패밀리 도메인에서 안전한 콘텐츠 배포를 지원하는 라이센스 관리 기법☆

License Management Method supporting secure contents distribution in Family Domain

왕 보 현* 이 병 욱**
Bohyun Wang Byungwook Lee

요 약

DRM 시스템의 재배포 서비스는 디지털 콘텐츠의 배포를 활성화시키는 중요한 요소이다. 그러나 기존 서비스는 재배포 범위를 소비자간으로 국한시키고 있다. 최근, 소비자 요구가 증가하면서 소비자는 자신의 여러 디바이스에서 콘텐츠를 실행하고자 한다. 본 논문에서는 소비자 소유의 디바이스간 재배포 서비스를 지원하는 라이센스 관리 기법을 제안한다. 제안된 기법에서는 소비자가 소유한 디바이스들의 식별 정보를 이용하여 디바이스 인증에 사용되는 도메인 키를 생성하고 라이센스에 저장한다. 디바이스에 변경이 생기면 도메인 키와 라이센스는 갱신된다. 이를 통하여 디바이스간 콘텐츠 배포가 안전하고 효율적으로 이루어 질 수 있도록 한다. 또한 제안된 라이센스 기법은 소비자간의 재배포 서비스에도 적용될 수 있음을 보인다.

Abstract

Superdistribution service of DRM system is an essential part for revitalization of digital contents distribution. However, it limits superdistribution range to superdistribution between consumers. Recently, as the demands of the consumer increase, the consumers want to use the contents in their multiple devices. In this paper, we propose a license management method supporting superdistribution between devices owned by a consumer. The proposed method creates domain key for device authentication by using identification informations of devices owned by a consumer and stores it in license. If devices are changed, domain key and license are updated. Through this method, contents distribution between devices can be achieved securely and efficiently. Also, this license management method can apply to superdistribution between consumers.

☞ Keyword : 패밀리 도메인, DRM, 재배포, 디바이스 식별자, 라이센스, 도메인 키

1. 서 론

DRM 시스템은 디지털 콘텐츠에 대한 저작권 보호에 많은 기여를 하였으며 재배포와 같은 서비스를 통하여 콘텐츠의 신속하고 원활한 유통을 가능하게 하였다. 그러나 기존 서비스에서는 재배포 범위를 소비자 간의 콘텐츠 배포로 국한 시키고 있으며 재배포 받은 소비자는 라이센스를 획득하여 자신의 한 디바이스에서만 콘텐츠를 실행할 수 있다.

미국 저작권법의 공정 사용 원칙(Fair Use Doctrine)에 의하면 소비자가 구매한 콘텐츠를 개인적인 용도로 백업하거나 공유하거나 여러 디바이스에서 자유롭게 이용하는 것은 저작권 위배가 아니다[8]. 그러므로 온라인상의 콘텐츠 유통에서 이러한 소비자 권리들은 보호되어야 하며 이들을 기술적으로 지원하고자 하는 연구들이 진행 중이

* 준 회 원 : 경원대학교 전자계산학과 박사과정
bhwang99@hanmail.net
** 종신회원 : 경원대학교 소프트웨어학부 교수
leebw@kyungwon.ac.kr
[2007/05/29 투고 - 2007/06/18 심사 - 2007/08/28 심사완료]
☆ 본 논문은 2006년도 경기도 차세대성장동력기술개발지원 사업에 의하여 연구되었음

다[5][14].

최근에 소비자 권익 보호에 대한 요구가 증가하면서 소비자들은 자신의 여러 디바이스에서 자유롭게 콘텐츠가 실행될 수 있는 권리를 요구한다[1]. 본 논문에서는 소비자 소유의 여러 디바이스에서 콘텐츠를 안전하고 효율적으로 재배포할 수 있는 라이센스 관리 기법을 제안한다.

제안 기법에서는 소비자가 여러 디바이스에서 안전하게 콘텐츠를 재배포할 수 있도록 디바이스 식별자들을 이용하여 도메인 키를 생성하고, 디바이스 인증을 수행한다. 도메인 키는 라이센스에 저장되고 소비자 소유의 디바이스들에 새로운 디바이스가 추가되거나 기존 디바이스가 제거되면 도메인 키는 변경되며 라이센스도 갱신되어 안전하며 효율적인 디바이스간 재배포를 수행할 수 있도록 한다. 디바이스 식별자를 이용한 도메인 키 정보는 소비자간 안전한 재배포를 위해서도 사용될 수 있다. 이로써 소비자 중심의 안전한 재배포 서비스를 활성화 시킬 수 있다.

2. 관련연구

2.1 디바이스 간 재배포

재배포(superdistribution)는 1983년 Ryoichi Mori에 의해 생성된 용어로서 소프트웨어 제품은 제한 없이 자유롭게 배포될 수 있지만 사용 비용을 지불해야 하고 소프트웨어 제품의 벤더들로부터 제시된 계약사항을 따라야 한다[4]. DRM이 적용된 디지털 콘텐츠 유통에서의 재배포 개념 역시 이와 같다. 콘텐츠는 소비자에 의해 자유롭게 배포될 수 있으나 사용권한은 콘텐츠 제공자의 계약사항에 따라 제한된다. 현재 많이 사용되는 DRM 시스템들은 이러한 전형적인 재배포 서비스의 특징으로 콘텐츠의 재배포가 소비자 간에 이루어 진다. 최근 디지털 콘텐츠 소비자들은 재배포 서비스가 자신이 소유한 디바이스 간에서도 수행될 수 있기를 원한다.

MS사의 WMRM은 라이센스 백업과 복구 기능, 콘텐츠 복사 및 이동 기능 등으로 자신의 여러 디바이스에서 콘텐츠가 실행될 수 있도록 하지만 디바이스의 개수를 엄격히 제한하고 권리를 유동적으로 할당할 수 없도록 함으로써 패밀리 도메인 지원을 제한한다[9].

DRM 표준인 OMA는 Domain이라는 개념으로 패밀리 도메인을 적극 지원하며 네트워크에 연결되지 않은 디바이스 간에도 패밀리 도메인 재배포를 가능하게 하는 메커니즘을 제공한다. OMA의 Domain에서는 하드웨어 식별자를 도메인 키 생성에 이용한다. 도메인을 구성하는 디바이스에 변경이 생겼을 때를 대비하여 이전 도메인 키를 기반으로 한 새로운 도메인 키를 미리 생성해 두는 특징이 있다. 이러한 특징으로 인해 미리 생성해 둔 도메인 키 개수 만큼의 도메인 변화만이 가능하다는 제한이 있다[10].

3G 모바일 폰에 대한 재배포 관련 연구에서는 소비자가 소유한 디바이스들을 패밀리 도메인(family domain)으로 정의하고 안전한 콘텐츠 배포를 위해 패밀리 도메인을 관리하는 기법을 제안한다. 제안된 기법에서는 동일한 개인 키를 이용하여 패밀리 도메인을 관리한다. 이 기법의 단점은 개인 키가 노출되면 패밀리 도메인에 포함되지 않는 디바이스에서도 콘텐츠를 실행할 수 있기 때문에 안전한 패밀리 도메인에서의 재배포가 어렵다는 단점이 있다[1].

홈네트워크에 대한 재배포 관련 연구에서는 개인이 소유한 디바이스들을 인증된 도메인(authorized domain)으로 정의한다. 이 기법은 네트워크가 연결되지 않은 디바이스 간에도 재배포가 가능하다. 인증된 도메인에서는 도메인 관리 키가 각 디바이스 마다 다르다. 이들 키는 마스터 디바이스 키 목록에 저장되어 있고 디바이스가 도메인에 추가될 때마다 목록에 있는 키를 하나씩 할당한다. 이 기법의 단점은 키가 부족하면 인증된 도메인을 다시 등록하고 마스터 디바이스 키 목록을 재 생성해야 하므로 효율적인 디바이스간

재배포가 어렵다. 또한 도메인 관리 키가 노출되면 인증된 도메인에 포함되지 않은 디바이스에서도 콘텐츠 실행이 가능하다는 단점이 있다. 그러므로 안전하며 효율적인 디바이스 간 재배포를 지원할 수 있는 관리 기법이 요구된다[2].

2.2 디바이스 식별자

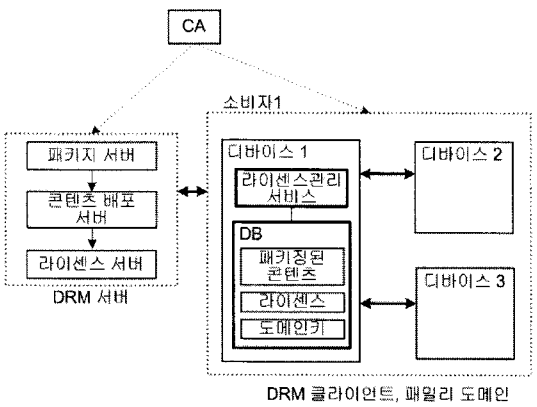
디지털 콘텐츠 이용에 있어서 인증은 중요한 기술이다. 인증에는 사용자 인증과 디바이스 인증이 있다. 둘 다 궁극적으로는 사용자 인증이 목적이지만 디바이스 인증은 콘텐츠가 실행될 디바이스를 제한하고자 하는 것에 초점을 두고 있다. 사용자 인증을 위한 식별정보로는 ID/PASSWORD, 인증서의 공개 키, 이메일 주소 정보, 지문, 홍채와 같은 생체 정보 등을 사용할 수 있다.

디바이스 인증을 위한 식별정보로는 IMEI(International Mobile Equipment Identification)나 IMSI (International Mobile Subscriber Identity), 그리고 MAC 주소 등이 있다. 디바이스의 일련 번호는 디바이스가 존재하는 한 변경되지 않기 때문에 IMEI로써 사용될 수 있다. 일련 번호는 주로 콘텐츠를 특정 디바이스에서만 사용하도록 규정할 때 사용된다. 디바이스의 모델 번호 또한 IMEI로써 사용될 수 있으며 디바이스와 디바이스에 설치된 소프트웨어의 버전을 식별할 때 사용된다[1][7]. MAC(Media Access Control) 주소값은 모바일 기기 및 데스크 탑에서 사용할 수 있는 네트워 카드의 48비트 하드웨어 주소를 말하며 모든 네트워크 카드가 유일한 값을 갖는다. 그러므로 네트워크가 가능한 모든 기기는 이 주소로써 식별가능하다. 본 논문에서는 추출의 용이성 때문에 MAC 주소 값을 디바이스 식별자로써 활용한다. 그러나 디바이스 식별자는 위에 언급된 어떤 종류의 값으로도 대치될 수 있다.

3. 패밀리 도메인 재배포를 위한 DRM 시스템 모델

본 논문에서는 소비자가 소유한 디바이스들을 [1]에서와 같이 패밀리 도메인으로 정의한다. (그림 1)은 패밀리 도메인에서의 재배포 서비스를 위한 DRM 모델이다. DRM 모델의 특징은 패밀리 도메인에서의 콘텐츠 재배포를 안전하게 관리할 수 있도록 도메인 키를 사용한다는 것과 각 디바이스의 라이센스 관리 서비스를 통하여 패밀리 도메인 재배포가 관리된다는 것이다.

(그림 1)의 DRM 모델은 크게 DRM 서버와 DRM 클라이언트로 나누어진다. DRM 서버는 콘텐츠를 패키징하고 배포하고 라이센스를 발급하는 등의 기능을 수행한다. 각 기능에 따라 패키지 서버, 콘텐츠 배포 서버, 라이센스 서버로 나뉜다. DRM 클라이언트는 콘텐츠를 구매하고 라이센스를 발급받아 콘텐츠를 권리에 따라 실행한다. (그림 1)에서 DRM 클라이언트인 소비자1은 디바이스 세 개로 패밀로 도메인을 구성하고 각 디바이스에서는 라이센스 관리 서비스로 라이센스 요청 및 갱신 등의 관리 작업을 수행한다. DRM 시스템 모델의 각 개체는 CA(Certification Authority)로부터 발급된 공개키/개인키 쌍과 공개키 인증서를 통해 인증된다[3].



(그림 1) 패밀리 도메인을 위한 DRM 모델

(그림 1)의 DRM 모델의 각 세부 구성 요소의 기능은 다음과 같다. DRM 서버의 패키지 서버는

패키징된 콘텐츠를 콘텐츠 배포 서버에게 전송한다. 콘텐츠 배포 서버는 소비자의 요청에 의해 패키징된 콘텐츠에 대한 다운로드 서비스 또는 스트리밍 서비스를 제공한다. 이 때 소비자는 콘텐츠에 대한 지불이 완료된 상태라고 가정한다. 콘텐츠 배포 서버는 라이센스 서버에게 판매된 콘텐츠에 대한 권리 정보를 전송한다. 라이센스 서버는 소비자에게 라이센스를 발급하고 발급된 라이센스를 관리한다. 그리고 패밀리 도메인 재배포 서비스를 관리한다. 재배포 서비스 관리 기능은 패밀리 도메인을 등록하고 소비자로부터 도메인 키를 전달 받아 라이센스에 도메인 키를 저장하고 콘텐츠 암복호화 키를 암호화 하는 등의 역할을 한다. 또 패밀리 도메인에 디바이스가 추가되거나 삭제되면 라이센스를 갱신하는 역할도 포함한다.

소비자1이 콘텐츠를 DRM 서버로부터 구매하고 라이센스를 발급 받으면 라이센스는 디바이스1의 DB에 저장되고 라이센스 관리 서비스가 설치된다. 이 때 소비자1이 패밀리 도메인 권리를 소유한다면 라이센스 관리 서비스는 DRM 서버의 라이센스 서버에게 패밀리 도메인을 등록해 줄 것을 요청한다. 새로운 디바이스인 디바이스2가 추가되어 콘텐츠가 재배포 되면 디바이스1의 라이센스 관리 서비스는 도메인 키를 갱신하고 라이센스 서버에게 갱신된 도메인 키를 전송하고 디바이스2의 라이센스 발급을 요청한다. 또한 라이센스 관리 서비스는 패밀리 도메인의 각 디바이스에서 콘텐츠 실행 전에 라이센스에 있는 도메인 키를 이용하여 디바이스가 올바른 패밀리 도메인 구성원인가를 인증한다. 인증 후에 올바른 디바이스라면 발급된 라이센스에 있는 권리 내역을 집행한다.

4. 패밀리 도메인 재배포를 위한 라이센스 관리 기법

4.1 패밀리 도메인 재배포 요소 정의

패밀리 도메인의 재배포 서비스는 기존의 전형적인 소비자간 재배포 서비스를 기반으로 하여 수행된다. 그러므로 패밀리 도메인 재배포 요소들은 기존 재배포 서비스 요소들을 기반으로 하여 정의될 수 있다.

〔정의 1〕 재배포 주체

재배포 주체 P는 재배포 서비스를 주고 받는 주체를 의미하며 튜플 <p, q>라고 정의한다. p는 콘텐츠를 재배포 한 소비자이며 q는 재배포 받은 소비자이다. p와 q가 같으면 패밀리 도메인의 재배포를 의미한다.

〔정의 2〕 패밀리 도메인 재배포 조건

재배포 조건 S는 튜플 <r, n, dn>이라고 정의한다. r은 재배포 되는 자원을 의미하며, n은 총 재배포 횟수를 의미한다. n이 0이면 재배포를 할 수 없다. dn은 패밀리 도메인에서의 재배포 횟수이다. dn이 0이면 패밀리 도메인에서의 재배포가 불가능하다. dn은 n보다 작거나 같아야 하며 작다면 n - dn 번의 소비자간 재배포가 가능하다.

〔정의 3〕 패밀리 도메인 키

패밀리 도메인 키 DK(Domain Key)는 패밀리 도메인에 포함된 디바이스를 인증하는 키로써 패밀리 도메인에 포함된 디바이스들의 식별정보를 이용하며 튜플 $\{DI_1 + DI_2 + ... + DI_i\}$로 정의된다. DI(Device Identifier)는 디바이스 식별자이며 패밀리 도메인에 포함된 i개의 디바이스 식별자를 누적하여 DK를 표현한다. 도메인 키는 패밀리 도메인의 디바이스가 바뀔 때마다 갱신되며 기존 도메인 키를 ODK라고 하고 새로운 도메인 키를 NDK라고 한다. ODK와 NDK가 같으면 패밀리 도메인의 변화가 없음을 의미하며 패밀리 도메인이 정의되지 않는다면 ODK와 NDK는 자신의 디바이스 식별자가 된다.

〔정의 4〕 라이센스

라이센스는 <P, S, U, ODK, NDK>에 의해 정의된다. P는 재배포 주체이자 콘텐츠 구매자를 의미하며 S는 패밀리 도메인 재배포 조건을 의미한다. U는 사용 규칙이다. ODK는 기존 도메인 키이고 NDK는 새로운 도메인 키이다.

다음은 라이센스의 예로써 라이센스 L은 p1이 r를 사용규칙 U에 따라 사용할 수 있으며 q1에게 한번 그리고 패밀리 도메인에서 두 번 재배포할 수 있는 라이센스이다. 도메인 키가 DI_{p1}인 것으로 보아 아직 패밀리 도메인에서의 재배포가 발생되지 않았다.

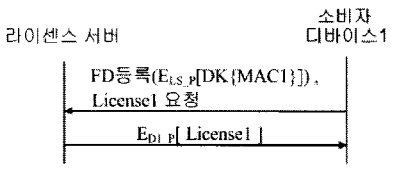
L : < <p1, {q1,p1}>, <r,3,2>, U, {DI_{p1}}, {DI_{p1}} >

4.2 패밀리 도메인 재배포를 위한 라이센스 관리 기법

패밀리 도메인에서의 라이센스 관리 기법의 핵심은 디바이스 식별 정보를 이용하여 도메인 키를 생성하고 패밀리 도메인을 구성하는 디바이스가 변경될 때마다 도메인 키가 갱신되며 이를 반영하여 라이센스도 갱신된다. 또한 재배포 받은 콘텐츠를 실행하기 위해서는 발급된 라이센스에 저장된 도메인 키를 이용한 디바이스 인증이 요구된다.

4.2.1 패밀리 도메인 재배포

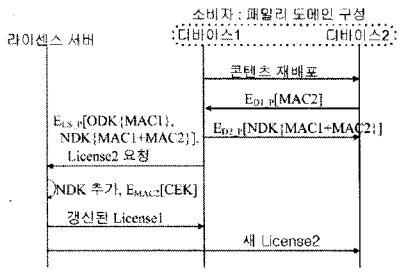
패밀리 도메인의 재배포 서비스를 위해서는 패밀리 도메인의 등록이 우선되어야 한다. (그림 2)는 패밀리 도메인의 등록 과정을 나타낸다. 재배포할 디바이스인 디바이스1은 라이센스 서버에게 패밀리 도메인 등록을 요청하며 자신의 디바이스 식별자인 MAC1을 도메인 키인 DK로 하여 라이센스 서버에게 전송한다. DK는 라이센스 서버의 공개키로 암호화되어 전송된다. 라이센스 서버는 소비자의 정보와 DK 정보를 함께 저장한다. 그리고 소비자의 디바이스1에게 DK값이 저장된 라이센스를 전송한다.



E : 암호화 , FD : 패밀리 도메인
D1_P : 디바이스1의 공개키
LS_P : 라이센스 서버의 공개키
MAC1 : 디바이스1의 MAC 주소
License1 : 디바이스1의 라이센스

(그림 2) 패밀리 도메인 등록

소비자가 디바이스1에서 실행하던 콘텐츠를 디바이스2에서 실행하기를 원하면 콘텐츠를 디바이스2에게 재배포한다. 이로써 디바이스2는 패밀리 도메인의 구성원이 된다. 디바이스1은 패밀리 도메인이 변경되었다는 것을 라이센스 서버에게 알리고 변경된 패밀리 도메인의 디바이스들을 위한 라이센스 요청을 하여야 한다. (그림 3)은 패밀리 도메인에서의 라이센스 관리 과정을 보여준다. 라이센스 관리 과정에 대한 내용은 다음과 같다.



D1_P : 디바이스1의 공개키
D2_P : 디바이스2의 공개키
LS_P : 라이센스 서버의 공개키
CEK : 콘텐츠 암복호화 키, E : 암호화
MAC1 : 디바이스1의 MAC 주소
MAC2 : 디바이스2의 MAC 주소
License1 : 디바이스1의 라이센스
License2 : 디바이스2의 라이센스

(그림 3) 패밀리 도메인 재배포를 위한 라이센스 관리 기법

디바이스1이 디바이스2에게 콘텐츠를 재배포하

면 디바이스2는 새로운 DK인 NDK의 생성을 위해 자신의 MAC 주소 MAC2를 디바이스1의 공개키로 암호화 하여 디바이스1에게 전송한다. 디바이스1은 MAC1과 MAC2 값으로 NDK{MAC1+MAC2}를 생성하고 이를 디바이스2의 공개키로 암호화하여 디바이스2에게 전송한다. 이로써 디바이스2의 DB에는 NDK가 저장된다. 디바이스1은 기존 DK인 ODK{MAC1}과 NDK를 라이센스 서버의 공개 키로 암호화 하여 라이센스 서버에게 전송하며 디바이스2의 라이센스를 요청한다. 디바이스2의 라이센스 요청에는 디바이스2에서 실행하고자 하는 권리 내용이 포함된다.

라이센스 서버는 ODK 정보를 이용하여 소비자의 패밀리 도메인 정보를 찾고 ODK를 NDK로 변경함으로써 패밀리 도메인의 변경내용을 관리한다. 그리고 라이센스 요청에 포함된 권리 내용을 반영하여 디바이스2의 라이센스를 새로 발급하고 디바이스1의 라이센스의 권리 부분과 DK 부분을 갱신한다. 두 라이센스에는 ODK와 NDK의 내용이 저장된다. 또 디바이스2의 라이센스에는 콘텐츠 암복호화 키인 CEK가 MAC2로 암호화되어 저장된다. 이러한 작업이 수행된 후에 라이센스 서버는 디바이스1과 디바이스2에 라이센스를 각각 전송한다.

4.2.2 패밀리 도메인 재배포의 안전성

콘텐츠가 디바이스2에서 실행되기 위해서는 라이센스 관리 서비스에서 (그림 4)와 같은 인증 과정을 거쳐 패밀리 도메인의 올바른 디바이스인가가 인증되어야 한다. 첫 번째 인증 과정은 디바이스2의 DB에 저장된 NDK와 디바이스2의 라이센스에 저장된 NDK를 비교하는 과정이다. (그림 3)의 과정을 통해 디바이스2가 라이센스를 발급 받은 후 그것의 DB에는 라이센스와 NDK가 저장되어 있다. (그림 3)의 과정에서 디바이스2와 라이센스 서버는 디바이스1로부터 NDK를 받았으므로 라이센스 서버로부터 발급된 라이센스에 포함된 NDK와 디바이스2의 DB에 저장된 NDK는 동일해야 한다. 이것은 (식 1)과 같이 표현될 수 있다.

$$A = B \text{ and } B = C \rightarrow A = C \quad \text{(식 1)}$$

(식 1)에서 A는 라이센스 서버로부터 발급된 라이센스에 있는 NDK이며 B는 디바이스1에 저장된 NDK 그리고 C는 디바이스2에 저장된 NDK이다.

```
DeviceAuthentication()
  Compare NDK within license and NDK within device
  if two NDKs equal then
    if MAC2 is included in NDK within license then
      Decrypt CEK encrypted with MAC2
      Decrypt content with CEK
      Excution content
    else return
  else return
```

(그림 4) 콘텐츠 실행을 위한 인증과정

두 NDK가 일치하면 (그림 4)의 두번째 if 문에서 디바이스2의 식별자 MAC2를 추출하여 라이센스에 저장된 NDK에 포함되었는지를 확인한다. DK는 4.1절의 [정의 3]에 의해 패밀리 도메인에 포함된 디바이스 식별자들을 누적하여 생성되기 때문에 올바른 디바이스라면 DK에 자신의 식별자가 포함되어야 한다. 포함되었다면 (그림 3)에서 MAC2로 암호화 된 CEK를 MAC2로 복호화하고 콘텐츠를 복호화한 후 콘텐츠를 실행한다.

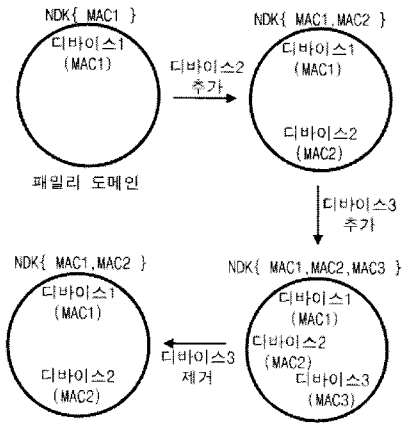
MAC2가 NDK에 포함되었는지를 검사하는 과정과 CEK를 MAC2로 복호화하는 과정에서 MAC2값은 직접 디바이스에서 추출되는 값이므로 불법으로 복사할 수 없다. 그러므로 허가된 디바이스라면 MAC값이 NDK에 포함될 것이며 라이센스가 요청된 올바른 디바이스라면 CEK가 MAC2로 암호화 되었기 때문에 MAC2로 복호화 되어 콘텐츠를 복호화 할 수 있으므로 정상적으

로 콘텐츠를 실행할 수 있다. 패밀리 도메인에서의 이러한 콘텐츠 실행 과정은 다음과 같은 이유로 안전하다는 것을 알 수 있다.

- 라이센스의 NDK와 디바이스에 저장된 NDK가 같다는 것은 패밀리 도메인의 올바른 디바이스임을 말한다. 만약 허가되지 않은 디바이스가 라이센스만을 불법 복제한다면 (그림 4)에서 첫 번째 인증 과정인 비교 과정을 통해 허가되지 않은 디바이스임이 드러날 것이다.

- 만약 허가되지 않은 디바이스가 허가된 디바이스의 라이센스와 디바이스에 저장된 NDK 모두를 불법 복제한다고 해도 (그림 4)에서 두 번째 인증 과정인 디바이스 식별자의 포함여부 확인 과정을 통해 허가되지 않은 디바이스임이 드러난다. NDK에는 허가되지 않은 디바이스의 식별자가 포함되어 있지 않을 것이다.

제안된 라이센스 관리 기법을 통해 패밀리 도메인에 새로운 디바이스가 추가되고 제거될 때마다 라이센스의 NDK값은 갱신되며 (그림 5)는 NDK값의 갱신 내용을 보여준다.



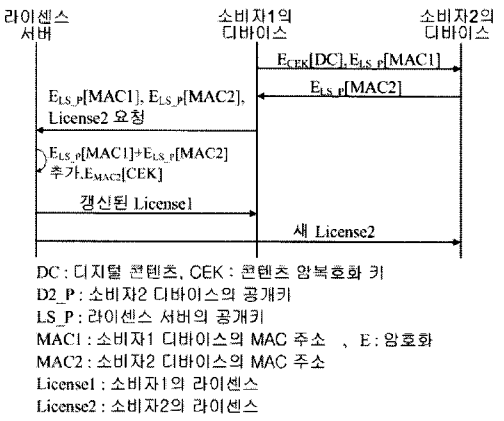
(그림 5) 패밀리 도메인의 변경에 따른 NDK의 갱신

만약 (그림 5)의 패밀리 도메인에서 제거된 디바이스3이 제거된 이후에 재배포 된 콘텐츠와 라이센스를 불법적으로 복사하여 실행하고자 해도 라이센스의 NDK에는 MAC3이 포함되어 있지 않기 때문에 콘텐츠와 라이센스는 불법 유출로 간주되고 콘텐츠는 실행되지 못한다. 이로써 패밀리 도메인의 변경에 따른 도메인 키의 갱신은 패밀리 도메인에서의 안전한 재배포를 가능하게 함을 알 수 있다. 또한 패밀리 도메인에 포함된 디바이스 식별자들을 누적하여 도메인 키로 이용함으로써 패밀리 도메인에 포함되는 디바이스의 개수에 독립적으로 패밀리 도메인을 관리할 수 있기 때문에 효율적인 도메인 관리가 가능하다.

4.2.3 소비자간 재배포

제안된 라이센스 기법은 소비자간의 안전한 재배포를 위해서도 적용될 수 있다. (그림 6)은 패밀리 도메인 재배포에서의 라이센스 관리 기법이 소비자간의 재배포에 적용된 과정을 보여준다. (그림 6)에서 소비자1이 소비자2에게 콘텐츠를 재배포하고 각 디바이스 식별자 MAC1과 MAC2를 교환함으로써 소비자1과 소비자2의 디바이스에는 MAC1과 MAC2가 저장된다. 소비자1은 MAC1과 MAC2를 누적하여 라이센스 서버에 전송하며 소비자2의 라이센스를 요청한다. 라이센스 서버는 재배포가 수행된 디바이스들의 식별자 MAC1+MAC2를 소비자2의 라이센스에 저장하여 소비자2에게 전송한다.

라이센스를 발급받은 소비자2의 디바이스에서 콘텐츠를 실행하기 위해서는 디바이스에 저장된 MAC1+MAC2와 라이센스에 저장된 MAC1+MAC2를 비교하여 일치할 때만 실행할 수 있다. 이것은 (식 1)에 의해 두 개의 누적된 디바이스 식별자들의 값이 일치해야 하기 때문이다. 또한, 누적된 디바이스 식별자를 자신이 가지고 있고 그것을 라이센스 서버에게 보내서 라이센스에 포함시킨 후 그 라이센스를 받아서 자신이 보낸 누적된 디바이스 식별자를 포함했는지를 비교함으로써 올바른 디바이스 임을 확인하는 것이다.



(그림 6) 소비자간 재배포에서의 라이센스 관리 기법

이와 같이 패밀리 도메인 재배포에서 사용된 라이센스 관리 기법은 소비자간의 재배포에도 적용되어 안전한 재배포를 가능하게 한다. 단지 패밀리 도메인과 차이가 있다면 서로 다른 소비자에게 MAC 주소를 공개하지 않기 위해서 MAC 주소는 라이센스 서버의 공개키로 암호화된 상태로 교환되고 저장된다.

5. 평가

제안된 패밀리 도메인 재배포를 위한 라이센스 관리 기법에서는 패밀리 도메인에서의 콘텐츠 재배포를 안전하게 수행하기 위하여 디바이스 식별자를 이용하여 도메인 키를 생성하고 라이센스에 저장하며 패밀리 도메인에 변경이 생기면 도메인 키를 갱신하고 라이센스를 갱신한다. 또한 디바이스 식별자를 이용한 도메인 키 생성은 패밀리 도메인에 포함된 디바이스의 개수에 영향을 받지 않으므로 효율적인 도메인 관리가 이루어질 수 있다.

(표 1)은 제안된 라이센스 관리 기법을 대표적인 상용화 시스템인 Microsoft 사의 WMRM, Fraunhofer사의 LWDRM과 대표적인 표준 DRM인 OMA와 [2]에서 제시된 인증된 도메인 기법(Authorized Domain: AD)과 비교한 내용을 요약한 표이다[9][10][11].

MS의 WMRM은 디바이스의 개수를 엄격히 제한하고 권리를 유동적으로 할당할 수 없도록 함으로써 패밀리 도메인을 매우 제한적으로 지원한다. OMA는 Domain이라는 개념으로 패밀리 도메인을 적극 지원한다. 그러나 도메인을 구성하는 디바이스에 변경이 생겼을 때를 대비하여 이전 도메인 키를 기반으로 한 새로운 도메인 키를 미리 생성한다는 특징으로 인해 미리 생성한 도메인 키 개수 만큼의 도메인 변화만이 가능하다는 제한이 있다. LWDRM은 콘텐츠를 콘텐츠 소유자만이 사용할 수 있는 형태인 LMF(Local Media File)와 소유자의 서명이 들어 있는 형태로써 자유롭게 배포될 수 있는 SMF(Signed Media File) 두 가지 형태로 저장한다. SMF가 허가되지 않은 디바이스에 배포되면 서명으로 인해 불법 배포자가 들어난다. 그러나 허가되지 않은 디바이스에서 콘텐츠의 실행을 막기는 어렵다. AD 기반의 기법은 마스터 디바이스 키 리스트를 이용하여 패밀리 도메인을 관리한다[2]. 마스터 디바이스 키 리스트에는 패밀리 도메인에 포함될 수 있는 최대 디바이스 개수 만큼의 서로 다른 도메인 키가 있다. 그러나 미리 만들어진 도메인 키가 모두 할당되어 새로운 디바이스에 할당할 키가 없으면 도메인을 다시 구성해야 하는 제약이 있다.

(표 1) 라이센스 관리 기법의 비교

	WMRM	OMA	LWDRM	AD기반 [2]	제안된 기법
패밀리 도메인 지원	제한적	적극 지원	적극 지원	적극 지원	적극 지원
도메인키 관리 효율성	도메인 키없음	낮음	도메인 키없음	낮음	높음
하드웨어 바인딩	유	유	무	무	유
키분배 방식	비대칭키	대칭키/ 비대칭키	대칭키/ 비대칭키	비대칭키	대칭키/ 비대칭키
사용자프 라이버시	낮음	낮음	높음	높음	높음
저작권 보호정도	높음	높음	높음	높음	높음

제안 기법의 도메인 키는 패밀리 도메인에 포함된 디바이스 식별자들을 누적하여 생성한다. 패밀리 도메인에 디바이스가 추가되면 도메인 키에 추가된 디바이스 식별자가 포함되고 디바이스가 제거되면 도메인 키로부터 제거된 디바이스 식별자도 삭제된다. 이러한 도메인 키 관리기법을 통하여 패밀리 도메인 변화 횟수에 대한 제한은 없다. 콘텐츠가 실행되기 전에 라이센스에 포함된 도메인 키와 디바이스에 포함된 도메인 키의 비교 단계와 도메인 키에 콘텐츠를 실행하고자 하는 디바이스의 식별자가 포함되는지 확인하는 단계를 거치고, 콘텐츠 암복호화 키를 디바이스 식별자로 암호화 함으로써 패밀리 도메인의 허가된 디바이스 만이 콘텐츠를 실행할 수 있도록 하였다. 이러한 단계들은 패밀리 도메인에서 제거된 디바이스에서 제거 이후에 배포된 콘텐츠가 실행되는 것과 제 3자에 의한 불법 사용을 불가능하게 한다. 또한 제안된 기법은 패밀리 도메인뿐만 아니라 사용자간 재배포에도 적용될 수 있음으로써 적용 범위에 융통성이 있다. 그러나 네트워크로 연결된 디바이스 간의 재배포라는 제약이 있다.

도메인 키 관리 효율성은 패밀리 도메인의 변경이 생겼을 때 도메인 키가 관리되는 방법과 도메인 변경에 가해지는 제약에 대해 비교한다. WMRM과 LWDRM은 도메인 키를 별도로 사용하지 않고 디바이스 개수를 제한하거나 서명을 이용한 배포로써 패밀리 도메인을 지원한다. OMA에서는 미리 도메인 키를 여러 개 생성하여 패밀리 도메인의 변화가 생기면 다른 도메인 키를 할당한다. AD 기반의 기법은 도메인 키를 여러 개 생성하여 디바이스 당 하나씩 다른 도메인 키를 할당한다. OMA와 AD 기반의 기법 모두 미리 생성된 도메인의 개수 만큼의 도메인 변화만이 가능하다는 제약이 있다. 제안 기법에서는 패밀리 도메인이 변경되면 도메인 키도 변경되며 도메인 변경횟수에 대한 제약은 없다. 그러나 패밀리 도메인에 포함된 디바이스 개수가 증가하면 도메인 키의 길이가 증가된다는 단점이 있지만 한 사람이 소유한 디바이스의 종류가 바뀌는 경우는 많으나 개수가 지속적으로 증가하지는 않으므로 극복될 수 있다.

하드웨어 바인딩은 도메인 키나 콘텐츠 암복화 키를 하드웨어 식별자와 연결시켜 놓고 콘텐츠가 특정 하드웨어에서만 실행될 수 있도록 하는 기능이다. LWDRM은 패밀리 도메인 내에서 공유될 SMF에 대해서는 하드웨어 바인딩을 제공하지 않는다. AD 기반의 기법 역시 하드웨어 바인딩 기능을 제공하지 않는다. 그 외 제안된 기법을 포함하여 나머지 기법들은 하드웨어 바인딩 기능을 제공한다. 특히 제안 기법에서는 패밀리 도메인에 포함된 디바이스 식별자들을 누적한 도메인 키를 통해 패밀리 도메인에 포함된 모든 디바이스에 동시에 바인딩된다. 그러므로 패밀리 도메인 내에서는 콘텐츠가 자유롭게 배포되어 실행될 수 있지만 패밀리 도메인이 아닌 디바이스에서는 실행이 불가능하다.

패밀리 도메인의 재배포 수행의 안전성을 측정하는 요소로 키 분배 방식을 비교하였다. 제안된 기법과 OMA 그리고 LWDRM은 비대칭키/대칭키 암호화 방법을 이용하여 키를 분배한다. 이는 디바이스 식별자를 이용한 대칭키 암호화 방법으로 한번 더 키를 암호화 함으로써 라이센스가 불법적으로 노출되더라도 콘텐츠 실행은 불가능하게 하기 위함이다. WMRM과 AD 기반의 기법은 비대칭키 암호화 기법만을 이용한다.

제안 기법에서는 사용자의 개인 정보와 관련된 디바이스 식별자 정보를 포함하는 모든 키를 암호화된 상태로 이용하고 라이센스 서버에서도 특정 모듈만이 이들 정보에 접근할 수 있게 함으로써 개인 프라이버시가 최대한 지켜질 수 있도록 하였다. LWDRM과 AD기반의 기법에서도 개인 프라이버시 정보를 가능한 사용하지 않도록 함으로써 개인 프라이버시를 지키고자 한다. 비교된 모든 시스템들의 라이센스 관리 기법은 모두 콘텐츠 제공자의 저작권을 적극 보호하고 있다.

6. 결론

제안된 라이센스 관리 기법의 목적은 디지털 콘텐츠 소비자의 콘텐츠 이용의 융통성을 제공하며, 안전한 콘텐츠 이용을 지원함으로써 콘텐츠 유통 활성화와 함께 소비자 중심의 콘텐츠 이용 환경을 마련하는 것이다.

콘텐츠 이용의 융통성을 위하여 패밀리 도메인에서 디바이스 간 재배포를 지원할 수 있도록 설계 하였다. 또한 패밀리 도메인의 안전한 관리를 위하여 패밀리 도메인 내의 디바이스 식별자들을 이용하여 도메인 키를 생성하고 라이센스에 저장한다. 도메인을 구성하는 디바이스에 변경이 생길 때마다 도메인 키가 변경되도록 하였으며 따라서 라이센스는 갱신된다. 그러므로 더 이상 패밀리 도메인에 포함되지 않는 디바이스들이나 허가되지 않은 디바이스들은 기존의 라이센스를 가지고 콘텐츠를 이용할 수 없다. 또한 도메인 키는 패밀리 도메인을 구성하는 디바이스의 개수에 독립적으로 생성되기 때문에 효율적인 관리가 가능하다. 소비자간 재배포 서비스에서도 제안된 라이센스 관리 기법을 적용하여 안전한 재배포를 수행할 수 있음을 보였다.

향후 연구 과제로는 패밀리 도메인에서의 콘텐츠 실행 권리를 지원할 수 있도록 기존 권리 표현 언어를 확장하는 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] Thomas S. Messerges, Ezzat A. Dabbish, "Digital Rights Management in a 3G Mobile Phone and Beyond", ACM Workshop DRM '03, pp.27-38, October 27, 2004.

[2] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum, Frank L.A.J. Kamperman, "A DRM Security Architecture for Home Networks", ACM Workshop DRM '04, pp.1-10, October 25, 2004.

[3] Jiang Zhang, Bin Li, Li Zhao, Shi-Qiang Yang. "LICENSE MANAGEMENT SCHEME WITH ANONYMOUS TRUST FOR DIGITAL RIGHTS MANAGEMENT", IEEE International Conference on Multimedia and Expo, July 6-8, 2005.

[4] R. Mori, M. Kawahara, "Superdistribution: The concept and the architecture", Transaction of the IEICE, E73(7), pp.1133-1146, 1990.

[5] Pasi Tyrväinen, "Concepts and a Design for Fair Use and Privacy in DRM", D-Lib Magazine, Volume11, Number 2, February 2005.

[6] 장혜진, "DRM 기술로 보호된 컨텐츠의 융통성 있는 공유를 위한 멤버/그룹 라이선스 메커니즘", 정보처리학회논문지 C, 제11-C권, 제 6호, pp.739-746, 2004년 12월

[7] GSM 02.09 (ETS 300 506), "Digital Cellular Telecommunications System(Phase 2); Security Aspects", Aug, 2000.

[8] Title 17-Copyrights, Chapter 1-Subject Matter And Scope of Copyright, Sec.107-US Code Collection. Legal Information Institute. http://www4.law.cornell.edu/uscode/107.html

[9] Windows Media Rights Management, http://www.microsoft.com/windows/windowsmedia

[10] Open Mobile Alliance, "DRM Architecture", OMA-DRM-ARCH-V2_0-20 040820-C, Draft Version 2.0-20 August 2004, http://www.openmobilealliance.org

[11] Fraunhofer Institute, "Light Weight DRM(LWDRM)", http://www.lwdrm.com

[12] Byungwook Lee, "Group License Management using Super-Distribution in DRM", The 2007 International Conference on Ubiquitous City Technology, pp.122-130, Feb 2~5, 2007.

[13] Bohyun Wang, Byungwook Lee, "A Study of License Distribution Mechanism using

Accumulated Device Identifier in DRM system", 2007 International Conference on Multimedia and Ubiquitous Engineering, Seoul Korea, pp.1118-1123, April 26-28, 2007.

[14] 한국문화콘텐츠진흥원, "2007년 세계 문화콘텐츠산업 전망", 2007.02

◐ 저 자 소 개 ◑

왕 보 현 (Bo-Hyun Wang)
1994년 경원대학교 전자계산학과(공학사)
1996년 경원대학교 대학원 전자계산학과(공학석사)
2001년 (주)한화 정보통신
2002년 현대전문학교 전임강사
2002~현재 경원대학교 전자계산학과 박사과정
관심분야 : 데이터베이스, DRM, 정보보안, 멀티미디어 etc.
E-mail : bhwang99@hanmail.net

이 병 욱(Byung-Wook Lee)
1973년 연세대학교 공과대학(공학사)
1984년 George Washington University 전자계산학과(공학석사)
1994년 중앙대학교 전자계산학과 공학박사
1985.3.1~ 현재 경원대학교 소프트웨어학부 교수
관심분야 : 분산 시스템, 데이터베이스, 저작권 관리 Digital Rights Management
E-mail : leebw@kyungwon.ac.kr