한국항행학회 논문지 제13권 제3호 2009년 6월

홈네트워크 환경에서의 안전한 DRM 시스템을 위한 라이센스 감사 모델

A License Audit Model for Secure DRM System in Home Network Environment

장의진*, 정병옥**, 여상수***, 신용태*

Ui-Jin Jang*, Byung-Ok Jung**, Sang-Soo Yeo*** and Yong-Tae Shin*

요 약

홈 네트워크 환경에서는 디지털 홈 기기들이 시간과 공간에 제약을 받지 않는 멀티미디어 서비스를 제공하는 것을 목적으로 한다. 하지만, 적법하게 콘텐츠를 구입한 사용자의 사적사용(fair use)을 보장하지 못하고 콘텐츠의 무차별적인 배포 및 불법 콘텐츠의 사용 등으로 인해 피해를 주고 있는 것이 현실이다. 이러한 문제점을 해결하기 위해 등장한 DRM 시스템은 단말기에 저장된 라이센스에 대한 보호나 재배포에 따른 라이센스 관리를 수행하지 못한다는 문제점을 갖는다. 이를 위해 본 논문에서는 홈 네트워크 환경에서 콘텐츠의 안전한 유통을 위하여 라이센스에 대한 사용자의 불법 접근 및 수정, 불법 재배포에 대한 오용행위 감사 및 서버로의 로그 리포팅 기능을 수행하는 라이센스 감사 모델을 제안한다.

Abstract

Digital home devices aims at providing the multimedia service which is not limited at time and space in home network environment. However, it is incapable of the fair use of consumers who legally buys contents, and causes damage to the contents providers owing to the indiscriminate distribution and use of illegal contents.

DRM system appeared to solve this problem cannot protect the license stored on digital home devices and manage license by redistribution. This paper proposes a license audit model which makes an inspection of illegal access, modification and redistribution and reports alert logs to server.

Key words : DRM, Digital Forensic, Ubiquitous Computing

I. 서 론

홈 네트워크 환경에서는 디지털 홈 기기들이 시간과 공간에 제약을 받지 않는 멀티미디어 서비스를 제공하는 것을 목적으로 한다. 하지만, 적법하게 콘텐츠를 구입한 사용자의 사적사용(fair use)을 보장하지 못하고 콘텐츠의 무차별적인 배포 및 불법 콘텐츠의 사용 등으로 인해 피해를 주고 있는 것이 현실이다.

이러한 문제점을 해결하기 위해 기존 유선 환경에서는 DRM 기술을 디바이스에 적용하였으나, 보유

* 숭실대학교 컴퓨터학부
** (주)디지캡 기술연구소
*** 목원대학교 컴퓨터공학부 전임강사
· 교신저자 (Corresponding Author) : 여상수
· 투고일자 : 2009년 3월 25일
· 심사(수정)일자 : 2009년 3월 26일 (수정일자 : 2009년 4월 23일)
· 게재일자 : 2009년 6월 30일

라이센스에 대한 보호나 재배포에 따른 라이센스 관리가 이루어지지 않고 단말 인증이나 암호 알고리즘에 의한 보호에만 의존하고 있어 라이센스의 발급에서 폐기까지의 라이프 사이클 내에서의 이용에 대해서는 관리가 되지 않는다는 문제점이 존재했다.

본 논문에서는 이러한 문제점을 해결하기 위하여 라이센스에 대한 사용자의 불법 접근, 불법 수정, 불법 재배포에 대하여 오용행위 감사를 하고, 불법적인 시도에 대한 로그를 서버에 보고하여 향후 불법 사용자의 접근을 차단할 수 있는 증거 수집 및 사후 관리까지 가능한 라이센스 감사 모델을 제안하고자 한다.

본 논문의 구성은 다음과 같다. II장에서는 디지털 홈 환경에서의 안전한 콘텐츠 보호를 위한 기반 기술 및 연구동향에 대해 살펴보고, III장과 IV장에서는 제안 모델인 라이센스 감사 모델의 설계, 프로토콜 구현 및 분석에 대해 설명한다. 마지막으로 V장에서는 본 연구의 결과와 향후 과제에 대하여 설명한다.

Ⅱ. 관련 연구

2-1 Finger Printing

핑거프린팅 기술은 인간의 지문처럼 콘텐츠에 저작권 정보를 삽입해서 나중에 이 저작권 정보(지문)로 사용자가 누구인지를 확인할 수 있게 한다. 이는 디지털 콘텐츠에 사용자에 대한 정보를 은닉함으로써 출력물이나 디지털 콘텐츠로부터 유출자에 대한 정보를 추출하여 불법행위를 추적하게 하는 기술로서 콘텐츠에 저작권자 또는 판매자의 정보를 삽입하는 워터마킹 기술과는 달리, 핑거프린팅은 콘텐츠를 구매한 사용자의 정보를 삽입하는 기술이다. 따라서 유통과정에서 거치게 되는 여러 구매자의 정보를 삽입함으로써 콘텐츠의 유통 경로와 개인 식별까지 추적할 수 있으므로 불법적인 콘텐츠의 유통을 한층 더 방지할 수 있다. 방송에서 상업광고의 방영 여부는 광고주의 주요 관심사이며 계약과 일치되게 방영되고 있는지 알고 싶어 하는데 이러한 방송 모니터링에서도 핑거프린팅 기술이 활용된다. 또한 정부기관의 전자문서 인증 서비스, 신용카드사의 소득공제서류 인증 서비스, 항공티켓 발권 서비스에 활용되며 P2P, 웹 하드 등에서 유통되고 있는 MP3, 영화 등의 불법 복제 콘텐츠의 추적에도 적용된다.

2-2 권리 표현을 위한 언어

3C SGML WG에서 제안되고 Content Guard에 의해 개발된 XrML은 현재 가장 많이 사용되는 XML 기반의 저작권 표현 언어이다. XrML은 디지털 콘텐츠 및 웹 서비스와 관련된 권리와 조건들을 표현하고, 저작권자, 콘텐츠 제공자, 사용자간에 권리항목들의 표준을 제정하기 위한 목적에서 시작되었다[1]. 콘텐츠 제공자는 XrML을 이용하여 사용자에게 특정 권한을 부여할 수 있고 모든 권한에 대해서 사용기간과 조건을 명시할 수 있으며, 사용기간과 사용 권한에 따른 과금이 가능하다. ODRL은 콘텐츠에 대한 권리 정보를 표현하기 위해 정의된 표준 언어로써, 권리언어를 표현하는 ODRL Expression Language와 데이터 사전에 들어가는 요소들을 정의하는 ODRL Data Dictionary가 표준화의 대상이며, 모두 XML schema를 사용하여 표현된다[2].

2-3 Digital Forensic

디지털 포렌식(Digital forensic)은 “정보처리 기기 등 디지털 소스로부터 각종행위에 대한 사실관계를 확정하거나 증명하기 위해 필요한 디지털 증거를 보존(Preservation). 수집(Collection), 증명(Validation), 식별(Identification), 분석(Analysis), 해석(Interpretation), 기록(Documentation), 제출(Presentation)하기 위하여 과학적으로 이끌어내고 증명하는 방법”이라고 정의할 수 있으며, “컴퓨터 등 디지털 기기를 매개로 이루어지는 행위에 대한 법적인 증거자료를 확보하기 위하여 컴퓨터 시스템과 네트워크 등 디지털 소스로부터 정보를 수집, 분석 및 보존절차를 통하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위”로 정의할 수 있다. 최근의 컴퓨터 포렌식(Computer Forensic)은 컴퓨터를 이용한 범죄뿐만 아니라 컴퓨터와 네트워크 등을 목표로 하는 범죄를 예방하고, 범죄가 발생하면 적절한 절차에 의해 디지털 증거를 수집하여 민·형사상 책임을 지울 수 있도록 법적 효력이 있는 증거로 가공하여 재판 결과에 적용하기 위

해 제출하는 일련의 과정을 포함한다.

2-4 DRM

DRM(Digital Rights Management)은 콘텐츠의 생성, 보관, 유통, 사용, 폐기에 이르는 전체 라이프 사이클에 걸쳐 콘텐츠의 저작권을 지속적으로 보호하기 위한 기술이다[3]. 기존의 DRM 기술은 디바이스에 저장된 콘텐츠를 대상으로 하며 암호화, 인증, 콘텐츠 패키징, 권리표현 기술, 탬퍼링 방지 기술 등을 이용하여 콘텐츠를 보호했으나, 디지털 홈 환경에서 서비스 되는 콘텐츠를 보호하기 위해서는 기존 DRM 기술 외에 스트리밍 콘텐츠의 보호, 도메인 권한 관리, DRM 기술 간 상호 연동 등이 지원되어야 한다[4]. 스트리밍 콘텐츠의 보호는 일대일 서비스를 목적으로 하는 VOD 콘텐츠용 DRM 기술과 여러 명의 사용자에게 동시에 서비스되는 멀티캐스트 콘텐츠용 DRM 기술로 구분한다. 현재 ISMA, OMA, DVB 등에서 표준화가 완료되었거나 진행 중에 있다. DRM 기술 간 상호 연동은 서로 다른 DRM 기술 간의 상호 호환성을 보장하는 기술로서 DMP 및 MPEG-21에서 표준화가 진행되고 있으며, 국내에서는 ETRI에서 DRM 호환 기술인 EXIM 기술을 개발하였다. 도메인 권한 관리는 사적복제 보장을 통한 콘텐츠의 이용 편리성 보장(fair use)을 지원하기 위해 사용자가 사용하는 기기들(도메인)간의 자유로운 콘텐츠 이용 및 배포를 허가하는 기술로 OMA, MPEG-21, DVB, DMP 등에서 표준화가 진행 중에 있다[5][6].

III. 제안 모델의 구성

3-1 용어 정의

디지털 포렌식을 제안하는데 사용되는 용어를 [표 1]에 정의한다[7][8].

표 1. 용어 정의
Table 1. Terms and Definition

구성요소		기능
기본	포렌식	DRM 클라이언트 모듈의 Access
구성객체	에이전트	Controller와 상호 연동하여 DRM 클라이언트 모듈에 저장된 라이센스 및 단말 환경을 모니터링 하는 주체
	포렌식 매니저	포렌식 데이터베이스에 수집된 Alert 로그 분석, 사용자가 보유한 디지털 콘텐츠와 라이센스 침해에 대한 증거 확보 및 보고서 생성·관리 기능 제공
	포렌식 데이터베이스	Alert 로그 관리를 위한 데이터베이스
	라이센스 관리 서버	라이센스 발급 및 라이센스 정보를 관리하는 DRM 관련 서버
	라이센스 발급 서버	라이센스를 발급하는 주체
	DRM 클라이언트 모듈	콘텐츠의 재생을 담당하는 모듈
	Access Controller	포렌식 에이전트로부터 수신한 정보를 통해 라이센스와 디지털 콘텐츠의 사용을 제한하는 기능을 제공
포렌식 에이전트 프로파일		DRM 클라이언트 모듈에 저장된 라이센스의 무결성(Integrity)을 확인하기 위해 라이센스 파일과 비교되는 대상 프로파일
라이센스 해시 프로파일		라이센스의 무결성 검사를 위한 프로파일
Alert 로그		라이센스가 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 라이센스 파일접근을 위해 전송하는 메시지
Alert Event 메시지		라이센스 해시 프로파일이 정상으로 확인되지 않을 경우 발생되는 메시지

3-2 제안모델의 구성객체

라이센스 감사 모델은 서버와 클라이언트로 구분한다. 서버 측에는 라이센스의 불법 사용과 대응을 위하여 포렌식 매니저(Forensic Manager), 라이센스 관리 서버(License Management Server), 라이센스 발급 서버(License Issuing Server), 포렌식 데이터베이스(Forensic Database)로 구성하였으며, 단말 측에는 콘텐츠의 사용을 담당하는 DRM 클라이언트 모듈과 라이센스 상태 및 보안 감사를 수행하는 포렌식 에이전트(Forensic Agent)로 구성하였다. [그림 1]은 라이센스 감사 모델의 구성 및 구성 요소 간 연동을 나타낸 것이다[9].

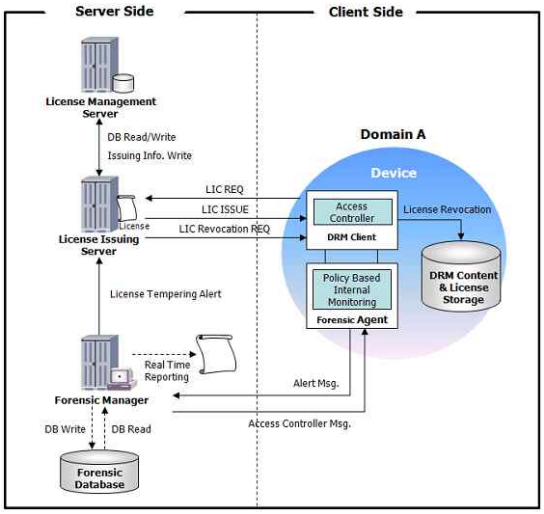


그림 1. 라이센스 감사 모델의 구성도
Fig. 1. The configuration of license audit model

3-2-1 포렌식 매니저, 포렌식 데이터베이스, 라이선스 발급 및 관리 서버

포렌식 매니저는 포렌식 에이전트의 접속을 분산시키고 데이터베이스에 보안감사 로그 저장 및 실시간 통계 Transaction 만을 담당하여 처리한다. 또한, 포렌식 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 로그 관리를 수행하며, 라이선스 관리 서버는 라이선스 발급 및 라이선스 정보를 관리한다.

3-2-2 포렌식 에이전트, DRM 클라이언트 모듈 및 Access Controller

포렌식 에이전트는 DRM 클라이언트 모듈의 Access Controller와 상호 연동하여 DRM 클라이언트에 존재하는 라이센스 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 라이센스를 확인하여 사용자의 콘텐츠 사용을 제어하는 기능을 수행한다. Access Controller는 포렌식 에이전트로부터 수신한 정보를 통해 라이센스와 디지털 콘텐츠의 사용을 제한하는 기능을 제공한다.

Ⅳ. 관련 연구

라이센스 감사 모델은 홈 네트워크 환경에서 사용자 단말기의 미디어 콘텐츠에 대한 저작권 보호기능 유지 및 라이센스 관리를 수행한다. 개인의 정보보호를 위해서 모니터링 대상에 대한 정보는 콘텐츠 사용자에게 충분히 공지되어야 하며 사용자의 동의를 얻어야만 모니터링 될 수 있도록 한다. 제안 모델의 주요 구성요소인 포렌식 매니저와 포렌식 에이전트의 동작 흐름은 [그림 2]와 같다.

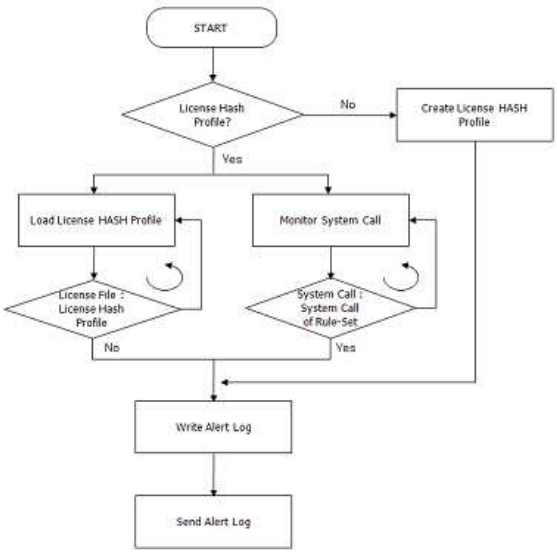


그림 2. 포렌식 에이전트의 흐름도
Fig. 2. The flow of Forensic Agent

포렌식 에이전트가 실행되면 사용 중인 라이센스 해시 프로파일이 존재하는지 확인을 한다. 이전에 사용 중이던 라이센스 해시 프로파일이 존재하지 않는

경우 라이센스 해시 프로파일을 생성하고, 생성 이유에 대한 Alert를 기록하여 포렌식 매니저로 Reporting을 한다. 라이센스 해시 프로파일이 존재하고 정상으로 확인이 되면, 라이센스 해시 프로파일을 로드하여 라이센스 디렉토리의 라이센스 파일들과 해시 항목을 주기적으로 검사 한다.

라이센스 해시 프로파일이 존재하고 정상으로 확인이 되면, 시스템 콜 모니터링을 수행하여 시스템의 시스템 콜을 검사한다. 획득한 시스템 콜들은 Rule-Set에 기록된 System Call Signature와 비교 검사를 수행한다. Rule-Set에는 보안 위협의 패턴을 저장하고 있는 정보의 집합으로 비정상적인 활동을 탐지하는데 이용한다. 시스템 콜이 수집될 때 마다 Rule-Set의 System Call Signature와 일치하는지 주기적으로 검사한다. 라이센스 해시 프로파일과 일치하지 않는 항목이 탐지되는 경우에는 탐지 이유에 대한 Alert Log를 기록하고, 포렌식 매니저로 Reporting을 한다. 시스템 콜 모니터링을 수행하는 중에 Rule-Set의 System Call Signature와 일치하는 항목이 탐지되면 비정상 행위로 간주한다. 비정상 행위로 판단한 이유를 Alert Log에 기록하고, 포렌식 매니저로 Reporting을 한다[10][11]. [그림 3]은 포렌식 매니저의 동작 흐름을 나타낸 것이다.

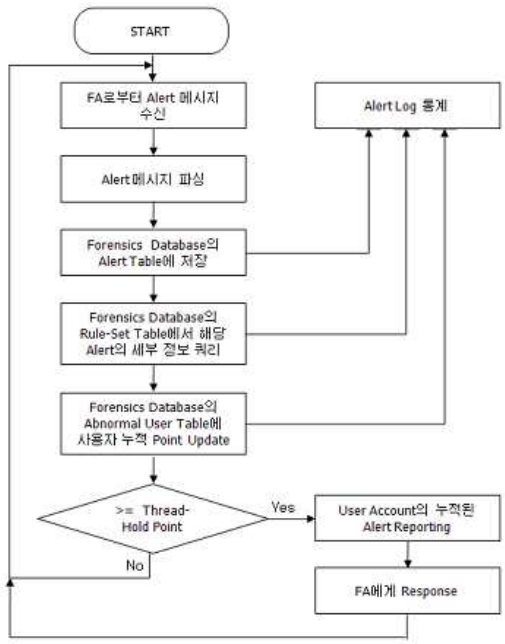


그림 3. 포렌식 매니저의 흐름도
Fig. 3. The flow of Forensic Manager

4-1 로그 수집 절차

사용자 단말기에서는 콘텐츠의 재생을 담당하는 DRM 클라이언트와 라이센스의 상태 및 보안 감사를 수행하는 포렌식 에이전트(1)가 운용된다.

$$Forensic\_Agent=\{Msg\_Type||Directory||License\_File\_Name||Active\_Type\} \quad (1)$$

포렌식 에이전트는 단말기가 부팅되는 시점부터 종료되는 시점까지 실행되며 단말기에 저장된 라이센스의 불법 위/변조에 대응하는 방안으로 라이센스 해시 프로파일(2)을 생성한다. 이는 발급된 라이센스의 무결성을 위한 프로파일이다.

$$License\_Hash\_Profile=\{ID||Time||Type||Hash\} \quad (2)$$

라이센스 파일과 라이센스 해시 프로파일은 주기적으로 비교하여 라이센스의 무결성을 검사하고, 두 값이 상이할 경우 해당 라이센스는 현재 단말기에 접속한 사용자의 Account에 의해서 공격을 당한 것으로 판단하여 Alert을 발생한다. 포렌식 에이전트는 라이센스 보안감사를 위해서 라이센스의 공격 시나리오에 대한 System Call Signature 정보로 이루어진 Rule-Set 구조를 갖는다. 포렌식 에이전트는 신뢰된 DRM 클라이언트 모듈 이외에 라이센스가 저장된 폴더로 접근·수정·추가·삭제·이동·복사·파일 열기에 대한 시스템 콜이 확인되면 Rule-Set의 Signature와 비교하여 해당하는 Signature의 Alert 로그(3)를 발생한다.

$$Alert\_Log=\{Phy\_Addr||Logi\_Addr||Account||Date||RS\_ID||ID\_type||Alert\_Type||RS\_Class\_Type||RS\_FSID\} \quad (3)$$

DRM 클라이언트는 콘텐츠를 사용하기 위해 대응하는 라이센스 파일에 접근하여 라이센스 권한(Usage Count, Usage Duration)과 권리(Contents Encryption Key)를 획득해야 한다. 라이센스 파일에 접근하기 위해서는 포렌식 에이전트로 Access Controller 메시지(4)를 전송하고 라이센스를 사용한

다. 사용 후에는 동일한 형식의 메시지를 포렌식 에이전트에게 통보하여 보안감사에서 예외로 Alert를 발생시키지 않는다.

$$Access\_Controller\_Msg=\{Time||User\_Account||License\_ID||Msg\_Type||Rev\} \quad (4)$$

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

$$Alert\_Event\_Msg=\{Date||License\_ID||User\_Account||Alert\_Class\_Type||Alert\_Signature\_ID\} \quad (5)$$

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 Abnormal User 테이블에 Alert 로그별로 설정된 보안 위협 등급에 따라 누적 관리한다. 보안 위협 등급은 제안 모델을 평가하기 위해 라이센스 위·변조를 최상위 등급으로 하고 그 이하는 임의로 설정하였다. 포렌식 매니저의 관리자에 의해 설정된 Thread-Hold 이상으로 보안 위협 Point가 누적되면, 해당 사용자의 Account와 라이센스를 라이센스 발급 서버(License Issuer Server) 및 라이센스 관리 서버(License Management Server)와 연동하여 사용자가 라이센스를 재발급 받도록 폐기한다. 사용자는 라이센스 재발급 및 재등록을 통해 콘텐츠를 정상적으로 이용할 수 있다. 사용자는 라이센스 관리 서버에게 원하는 콘텐츠에 대한 라이센스를 요청하고 다운로드 받은 라이센스는 주기적으로 라이센스 해시 프로파일과 비교하여 무결성을 검사한다. 사용자는 라이센스 변조 등의 의심이 생기면 Alert을 발생하고 이를 포렌식 매니저에 안전하게 보고 및 관리될 수 있도록 암호화한다. 변조가 확인된 라이센스는 폐기 시나리오를 거치고, 폐기된 라이센스는 재발급 등의 절차를 거쳐 정상적으로 사용할 수 있다. 변조된 라이센스에 대한 로그 수집 절차는 [그림 4]와 같다[12].

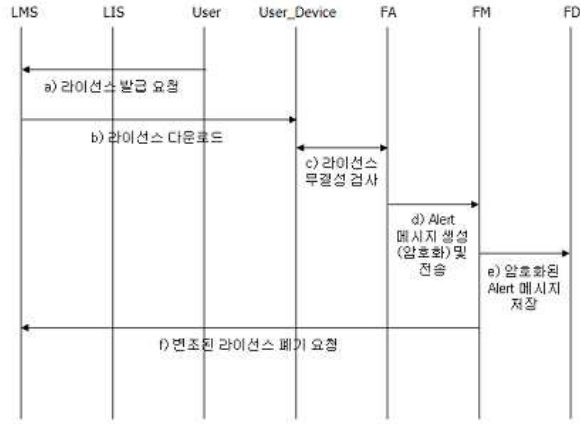


그림 4. 라이센스 로그 수집 절차
Fig. 4. The gathering process of license log

step 1 : User(멀티미디어 콘텐츠와 라이센스의 소비자)는 라이센스 관리 서버에게 선택한 콘텐츠에 대한 라이센스를 요청한다.

step 2 : User는 라이센스 발급 서버를 통해 선택한 콘텐츠의 라이센스를 다운로드한다.

step 3 : User_Device에 다운로드 된 라이센스는 FA(Forensic Agent)가 생성한 라이센스 해시 프로파일과 비교하여 무결성을 검사한다.

step 4 : 라이센스와 라이센스 해시 프로파일의 값이 상이할 경우 FA는 Alert 메시지를 생성하고 FM(Forensic Manager)에게 안전하게 보고 및 관리될 수 있도록 Alert 메시지를 암호화하여 전송한다.

step 5 : FM는 수신한 Alert 메시지를 FD(Forensic Database)에 저장한다.

step 6 : FA는 LMS(License Management Server)에게 변조가 확인된 라이센스에 대한 폐기 요청을 하고 사용자가 폐기된 라이센스를 재발급 받을 수 있도록 한다.

4-2 증거 수집 절차

제안하는 라이센스 감사 모델은 포렌식 에이전트

와 포렌식 매니저와의 연동을 통해 디지털 콘텐츠와 라이센스에 대한 사용자의 불법 접근에 대한 증거 수집 절차를 수행한다. 포렌식 에이전트와 포렌식 매니저와의 연동은 약속된 보안 프로토콜을 사용하여 송·수신되는 메시지를 안전하게 관리한다. 포렌식 에이전트와 포렌식 매니저의 프로토콜 동작방식은 [그림 5]와 같다.

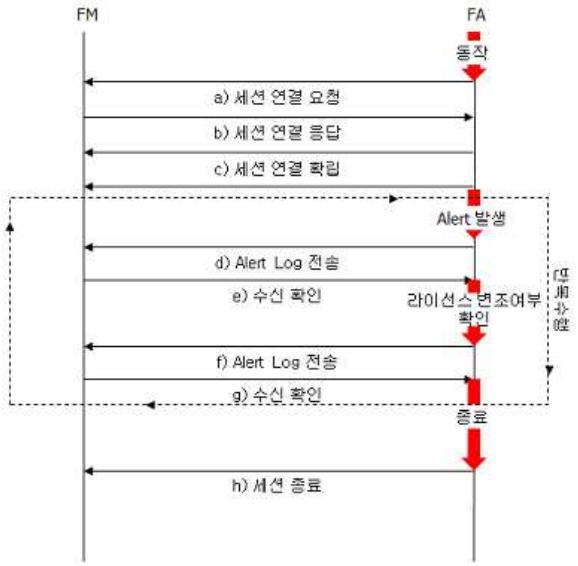


그림 5. 포렌식 에이전트와 포렌식 매니저의 연동
Fig. 5. The interworking of Forensic Agent and Forensic Manager

step 1 : 사용자 단말기가 실행되면 FA(Forensic Agent)가 실행되고 현재 가용한 FM(Forensic Manager)에게 세션 연결을 요청한다.

step 2 : FM은 FA에게 세션 연결 요청을 수락한다.

step 3 : FA와 FM간의 세션 연결이 이루어지고 사용자 단말기가 종료되기 전까지 세션 연결이 유지된다.

step 4 : FA에서 Alert이 발생하면 FA는 FM에게 Alert Log를 전송한다.

step 5 : FM은 수신한 Alert Log에 대한 수신 확인 메시지를 전송한다. FA에서는 라이센스 파일과 라이센스 해시 프로파일의 비교 검사를 통해 변조된 라이센스가 탐지되면 Alert Log를 서버에 전송하고, FM으로부터 수신 확인 메시지를 확인한다.

step 6 : Alert 이벤트가 발생할 때마다 step 4~6의 과정을 반복한다.

step 7 : 사용자 단말기가 종료되거나 시스템이 Off-Line 상태가 되면 연결된 세션은 종료된다.

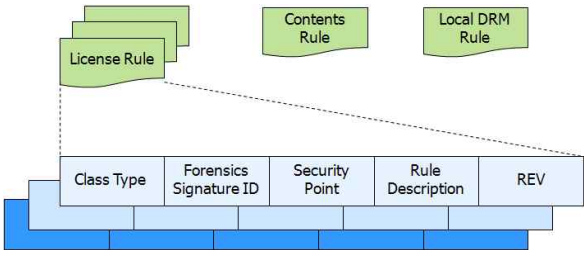


그림 6. Rule-Set 구조
Fig. 6. The structure of Rule-Set

Rule-Set은 포렌식 에이전트와 포렌식 매니저에 존재하는 파일로 보안 위협에 대한 Signature를 모아 놓은 데이터의 집합이다. 포렌식 에이전트는 시스템 콜을 모니터링 하여 Rule-Set 파일에서 일치하는 Signature가 있는지 비교한다. 일치하는 Signature 정보가 탐지되면 보안에 위협하는 행위로 판단하여 Alert Log를 기록하고 포렌식 매니저로 전송한다.

4-3 제안 모델 검증

포렌식 에이전트에서 수집한 정보 상태를 확인하고 대응할 수 있도록 포렌식 매니저와의 통신 및 Alert Log 관리로 구분하여 구성해 보았다. 라이센스 관리 모델 정보는 Local Machine Info, Remote Machine Info, AGENT STATE로 구분되며, 각 정보가 의미하는 것은 다음과 같다.

- Local Machine Info: 현재 로컬 시스템의 네트워크 상태 정보
- Remote Machine Info: 포렌식 수신서버 시스템의 네트워크 연결 정보
- AGENT STATE: 포렌식 에이전트의 프로세스 실행 상태 정보

본 논문에서 제안된 모델의 성능을 테스트해 보기 위해 콘텐츠 라이센스의 권한 조건중 사용 횟수 부분을 50회에서 강제로 100회로 변경해 보았다. 포렌식

에이전트는 라이센스 위·변조 행위 탐지시 포렌식 매니저로 Alert을 전송하고 DRM Client에 대응을 위한 보고를 한다. DRM Client에 통보된 누적된 Alert 정보는 포렌식 에이전트를 통해 확인할 수 있다.

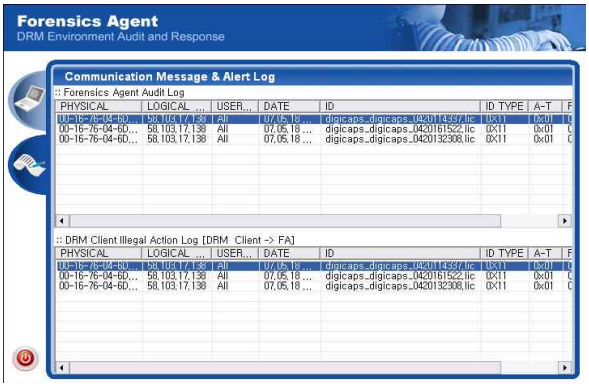


그림 7. DRM Client로 보고한 Audit Log 내역
Fig. 7. Audit log reported to DRM Client

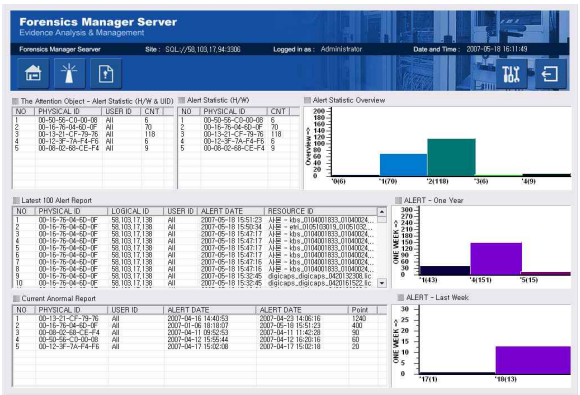
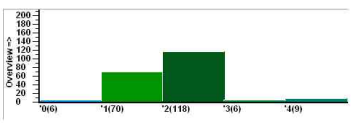


그림 8. 포렌식 매니저의 실행 화면
Fig. 8. The execution screen of Forensic Manager

Overview Report Generator Date : 20070518_162257/

Forensics Management - Overview Report

The Attention Object - Alert Statistic (H/W & UID)



NO	PHYSICAL ID	USER ID	COUNT
1	00-50-56-C0-00-08	All	6
2	00-16-76-04-6D-0F	All	70
3	00-13-21-CF-79-76	All	118
4	00-12-3F-7A-F4-F6	All	6
5	00-08-02-68-CE-F4	All	9

The Attention Object - Alert Statistic (H/W)

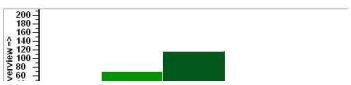


그림 9. HTML 포맷으로 작성된 보고서
Fig. 9. Report written by HTML format

수집된 정보에 대한 리포트를 작성할 경우 보고서 생성 기능을 통해 HTML 형태의 보고서가 생성됨을 확인하였다.

반면 포렌식 매니저는 포렌식 에이전로부터 보고된 정보를 관리하고 리포트를 작성한다.

V. 결과 분석

기존 DRM 환경에서는 암호화 알고리즘을 적용하여 배포한 콘텐츠와 라이센스에 대한 유통 추적 및 관리가 어렵고 단말기에 저장된 콘텐츠와 라이센스에 대한 사용자의 접근이 용이하여 보안 위협의 발생 가능성이 높다는 문제점이 있었다. 제안 모델은 라이센스와 콘텐츠의 보안 취약점을 이용해 사용자가 공격을 시도하여 보안요소를 해제하고 콘텐츠와 라이센스를 불법 유통할 경우 효과적으로 제한할 수 있다. 또한, 콘텐츠와 라이센스의 불법 사용을 사전에 차단하여 사용자의 라이센스를 안전하게 보호할 뿐만 아니라 콘텐츠의 fair use가 가능하다. 홈 네트워크 환경에서 재생산된 라이센스에 대한 안전한 관리를 위해서는 포렌식 알고리즘이 적용되어야 하며, 타 DRM 시스템은 II에서 제시한 요구사항을 만족하기 어렵다. 따라서 본 논문에서는 DRM 라이센스의 위·변조등과 같은 위협요소를 해결하기 위해 DRM에 적용 가능한 라이센스 감사 모델을 제시함으로써 기 도출된 문제점을 해결하고자 하였다. [표 2]는 제안 모델과 타 DRM 시스템을 비교한 결과이다.

표 2. 제안 모델의 비교 평가
Table 2 Comparison and Valuation of the proposed model

요구사항	OMA DRM	WMRM	제안 모델
일관된 포렌식 절차에 의한 라이센스 정보 수집	x	x	○
자동화된 증거 수집	x	x	○
라이센스 Policy를 통한 정보 수집의 연동 지원	x	x	○
라이센스 접근제어 (Access Control) 지원	x	x	○
디바이스 인증 지원	○	○	○

라이센스 불법 사용에 대한 대응 기능	x	○	○
라이센스 사용현황 리포팅 기능	x	x	○

VI. 결 론

본 논문에서는 포렌식 에이전트 및 포렌식 매니저와 DRM 시스템을 연동하여 라이센스의 발급에서 폐기까지 전 유통 라이프 사이클에 대한 관리가 가능하고, 라이센스에 대한 불법적인 보안 위협을 관리하여 라이센스 공격에 대응할 수 있는 모델을 제안하였다. 제안 모델은 Access Control을 이용한 사용자의 접근 제한을 통해 향후 유비쿼터스 환경에서도 라이센스에 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 라이센스와 콘텐츠에 대한 감사 로그를 법적 증거로 이용하여 저작자의 권리와 창작을 보장하며 향후 다양한 디지털 디바이스에서의 사적사용을 보장하기 위한 메커니즘을 제공한다. 향후 라이센스 감사 모델의 구성 객체 간 전송되는 메시지 구성을 구체화하고, 암호 알고리즘에 대한 연구를 통해 효과적으로 동작할 수 있는 실제 구현 모델의 개발이 필요하다고 판단된다.

참 고 문 헌

[1] DMP, "TIRAMISU(IST-2003-506983) DRM Requirements", 2004.

[2] OMA, "OMA DRM Requirements Version 2.0", 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] 최동현, 이윤호, 강호갑, 김승주, 원동호, "재생 공격에 안전한 Domain DRM 시스템을 위한 License 공유방식", *한국정보보호학회 논문지*, 제17권 제1호, pp97-101, 2007.

[6] 김후종, 정은수, 임재봉, "능동형 콘텐츠 지원을 위한 OMA DRM 프레임워크의 확장", *한국정보보호학회 논문지*, 제16권 제5호, pp93-106, 2006.

[7] Warren G, Kruse II, Jay G.Heiser, "COMPUTER forensic: Incident Response Essentials," *Addison Wesley,* 2001.

[8] Kevin Mandia, Chris Prosise, Matt Pepe, "Incident response and computer forensic, Second Edition", *McGraw-Hill*, 2003.

[9] RFC 3227, "Guidelines for Evidence Collecting and Archiving", http://www.faqs.org/rfcs/rfc3227.html. 2002.

[10] Mariusz Burdach, "Forensic Analysis of a Live Linux System I", http://www.securityfocus.com/infocus/1769. 2004.

[11] Mariusz Burdach, "Forensic Analysis of a Live Linux System II", http://www.securityfocus.com/infocus/1773 , 2004.

[12] Seok-Hee Lee, "A Study of Memory Information Collection and Analysis in a view of Digital forensic in Window System", *Center for Information Technologies,* Korea University, 2006. 2.

장 의 진 (Ui-Jin Jang)

1999년 8월 : 숭실대학교 컴퓨터공학과(공학사)

2002년 8월 : 숭실대학교 컴퓨터공학과(공학석사)

2004년 3월~현재 : 숭실대학교 컴퓨터공학과 박사과정

관심분야 : DRM, 디지털 포렌식, 네트워크 보안

여 상 수 (Sang-Soo Yeo)

2001년 2월 : 순천향대학교 컴퓨터공학부(공학사)
2005년 8월 : 중앙대학교 컴퓨터공학과 공학박사
2006년 3월~2007년 2월 : 단국대학교 강의전임강사
2007년 2월~2008년 1월 : 큐슈대학교 정보공학부 방문연구원
2008년 2월~2009년 2월 : (주)비티웍스 연구개발본부 부장
관심분야 : 정보보호 기술 및 정책, 멀티미디어 시스템, 임베디드 시스템

정 병 옥 (Byung-Ok Jung)

2005년 2월 : 대전대학교 컴퓨터공학과 학사
2007년 2월 : 대전대학교 컴퓨터공학과 석사
2006년 10월~현재 : (주)디지캡 기술연구소 연구원
관심분야 : DRM, 디지털 포렌식, 컴퓨터 통신 보안

신 용 태 (Yong-Tae Shin)

1985년 : 한양대학교 산업공학과 졸업
1990년 : Iowa대학교 전자계산학과 석사
1994년 : Iowa대학교 전자계산학과 박사
1995년~현재 : 숭실대학교 컴퓨터학부 교수
관심분야 : 컴퓨터 네트워크, 그룹통신, 분산 컴퓨팅, 인터넷 프로토콜, 초고속 통신망, 전자상거래 기술