누적된 디바이스 식별자를 이용한 Family Domain 관리 기법에 관한 연구

왕보현*, 이병욱*
*경원대학교 전자계산학과
e-mail:bhwang99@hanmail.net, leebw@mail.kyungwon.ac.kr

Family Domain Management Method using Accumulated Device Identifier

Bo-Hyun Wang*, Byung-Wook Lee*
*College of Software, Kyung-Won University

요 약

디지털 콘텐츠 소비자들은 자신이 소유한 여러 디바이스에서 콘텐츠를 실행할 수 있는 권리를 요구한다. 최근 DRM 시스템에서 이러한 소비자 권리를 기술적으로 지원할 수 있는 많은 연구가 진행되고 있다. 사용자 소유의 디바이스들은 family domain으로 정의할 수 있다. 기존의 family domain 관리기법들은 지정된 디바이스 외의 디바이스에서도 콘텐츠가 실행될 수 있거나 또는 도메인에 지정된 최대 디바이스 개수에 도메인 관리 키가 영향을 받게 되어 키 관리를 효율적으로 할 수 없다는 단점이 있다. 본 논문에서는 family domain에 현재 포함된 디바이스들의 누적된 식별자를 이용하여 지정된 디바이스 중 하나가 교체되어도 새로 지정된 디바이스를 포함하는 디바이스에서만 콘텐츠가 안전하게 실행될 수 있으며 지정된 디바이스의 최대 개수와 독립적으로 도메인 관리 키는 실제 사용하는 디바이스에 따라 동적으로 생성될 수 있는 family domain 관리 기법을 제안한다.

1. 서론

디지털 콘텐츠의 온라인 유통 시장은 많은 편리함을 가져 왔지만 거의 완벽한 복제 가능의 특징과 온라인 환경의 특징으로 인하여 콘텐츠 저작자들에게 많은 피해가 돌아갔다. 이에 디지털 콘텐츠의 불법 유통을 막는 DRM 시스템이 등장하였다. 그러나 소비자 입장에서는 DRM이 적용된 콘텐츠를 이용하는데 있어서 많은 제약과 불편이 따르게 되어 콘텐츠 사용을 포기하는 사례가 증가하였다.

사용자들은 지불한 콘텐츠에 대해서 오프라인 환경에서와 같이 온라인 환경에서도 최대한의 권리를 갖고자 한다. 권리의 유형 중 한 가지는 자신이 소유하고 있는 여러 디바이스에서 구매한 콘텐츠를 실행시키고자 하는 것이다. 기존 DRM시스템에서는 이러한 사용자 권리를 허용하지 않으나 최근 많은 연구들이 이러한 권리를 기술적으로 지원하는 내용을 다루고 있다.

"본 논문은 2006년도 경기도 차세대성장동력기술개발지원사업에 의하여 연구되었음"

본 논문에서는 [1]에서 제시한 FD(Family Domain) 개념을 이용하여 사용자들이 소유하고 있는 여러 디바이스를 FD로 정의하고 FD에 포함된 디바이스들의 식별자를 이용하여 도메인을 효율적으로 관리할 수 있는 기법을 제안한다. 제안된 기법을 통해 FD에 속한 디바이스에서만 콘텐츠 실행이 가능하며 소속 디바이스가 변경되더라도 FD에서 제거된 디바이스에서는 콘텐츠가 실행될 수 없음을 보인다. 또한 도메인 관리를 위해 필요한 도메인 키가 기존 연구와는 달리 도메인에 포함될 디바이스 최대 개수와는 독립적으로 생성된다는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 기술하고 3장에서는 제안하는 FD 관리 기법에 대해 기술한다. 4장에서는 평가에 대한 내용을 기술하고 5장에서 결론을 맺는다.

2. 관련연구

Fair use 개념과 기존 연구에 대해 언급한다. 또, 디바이스 식별자의 종류를 기술한다.

2.1 fair use

Fair use는 콘텐츠를 구매한 구매자들의 콘텐츠 이용 권리를 지켜주기 위해 미국 저작권법에서 사용되는 용어이다. 이 저작권법의 내용에 의하면 연구나 교육과 같은 목적으로 콘텐츠를 복제 사용하거나 인용하는 경우, 소비자가 구매한 콘텐츠를 재 판매하고 개인적인 용도로 백업하는 경우, 소비자가 다른 소비자에게 콘텐츠를 선물하거나 연구나 교육의 목적으로 콘텐츠를 공유 경우는 fair use에 해당되며 저작권법에 위배되지 않는다[4].

2.2 기존 연구에서의 도메인 관리

[1]에서는 fair use 유형 중 하나인 한 명의 구매자가 소유한 여러 대의 디바이스에서 콘텐츠를 지원하기 위해 FD(Family Domain)라는 개념을 제안하였다. 디바이스가 FD에 속해 있다는 것을 DRM 인증서를 통해 인증하고 인증서에 대응하는 공개 키로 콘텐츠 암호화 키를 암호화 한다. FD에 속해 있는 모든 디바이스들은 동일한 비밀키/공개키 쌍을 갖게 된다. 이러한 도메인 관리 기법에서는 비밀키/공개키 쌍이 노출되면 FD에 속하지 않는 디바이스에서도 콘텐츠가 실행될 가능성이 있다.

[2]에서는 홈네트워크에서의 보안 구조를 제안한다. 홈네트워크에 속한 디바이스들을 AD(Authorized Domain)로 정의하고 AD 관리를 위하여 마스터 디바이스 키 리스트를 생성한다 이것은 AD에 포함되는 디바이스들에게 하나씩 할당되는 키로써 AD에 포함될 예상 디바이스 개수 만큼의 키를 갖는다. 그러므로 항상 AD에 포함될 최대 디바이스 개수만큼의 키가 요구된다. 그 이상이 되면 AD를 다시 설정해 주어야 한다. 또, 마스터 디바이스 키 리스트가 노출되면 허가되지 않은 디바이스도 콘텐츠를 실행시킬 수가 있다.

2.3 디바이스 식별자

모바일 기기나 데스크탑 등 거의 모든 디바이스들은 그들을 유일하게 식별할 수 있는 식별자를 가질 수 있다.

모바일 기기의 경우 디바이스 사용자와 디바이스를 식별할 수 있는 IMEI(International Mobile Equipment Identificaiton)나 IMSI(International Mobile Subscriber Identity) 번호를 제공한다[3]. SN(Serial Number)은 디바이스가 존재하는 한 변경되지 않기 때문에 IMEI 번호로써 사용될 수 있다. SN은 주로 콘텐츠를 특정 디바이스에서만 사용하도록 규정할 때 사용될 수 있다. MN(Model Number)은 디바이스와 디바이스에 설치된 소프트웨어의 버전을 식별할 때 사용된다[1]. MAC(Media Access Control) 주소값은 모바일 기기 및 데스크 탑에서 사용할 수 있는 네트웍 카드의 48비트 하드웨어 주소를 말하며 모든 네트워크 카드가 유일한 값을 갖는다. 그러므로 네트워크가 가능한 모든 기기는 이 주소로써 식별가능하다.

3. 본론

본 논문에서는 누적된 디바이스 식별자를 이용하여 FD에서 콘텐츠가 안전하게 실행될 수 있는 도메인 관리 기법을 제안한다. 디바이스 식별자로는 가장 범용적으로 사용될 수 있는 MAC address를 사용한다. 먼저 도메인 관리 기법에서 제시되는 몇 가지 개념을 정의한다.

3.1 개념 정의

FD 관리에서 제시되는 몇 가지 개념을 정의한다.

정의 1. Family Domain Manager(FDM)

FD 생성 및 관리를 주관하는 주체이다. 라이센스 서버와 상호작용하며 FD 등록 요청 및 디바이스 추가 및 삭제로 인한 도메인 키 갱신 요청 그리고 도메인 키 갱신 등의 작업을 수행한다.

정의 2. 누적된 디바이스 식별자

튜플 $\{DI_1 + DI_2 + ... + DI_i\}$로 정의되며 FD에 포함된 디바이스 식별자들을 차례로 누적시킨 것이다

정의 3. 도메인 키

FD에 포함된 디바이스임을 인증하는 키로써 FD에 포함된 디바이스의 식별자들을 누적시켜 생성되며 다음과 같이 정의된다. n은 FD에 포함된 디바이스 개수이다.

$$DK[\ \{\ DID_1 + DID_2 + ... + DID_n\ \}\ ]$$

정의 3. 도메인 라이센스

FD에 포함되는 디바이스들에게 주어지는 라이센스로써 튜플 DL< ODK, NDK, N, P, U, K >로써 정의한다. ODK는 구 도메인 키를 나타내며 NDK는 새로운 도메인 키를 나타낸다. N은 도메인에 포함될 수 있는 디바이스 개수이며 P는 사용자 식별자이다.

U는 콘텐츠 사용규칙이며 K는 콘텐츠 암호화 키이다. DL에 DK가 하나밖에 없다면 초기 FD 생성 시 FDM에게 발급된 DL임을 의미한다.

3.2 Family Domain의 등록

FD를 생성하기 위해서는 FD 등록 과정이 요구된다. FD에 속한 디바이스들은 모두 디바이스 인증을 위한 인증서를 갖는다고 가정한다. 또한 FD에 속하는 디바이스 개수는 작은 수로 정해진다.

등록 과정은 FD의 관리자로써 역할을 할 디바이스 즉 FDM과 라이센스 서버간에 이루어지며 다음과 같은 절차를 갖는다. LS는 라이센스 서버를 나타낸다.

(1) LS-->FDM : CertLS
(2) FDM-->LS : CertFDM, Req(DL), NumOfDevice, $E_{LS\_PUB}[\ DK\{\ DID_1\ \}\ ]$
(3) LS-->FDM : DL< $E_{FDM\_PUB}[\ DK\{\ DID_1\ \}\ ]$, N, P, U, $E_{DID1}[CEK]$ >

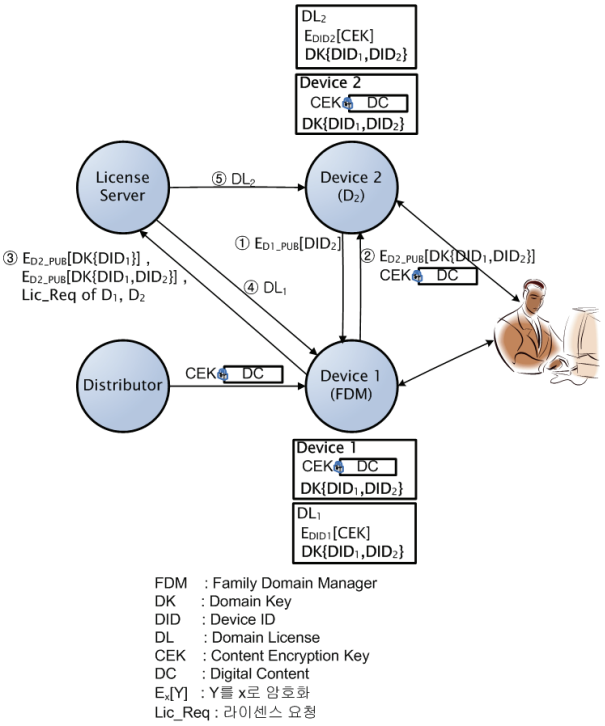
(1)번과 (2)번 과정은 라이센스 서버와 FDM에 해당하는 디바이스 간의 인증과정이다. 라이센스 서버는 FDM에게 자신의 인증서를 보낸다. FDM은 자신의 인증서와 함께 도메인 키에 해당하는 자신의 디바이스 식별자 DID_1과 도메인에 포함될 수 있는 디바이스의 개수 그리고 도메인 라이센스 발급요청을 보낸다. 인증과정이 끝나면 라이센스 서버는 도메인 라이센스를 FDM에게 보낸다.

3.3 구성원 등록 및 라이센스 발급

FD로 등록된 후 새로운 디바이스가 FD의 구성원이 되려면 구성원 등록이 필요하다. 구성원 등록 과정 절차는 다음과 같다. D_2는 새로운 디바이스이다.

(1) FDM-->D_2 : CertFDM
(2) D_2-->FDM : CertD_2, $E_{FDM\_PUB}[DID_2]$
(3) FDM-->D_2 : $E_{D2\_PUB}[DK\{DID_1 + DID_2\}]$
(4) FDM-->LS : ODK, NDK, Req(DL_1, DL_2)
(5) LS-->FDM, D_2 : DL_1 , DL_2

FDM과 새로운 디바이스인 D_2는 서로 인증서를 교환함으로써 디바이스 인증을 수행한다. D_2는 자신의 디바이스 식별자인 DID_2를 새로운 도메인 키를 생성하기 위하여 FDM에게 보낸다. FDM은 DID_1과 DID_2를 누적시켜 새로운 도메인 키를 생성하여 D_2에게 보낸다. 도메인 키가 바뀌었다는 것을 라이센스 서버에 알리기 위하여 이전 도메인 키와 새로운 도메인 키를 라이센스 서버에 보낸다. 그리고 새로운 FDM과 D_2의 도메인 라이센스를 요청한다. 라이센스 서버는 도메인 키와 각각의 디바이스 식별자로 암호화된 콘텐츠 암복호화 키를 포함하는 새로운 도메인 라이센스를 FDM과 D_2에게 보낸다. 그림 1은 이러한 과정을 나타내는 그림이다.



(그림 1) 디바이스 등록 과정

3.4 구성원 제거

FD로부터 디바이스가 제거되는 과정은 첫째, 제거되는 디바이스가 도메인 키와 자신의 디바이스 식별자를 FDM에 알린다. 둘째, FDM이 제거된 디바이스의 식별자가 제외된 새로운 도메인 키를 생성하고 라이센스 서버에 이를 알린다. 셋째, 새로운 도메인 키가 반영된 새로운 라이센스들을 도메인의 디바이스들에게 발급한다.

위와 같은 과정으로 FD에 포함된 디바이스들이 관리되며 디바이스에서 콘텐츠의 실행은 다음과 같은 두 단계를 거쳐야 한다. 첫째, 도메인 인증과정과 둘째, 키 복호화 과정이다.

도메인 인증은 라이센스에 포함된 도메인 키와 디바이스에 저장된 도메인 키의 비교 후에 도메인

키에 자신의 디바이스 식별자의 포함관계를 파악함으로써 수행된다. 그림 1에 의하면 디바이스 등록 과정으로부터 도메인 키가 디바이스와 라이센스에 각각 저장됨을 알 수 있다. 두 도메인 키가 일치한다면 디바이스를 도메인의 구성원으로써 인증하고 일치하지 않는다면 도메인의 구성원으로써 간주하지 않는다. 디바이스가 도메인 구성원으로 간주되면 도메인 키가 불법 복제 된 것인지 아닌지를 확인하기 위하여 도메인 키에 디바이스 식별자가 포함되었는지를 확인한다. 포함되었다면 도메인 인증과정이 끝난다. 도메인 인증이 끝나면 디바이스 식별자로 암호화 되어 있는 콘텐츠 암복호화 키를 복호화 한다.

위에 기술한 도메인 관리 및 콘텐츠 실행 과정에서 다음과 같은 특징을 알 수 있다.

① 도메인 키는 FD에 포함된 디바이스들의 식별자들을 누적하는 것만으로 생성될 수 있기 때문에 FD에 포함될 디바이스의 수에 독립적이다.

② FD에서 디바이스들이 추가되고 제거될 때마다 도메인 키가 변경된다. 이로 인해 도메인으로부터 제외된 디바이스가 기존의 도메인 키를 소유하고 있어도 지속적으로 콘텐츠를 사용할 수 없다.

③ 콘텐츠 암복호화 키를 디바이스 식별자로 암호화 함으로써 도메인에 속하지 않는 디바이스가 도메인 키를 불법 복제하여 도메인 구성원으로 인증되더라도 콘텐츠 암복호화 키를 복호화 할 수 없으므로 콘텐츠 실행이 불가능하다.

4. 평가

본 논문에서 제시한 FD 관리기법은 [1]과 [2]에 나타난 기존 도메인 관리 기법과 표 1의 나타난 항목들에 대해 비교하였다.

<표 1> 제안기법과 기존 연구와의 비교

	제안기법	Family Domain	Authorized Domain
Key 관리	Hybrid	Public/Private Key	Hybrid
오프 라인 지원	온라인전제	온라인전제	지원
도메인키	유동적	불변	불변

콘텐츠 암호화 키관리, 도메인 관리를 위해 제안기법과 Authorized Domain 기법에서는 대칭키와 비대칭키 기법을 사용하여 관리 속도를 향상 시켰다. AD 기법은 오프 라인에서도 도메인 관리가 가능하다는 장점을 갖는다. 제안 기법에서는 도메인 키가 유동적이지만 나머지 두 기법에서는 도메인 키가 도메인 소멸시까지 불변하여 노출되면 허가되지 않은 디바이스에서도 콘텐츠가 실행될 수 있다.

5. 결론

본 논문에서는 FD에서 콘텐츠가 안전하게 실행 및 관리될 수 있도록 하는 도메인 관리 기법을 제안하였다. 제안된 기법에서는 디바이스들이 도메인에 포함되었음을 도메인 키로 인증한다. 도메인 키는 디바이스들의 식별자를 누적하여 생성된다. 새로운 디바이스가 도메인에 추가되거나 제거될 때 도메인 키에 추가된 디바이스의 식별자가 연결되고 도메인에서 제거된 디바이스의 식별자가 삭제된다. 도메인 키를 통한 도메인 인증이 끝나면 자신의 디바이스 식별자를 이용하여 콘텐츠 암호화 키를 복호화 하여 콘텐츠를 이용할 준비를 한다.

이와 같이 디바이스 식별자 누적을 이용한 도메인 키 관리를 통해 도메인으로부터 제외된 디바이스가 기존의 도메인 키를 소유하고 있어도 지속적으로 콘텐츠를 사용할 수 없다. 도메인에 현재 포함된 디바이스들의 식별자들만을 이용하여 도메인 키를 생성함으로써 향후 포함될 디바이스를 위한 추가적인 정보를 관리할 필요가 없다. 또한, 도메인 인증 후 콘텐츠 암호화 키를 해당 디바이스의 식별자로 복호화 함으로써 도메인 키와 라이센스 그리고 암호화된 콘텐츠가 불법적으로 배포되어도 허가되지 않은 디바이스에서는 실행이 불가능하다는 것을 알 수 있다. 향후 연구 과제로는 좀 더 다양한 Fair Use를 지원할 수 있는 라이센스 관리 및 권리 표현 언어에 대한 연구가 진행되어야 할 것이다.

참고문헌

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

[2] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum. "A DRM Security Architecture for Home Networks", ACM Workshop DRM '04 October 25, 2004

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

[4] 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