IPTV 방송 콘텐츠의 보호 기술

IPTV Contents Protection Technology

이완복, 노창현, 우제학*
중부대학교, (주)코어트러스트*

Lee Wan-Bok, Roh Chang-Hyun, Woo Je-Hak*
Joongbu Univ., CoreTrust Inc.*

요약

최근 정보통신부가 발표한 IT839 전략에 따르면, 향후 방송과 통신의 융합 흐름은 더욱 가속화될 전망이다. 특히, 광대역 통합망(BCN) 환경이 구축되면 IPTV 서비스는 더욱 많은 수요를 불러올 것으로 예상되는데, 성공적인 사업화와 서비스 활성화를 위해서는 방송 콘텐츠의 저작권 보호 방안이 절실히 요구되고 있다. 본 논문에서는 IPTV 방송 서비스의 특성과 그에 따라 요구되는 콘텐츠 보안의 문제점들을 살펴보고자 한다. 이를 위해 IPTV의 기본 보안 모델을 제시하고, 그것을 기반으로 기존의 CAS, DRM 기술을 적용하는데 어떠한 한계점들이 있는 지를 분석한다.

Abstract

According to the IT839 strategy which was announced by the Ministry of Information and Communication(MIC) in 2004, the convergence trend of the broadcasting and the communication would be much more promoted. Thus, the methods for protecting the broadcasting contents will be indispensible elements for the successful IPTV service achievement. This paper describes the characteristics of IPTV and the related contents protection techniques. To evaluate several security issues, we suggest a security model for IPTV, and speculate the most widespread, two security technologies for IPTV such as CAS and DRM.

I. 서 론

최근에 전개되고 있는 방송과 통신의 융합 흐름은 방송 영역에서 제공되던 멀티미디어 콘텐츠를 초고속 인터넷, 케이블 TV망, 위성망 등을 통해 실시간 전송하는 서비스로 구체화되고 있다. 이미 기간 통신사업자를 비롯한 케이블 TV 서비스 제공자 등 주요 통신 및 방송사업자들이 초고속 인터넷과 인터넷 전화 (VoIP), TV를 하나로 묶는 트리플 플레이 서비스(Triple Play Service)의 제공을 계획하고 있다. 위성DMB, 지상파DMB 등 TV 콘텐츠와 각종 데이터 방송 콘텐츠를 통합하는 신개념의 방송 통신 융합 서비스도 2005년부터는 본격화 될 전망이다.

이러한 추세에 따라 대부분의 대형 통신사업자들이 주문형 비디오(VOD)뿐만 아니라 IPTV가 가능한 IP 셋톱박스의 시범 서비스를 추진 중이거나 초기 상용 서비스를 시작했다. 대표적으로 KT의 홈엔(HomeN) 서비스나 독일 T—Online의 서비스가 이런 범주에 해당된다.

그러나 디지털 방송 서비스가 다양한 매체로 확장되는 것이 필연적임에도 불구하고, 이 서비스에 콘텐츠를 공급하는 대부분의 콘텐츠 공급자들은 콘텐츠 보호에 대한 근원적인 불안감을 떨치지 못한 상태이

다. 특히, 디지털 콘텐츠가 IP 망을 통해서 내부 데이터의 복제가 자유로운 PC와 유사한 구조의 IP 셋톱 박스로 서비스되는 IPTV 모델에서의 콘텐츠 보안 문제를 심각한 걱정거리로 생각하고 있다. 본 연구에서는 IPTV 서비스에 필요한 콘텐츠 보안의 기본 모델을 제시하고, 그에 대한 근본적인 해결 방안을 모색하고자 한다. TV 콘텐츠 보안에 대해서는 CAS (Conditional Access System)와 DRM (Digital Rights Management) 기술이 이미 상용 서비스에 활용되고 있다. 이들 기술의 특성과 IPTV 보안에 대한 적합성을 살펴 보도록 한다.

논문의 구성은 다음과 같다. 2장에서는 IPTV 서비스의 특성과 논란거리, 그리고 IPTV 보안모델을 제시하고, 3장에서는 주요 IPTV 보안 기술을 소개하고 장단점을 평가해본다. 4장에서는 결론을 맺는다.

II. IPTV 서비스와 보안모델

1. IPTV 서비스

IPTV(Internet Protocol TV: 인터넷 TV)는 일반적으로 IP 네트워크를 통해 고화질 생방송·주문형 비디오(VOD)·TV 콘텐츠 등을 제공하는 방송·통신 융합 서비스이다[1]. 이와 같은 IPTV서비스가 도래하게 된 배경으로서는 다음과 같은 디지털 방송의 특성을 생각해 볼 수 있다.

- **유연성** : 단순한 방송뿐 만이 아니라, 디지털 컴퓨터에서 제공할 수 있는 다양한 신규 부가 서비스를 제공할 수 있다.
- **기능성** : 사용자의 기호에 부합하도록 맞춤 프로그램 및 데이터의 제공이 가능하다
- **효율성** : 전송 파워가 적어진다
- **품질** : 전송 노이즈가 없으며, 채널간의 혼선 등이 사라지게 된다.

특히, IPTV는 단방향으로 서비스되던 기존 방송의 틀을 깨고, 양방향으로 데이터 송수신이 가능한 IP망을 기반으로 하고 있기 때문에 여러 장점을 가질 수 있다. 그 중 한 가지는 쌍방향(Interactive) 서비스가 가능해짐에 따라 소비자가 원하는 대로 비디오 서비스(VoD) 뿐만 아니라 T-Commerce 구현이 용이해진다는 것이다. 이밖에도 P2P 전달방식으로 개인화된 채널을 볼 수 있게 되고, 여러 개인화된 TV 포털이 등장할 수 있게 되며, 초고속 인터넷, VoIP 와의 결합을 통해 번들 서비스가 용이해짐에 따라 트리플 플레이 서비스 제공이 가능하다는 이점이 있다.

그러나 IPTV 서비스를 제공할 수 있는 커다란 두 주체, 통신사업자와 방송사업자 사이에서는 IPTV 서비스의 성질과 그 규제에 있어 큰 시각차를 보이며 논쟁이 심화되고 있다. 통신사업자는 IPTV가 통신기술 발전에 의한 자연적인 신규 서비스로서, 방송콘텐츠를 인터넷·서버 등에 결합한 통신서비스로 바라보고 있다. 반면, 방송사업자는 방송 프로그램을 기획·편성·제작해 공중에 송신하는 것이므로 방송에 해당하며, 비밀성이 없으므로 통신이 아니라고 주장한다. 통신업계와 방송업계의 주장이 팽팽히 맞서자 정통부와 방송위는 지난해부터 네 차례나 만나 협상을 벌였으나 아직까지 합의점을 찾지 못한 실정이다.

2. IPTV 보안 모델

IPTV 시스템은 IP 기술의 발전에 따라 자생적으로 생성된 모델이기 때문에, 특정 표준이나 시스템 모델이 압도적인 지위를 갖지 못하는 초기 단계의 기술이다. 실제로, 대체적인 서비스와 비용 구조는 나타나 있지만 전달 콘텐츠에 대한 포맷과 코덱이 특정 표준으로 정해지지 않았고, 관련 서비스에 대한 구체적인 기능도 설정되지 못한 상황이다. 현재는 방송 관련된 여러 표준을 준용하여 다양한 형태의 시스템을 구성하고 시범 서비스 정도를 제공하고 있는 단계라고 볼 수 있다.

IPTV 시스템에 대한 표준 모델이 존재하지 않는 것과 마찬가지로 콘텐츠 보안에 대한 대응 방안 또한 구체적으로 제시되지 않고 있다. 기존의 방송 시스템

에서 시청자의 접근 제어를 목적으로 사용되던 CAS가 하나의 대안으로 활용될 수 있지만, IPTV가 제공하고자 하는 다양한 부가 서비스에 대해서는 여러 가지 단점을 보이고 있다. 예를 들어 PVR (Private Video Recording)과 같이 하드 디스크 저장이 필요한 서비스에 대한 콘텐츠 보호 문제는 CAS만으로는 대응이 어려운 문제이다.

CAS의 부족한 기능을 대체할 수 있는 시스템으로 IP 및 PC 환경에서 발전되어 온 DRM 기술을 생각할 수 있다. DRM 기술은 디지털로 유통되는 모든 콘텐츠 종류에 대한 불법 사용 및 불법 복제에 대응하기 위한 기술로서, CAS 보다는 더 넓은 범위에서 콘텐츠 보안 문제를 해결할 수 있다. 그러나, DRM 기술이 PVR같은 서비스에 적용이 용이한 기술이긴 하나, 현재의 방송 시스템에 그대로 적용하기에는 부족한 점이 존재한다. 왜냐하면 DRM은 온라인 기반의 양방향 통신 구조를 전제로 고안된 기술이기 때문이다.

이와 같이 어느 한 종류의 기존 기술만 가지고 IPTV의 콘텐츠 보안 문제를 대응하기에는 실제적으로 어려운 문제들이 존재한다. 그렇다면 CAS와 DRM의 융합을 통한 문제 해결 방안의 도출이 가능할 수 있을까? 이 질문에 대한 답을 바로 제시하기가 어려운 여러 가지 이유가 있을 수 있는데, 그 중 가장 큰 문제점은 어느 단계에서의 통합이 적절한 가를 결정하는 것이다. 이 절에서는 CAS와 DRM의 단순 통합을 논하기에 앞서, IPTV 시스템이 가져야 하는 근본적인 보안 요소들을 먼저 분석해 보고자 한다. 이러한 보안 요소들의 집합을 IPTV 보안 모델이라 정의하도록 하자. 다음은 IPTV 보안 모델의 구성 요소와 그 내용을 요약한 것이다.

■ 사용자 인증 (User Authentication)

전체 서비스에 대한 사용자를 식별하고 권한을 부여하는 과정을 의미한다. 사용자의 식별 방법은 크게 ID와 패스워드를 이용하는 전통적인 방법과 스마트 카드를 이용하는 방법으로 나눌 수 있다.

■ 디바이스 인증 (Device Authentication)

디바이스 인증은 사용자 인증과 병행하여 이루어진다. 사용자 인증 바로 다음 단계에 디바이스 인증을 수행할 수도 있고, 디바이스를 먼저 인증하고 그 범위 내에서 사용자 인증을 수행할 수도 있다.

■ 스트림 접근 제어 (Stream Access Control)

특정 방송 프로그램 또는 채널의 스트림에 대한 접근을 제어해야 한다. 접근 권한을 가진 사용자만이 스트림을 정상적으로 렌더링할 수 있도록 한다. 이러한 제어는 VOD 콘텐츠의 스트림에 대해서도 그대로 적용된다. 아울러 PPV (Pay Per View), 시청 지역 제한, 시청 등급 제한 등과 같은 부가 기능에 대한 제어도 포함된다.

■ 스트림 복사 제어 (Stream Copy Control)

모든 콘텐츠 스트림에 대한 불법 복제 방지 기능을 구현해야 한다. 이를 위해 스트림 통로에 대한 보호, 불법 저장 방지, 저장 콘텐츠 보호 등의 작업을 수행한다. 구체적으로는 하드 디스크 저장 제어 기능을 실행한다. 저장된 콘텐츠에 대해 유효 기간 및 플레이 횟수 제어 등을 수행한다. 끝으로 W&R(Watch and Record), TSR(Time Shift Recording), PVR 등의 기능으로 인한 콘텐츠 불법 유출이 발생하지 않도록 제어해야 한다.

III. IPTV 콘텐츠 보호 기술

1. Conditional Acces System(CAS)

CAS는 과거 아날로그 방송 시절부터 유료 방송 서비스를 위해 방송 서비스에 대한 고객의 접근 여부를 제어하는 기본 시스템으로 사용되어 왔다[2]. CAS가 제어하는 접근 조건으로는 시청료 납부, 수신 지역,

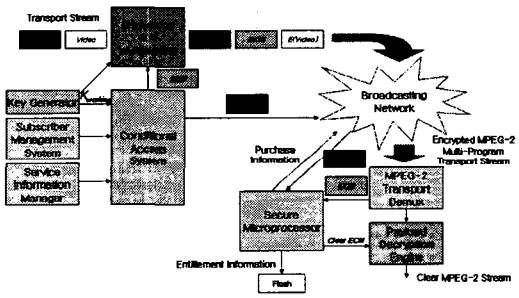
수신 등급 등이 포함된다. 따라서 CAS는 유료 방송 사업자의 비즈니스와 수익을 보호하는 것이 기본 목적인 시스템이다. 표준으로는 유럽의 DVB CAS, 미국의 ATSC CAS가 제정되어 있으며, OpenCable CAS는 ATSC CAS에 기반을 둔 미국의 디지털 케이블 TV를 위한 표준이다. CAS에 대한 표준이 제정되어 있기는 하지만, CAS의 내부 상세 구현에 대한 규격은 정의되어 있지 않다. 따라서 여러 CAS의 병존은 가능하나 이종 CAS간의 호환은 불가능한 구조로 되어 있다.

특정 방송 서비스를 시청할 수 있도록 사용자에게 부여되는 권한을 수신자격(Entitlement)이라 하는데, CAS 는 이 수신자격을 가진 사용자가 허용된 서비스만을 시청하도록 제어하는 시스템 이다. 수신자격의 적용 대상은 특정 프로그램이 될 수도 있고, TV 채널의 집합이 될 수도 있다.

CAS는 사용자가 자신의 수신자격을 행사하기 위해 필요한 복호화 키 및 수신 조건을 포함하는 ECM(Entitlement Control Message)과 방송 서비스에 대한 수신자격 정보와 그 수신자격을 받을 사용자 정보를 포함하는 EMM(Entitlement Management Message)을 기본 요소로 구성된다. 각 프로그램 또는 채널 별로 생성되는 ECM은 MPEG-2 트랜스포트 스트림(Transport Stream)을 통해 비디오 및 오디오 콤포넌트들과 같이 전달된다. ECM에는 실제 서비스 키에 의해 암호화된 제어 단어(Control Word)가 포함되는데, 이 제어 단어가 바로 방송 스트림을 복호화 하기 위해 사용되는 복호화 키이다. 이 ECM은 사용자의 방송 채널 전환 요구에 바로 대응할 수 있기 위해 초 단위의 빠른 주기로 계속해서 전송될 필요가 있다.

EMM을 통해 전달되는 실제 수신자격 정보에는 서비스 키가 포함되고, 이 키는 ECM의 제어 단어를 추출하는데 사용된다. 한번 전송된 수신자격 정보는 보통 스마트 카드(Smart Card) 내에 저장되고, 가입자 정보가 변경되었을 때나 또는 주기적으로 신규 EMM을 통해 발급된다. 이 EMM은 OpenCable 표준에서는 OOB (Out of Band)로 전달되고, DVB 표준에서는 트랜스포트 스트림과 함께 전달된다.

다음 그림 1은 이러한 ECM과 EMM이 어떻게 생성되고 전송되어 서비스되는 지를 보여주는 전체 동작 구조도이다. 여기서 셋톱박스의 보안 마이크로프로세서(Secure Microprocessor)는 EMM과 ECM으로부터 현재 시청되는 방송 서비스의 제어 워드를 추출하고, 수신자격을 스마트 카드에 저장하기 위한 동작을 실행한다. 실제 암호화된 스트림 데이터에 대한 복호화가 이루어지는 곳은 유효데이터 복호화 엔진(Payload Decryption Engine)이다. 이 모델 구조는 표준에 따라 실제 구성 형태가 틀려지지만, 논리적으로는 동일한 동작 모델을 표현하고 있다.

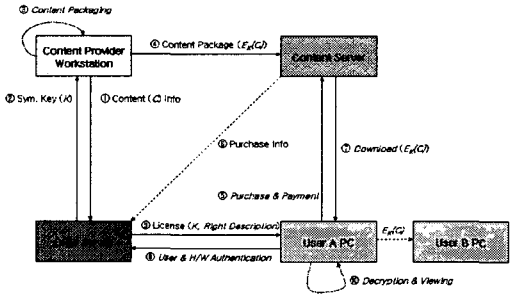


▶▶ 그림 1. CAS의 기본 동작 모델

2. Digital Right Management(DRM)

DRM은 인터넷 환경에서 디지털 콘텐츠에 대한 지적 재산권을 관리하고 제어하기 위해 주로 사용되는 기술이다. 불법 복제를 방지하기 위하여 디지털 콘텐츠의 데이터를 암호화하여 유통하고, 인증된 사용자 및 단말기에 대해서만 라이센스를 발급함으로써 콘텐츠의 이용을 제어한다. 라이센스는 콘텐츠에 대한 사용 권한과 복호화 키를 포함하는데, 사용 권한에 의한 제한 조건이 만족되는 경우에만 복호화를 수행할 수 있도록 강제한다. 이러한 전체 과정을 위조 방지(Tamper-Resistance) 기술에 의해 보호함으로써 해커에 의한 콘텐츠 불법 유출을 차단한다.

다음 그림 2는 일반적인 DRM 시스템의 기본 동작 모델을 보여주는 구조도이다. 번호 순서는 시간적으로 진행되는 절차에 따라 매겨진 것이다. 디지털 콘텐츠에 DRM을 적용하여 서비스하기 위해서는 우선 콘텐츠 제공자 (Content Provider)의 컴퓨터상에서 패키징(Packaging) 과정을 거쳐야 한다. 이 과정을 통해 콘텐츠 정보가 DRM 서버에 등록되고, 콘텐츠 데이터에 대한 암호화가 이루어진다. 이렇게 패키징된 결과물을 콘텐츠 패키지(Content Package)라 부르는데, 이 콘텐츠 패키지는 사용자가 콘텐츠에 접근하기 위해 직접 사용하는 콘텐츠 서버(Content Server)에 게시된다. 사용자가 적합한 결제 과정을 거쳐 콘텐츠를 다운로드 하면, 실제로 전달되는 것은 콘텐츠 패키지 형태의 파일이다. 이 콘텐츠 패키지를 사용자가 이용하기 위해서는 DRM 서버로부터 라이센스를 발급받아야 하는데, DRM 서버는 라이센스 발급 가능 여부를 판단하고 복호화 키 및 사용 권한을 담고 있는 라이센스를 생성해 발급한다. 사용자는 발급받은 라이센스를 이용하여 콘텐츠 패키지를 복호화하여 이용할 수 있게 된다. 보통 이 과정은 DRM 콘트롤러라는 모듈에 의해 강제적으로 제어된다. 사용자가 제 3자에게 콘텐츠 패키지를 복사해 주더라도, 자신이 갖고 있는 라이센스는 제 3자에게는 무용한 것이기 때문에 콘텐츠에 대한 이용을 제어할 수 있다.



▶▶ 그림 2. DRM의 기본 동작 모델

3. 비교 분석

3.1 IPTV와 CAS

CAS는 기존 방송 서비스에서 사용해 왔던 콘텐츠 보안 솔루션이란 측면에서 많은 방송 사업자들에게 신뢰를 얻고 있는 솔루션이지만 IPTV 서비스의 경우에는 상황이 좀 다르다. 처음에 단방향 방송에 적합한 구조를 바탕으로 도입된 CAS의 태생적인 문제 때문이다. CAS는 Request / Response 구조가 아닌 폴링 방식으로, 현재 필요하지도 않은 ECM을 트랜스포트 스트림의 대역폭을 낭비하면서 계속 전송하는 문제를 근본적으로 가지고 있다.

수신자격 정보를 가진 EMM 또한 방송 매체를 통해 전송되는데, 한 매체의 대역폭을 모든 이용자가 공유하는 방송의 특성 상 특정 목적 셋톱박스를 향하는 모든 EMM은 대역폭을 항상 낭비하고 있는 것이다[3].

CAS 표준에서는 스마트 카드 및 POD 모듈 등의 별도 하드웨어 장착을 채택하고 있는데, 이러한 하드웨어의 필요성은 전체 서비스 가격 상승의 주요 요인으로 작용해 결국 가입자에게 부담을 안기는 결과를 초래한다.

CAS의 내재적인 문제점 이외에도 CAS는 콘텐츠의 전송 통로에 대한 접근 제어 솔루션이라는 점에서 IP 네트워크 환경 하의 순수 VOD 나 PVR 등의 기능에 직접적으로 대응하기 어렵다는 문제점을 가지고 있다. 이 문제에 대해서는 POD 모듈 구조에서 콘텐츠 보호 기능을 일부 정의하고 있지만, 결국은 전송 통로 보호에만 치중함으로써 근본적인 문제 해결에는 미치지 못하고 있다.

특히, IPTV의 고급 서비스인 하드 디스크 저장 콘텐츠에 대한 불법 복제 방지 및 사용 권한 제어에 대한 대응이 전혀 이루어지지 않고 있다는 것이 큰 문제이다. 저장된 콘텐츠를 지속적으로 관리할 수 있는 안전한 키 관리와 VOD를 포함한 다양한 서비스에 대한 결제 방식 및 권한 제어 문제가 IPTV 서비스 보안에 있어 CAS가 우선적으로 풀어야 할 숙제인

것이다.

3.2 IPTV와 DRM

DRM은 인터넷 및 PC 기반의 콘텐츠 유통 환경에 적합하게 발전된 기술이므로 기본적으로 IPTV 서비스에 적합한 콘텐츠 보호 기술이다. 원래 인터넷 상에서의 콘텐츠 불법 복제 방지를 기본 목적으로 한 기술이므로 IPTV 서비스에 있어서 DRM 만 가지고도 CAS 기능의 구현이 가능하다. 가입제(Subscription), PPV, VOD, 이용도 측정(Usage Metering), 선지불(Prepay), 후지불(Post Pay) 등 다양한 결제 방식을 가능하게 하는 것도 큰 장점이지만, POD모듈 또는 스마트 카드를 제외시킴으로써 얻는 가격 절감 효과 또한 무시할 수 없는 장점이다. 셋톱박스에 탑재된 보안 관련 모듈의 변경 및 업그레이드가 용이하고, DRM 기본 구조 상, 저장 콘텐츠에 대한 키 및 권한 관리가 매우 용이한 것도 중요한 특징이다.

기존의 방송 체계에선 중간의 유통 채널을 통한 유출이 항상 가능했던 것에 반해 DRM은 콘텐츠 제공자로부터 최종 사용자까지의 종단간 콘텐츠 보호(End-to-End Content Protection)에 대응이 가능하다는 것이 가장 큰 장점이라 할 수 있다.

다만, 라이센스 발급 요청을 하기 위한 회귀 경로(Return Path)가 없는 경우에는 DRM도 CAS와 마찬가지로 ECM / EMM 기능이 반드시 필요하다는 문제점을 갖는다.

IV. 결 론

지금까지 최근에 떠오르는 IPTV 서비스의 특성과 그에 따라 대두된 콘텐츠 보안의 문제점 및 해결 방안에 대해 살펴 보았다. IPTV 서비스에 대한 표준 구조가 없는 상황에서 이에 대한 보안 문제를 접근함에 있어, IPTV의 기본 보안 모델을 제시하였고, 이를 기반으로 기존의 CAS와 DRM 기술을 적용하는데 어떤 한계점들이 있는 지를 분석하였다. 결론적으로 어느 하나의 기존 기술만 가지고는 IPTV의 콘텐츠 보안 문제에 대해 근본적인 대응이 어렵다는 것을 알 수 있었다.

▌참 고 문 헌▐

[1] Margherita Pagani, Multimedia and Interactive Digital TV - Managing the Opportunities Created by Digital Convergence, IRM Press, 2003.

[2] Ahmet M. Eskicioglu, "Protecting Intellectual Property in Digital Multimedia Networks", IEEE Computer, July 2003, pp.39-45.

[3] Herve Benoit, Digital Television-MPEG-1, MPEG-2 and principles of the DVB system, Focal Press, 2002.