情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

안전한 디지털 저작권 관리를 위한 디지털 포렌식 모델 제안

장 의 진[1†], 정 병 옥[2], 임 형 민[3], 신 용 태[1‡]
[1]숭실대학교, [2](주)디지캡, [3]파주시청

A Proposal for Digital Forensic Model for Secure Digital Rights Management

Ui-jin Jang[1†], Byung-ok Jung[2], Hyung-min Lim[3], Yong-tae Shin[1‡]
[1]Soongsil University, [2]DigiCAPS, [3]Paju City

요 약

유비쿼터스 환경은 디지털 홈 기기들이 시간과 공간에 제약을 받지 않는 멀티미디어 서비스를 제공한다. 하지만, 디지털 콘텐츠의 사적복제 보장을 통한 콘텐츠의 이용 편리성 보장(Fair Use)이 이루어지지 않고 콘텐츠의 무차별적인 배포와 불법 콘텐츠의 사용 등으로 인해 피해를 주고 있는 것이 현실이다. 이러한 문제점을 해결하기 위해 등장한 DRM 시스템은 단말기에 저장된 라이선스의 보호와 콘텐츠의 재배포에 따른 라이선스 관리를 수행하지 못하는 문제점이 있다. 본 논문에서는 유비쿼터스 환경에서 DRM 시스템의 문제점을 해결하기 위한 대안으로서 콘텐츠와 라이선스에 대한 오용행위 감사 및 불법 대규모 유통을 사전에 차단하고 법적 대응을 위해 디지털 증거 생성 및 관리가 가능한 디지털 포렌식 모델을 제안한다.

ABSTRACT

The devices for the digital home in ubiquitous environment aim at providing multimedia services which are not limited to the time and space. However, it does not ensure the fair use of digital contents and causes damage to the contents providers because of indiscriminate distribution of digital contents and the use of illegal contents. DRM system for solving this problems cannot protect the license stored on digital home devices and manage license by redistribution of contents. In this paper, digital forensic model that enables the misuse detection and previous interception of large-scale illegal distribution for contents and license, and also enables the creation and management of digital evidence for legal countermeasure.

Keywords : Digital Forensic, DRM, Ubiquitous home

Ⅰ. 서 론

유비쿼터스 환경은 디지털 홈 기기들이 시간과 공간에 제약을 받지 않는 멀티미디어 서비스를 제공한다. 하지만, 이러한 멀티미디어 서비스 환경에서는 사용자의

접수일 : 2008년 8월 18일; 수정일: 2008년 10월 7일;
채택일 : 2008년 10월 24일
† 주저자, neon7624@gmail.com
‡ 교신저자, shin@ssu.ac.kr

Fair Use가 이루어지지 않고 콘텐츠의 무차별적인 배포 및 불법 콘텐츠의 사용 등으로 인해 막대한 피해를 주고 있다. 이러한 문제점을 해결하기 위해 등장한 DRM 시스템은 단말 인증이나 암호 알고리즘에 의한 보호에만 의존하여 단말기에 저장된 라이선스의 보호와 콘텐츠의 재배포에 따른 라이선스 관리가 되지 않는다는 문제점이 있다. 본 논문에서는 DRM 시스템의 문제점을 해결하기 위한 대안으로서 콘텐츠와 라이선스에 대한 오용행위 감사 및 불법 대규모 유통을 사전에 차단하고 법적 대응을 위해 디지털 증거 생성 및 관리가 가능한 디지털 포렌식 모델을 제안한다. 본 논문의 구성은 다음과 같다. II장에서는 제안 모델의 요구사항을 설명하고 III장에서는 제안하는 디지털 포렌식 모델에 대한 설명, IV장에서는 제안하는 모델과 타 DRM 시스템을 비교 평가한다. 마지막으로 V장에서는 결론과 함께 향후 연구방향에 대해 설명한다.

Ⅱ. 제안 모델의 요구사항

유비쿼터스 환경에서의 디지털 포렌식 모델은 다양한 디지털 홈 기기들이 디지털 홈 네트워크를 통하여 콘텐츠 공유 등이 가능해야 하므로 아래와 같은 조건을 만족하여야 한다[1-4].

- 라이선스 정보 수집

유료 콘텐츠의 경우 홈 네트워크에서는 Fair Use에 한하여 콘텐츠를 자유롭게 공유 및 사용할 수 있어야 한다. 따라서 해당 콘텐츠에 대한 라이선스의 공유 및 이동, 배포 및 수정 등에 따른 라이선스 정보 수집이 가능해야 기기 인증이나 사용자 인증 등을 통해 안전하게 관리될 수 있다.

- 콘텐츠와 디바이스의 유연한 인증 체계

유비쿼터스 홈 네트워크에서 사용자 및 디바이스의 인증은 각각의 위치 변화에 따라 유연하게 인증 처리가 되어야 한다. 즉 위치 변화에 따라 인증을 반복하는 메커니즘 보다는 사용자가 등록한 도메인 내에서는 한번의 인증으로 모든 콘텐츠를 편리하게 이용할 수 있는 Single Sign-On 메커니즘이 요구된다.

- 사용 권한(usage rule) 관리와 콘텐츠의 재배포 (super-distribution)

유비쿼터스 홈 네트워크 환경에서는 DMB, Cable, IPTV 등을 통해 수신한 방송 콘텐츠에 대하여 PVR (Personal Video Recorder) 기능을 수행하기 때문에 각

[표 1] 용어 정의

포렌식 에이전트(Forensic Agent)	DRM 클라이언트 모듈에 있는 Access Controller와 상호 연동하여 DRM 클라이언트 모듈에 저장된 라이선스 및 환경을 모니터링 하는 주체
포렌식 매니저(Forensic Manager)	포렌식 데이터베이스에 수집된 Alert 로그를 분석하고 사용자가 보유한 디지털 콘텐츠와 라이선스 침해에 대한 증거 확보 및 보고서를 생성하여 관리하는 주체
포렌식 데이터베이스(Forensic Database)	Alert 로그 관리를 위한 데이터베이스
라이선스 관리 서버(License Management Server)	라이선스 발급 및 라이선스 정보를 관리하는 DRM 관련 서버
라이선스 발급 서버(License Issuer Server)	라이선스를 발급하는 주체
DRM 클라이언트 모듈	콘텐츠의 재생을 담당하는 모듈
Access Controller	포렌식 에이전트로부터 수신한 정보를 통해 라이선스와 디지털 콘텐츠의 사용을 제한하는 기능 제공
포렌식 에이전트 프로파일(Forensic Agent Profile)	DRM 클라이언트 모듈에 저장되어 있는 라이선스의 불법 위·변조 즉 라이선스의 무결성(Integrity)을 확인하기 위해 라이선스 파일과 비교되는 대상 프로파일
라이선스 해시 프로파일(License Hash Profile)	라이선스의 무결성 검사를 위한 프로파일
Alert 로그	라이선스가 저장된 폴더로 신뢰된 DRM 클라이언트 모듈의 접근/수정/추가/삭제/이동/복사/파일 열기 등의 시스템 콜이 확인될 경우 발생되는 로그
Access Controller 메시지	DRM 클라이언트가 디지털 콘텐츠의 사용을 위하여 해당 라이선스 파일 접근을 위해 전송하는 메시지
Alert Event 메시지	라이선스 해시 프로파일이 정상으로 확인되지 않을 경우 발생되는 메시지

기 다른 디바이스로의 Copy Protection 및 Set-top box의 사용자 이용 정책을 고려하여야 한다.

- 라이선스 접근제어(Access Control) 지원

유비쿼터스 환경에서 사용자가 보유한 저장장치는 여러 사람에게 공유되는 기기일 가능성이 높다. 따라서 사용자의 저장장치에 저장된 콘텐츠는 사용이 가능한 라이선스에 대해 접근제어 기능을 제공하여 사용자별로 사용권한을 부여할 수 있도록 해야 한다.

- 라이선스 위 · 변조에 따른 대응

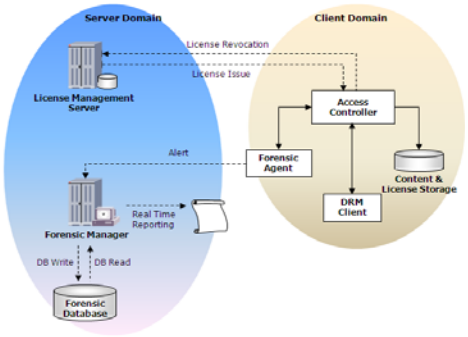
일반적인 DRM 시스템은 콘텐츠를 불법적으로 사용하지 못하게 하는 알고리즘은 제공하지만 불법적으로 사용된 콘텐츠(혹은 라이선스)에 대한 대응 기능은 제공하지 못한다.

2.1 용어 정의

디지털 포렌식[5-6] 모델을 제안하는데 사용되는 용어를 [표 1]에 정의한다.

2.2 제안 모델의 구성객체

디지털 포렌식 모델은 라이선스의 불법 사용과 대응을 위하여 포렌식 에이전트(Forensic Agent), 포렌식 매니저(Forensic Manager), 포렌식 데이터베이스(Forensic Database)로 구성하였으며, 단말은 콘텐츠 사용을 담당하는 DRM 클라이언트 모듈과 라이선스 상태 및 보안 감사를 수행하는 Forensic Agent로 구성하였다. [그림 1]은 디지털 포렌식 모델구성과 각 객체간의 관계를 도식화한 것이다.



[그림 1] 디지털 포렌식 모델의 기본 구성

2.2.1. 포렌식 매니저, 포렌식 데이터베이스 및 라이선스 관리 서버

포렌식 매니저는 포렌식 에이전트의 접속을 분산시키고 데이터베이스에 보안감사 로그 저장 및 실시간 통계 Transaction 만을 담당하여 처리한다. 또한, 포렌식 관리 데이터베이스에 수집된 Alert 로그를 등급에 따라 분석하고 실시간으로 모니터링하여 사용자가 보유한 디지털 콘텐츠 및 라이선스의 침해 사실에 대해서 증거를 확보한다. 확보된 증거를 기반으로 연관성과 가독성 있는 보고서를 생성하여 관리한다. 포렌식 매니저는 누적된 보안위협을 고려하여 수집된 로그를 분석하고 대응이 필요한 수준의 이벤트 발생 시 라이선스 및 디지털 콘텐츠의 사용제한 제어신호를 포렌식 에이전트에게 전송한다. 포렌식 에이전트는 해당 정보를 DRM 클라이언트의 Access Controller에게 통보하여 해당 라이선스나 디지털 콘텐츠의 사용을 제한한다.

포렌식 데이터베이스는 Alert[7] 로그 관리를 수행하며, 라이선스 관리 서버는 라이선스 발급 및 라이선스 정보를 관리한다.

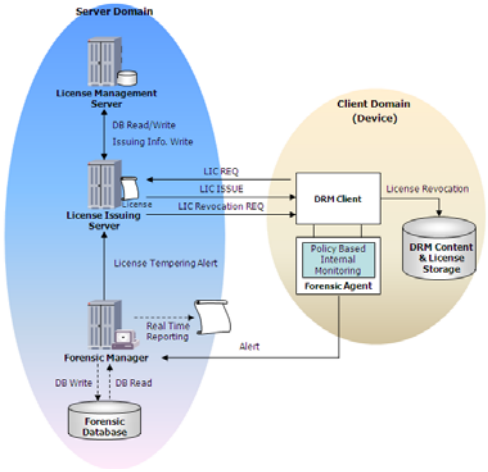
2.2.2 포렌식 에이전트, DRM 클라이언트 모듈 및 Access Controller

포렌식 에이전트는 DRM 클라이언트 모듈의 Access Controller와 상호 연동하여 DRM 클라이언트에 존재하는 라이선스 및 단말기의 환경을 감시하며, 원격의 포렌식 매니저와 연동하여 Alert 발생 시 해당 로그를 보고하고, 포렌식 매니저의 제어신호를 처리한다. DRM 클라이언트는 DRM이 적용된 콘텐츠를 복호화하여 재생하는 기능을 담당하는 모듈로서, 콘텐츠 구매 시 발급받은 라이선스를 확인하여 사용자의 콘텐츠 사용을 제어하는 기능을 수행한다. Access Controller는 포렌식 에이전트로부터 수신한 정보를 통해 라이선스와 디지털 콘텐츠의 사용을 제한하는 기능을 제공한다.

III. 디지털 포렌식 모델

디지털 포렌식 모델은 유비쿼터스 홈 네트워크 환경에서 사용자 단말기의 미디어 콘텐츠에 대한 저작권 보호기능 유지 및 라이선스 관리를 수행한다. 개인의 정보보호를 위해서 모니터링 대상에 대한 정보는 콘텐츠 사

용자에게 충분히 공지되어야 하며 사용자의 동의를 얻어야만 모니터링 될 수 있도록 한다. [그림 2]는 제안한 DRM 시스템과 디지털 포렌식 시스템과의 논리적 시스템 연동 구조를 나타낸 것이다.



[그림 2] 디지털 포렌식 모델의 논리적 구성도

사용자 단말기에서는 콘텐츠의 재생을 담당하는 DRM 클라이언트와 라이선스의 상태 및 보안 감사를 수행하는 포렌식 에이전트가 운용된다(1).

Forensic_Agent={Msg_Type||Directory||License_File_Name||Active_Type} (1)

포렌식 에이전트는 단말기가 부팅되는 시점부터 종료되는 시점까지 실행되며 단말기에 저장된 라이선스의 불법 위·변조에 대응하는 방안으로 라이선스 해시 프로파일을 생성한다(2). 이는 발급된 라이선스의 무결성을 위한 프로파일이다.

License_Hash_Profile={ID, Time|| Type|| Hash} (2)

라이선스 파일과 라이선스 해시 프로파일은 주기적으로 비교하여 라이선스의 무결성을 검사하고, 두 값이 상이할 경우 해당 라이선스는 현재 단말기에 접속한 사용자의 Account에 의해서 공격을 당한 것으로 판단하여 Alert를 발생한다. 포렌식 에이전트는 라이선스 보안 감사를 위해서 라이선스의 공격 시나리오에 대한 System Call Signature 정보로 이루어진 Rule-Set 구조를 갖는다. 포렌식 에이전트는 신뢰된 DRM 시스템 이외에 라이선스가 저장된 폴더로 접근·수정·추가·삭제·이동·복사·파일 열기에 대한 시스템 콜이 확인되면 Rule-Set의 Signature와 비교하여 해당하는 Signature의 Alert 로그를 발생한다(3)[8].

Alert_Log={Phy_Addr||Logi_Addr||Account||Date||Res_ID||ID_type||Alert_Type||RS-Class_Type||RS=FSID} (3)

DRM 클라이언트는 콘텐츠를 사용하기 위해 대응하는 라이선스 파일에 접근하여 라이선스 권한(Usage Count, Usage Duration)과 권리(Contents Encryption Key)를 획득해야 한다. 라이선스 파일에 접근하기 위해서는 포렌식 에이전트로 Access Controller 메시지를 전송하고 라이선스를 사용한다(4). 사용 후에는 동일한 형식의 메시지를 포렌식 에이전트에게 통보하여 보안감사에서 예외로 Alert를 발생시키지 않는다.

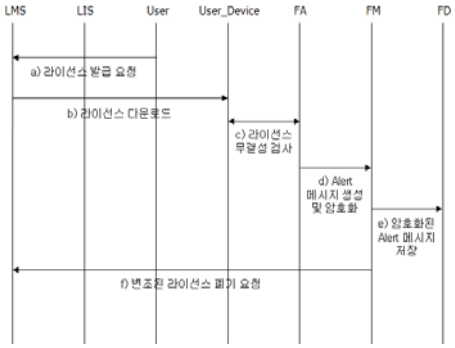
Access_Controller_Msg={Time||User_Account||License_ID||Msg_Type||Rev} (4)

'HASH Profile Miss-Match' 와 'Rule-Set Signature Identity' 이벤트가 발생한 경우 포렌식 에이전트는 Alert 로그를 Alert Event 메시지의 형태로 생성한다(5).

Alert_Event_Msg={Date||License_ID||User_Account||Alert_Class_Type||Alert_Signature_ID} (5)

생성된 Alert 로그는 사용자 단말기가 오프라인일 경우 포렌식 매니저의 공개키로 암호화 하여 보관하고, 온라인이 되는 시점에서 VOD나 스트리밍 서비스를 위해 포렌식 매니저로 전송된다. 포렌식 매니저는 수신한 Alert 로그를 포렌식 데이터베이스의 Alert 테이블에 저장하고, 보고된 사용자의 Account별 Abnormally User 테이블에 Alert 로그별로 설정된 보안 위협 등급에 따라 누적 관리한다. 보안 위협 등급은 제안 모델을 평가하기 위해 라이선스 위·변조를 최상위 등급으로 하고 그 이하는 임의로 설정하였다. 포렌식 매니저의 관리자에 의해 설정된 Thread-Hold 이상으로 보안 위협 Point가 누적되면, 해당 사용자의 Account와 라이선스를 라이선스 발급 서버(License Issuer Server) 및 라이선스

관리 서버(License Management Server)와 연동하여 사용자가 라이선스를 재발급 받도록 폐기한다. 사용자는 라이선스 재발급 및 재등록을 통해 콘텐츠를 정상적으로 이용할 수 있다. 사용자는 라이선스 관리 서버에게 원하는 콘텐츠에 대한 라이선스를 요청하고 다운로드 받은 라이선스는 주기적으로 라이선스 해시 프로파일과 비교하여 무결성을 검사한다. 사용자는 라이선스 변조 등의 의심이 생기면 Alert을 발생하고 이를 포렌식 매니저에 안전하게 보고, 관리될 수 있도록 암호화한다. 변조가 확인된 라이선스는 폐기 시나리오를 거치고, 폐기된 라이선스는 재발급 등의 절차를 거쳐 정상적으로 사용할 수 있다. 변조된 라이선스에 대한 로그 수집 절차는 [그림 3]과 같다.



[그림 3] 라이선스 로그 수집 절차

a) User(멀티미디어 콘텐츠와 라이선스의 소비자)는 라이선스 관리 서버에게 선택한 콘텐츠에 대한 라이선스를 요청한다.
b) User는 라이선스 발급 서버를 통해 User가 선택한 콘텐츠의 라이선스를 다운로드한다.
c) User_Device에 다운로드 된 라이선스는 FA (Forensic Agent)가 생성한 라이선스 해시 프로파일과 비교하여 무결성을 검사한다.
d) 라이선스와 라이선스 해시 프로파일의 값이 상이할 경우 FA는 Alert 메시지를 생성하고 FM(Forensic Manager)에게 안전하게 보고 및 관리될 수 있도록 Alert 메시지를 암호화하여 전송한다.
e) FM은 수신한 Alert 메시지를 FD(Forensic Database)에 저장한다.
f) FA는 LMS(License Management Server)에게 변조가 확인된 라이선스에 대한 폐기 요청을 하고 사용자가 폐기된 라이선스를 재발급 받을 수 있도록 한다.

IV. 결과 분석

기존 DRM 환경에서는 암호화 알고리즘을 적용하여 배포한 콘텐츠와 라이선스에 대한 유통 추적 및 관리가 어렵고 단말기에 저장된 콘텐츠와 라이선스에 대한 사용자의 접근이 용이하여 보안 위협 발생 가능성이 높다는 문제가 있었다. 제안 모델은 라이선스와 콘텐츠의 보안 취약점을 이용해 사용자가 공격을 시도하여 보안요소를 해제하고 콘텐츠와 라이선스를 불법 유통할 경우 효과적으로 제한할 수 있으며, 콘텐츠와 라이선스의 불법 사용을 사전에 차단하여 사용자의 라이선스를 안전하게 보호할 뿐만 아니라 콘텐츠의 Fair Use가 가능하다. 유비쿼터스 환경에서 재생산된 라이선스에 대한 안전한 관리를 위해서는 포렌식 알고리즘이 적용되어야 하며, 타 DRM 시스템의 경우에는 II에서 제시한 요구사항을 만족하기 어렵다. 따라서 본 논문에서는 DRM 라이선스의 위·변조등과 같은 위협요소를 해결하기 위해 DRM에 적용 가능한 포렌식 모델을 제시함으로써 기 도출된 문제점을 해결하고자 하였다. [표 2]는 제안 시스템과 타 DRM 시스템을 비교한 결과이다.

[표 2] 제안시스템 비교 평가

요구사항	OMA DRM	WMRM	제안 시스템
일관된 포렌식 절차에 의한 라이선스 정보 수집	x	x	○
자동화된 증거 수집	x	x	○
라이선스 Policy를 통한 정보 수집의 연동 지원	x	x	○
라이선스 접근제어 (Access Control) 지원	x	x	○
디바이스 인증 지원	○	○	○
라이선스 불법/사용 대응 기능	x	○	○
라이선스 사용현황 리포팅 기능	x	x	○

(지원가능 : O, 지원불가 : X)

V. 결 론

본 논문에서는 포렌식 에이전트 및 포렌식 수신 서버와 DRM 시스템을 연동하여 라이선스의 발급에서 폐기까지 전 유통 라이프 사이클에 대한 관리가 가능하고, 라이선스에 대한 불법적인 보안 위협을 관리하여 라이선스 공격에 대응할 수 있는 모델을 제안하였다. 제안 모델은 Access Control을 이용한 사용자의 접근 제한을 통해 향후 유비쿼터스 환경에서도 라이선스에 대한 보안 적용이 유연하다. 또한, 기존 DRM 기술보다 한 단계 발전하여 디지털 콘텐츠의 불법 유통을 예방하고 사건 발생 후 불법유통 사실에 대한 부인봉쇄 기능을 통해 라이선스와 콘텐츠에 대한 감사 로그를 법적 증거로 이용하여 저작자의 권리와 창작을 보장하며 향후 다양한 디지털 디바이스에서의 사적사용을 보장하기 위한 메커니즘을 제공한다. 향후 제안 시스템의 구성요소에 대한 세부 기능 추가 및 포렌식 에이전트와 포렌식 수신 서버의 연동을 구체화하고 제안 시스템의 비교 평가표를 세분화하여 제안 시스템의 기능을 좀 더 효과적으로 동작하도록 하는 연구가 필요하다.

참고문헌

[1] DMP: TIRAMISU IST-2003-506983 DRM Requirements, 2004.

[2] http://www.openmobilealliance.org, OMA-DRM-REQ-v2_0-20030515-C.pdf, 2003.

[3] MPEG-21 Overview v.5, ISO/IEC JTC1/SC29/WG11 N5231, Shanghai, 2002.

[4] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, “Digital rights management for content distribution,” AISW2003, 2003.

[5] Warren G, Kruse II, Jay G.Heiser, “COMPUTER FORENSICS: Incident Response Essentials,” Addison Wesley, 2001.

[6] Kevin Mandia, Chris Prosise, Matt Pepe, “Incident response and computer forensics, Second Edition”, McGraw-Hill, 2003.

[7] RFC 3227 Guidelines for Evidence Collecting and Archiving.

[8] Seok-Hee Lee, “A Study of Memory Information Collection and Analysis in a view of Digital Forensics in Window System”, Center for Information Technologies, Korea University, 2006.2.