안드로이드 폰을 이용한 멀티미디어 콘텐츠 보안에 관한 연구

신승수
동명대학교 정보보호학과

A Study on Multi-Media Contents Security Using Android Phone

Seung-Soo Shin
Dept. of Information Security, College of Information & Communication

요 약 본 논문에서는 기존 WCDRM(Watermark & Criptography 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** : 디지털콘텐츠, 저작권보호, 광대역코드분할, 스마트그리드, 보안, 안드로이드 폰

Abstract 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

초기 인터넷 연구의 대부분은 네트워크 인프라 즉, 데이터 링크, 네트워크, 트랜스포트 계층에 집중되었다. 그러나 웹, 스트리밍 등의 새로운 대표적 응용분야가 발생하고, 이에 대한 수요가 기하급수적으로 증가함에 따라 인터넷 인프라는 한계에 다다랐다. 인터넷 인프라의 확충은 기본적으로 고비용을 요구하기 때문에 연구자들은 애플리케이션 계층에서 해결을 시도하였다. 이로 인해 나온 기술이 콘텐츠 네트워킹 기술이다. 기존 연구들이 네트워크 대역폭 증가, 전송의 효율화에 중점을 두었다

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 2011년 11월 25일 수정일 2012년 2월 1일 게재확정일 2012년 2월 26일

면, 콘텐츠 네트워킹 기술은 네트워크에 지능을 부여한다. 사용자와 보다 인접한 위치에 콘텐츠를 준비하고, 사용자에게 가장 인접한 위치에 콘텐츠로 안내함으로써 보다 고품질의 콘텐츠 서비스가 가능하도록 한다.

콘텐츠 네트워킹의 가장 대표적인 기술은 CDN(Contents Delivery Network)이다. CDN은 콘텐츠를 사용자와 보다 인접한 위치로 이동시켜 네트워크상에서 콘텐츠 전송 비율을 줄인다. 뿐만 아니라, CDN은 지능적 전송과 체계적 관리를 부여함으로써 관리자가 한 지점에서 전체 콘텐츠 전송을 완벽하게 제어할 수 있도록 한다[1].

그러나 무선인터넷이 발전함에 따라서 콘텐츠 네트워킹 기술도 많은 발전을 이루었다. 최근 들어 스마트폰은 우리 생활에 있어서 없어서는 안 될 중요한 요소로 자리잡게 되었다.

국내 스마트폰 가입자 및 와이파이망 구축 현황

업 체	가입자(점유율)	스마트폰가입자	와이파이존
SK텔레콤	2544만명(50.7%)	285만명(11.2%)	1만4000개
KT	1583만명(31.5%)	200만명(12.6%)	4만개
LG유플러스	893만명(17.8%)	37만명(4.1%)	1만6000개
합 계	5020만명(100%)	522만명(10.3%)	7만개

※2010년 10월말 기준 (자료 : 각 업체)

[Fig. 1] Domestic smart-phone subscribers and construction

스마트폰은 기존 모바일의 전화, 문자메시지 기능을 포함해 다양한 콘텐츠 제공한다. 모바일 인터넷을 통한 정보 검색 및 GPS 기능, 사진, 음악, 동영상의 멀티미디어 서비스, 게임, 이메일, 일정관리, 인터넷 뱅킹, 증권, 금융결제, 전자 지갑 등이 스마트폰으로 이용 가능하다[2].

스마트폰의 모바일 인터넷을 통한 다양한 서비스는 사용자에게 편리함을 제공하고 있지만 개인 혹은 기업의 민감한 정보를 담고 있으므로 다양한 프라이버시 공격에 노출될 가능성이 높다.

인터넷이 유선에서 무선으로 급속하게 발전함으로 Jiaming He[3] 등은 디지털 콘텐츠의 저작권을 보호하고 디지털 콘텐츠의 불법유통 및 복제를 방지함으로써 저작자의 이익과 권리를 보호할 수 있는 방법으로 디지털 콘텐츠의 암호화와 워터마크를 사용하여 콘텐츠를 보호하는 WCDRM(Watermark & Cryptography DRM) 모델을 제안하였다. Jiaming He 등이 제안한 방법을 사용함으로써 저작권 분쟁이 일어났을 때 내부에 삽입된 워터마크와 암호화된 콘텐츠를 이용하여 저작자의 이익과 불법복제를 보호할 수 있다.

박종용 등[4]은 다음과 같은 문제를 제시하였다. 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 갖는다.

박종용 등이 제안한 모델은 Jiaming He 등이 제안한 방법을 근간으로 하나 다음과 같은 차이점을 갖는다. 첫째, 사용자의 고유정보를 보안기능이 강화된 스마트카드에 저장함으로서 공격자가 고유정보를 알 수 없도록 하여 복제방지를 강화한다. 둘째, 저작자, 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 저작자의 권리를 보장한다. 이러한 방법을 통하여 시스템이 공격받더라도 스마트카드 내의 정보를 보호하여 보다 신뢰성을 갖는 콘텐츠 관리기법을 제시한다.

본 논문에서는 스마트폰에서 사용자의 정보를 최소한으로 이용하여 사용자를 인증할 수 있는 인증 프로토콜과 멀티미디어 콘텐츠를 이용하는 사용자뿐만 아니라 배포권자와 저작권자의 권리를 보호할 수 있는 시스템을 설계하고 구현한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존연구에 대하여 알아보고, 3장에서는 안드로이드 폰을 이용한 사용자 인증 시스템을 구현하고 분석한다. 4장에서 결론을 맺는다.

2. 관련연구

2.1 WCDRM 모델

WCDRM 모델은 2008년에 Jiaming He[3]등에 의해 제안되었으며 그 구성요소는 콘텐츠의 암호화 및 라이선스 발급을 담당하는 CA와 콘텐츠의 저작자(Author), 그리고 저작자로부터 판권을 구입하여 암호화된 콘텐츠를 CA로부터 사용자에게 전송하는 배포권자(Contents

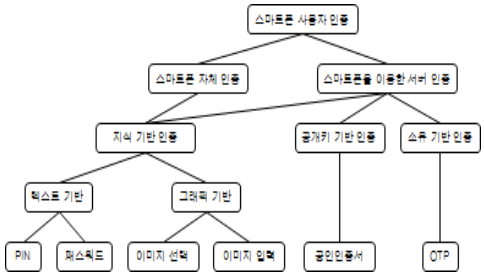
Publisher)가 있다. 마지막으로 배포권자에게 콘텐츠를 요청하여 암호화된 콘텐츠를 다운로드하고, CA에 인증을 시도하여 라이선스를 다운로드한 뒤 복호화하여 콘텐츠를 재생하는 사용자(Customer)가 있다.

2.2 스마트카드 인증 기반 모델

Jiaming He등[2]에 의해 제안된 모델을 바탕으로 스마트카드를 사용한 새로운 DRM 시스템을 박종용 등은 제안하였다. 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. 박종용 등[4]은 Jiaming He 등[3]이 제안한 WCDRM 모델을 기본 구조로 사용하나 스마트카드를 사용한 인증과정을 도입한다. WCDRM 모델에서 불명확하게 추상적으로 정의된 콘텐츠의 인증 과정을 구체적으로 정의하였다. 박종용 등이 제안한 모델은 다음과 같은 특징을 갖는다. 첫째, 사용자의 고유정보를 보안기능이 강화된 스마트카드에 저장함으로서 공격자가 고유정보를 알 수 없도록 하여 복제방지를 강화한다. 둘째, 저작자, 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.

2.3 스마트폰 사용자 인증

스마트폰 사용자 인증 기법은 크게 지식 기반 인증, 소유 기반 인증 및 이 둘을 동시에 이용하는 공개키 기반 인증 기법으로 분류 될 수 있다. 지식 기반 인증의 텍스트 기반으로는 PIN, 패스워드를 사용하는 인증 기법이 있으며, 그래픽 기반으로는 패스페이스[5]와 같은 이미지 선택 방식과 패턴 락과 같은 이미지 선택 방식과 패턴 락과 같은 이미지 입력 방식이 있다. 소유 기반 인증 기법으로는 OTP를 사용하는 기법과 공인 인증서와 같이 공개키 암호와 전자서명을 이용하는 인증 기법이 있다. 스마트폰을 이용한 인증은 텍스트 기반 인증 기법의 PIN이나 텍스트 패스워드가 가장 널리 사용되고 있다[6]. 다음은 스마트폰 사용자 인증 분류이다.



[Fig. 2] Classification user authentication

3. 스마트폰 사용자 인증 기반 모델

본 장에서는 사용자의 최소한의 정보로 인증이 가능한 스마트폰 사용자 인증 모델을 제시하고, 이를 통해 사용자의 인증을 강화하며, 저작자와 배포권자, 사용자의 권리를 보호한다.

3.1 사용자 인증 모델

최근 디지털콘텐츠 시장의 성장과 함께 모바일 환경에서 콘텐츠 이용자들이 빈번히 발생하고 있으며, 스마트폰상의 다양한 서비스가가 급증하고 있어, 모바일 환경에서의 보안관련 문제들이 이슈화 되고 있다. 이에 따라서 스마트폰 사용자 인증이 중요하다. 스마트폰 인증은 스마트폰 자체 인증과 스마트폰을 이용한 서버 인증으로 나눌 수 있다. 스마트폰 인증은 스마트폰 혹은 애플리케이션을 이용하기 위해 사용자를 인증하는 것이다. 스마트폰을 이용한 서버 인증은 스마트폰을 이용해서 웹사이트 및 인터넷 뱅킹 등의 서버 인증을 받는 것이다.

다음은 스마트폰 기반의 멀티미디어 콘텐츠 유통에 관한 시퀀스이다.

① 저작권자 등록 : 저작권자는 자신을 인증하기 위하여 ID 및 PW, 고유정보를 서버에 등록한다.
② 콘텐츠 전송 : 저작권자는 저작권을 갖는 멀티미디어 콘텐츠를 서버에 전송한다.
③ 배포권자 등록 : 배포권자는 자신의 ID, PW와 고유정보를 서버에 등록한다.
④ 저작권료 지불 : 배포권자는 서버에서 콘텐츠를 검색한 후 콘텐츠에 대한 저작권을 갖는 저작권자에게 저작권료를 지불한다.
⑤ 지불완료 메시지 전송 : 저작권자는 배포권자에게

서 자신이 저작권을 갖는 콘텐츠에 대한 비용을 지불 받고 지불완료를 알리는 메시지를 서버에게 전송한다.

⑥ 콘텐츠 요약정보 전송 : 콘텐츠 요약정보는 콘텐츠의 이름, 등록시간 등의 메타데이터이며 서버로부터 전송받은 요약정보를 게시함으로써 사용자에게 콘텐츠 정보를 제공하게 된다.

⑦ 사용자 등록 및 인증 : 사용자는 자신의 ID, PW와 단말기정보를 서버에 등록하고, 자신이 등록한 정보와 함께 사용자의 단말기 정보를 이용하여 서버에 인증을 받는다. 이후 서버에 저장된 사용자의 단말기 정보를 식별하여 본인의 단말기에서만 콘텐츠에 접근이 가능하도록 한다.

⑧ 콘텐츠 요청 및 사용료 지불 : 사용자는 배포권자가 게시한 콘텐츠들의 요약정보를 보고 배포권자에게 자신이 원하는 콘텐츠를 요청한다. 사용자가 콘텐츠를 요청할 때에는 자신의 정보도 함께 전송한다. 전송받은 사용자 정보는 배포권자가 요청받은 콘텐츠 정보와 함께 서버에 알릴 때 사용한다. 그리고 사용자는 배포권자에게 콘텐츠에 대한 요금을 지불하게 된다.

⑨ 요청된 콘텐츠 정보 : 배포권자는 사용자가 요청한 콘텐츠의 정보를 서버에게 전송하게 된다.

⑩ 콘텐츠 암호화 : 서버는 배포권자로부터 전송받은 콘텐츠 정보를 통하여 사용자가 원하는 콘텐츠를 알 수 있고, 콘텐츠를 불러와 콘텐츠 암호화키를 생성하여 콘텐츠를 암호화한다. 콘텐츠 암호화키는 임의의 난수를 사용한다.

⑪ 라이선스 생성 : 서버는 콘텐츠를 요청한 사용자의 정보를 불러와서 콘텐츠에 대한 라이선스를 생성한다. 라이선스는 사용자의 정보로 생성한 난수로 콘텐츠 암호화키를 암호화하여 생성한다.

⑫ 암호화된 콘텐츠 전송 : 서버는 암호화된 콘텐츠를 사용자에게 전송한다. 암호화된 콘텐츠는 중간에 공격자가 획득하더라도 콘텐츠의 암호화키를 알 수 없기에 사용이 불가능하다.

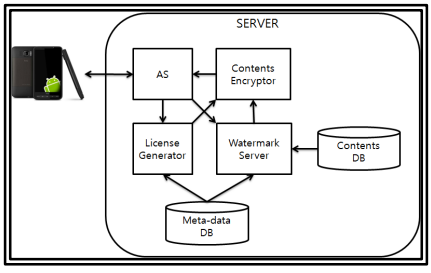
⑬ 라이선스 전송 : 서버는 배포권자에게 사용자가 요청한 콘텐츠의 라이선스를 전송한다. 이때 전송한 라이선스를 배포권자가 가지더라도 콘텐츠의 대한 모든 것은 서버가 관리를 하기에 배포권자는 콘텐츠를 이용할 수 없다.

⑭ 라이선스 요청 : 사용자는 배포권자에게 라이선스를 요청한다. 사용자는 서버로부터 전송받은 콘텐츠를 재생하기위해서 라이선스가 필요하다. 서버로부터 전송받은 콘텐츠는 암호화된 상태이기 때문에, 라이선스가 없이는 재생이 불가능하다.

⑮ 라이선스 전송 : 배포권자는 사용자의 라이선스 요청에 따라 자신이 서버로부터 전송 받은 라이선스를 사용자에게 전송한다. 사용자는 전송받은 라이선스에서 콘텐츠 암호화키를 추출할 수 있고, 암호화된 콘텐츠를 복호화하여 재생이 가능하다.

3.2 시스템 구성도

아래의 [그림 3]는 제안된 시스템의 구성도이다. 기본적인 스마트폰에서 서버로 접속하게 되며, 서버의 구성은 인증서버(AS : Authentication Server)와 콘텐츠 암호기(Contents Encryptor), 라이선스 생성기(License Generator), 워터마크 서버(Watermark Server), 콘텐츠 데이터베이스(Contents DB), 메타데이터 데이터베이스(Meta-data DB)로 구성된다.



[Fig. 3] Configuration of system

[그림 3]의 시스템 구성도에서 보는 바와 같이 사용자는 자신의 스마트폰에서 서버로 접속을 하게 되며, 인증서버의 인증을 거치게 된다. 인증과정에서 사용자의 정보가 서버에 저장되며, 라이선스 생성기와 콘텐츠 워터마크 서버에서 필요한 정보를 사용하게 된다. 콘텐츠 데이터베이스에는 콘텐츠 데이터가 저장되고, 메타데이터 데이터베이스에는 콘텐츠의 요약정보가 저장된다. 워터마크 서버에서 콘텐츠에 저작권자, 배포권자, 사용자의 워터마크를 마킹하며, 워터마크 된 콘텐츠는 콘텐츠 암호기를 통해 암호화 된다. 인증과정에서 얻은 사용자의 정보를 이용하여 라이선스 생성기는 콘텐츠의 암호화키를 숨겨 라이선스를 생성하며, 생성된 라이선스는 배포

권자에게 전송된다.

3.3 구현 및 분석

스마트폰 사용자 인증 모델은 WCDRM 모델을 기본 구조로 사용하지만 스마트폰에서의 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. 프로토콜은 회원등록, 로그인, 세션키 생성, 콘텐츠 등록 및 요약정보 전송, 콘텐츠의 암호화 및 라이선스 생성과정, 콘텐츠 전송 및 사용자의 콘텐츠 재생과정으로 구성된다.

본 장에서는 스마트폰에서 안전한 멀티미디어 보안 프로토콜을 구현한다. 스마트폰 사용자를 대상으로 하며 스마트폰 단말기 1대와 서버로 사용할 컴퓨터 1대를 이용하여 시스템을 구현한다.

3.3.1 구현 환경

사용자가 서비스를 받고 서버에 접속이 가능한 '스마트폰 어플리케이션'과 콘텐츠의 암호화 그리고 라이선스 생성 등의 기능을 가진 서버를 구현하고자 한다. 구현 환경은 아래와 같다.

[Table 1] Implementation of environmental

	안드로이드 폰	서버
O/S	Android OS 2.5	Windows 7 Home premium K
Process	퀄컴 스냅드래곤 1.5GHz 듀얼코어	Intel(R) Core(TM)2 Duo
CPU	Adreno 220	1.83GHz
HDD	20GB(SD card)	300GB
RAM	1GB RAM	3GB RAM

3.3.2 구현

스마트폰에 어플리케이션을 설치 후 실행을 하게 되고, 로그인 과정을 통하여 일차적으로 사용자를 인증한 후, 사용자의 정보를 이용하여 서버에 저장되어 있는 정보 값들로 세션키를 생성한다. 세션키를 생성할 때 사용되어지는 값들 중에 디바이스 정보 값도 있기 때문에 가입할 때의 디바이스가 아니면 인증에 실패하게 되는 것이다. 인증과정을 완료한 뒤 서버에 있는 콘텐츠들의 목록을 불러오게 되며, 이러한 목록을 선택한 뒤 재생을 하는 과정이다. 이러한 과정은 [그림 4]와 같다.

[Fig. 4] Smartphone authentication

로그인 단계에서는 사용자의 디바이스에서 서버에게 사용자의 로그인 정보가 전송된다. 여기서 사용자가 입력하는 정보는 사용자의 ID와 패스워드뿐이지만 실제로 전송되는 정보는 디바이스 정보까지 같이 연산되어 전송되어진다. 로그인 단계는 아래의 그림과 같다.

[Fig. 5] Login information

사용자는 애플리케이션을 실행한 후 로그인을 하기 위하여 자신의 아이디와 패스워드를 입력하게 된다. 그리고 서버에게 입력된 정보들과 자신의 스마트폰의 디바이스 정보들로 로그인 정보를 연산하여 서버에게 전송한다. 서버는 사용자의 아이디와 암호화된 내용이 사용자의 정확한 정보인지를 확인하는 과정은 [그림 6]과 같다.

[Fig. 6] User information in server

[그림 6]과 같이 서버에서는 사용자의 로그인 정보를 전송받고 전송받은 사용자 정보를 확인할 수 있다.

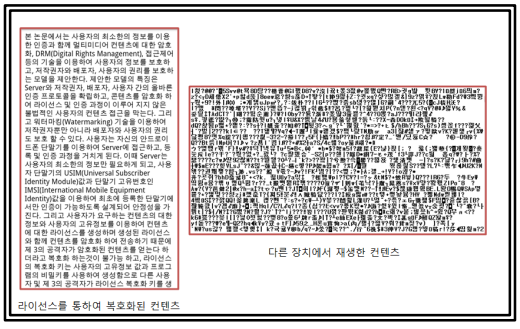
사용자 인증은 사용자가 로그인을 완료 후 입력받은 사용자의 로그인 정보로부터 서버에 저장되어 있는 정보와 연산하여 세션키를 발급한다.

사용자는 서버가 전송해준 콘텐츠의 목록에서 콘텐츠를 선택하고, 콘텐츠를 요청하게 된다. 서버가 가지고 있는 콘텐츠의 목록을 사용자에게 전송하여 사용자가 선택할 수 있도록 하고 있다.

서버는 사용자로부터 요청받은 콘텐츠를 키를 생성하여 암호화한다. 구현에서는 텍스트 파일을 이용하여 암호화를 구현한다.

[Fig. 7] Encrypted content

서버는 콘텐츠의 암호화가 완료되면 콘텐츠를 라이선스와 전송한다. 전송된 라이선스를 사용자는 자신의 정보와 함께 연산하여 콘텐츠 암호화키를 추출하게 된다. 이때 다른 장치에서 암호화된 콘텐츠를 재생하려고 한다면, 복호화 되지 않았기 때문에 재생이 불가능 하다. 다른 장치에서 라이선스를 획득하여 소유하고 있더라도 디바이스 정보 등의 사용자 정보가 다르기 때문에 라이선스에서 콘텐츠 암호화키를 추출하기가 불가능하기 때문이다. <그림 8>은 라이선스를 통하여 복화화된 콘텐츠와 다른 장치에서 복호화된 콘텐츠를 비교한 것이다.



[Fig. 8] Comparison of encrypted content

3.3.3 분석

회원가입 단계에서 비밀번호 정보 r_U는 이전의 인증 과정에서 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.

로그인 단계에서 사용자는 서비스를 제공받기 위해 서버에 접속하여야 하고, 접속을 위해서 서버에 로그인을 해야 한다. 사용자는 로그인을 위해 메시지를 생성하고 전송함으로써 서버에 접속을 시도 하게 된다. 하지만 공격자가 로그인을 위한 메시지 전체를 가지고 있다면 재전송 공격으로 인하여 로그인이 쉽게 가능해짐으로 시간 값인 T(Time-stamp)를 이용하여 재전송 공격을 차단할 수 있다.

- 내부자 공격(Insider attack)

만약 서버 관리자는 내부 데이터베이스에서 악의적인 의도를 가지고 사용자의 주민번호, 집 주소, 전화번호 등을 모두 알 수 있었다. 하지만 제안된 프로토콜은 인증에 필요한 최소한의 사용자 정보만 이용하여 서버로 전달되고 패스워드는 해시 함수를 거쳐서 전달되기 때문에 안전하다. 즉, 암호학적 해시 함수의 일방향성 때문에 서버 관리자라 하여도 사용자의 패스워드나 사용자의 개인정보를 추측 하거나 알 수 없기 때문에 내부자 공격에 안전하다.

- 재전송 공격(Replay attack)

제안한 프로토콜에서는 타임스탬프(T)를 이용하여 메시지의 유효성을 검증하고 있다. 만약 공격자가 사용자의 메시지를 중간에서 가로채 저장하고 재전송 할 경우, 그 메시지는 처음 단계인 타임스탬프(T), $M_2 = \mathrm{ID}_U$, $h(h(PW_U) \oplus T), T\}$에 대한 검증을 통과 할 수 없다. 또한 공격자가 다른 정보는 변경하지 않고 T만 변경할 경우 두 번째 단계인 무결성 검증 $h(M) \cong h'(M)$을 통과 할 수 없다. 그러므로 공격자의 재전송 공격에 안전하다.

- 중간자 공격(Man in the middle attack)

Alice와 Bob이 통신할 경우 공격자는 Alice와 Bob의 메시지를 중간에서 가로챌 수 있다. 공격자가 메시지

$M_1 = \{ID_U, r_u, H_U\}$를 가로챈다 하더라도 메시지의 $r_u = h(PW) \oplus S_N$에서 사용자 정보를 추출할 수 없고, 세션키 생성을 통하여 안전하게 서비스 받을 수 있다.

- 전방향 안전성(Forward secrecy)

제안한 프로토콜에서는 이전에 사용한 세션 키의 정보를 저장하지 않고, 한 세션 마다 세션키를 생성하고, 난수를 분배하기 때문에 안전하다. 또한, 생성하는 난수는 BBS알고리즘을 이용한 강력한 난수를 제공한다. 그러므로 현재의 세션 키로 이전의 세션 키를 계산한다는 것은 불가능하다.

4. 결 론

기존의 모델인 WCDRM 모델과 스마트카드를 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.

REFERENCES

[1] SeungRak Choi, “Content Delivery Networking : Core Techniques and Trends”, Korea Institute of Infomation Scientists and Engineers, Vol. 20, No. 9, 2002.

[2] Smartphone, wikipedia, http://ko.wikipedia.org/wiki/Smartphone.

[3] Jiaming He, "Digital Right Management Model Based on Cryptography and Digital Watermarking", Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Vol. 3, 2008.

[4] JongYong Park, “Design and Evaluation of DRM Model with Strong Security Based on Smart Card”, Journal of Digital Content Society, Vol. 12, No. 2, pp. 165-176, 2011.

[5] PassfacesTM, http://www.realuser.com.

[6] SaRang Na. “User Authentication f Smartphone to usage and store management for Mobie”, Korea Institute of Information Security and Cryptology, Vol. 21, No. 4, 2011.

저자소개

신 승 수

- 2001년 : 충북대학교 수학과 (이학박사)
- 2004년 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 ~ 현재 : 동명대학교 정보보호학과 부교수

<관심분야> : 네트워크보안, USN, 스마트카드. 암호이론, 정보보호