무선 DRM 시스템에서의 인증방법에 대한 연구

김봉선†○ 이권일* 신영찬† 류재철† 이준석**
†충남대학교 컴퓨터 과학과
*대덕대학 컴퓨터 인터넷 정보계열
**한국전자통신연구원 컴퓨터소프트웨어연구소
†{bskim○, ycshin, jcryou}@home.cnu.ac.kr
*kilee@mail.ddc.ac.kr
**jslee@etri.re.kr

A Study on Authentication Method for Wireless DRM System

Bong-Seon Kim†○, Kwon-Il Lee*, Young-Chan Shin†, Jae-Cheol Ryou†, Jun-Seok Lee**
†Dept of Computer Science, Chungnam University
*Faculty of Computer and Internet Information, Daeduck College
**Computer & Software Research Laboratory, ETRI

요 약

DRM (Digital Rights Management)은 디지털 저작권 관리를 뜻하는 말로, 전자책, 음악, 게임 등의 디지털 컨텐츠의 지적 재산권을 보호하기 위해 디지털 컨텐츠의 무단 유통을 방지하는 서비스를 의미한다. 이러한 DRM 시스템은 주로 유선 환경에서 사용되고 있었으나, 최근 정보통신 기술의 발달로 인한 무선 환경에서의 디지털 컨텐츠의 사용 요구가 증가함에 따라 DRM 시스템은 유선 환경 뿐만 아니라 무선 환경에서도 그 중요성이 날로 커지고 있는 실정이다. 현재 DRM은 디지털 컨텐츠에 대한 저작권에 대한 보호 뿐 아니라 더 나아가 디지털 컨텐츠를 이용한 마케팅 솔루션을 제공하는 것까지 그 영역을 확장함에 따라 각 비즈니스 영역별로 적합하도록 다양한 DRM 솔루션이 제시되고 있다. 이로 인해 시스템간의 호환성을 위해 현재 OMA 등의 단체에서 무선 DRM에 관한 표준을 제시하고 있다. 그러나 표준으로 제시되고 있는 DRM 모델에서는 인가된 사용자만이 컨텐츠를 사용할 수 있도록 하는 인증서비스에 관한 부분이 매우 취약한 상황이다. 이에 따라 본 논문에서는 키 관리 서버와 사용자별 암호키 리스트를 다르게 소유할 수 있도록 하는 방법을 사용하는 인증서비스를 제시해보고자 한다.

1. 서 론

DRM (Digital Rights Management)은 디지털 저작권 관리를 뜻하는 말로, 전자책, 음악, 게임 등의 디지털 컨텐츠의 지적 재산권을 보호하기 위해 디지털 컨텐츠의 무단 유통을 방지하는 서비스를 의미한다.

정보통신의 발달로 인한 PDA 및 휴대 전화 등을 이용한 무선 환경에서의 디지털 컨텐츠의 사용 요구가 증가함에 따라 무선 컨텐츠 제공자들은 이미 무선 환경에 맞는 DRM 시스템을 제공하고 있으며, 보다 안전하고 효율적인 DRM 서비스 제공을 위한 솔루션을 연구, 개발 중에 있다.

현재 DRM은 디지털 컨텐츠에 대한 저작권에 더 나아가 디지털 컨텐츠를 이용한 마케팅 솔루션을 제공하는 것까지 그 영역을 확장하고 있다. 이에 따라 정형화된 모델이 존재하는 것이 아니라 각 비즈니스 영역별로 적합한 다양한 DRM 솔루션이 제시되어 왔다. 이로 인해 서로 상이한 DRM 시스템 상호간의 호환성 결여 문제로 사용자들의 불편이 커지고 있고, 컨텐츠 제공 업체에서도 한 번 채택한 DRM 시스템을 변경하는 것이 어렵다는 문제점을 지니고 있어 DRM간의 표준화가 매우 필수적인 상황이다.

현재 무선 DRM의 표준을 제정하고 있는 대표적인 단체로는 OMA (Open Mobile Alliance) 가 있다.

OMA 등에서 제시한 무선 DRM 솔루션에는 인가된 사용자에게만 컨텐츠의 사용 및 실행을 허용하도록 하기 위한 인증서비스 부분이 매우 취약한 상황이다. 이에 따라 본 논문에서는 현재 표준으로 제시되고 있는 무선 DRM 솔루션에 적합한 인증서비스를 제시하여 보다 효율적이며 안전한 DRM 솔루션을 제안하고자 한다.

본 논문의 2장에서는 관련 연구로써 현재 무선 DRM 솔루션의 표준으로 제시되고 있는 OMA의 DRM 솔루션들에 대해 알아본다. 3장에서는 표준 무선 DRM 솔루션에 존재할 수 있는 위협에 어떤 것들이 있는지 알아보고, 이에 대처할 수 있는 인증서비스 메커니즘을 제시하고, 마지막으로 4장에서는 향후 연구방향에 대해 알아보고, 본 논문의 결론을 내린다.

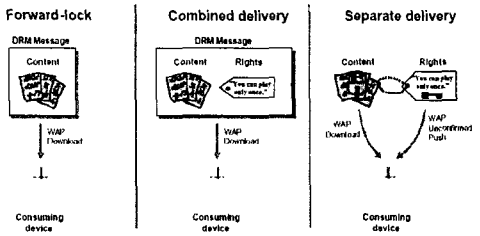
2. OMA 무선 DRM

OMA에서는 보다 구체적으로 무선 DRM에 관련된 규격을 제시하고 있다. OMA는 WAP 기반에서 작동하는 무선 통신에 적용하는 응용으로서 무선 DRM을 규정하고 있으며, 현재 DRM과 관련하여 OMA DRM 버전 1.0, DRM 컨텐츠 형식, DRM 권한 표현 및 컨텐츠 다운로드에 관한 규격이 나와있다.

OMA DRM의 경우 DRM 권한과 컨텐츠를 분배하는 방식으로 "Forward Lock", "Combined Delivery", "Separate Delivery"의 3 가지를 정의하고 있다. [그림 1]은 OMA에서 제시하는 3가지 DRM 방식에 대하여 보여주고 있다.

"Forward Lock"은 한 클라이언트 기기에서 사용되는 컨텐츠가 다른 클라이언트에게 전송되어 실행되거나 사용할 수 없도록 하는 것이다. 이 방식은 메시지에 권한은 삽입되지 않으며 한 클라이언트 기기에서 다른 클라이언트 기기로의 컨텐츠 포워딩을 허용하지 않는 방식이다.

"Combined Delivery"는 DRM 컨텐츠와 사용 권한이 함께 클라이언트 기기로 전송되는 방식을 말한다.



[그림 1] OMA DRM 방식

"Separate Delivery"는 DRM 컨텐츠와 사용권한을 별도로 클라이언트 기기에 전송해주는 것으로 Superdistribution을 지원한다.

3. 무선 DRM 시스템 취약점 및 인증 메커니즘

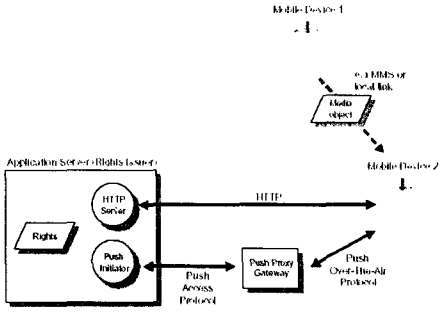
3.1. 무선 DRM 시스템 취약점

현재 진행 중인 무선 DRM 표준에서는 보안에 관련된 부분들은 아직 자세히 다루지 않고 있으며, 오히려 사용자 기기에서 충실히 사용 권한에 따를 것이라고 신뢰하고 있는 입장이다.

DRM은 시스템의 성격상 기존의 보안 시스템들과는 다른 특성을 갖는다. 기존의 보안 시스템이 공격자로부터 사용자를 보호하는 구조를 갖는다면, DRM 시스템에 있어서 사용자는 공격자 자체가 될 수 있다. 즉, 임의의 사용자가 자신이 받은 컨텐츠와 컨텐츠 암호 키를 가까운 누군가에게 전달하여 사용할 수 있게 해줌으로써 DRM 시스템의 기능을 쓸모없게 만들 수 있는 가능성이 존재한다.

DRM 시스템에 있어 가장 중요한 보안요소 중 하나가 인가된 사용자만이 컨텐츠를 사용할 수 있도록 하는 인증서비스이다. 컨텐츠에 대하여 적절한 지불을 하고, 지불에 대한 사용 권한을 받은 사용자만이 컨텐츠를 사용하도록 하며, 복호화된 컨텐츠를 임의의 다른 사용자 기기로 전송하거나 사용권한을 함부로 변경할 수 없도록 하는 것이 DRM 시스템의 기능 중 하나이다.

그러나 현재 제시된 표준 시스템들은 이러한 인증 부분에 대한 것은 자세히 언급하지 않고 있다. [그림 2]는 현재 OMA에서 제시한 Superdistribution을 지원하는 DRM 시스템의 서비스 흐름도이다.



[그림 2] 재분배 방식의 구조의 예

[그림 2]에서 Mobile Device 1에서 컨텐츠와 컨텐츠의 암호키를 포함하는 사용 권한을 받아서 컨텐츠를 사용하거나 실행할 수 있게 되며, 이 컨텐츠를 Mobile Device 2에게 전달하는 경우 컨텐츠는 DRM 컨텐츠 형식(DCF)으로 변환된 상태로 Mobile Device 2에 전달될 수 있다. OMA에서 제시한 방식에서는 Mobile Device 2에서 컨텐츠를 사용하기 위해서는 따로 사용 권한을 받도록 하고 있으나 Mobile Device 1의 사용자는 컨텐츠의 암호키를 포함하는 사용 권한을 소유하고 있기 때문에 이 암호화키를 Mobile Device 2에게 함께 전달해줄 수 있는 가능성이 존재한다.

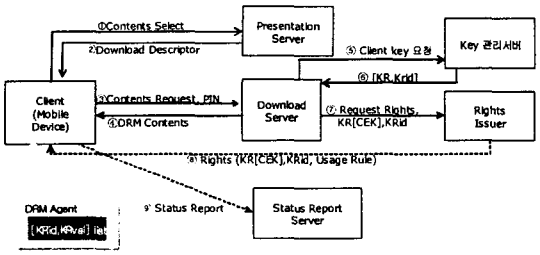
이러한 위험에 대처할 수 있도록 하기위해서는 적절한 키 관리 메커니즘과 디바이스 내에서의 응용 엔티티 사이의 적절한 구분을 두어 DRM 적용을 받는 컨텐츠를 다른 응용에서 접근하여 사용하는 일이 발생하지 않도록 해야 한다.

3.2 무선 DRM 시스템을 위한 인증 메커니즘

무선 DRM 시스템의 보안서비스를 제공하는 데 있어서 공개키 기반구조를 사용하면 사용자 인증, 기밀성, 무결성, 부인봉쇄 등의 필수 보안 서비스를 모두 제공할 수가 있으나, 무선 환경 및 무선 디바이스의 리소스의 제한 등에 의한 성능저하가 발생할 수 있기 때문에 관용 암호방식을 이용하여 위의 취약점들을 보완해보고자 한다.

본 논문에서는 컨텐츠 암호키(CEK)를 암호화하는 키의 아이디와 키값으로 이루어진 리스트와 이를 관리하는 서버를 사용한다. 이 리스트는 DRM 에이전트가 사용자 기기에 설치될 때 각 사용자 기기마다 일정하지 않은 순서로 키 리스트를 저장하게 되고, 각 키 리스트와 사용자 기기의 관계는 키 관리 서버에서 관리하도록 한다. 사용 권한 발급기관은 사용 권한에 암호화된 CEK와 사용된 키의 아이디를 사용자에게 제공한다. 사

용자는 자신이 가지고 있는 키 리스트 중에서 키 아이디에 해당하는 키 값을 이용하여 CEK를 복호화하고, 복호화한 CEK를 이용하여 DRM 컨텐츠를 복호화한 후 사용 규칙에 따라 이를 실행시키거나 사용할 수 있게 된다.



[그림 3] DRM 에이전트 키 리스트를 이용한 DRM 시나리오

[그림 3]은 DRM 에이전트에 키 아이디 및 키 값 쌍의 리스트를 포함시켜 이를 이용하여 제공되는 DRM 시스템의 시나리오이다.

① Presentation Server의 컨텐츠 리스트 중에서 사용자는 마음에 드는 컨텐츠를 선택한다.

② Presentation Server는 사용자가 선택한 컨텐츠에 대한 메타정보를 포함하고 있는 Download Descriptor를 사용자에게 전송한다.

③ 사용자는 Download Descriptor에서 제공하는 컨텐츠 정보를 확인한 후 Download Server에 컨텐츠를 요청한다. 이 때 사용자 확인을 위해서 자신에 해당하는 PIN 번호를 함께 전송한다.

④ Download Server는 PIN을 확인한 후(사용자 확인) DCF 형태의 DRM 컨텐츠를 전송한다.

⑤ Downlaod Descriptor는 키 관리 서버에게 해당 사용자 기기의 키 리스트에 존재하는 키와 키 아이디를 요청한다.

⑥ 키 관리 서버는 Download Server에게 키와 키 아이디를 전달한다.

⑦ Download Server는 Rights Issuer에게 사용 권한을 요청한다. Download Server는 컨텐츠를 암호화한 키(CEK)를 키 관리 서버로부터 받은 키를 이용하여 암호화한 후 사용된 키 아이디와 암호화한 컨텐츠 키(Ekr[CEK])를 Rights Issuer에게 전송한다.

⑧ Rights Issuer는 Download Server에서 받은 암호화된 CEK와 암호화에 사용된 키의 아이디를 사용권한에 포함시키고, 사용 규칙을 생성하여 사용자 기기에게 전송하게 된다.

⑨ 사용권한을 받은 사용자 기기는 권한에 명시되어 있는 키 아이디와 동일한 키 아이디를 자신이 소유하고 있는 키 리스트에서 검색한 후 해당되는 키 아이디의 키 값을 이용하여 CEK를 복호화한다. 그 후 CEK를 이용하여 Download Server로부터 받은 컨텐츠를 복호화한 후 사용가능하게 된다.

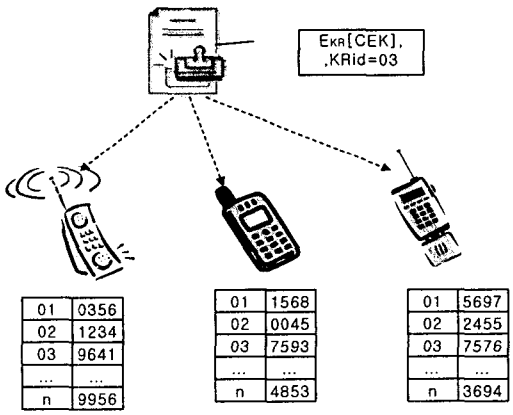
⑩ 컨텐츠 및 사용권한이 올바르게 전송된 경우 사용자 기기에서는 Status Server에게 전송 상태 보고를 보낸다. (이 항목은 선택적이다.)

본 논문에서 제시한 방법은 불법적인 사용권한 분배의 경우 [그림 4]에서처럼 키 아이디로 사용되는 키 리스트의 순서가 DRM 에이전트마다 다르기 때문에 디바이스가 컨텐츠와 사용권한을 모두 획득하더라도 CEK를 복호화할 수 없게 되므로 컨텐츠를 사용하지 못하게 된다. 또한 사용자의 의지와 상관없이 PIN이 노출되어 악의적인 사용자가 인가된 사용자처럼 사용자 확인을 받게되면, 컨텐츠 및 사용 권한의 획득은 가능하다. 그러나 CEK의 복호화는 불가능하기 때문에 컨텐츠를 사용할 수 없다.

4. 결 론 및 향후 연구방향

본 논문에서는 키 리스트를 사용한 무선 DRM 시스템을 위한 인증방법을 제안하였다. 각 DRM 에이전트마다 서로 다른 키 리스트를 사용함으로써 사용자 의 의도적인 DRM 컨텐츠의 무단 배포 및 제어되지 않은 사용과 사용자 의도와 상관없는 DRM 컨텐츠의 도용 및 사용을 방지할 수 있다.

그러나 무선 DRM 시스템의 표준화가 현재 진행 중이므로 무선 DRM 시스템의 인증 서비스에 대한 연구는 본 논문에서 제안한 방법뿐만 아니라 표준화 진행 상황에 맞추어 더 많은 연구가 필요하다.



[그림 4] 각 핸드셋 DRM 에이전트마다 다른 키 리스트 소유

참고문헌

[1] 3GPP "Digital Rights Management Technical Specification", 2002. 01.

[2] OMA "Digital Rights Management V1.0", 2002. 09

[3] OMA "Generic Content Download Over The Air Specification V1.0", 2002. 12.

[4] OMA "DRM Rights Expression Language", 2002. 12.

[5] OMA "DRM Contents Format V1.0", 2002. 12.