무선 네트워크상에서 콘텐츠 보호를 위한 동적 디코딩 기술 설계

하태진*, 한승조*

* 조선대학교 정보통신공학과

Dynamic dicoding technique Design for contents protection on radio network

Tae-Jin Ha*, Seung-Jo Han*

* Department of Information Communication Eng. Chosun Univ.

요 약

DRM은 디지털콘텐츠의 지적재산권이 디지털 방식에 의해서 안전하게 보호. 유지되도록 하여 디지털콘텐츠의 창작에서부터 소비에까지 이르는 모든 유통 시점에서 거래규칙과 사용규칙이 지속적이고 적법하게 성취되도록 하는 기술이다. DRM은 디지털 형태로 유통되는 문서, 음악, 비디오, 게임, 소프트웨어, 이미지 등의 각종 디지털 콘텐츠를 불법 복제로부터 안전하게 보호하고, 콘텐츠 서비스의 유료화를 가능케 하는 기술 및 서비스를 말한다. 또한, 콘텐츠 자체와 보안과 저작권 보호뿐만 아니라 콘텐츠의 생성·유통·사용·관리에 필요한 모든 프로세스를 제어할 수 있게 해준다. 본 논문에서 구현된 기술은 암호알고리즘을 사용하여 함수의 위치 및 내용에 쉽게 접근할 수 없고 소프트웨어의 불법적인 분석 시도를 어렵게 하였다.

키워드

DRM 콘텐츠 불법복제 인증

Ⅰ. 서 론

새로운 콘텐츠 서비스의 제공에 있어서 효율적인 기술 개발 뿐만 아니라, 고급 디지털 콘텐츠의 생산 또한 중요한 부분이다. 그러나 많은 시간과 비용, 그리고 노력을 투자한 디지털 콘텐츠가 불법 복제와 불법 유통으로 인해 투자한 만큼의 경제적 이익을 얻을 수 없는 경우에는 콘텐츠 창작과 의지가 위축되고 고품질 다기능 디지털 콘텐츠 서비스의 성공 또한 어렵게 될 것입니다.[1] 따라서 다양한 비즈니스 모델을 지원하고 각 유통 주체들 간의 상호 독립성을 보장하면서, 디지털 콘텐츠의 보호 및 유통 기술이 절실히 요구되고 있다.

Ⅱ. 관 련 기 술

1. 3GPP

3GPP(Third Generation Partnership Project)는 1998년 12월에 설립된 수많은 표준화 기구들 사이의 공동연구 합의로 이루어졌다. 3GPP의 목적은 third generation mobile communications(3G)를 위해 광범위하게 적용할 수 있는 기술적인 규격을 제공하는 것이다. 현재 이동통신 사업자를 포함하여 500개의 회원사가 가입되어 있다. 3GPP는 2003년 중순에 release 6에서 무선 DRM 규격을 소개할 계획이었으나, 2002년 9월 3GPP의 무선 DRM 표준화 작업에 대한 책임이 Open Mobile Alliance(OMA)로 전가되면서 DRM에 대한 활발한 활동은 더 이상 진전이 없게 되었다 현재 3GPP TS 22.242 Digital Rights Management(DRM); Stage 1까지 완성되었으며, DRM 솔루션을 제공하기 위한 시스템의 기능 및 역할에 대한 요구사항이 정리된 상태이다. 요구사항 문서에서는 사용자와 사용자 단말기, 사용권리, 보안, 프라이버시, 과금을 위한 DRM의 일반적인 조건과 요구사항을 기술하고 있다.[2]

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

2. OMA

OMA(Open Mobile Alliance)는 Open Mobile Architecture Initiative 와 WAP Forum에 의해 2002년 6월에 설립되었다. OMA는 모바일 산업을 위하여 사용자와 시장의 요구사항에 근거한 개방된 표준과 스펙에 대한 소개를 목적으로 한다.

Ericsson, Microsoft, Motorola, Nokia, Openwave, Siemens, DoCoMo, Vodafone, Sonera와 같은 국외 업체 및 삼성, SKT등과 같은 국내 업체를 포함 300여개의 회원사가 가입되어 있다. OMA DRM Version 1.0 규격은 2002년 9월에 승인되었고 신속히 구현될 수 있는 초기 단계의 간단한 무선 DRM 표준을 제안하는데 중점을 두었다.[3]

OMA DRM Version 1.0은 두 가지 문제점을 해결하기 위해 개발되었는데 첫째, Forward-lock 없이 단말기 상에 있는 콘텐츠를 다른 사용자에게 불법적으로 전송하는 것을 방지하기 위한 표준화된 방법이 없다는 점이며, 둘째, 무선 단말기 사용자가 콘텐츠를 구입하기 전에 맛보기를 위한 간편하고 효과적인 방법을 갖고 있지 못하다는 점이다. 따라서 OMA DRM Version 1.0은 Forward-lock과 맛보기 기능뿐만 아니라 좀 더 포괄적인 개념의 DRM을 제안하는데 초점을 맞추었다. 실제로, OMA DRM은 Forward-lock, Combined delivery, 그리고 Separate delivery의 세 가지 방식을 정의한다.

OMA는 디지털 권리 표현 언어를 정의하기 위해 XML기반의 ODRL을 채택했다. ODRL은 e-books, 음악, 오디오, 그리고 소프트웨어 형태의 디지털 콘텐츠와 함께 사용될 수 있으며 라이센스에 대한 제약사항 없이 사용 가능하다. OMA DRM Version 1.0 규격에서는 콘텐츠 전달방식, 포맷, 권리 명세, 다운로드 방식 등에 대한 명세가 이루어졌다.[4][5]

III. 무선 DRM 시스템 구조 및 기능

본 논문에서 제안된 DRM 시스템의 보호범위는 다음과 같다.

- 인증서를 이용한 전자서명 생성 및 검증, 암/복호화
- 불법 콘텐츠 배포의 부인 방지
- 저작권 자동 지불 시스템
- PKI기반의 권한정보 처리 기법 활용으로 위변조 방지
- 콘텐츠의 사용권한 제한 : 읽기 회수 및 사용기간 제어, 인쇄 제어, 문서 전달 제어
- 설정된 사용 권한이 종료되면 자동 파기
- Copy & Paste 방지, Drag & Drop 방지, 화면 캡쳐 방지, 저장 방지 등

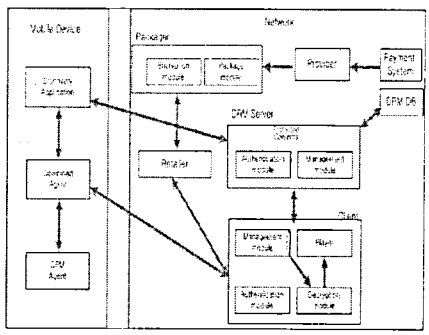

그림 1 제안된 무선 DRM 시스템

본 논문에서 제안된 DRM 시스템의 기능 및 구조는 다음과 같다.

OMA 다운로드의 기본구조는 presentation server와 download server, contents storage를 논리적으로 분리하고 있다. 그러나 presentation server에 아무런 특정 기능을 두지 않고, download server와 download server에 집중된 배치 구조와 분산된 배치 구조 모두 가능하도록 한다. 뿐만 아니라 승인되고 신뢰성 있는 구현을 통해 서버 엔티티와 클라이언트 기기 간에 법적 책임을 물을 수 있는 교류가 발생하도록 한다. 또한 다운로드는 콘텐츠 종류에 구애받지 않도록 한다. OMA 다운로드 모델은 HTTP 다운로드 메커니즘에 이 문서에 제시된 여러 성질을 추가한다. 여기에는 콘텐츠 협상을 위한 추가적인 도구와 프로토콜에 독립적으로 잘 정의된 META 데이터 표현과 응용계층의 설치의 확인 등이 포함된다. 협상 모델은 다운로드가 데이터 객체가 디바이스로 전달되는 단계로 진행되고 있는 지에 대해 클라이언트 장비와 사용자 모두가 평가할 수 있도록 한다. Download Descriptor의 몇 가지 특성이 다운로드 에이전트로 하여금 현재 클라이언트 기기상의 사용 가능한 자원과 다운로드 될 미디어 객체를 표현하는 메타 데이터를 비교하도록 한다.

- 사용자 신뢰성과 인증 문제

DRM 시스템에서 End-User 사이에서 허위사용자나 신뢰할 수 있는 사용자인지를 확인하고 자신의 신분을 증명할 수 있는 시스템 개발하고자 한다. 이러한 기능은 허가 받지 않은 사용자의 접속이나 위장접속의 문제를 해결할 수 있는 기능

이다. 이러한 문제를 해결하기 위해서 PKI를 이용하여 신분을 확인토록 하는 프로그램을 개발한다. PKI를 이용하여 상대방의 인증을 함으로써 신뢰성 있는 콘텐츠 공유를 할 수있다.

· 불법 콘텐츠 배포의 부인방지

많은 불법 자료들이 인터넷을 통하여 배포되고 있다. 이러한 문제는 법적으로도 문제가 있는 만큼 불법 자료 배포자에 대한 증거를 확보할 수 있는 기능이 제공되어야 한다.

· 저작권 해결 문제

현재 저작권 콘텐츠 자료의 불법 유통으로 인하여 사회적 물의를 일으키고 있다. 디지털 시장이 커짐에 따라 이러한 불법 행위의 단속은 점점 힘들어 지고 있다. 또한 현재의 디지털 환경상 저작권료 지불에 대한 뚜렷하고, 안전한 방법이 없다.

· 불법 다운로드 및 고의적 접속 차단자의 해결

AES 알고리즘을 이용하여 디지털 콘텐츠를 보호한다. 데이터 전송시 AES 알고리즘을 이용하여 암호화한 후, 완료시 마지막에 인증된 전송받은 사용자의 공개키를 이용하여 키값을 전송하는 구조로 설계한다. 이러한 방법은 고의적인 접속 차단자뿐만 아니라, 불법적인 도청 및 해킹을 방지할 수 있다.

· 불법 복사 방지 및 불법 배포 등 실행 제한 기능

콘텐츠의 복사나 배포, 불법 사용에 제한을 가할 수 있는 기능은 콘텐츠에 제한적 사용 옵션이 설정되어 있는 경우, DRM 시스템이 사용자 컴퓨터의 고유 정보를 이용하여 킷값을 생성 암호화하여 저장한다. 제한 옵션이 설정되어 있는 콘텐츠의 경우 실행을 위해서는 반드시 DRM 프로그램을 이용하여 복호화하여 실행되게 한다. 이러한 콘텐츠는 만약 본인이 사용하여 제한된 사항을 전부 소진하였다 하여 쓸모 없게 되더라도, DRM 시스템을 이용하여 타인에게 배포할 수 있다. 제한 옵션에는 '몇 번만 실행', '몇 번 복사 가능', '복사 불가', 등의 정보가 들어 있다.

Ⅳ. 콘텐츠 보호시스템의 동적디코딩 기술 설계

프로그램의 전체를 암호화하여 실행을 위한 메모리 로딩시 복호화 하는 자동 보호 기술과는 달리 콘텐츠의 동적 디코딩 기술은 프로그램의 실행중에 특정영역만을 복호화 하는 기술로 블록의 실행 후 메모리에서 제거하는 기술이다. 따라서 함수의 위치 및 내용을 쉽게 추출하지 못하여 소프트웨어의 불법적인 분석 시도를 어렵게 한다. 본 논문에서 제안한 알고리즘의 유효성은 어떤 기업 자체의 노하우에 속하는 기술의 구현에 있어서 알고리즘의 보호가 필요할 경우 보다 강력하게 보호하기 위한 적용에서 효과적이며, 루틴의 접근 빈도에 따른 프로그램의 수행 시간의 부하를 줄이기 위한 방법이 병행 구현되어야 한다. 이를 해결한 방법으로 제3의 보안 모듈 관리용 서비스 프로그램에 의해 일정시간만큼만 복호화 된 채로 보관하고, 그 경과 후 다시 원상태로 인코딩하는 방법을 사용한다.

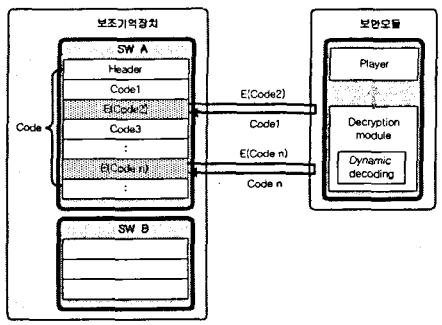

그림 2 콘텐츠의 동적 디코딩 과정

이 경우 자주 사용되는 블록은 계속 디코딩 된 채로 보관되게 되면 자주 사용되지 않으면 다시 디코딩을 해 놓게 된다. 따라서 매우 자주 호출하게될 때 발생되는 시스템 폭주를 예방할 수 있다.

· **Protect Macro**

Protect Macro 란 App. 동적 디코딩을 위한 자동 복호화 제어용 함수를 매크로 형태로 제공함으로써 보호하고자 하는 프로그램의 제작단계에서 매크로의 추가만으로 자동 복호 회로가 갖추어 지게 된다. 이와 함께 대상 프로그램의 컴파일 후 Macro를 포함하는 함수의 암호화를 수행하여야 한다. 이때 Index Macro 가 함수의 위치를 찾는데 사용된다.

그림은 Protect Macro를 적용한 함수의 기본 모양이다. 보호하고자 하는 함수의 시작에 MACRO_PROTECT_CODE 매크로를 호출하면 매크로는 장치를 통해서 INDEX_MACRO_START와 INDEX_MACRO_END로 묶여 있는 구간을 모듈을 통해서 복호화를 수행한다. 또한 함수의 리스트를 장치관리자에 보내서 원하는 시간 후에 복호화 값을 지우게 할 수 있다. 장치 핸들은 장치관리자에게 반납하여야만 다른 블록에서 사용을 할 수 있다.

```
func ProtectedFunc
begin
        MACRO_PROTECT_CODE
        INDEX_MACRO_START
        :
        Original Algorithm code
        :
        INDEX_MACRO_END
end
```

```
MACRO_PROTECT_CODE macro
        GetDeviceHandle()
        AddFuncList()
        DeviceSet()
        FuncUnPack()
        PutDeviceHandle()
        macro end
```

그림 3 Protect Macro의 적용 후의 함수

· **Index Macro**

Index Macro란 Protect Macro가 수행될 때 복호화 하여야 할 함수의 범위를 지시하는 역할을 하는 것이다.

```
INDEX_MACRO_START macro
        predefined string 1
        macro end

INDEX_MACRO_END macro
        predefined string 2
        macro end
```

그림 4 Index Macro

V. 결 론

본 논문에서 제안한 콘텐츠 보호를 위한 동적 디코딩 기법은 어떤 기업 자체의 노하우에 속하는 기술의 구현에 있어서 알고리즘의 보호가 필요할 경우 보다 강력하게 보호하기 위한 적용에서 효과적이며, 루틴의 접근 빈도에 따른 프로그램의 수행 시간의 부하를 줄이기 위한 방법이 병행 구현되어야 한다. 이를 해결한 방법으로 제3의 보안 모듈 관리용 서비스 프로그램에 의해 일정 시간만큼만 복호화 된 채로 보관하고, 그 경과 후 다시 원상태로 인코딩 하는 방법을 사용한다. 본 논문에서 설계한 DRM 콘텐츠의 동적 디코딩 기법은 창조자, 저작권자, 제공업자, 유통업자, 사용자 등 유통 주체 모두가 안전하고 효율적이면서 경제적인 방법으로 콘텐츠를 제작 유통, 소비할 수 있는 기반이 되며 콘텐츠 유료화에 따른 과세/통계 처리 등을 위한 투명한 전자 상거래 인프라로 활용되어 디지털 콘텐츠 제작과 전자상거래 분야의 활성화뿐만 아니라 콘텐츠 유통과 관련된 산업 전 분야에 활용될 수 있을 것으로 기대된다.

감사의 글

본 연구는 산업자원부의 지역혁신 인력양성 사업의 연구결과로 수행되었음.

참고문헌

[1] Intel, "Content Protection in the Digital Home", Volume 06, Issue 04, Intel Technology Journal, 2002/11/15

[2] Michael Ripley, "Utilizing Content Protection Technologies", Intel Developer Forum, 2002/09/12

[3] Intel, "Advanced Digital Set Top Box Design - White Paper Revision 1.0", 2003/09

[4] Ahmet M. Eskicioglu, "MULTIMEDIA PROTECTION IN DIGITAL NETWORKS", CNIS 2003, 2003

[5] Matei Ripeanu, "Peer-to-Peer Architecture Case Study: Gnutella Network", techreports TR-2001-26, University of Chicago, July, 2001.