스를 다운로드한 뒤 복호화하여 콘텐츠를 재생하는 사용자(Customer)가 있다.



(그림 1) WCDRM의 구성 및 흐름

CA는 콘텐츠에 대한 라이선스를 제작하기 위하여 라이선스 서버를 내부에 가지고 있다. CA의 역할은 콘텐츠의 암호화와 암호화 키를 라이선스 서버로 전송하는 역할을 담당한다. 라이선스 서버는 복제 방지를 위한 라이선스 생성을 담당하며 라이선스의 복호화 키를 휴대용기기의 핑거프린트를 이용하여 제작한다. 사용자는 콘텐츠를 이용하기 위해서 배포권자의 웹 페이지에 접속하여 원하는 콘텐츠를 요청한다. 배포권자는 CA에 사용자 요청이 있음을 알리고 콘텐츠의 암호화와 라이선스를 생성하는 과정을 수행하고 사용자에게 등록 및 지불 과정을 수행하도록 한다. 사용자는 정상적인 절차를 완료한 후에 콘텐츠와 라이선스를 자신의 장치에 다운로드하여 재생한다.

이 시스템에서는 총 3번의 워터마크가 일어난다. 먼저 저작권자가 CA에게 콘텐츠를 전송하는 과정에서 저작권자의 워터마크가 삽입되고, 다음에 CA가 배포권자에게 콘텐츠를 전송하는 과정에서 배포권자의 워터마크가 삽입된다. 마지막으로 사용자의 요청이 있을 경우 사용자의 특정 워터마크가 삽입된다. 또한 CA가 콘텐츠를 배포권자에 전송할 때와 사용자가 배포권자에게 요청시 휴대용기기의 핑거프린트를 사용하여 같은 콘텐츠에 대해 2회의 암호화 과정을 수행한다.

WCDRM 모델은 워터마크 및 암호화를 사용하여 유통단계에서 공격자와 콘텐츠를 다운로드한 사용자가 콘텐츠를 위·변조하는 공격에는 효율적으로 대체할 수 있다. 콘텐츠가 암호화되어 전송되기 때문에 라이선스를 획득하지 못하여 콘텐츠의 복호화 키를 획득할 수 없는 공격자는 콘텐츠를 복호화 할 수 없기 때문에 콘텐츠는 안전하다고 할 수 있다. 그리고 라이선스를 획득한 경우에도 라이선스를 복호화 할 수 없기 때문에 콘텐츠는 무의미한 파일이 되어버리게 된다.

그러나 이 모델은 불법복제가 일어나는 것을 감지하거나 방지할 수 있는 것은 아니다. 이 모델은 불법복제를 방지하기 위해 라이선스를 발급하여 사용하는 것이 전부이며 라이선스 발급 과정에서 라이선스 생성을 위해 휴대용기기의 고유한 값을 사용한다. 휴대용기기의 고유한 값이 공격자에게 유출될 경우에는 라이선스의 복호화 키를 생성하여 라이선스를 복호화하여 콘텐츠의 암호화키를 얻을 수 있다. 이후 공격자는 콘텐츠를 복호화하여 재생이 가능하다. 이외에도 사용자의 불법복제를 목적으로 악의적인 복제 프로그램을 이용하여 콘텐츠를 복호화하여 파일을 불법복제 할 수 있다.

2.2 스트리밍서비스

스트리밍이란 인터넷(네트워크)을 바탕으로 사용자들에게 각종 비디오, 오디오 등의 멀티미디어 디지털 정보를 제공하는 기술로서 전송되는 데이터가 마치 물이 흐르는 것처럼 처리된다

고 해서 붙여진 이름이다. 보통 암호화된 콘텐츠는 다운로드가 완료된 뒤에 복호화를 거쳐 콘텐츠가 재생되지만 스트리밍서비스는 암호화된 콘텐츠를 다운로드하는 것과 동시에 복호화를 수행하여 재생이 가능하다. 콘텐츠를 여러 부분으로 나누어 저장한 뒤 압축하여 전송함으로써 대용량 멀티미디어 콘텐츠도 재생이 가능하다. 스트리밍서비스는 데이터의 전송방식에 따라 라이브 스트리밍과 프로그레시브 다운로드의 2가지 형태가 있다.

라이브스트리밍은 하드 디스크에 파일을 저장하지 않고 컴퓨터 또는 휴대용기기에 콘텐츠를 직접 전송하는 방식이다. 따라서 이때 사용되는 데이터인 라이브 스트림은 방송되는 동안만 사용이 가능하다. 우리나라에서 실시간 중계를 하고 있는 매체 및 사이트인 아프리카, 다음팟, 방송사의 Live TV 등과 같은 인터넷 방송매체를 예로 들 수 있다.

프로그레시브 다운로드는 콘텐츠를 분할하여 일정한 크기로 나누고 각 부분을 독립적으로 압축한다. 사용자는 압축한 데이터를 다운로드한 뒤 압축을 해제하여 다운로드하는 중에 미디어를 재생할 수 있다. 라이브스트리밍과의 차이점은 다운로드 되는 콘텐츠가 사용자의 컴퓨터에 일시적, 영구적으로 저장되어 처리된다는 것이다. 이는 사용자가 콘텐츠를 복제할 수 있는 문제를 발생시키는 원인 중의 하나이다.

스트리밍서비스의 가장 큰 장점이자 단점은 '온라인(네트워크) 상태를 유지해야한다'는 것이다. 쉽고 간편하게 콘텐츠를 다운로드하여 재생할 수 있지만 오프라인 환경에서는 사용이 불가능하다. 더군다나 네트워크뿐만 아니라 클라이언트 쪽의 성능에 따라 처리 속도가 달라진다. 처리속도에 따른 재생 속도의 불안정함은 사용자에게 큰 불편을 줄 수 있다. 예를 들면 콘텐츠의 다운로드가 완료되지 않았거나 다운로드된 콘텐츠의 복호화가 끝나지 않은 경우는 버퍼링이 발생하게 되는데 이 부분이 사용자에게 불편을 유발하게 된다.

3. 스마트카드 인증 기반의 제안 시스템 모델

3.1 개요

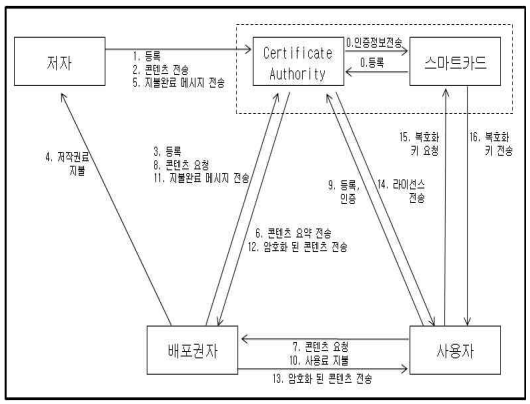
본 논문에서 제안한 모델은 다음과 같은 특징을 갖는다. 첫째, 사용자의 고유정보를 보안기능이 강화된 스마트카드에 저장함으로써 공격자가 고유정보를 알 수 없도록 하여 복제방지를 강화한다. 둘째, 저작권자, 배포권자, 인증기관, 사용자 간에 올바른 인증 프로토콜을 확립하고 콘텐츠 암호화에 대한 부담을 줄인다. 셋째, 오프라인 환경에서도 동작하며 사용자의 고유정보를 스마트카드에 저장하여 핵심적인 정보가 노출되는 것을 최소화한다.

이러한 시스템 구현을 위해 스트리밍서비스 기술에 사용된 콘텐츠의 분할 기법을 본 모델에 적용한다. 콘텐츠를 일정한 크기로 분할하여 암호화할 경우 콘텐츠가 부분적으로 노출되더라도 전체 콘텐츠가 불법복제 되는 것을 방지할 수 있다. 다음에 스마트카드를 이용하여 사용자의 정보를 저장하여 보안을 강화한다. 스마트카드는 PIN(Personal Identification Number)을 이용하여 스마트카드에 대한 인증을 우선적으로 수행해야 사용이 가능하다. 그리고 휴대용기기에 장착하여 사용할 수 있기 때문에 휴대용기기에 저장된 콘텐츠와 사용자 보호가 가능한 콘텐츠 관리 환경을 구축하는데 유용하다.

본 논문에서는 내부 공격자가 복호화된 콘텐츠를 유출시킬 가능성이 있으므로 재생프로그램에 비밀번호를 저장하여 라이선스 복호화 키의 부분정보와 해시 연산을 통하여 라이선스 복호화 키를 생성한다. 본 논문에서 제안한 시스템은 공항, 기차역, 버스터미널, 학교 등 사람들이 많이 모이는 장소에 설치되어 사용자가 원하는 디지털 콘텐츠를 사용자의 휴대용기기에 제공할 수 있다. 또한 사용자는 커피 자판기에서 커피를 뽑듯이 일정 금액을 지불하면 자신의 휴대용기기에 원하는 콘텐츠를 다운로드할 수 있으며 그 콘텐츠를 오프라인 환경에서 사용할 수 있다.

본 논문은 Jiaming He 등[3]의 WCDRM 모델을 기본 구조로 사용하나 스마트카드 기반의 인증과정을 거친다. 본 논문에서는 먼저 WCDRM 모델에서 불명확하게 추상적으로 정의된 콘텐츠

의 인증과정을 (그림 2)와 같이 구체적으로 정의한다. 다음에 이러한 콘텐츠의 인증과정이 스마트카드를 사용하여 진행됨을 설명한다.



(그림 2) 스마트카드 기반의 콘텐츠 유통 흐름

(그림 2)에서 보인 것과 같이 전체 시스템은 저작권자, 배포권자, 인증기관(CA), 사용자, 사용자의 스마트카드로 구성된다. 전체 시스템에 대한 개괄적인 흐름은 다음과 같으며 괄호 안의 번호는 그림에서 표기한 각 단계의 번호를 의미한다.

- ○ 초기단계(점선부분)로 사용자는 CA와 연계한 스마트카드 판매처에서 스마트카드를 구매하여 CA에 등록한다. CA는 사용자의 스마트카드에 고유 식별 값과 인증에 필요한 해시함수를 저장한다(0).
- ○ 저작권자는 자신의 정보를 CA에 등록(1)하고 저작권을 갖는 콘텐츠를 CA에 전송(2)한다.
- ○ 배포권자는 자신의 정보를 CA에 등록(3)하고 배포를 원하는 콘텐츠를 선택하여 저작료를 저작권자에 지불(4)한다. 저작권자는 지불완료 메시지를 CA에 전송(5)하고 CA는 콘텐츠의 요약 정보를 배포권자에 전송(6)한다. 배포권자는 콘텐츠의 요약 정보를 자신의 웹 사이트에 게재하여 사용자에게 홍보한다.
- ○ 사용자는 배포권자의 웹 사이트에 접속하여 자신이 원하는 콘텐츠를 선택하여 요청(7)한다. 그러면 배포권자는 사용자의 정보와 사용자가 원하는 콘텐츠를 CA에 요청(8)한다. 이때 사용자는 CA를 통하여 등록 및 인증절차(9)를 거치게 된다. 사용자가 배포권자에게 사용료 지불을 완료(10)하면 배포권자는 지불 메시지를 CA에 전송(11)하고 CA는 사용자의 정보를 포함하여 해당 콘텐츠를 완전하게 암호화한 후에 그 결과를 배포권자(12)에 전송한다. 마지막으로 배포권자는 사용자가 자신의 휴대용 기기에 요청한 암호화된 콘텐츠를 다운로드(13)하게 하고 CA는 스마트카드 인증 기반의 라이선스를 생성하여 사용자에게 전송(14)한다.
- ○ 사용자는 자신의 스마트카드를 사용하여 복호화 키를 알아내고 이 키를 이용하여 암호화된 콘텐츠를 복호화 하여 재생할 수 있다(15,16). 스마트카드 내에는 CA가 인증한 사용자 식별 값 및 해시 알고리즘이 저장되어 있어 이를 기반으로 복호화 키를 생성하게 된다.

CA는 사용자 등록 및 인증과정을 수행하고 이에 필요한 인증서를 관리하며 콘텐츠의 암호화 및 라이선스를 생성하는 역할을 수행한다. 실제로 구현과정에서 CA의 부담을 줄이기 위해 내부에 로그인 서버(Login Server), 콘텐츠 서버(Contents Server), 라이선스 서버(License Server)를 별도로 둘 수 있다. 그러나 CA의 작업량이 적은 경우에는 이 서버들을 하나의 컴퓨터시스템 내에서 통합하여 운영할 수 있다. 작업량이 많을 경우는 별도의 컴퓨터를 사용하여 병렬처리를 통하여 CA의 부하를 줄일 수 있다. 라이선스 서버는 콘텐츠를 암호화할 때 사용했던 키를 암호화하는 역할을 수행하며 로그인 서버는 사용자 인증을 수행한다.

콘텐츠의 전체 흐름과정에서 CA는 스마트카드의 비밀번호를 설정하는 보안 관리자의 역할과 콘텐츠의 암호화를 위해 키를 생성하는 역할을 수행한다. 또한 등록과정에서 사용자의 정보를 데이터베이스에 저장하고 이를 이용하여 사용자가 인증을 시도할 때 사용자의 인증정보를 받아 인증과정을 처리한다. 본 논문에서는 스마트카드의 인증을 위해 Das 등[10]이 제안한 알고리즘을 응용하여 본 시스템에 적용한다.

3.2 주요루틴

3.2.1 저작권자의 등록과정

저작권자는 CA에 콘텐츠를 등록하기 위하여 CA와 저작권자간의 상호 인증과정이 필요한데, 이를 위해 상호간의 공개키 인증서를 이용한다 [11]. 인증이 완료되면 CA와 사용자는 서로의 인증서를 이용하여 세션 키를 교환함으로써 비밀채널을 개설하고 CA는 이 비밀채널을 이용하여 태그가 삽입된 콘텐츠를 저작권자로부터 수신한다. 최초에 저작권자가 CA에 자신의 정보를 등록하는 과정은 다음과 같으며 등록 후에는 CA의 인증과정을 거쳐 자신의 저작물을 관리할 수 있다.

【Procedure 1 : 저작권자의 등록】

1. Login 서버는 등록양식을 저작권자에게 전송한다.
2. 저작권자는 ID, Password, E-mail 등의 등록양식을 작성하여 서버에 전송한다.
3. Login 서버는 저작권자의 정보를 데이터베이스에 저장한다.

3.2.2 배포권자의 등록과정

콘텐츠를 이용하여 이익을 얻고자 하는 배포권자에 대해서도 등록과정이 필요하다. 배포권자의 등록과정은 저작권자의 등록과정과 유사하며 콘텐츠의 획득을 위해 저작권자에게 비용을 지불하여야 한다. 비용을 지불하는 방법은 현재 사용되고 있는 인터넷뱅킹, 신용카드 등을 사용할 수 있으며 배포권자의 등록과정은 다음과 같다.

【Procedure 2 : 배포권자의 등록과정】

1. (Procedure 1)의 절차에 따라 배포권자의 정보를 CA에 등록한다.
2. 등록과 동시에 배포권자는 해당 콘텐츠의 저작권자에게 저작권료를 지불하고 판권을 획득한다.
3. CA가 해당 콘텐츠에 배포권자의 태그를 삽입 후 판권 획득 확인 메시지와 콘텐츠의 요약정보를 전송한다. 이 단계에서 암호화된 전체 콘텐츠를 전송하지 않고 요약정보만을 전송하여 서버의 부담과 통신 과부하를 줄인다.
4. 배포권자는 콘텐츠의 판매를 위해 자신의 웹 사이트에 CA로부터 인증 받은 콘텐츠들의 이름과 요약정보 등을 사용자를 위해 게시한다.

3.2.3 사용자의 콘텐츠 요청

사용자는 배포권자가 운영하는 웹 사이트에 접속하여 게시된 콘텐츠의 목록을 검색하고 요약정보를 확인한 후에 원하는 콘텐츠를 선택하여 요청한다. 배포권자는 사용자가 요청한 콘텐츠를 확인하고 CA에게 알리며, CA는 사용자에게 해당 콘텐츠에 대한 라이선스를 부여하고 배포권자에게는 그 콘텐츠 전체를 암호화하여 전송한다. 콘텐츠의 불법복제, 변형 등의 방지를 위해 CA는 스마트카드를 기본으로 하는 인증절차를 시도한다.

본 시스템에서는 사용자가 스마트카드 구입 시 선택한 사용자 계정 정보가 CA의 승인을 받아 미리 스마트카드에 저장되어 있다고 가정한다. 이러한 부분은 스마트카드 판매처를 CA와 연계함으로서 구현될 수 있다. 스마트카드가 CA에 정상적으로 등록되면 스마트카드에는 CA가 제공한 스마트카드의 고유 식별 값인 S_n과 향후 인증에 사용될 해시함수 $h(\cdot)$가 저장된다.

사용자가 콘텐츠를 요청하기 위하여 배포권자의 웹 사이트에 접속할 때 익명의 사용자가 콘텐츠를 요청하여 사용하는 것을 방지하기 위하여 사용자 인증이 필요하다. 이러한 문제 해결을 위해 CA는 스마트카드가 등록되지 않은 사용자에 대해서는 신규로 등록을 요청한다. CA는 ID(사용자 계정), PW(비밀번호), $E\text{-}Mail$(이메일 주소), S_n(서버에 등록된 스마트카드 식별값), 난스 (nonce) N, 그리고 P(재생프로그램의 정보) 항목들을 포함한 등록양식을 사용자에게 전송하게 되고 사용자는 등록양식을 작성하여 CA로 전송한다. 여기서 난스 N은 사용자 입장에서 상대방이 적합한 CA인가를 확인하기 위해 사용한다.

CA는 배포권자에 재생 프로그램의 정보 P를 보내서 그 프로그램의 비밀 값 X(재생프로그램의 비밀키)를 수신한 뒤 데이터베이스에서 사용자의 계정 ID를 키 값으로 검색하여 PW, $E\text{-}Mail$, X, 그리고 S_n을 저장한다. 이후 인증 프로토콜이 진행될 때 이 값들과 스마트카드 내부에 저장되어 있는 값들을 이용한다. 여기서 X

는 휴대용기기에서 수행되는 콘텐츠 재생프로그램의 내부 비밀 값으로 정식 사용자가 구입한 콘텐츠를 악의적으로 복제하는 것을 방지하기 위해 사용된다. 이 값은 재생프로그램의 버전이 변경될 때마다 바뀐다. X값이 역공학을 통해 드러나는 것을 어렵게 하기 위해 코드 난독화(obfuscation)를 사용할 수 있다[12].

인증은 사용자와 CA의 처리과정으로 나뉘게 되고 인증과정에서 사용자는 우선적으로 스마트카드를 휴대용기기에 연결하고 연결프로그램을 사용하여 스마트카드의 비밀번호를 입력하여 스마트카드를 인식시킨다. 스마트카드가 인식된 이후에 사용자 인증요청과 처리과정은 (Procedure 3)과 (Procedure 4)와 같은 절차를 따라 진행된다. 인증을 완료한 CA는 사용자에게 지불과정에 필요한 사용 약관을 시스템의 화면에 출력한다. 사용자가 콘텐츠를 휴대용기기로 다운로드를 원한다면 약관에 동의를 하게 되고 결재과정을 통하여 콘텐츠 이용료를 지불하게 된다. 다음에서 $h(\cdot)$는 해시함수를 의미한다.

【Procedure 3 : 사용자의 인증요청】
1. 사용자는 자신의 휴대용기기에서 인증 프로그램을 실행하여 스마트카드를 통하여 CA에 전송할 인증 데이터를 요청한다.
2. 스마트카드는 내부에 저장된 ID, PW, S_n 등의 정보를 사용하여 스스로 $Data_{Login} = h(ID|h(PW)|S_n)$을 계산하여 그 결과를 휴대용기기에 전송한다.
3. 휴대용기기의 인증 프로그램은 스마트카드로부터 전송된 사용자의 인증 정보 $Data_{Login}$과 사용자 계정 ID, 콘텐츠 재생 프로그램의 정보 P를 포함한 $ID|P|Data_{Login}|N$을 CA에 전송하여 합법적인 인증을 요청한다.

【Procedure 4 : CA의 인증처리】
1. CA는 사용자의 휴대용기기로부터 인증요청 정보 $ID|P|Data_{Login}|N$을 수신한다.
2. CA는 ID를 키 값으로 검색하여 해당 PW, S_n을 CA 내부의 데이터베이스로부터 얻는다.
3. CA는 단계 2에서 찾은 값들을 이용하여 $h(ID|h(PW)|S_n)$를 계산하고 이를 $Data_{Login}$과 비교한다. 두 값이 동일하면 인증요청을 승인한다.

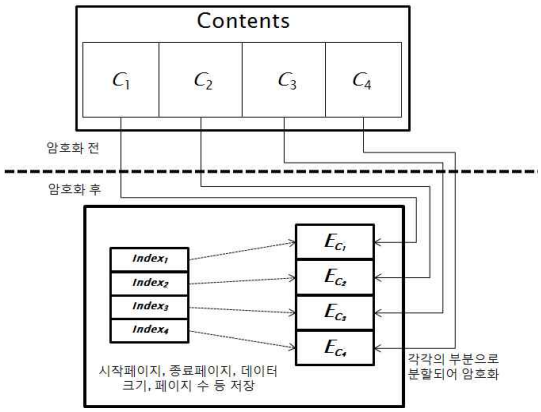
3.2.4 콘텐츠 암호화와 라이선스 제작과정

결재과정이 완료되면 CA는 콘텐츠의 암호화에 필요한 키 K_C를 난수생성기를 이용하여 생성한다. 앞에서 설명한 것과 같이 CA는 병렬처리를 통하여 서버의 부하를 줄이기 위해 하위 서버로 콘텐츠 서버와 라이선스 서버를 가지고 있다. CA는 사용자가 원하는 콘텐츠 파일과 비밀키 K_C를 콘텐츠 서버로 전송하면 콘텐츠 서버는 이를 수신하여 암호화된 콘텐츠를 제작한다. 동시에 라이선스 서버는 CA로부터 비밀키 K_C, S_n, ID, PW, 그리고 X를 전송받아 사용자의 라이선스를 제작한다. (Procedure 5)는 콘텐츠 서버에서 콘텐츠를 암호화하는 과정을 보여준다. 콘텐츠의 암호화는 3DES나 AES[13] 등 이미 알려진 여러 가지 알고리즘을 사용하여 구현될 수 있다.

【Procedure 5 : 콘텐츠 서버의 암호화 과정】
1. 콘텐츠 서버는 CA로부터 사용자가 요청한 콘텐츠 $Contents$와 콘텐츠의 암호화 키 K_C를 수신한다.
2. 콘텐츠의 분할된 암호화 작업을 위해 콘텐츠를 일정한 크기로 분할하고 그 정보를 유지하기 위해 인덱스 테이블을 생성한다.
3. 암호화 키 K_C를 이용하여 각각의 분할된 영역 C_i을 암호화하여 $E_i = E(C_i, K_C)$를 생성한다. 만일 단계 2에서 콘텐츠가 n개로 분할되었을 경우 E_i는 n개가 만들어진다.
4. 분할되어 암호화된 각 콘텐츠인 E_i를 결합하여 암호화된 전체 콘텐츠인 $Contents_{Temp}$를 생성하여 라이선스 서버로 전송한다.

(Procedure 5)의 과정이 완료되면 라이선스 서버에서 라이선스를 생성하여 콘텐츠 서버에서 전송받은 암호화된 콘텐츠와 결합하여 완성된 콘텐츠를 만들게 된다. (그림 3)은 (Procedure 5)에서 해당 콘텐츠가 일정한 크기로 분할되어 각각 암호화된 후에 결합되는 과정을 보여준다. 그림에서 전체 콘텐츠가 $C_1 \sim C_4$의 4개 영역으로 분할되어 각 영역이 별도로 암호화되고 인덱스

테이블을 통하여 그 정보가 관리되는 과정을 보여준다. 인덱스 테이블은 분할된 영역의 시작주소, 크기 및 페이지 번호 등의 정보를 저장한다. 콘텐츠가 분할되어 암호화되는 이유는 상대적으로 컴퓨팅 성능과 주기억장치의 용량이 부족한 휴대용 기기에서 다양한 용량의 콘텐츠를 효율적으로 관리하기 위해서이며 [14]에서 제안한 부분암호화 아이디어를 변경하여 적용하였다.



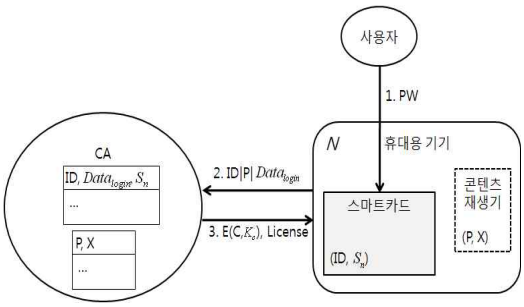
(그림 3) 암호화된 콘텐츠

스마트카드 식별값 S_n은 3절에서 사용자 등록과정을 수행하기 전의 선행 과정인 스마트카드 등록과정에서 CA가 스마트카드에게 부여하는 값으로 해당 스마트카드와 CA의 데이터베이스에 저장되어 있다. (Procedure 6)은 (Procedure 5)에서 전송한 암호화된 콘텐츠인 $Contents_{Temp}$를 라이선스 서버가 전송받아 라이선스를 포함한 완전한 콘텐츠를 제작하는 과정을 보여준다.

(Procedure 4)에서 사용자로부터 받은 난스 N을 (Procedure 6)의 5번째 단계에서 1을 더한 후 라이선스에 포함하여 전송한다. (Procedure 3)부터 (Procedure 6)까지의 진행과정은 인증과정, 콘텐츠 암호화, 라이선스 생성 과정을 모두 포함하고 있다. 이중에서 사용자의 휴대용기기와 CA 간에 교환되는 메시지 전송에 대한 프로토콜을 요약하면 (그림 4)와 같다. 사용자는 콘텐츠를 구입하기 위해 패스워드(PW)를 입력하고, 휴대용기기는 PW를 스마트카드에 전달하여 ID와 $Data_{login}$을 얻어 CA에 인증을 요청하는 메시지를 보낸다. 최종적으로 배포권자는 비밀키 K_c로 암호화된 콘텐츠를, CA는 비밀키 K_c가 암호화된 라이선스를 사용자의 휴대용 기기로 전송한다.

【Procedure 6 : 라이선스 제작 및 콘텐츠 완성】

1. CA로부터 콘텐츠의 암호화 키 K_C를 수신한다.
2. 로그인 서버로부터 사용자의 정보인 ID, PW, S_n, X를 수신한다.
3. $K_{LE} = h(ID|PW|S_n)$를 생성한다.
4. $K_L = h(K_{LE}|X)$를 생성한다.
5. $License = E(K_C|(N+1), K_L)$를 생성한다.
6. 콘텐츠 서버로부터 암호화된 콘텐츠인 $Contents_{Temp}$를 수신한다.
7. 콘텐츠와 라이선스를 결합하여 최종 완성된 $Contents_{Complete} = License \mid Contents_{Temp}$를 생성한다.
8. $Contents_{Complete}$를 사용자의 휴대용기기에 전송한다.



(그림 4) CA와 휴대용 기기간의 메시지 전송 과정 요약

3.2.5 콘텐츠 재생 과정

다음은 사용자의 휴대용기기에서 콘텐츠의 재생 과정을 설명한다. 앞 절에서 설명한 것과 같이 사용자는 먼저 배포권자의 웹사이트를 통하여 콘텐츠를 요청하기 전에 CA에 스마트카드를 등록하고 인증을 완료한다. 다음에 사용자는 콘텐츠를 요청할 때 결재기관에 결재를 완료한 후에 CA 내의 라이선스 서버로부터 자신의 휴대용기기에 암호화된 콘텐츠를 다운로드 받는다. 이후에 사용자는 자신의 휴대용기기에서 콘텐츠를 재생하고자 할 때 복호화 과정을 수행하게 된다. 만일 사용자가 전체 콘텐츠를 순서대로 재생을 원할 경우 전체를 복호화 할 수 있으며, 임의의 부분을 원할 경우 해당 부분의 인덱스를

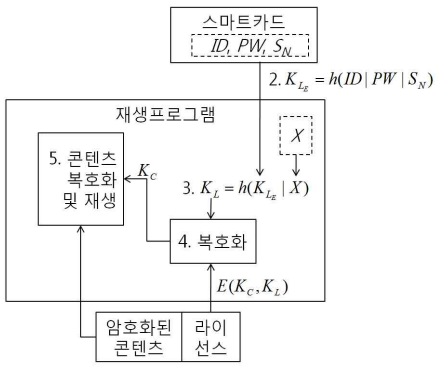
참조하여 필요한 부분만을 복호화하여 콘텐츠를 사용할 수 있다.

(Procedure 7)과 (그림 5)는 사용자가 자신의 휴대기기에 다운로드 되어 저장된 콘텐츠의 복호화 및 재생과정을 보여준다. 휴대용기기 내의 콘텐츠 재생기는 (Procedure 6)의 단계 3과 4를 스마트카드를 통해서 수행하여 복호화키 K_L을 얻고, 이를 라이선스에 적용하여 K_c와 N+1을 복호화한다. N+1이 확인되면 상대방이 정당한 CA라는 것을 인증한다.

【Procedure 7 : 휴대용기기에서 콘텐츠 복호화 및 재생과정】

1. 휴대용기기 내에 있는 재생프로그램은 사용자가 배포권자로부터 다운로드한 콘텐츠로부터 인덱스 테이블을 추출한다.
2. 사용자는 자신의 스마트카드를 휴대용기기에 연결하고 스마트카드 소유자임을 입증하는 PIN을 사용하여 스마트카드로부터 $K_{LE} = h(ID/PW/S_n)$를 얻어 재생 프로그램에 보낸다. 여기서 ID, PW, 그리고 S_n은 스마트카드에 저장된 값들이다.
3. 재생프로그램은 스마트카드로부터 받은 값 K_{LE}와 자신이 가진 값 X를 이용하여 $K_L = h(K_{LE}/X)$를 계산한다.
4. 재생프로그램은 CA로부터 전송받은 콘텐츠의 라이선스인 $E(K_C|(N+1), K_L)$를 K_L로 복호화하여 키 K_c와 N+1을 획득한다.
5. 재생프로그램은 $N+1$을 저장된 N과 비교하여 상대가 정당한 CA임을 확인한다.
6. 재생프로그램은 복호화 키 K_c를 이용하여 암호화되어 있는 콘텐츠를 복호화하여 재생한다.

(Procedure 7)의 2번에서 콘텐츠의 라이선스 복호화 키 생성과정에서 사용되는 값 중 S_n은 이미 설명한 것과 같이 사용자 등록과정을 수행하기 전에 얻어진 값을 의미한다. 사용자의 스마트카드 등록과정에서 CA가 스마트카드에게 부여하는 고유의 식별 값으로 스마트카드 내에 저장되어 있다. K_{LE}는 (Procedure 3)의 $Data_{Login}$과 차이를 두기 위해서 PW 값에 대해 해시 함수를 적용시키지 않았다. X는 재생프로그램의 비밀키로 스마트카드 내에 저장되어 있는 ID, PW, S_n 값을 이용하여 생성된 K_{LE} 값과 해시 연산을 수행하여 K_L을 생성한다. 이 K_L 값은 라이선스의 복호화 키로 사용된다.



(그림 5) 휴대용기기에서 콘텐츠 복호화 및 재생과정

4. 이전 모델과 제안된 모델과의 비교

본 논문에서는 스마트카드를 기반으로 하는 새로운 형태의 디지털 저작권 관리 시스템을 제안하였다. 또한 본 논문에서는 WCDRM[3] 모델을 기본으로 하여 더 강화된 보안과 더 명확한 프로토콜을 갖는 시스템을 설계하였다. DRM에 관한 다수의 연구가 진행되었으나 대부분 스트리밍 환경을 기반으로 하고 있어 본 연구와 가장 적합한 WCDRM에 대해서만 비교한다. <표 1>은 제안된 모델과 기존 모델에 대해 복제 공격의 관점에서 비교한 결과를 보여준다.

<표 1> 제안된 시스템과의 비교

구분	WCDRM[3]	제안시스템
인증방식	핑거프린트	스마트카드
타 휴대용기기에서 다운로드 콘텐츠 사용	불가	가능
복호화 키에 대한 공격	가능	불가
콘텐츠 유출 공격	완전	부분
암호화 횟수	2회	1회
사용자의 공격 (불법복제)	가능	불가

사용자 인증을 위해 제안된 시스템은 스마트카드를 사용하고 WCDRM은 핑거프린트 방식을

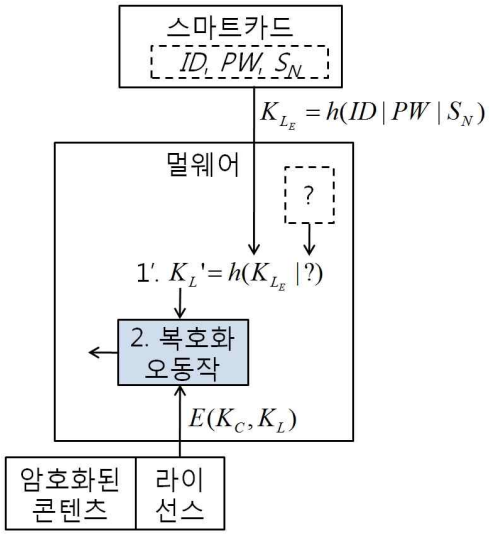
사용한다. 핑거프린트 방식은 사용자 휴대용기기의 기본 정보를 사용하기 때문에 이 정보가 유출될 경우 인증과정이 공격자에게 노출될 가능성이 높다. 반면에 스마트카드는 사용자의 고유정보가 카드 내에 저장되기 때문에 핑거프린트 방식보다 훨씬 안전하다고 할 수 있다.

사용자는 정상적인 인증과정을 거쳐 암호화된 콘텐츠를 자신의 휴대용기기에 다운로드 할 수 있다. 본 시스템의 경우 스마트카드를 사용하기 때문에 다운로드한 콘텐츠를 같은 재생프로그램이 설치된 다른 장치에 옮겨 활용할 수 있는 편의성을 제공한다. 제안된 시스템에서 다운로드한 콘텐츠가 다른 장치에 저장되어 있더라도 스마트카드가 없이는 라이선스 복호화가 불가능하기 때문에 스마트카드에 의해 해당 콘텐츠의 사용여부가 귀속된다. WCDRM 모델은 핑거프린트 방식을 사용하기 때문에 다른 장치에 콘텐츠를 옮겨 사용하는 것이 원천적으로 가능하지 않다.

복호화 키에 대한 공격 측면을 고려할 경우 WCDRM 모델은 휴대용기기의 핑거프린트를 사용하여 복호화 키를 생성하기 때문에 커널이 공격을 받을 경우 해당 정보가 노출될 가능성이 존재한다. 반면 제안된 시스템은 라이선스의 복호화 키를 생성하는 정보가 스마트카드에 저장되어 있기 때문에 커널이 공격을 받더라도 복호화 키의 정보가 유출되지 않는다. 이러한 측면에서 제안된 시스템은 WCDRM 모델과 비교하여 훨씬 강한 보안성을 가지게 된다. 또한 콘텐츠의 최종 복호화키 K_c는 콘텐츠 재생 프로그램에서만 생성되고 사용이 끝난 후 메모리에서 제거되기 때문에 외부에 노출되지 않는다.

다음은 DRM 처리가 되어있지 않은 콘텐츠, 즉 각 부분으로 분할되어 암호화되어있지 않은 콘텐츠를 휴대용기기 내에 다운로드 받아서 재생을 요청하는 경우를 고려한다. 제안된 시스템에서 콘텐츠는 여러 부분으로 분할되어 암호화되어있으며, 이때 재생프로그램은 콘텐츠의 분할 암호화 여부 및 태그를 비교분석하여 DRM 처리가 되어있지 않은 콘텐츠인 경우는 재생프로그램에서 재생을 거부한다. 제안된 시스템에서 콘텐츠를 분할하여 복호화하는 이유는 완전한 데이터가 공격자에게 유출되는 것을 막기 위함이기도 하다. 콘텐츠를 두 개 이상의 여러 부분으로 나누어 암호화한 뒤 한 부분만 복호화하고 재생이 끝나면 바로 메모리에서 삭제함으로써 공격자가 온전한 데이터를 쉽게 얻을 수 없도록 하여 보안성을 강화하였다.

본 시스템에서 배포권자가 저작권자에 사용료를 지불한 후에 CA가 배포권자에게 요약 정보만을 보내고 후에 사용자의 콘텐츠 요청이 있을 경우 암호화된 콘텐츠를 전송한다. 이러한 방법을 사용하여 WCDRM 모델에서 같은 콘텐츠를 2회 암호화 하던 과정을 1회로 줄여 서버의 부담을 경감하였다.



(그림 6) 사용자의 불법복제 시도

DRM을 사용하는 시스템에서 가장 치명적인 공격의 하나로 예상되는 내부자에 의한 공격가능성에 대하여 살펴본다. 사용자가 의도적으로 복호화된 콘텐츠를 외부로 복사하려는 시도를 할 수 있다. (그림 6)에서 보인 것과 같이 보통 악성 프로그램 혹은 바이러스 등으로 알려진 멀웨어 (Malware)는 의도적으로 공격을 하기 위해 만들어진 프로그램을 말하고 여기서는 사용자의 불법복제 프로그램에 한정한다. 즉, 본 논문상에서 멀웨어는 사용자가 복호화된 콘텐츠를 시스템의 외부로 반출하기 위하여 시스템 내부로 다운로드한 프로그램을 뜻한다.

멀웨어로 일어날 수 있는 공격 중의 하나는 재생 프로그램처럼 동작하면서 시스템에 라이선스 및 콘텐츠의 복호화를 요청하여 시스템 내부

에서 복호화된 콘텐츠를 받아서 유출할 수 있다는 것이다. 재생 프로그램과 동등한 권한으로 라이선스의 복호화를 요청하므로 시스템은 재생 프로그램이 요청하는지 사용자의 불법복제 프로그램이 요청하는지 판단할 수가 없다. 여기서 사용자의 불법복제 프로그램을 이용한 공격은 내부자가 다른 휴대용기기에 복호화된 원본의 콘텐츠를 얻기 위하여 실행하는 공격으로 한정한다.

WCDRM 모델의 DRM은 워터마크 기반으로 설계되었기 때문에 자료의 복사여부를 판단할 수 없다고 관련연구에서 언급하였다. 특히 휴대용기기의 사용자가 공격자인 경우, 사용자가 라이선스의 복호화를 요청하여 콘텐츠를 얻는 것에 대하여 방어할 대책이 없다. 그러나 제안된 시스템에서 먼저 스마트카드에 비밀번호를 입력하여 내부의 함수에 대한 사용권한을 얻은 뒤 사용을 할 수 있으므로 사용자의 불법복제 프로그램의 공격에 안전하다고 생각할 수 있다. 반면에 내부자 공격에 의해 발생할 수 있는 불법복제로부터는 안전하다고 말할 수 없다. 내부자가 스마트카드의 비밀번호를 입력하여 스마트카드로부터 라이선스의 복호화 키를 얻을 수 있다. 따라서 완전히 복호화된 콘텐츠를 얻어서 복사할 수 있다.

제안된 시스템에서는 이러한 멀웨어에 의한 공격을 방어하기 위해서 3.2.3에서 설명한 휴대용기기 내의 재생프로그램의 비밀값 X를 이용하여 라이선스의 복호화 키를 생성하는 방법을 사용함으로써 방어가 가능하다. 라이선스의 복호화 키를 요청하는 과정을 수행할 때 스마트카드에서 얻을 수 있는 부분은 K_{LE}이다. 라이선스의 복호화키 K_L은 K_{LE}와 재생프로그램의 비밀값 X에 해시 연산을 수행함으로써 얻기 때문에 사용자의 불법복제 프로그램이 요청하여 얻을 수 있는 부분은 라이선스의 복호화 키가 아닌 라이선스의 복호화 키를 생성하는 일부의 정보이다. 멀웨어는 X값을 가지고 있지 않으며, 생성할 수도 없기 때문에 라이선스의 복호화 키를 생성할 수 없다(그림 6). 따라서 라이선스의 복호화가 불가능하게 되고 콘텐츠의 복호화도 불가능하다.

5. 결론 및 향후 연구

최근에 디지털 콘텐츠를 보호하기 위한 DRM 기술에 관련된 연구들이 광범위하게 진행되고 있다. 이러한 방법을 사용함으로써 디지털 콘텐츠의 저작권을 보호하고 디지털 콘텐츠의 불법 유통 및 복제를 방지하여 저작권자의 이익과 권리를 보호해 준다. 본 논문에서는 스마트카드를 기반으로 하는 인증 시스템을 사용하여 기존의 연구결과인 WCDRM 모델보다 보안 및 활용 측면에서 훨씬 강화된 새로운 시스템 모델을 제안하였다.

본 논문에서 제안한 모델은 기존의 WCDRM 모델에 비해 다음과 같이 강화되었다. 첫째, 사용자의 고유정보를 보안기능이 강화된 스마트카드에 저장함으로써 공격자가 고유정보를 알 수 없도록 하여 복제방지를 강화하였다. 둘째, 저작권자, 배포권자, 인증기관, 사용자 간의 프로토콜을 명확하게 하여 콘텐츠 암호화에 대한 서버의 부담을 줄였다. 셋째, 오프라인환경에서도 동작하며 스마트카드에 사용자의 고유정보를 저장하여 핵심적인 정보가 노출되는 것을 최소화하였다. 또한 등록과정에서 해시 알고리즘을 적용하여 휴대용기기내의 재생프로그램이 복제방지 여부를 판단하도록 함으로써 저작권자의 권리를 보장하였다. 또한 임의의 공격자에 대해 여러 가지 공격 매개변수에 대해 두 시스템을 비교하여 제안된 시스템이 우위에 있음을 보였다.

본 논문에서 제안한 DRM 모델은 사용자 인증을 위해 비밀키를 사용하는 관계로 서버 내부자 공격에 취약점을 보인다. 이의 보완을 위해 스마트카드에 공개키 인증서를 적용한 DRM 모델을 개발할 예정이다.

참 고 문 헌

[1] 저작권 보호협회,“2010 저작권 보호 연차보고서,” http://www.cleancopyright.or.kr/data/document/2010_data_mon0422.pdf, 2010.

[2] 최동현, 이병희, 김승주, 원동호, “DRM(Digital Rights Management) 기술,” 한국정보과학회, 정보과학회지, 제25권 제5호(통권 제216호) May 2007.

[3] Jiaming He, Hongbin Zhang, “Digital Right Management Model Based on Cryptography and Digital Wat

ermarking," December 2008 CSSE '08 : Proceedings of the 2008 International Conference on Computer Science and Software Engineering - Volume 03, December 2008.
[4] 박종용, Offline 환경에서 스마트카드를 이용한 복제 방지 기법에 관한 연구, 금오공과대학교 석사논문, 2010.
[5] "Microsoft DRM", http://www.microsoft.com/windows/windowsmedia/drm/default.aspx
[6] Hung-Min Sun, Chi-Fu Hung, Chien-Ming Chen, "An Improved Digital Rights Management System Based on Smart Cards," Digital EcoSystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES.
[7] 임영이, 이윤철, 강회일, 이동일, "스마트카드 시스템의 보안 기술," [ETRI]전자통신동향분석 제14권 제5호, June 2001.
[8] L. Hu, Y. Yang, X. Niu. "Improved remote user authentication scheme preserving anonymity," Fifth Annual Conference on Communication Network and Services Research, pp.323-328, 2007.
[9] S Kim, H Rhee, J Chun, D Lee, "Anonymous and Traceable Authentication Scheme using Smart Cards," International Conference on Information Security and Assurance, pp.162-165, April, 2008.
[10] M. L Das, A. Saxena, V. P Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, Vol.50, No. 2, pp. 629-631, May 2004.
[11] J. J Tardo, K. Alagappan, "SPX: Global Authentication Using Public Key Certificates," IEEE Symposium on Security and Privacy, pp.232-244, 1991.
[12] S. Bhatkar, D. C DuVarney, and R. Sekar, "Address Obfuscation: an Efficient Approach to Combat a Broad Range of Memory Error Exploits," 12th USENIX, pp.105-120, 2003.
[13] Announcing the Advanced Encryption Standard (AES) [S]. FIPS Publication 197.
[14] 유경인, 김민재, 이진영, 조성제, 김준모, "모바일 콘텐츠의 안전한 부분암호화 방법에 대한 연구," 한국컴퓨터종합학술대회 논문집, Vol.35, No.1(D), 2008.

박 종 용

2008년 : 금오공과대학교 컴퓨터공학부 공학사

2008년～현 재: 금오공과대학교 컴퓨터공학과 석사
관심분야 : 스마트카드, 컴퓨터시스템보안, 디지털저작권 등

김 영 학

1989년 : 서강대학교 전자계산학과 공학석사
1997년 : 서강대학교 전자계산학과 공학박사

1989년~1997년 : 해군사관학교 전산과학과 교수
1998년~1999년 : 여수대학교 멀티미디어학부 교수
2006년~2007년 : 미국 조지아텍 방문교수
1999년~현재 : 금오공과대학교 컴퓨터공학과 교수
관심분야 : 병렬 알고리즘, 임베디드시스템 등

최 태 영

1996년 : 포항공대 컴퓨터공학과 공학석사
2002년 : 포항공대 컴퓨터공학과 공학박사

2002년～현재 : 금오공과대학교 컴퓨터공학과 교수
2007년～2008년 : 미국 조지아텍 방문교수
관심분야 : 분산 및 병렬처리, 컴퓨터시스템 보안 등