情報保護學會論文誌
第18卷 第4號, 2008. 8

개인 콘텐츠 접근제어 기능을 갖는 개선된 AACS 보안 Framework

김 대 엽†
삼성전자

Improvement of AACS Security Framework with Access Control to Personal Contents

DaeYoub Kim†
Samsung Electronics

요 약

디지털 카메라와 캠코더의 보급이 증가함에 따라 일반 사용자들의 UCC(User Created Contents) 역시 일반화 되고 있다. 그러나 이에 따른 사생활 침해 또한 증가하고 있다. UCC는 인터넷 포탈 서비스를 통해 공유될 뿐 아니라 DVD(Digital Versatile/Video Disk)와 같은 저장매체(Recordable Media, 이하 Media)를 이용하여 보관된다. 포탈 서비스를 이용해서 콘텐츠를 게시하는 경우 포탈 시스템이 제공하는 사용자 인증 및 불법 다운로드 제어 기술을 이용하여 사생활 침해를 부분적으로 막을 수 있다. Media의 경우도 불법복제 제어기술을 채택하고 있지만, Media의 도난 또는 분실로 인한 콘텐츠 유출과 사생활 침해를 막을 수 있는 방법이 현재로서는 제공되지 않고 있다. 그러므로 Media를 이용하여 개인 콘텐츠를 관리하는 경우에도 사생활 침해를 막을 수 있는 추가적인 보안 기술의 연구가 필요하다. 본 논문에서는 Media 보안을 위해 제정된 AACS(Advanced Access Content System)의 Framework을 살펴보고 개인 콘텐츠의 접근을 제어할 수 있는 개선된 AACS 보안 Framework을 제안한다.

ABSTRACT

As both a digital camera and a digital camcorder are popularized in recent years, UCC created by general users is also popularized. Unfortunately, according to that, the lack of privacy is also increasing more and more. The UCC is saved on the recordable media(Media) like DVD and deposited personally as well as distributed through Internet portal service. If you use Internet portal service to put up your contents, you can partially prevent the violation of privacy using security technologies such as authentication and illegal copy protection offered by internet portal service providers. Media also has technologies to control illegal copy. However, it is difficult to protect your privacy if your Media having personal contents is stolen or lost. Therefore, it is necessary to develope an additional security mechanism to guarantee privacy protection when you use Media. In this paper, we describe AACS framework for Media Security and propose improved AACS framework to control the access to personal contents saved on Media.

Keywords : AACS, Password Based Encryption Scheme, PKIS

접수일 : 2008년 2월 25일; 채택일 : 2008년 5월 22일
† 주저자, daeyoub69@paran.com

1. 서 론

디지털 카메라와 캠코더의 보급이 증가함에 따라 콘텐츠를 직접 촬영/편집하는 일반 사용자들이 늘고 있다. 일반 사용자는 이렇게 제작된 콘텐츠를 인터넷을 통해 다수의 사람들과 공유하거나, DVD 같은 저장매체(Recordable Media, 이하 Media)에 저장한 후 개인적으로 보관한다. 이와 같은 UCC의 증가는 풍요롭고 창조적인 생활을 개인에게 제공할 수 있는 반면에 사생활 침해라는 새로운 문제를 발생시키기도 한다. 특히, Media에 저장된 개인 콘텐츠의 경우, 콘텐츠의 내용이 개인 사생활과 관련된 내용인 경우가 많기 때문에 도난 및 분실에 따른 사생활 침해와 그 피해가 인터넷을 통해 공유하는 경우 보다 더 클 수 있다. 또한, 악의적인 의도를 갖고 확보한 콘텐츠를 인터넷을 통해 유포하는 경우가 발생하여 사회적인 물의를 일으킨 경우도 종종 발생하고 있다.

인터넷 포탈 서비스를 통해 사용자가 개인 콘텐츠를 공유하거나 게시하는 경우에는 포탈에서 제공하는 기본적인 접근제어 기술들을 이용하여 해당 콘텐츠로의 접근을 부분적으로 제어할 수 있다. 이러한 접근제어 기법들은 일반적으로 콘텐츠를 게시하는 사용자가 자신이 관리하는 콘텐츠에 접근할 수 있는 사람 또는 그룹을 지정할 수 있도록 하고 있다. 또한, 콘텐츠의 스크랩이나 복사 등을 제어할 수 있는 기능 또한 기본적으로 제공하고 있다.

현재 DVD 또는 HDDVD(High Definition DVD)와 같은 Pre-Recorded/ Recordable Media에는 불법복제 방지를 위해 CSS (Content Scrambling System), CPPM (Content Protection Prerecorded Media), CPRM (Content Protection Removal Media), AACS 와 같은 다양한 기술들이 적용되어왔다[1-5]. CSS는 인증 및 콘텐츠 암호 기법을 이용하여 DVD 불법복제를 막기 위해 1996년에 제안되었으나 DeCSS와 같은 공격 소프트웨어가 인터넷을 통하여 공개되었다[1,2]. DVD 복제방지 기술인 CSS를 발전시킨 CPPM은 DVD 오디오 복제 방지를 위해 개발된 기술이다[3]. CPRM은 비인가 파일 복사를 막기 위해 저장 매체 구조에 복제 제약 조건을 넣도록 설계된 하드웨어 기반 기술로 1993년에 개발된 방송 암호화 기술에 기반을 두고 있으며, 녹화용 DVD와 플래시 메모리 카드와 같은 저장 매체의 저장 데이터의 비인가 복사를 방지하는 기술로 사용되었다[4]. AACS는 차세대 광 Media의 불법복제를 막기 위하여 2005년도에 새롭게 제안된 기술로 현재 HDDVD와 BD (Blue-ray Disk)에 적용되고 있다[5].

이와 같은 콘텐츠 보안 시스템은 일반적으로 콘텐츠를 암호화해서 Media에 저장한다. 인가된 기기만이 콘텐츠 암호화에 사용된 암호키를 획득할 수 있도록 제어하는 기술이 사용된다. 특히, Media를 통한 콘텐츠 서비스는 서비스 제공자가 콘텐츠의 사용자 또는 기기가 언제 서비스를 이용하는지 알 수 없기 때문에 단방향 암호키 관리 기술이 사용된다. 이와 같은 단방향 키 관리 기술을 Broadcast Encryption Scheme(BES)이라 부른다[6-8].

BES 기반의 Media 보안 시스템은 다음과 같은 3가지 종류의 키로 구성된다.

- Title Key (K_t) : 콘텐츠를 스크램블하고, 디스크램블 할 때 사용한다.
- Media Key (K_m) : K_t를 암호화 하고 복호화 할 때 사용한다.
- Device Key (K_d) : K_m을 암호화 하고 복호화 할 때 사용한다. 사용자 기기는 서로 다른 K_d 집합을 할당 받는다.

불법 복제된 콘텐츠의 사용을 제한하기 위하여 K_m은 폐지된 기기(Revoked Device)가 갖고 있는 K_d 집합을 제외한 K_d들로 암호화 된다. 이렇게 암호화된 K_m을 미디어 키 블럭(Media Key Block, MKB)이라 부른다. MKB는 K_t로 암호화된 콘텐츠 및 K_m으로 암호화된 K_t와 함께 Media에 저장된다.

BES를 이용한 Media 보안 기술로 보호된 콘텐츠는 모든 인가된 기기(Privileged Device)에서 제약 없이 이용할 수 있다. 개인 콘텐츠를 Media에 저장/관리하는 경우, 앞서 설명한 Media 보안 기술로 암호화 시켜도 인가된 기기에서는 콘텐츠를 자유롭게 이용할 수 있기 때문에 Media의 도난 또는 분실로 인하여 콘텐츠가 외부로 유출되는 경우 사생활 침해를 막을 수 없다. 이와 같은 사생활 침해를 막기 위해 콘텐츠 불법복제 방지 외에도 개인 콘텐츠 관리를 위한 별도의 인증 및 암호 정책이 필요하다.

일반적으로 암호키는 안전성을 보장하기 위하여 128 비트 이상의 난수 키를 사용하고 있다. 그러나 이와 같은 키를 사용자가 정확히 기억하기는 어렵다. 이러한 문

제를 해결하기 위한 방안의 하나가 사용자 패스워드 기반의 암호 키 관리 기법(Password based Encryption Scheme, PES)이다[9]. PES는 현재 인터넷 뱅킹 등에서도 사용되는 PKCS에 정의되어 실제 사용되고 있다.[10] PES는 사용자가 입력한 패스워드를 이용하여 암호키를 생성하는 기법으로 사전 공격(Dictionary Attack)에 대해 강인성을 갖도록 설계되었다.

본 논문에서는 HDDVD등에서 채택한 AACS의 Recordable Media의 보안 표준을 분석하고, PES를 활용하여 개인 콘텐츠를 안전하게 관리할 수 있는 접근 제어 방안을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 AACS에서 정의한 Media 보안과 PES에 대하여 설명한다. 3장에서는 AACS의 Media 보안 Framework에 사생활 보호 기능을 추가한 개선된 Media 보안 Framework를 제안한다.

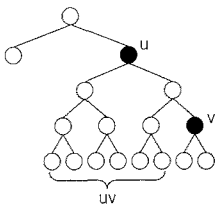
Ⅱ. Media Security

2.1 Security Technology

이 절에서는 AACS의 BES와 PES에 대하여 간략하게 설명한다. AACS는 콘텐츠를 암호화 하고 비인가 기기를 제어하기 위해서 Subset Difference(SD) Scheme을 사용한다[7,12]. SD에서는 사용자 기기를 관리하기 위하여 이진 트리 구조를 이용하며, 이진 트리의 최하위 노드(Leaf Node)에 사용자 기기를 대응시켜 관리한다. 또한, K_d의 관리를 위해 부분차(Subset Difference) 개념을 이용하여 사용자 기기를 관리한다.

정의 1. u와 v를 이진 트리의 내부 노드라 하자. u는 v의 상위 노드라 하자. 부분차 uv는 u를 루트 노드로 하는 부분 트리(subtree)에서 v를 루트 노드로 하는 부분 트리를 제외시킨 부분 트리이다.

[그림 1]에서 부분차 uv는 u를 루트 노드로 갖는 부분 트리의 최하위 노드 8개 중에서 v를 루트 노드로 갖는 부분 트리의 최하위 노드 2개를 제외한 6개의 최하위 노드들로 구성된 부분 트리를 의미한다. 부분차 uv마다 서로 다른 K_d가 할당되며, uv에 할당된 K_d를 $K_{d(uv)}$라고 표시하도록 한다. $K_{d(uv)}$는 uv의 최하위 노



[그림 1] 부분차 uv

드에 대응되는 기기들만 공유한다. 전체 기기 집합을 D라 하고, 폐지된 기기의 집합을 R이라 하자. 또한 uv의 최하위 노드들의 집합을 $\overline{uv}$ 라 하자. 암호화된 K_m을 안전하게 전송하기 위하여 서비스 제공자는 우선 부분차들의 집합 $\{u_iv_i\}$를 다음과 같이 선택 한다 :

$$D-R=\bigcup_i \overline{u_iv_i}\,. \tag{1}$$

서비스 제공자는 이렇게 선택된 부분차들의 집합 $\{u_iv_i\}$에 할당된 $\{K_{d(u,v)}\}$로 K_m을 암호화해서 모든 기기들에게 전송한다. 폐지된 기기에 대응되는 최하위 노드는 $\bigcup_i \overline{u_iv_i}$의 원소가 될 수 없으므로, $\{K_{d(u,v)}\}$에 속한 어떤 $K_{d(u,v)}$도 확보할 수 없다. 그러므로 폐지된 기기는 스크램블된 콘텐츠를 디스크램블해서 이용할 수 없다.

PES는 Morris 와 Thompson에 의해 소개되었다[9]. 패스워드는 일반적으로 사용자가 쉽게 기억할 수 있을 정도의 값을 사용하기 때문에 암호키로 바로 사용할 수 없다. 그러므로 패스워드를 추측하는 공격 기법에 대응하기 위해 키 생성을 위한 추가적인 과정이 필요하다. Morris와 Thompson은 패스워드 추측을 위한 사전 공격(Dictionary Attack)에 대응하기 위하여 salt 개념을 도입하였다. 암호키를 생성할 때 사용자 패스워드와 함께 salt를 사용함으로써, 암호키에 대한 사전 공격을 어렵게 하는 효과를 거둘 수 있다. PKCS #5 v1.5에서는 패스워드, salt 와 함께 iteration count를 사용한다. 현재 v2.0이 인터넷 뱅킹과 같은 공개키 인증서 기반의 서비스에 적용되고 있다[10,11].

본 논문에서는 이와 같이 PES를 통해 생성된 키를 다른 키들과 구분하기 위하여 패스워드키라 부르고, K_p로 표시한다.

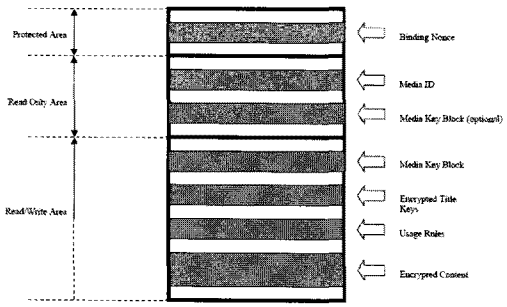
2.2 AACS 보안 구성

AACS의 Recordable Media는 콘텐츠의 불법복제를 제어하기 위하여 [그림 2]와 같은 데이터 구조를 사용한다. Read/Write Area에 암호화된 콘텐츠와 암호키가 저장된다. 주요 구성은 다음과 같다 :

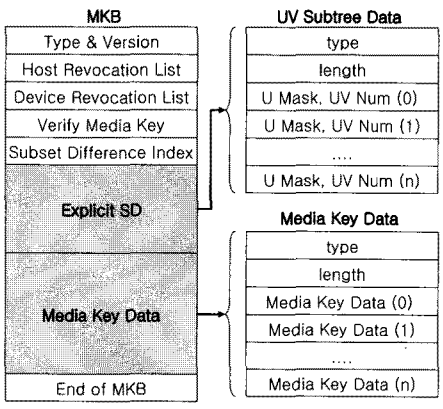
- Encrypted Content : K_t로 암호화된 콘텐츠 저장.
- Encrypted Title Keys : K_m으로 암호화된 K_t 저장.
- Media Key Block(MKB) : K_d들로 암호화된 K_m 저장.

콘텐츠를 불법 복제에 사용될 수 있는 폐지 기기를 제어하기 위해, 콘텐츠를 암호화해서 저장하고, 폐지된 기기들이 K_m과 K_t를 확보할 수 없도록 MKB를 구성한다. [그림 3]은 SD를 이용한 MKB의 구성 예이다. MKB의 주요 구성은 다음과 같다 :

- Explicit Subset Difference(SD) : 인가된 기기들의 정보를 저장한다. Explicit SD에 속한 부분차 uv의 최하위 노드에 대응하는 기기는 인가된 정상 기기로 간주한다.
- Media Key Data : K_d들로 암호화된 K_m의 집합으로 구성된다.



[그림 2] Recordable Media Framework

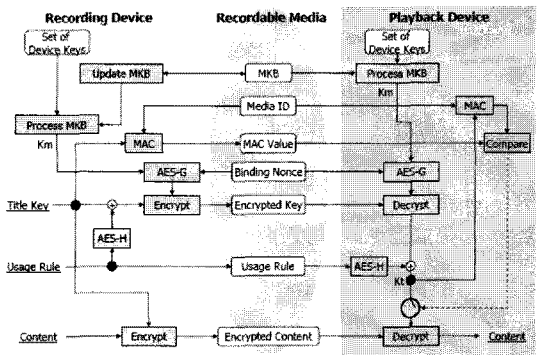


[그림 3] Example of MKB

Explicit SD에 포함된 uv와 Media Key Data에 속한 암호화된 K_m은 일대일 순차 대응된다. 그러므로 사용자 기기가 n번째 uv의 최하위 노드에 대응되면 Media Key Data의 n번째 암호화된 K_m를 복호화 할 수 있다. 사용자 기기가 암호화된 콘텐츠를 복호화 하는 과정은 다음과 같다 :

- 사용자 기기는 Explicit SD를 확인하여 해당 기기에 대응되는 최하위 노드를 포함하는 uv가 있는지 확인한다.
- 확인된 uv를 할당된 $K_{d(uv)}$ 선택한다.
- Media Key Data에서 uv에 대응되는 암호화된 K_m을 선택한 후, $K_{d(uv)}$로 복호화한다.
- 순차적으로 K_t와 콘텐츠를 복호화 한다.

[그림 4]는 앞서 설명한 것처럼 사용자가 콘텐츠를 저장하고, 이를 이용하기 위한 절차를 설명한다. 사용자 기기는 난수 키 K_t를 생성하여 콘텐츠를 암호화 한 후 Media에 저장하고, K_d들을 이용하여 갱신된 MKB로부터 K_m을 추출하여 난수 키인 K_t를 암호화해서 Media에 저장한다. 마지막으로 갱신된 MKB를 Media에 저장한다. 재생기기는 역순으로 키를 추출하여 콘텐츠를 복호화 한다.



[그림 4] 콘텐츠 암/복호 과정

Ⅲ. Privacy 보호를 위한 MKB 구성

3.1 사용자 제작 콘텐츠 보안 요구 사항

사용자의 개인 콘텐츠가 저장된 Media의 도난이나 분실 등과 같은 사고에 대응하기 위해서는 다음과 같은 요 사항이 만족 되어야한다 :

요구사항 1. 사용자는 자신의 콘텐츠 재생기기 또는 자신이 지정한 재생기기에서만 개인 콘텐츠를 이용할 수 있도록 제어할 수 있어야한다.

요구사항 1이 만족된다고 가정할 때, 지정한 기기의 고장, 분실, 교체 등이 발생할 경우, 사용자는 더 이상 해당 콘텐츠를 이용할 수 없게 된다. 그러므로 다음과 같은 요구 사항이 만족 되어야한다 :

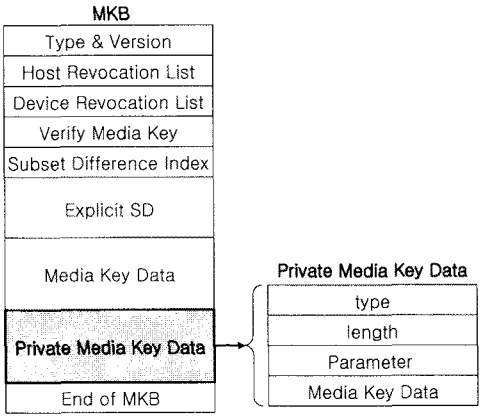
요구사항 2. 기존의 사용자 기기가 교체되어도 콘텐츠 소유자는 해당 콘텐츠를 계속 이용할 수 있어야 한다.

3.2 새로운 MKB 구성

이 절에서는 사용자가 개인 콘텐츠를 Media에 저장할 때, 3.1절의 2가지 요구사항을 만족시킬 수 있는 새로운 MKB 구조와 처리 방안을 제안한다. 요구사항 1과 2를 동시에 만족시키기 위해 본 논문에서는 사용자가 지정한 콘텐츠 재생기기에만 유일하게 할당된 K_d로 MKB의 부분차를 구성하고, 해당 기기의 교체 시에도 MKB의 판독이 가능할 수 있도록 사용자 패스워드 기반으로 K_m을 암/복호화 할 수 있도록 필요한 정보를 MKB에 추가한 새로운 MKB 구조를 제안한다.

[그림 5]는 요구사항 1과 요구사항 2를 만족시키기 위해 본 논문에서 새롭게 제안하는 MKB의 구조를 나타낸다. 새롭게 제안하는 MKB에는 Private Media Key Data 항목이 추가 되었다. Private Media Key Data는 사용자가 패스워드를 기반으로 K_m를 암호화 하고, 이를 복호화 할 때 필요한 정보를 저장한다. 본 논문에서는 PKCS #5를 기반으로 Private Media Key Data 항목의 구조를 다음과 같이 제안 한다 :

- Parameter : 사용자가 지정한 패스워드로부터 암호키(K_p)를 생성할 때 필요로 하는 정보를 저장한다.



[그림 5] 새로운 MKB의 구조

```
PBKDF2-params::=SEQUENCE{
 salt CHOICE {
  specified OCTET STRING,
  otherSource AlgorithmIdentifier {{PBKDF2-SaltSources}}
 },
 iterationCount INTEGER (1..MAX),
 keyLength INTEGER (1,..,MAX) OPTIONAL,
 prf AlgoritihmIdentifier {{PBKDF2-PRFs}} DEFAULT
  algid-hmacWithSHA1}
```

[그림 6] PBKDF2-params 구조

안전한 난수 암호키 생성을 위하여 PKCS#5에서는 salt와 iteration number가 사용 된다. 본 논문에서는 PKCS#5의 PBKDF2에서 정의된 parameter 구조를 사용한다. PKCS#5의 PBKDF2의 ASN.1 구조는 [그림 6]과 같다.

- Media Key Data : PKCS#5의 PBKDF2를 이용하여 생성된 K_p로 암호화된 K_m을 저장한다.

3.3 새로운 MKB 운영

본 논문에서 제안하는 MKB를 구성하기 위해서, 본 논문에서는 사용자가 지정한 재생기기와 녹화기기는 다음과 같은 성능을 갖고 있다고 가정 한다 :

가정 1. 녹화기기는 사용자가 지정한 재생 기기와 보안 통신이 가능하다. 사용자 기기 사이의 인증 및 보안 채널 형성은 본 논문의 범위를 벗어나는 주제이므로, 이와 같은 기능은 사용자 기기 사이에 정의 되고, 구현 되어 있다고 가정한다.

가정 2. 녹화기기 또는 재생 기기는 사용자로부터 필요한 정보(기기 식별자, 사용자 패스워드)를 입력받을 수 있다.

제안하는 MKB 운영은 [그림 4]에서 설명한 기존의 MKB 운영과 유사하다. 단, K_m을 암호화 하고 이를 저장하는 방법에 차이가 있다. 본 절에서는 K_m의 처리 과정만을 자세히 설명하도록 하겠다.

3.3.1 Media Key 암호화

사용자가 지정한 재생기기(Playback Device, PD)에 대응하는 최하위 노드와 그 형제 노드(Sibling Node)를 각각 v_i와 v_{i+1}라 하자. 또한 v_i의 부모 노드(Parent Node)를 u라고 하자. 제안하는 MKB의 구성을 위해 녹화기기(Recording Device, RD) 및 재생기기(PD)는 다음과 같은 과정을 수행 한다 :

- K_m 생성 및 전송 : RD는 K_m을 랜덤하게 생성한 후, 사용자가 지정한 PD로 전송한다. 이 때, 두 기기 사이에는 인증 및 보안 채널이 형성되었다고 가정한다.
- 부분차 uv_{i+1} 및 $K_{d(uv_{i+1})}$ 선택 : PD는 uv_{i+1}와 $K_{d(uv_{i+1})}$을 선택한다. K_m을 $K_{d(uv_{i+1})}$로 암호화 한 후, uv_{i+1} 정보와 함께 RD로 전송한다.
- MKB 구성 : RD는 수신된 uv_{i+1} 정보를 가지고 Explicit SD와 Subset Difference Index를 구성한다. 또한 암호화된 K_m으로 Media Key Data를 구성한다.
- 사용자 패스워드 처리 : RD는 salt와 iteration count를 랜덤하게 생성한다. 또한 사용자에게 패스워드 입력을 요청한 후, 입력된 패스워드와 생성한 salt 및 iteration count를 사용하여 난수 암호키를 생성한 후, K_m을 암호화 한다. salt, iteration count 및 암호화된 K_m으로 Private Media Key Data를 구성한다.

이렇게 구성된 MKB는 해당 사용자가 지정한 기기에서만 암호화된 K_m을 복호화 시킬 수 있다. 그러므로 다른 기기의 일반적인 MKB 갱신 과정과 구분되어야 한다. 이를 위하여 MKB의 Type and Version 값을 새롭게 정의한다. 현재 Type3과 Type4를 위한 값이 지정되어 있으므로, Type 5 이상의 값으로 새롭게 지정할 필요가 있다. 본 논문에서는 설명을 위하여 사용자 지정 MKB를 Type 5로 정의하고, 00051003_{16} 값으로 MBK Type을 지정한다.

3.3.2 Media Key 복호화

사용자가 Media를 PD에 삽입하면, PD는 해당 Media의 MKB의 Type and Version을 확인한다. 지정된 type이 Type 5인 경우, MKB 갱신과정을 생략하고 다음을 수행 한다 :

- 부분차 탐색 : Explicit SD와 Subset Difference Index에서 PD에 대응하는 부분차 uv 를 찾는다.
- K_d 선택 또는 K_p 계산 : 대응되는 부분차 uv 를 찾았다면, 해당 uv 에 대응하는 $K_{d(uv)}$를 선택한다. 만약 적당한 부분차를 찾을 수 없다면, PD는 사용자에게 패스워드 입력을 요청하고, 입력된 패스워드와 Private Media Key Data의 salt와 iteration count를 이용하여 K_p를 생성한다.
- K_m 복호화 : K_d 또는 K_p를 이용하여 암호화된 K_m을 복호화 한다. 복호화 된 K_m을 확인하기 위해 MBK의 Verify Media Key의 Verification Data (D_v)와 복호화된 K_m을 이용하여 다음을 계산한다 :

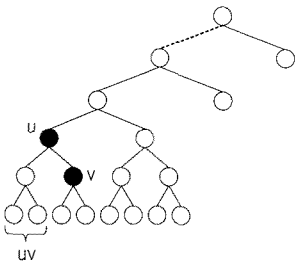
$$AES_{128}(K_m, D_v) \tag{2}$$

계산된 값의 상위 64비트의 값이 아래 값과 같다면 복호화된 K_m의 값이 정확한 것으로 간주한다 :

$$0123456789ABCDEF_{16}. \tag{3}$$

3.3.3 MKB 예

본 절에서는 MKB의 실제 구성 예를 들어 제안하는 MKB의 구성을 설명한다. 설명을 위해 사용자가 2개의 PD만을 지정한 경우를 가정하고, 사용자의 PD에 할당된 최하위 노드들의 위치는 [그림 7]와 같이 binary tree에서 가장 좌측에 위치한 2개라 가정하자. MKB 구성을 위한 정보는 다음과 같다 :



〔그림 7〕 Example

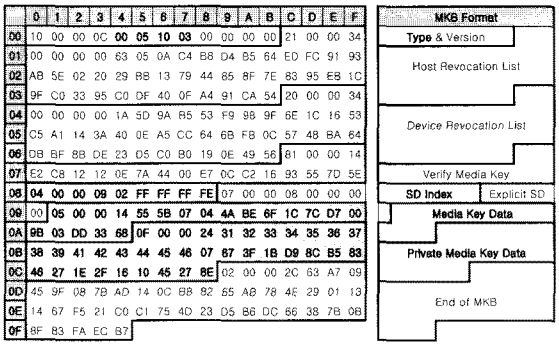
- device number (31bits)=
  - device A : $0000...000_2$
  - device B : $0000...001_2$
- K_m = $000102030405060708090A0B0C0D0E0F_{16}$
- 부분차 uv
  - uv = $FFFFFFFE_{16}$, u bit mask = 02_{16}
  - $K_{d(uv)}$ = $FF102030405060708090A0B0C0D0E0F0_{16}$
  - encryted K_m = $555B07044ABE6F1C7CD7009B03DD3368_{16}$
- 패스워드 정보
  - salt = "123456789ABCDEF"
  - iteration number = 7
  - 패스워드 = "aacs07security"

위와 같은 패스워드 정보를 이용하여 SHA1기반으로 생성된 키 K_p와 암호화된 K_m은 다음과 같다 :

- K_p=$F2C58618BAC297B7F88F3D66B80E608F_{16}$
- encryted K_m = $673F1BD98CB58346271E2F161045278E_{16}$

단, 각각의 record에 포함된 서명 값 생성을 위해 사용된 비밀 키 및 공개 키는 각각 다음과 같다 :

- Private Key : $367D76ADB6A0056F528E3F1EF317E00B14852449_{16}$
- Public Key
  - x : $2CFF17FF209F1656CB42BC93E82403A3033C85CF_{16}$
  - y : $75B97D8E247795EAC781FBF09D5736856ABBF37716$



〔그림 8〕 MKB 예

[그림 8]은 이와 같은 정보를 바탕으로 구성된 MBK이다.

3.3.4 분석

저장매체(Recordable Media)를 위한 AACS의 보안은 서론에서 언급한 것처럼 불법 복제를 방지하기 위해 폐지된(Revoked) 기기들의 콘텐츠 접근을 제어하는 것을 목적으로 하고 있다. 이러한 폐지된 기기는 불법 복제에 악용될 수 있는 기기를 의미하며, 그 목록은 공인된 협회에서 관리된다. 폐지된 기기들의 목록에 기반 한 콘텐츠 접근 제어는 상업 영화와 같은 유료 콘텐츠 보호에는 적합하다. 그러나 개인의 사생활을 주 내용으로 하는 개인 콘텐츠에 이와 같은 접근 제어 방식을 적용할 경우, 분실 또는 도난과 같은 사고로 인하여 개인의 사생활이 노출되는 문제를 해결할 수 없다.

개선된 AACS Framework는 폐지된 기기 목록에 기반 한 접근 제어뿐만 아니라 개인 콘텐츠의 특성을 고려하여 3.1절에서 정의한 보안 요구사항1과 2를 모두 만족하도록 설계되었다. 즉, 사용자가 지정한 기기의 고유 키들로만 한정하여 MKB를 구성하게 함으로써 개인 콘텐츠 소유자는 폐지 목록에 없는 인가된 기기들의 접근을 제어 할 수 있도록 설계되었다(요구사항 1). 사용자가 지정하지 않은 기기는 폐지 목록에 포함되지 않았어도 MKB에서 콘텐츠 복호화에 필요한 키 정보를 추출할 수 없다. 또한, 기기의 교체 또는 다른 기기에서 콘텐츠를 재생할 경우와 같이 MKB를 구성할 때 사용한 고유 키들을 획득할 수 없는 경우에도 콘텐츠 소유자는 자신이 지정한 패스워드 정보를 기기에 입력하여 Private MKB를 이용하여 콘텐츠를 재생할 수 있다(요구사항 2).

그러므로 개선된 AACS는 기존의 폐지 목록 기반의

접근제어 뿐만 아니라 인증된 기기들의 접근 제어 기능을 추가적으로 제공함으로써 개인 콘텐츠 유출에 따른 Privacy 침해를 예방할 수 있다.

Ⅳ. 결 론

DVD 또는 HD-DVD와 같은 Media를 통한 개인 콘텐츠 관리는 보편적으로 이용될 것이다. 그러나 개인의 콘텐츠가 외부로 유출될 경우, 사생활 침해와 같은 문제를 발생시킬 수 있다. 현재 Media 보안 표준은 불법복제 방지를 위한 기기제어에 초점이 맞춰져 있다. 그러므로 도난 또는 분실로 인한 사생활 침해와 같은 문제를 해결할 수 없다.

본 논문에서는 차세대 Media 표준에서 채택하고 있는 AACS를 바탕으로, 사용자의 개인 콘텐츠를 안전하게 저장/관리 할 수 있는 수정안을 제안한다. 제안된 수정안은 사용자가 지정한 디바이스의 키로 콘텐츠를 암호화 할 뿐 아니라 사용자 패스워드 기반으로 콘텐츠를 암호화 하는 기능을 제공함으로써 기기교체 시에도 콘텐츠를 계속 이용할 수 있도록 설계 되었다.

참고문헌

[1] CSS, Content Scramble System, available at http://www.dvdcca.org/ccs/

[2] Jeffrey A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul M. G. Linnartz, Mattehew L. Miller, C. Brendan S. Traw, "Copy Protection for DVD Video", Proceedings of the IEEE. Vol. 87, No. 7, 1267-1276, July 1999.

[3] CPPM, Content Protection for Prerecorded Media, available at http://www.4centity.com/docs/vers ions.html

[4] CPRM, Content Protection for Recordable Media, available at http://www.4centity.com/docs/vers ions.html

[5] AACS. Recordable Video Book, Revision 0.91, February 17, 2006.

[6] A. Fiat and M. Naor, "Broadcast Encryption", CRYPTO 1993, LNCS 773, pp. 480-491. 1993.

[7] D. Naor, M. Naor and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", CRYPTO 2001, LNCS2139, pp. 41-62, 2001.

[8] Nam-Su Jho, Jung Yeon Hwang, Jung Hee Cheon, Myung-Hwan Kim, Dong Hoon Lee, and Eun sun Yoo, "One-Way Chain Based Broadcast Engryption Schemes", EUROCRYPT 2005, LNCS 3494, pp. 559-574, 2005.

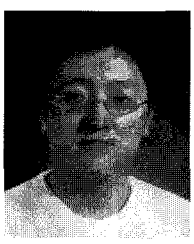
[9] Robert Morris, Ken Thompson, "Password security : A case history", Communication of ACM, 22(11): 594-597, November 1979.

[10] PKCS#5 v2.0: Password-based cryptography standard, RSA Laboratories, March 25, 1999

[11] PKCS#8 v1.2: Private-Key Information Syntax Standard, RSA Laboratories, November 1, 1993.

[12] AACS. Introduction and Common Cryptographic Elements, Revision 0.91, February 17, 2006.

〈著者紹介〉



김 대 엽 (DaeYoub Kim) 종신회원

1994년 2월 : 고려대학교 수학과 졸업
1996년 8월 : 고려대학교 수학과 석사(대수학 전공)
2000년 2월 : 고려대학교 수학과 박사(대수학 전공)
1997년 8월~2001년 3월 : (주)텔리맨, 위성통신 연구소, CAS팀 선임연구원
2001년 4월~2002년 7월 : 삼성 시큐아이닷컴(주) 정보보호 연구소 PKI실 차장
2002년 9월~현재 : 삼성전자, 기술총괄, SAIT, 수석연구원
<관심분야> CAS/DRM, PKI, Smart Card, 보안프로토콜, 네트워크보안