강력한 사용자 인증을 위한 Mobile DRM 시스템의 설계 및 구현

박수환*, 전진오, 강민섭
안양대학교 컴퓨터공학과
e-mail: jeimo@naver.com

Design and Implementation of Mobile DRM System for Robust User Authentication

Su Hwan Park*, Jeen Oh Jun, Min Sup Kang
Dept. of Computer Engineering, Anyang University

요 약

통신망 기술의 발달로 모바일 디지털 컨텐츠 분야에서도 다양한 방법으로 컨텐츠를 보호하려는 연구가 활발히 진행되고 있다. 본 논문에서는 불법사용방지 및 저작권 보호를 위해 강력한 사용자 인증을 위한 국제 표준 알고리듬 AES를 이용하여 컨텐츠를 암호화하고, 휴대폰 번호, 단말기 번호 등을 이용하여 컨텐츠 사용에 따른 권한을 이중화하여 관리한다. 또한 3차에 걸친 사용자 인증 과정을 통해 디지털 컨텐츠의 배포가 안전하게 이루어지는 시스템을 구축한다.

1. 서론

디지털 정보의 편리성으로 디지털 컨텐츠에 대한 수요가 증가함에 따라 실생활의 모든 컨텐츠들이 디지털화 되어가고 있다. 그러나 디지털 컨텐츠는 인터넷으로 컨텐츠의 유통 및 지불이 이루어지므로 보안상의 문제가 심각하게 대두되고 있다. 이에 대한 해결책으로 DRM이 등장하게 되었다[1,2].

유선 환경에서 제공되어 오던 DRM이 현재는 급격한 무선 인터넷 기술의 발전 및 사용자 증가로 인해 그 무대를 무선 인터넷 환경에까지 넓히고 있다. 따라서 또 다른 형태의 컨텐츠 보호에 대한 연구가 요구되고 있다.

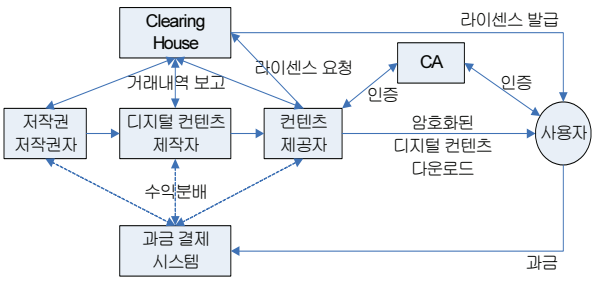
컨텐츠 보호를 위한 방안으로 키 수열에 비선형성을 증가시켜 상관 공격 등에 강한 암호알고리듬과[5], Puzzle기법과 OTP(One Time Password)를 이용해서 암호화 하는 방법들이 제안되었다[6]. 그러나 제안한 방법들은 휴대폰 및 PDA와 같은 이동단말기에 대한 적용의 어려움이 있다.

본 논문에서는 강력한 인증을 이용하여 무선 인터넷 환경에서 디지털 컨텐츠 보호를 위한 Mobile DRM 시스템의 설계 및 구현에 관하여 기술한다. 제안된 시스템은 국제 표준 알고리듬 AES(Advanced Encryption Standard)를 이용하여 컨텐츠를 암호화하고, 휴대폰 번호, 단말기 번호 등을 이용하여 컨텐츠 사용에 따른 권한을 이중화하여 관리한다. 또한 3차에 걸친 사용자 인증 과정을 통해 디지털 컨텐츠의 배포가 안전하게 이루어지는 시스템을 구축한다.

2. DRM과 무선 인터넷 서비스

DRM이란 디지털 컨텐츠의 불법 사용을 막아, 저작권 관련 당사자들의 권리와 이익을 지속적으로 보호해주는 기술로 이를 위한 요소기술로는 암호화, 핑거프린팅, 공개키 기반 구조 등이 있다.

(그림 1)은 DRM 시스템의 컨텐츠와 저작권에 대한 유통 흐름을 보여주고 있다[3].



(그림 1) DRM 시스템에서의 컨텐츠 유통 흐름도

DRM 시스템은 저작권자, 디지털 컨텐츠 제작자, 컨텐츠 제공자 및 사용자간의 유기적인 관계로 구성되어 있다. 이들의 관계는 수익분배나 거래내역 보고, 인증, 라이센스 발급에 대한 원칙을 가지고 있다.

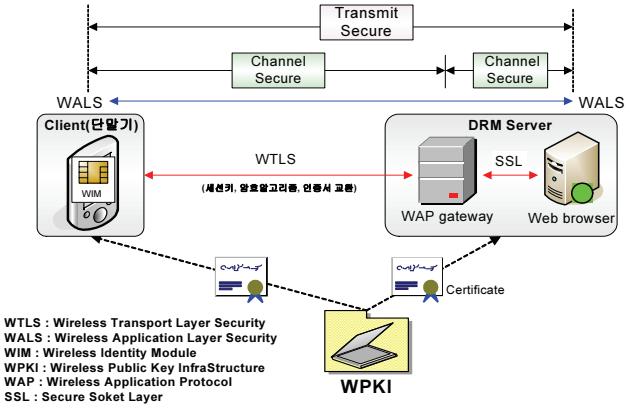
무선 인터넷에서 사용되는 프로토콜은 유선 인터넷에서 사용하는 HTTP, HTML을 기반으로 경량화시켜 만든 프로토콜을 사용하고 있다. 현재 사용되고 있는 대표적인 무선 인터넷 프로토콜은 WAP, ME, i-mode등이 있다[4].

WAP(Wireless Application Protocol)은 이동형 단말기에서 인터넷에 접속할 수 있도록 하기 위해 고안된 통신규약으로 유선 인터넷 네트워크와 무선 네트워크를 연결하는 WAP Gateway는 프로토콜의 변환, HTML의 WML로의 변환, WML 컨텐츠의 부호화와 복호화 등의 기능이 있다.

3. 모바일 DRM을 위한 시스템의 설계

3.1 시스템의 구성도

(그림 2)는 WAP PKI를 이용한 시스템 구성도를 나타낸다.

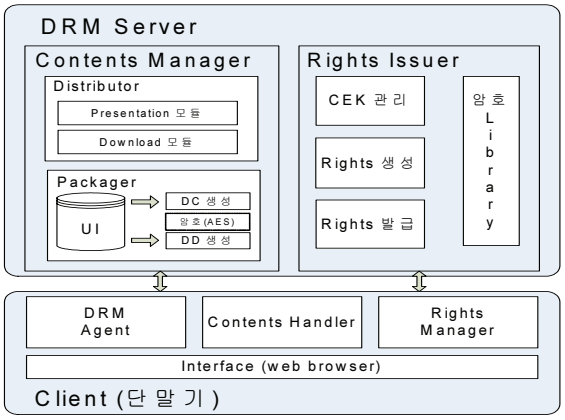


(그림 2) WAP PKI를 이용한 시스템 구성도

Client(단말기)와 DRM Server가 WTLS를 통해서 연결을 할 경우, 먼저 핸드쉐이크 프로토콜을 수행하여 한 세션 동안 보안서비스 제공에 사용되는 세션 키, 암호 알고리듬, 인증서 등과 같은 암호 매개변수를 서로 공유하게 된다. 여기서 생성된 세션 정보는 레코드 프로토콜에서 보안서비스를 제공하는데 이용된다. 보안 전송방식은 Client에서 WAP 게이트웨이까지의 채널 보안에 WTLS를 사용하고 WAP 게이트웨이에서 웹브라우저까지의 보안에는 SSL을 사용한다[4].

3.2 시스템의 구조 설계

(그림 3)은 본 논문에서 제안하는 모바일 DRM 시스템의 구조를 나타낸다.



(그림 3) 모바일 DRM 시스템 구조

모바일 DRM 시스템은 Contents Manager와 Rights Issuer를 포함하고 있는 DRM Server와 Client로 구성되어 있다.

3.2.1 DRM Server

(1) Contents Manager(CM)

CM은 컨텐츠 정보와 DRM 컨텐츠를 보관하고 있는 Distributor와 디지털 컨텐츠 제공자로부터 디지털 컨텐츠를 가공하여 DRM 컨텐츠를 생성하는 Packager로 구성되어 있다.

Distributor는 컨텐츠 목록 및 컨텐츠 메타데이터인 Download Descriptor를 브라우징하는 Presentation 모듈과, 컨텐츠 요청 시 DRM 컨텐츠를 사용자에게 전송해주는 Download 모듈로 구성되어 있다.

Packager는 컨텐츠 제공자가 등록한 컨텐츠를 암호화하고, 컨텐츠의 정보인 UI(User Interface)를 이용하여 DRM Contents(DC)로 패키징하고, 컨텐츠에 대한 메타데이터인 Download Descriptor(DD)를 생성한다. 그리고 컨텐츠 암호화에 사용된 암호키(CEK)는 권한 객체에 포함되어 WAP Push를 이용하여 클라이언트의 무선단말기로 전송된다.

(2) Rights Issuer(RI)

RI는 Packager로부터 데이터를 받아 Storage에 저장하고, 암호 Library에서는 생성된 Right와 Content Encryption Key(CEK)를 사용자 공개키로 암호화 하는 역할과 유효한 사용자에게 해당 컨텐츠에 대한 사용권한인 Right를 발급해주는 역할을 하며 사용자가 컨텐츠를 요청하면 Download 모듈은 RI에게 해당 컨텐츠에 대한 사용권한을 요청하는 기능을 한다.

3.2.2 Client(단말기)

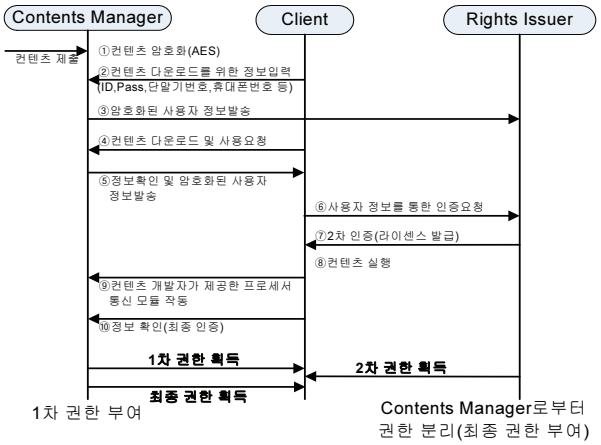
Client는 WAP을 통해 무선 인터넷에 접속하는 이동통신 단말기를 말한다. Client는 DRM Distributor에 접속하여 컨텐츠를 다운로드 받고, RI에게서

WAP Push 메시지를 통해 해당 컨텐츠에 대한 사용권한을 전달받는다. 유효한 사용권한이 존재하는 경우에만 DRM 컨텐츠를 사용할 수 있게 되며 DRM Agent, Contents Handler(CH), Rights Manager(RM)와 Interface로 구성되어 있다.

DRM Agent는 DRM 컨텐츠 사용을 권한에 따라 제어하며 CH에서 컨텐츠를 사용하겠다는 요청이 있을 경우, RM을 호출하여 사용권한을 확인하고, 사용권한이 올바른 경우에만 컨텐츠의 복호화를 진행하여 사용이 가능하도록 한다. CH는 DRM 컨텐츠를 사용자가 이용할 수 있도록 해주는 응용 프로그램이며, RM은 Right의 암호화를 위해 공개키/비밀키 쌍을 생성하여 RI로부터 WAP Push 메시지를 받으면 공개키를 전송하고 DRM 컨텐츠를 사용하는데 있어서 Right 정보를 점검하고 갱신한다. Interface는 무선 인터넷에서 사용하는 웹 브라우저를 이용한다.

3.3 모바일 DRM 컨텐츠의 사용자 인증 과정

(그림 4)는 모바일 DRM 컨텐츠의 인증 과정을 나타낸다.



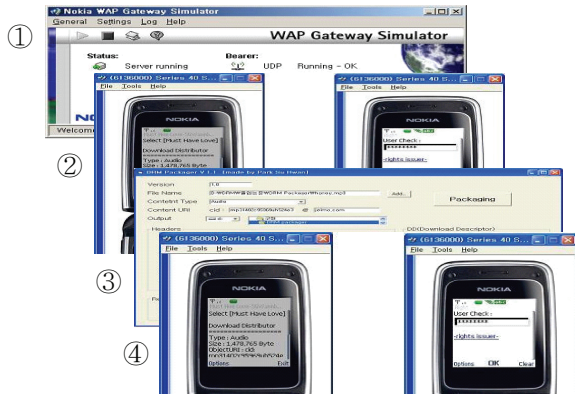
(그림 4) 모바일 DRM 컨텐츠 유통 흐름도

디지털 컨텐츠 제작자는 자신의 컨텐츠를 AES 알고리듬[9]을 이용하여 암호화 한 후 CM에 등록한다. Client에서는 컨텐츠를 다운로드 하기 위해 ID, Password, 단말기번호, 휴대폰번호 등의 정보를 CM에게 입력하면 CM은 Client의 정보를 확인하고 입력된 사용자 정보를 암호화한다. 암호화된 사용자 정보는 인증에 따른 권한 분리를 위하여 RI에게 전송한다. Client는 CM에서 컨텐츠를 다운로드 받고 사용요청을 한다. CM은 처음에 Client가 입력한 정보를 확인한 후 암호화된 사용자 정보를 Client에게 전송한다. Client는 암호화된 사용자 정보를 통해서 RI에게 인증을 요청하고, RI는 이 정보를 통해서 인증을 하고 Client에게 라이센스를 발급한다. 이로써 CM에게서 다운받은 컨텐츠를 사용할 수 있는 권한을 부여 받고, 컨텐츠를 실행한다. 컨텐츠 실행과 동시에 최종 사용자와 프로세서 통신을 하기 위해 컨텐츠 개발자가 제공한 프로세서 통신 모듈이 작동된다. CM은 사용자 정보(ID, Password, 단말기번호, 휴대폰번호 등)를 통해 최종적으로 컨텐츠를 사용할 수 있는 권한을 부여하게 된다.

4. 모바일 DRM 보안 시스템 구현

제안된 시스템은 Windows 2003환경에서 서버를 구축하였으며, 웹서버로는 IIS(Internet Information Server)를 사용하였고, Nokia의 WAP Gateway Simulator[10]를 통해서 Client Device와 서버간의 통신을 시험하였다. Packager는 .NET을 통해 설계하였으며, 컨텐츠 암호화부분은 C로 구현된 AES알고리듬을 사용하였다. 패키징되는 컨텐츠를 다운받고 실행할 Client는 Nokia의 Mobile Browser Simulator[10]를 사용하여 가상으로 실험하였다.

(그림 5)는 2차 권한 획득을 위한 모바일 DRM 시스템의 실행 과정을 나타내며 번호는 실행 순서를 나타낸다.



(그림 5) 1,2차 권한 획득을 위한 실행 과정

4.1 사용자 인증(1차)

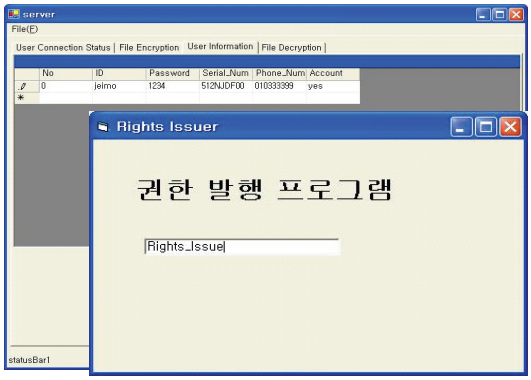
컨텐츠 제작자로부터 제공되는 Packaging 컨텐츠는 Distributor에게 전달되어 사용자가 Client를 통해 컨텐츠를 요청할 때 컨텐츠의 목록을 보여준다. 사용자는 컨텐츠를 다운로드 받기 전에 단말기 번호, 휴대폰 번호, 권한 등의 정보를 입력하게 된다. CM은 컨텐츠와 사용자 정보를 재패키징하고, 사용자가 요구할 때 사용자 정보 확인을 통하여 자신이 정당한 컨텐츠 사용자인지 확인하고 컨텐츠를 사용할 수 있도록 RI에게 암호화된 사용자 정보를 보낸 후 사용권한인 Right를 획득하게 된다.

4.2 권한 획득(2차)

사용자 인증 후 RI에게서 발급 받은 권한(Right)으로 인해 사용자는 DRM Contents를 사용할 수 있는 2차 권한을 획득한다. 자신의 단말기에 저장된 컨텐츠는 각 컨텐츠 타입에 따라 단말기 내의 응용 프로그램을 통해서 실행이 가능하다. 그러나 2차 권한을 획득한 컨텐츠도 다른 사용자에게도 쉽게 전달될 수 있다. 하지만 DRM 컨텐츠를 전달받은 다른 사용자는 컨텐츠를 사용하기 위해서 최종 권한을 획득해야 한다.

4.3 최종 사용 권한 획득(3차)

(그림 6)은 최종 사용권한을 부여한 컨텐츠 실행 과정을 나타낸다.



(그림 6) 최종 사용권한 획득 과정

최종 RI에게서 권한을 획득하기 위해 먼저 CM에게 1차 권한을 획득해야 하며, 또한 RI에게 권한을 획득했다 하더라도 실행 시 컨텐츠 개발자가 제공한 프로세서 통신 모듈을 통해 3차 인증을 받아야 하므로 사실상 불법 컨텐츠 사용이 불가능하다.

개발자 프로세서 통신 모듈은 컨텐츠 실행 시 사용자의 시스템 정보를 확인하고 결제 확인을 체크하여 사용자에게 메시지를 전송하여 주며, 사용자의 시스템 정보와 결제가 이루어진 사용자는 권한 발행 프로그램을 통하여 컨텐츠를 사용할 수 있는 실질적인 사용권한을 부여받게 된다. 최종 사용자와 컨텐츠는 프로세서 통신을 위해 컨텐츠 개발자가 제공한 프로세서 통신 모듈을 포함하게 되므로 보다 강력한 인증 체계를 보장 할 수 있다. 결국, CM와 RI간의 권한 분리와 3단계에 걸친 인증 체계를 통하여 Client 인증 과정을 더욱 강화시켰다.

5. 결론

본 논문에서는 강력한 사용자 인증을 위한 Mobile DRM 시스템의 설계 및 구현에 관하여 기술하였다.

다양한 모바일 DRM 시스템중에 OMA에서 제안한 방식인 컨텐츠와 권한을 분리해서 전송하는 Seperate Deliver 방식을 기본으로 하여 파일 암호화, 단말기 번호, 권한부여 등을 통하여 컨텐츠 사용에 따른 권한을 이중화하였다. 강력한 사용자 인증을 위하여 1차와 2차에서는 AES 알고리듬을 사용하여 컨텐츠의 보안을 강화시켰으며, 그리고 정당한 사용자가 자신의 컨텐츠를 제3자에게 재분배했을 경우를 고려하여 불법적인 컨텐츠 사용시에 개발자 프로세서 통신 모듈을 통해 최종(3차)적으로 컨텐츠를 사용할 수 있는 권한을 부여함으로써 Client 인증과정을 더욱 강화시켰다.

그러나 현 시점에도 모바일 DRM은 무선 인터넷의 접속시간과 데이터크기에 따른 요금, 보안에 대한 문제 때문에, 이 부분에 대한 더 많은 연구가 필요하다.

참 고 문 헌

[1] 김충남, “차세대 무선인터넷 서비스,” 전자신문사, 2003.

[2] 윤기송, “DRM 기술 현황 및 컨텐츠 유통 인프라 구축 방안”, 정보과학회지, 2005.

[3] 장용철, 오태석, 오무송, “암호화를 위한 전자결제 시스템의 설계 및 구현”, 정보처리 논문지 Vol.21, No. 8, 1997.

[4] 한국정보학회, “차세대 네트워크 보안기술”, 한국정보보호진흥원, 2002.

[5] 조상일 외1명, “디지털 컨텐츠 보호에 적합한 암호알고리즘 제안”, 한국정보처리학회, 2006.

[6] 이광형 외4명, “멀티미디어 컨텐츠 보호를 위한 향상된 인증 프로토콜 보안 시스템에 관한 연구”, 한국정보처리학회, 2006.

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

[8] I. J. Cox, J. Killian, T. Leighton, “Secure Spread Spectrum Watermaking for Multimedia”, IEEE Trans. in Image Processing, Vol6, No12, 1997.

[9] Advanced Encryption Standard Development Effort, http://www.nist.gov/aes.

[10] Forum NOKIA, http://www.forum.nokia.com.