멀티미디어 콘텐츠의 안전한 유통을 위한 안드로이드 폰에 기반을 둔 보안에 관한 연구

신승수*, 김용영**

A Study on Multi-Media Contents Security Using Android Phone for Safety Distribution

Seung-Soo Shin*, Yong-Young Kim**

요 약 본 논문에서는 기존 WCDRM(Watermark & Cryptography DRM) 모델과 스마트카드를 이용한 모델에서 제안한 방법의 문제점을 해결하기 위해 사용자의 최소한 정보를 이용한 인증과 멀티미디어 콘텐츠에 대한 암호화, DRM(Digital Right Management), 접근제어 등의 기술을 이용하여 사용자의 정보를 보호하고, 저작권자와 배포권자, 사용자의 권리를 보호하는 콘텐츠 유통 모델을 제안하였다. 제안한 시스템은 기존 방식의 단점을 해결하였을 뿐만 아니라 네 가지 유형의 위험, 즉 타 휴대기기에서 다운로드한 콘텐츠의 사용 여부와 복호화 키에 대한 공격, 콘텐츠 유출 공격, 불법 복제 등 내부자 공격 등을 모두 방어할 수 있다는 점에서 가장 안전한 방법으로 평가되었다.

주제어 : 디지털 콘텐츠, DRM, WCDRM, 스마트카드, 보안, 안드로이드 폰

Abstract This paper tries to solve the problems which previous methods have such as the WCDRM(Watermark and Cryptography DRM) and the model using smart card for protecting digital contents. This study provides a contents distribution model to protect the rights of author, distributor, and user as well as user's information by using technologies such as cryptography, DRM(Digital Right Management), access control, etc. The proposed system is evaluated as the most safety model compared with previous methods because it not only solves the problems which the previous methods have, but also protects four type of risks such as use of contents which other mobile devices download, the attack on the key to decode the message, the attack on leaking the contents, and the internal attack such as an illegal reproduction.

Key Words : Digital Contents, DRM, WCDRM, Smart Card, Security, Android Phone

1. 서론

스마트폰 시장이 확대함에 따라 스마트폰은 우리 생활의 일부로 자리 잡고 있다. 2009년 초기 스마트폰인 애플사의 아이폰(iPhone)이 국내에 도입되고 2010년에 구글의 안드로이드 OS를 기반으로 한 스마트폰이 대거 출시되면서 스마트폰 시장은 급속도로 성장하였으며, 2012년 2월말 현재 가입자 수가 2,479만 명에 도달하였다[5].

스마트폰 시장이 확대되고 수요가 급증하면서, 스마트폰 기기(device)의 가치뿐 아니라 스마트폰으로 이용이 가능한 멀티미디어 콘텐츠에 대한 가치에 대한 관심도 증대되어 왔다. 스마트폰을 통해 음악, 영화, 도서, 게임 등의 콘텐츠의 유통이 활발하게 이루어지 있으며, 관련 어플은 이러한 유통을 촉진시키고 있다. 하지만 콘텐츠 자체 데이터뿐 아니라 디지털 콘텐츠를 이용하는 사용자의 정보 유출 등과 관련된 보안상 문제점을 지닌 채 디지털 콘텐츠가 유통되고 있다.

유통 과정에서 디지털 콘텐츠를 보호하기 위해 DRM

*동명대학교 정보보호학과 부교수
**건국대학교 경영학과 조교수: 교신저자
논문접수: 2012년 6월 21일, 1차 수정을 거쳐, 심사완료: 2012년 7월 2일

(Digital Right Management, 디지털 저작권 관리) 기술에 대한 관심이 증대되고 있다. 이 방법을 이용할 경우 디지털 콘텐츠의 저작권을 보호하고 디지털 콘텐츠의 불법유통 및 복제를 방지함으로써 저작권자의 이익과 권리를 보호할 수 있다[9]. DRM는 일반적으로 “디지털 콘텐츠의 불법 유통과 복제를 방지하고, 적법한 사용자만 콘텐츠를 사용하게 하며, 과금 서비스 등을 통하여 디지털 콘텐츠 저작권을 관리하는 기술”로 정의할 수 있다[6].

Jiaming He 등은 디지털 콘텐츠의 암호화와 워터마크를 사용하여 콘텐츠를 보호하는 WCDRM(Watermark & Cryptography DRM) 모델을 제안하였다[10]. 이 모델의 특징은 콘텐츠를 등록할 때 CA(Certificate Authority, 인증기관)가 저작권자와 배포권자의 워터마크를 삽입하고 사용자의 라이선스 키를 생성하기 위해 휴대용기기의 핑거프린트와 같은 고유정보를 이용한다는 점이다.

하지만 Jiaming He 등이 제안한 모델은 추상적인 프로토콜 정의로 인증과정을 명확하게 설명하지 못하였으며, 동일한 콘텐츠에 대해 중복된 암호화 루틴을 수행하여 서버에 과중한 부담을 준다는 문제점이 있다. 또한 불법복제가 일어나는 여부를 파악할 수 없으며, 휴대용기기의 핑거프린트를 사용하여 라이선스 키를 생성하기 때문에 이 정보를 입수한 악의적 사용자에 의해 공격을 받을 가능성도 있다.

박종용 등[3],[4]은 Jiaming He 등이 제안한 방법의 문제점들을 개선하여 스마트카드를 사용하는 새로운 형태의 DRM 모델을 제안하였다. 새로운 형태의 DRM 모델은 스마트카드를 사용하기 때문에 휴대용 기기가 변경되거나 오프라인 환경에서도 활용 가능하다는 장점이 있다.

하지만 박종용 등이 제안한 방법은 스마트카드 기반의 모델이기 때문에, 몇 가지 문제점이 존재한다. 먼저 공격자는 통신과정에서 스마트카드의 메시지를 도청, 삭제 또는 수정할 수 있다. 공격자는 (i) 사용자의 스마트카드를 훔쳐서 그 안에 저장되어 있는 내용을 추출하거나 (ii) 사용자의 패스워드를 획득할 수 있다. (iii) 그러나 동시에 (i) 또는 (ii)을 수행할 수는 없다. (i)의 경우, Kocher 등[11]과 Messerges 등[12]은 전력 소비를 모니터링 함으로써 스마트카드 안에 저장된 모든 비밀 정보를 추출할 수 있음을 지적하였다. 따라서 스마트카드를 분실하면 그 안에 수록된 모든 정보는 노출될 수 있다. 또한 이 방식은 사용자의 고유정보를 스마트카드에 저장하기 때문에 스마트카드 분실 시 스마트카드를 재발급 받아야하는 불편함을 감수해야 하는 단점도 있다.

Jiamng He 등과 박종용 등이 제안한 방법의 문제점을 해결하기 위해 본 논문에서는 사용자의 최소한 정보를 이용한 인증과 멀티미디어 콘텐츠에 대한 암호화, DRM, 접근제어 등의 기술을 이용하여 사용자의 정보를 보호하고, 저작권자와 배포권자, 사용자의 권리를 보호하는 모델을 제안하고자 한다.

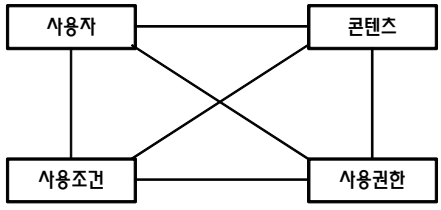
본 논문의 구성은 다음과 같다. 2장에서는 DRM에 대한 기존연구와 안드로이드 폰에 대하여 알아보고, 3장에서는 안드로이드 폰을 이용한 유통 모델을 제안한다. 4장에서는 제안한 모델과 기존 모델에 대하여 안전성을 비교·분석하고, 5장에서 결론을 제시하고 하고자 한다.

2. 관련연구

2.1 DRM 모델

DRM을 구성하는 가장 기본적인 네 가지 핵심 요소는 사용자(User), 콘텐츠(Content), 사용권한(Permission), 사용조건(Condition)이며, 이들 구성 요소들 간의 연관관계는 [그림 1]과 같다.

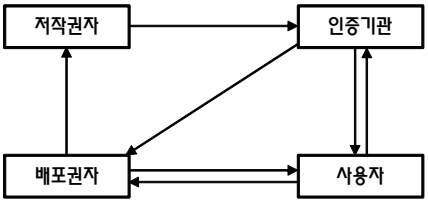
‘콘텐츠’는 지적자산의 가치가 있는 정보단위이며, 허가되지 않은 사용자로부터 보호해야 할 대상이다. ‘사용자’는 부여된 사용권한과 사용조건에 따라 콘텐츠를 이용할 주체이며, ‘사용권한’에 의해 콘텐츠의 이용 권리가 콘텐츠별로 정해진다. ‘사용조건’은 사용권한이 수행되기 위한 핵심 조건 및 제한 요소를 포함하고 있다. 이들 핵심 요소들 간의 연관성은 콘텐츠의 생명주기가 사라지지 않는 한 지속적으로 보호(Persistent protection)될 수 있어야 하며, 시스템적으로 처리 가능하도록 기술(Descriptive) 가능하여야 한다. 또한 명시된 권리에 따라서 콘텐츠가 통제(Rights Enforcement) 될 수 있어야 한다[1].



[그림 1] DRM의 구성 및 흐름

2.2 WCDRM 모델

WCDRM 모델은 2008년에 Jiaming He 등에 의해 제안되었으며 그 구성은 [그림 2]와 같다[10]. 구성요소는 콘텐츠의 암호화 및 라이선스 발급을 담당하는 CA(Certificate Authority)와 콘텐츠의 저작권자(Author), 그리고 저작권자로부터 판권을 구입하여 암호화된 콘텐츠를 CA로부터 사용자에게 전송하는 배포권자(Content Publisher)가 있다. 마지막으로 배포권자에게 콘텐츠를 요청하여 암호화된 콘텐츠를 다운로드하고, CA에 인증을 시도하여 라이선스를 다운로드한 뒤 복호화하여 콘텐츠를 재생하는 사용자(Customer)가 있다.



[그림 2] WCDRM의 구성 및 흐름

2.3 안드로이드 운영 시스템

안드로이드(Android)는 휴대 전화를 비롯한 휴대용 장치를 위한 운영 체제와 미들웨어 그리고 핵심 응용 프로그램을 포함하고 있는 소프트웨어 스택이다. 안드로이드는 개발자들이 자바 언어로 응용 프로그램을 작성할 수 있게 하였으며, 컴파일 된 바이트코드를 구동할 수 있는 런 타임 라이브러리를 제공한다. 또한 안드로이드 SDK(Software Development Kit, 소프트웨어 개발 도구)를 통해 응용 프로그램을 개발하기 위해 필요한 각종 도구들과 API(Application Program Interface, 응용 프로그램 인터페이스)를 제공한다.

안드로이드는 리눅스 커널 위에서 동작하며, 다양한 안드로이드 시스템 구성 요소에서 사용되는 C/C++ 라이브러리를 포함하고 있다. 안드로이드는 기존의 자바 가상 머신과는 다른 달빅 가상 머신(dalvik virtual machine)을 통해 자바로 작성된 응용 프로그램을 별도의 프로세스에서 실행하는 구조로 되어 있다.

2005년에 안드로이드사(社)를 구글에서 인수한 후 2007년 11월에 안드로이드 플랫폼을 휴대용 장치 운영 체제로서 무료 공개한다고 발표한 후 48개의 하드웨어, 소프트웨어, 통신 회사가 모여 만든 OHA(Open Handset Alliance, 개방형 휴대 전화 동맹)에서 공개 표준으로 개발하고 있다. 구글은 안드로이드의 모든 소스 코드를 오픈 소스 라이선스인 아파치 라이선스로 배포하고 있다 [7].

2.4 USIM과 IMEI

SIM(Subscriber Identity Module : 가입자 식별 모듈)이란 이동 전화기에서 사용할 수 있는 카드 형태의 모듈로써 가입자에게 인증과 요금 부과, 보안 기능 등의 다양한 서비스를 제공할 수 있도록 개인정보를 저장할 한 것이다. USIM(Universal SIM : 범용 가입자 식별 모듈)은 SIM보다 한 단계 진화한 방식으로, 현재 출시되는 핸드폰 단말기에 필수적으로 삽입되는 손톱만한 크기의 칩이다. USIM은 가입자 인증을 하는 SIM의 역할과 교통카드나 신용카드 등의 기능을 담을 수 있는 UICC(Universal IC Card : 범용 IC 카드)의 기능을 동시에 수행한다. UICC는 다양한 다중 애플리케이션의 보안 지원을 통해 모든 개인 정보 데이터의 무결성과 보안을 보장한다. USIM은 소형 CPU와 메모리로 구성된다. CPU는 암복호화 기능으로 사용자를 식별하고, 메모리는 부가서비스를 위한 저장 공간으로 이용된다. 메모리에는 신용카드나 교통카드, 멤버십카드 등의 기능을 넣을 수 있으며, 특히 OTA(Over The Air) 기술로 뱅킹이나 카드 서비스 승인만 받으면 별도의 칩을 발급받지 않고도 무선으로 서비스를 탑재할 수 있다[2].

USIM이 가지고 있는 정보 중의 하나인 IMSI(International Mobile Station Identity : 국제 이동국 식별번호)는 서비스 가입 시에 단말기에 할당되는 고유의 15자리 식별번호를 말한다. 이 번호는 국가 코드, 이동 네트워크 코드, 이동 가입자 식별번호 및 국가 이동 가입자 식별 번호로 구성된다. MCC(Mobile Country Code : 이동 국가 코드), MNC(Mobile Network Code : 이동 네트워크 코드)는 이동전화 가입자의 네트워크를 전 세계 어떠한 망에서든지 유일하게 식별할 수 있도록 해준다. 다른 네트워크가 조회를 통해 이동전화 가입자의 홈네트워크를 조회할 수 있다는 것이다. MSIN(Mobile Subscriber Identifier Number : 이동 가입자 식별 번호)은 MCC와 MNC가 주어진 경우, 이동전화 단말기를 식별하기 위해 사용된다.

2.5 멀티미디어 보안

일반적으로 멀티미디어란 사용자에게 정보를 제공하고 즐거움을 주는 미디어를 뜻한다. 초기 컴퓨터는 문자만 처리할 수 있었지만 입력과 출력의 기술 향상으로 음향, 영상으로 되어있는 다양한 매체를 처리할 수 있게 되었다. 이에 따라서 텍스트, 오디오, 스틸 이미지, 애니메이션, 비디오 등이 멀티미디어에 속하지만, 본 논문에서는 스마트폰의 안드로이드 어플 패키지까지 포함한다.

■ 디지털 워터마킹

디지털 워터마킹(Digital Watermarking)은 사진이나 동영상 같은 각종 디지털 데이터에 저작권 정보와 같은 비밀 정보를 삽입하여 관리하는 기술을 말한다. 그림이나 문자를 디지털 데이터에 삽입하며 원본 출처 및 정보를 추적할 수 있으며, 삽입된 워터마크는 재생이 어려운 형태로 보관된다. 디지털 워터마킹의 주요 기능은 저작권 보호, 위조나 변조 판별, 불법 복제 추적, 무단 복사의 방지, 사용자 제어 등의 기능이 있다[10].

■ 멀티미디어 암호화

멀티미디어 암호화의 경우는 서버가 사용자에게 멀티미디어를 전달할 때, 서버와 사용자를 제외하고는 누구든지 읽어볼 수 없도록 알고리즘을 이용하여 정보를 전달하는 과정이다. 본 논문에서는 사용자의 콘텐츠 요청을 받은 서버가 키를 생성하고 콘텐츠를 암호화하여 사용자에게 전송한다.

■ 접근 제어

접근 제어는 서버가 전송한 암호화된 콘텐츠의 복호화 키를 획득 할 수 있는 권한을 의미한다. 암호화된 콘텐츠를 얻었다고 하더라도, 그것을 복호화 할 수 있는 키를 소유하지 못하면 콘텐츠를 사용할 수 없다. 때문에 서버는 인증과정을 거친 사용자에게 콘텐츠의 라이선스를 생성 및 전송을 하게 되며, 사용자는 자신이 서버에 등록할 때 사용한 정보 값들로 라이선스를 복호화 함으로써, 콘텐츠 복호화 키를 얻을 수 있다.

본 논문에서 제안하는 모델의 목적은 서버(CA: Certificate Authority)와 저작권자, 배포권자, 사용자 간 올바른 인증 프로토콜을 확립하여, 콘텐츠를 암호화 하여 라이선스 및 인증 과정이 이루어 지지 않은 불법적인 사용자의 콘텐츠 접근을 막는 것이다. 그리고 워터마킹 기술을 이용하여 저작권자뿐만 아니라 배포권자와 사용자의 권리도 보호하는 것이다.

사용자는 안드로이드 운영체제를 탑재한 자신의 단말기를 이용하여 서버에 접근하고, 등록 및 인증 과정을 거치게 된다. 이때 서버는 사용자의 최소한의 정보만 요구하고, 사용자 단말기의 USIM값과 단말기 고유번호인 IMSI값을 이용하여 최초에 등록한 단말기에서만 인증이 가능하도록 설계하여 안정성을 확보한다. 그리고 사용자가 요구하는 콘텐츠에 대한 정보와 사용자의 고유정보를 이용하여 콘텐츠에 대한 라이선스를 생성하며, 생성된 라이선스와 함께 콘텐츠를 암호화하여 전송하기 때문에 제3의 공격자가 암호화된 콘텐츠를 얻는다 하더라고 복호화하는 것이 불가능하다. 또한 라이선스의 복호화 키는 사용자의 고유정보 값과 프로그램의 비밀키를 사용하여 생성함으로 다른 사용자 및 제3의 공격자가 라이선스 복호화 키를 생성할 수 없다.

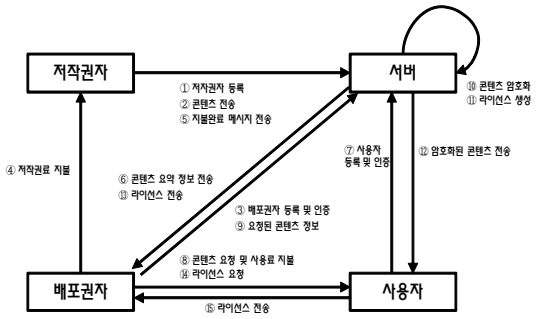
3. 제안 시스템 및 프로토콜

디지털 콘텐츠는 많은 저작자들의 창의성과 노력으로 만들어진다. 하지만, 디지털 데이터는 그 특성상 원본과 복사본의 구분이 불가능하기 때문에 디지털 콘텐츠 파일의 무단 복사 및 도용은 많은 저작자들의 저작 의욕을 저하시킬 뿐만 아니라 디지털 콘텐츠 사업에 심각한 위협을 초래하게 한다. 따라서 디지털 콘텐츠에 대한 불법 복제를 방지하기 위해서 저작권 정보를 생성하고 이를 디지털 콘텐츠 파일에 워터마킹하는 정보보호 기법의 적용은 필수적이다. 최근에는 디바이스 장치의 가치보다 멀티미디어 콘텐츠의 가치가 증대되고 있다. 하지만 이러한 콘텐츠의 제작과 판매 그리고 사용의 권리에 대한 인식은 부족한 실정이다. 저작자의 권리, 배포권자의 권리, 사용자의 권리가 보호 되어야만 멀티미디어 콘텐츠의 가치가 올바르게 확립 될 수 있다고 생각된다.

안드로이드 폰에서 멀티미디어 콘텐츠를 이용할 경우 데이터가 보호되지 않아 저작자들의 권리가 위협을 받을 수 있었다. 이러한 문제를 해결하기 위해 본 논문에서는 사용자 정보를 보호하며, 저작자들의 권리를 보호하는 유통 과정을 제안하고자 한다.

[그림 3]에서 저작권자, 배포권자, 서버, 사용자 등으로 구성된 개선된 WCDRM 모델을 통해 멀티미디어 콘텐츠

가 유통되는 과정을 볼 수 있다. 개선된 WCDRM 모델은 WCDRM 모델을 기본 구조로 사용하지만 안드로이드 폰에서의 고유정보 값을 사용한 인증 과정을 특징적으로 보여준다. 구체적으로 저작권자는 서버에 등록 및 인증 콘텐츠 전송 등의 과정을 거치고, 배포권자는 서버에 등록 및 인증 라이선스 요청 등의 과정을 거친다. 사용자는 서버에 등록 및 인증 콘텐츠 전송 및 라이선스를 전송 받게 된다.



[그림 3] 일반적 멀티미디어 콘텐츠 유통

3.1 시스템 파라미터

제안된 프로토콜에 사용할 파라미터는 <표 1>과 같이 정의된다.

〈표 1〉 표기

기호	설명
PN_U	사용자의 안드로이드 폰 번호
SSN_U	사용자의 고유번호
MNN_U	사용자의 이동통신사업자번호
MNO	이동통신사업자
SN_U	서버가 생성한 사용자의 난수
T	타임스탬프
ID_U	사용자의 아이디
PW_U	사용자의 패스워드
$h(\bullet)$	일방향 해시함수
StatementP	과금에 대한 송금 내역서

3.2 제안 프로토콜

본 절에서는 제안한 안드로이드 폰에서의 안전한 콘텐츠 유통에 대해 각 단계별 수행에 따른 프로토콜에 대해 설명한다. 프로토콜은 회원등록 및 로그인, 세션키 생성, 콘텐츠 등록 및 요약정보 전송, 콘텐츠의 암호화 및 라이선스 생성과정, 콘텐츠 전송 및 사용자의 콘텐츠 재생과정으로 구성된다.

3.2.1 회원등록 및 로그인

사용자는 마켓에서 프로그램을 다운 받은 후, 자신의 단말기에 설치를 하고 서비스를 받기위해서 회원등록을 하여야한다. 회원가입의 절차는 다음과 같다.

① 회원가입을 요청하는 사용자는 실제 안드로이드 폰 단말기의 사용자인지에 대한 인증을 요청한다. 사용자는

$$M_1 = \{PN_U, h(SSN_U), MNN_U\}$$

을 생성하고 M_1과 $h(M_1)$을 서버에게 전송한다.

② 서버는 사용자로부터 수신한 정보에 대한 무결성을 검증한다.

$$h(M_1) \cong h'(M_1)$$

무결성 검증이 이루어진 뒤, 서버는

$$M_2 = \{PN_U, h(SSN_U)\}$$

생성하고 M_2와 $h(M_2)$을 이동통신 사업자에게 전송한다.

③ 이동통신사업자는 서버에게 전송받은 정보와 저장하고 있는 정보를 대조한다.

$$h(SSN_U) \cong h'(SSN_U')$$

사용자의 정보가 맞으면 서버에게 응답 값을 전송한다.

④ 서버는 이동통신 사업자에게 받은 응답 값이 true이면 난수 SN_U 값을 생성하고 저장한다. SN_U는 사용자의 인증 값으로 프로그램의 일련번호로 사용된다. 서버는 SN_U값을 SMS를 이용하여 사용자에게 전송한다.

⑤ 사용자는 서버로부터 SMS로 SN_U을 전송받으면, 회원가입을 수행하게 된다. 사용자는 다음을 계산한다.

$$H_U = h(USIM \| IMEI \| PW_U),$$
$$r_u = h(PW_U) \oplus SN_U,$$
$$M_4 = \{ID_U, r_U, H_U\}$$

M_4와 $h(M_4)$을 함께 서버에게 전송한다.

⑥ 서버는 수신된 정보에 대하여 메시지의 무결성을 검증한다.

$$h(M_4) \cong h'(M_4)$$

무결성 검증이 이루어진 뒤 서버는 M_4와 생성하였던 SN_U와 함께 저장한다. M_4에서 추출한 H_U로 인하여 사용자는 회원가입 할 때 등록한 안드로

이드 폰 단말기에서만 서버로부터 서비스 받을 수 있다.

비밀번호 정보 r_U는 이전의 인증과정에서 SMS로 전송받은 SN_U와 $h(PW_U)$을 사용하는데 전송되는 과정에서 공격자가 r_U을 알아냈다고 하더라도 SN_U을 알 수 없기에 사용자의 $h(PW_U)$는 알아낼 수 없다.

사용자는 서비스를 제공받기 위해 서버에 접속하여야 하고, 접속을 위해서 서버에 로그인을 해야 한다. 사용자는 로그인을 위해 메시지를 생성하고 전송함으로써 서버에 접속을 시도하게 된다. 로그인 절차는 아래와 같다.

⑦ 사용자는 로그인 요청 메시지인

$$M_5 = \{ID_U, h(h(PW_U) \oplus T), T\}$$

을 생성하고 M_5와 $h(M_5)$을 서버에게 전송한다. 여기서, T값은 재전송 공격(Replay Attack)에 대비하여 사용하는 값이다.

⑧ 서버는 전송받은 메시지의 무결성을 검증하기 위하여 $h(M_5) \cong h'(M_5)$을 비교하여 검증한다. 무결성 검증을 완료한 뒤, M_5에서 사용자 정보를 검색하여 다음을 계산한다.

$$r_u = h(PW_U) \oplus SN_U,$$

$$r_u \oplus SN_U = h(PW_U),$$

그리고 다음을 검증한다.

$$h(h(PW_U) \oplus T) \cong h'(r_U \oplus SN_U \oplus T)$$

3.2.2 세션키 생성

사용자는 로그인이 완료된 후, 서비스를 제공 받기 위해 서버에 서비스 권한 요청을 한다. 서버는 사용자의 요청에 대한 응답을 하게 되면 아래와 같이 세션 키를 생성하게 된다.

① 사용자는 난수 R_U을 다음과 같이 생성한다.

$$R_U = \{SN_U \| H_U \| T\}$$

생성한 R_U는 SN_U와 XOR 연산을 수행하여

$$I_U = (R_U \oplus SN_U)$$

을 생성한다. I_U는 생성된 R_U을 보호하기 위한 값이며 통신상에서 공격자가 I_U을 취득해도 SN_U을 알 수 없기에 R_U도 알 수 없다. 사용자는 M_1와 $h(M_1)$을 함께 서버에게 전송한다.

$$M_1 = \{ID_U, h(R_U), I_U\}$$

서버는 수신한 정보에 대한 무결성 검증을 한다. M_1에서의 $h(R_U)$는 서버가 I_U로부터 R_U을 추출하였을 때 추출한 R_U'가 올바른 것인지를 검증하기 위한 값이다.

② M_1에서 ID_U을 이용하여 서버에 저장되어 있는 사용자 정보 ID_U', H_U', SN_U'을 검색한다.

③ 서버는 R_U'을 추출한다. 서버는

$$h(R_U') \cong h(R_U)$$

가 일치하는지 검증한다.

$$R_U' = I_U \oplus SN_U$$

④ 서버는 사용자 정보를 이용하여 난수 R_S을 생성한다.

$$R_S = \{SN_U \| H_U \| T'\},$$

$$I_S = R_S \oplus SN_U$$

I_S는 생성된 R_S을 보호하기 위한 값이다.

⑤ 서버는 $M_2 = \{h(R_S), I_S\}$을 사용자에게 전송한다. 여기서 $h(R_S)$는 사용자가 I_S로부터 R_S을 추출했을 때, 추출한 R_S'가 서버가 생성한 R_S와 일치하는지 검증하기 위한 값이다.

⑥ 사용자는 수신된 M_2로부터 R_S'을 추출하고, R_S'가 서버가 생성한 R_S와 일치하는지 검증하게 된다.

$$R_S' = I_S \oplus SN_U,\ h(R_S') \cong h(R_S)$$

⑦ 사용자는 세션키 K_{US}을 다음과 같이 생성한다.

$$K_{US} = R_U \oplus R_S$$

⑧ 서버도 동일한 방법으로 세션키 K_{SS}을 생성한다.

3.2.3 콘텐츠 등록 및 요약정보 전송

서버에 등록되어 있는 콘텐츠에 대한 판권은 얻기 위해 배포권자는 저작권자에게 콘텐츠에 대한 과금을 지불하고, 저작권자는 지불받은 과금에 대한 지불완료 메시지를 서버에게 전송함으로써, 배포권자는 콘텐츠에 대한 판권을 가지게 된다.

① 저작권자는 자신이 제작한 콘텐츠를 서버에 등록하기 위해 M_1과 $h(M_1)$을 서버에게 전송한다.

$$M_1 = \{ID_A, K_{AS}(C_A), CN_A\}$$

여기서, ID_A는 저작권자의 ID, K_{AS}는 저작권자와 서버의 세션키, C_A는 저작권자가 제작한 콘텐츠,

CN_A는 콘텐츠의 이름, $K_{AS}(C_A)$는 저작권자와 서버의 세션키로 암호화된 콘텐츠이다.

② 서버는 저작권자가 전송한 콘텐츠와 저작권자의 정보로 콘텐츠의 메타데이터(MD_{C_A})를 생성한다.

③ 배포권자는 콘텐츠에 대한 과금을 저작권자에게 지불하게 되고, $M_2 = \{ID_P, StatementP\}$을 생성하여 저작권자에게 $h(M_2)$을 같이 전송한다. StatementP는 배포권자가 지불한 과금에 대한 송금 내역서이다.

④ 저작권자는 자신과 배포권자의 거래가 완료되었음을 서버에게 알리기 위해, 서버에게 M_3와 $h(M_3)$을 전송한다.

$$M_3 = \{K_{AS}(ID_P, CN_A)\}$$

⑤ 서버는 저작권자로부터 전송받은 M_3로부터 추출한 CN_A로부터 콘텐츠의 메타 데이터인 MD_{CA}을 호출한다. 그리고 서버는 메타 데이터를 세션키로 암호화하여 배포권자에게 M_4와 $h(M_4)$을 전송한다.

$$M_4 = K_{PS}(MD_{C_A})$$

⑥ 배포권자는 수신된 정보를 복호화하여 MD_{C_A}를 추출하고, 추출한 메타데이터를 배포권자의 웹페이지에 게시함으로써 자신이 배포권을 가진 콘텐츠를 공개 할 수 있다.

3.2.4 사용자의 콘텐츠 요청

사용자의 콘텐츠 요청 과정은 사용자가 요구한 콘텐츠가 무엇인지를 서버에게 알리는 과정이기도 하지만, 사용자가 배포권자에게 요청하는 과정에서 주고받는 정보 값들에 의하여 서로의 부인방지를 위한 기능도 가지게 된다. 사용자의 콘텐츠 요청은 다음과 같다.

① 사용자는 M_1과 $h(M_1)$을 배포권자에게 전송한다.

$$M_1 = \{ID_U, CN_A, K_{US}(CN_A)\}$$

② 배포권자는 M_1에서 CN_A로부터 사용자가 요청한 콘텐츠의 이름을 알 수 있고, $K_{US}(CN_A)$을 저장한다. 배포권자는 사용자에게 M_2와 $h(M_2)$를 전송한다.

$$M_2 = K_{PS}(CN_A)$$

③ 배포권자는 서버에게 사용자가 요청한 콘텐츠를 알리기 위해 M_3과 $h(M_3)$을 전송한다.

$$M_3 = \{ID_U, ID_P, K_{US}(CN_A)\}$$

④ 서버는 세션키 K_{SS}로 복호화하여 사용자가 요청한 콘텐츠의 이름을 알고, 이것을 확인하기 위하여 M_4과 $h(M_4)$을 사용자에게 전송을 한다.

$$M_4 = K_{US}(CN_A)$$

⑤ 사용자는 세션키 K_{US}로 복호화하고, 사용자가 요청한 콘텐츠의 이름이 맞는지 확인 후, M_5과 $h(M_5)$을 서버에게 전송을 한다.

$$M_5 = K_{PS}(CN_A)$$

⑥ 서버는 M_4에서 $K_{US}(CN_A)$로 사용자가 요청한 콘텐츠의 이름을 확인하고, M_5에서 $K_{PS}(CN_A)$로 배포권자가 요청 받은 콘텐츠를 확인할 수 있게 된다.

3.2.5 콘텐츠의 암호화 및 라이선스 생성 과정

서버는 요청된 콘텐츠를 데이터베이스에서 불러와 암호화 및 라이선스를 생성하게 된다.

① 서버는 콘텐츠 암호화키인 K_C를 생성하여 콘텐츠를 암호화한다.

② 사용자의 아이디로부터 서버는 사용자의 정보를 검색하여 K_{K1}을 계산한다.

$$K_{L1} = h(ID_U \| h(PW_U) \| H_U)$$

③ 서버는 사용자의 프로그램 일련번호인 SN_U를 검색하여 K_{K2}을 계산한다.

$$K_{L2} = h(K_{L1} \| SN_U)$$

④ 서버는 콘텐츠 암호화키를 K_{K2}로 암호화하여 사용자 라이선스를 계산한다.

$$License_U = K_{L2}(K_C)$$

3.2.6 콘텐츠 전송 및 사용자의 콘텐츠 재생

서버는 사용자에게 암호화된 콘텐츠와 라이선스를 전송한다. 사용자는 서버로부터 전송받은 라이선스를 이용하여 콘텐츠를 복호화하고 재생할 수 있다. 콘텐츠 전송 및 재생은 아래와 같은 과정을 거친다.

① 서버는 사용자에게 암호화된 콘텐츠를 전송하기 위하여 M_1와 $h(M_1)$을 사용자에게 전송한다.

$$M_1 = \{K_C(C), h(K_C(C))\}$$

② 서버는 사용자의 라이선스 정보를 M_2와 $h(M_2)$을 배포권자에게 전송한다.

$$M_2 = \{License_U, K_{L1}\}$$

이때 배포권자가 K_{L1}을 알더라도 $License_U$로부터 K_C을 추출 할 수 없기 때문에 안전하다.

③ 사용자는 배포권자에게 라이선스를 요청하기 위하여 M_3와 $h(M_3)$을 배포권자에게 전송한다.

$$M_3 = \{ID_U, K_{US}(ID_U)\}$$

이때, $K_{US}(ID_U)$ 는 이후 사용자의 부인방지를 위하여 배포권자가 가지고 있는 정보 값이다.

④ 배포권자는 서버로 부터 전송받은 M_2을 사용자에게 전송한다.

⑤ M_2을 전송받은 사용자는 K_{L2}을 생성하여 K_C를 계산할 수 있다. K_C을 이용하여 콘텐츠를 복호화하고 콘텐츠를 재생한다.

$$K_{L2} = h(K_{L1} \| SN_U),$$
$$K_C = K_{L2}(License_U)$$

4. 제안한 모델과 비교

본 논문에서는 안드로이드 폰을 기반으로 하는 새로운 형태의 디지털 저작권 관리 시스템을 제안하였다. 또한 본 논문에서는 WCDRM[10]과 박종용[4]의 모델을 기본으로 보안이 강화된 시스템을 설계하였다. 제안한 모델과 기존의 모델에 대해 비교·평가한 결과를 [표 2]에 제시 하였다.

〈표 2〉 제안된 시스템과의 비교

구분	WCDRM[10]	박종용[4]	제안 시스템
인증방식	핑거프린트	스마트카드	안드로이드 폰
타 휴대기기에서 다운로드 콘텐츠 사용	불가	가능	불가
복호화 키에 대한 공격	가능	불가	불가
콘텐츠 유출 공격	완전	부분	불가
내부자의 공격 (불법복제)	가능	불가	불가

먼저 인증방식에 있어서 WCDRM은 핑거프린트, 박종용 등은 스마트카드, 본 연구에서 제안한 방식은 안드로이드 폰을 이용하는 데 차이가 있다. 이로 인해 각 방식은 네 가지 유형의 위험, 즉 타 휴대기기에서 다운로드한 콘텐츠의 사용 여부와 복호화 키에 대한 공격, 콘텐츠 유출 공격, 불법 복제 등 내부자 공격 등을 방어할 수 있는지 여부에 있어서도 차이가 발생한다.

WCDRM 모델은 핑거프린트 방식을 사용하기 때문에 다른 장치에 콘텐츠를 옮겨 사용하는 것이 원천적으로 가능하지 않다. 하지만 기본 정보가 유출될 경우 인증과정이 공격자에게 노출될 가능성이 높다. 또한 휴대기기의 핑거프린트를 사용하여 복호화 키를 생성하기 때문에 커널 공격을 받을 경우 해당 정보가 노출될 가능성이 존재한다. 이러한 이유로 콘텐츠 유출 공격에도 완전히 노출될 수 있으며, 불법복제 등 내부자의 공격도 가능하다는 단점이 있다.

스마트카드를 이용하는 박종용 등이 제안한 방식은 핑거프린트 방식보다 상대적으로 안전하다. 스마트카드는 사용자의 고유정보가 카드 내에 저장되기 때문에 타 휴대기기에서 다운로드한 콘텐츠를 사용할 있다. 특히 라이선스의 복호화 키를 생성하는 정보가 스마트카드에 저장되어 있기 때문에 커널이 공격을 받더라도 복호화 키의 정보가 유출되지 않는다. 또한 불법복제 등 내부자의 공격을 효과적으로 방어할 수 있는 장점이 있다.

하지만 박종용 등이 제안한 시스템은 스마트카드 안에 저장된 비밀 정보를 전력 소비를 모니터링 함으로써 추출할 수 있다. 따라서 카드를 분실하면 카드안의 모든 정보는 노출된다. 또한 이 방식은 사용자의 고유정보를 스마트카드에 저장하기 때문에 스마트카드 분실 시 스마트카드를 재발급 받아야하는 불편함이 있다.

또한 복호화 키에 대한 공격 측면에 있어서 박종용 등이 제안한 방식은 스마트카드 사용 시 공격자는 통신과정에서 메시지를 도청, 삭제 또는 수정할 수 있다. Kocher 등과 Messerges 등에 의해 제안한 방식으로 스마트카드 안에 있는 모든 정보를 알아 낼 수 있다는 단점이 존재한다.

제안한 시스템은 기존 방식의 단점을 해결하였을 뿐만 아니라 네 가지 유형의 위험 모두 방어할 수 있다는 점에서 상대적으로 가장 우수한 방법으로 평가될 수 있다.

5. 결 론

본 논문에서는 기존의 모델인 WCDRM 모델과 스마

트카드를 이용한 모델에서 보안 측면의 단점을 보완하기 위해 사용자의 최소한의 정보를 이용한 인증과 멀티미디어 콘텐츠에 대한 암호화, DRM, 접근제어 등의 기술을 이용하여 사용자의 정보를 보호하고 저작권자, 배포권자와 사용자의 권리를 보호하는 콘텐츠 유통 모델을 제안하였다.

제안한 모델은 콘텐츠 저작자의 저작권을 보호하고, 배포권자와 사용자들이 안드로이드 폰을 이용하여 편리하게 사용할 수 있는 멀티미디어 보안 유통 구조를 제시하였다. 이러한 멀티미디어 보안 유통 모델이 게임, 음악, 동영상 등 디지털 콘텐츠를 유통하는 다양한 분야에서 활용될 수 있다 생각된다.

참 고 문 헌

[1] 강호갑. (2004), “DRM 최신 국제표준 기술사향 분석 및 세계 유명제품 동향과 전망에 관한 연구”, 소프트웨어진흥원.

[2] 김주용・장재열・이병관. (2005), “SIM/USIM의 표준화 동향에 관한 연구”, 한국정보보호학회지, 제15권, 제3호, pp.48-60.

[3] 박종용. (2010), “Offline 환경에서 스마트카드를 이용한 복제방지 기법에 관한 연구”, 금오공과대학교 석사논문.

[4] 박종용・김영학・최태영. (2011), “스마트카드 기반의 강한 보안을 갖는 DRM 모델의 설계 및 평가”, 디지털콘텐츠논문지, 제12권, 제2호, pp.165-176.

[5] 방송통신위원회 통계자료. (2012. 3. 20) http://www.kcc.go.kr/user.do?mode=view&page=P02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=33497.

[6] 오원근. (2005), “DRM 표준화 및 평가 기술”, 전자통신동향 분석, 제20권, 제4호.

[7] 위키피디아, http://www.wikipedia.org/

[8] 정성환・이문호, “오픈소스 CxImage를 이용한 Visual C++ 디지털 영상처리”, 홍릉과학 출판사.

[9] 최동현・이병희・김승주・원동호. (2007), “DRM(Digital Rights Management) 기술”, 한국정보과학회, 정보과학회지, 제25권, 제5호.

[10] Jiaming He・Hongbin Zhang. (2008), "Digital Right Management Model Based on Cryptography and Digital Watermarking," December 2008, Proceed ings of the 2008 International Conference on Computer Science and Software Engineering (CSSE) Volume 03.

[11] P. Kocher, J. Haffe, B. Jun. (1999), "Differential Power Analysis," Proceedings of Advances in Cryptology(CRYPTO 99), pp.388-398.

[12] T. S. Messerges, E. A. Dabbish, R. H. Sloan. (2002), “Examining Smart Cards Security under the Threat of Power Analysis,” IEEE Transactions on Computers, 51(5), pp.541-552.

신 승 수

・2001년 : 충북대학교 수학과 (이학박사)
・2004년 : 충북대학교 컴퓨터공학과 (공학박사)
・2005년 ~ 현재 : 동명대학교 정보보호학과 부교수
・관심분야 : 네트워크보안, USN, 스마트카드. 암호이론, 정보보호
・E-Mail : shinss@tu.ac.kr

김 용 영

・2007년 : 서울대학교 대학원 경영학과(경영학박사)
・2007년 ~ 2009년 : 미국 Temple University 박사후연구원
・2010년 : 경북대학교 초빙교수
・2011년 ~ 현재 : 건국대학교 경영학과 조교수
・관심분야 : 개인정보보호, 스마트워크, u-비즈니스
・E-Mail: kyyoung@kku.ac.kr