Journal of Korea Multimedia Society Vol. 12, No. 4, April 2009(pp. 550-558)

유비쿼터스 환경의 안전한 콘텐츠 유통을 위한 라이센스 관리 모델 연구

장의진[†], 임형민[††], 신용태[†††]

요 약

언제 어디서나 편리하게 네트워크에 접속할 수 있는 유비쿼터스 컴퓨팅 환경에서는 유선 네트워크 환경에서의 디바이스 보다 작고, 경량이며, 값싸고, 이동 가능한 디바이스를 사용한다. 이러한 디바이스를 통해서 시간과 공간에 제약을 받지 않는 멀티미디어 서비스가 제공되지만 멀티미디어 서비스의 주체인 콘텐츠에 대한 사용자의 사적사용이 보장되지 않고 콘텐츠의 대량 불법 복제 및 배포와 무차별적인 사용 등으로 저작권자의 권리를 보호하기에는 어려움이 많은 것이 현실이다. 이러한 문제점을 해결하기 위해 기존 유선 환경에서는 DRM 기술이 적용되었으나 저장된 라이선스에 대한 보호나 재배포에 따른 관리가 이루어지지 않고 단말 인증이나 암호 알고리즘 등의 단순 보호에만 의존하여 라이선스의 생성에서 폐기까지의 총체적 관리가 되지 않는다는 문제가 있다. 본 논문은 디지털 포렌식과 DRM 기술을 연동하여 콘텐츠와 라이센스의 불법 유통을 사전에 차단하고 법적 대응을 위한 증거 생성 및 전체 라이프 사이클에서의 라이센스 보호가 가능한 모델을 제안한다.

A Study on the License Management Model for Secure Contents Distribution in Ubiquitous Environment

Ui Jin Jang[†], Hyung Min Lim[††], Yong Tae Shin[†††]

ABSTRACT

In ubiquitous environment, more small, lightweight, cheap and movable device is used than one device used in wired network environment. Multimedia service which is anytime, anywhere, is provided by device. However, it does not ensure the fair use of multimedia contents and causes damage to the contents providers because of illegal copy and distribution and indiscriminate use of digital contents. For solving this problems, DRM is applied to wired network but it has the problems does not protect stored license and manage license completely because of depending on simple protection such as device authentication and cryptographic algorithm. This paper proposes the license management model using digital forensic and DRM that prevents contents and licenses from distributing illegally and also enables the creation of evidence for legal countermeasure and the protection of license in whole life cycle.

Key words: DRM(디지털 저작권 관리), Digital Forensic(디지털 포렌식), Ubiquitous Environment(유비쿼터스 환경)

1. 서 론

언제 어디서나 편리하게 네트워크에 접속할 수 있는 유비쿼터스 컴퓨팅 환경에서는 유선 네트워크 환경에서의 디바이스 보다 작고, 경량이며, 값싸고, 이동 가능한 디바이스를 사용한다. 이러한 디바이스를

※ 교신저자(Corresponding Author) : 장의진, 주소 : 서울시 동작구 상도5동 1-1(156-743), 전화 : 02)826-0680, E-mail : neon7624@gmail.com
접수일 : 2008년 11월 3일, 완료일 : 2009년 3월 24일
[†] 정회원, 숭실대학교 컴퓨터학부 박사과정
[††] 정회원, 숭실대학교 컴퓨터학부 박사과정
(E-mail : atskyo@gmail.com)
[†††] 숭실대학교 컴퓨터학부 교수
(E-mail : shin@ssu.ac.kr)

통해서 시간과 공간에 제약을 받지 않는 멀티미디어 서비스가 제공되지만 멀티미디어 서비스의 주체인 콘텐츠에 대한 사용자의 사적사용이 보장되지 않고 콘텐츠의 대량 불법 복제 및 배포와 무차별적인 사용 등으로 저작권자의 권리를 보호하기에는 어려움이 많은 것이 현실이다.

이러한 문제점을 해결하기 위해 기존 유선 환경에서는 DRM 기술이 적용되었으나 저장된 라이선스에 대한 보호나 재배포에 따른 관리가 이루어지지 않고 단말 인증이나 암호 알고리즘 등의 단순 보호에만 의존하여 라이선스의 생성에서 폐기까지의 총체적 관리가 되지 않는다는 문제가 있다.

본 논문은 디지털 포렌식과 DRM 기술을 연동하여 콘텐츠와 라이센스의 불법 유통을 사전에 차단하고 법적 대응을 위한 증거 생성 및 전체 라이프 사이클에서의 라이센스 보호가 가능한 모델을 라이센스 관리 모델을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 제안 모델의 요구사항을 설명하고 3장에서는 제안 모델의 구성, 4장에서는 제안 모델의 세부 동작 방식 및 그 절차를 설명하고 5장에서는 제안 모델과 타 DRM 시스템을 제안 모델의 요구사항에 근거하여 분석한다. 마지막으로 6장에서는 결론과 함께 향후 연구방향에 대해 설명한다.

2. 제안 모델의 요구사항

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

(1) 라이센스 정보 수집 - 유료 콘텐츠의 경우 유비쿼터스 홈 환경에서는 사적사용에 한하여 콘텐츠를 자유롭게 공유 및 사용할 수 있어야 한다. 따라서 해당 콘텐츠에 대한 라이센스의 공유 및 이동, 배포 및 수정 등에 따른 라이센스 정보 수집이 가능해야 기기 인증이나 사용자 인증 등을 통해 안전하게 관리될 수 있다.

(2) 콘텐츠와 디바이스의 유연한 인증 체계 - 유비쿼터스 홈 환경에서 사용자 및 디바이스 인증은 각각의 위치 변화에 따라 유연하게 처리가 되어야 한다. 즉 위치 변화에 따라 인증을 반복하는 것이 아닌 사용자가 등록한 도메인 내에서는 한 번의 인증으로 모든 콘텐츠를 편리하게 이용할 수 있는 Single Sign-On 메커니즘이 요구된다[5-6].

(3) 사용 권한(usage rule) 관리와 콘텐츠의 재배포(super-distribution) - 유비쿼터스 홈 환경에서는 DMB, Cable, IPTV 등을 통해 수신한 방송 콘텐츠에 대하여 PVR(Personal Video Recorder) 기능을 수행하기 때문에 각기 다른 디바이스로의 Copy Protection 및 Set-top box의 사용자 이용 정책을 고려하여야 한다.

(4) 라이센스 접근제어(Access Control) 지원 - 유비쿼터스 홈 환경에서 사용자가 보유한 저장장치는 여러 사람에게 공유되는 기기일 가능성이 높다. 따라서 사용자의 저장장치에 저장된 라이센스에 대한 접근제어 기능을 제공하여 사용자별로 사용권한을 부여할 수 있도록 한다.

(5) 라이센스 위변조에 따른 대응 - 일반적인 DRM 시스템은 콘텐츠의 불법적인 사용을 방지하는 알고리즘은 제공하지만 불법적으로 사용된 콘텐츠(혹은 라이센스)에 대한 대응 기능은 제공하지 못한다.

3. 제안 모델의 구성

3.1 용어 정의

라이센스 관리 모델을 제안하는데 사용되는 용어를 표 1에 정의한다[7-8].

3.2 라이센스 관리모델의 구성객체

라이센스 관리 모델은 서버와 단말로 구성한다. 서버는 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, 단말은 콘텐츠의 사용을 담당하는 DRM 클라이언트 모듈과 라이센스 상태 및 보안 감사를 수행하는 포렌식 에이전트(Forensic Agent)로 구성하였다. 그림 1은 라이센스 관리 모델의 구성 및 구성 요소 간 연동을 나타낸 것이다[9].

3.2.1 포렌식 매니저, 포렌식 데이터베이스, 라이센스 발급 및 관리 서버

포렌식 매니저는 포렌식 에이전트의 접속을 분산

표 1. 용어 정의

구성요소		기 능
기본 구성 객체	포렌식 에이전트	DRM 클라이언트 모듈의 Access 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

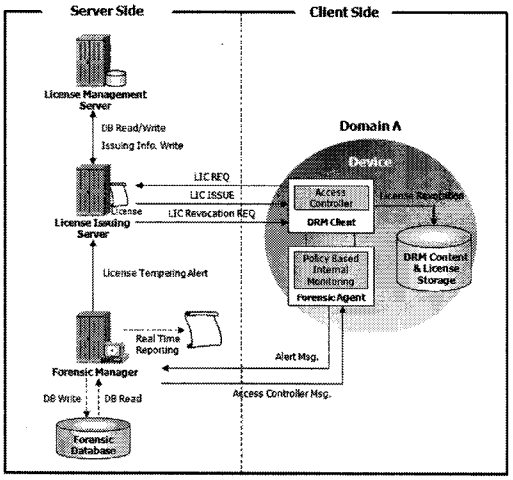

그림 1. 라이센스 관리 모델의 구성

시키고 데이터베이스에 보안감사 로그 저장 및 실시간 통계 트랜잭션만을 담당하여 처리한다. 또한, 포렌식 데이터베이스에 수집된 Alert 로그를 등급에 따라 분석하고 실시간으로 모니터링하여 사용자가 보유한 디지털 콘텐츠 및 라이센스의 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 라이센스 및 디지털 콘텐츠의 사용제한 제어신호를 포렌식 에이전트에게 전송한다. 포렌식 에이전트는 해당 정보를 DRM 클라이언트의 Access Controller에게 통보하여 해당 라이센스나 디지털 콘텐츠의 사용을 제한한다.

포렌식 데이터베이스는 Alert 로그 관리를 수행하며, 라이센스 관리 서버는 라이센스 발급 및 라이센스 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.

4. 제안 모델

라이센스 관리 모델은 유비쿼터스 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 2와 같다.

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 리포팅 한다. 라이센스 해시 프로파일이 존재하고 정상으로 확인이 되면, 라이센스 해시 프로파일을 로드하여 라이센스 디렉토리의 라이센스 파일들과 해시 항목을 주기적으로 검사한다.

라이센스 해시 프로파일이 존재하고 정상으로 확인이 되면, 시스템 콜 모니터링을 수행하여 시스템의

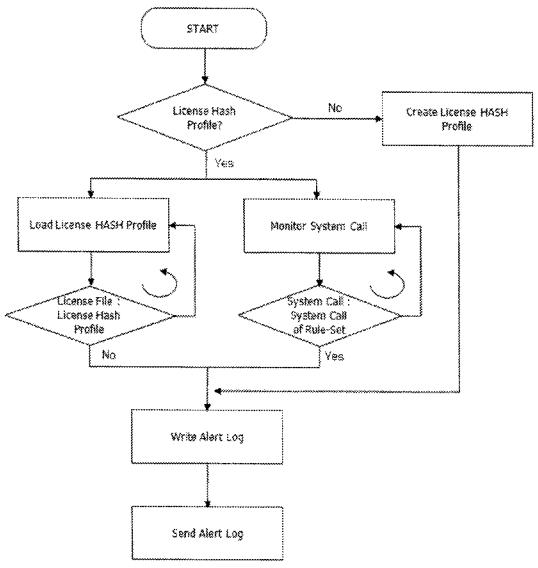

그림 2. 포렌식 에이전트의 흐름도

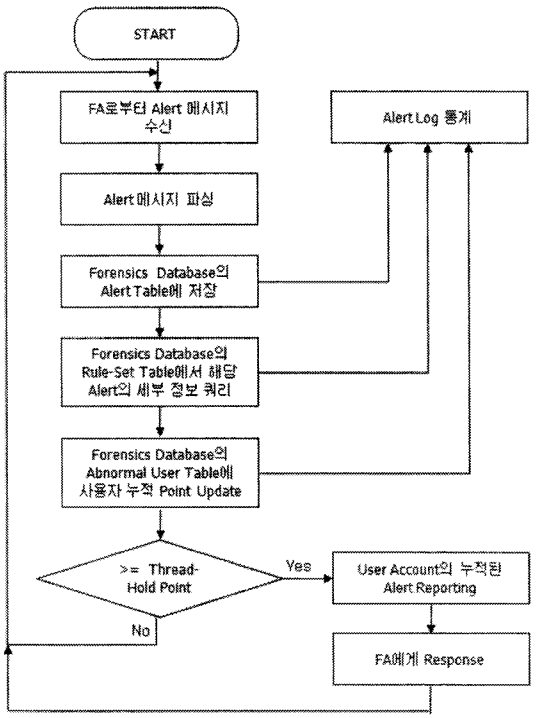

그림 3. 포렌식 매니저의 흐름도

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 리포팅 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 리포팅 한다[10-11]. 그림 3은 포렌식 매니저의 동작 흐름을 나타낸 것이다.

4.1 로그 수집 절차

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

표 2. Forensic_Agent 정의

필드 이름	의 미
Msg_Type	DRM Client에서 발생하는 error code 값
Directory	DRM Client에서 관리하는 라이센스 저장 디렉토리
License_ File_Name	저장된 라이센스의 파일명
Active_Type	접근/수정/추가/삭제/이동/복사/파일 열기와 같은 파일이나 디렉토리의 접근 형태

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

Forensic_Agent는 표 2와 같이 정의한다.

포렌식 에이전트는 단말기가 부팅되는 시점부터 종료되는 시점까지 실행되며 단말기에 저장된 라이센스의 무결성을 위한 프로파일(2)을 생성한다.

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

License_Hash_Profile은 표 3과 같이 정의한다.

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.

표 3. License_Hash_Profile 정의

필드 이름	의미
ID	License_Hash_Profile의 고유 아이디
Time	프로파일 생성일자
Type	대상 프로파일 타입 (예. 라이센스/콘텐츠)
Hash	해당 Rule-Set

표 4. Alert_Log 정의

필드 이름	의 미
Phy_Addr	시스템 고유 하드웨어 식별 번호
Logi_Addr	접속한 포렌식 에이전트가 실행되고 있는 시스템의 주소
Account	Audit Event 발생 시점의 DRM Client 로그인 사용자 계정
Date	Audit Event 발생 '년.월.일 시:분:초'
RS_ID	Audit Object의 파일 이름
ID_Type	탐지된 Resource ID의 타입 정보
Alert_Type	Alert 발생 근거에 대한 타입 정보
RS-Class Type	Event 탐지 근거 룰 집합 타입
RS-FSID	Event 탐지 근거 요소

Alert_Log={Phy_Addr||Logi_Addr||Account||Date||RS_ID||ID_Type||Alert_Type||RS_Class_Type||RS_FSID} (3)

Alert_Log는 표 4와 같이 정의한다.

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 사용한다. 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)

Access_Controller_Msg는 표 5와 같이 정의한다. 'HASH Profile Miss-Match'와 'Rule-Set

표 5. Access_Controller_Msg 정의

필드 이름	의 미
Time	Audit Event 발생 '년.월.일 시:분:초'
User_Account	Audit Event 발생 시점의 DRM Client 로그인 사용자 계정
License_ID	Audit Event가 발생한 파일의 라이센스 ID
Msg_Type	탐지된 Resource ID의 타입 정보
Rev	탐지 룰의 버전

표 6. Alert_Event_Msg 정의

필드 이름	의 미
Date	Audit Event 발생 '년.월.일 시:분:초'
License_ID	Audit Event가 발생한 파일의 라이센스 ID
User_Account	Audit Event 발생 시점의 DRM Client 로그인 사용자 계정
Alert_Class_ Type	Event 탐지 근거 룰 집합 타입
Alert_Signature_ID	Event 탐지 근거 요소

Signature Identity' 이벤트가 발생한 경우 포렌식 에이전트는 Alert 로그를 Alert Event 메시지(5)의 형태로 생성한다.

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

Alert_Event_Msg는 표 6과 같이 정의한다.

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 관리자가 설정한 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

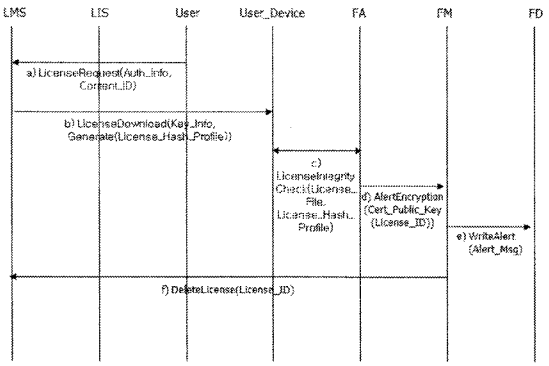

그림 4. 라이센스 로그 수집 절차

시나리오를 거치고, 폐기된 라이센스는 재발급 등의 절차를 거쳐 정상적으로 사용할 수 있다. 변조된 라이센스에 대한 로그 수집 절차는 그림 4와 같다.

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(Forensics Agent)가 생성한 라이센스 해시 프로파일과 비교하여 무결성을 검사한다.

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

Step 5. FM는 수신한 Alert 메시지를 FD(Forensics 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

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

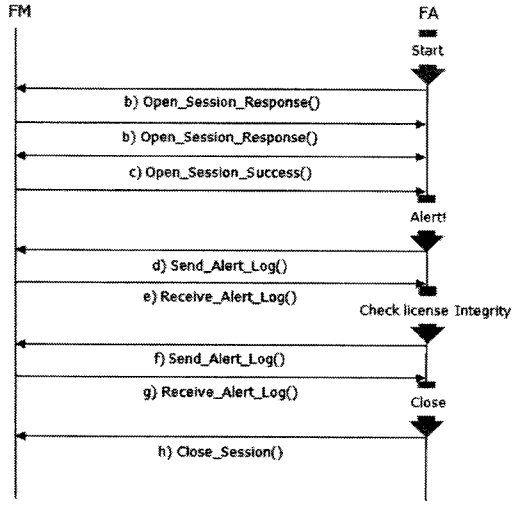

그림 5. 포렌식 에이전트와 포렌식 매니저의 연동

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 6은 라이센스에 대한 무결성 참조를 위해 라이센스 해시 프로파일의 데이터 구조를 도식화한 것이다. 라이센스 해시 프로파일은 가장 최근의 정상적인 라이센스 해시를 보관하며 라이센스를 이용하는 시점에서 정상 라이센스인지 검사하는데 이용한다.

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. Rule-Set의 종류는 표 7과 같다.

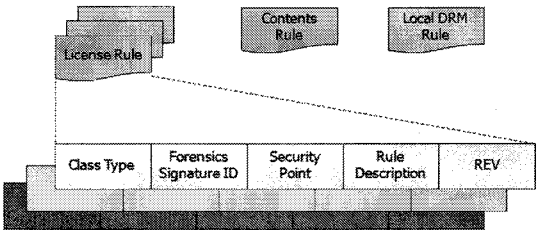

그림 6. Rule-Set 구조

표 7. Rule-Set 정의

룰셋 이름	의미
License_Rule	사용자 디바이스에 저장된 라이센스에 대한 불법적인 접근 및 불법 변경 공격을 탐지하기 위한 공격 Signature 정의
Contents_Rule	불법 콘텐츠의 사용, 불법 배포, DRM 공격시도에 대한 Signature 정의
Local_DRM_Rule	DRM Client에 대한 Tempering 보안 공격 시도 및 어플리케이션 공격 Signature 정의

표 8. License Rule 정의

필드 이름	의미
Class Type	탐지 룰의 분류 ID (0x00~0xFF)
Forensic Signature ID	탐지된 룰의 ID (0x0000~0xFFFF)
Priority Level	탐지된 룰의 보안 레벨 (1~9)
Rule Description	해당 룰에 대한 자세한 설명 (문자열)
REV	예약필드 (N/A)

License_Rule은 표 8과 같이 Class Type, Forensic Signature ID, Security Point, Rule Description, REV 필드로 구성된다.

5. 결과 분석

기존 DRM 기술은 암호화 알고리즘을 적용하여

표 9. 제안 모델 비교 평가

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	○

(지원가능 : O, 지원불가 : X)

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 보안적 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 사적사용이 가능하다는 장점이 있다. 유비쿼터스 환경에서 재생산된 라이센스에 대한 안전한 관리를 위해서는 포렌식 알고리즘이 적용되어야 하며, 타 DRM 시스템은 2장에서 제시한 요구사항을 만족하기 어렵다. 따라서 본 논문에서는 DRM 라이센스의 위·변조등과 같은 위협요소를 해결하기 위해 유비쿼터스 환경에 적용 가능한 라이센스 관리 모델을 제안함으로써 기 도출된 문제점을 해결하고자 하였다. 표 9는 제안 모델과 타 DRM 시스템을 비교한 결과이다.

6. 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 시스템보다 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. 후 라이센스 관리 모델의 구성 객체 간 전송되는 메시지 구성을 구체화하고 암호 알고리즘에 대한 연구를 통해 효과적으로 동작할 수 있는 제안 모델의 구현이 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, "재생공격에 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 FORENSICS: Incident Response Essentials," Addison Wesley, 2001.

[8] Kevin Mandia, Chris Prosise, Matt Pepe, "Incident response and computer forensics, 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 Forensics in Window System," Center for Information Technologies, Korea University, 2006. 2.

장 의 진

1997년 9월~1999년 8월 숭실대 컴퓨터학부 공학사
2000년 9월~2002년 8월 숭실대 컴퓨터학부 공학석사
2004년 3월~현재 숭실대학교 컴퓨터학부 박사과정
2002년 12월~2006년 3월 (주) 디지캡 연구기획팀 과장
관심분야 : 네트워크 보안, 디지털포렌식, DRM, 유비쿼터스 컴퓨팅 & 보안

임 형 민

2001년 숭실대학교 컴퓨터학부 학사
2003년 숭실대학교 컴퓨터학부 석사
2003년~숭실대학교 컴퓨터학부 박사과정
2007년 5월~현재 파주시청 u-City 전문위원
관심분야 : u-City 기획, 서비스개발 및 통합, 공공정책

신 용 태

1985년 한양대학교 산업공학과 학사
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