IPTV 서비스를 위한 보안 기술

박종열 | 문진영 | 김정태 | 백의현
한국전자통신연구원

요 약

최근 초고속 인터넷의 급속한 발달로 IP 기반의 방송 및 영상의 분배 기능이 빠르게 개발되고 있다. 과거 아날로그 방송에서는 영상을 변조(scramble) 하여 보내고 대응 복조기를 이용하여 정당한 가입자만 시청 할 수 있도록 하는 기술이다. 하지만 최근 IP 기반의 방송 시스템에서는 과거의 변조 (Scramble) 방식이 한계점을 보이고 있다. IPTV는 방송망과 달리 개방형 특징을 가지고 있다. 이는 인터넷 기반의 다양한 공격(man-in-the-middle-attack, TCP-hijacking)이 IPTV에서도 가능하다는 것이다.

본 고에서는 IP 환경에서 제공 가능한 보안 서비스에 대한 기술을 정리한다. 특히 IPTV 서비스를 위한 보안 요구사항, 적용 기술 및 대표적인 연구를 소개한다.

I. 서 론

인터넷 사용자의 급속한 증가는 IT 산업 발전에 큰 견인차 역할을 수행하여 왔다. 그 중에서 인터넷을 이용한 방송 분배 및 VoD(Video on Demand) 서비스는 네트워크 기술의 발달과 더불어 크게 발전하고 있다. 인터넷을 통한 콘텐츠의 유통은 무료라는 고정 관념과 달리 IPTV 서비스는 실시간 방송으로 유료화가 추진되고 있다. 유료 방송 정책은 방송 제공 형태에 따라서 크게 달라지고 서비스를 제공하기 위해 필요한 기술 및 사용하는 자원(Network)에 따라서도 상당히 다르다.

〈표 1〉 방송 특징 비교

분 류	전 송	요 금	특 징	비 고
지상파	무선(공중파)	무료	공익 차원의 방송	무료 제공
케이블	유선(케이블)	유료	저렴한 가격, 안전성	저렴한 서비스
위성	무선(위성)	유료	비싼 가격, 다양한 콘텐츠	고품질 콘텐츠
IPTV	유선(인터넷)	유료	비싼 가격, 다양한 콘텐츠	인터넷 결합 상품

〈표 1〉은 각각의 방송 서비스에 대한 요금 체계 및 특징을 보여주는 표이다. 위의 표에서 보듯이 IPTV 방송이 다른 방송 서비스와 차별화 되는 부분은 크지 않다. 특히 인터넷을 이용하기 때문에 케이블이나 위성과 달리 서비스 품질을 보장하기 힘들다. 이는 인터넷에서는 보장된 자원을 사용하지 않고 다른 사용자와 공유하는 네트워크를 이용하기 때문에 발생하는 문제점이다.

IPTV 서비스를 다른 방송 서비스와 차별화하기 위해서는 인터넷이 가지고 있는 장점을 최대한 부각 시켜야 한다. 가장 쉽게 생각할 수 있는 특징은 양방향 데이터 방송이다. 인터넷의 양방향성을 활용하여 인터넷의 지식검색, 시청중인 프로그램의 제작자 정보, 인기 드라마 순위와 같은 정보를 연동하는 것이 가능하다. 이는 단방향인 기존 방송을 양방향으로 진화하는 것으로 데이터 방송이라는 형태로 개발되

본 연구는 한국정보통신기술협회의 IT 표준화 활동 강화 사업의 일환으로 수행하였음. [2008-P1-08-08K83, IPTV 표준 기술 개발]

고 있다. 기존 방송 시스템에서도 양방향 통신 채널(return channel)을 확보하기 위해 전화선(PSTN), 케이블(DOCSIS), 인터넷 모뎀을 설치하고 있다. 기존의 방송망에서는 양방향 방송을 수신하기 위해서 별도의 통신 채널을 만들어야 하기 때문에 사용자에게 불편함과 추가비용을 발생시킨다.

IPTV의 경우 이와 같은 문제점을 쉽게 해결할 수 있다. 또한 사용자의 성향에 따라 제공하는 맞춤형 방송, 사용자들의 실시간 참여가 가능한 대화형 방송 및 다차원 정보를 제공하는 3D TV와 같은 새로운 방송 환경 적응도 쉬운 특징이 있다. 또한 이러한 방송이 특정 사용자에게 한정되지 않고 IPTV 가입자라면 누구에게나 사용될 수 있는 개방형 서비스의 특징을 가진다.

IPTV 방송은 방송 그 자체 보다는 방송과 연계되는 부가 서비스의 개발이 용이하고 다양한 형태의 시스템 적용이 가능하다는 특징이 다른 방송과 차별화된다. 이와 같이 유연한 서비스를 제공하기 위해서는 기존의 방송 수신 제어 기술도 변화가 필요했다. 그래서 현재 다양한 특징을 가지는 방송 수신 제한 기술(Conditional Access System: 이하 줄여서 CAS)이 개발되고 있다.

IPTV는 기본적으로 IP라는 공개된 망을 통해서 전송되기 때문에 무한대에 가까운 채널 확장이 가능한 반면 개방형 특징으로 인한 불법적인 시청이 용이하다. CAS 기술이 적용되지 않는다면 옆집에서 시청중인 유료 채널의 방송 콘텐츠가 같은 서브 네트워크를 통해 전송되기 때문에 쉽게 도청할 수 있다. 현재 유료 방송의 경우는 암호화 기술을 이용하여 불법적인 접근을 차단하고 있다.

시장에서 방송 수신 제한(CAS) 기술은 방송의 형태 보다는 사업자의 논리에 따라서 상호 배타적인 기술로 개발되고 있다. 실제 지상파 방송을 위한 ACAP[1], 케이블 방송을 위한 OCAP[2], 위성 방송을 위한 MHP[1]가 표준 기술이지만 방송 수신 제한(CAS)는 표준보다는 업체별, 사업자 별 기능을 서로 다르게 하고 기능을 공개하거나 호환성을 위한 노력을 하고 있지 않다.

II. IPTV 보안 요구사항

IP 망을 이용한 방송 전송 기술은 초고속 인터넷 과 BCN(Broadband Convergence Network), CDN(Contents Distribution Network) 기술의 발전으로 IPTV서비스에 접목이 가능하게 되었다. 특히 사용자의 고품질 방송에 대한 욕구로 인해 HD급 영상의 손실 없는 전송 방법으로 IP 망을 선호하게 되었다. 특히 오래된 도시에서는 낡고 오래된 기존 방송 케이블을 새로 설치하기 보다는 빠른 IP 네트워크 망을 설치하는 것이 더욱 효과적이고 경제적이다.

IP 망을 이용하여 고품질의 영상을 전송하는 경우 손실 없는 영상을 전송할 수 있는 장점과 IP 망을 이용한 새로운 서비스의 적용이 쉬운 특징을 가지고 있지만, 공개된 네트워크인 IP를 이용하기 때문에 불법적인 시청 가능성이 높다. 이와 같은 문제점을 정리하면 다음과 같다.

1. 사용자의 불법적인 방송 시청

IPTV에서 방송 데이터는 멀티캐스트 방식을 이용해서 전송한다. 멀티캐스트 방식이란 동일 네트워크에 다른 사용자가 있는 경우 하나의 전송으로 여러 사용자가 받아서 볼 수 있는 특징을 제공한다. 따라서 가입자 정보를 기반으로 채널인증을 하는 경우에는 동일 네트워크의 다른 사용자가 접근 하는 것을 방지 할 수 있다. 또한 사용자의 전송 중간에서 네트워크 가로채기(TCP-hijacking) 기술을 이용해서 연결되어 있는 세션에 대해서 연결을 가로채는 방식의 공격이 가능하다.

기존 시스템에서도 이와 관련하여 많은 연구 개발이 진행되고 있지만 새로운 공격 방법으로 인해 시스템이 피해를 입는 경우 모든 단말기 (STB)의 관련 기능을 갱신해야 하는 문제점이 있다. 때문에 수신 제한 시스템을 개발하는 많은 회사들이 케이블카드(스마트카드의 일종)에 관련 모듈을 탑재하고 해킹 등의 문제점이 발견되면 케이블카드를 교체하는 방식을 취하고 있다.

2. 사업자에 종속적인 접근 제어 기술의 보급

콘텐츠 제공자는 자사의 콘텐츠가 불법으로 유출되는 것을 방지하기 위해서 다각도의 노력을 취하고 있다. 콘텐츠의 불법 유출은 "영화 → 비디오 → 방송" 이어지는 자사의 수익 모델에 큰 영향을 미치기 때문이다. 최근에는 불법적인 유출뿐 아니라 유통에 대해서도 처벌을 하는 등 그 대응이 더욱 적극적이다. 특히 유료 방송의 경우 불법 유출에 대

해서 더욱 적극적이다. 대부분의 영화사들이 자사의 영화를 방송으로 전송하기 위해서는 일정 수준 이상의 수신 제한 기술을 요구하는 경우가 많아 지고 있다.

특히 방송 수신 제어 기술을 가지고 있는 회사와 콘텐츠 제작사들 사이의 공조가 강해지면서 세계적인 기술을 인정받은 몇 개 업체가 전체 시장을 석권하는 문제점이 발생시켰다. 특히 선도 기업들은 그 내부의 메커니즘을 공개하지 않아 신규 사업자들의 시장 진출을 막을 뿐만 아니라 새로운 기술 개발도 더디게 하는 결과를 낳았다. 결과적으로 콘텐츠 제공자의 요구에 맞는 수신 제한 기술 업체의 기술료는 올라가고, 그 회사의 서버 제품, 그 회사의 방송 수신 제어 모듈을 탑재한 단말(STB), 케이블 카드를 일괄 구입해야 한다.

3. 새로운 접근 제어 기술 보급의 어려움

방송 수신 제어 기술은 그 기술의 안정성이 가장 중요한 요소이다. 따라서 새로운 기술을 적용하기 위해서는 그 기술의 안전성 및 장기간의 시험을 거쳐야 한다. 이것은 그런 과정을 거치지 않으면 새로 개발된 방송 수신 제어 기술의 오류가 발생하는 경우 관련 기기의 교체 비용은 상상하기 힘들 정도로 커지기 때문이다. 때문에 많은 사업자들이 새로운 기술 적용을 꺼리게 되는 것이다. 따라서 새로운 방식의 방송 수신 제한 기술을 적용하기 쉽고 해킹이나 오류가 발생하는 경우 이를 쉽게 대치할 수 있는 기술의 개발이 필요하다.

4. 시청자 맞춤형 서비스의 어려움

사용자 맞춤형 시청이란 사용자의 취향 및 과거 시청 내역을 기반으로 사용자의 선호 채널을 선택해서 보여주는 방식이다. TV-Anytime Forum[5]에서는 이와 관련된 방송 메타 정보 처리를 위한 기술 개발이 활발하게 진행되고 있다. 디지털 방송과 더불어 SI(System Information) 정보를 가공한 EPG(전자 프로그램 가이드) 서비스는 사용자에게 방송에 대한 안내를 하는 것으로 방송 메타 정보를 처리한 것이다. 이것을 사용자의 선호에 따라서 가공하는 것이 맞춤형 시청 기능이다.

맞춤형 시청을 하기 위해서는 SI(System Information)정보를 처리하는 기술도 중요하지만 사용자의 요구에 따른 다양한 형태의 유료 방송 서비스가 필요하다. PPV(Pay Per View)의 경우 사용자가 보고 싶은 프로그램의 대금을 지불하고 시청할 수 있다. 위성 방송에서는 이미 상용 서비스가 되고 있는 것으로 사용자는 기본 채널 이외에 상황에 따라 보고 싶은 채널을 시청할 수 있다. PPV 시청의 경우 사용자의 대금 청구나 사용자의 인증을 위해서 별도의 전화망 연결(상담원 연결)이나 전용 단말기를 필요로 하고 있다.

PPV에서 전용 단말기가 필요한 것은 PPV를 제공하기 위해 필요한 인증 및 대금 지불 과정이 추가되기 때문이다. IPTV의 맞춤형 방송이 활성화 된다면 일방적인 방송 가입(기본 채널 가입)보다는 사용자가 선호하는 채널 혹은 프로그램에 대해서만 지불하는 등 다양한 형태의 방송 시청이 가능하다. 특히 VOD 나 PPV와 같은 유료 콘텐츠에 대해서는 해당 서비스를 받는 동안 수행되는 방송 수신 기술의 실행이 필요하다. 특히 콘텐츠 제공 사업자마다 서로 다른 수신 제한 기술을 요구하는 경우에 동적 재구성이 가능한 수신 제한 기술이 필요하다.

5. 방송 단말 사이의 상호 호환성 부재

기존의 방송 수신 단말기는 서비스 사업자가 제공하고 있다. 동일 방식의 방송을 제공하고 있더라도 서비스 사업자마다 서로 다른 수신 제한 기술을 적용하고 있기 때문에 '갑' 에서 제공 받은 단말기는 '을' 에서 사용이 불가능 했다.

케이블 방송의 경우 이와 같은 문제점을 해결하기 위해서 케이블카드 방식으로 수신 제한 기능을 분리(국내에서 분리 의무화, 미국은 2007년 7월로 연기)하고 있지만 실질적으로 케이블카드와 방송 수신 단말이 독립적으로 동작하지 않는 경우가 대부분이다.

방송 채널, 프로그램, 장르, 주인공, 횟수 등 다양한 형태의 수신 제한이 가능하고 콘텐츠 제공자마다 서로 다른 수신 제한 기술이 동작할 수 있도록 하기 위해서는 특정 수신 제한 기술에 종속되지 않고 동적으로 재구성이 가능한 구조가 필요하다. 따라서 본 논문에서는 동적 재구성이 가능하며 다운로드가 가능한 수신 제한 기술을 제안한다.

III. IPTV 보안 기술

위성 혹은 케이블 방송 시스템에서 유료 채널에 대한 사용자의 불법적인 시청 방지 기술은 사업자의 수익성과 직접적인 관계를 가지고 있기 때문에 중요한 기술로 인식되고 있고, 그 기술은 물론이고 사용되는 알고리즘 자체가 외부에 공개되는 것을 꺼릴 정도로 중요시 여겨지고 있다.

이러한 사용자의 불법적인 시청을 방지하기 위해서 사용자를 인증하고 그의 접근을 적절히 제어할 수 있는 기술이 필요하였고 이를 시스템에 적용하는 방식에 따라 CAS (Conditional Access System) 방식과 DRM (Digital Right Management) 방식으로 분류 된다. 또는 이 두 가지 기능이 혼합된 암호 이론 기반의 접근 제어 기술에 대한 연구도 최근 활발히 진행되고 있다.

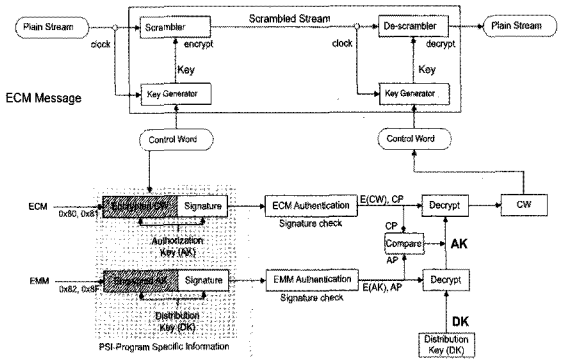
1. CAS 기반의 접근 제어 기술

CAS란 전통적인 의미로 조건에 맞게 사용자의 접근을 제한하는 기술로 과거 아날로그 방송에서 사용되는 스크램블(Scramble) 방식을 주로 의미한다. 방송 채널에 대한 접근을 제어 한다는 광의적인 의미에서는 수신 제한을 위한 모든 기술을 의미하기도 한다. CAS는 방송을 전송하는 측에서 비밀번호(control word)를 생성하고 생성된 비밀번호를 기반으로 스크램블(Scramble) 하여 방송을 전송한다.

수신기는ECM (Entitlement Control Message), EMM (Entitlement Management Message) 정보를 기반으로 스크램블 정보를 복호화 (De-scramble)한다. 복호화 과정에서 사용자의 스마트카드(Smart-card)에서 제공하는 복호화 키(Distribution Key)를 이용해서 ECM, EMM 메시지를 다시 CW로 복호화하는 과정을 거치면 정상적으로 방송을 수신할 수 있다[1].

(그림 1)은 기존 방송의 수신제한 시스템을 보여준다. CW(control word)를 이용하여 실시간 복호화(De-scrambling) 과정을 수행하기 때문에 그 과정이 단순하다. 이로 인해 제공되는 제어 방법은 한정된 수준에 그치고 있는 단점이 있다.

최근 케이블 방송 진영(The National Cable & Telecommunications Association-NCTA)에서는 다음 세대의 방송 기술로 NGNA(Next Generation Network Architecture)를 개발하고 있으며 이는 CAS의 POD(Point of Deploy) 모듈(스마트카드 형태로 제공)을 대치하는 다운로드형태의 보안 솔루션을 개발하는 것이다.



(그림 1) CAS 기반의 접근 제어 기술

2. DRM 기반의 접근 제어 기술

협의적인 의미에서 DRM 기술은 임의의 디지털 정보에 대해서 그 정보의 생성자가 누구이며, 어떤 사람에서 어떤 권리를 부여했는가를 전자적으로 표현하는 기술이다. 멋진 예술 사진이 인터넷에 공개되면 그 그림의 원 저자가 누구이며, 누가 그 정보에 대한 기술적 권리를 가지는가를 가지는 나타내는 기술로 원 저자의 승인 없이 불법적으로 게시 되거나 사용하는 것을 차단하기 위한 기술이다.

광의적인 의미에서 DRM 기술은 불법적인 콘텐츠의 사용과 접근을 방지하기 위한 일련의 기술을 의미한다. DRM 기술은 원 정보에 DRM을 위한 추가적인 정보를 삽입하는 것으로 원 저자 이외에는 그 정보를 식별하거나 확인할 수 없다.

최근 DRM 기술은 저작권 보호 기술은 물론 암호화 알고리즘을 이용한 콘텐츠의 배포 관리, 워터마킹 기술을 이용한 콘텐츠 관리 기술이 개발되고 있다. 방송 수신 제한 기술을 위해서는 방송 스트림의 암호화 키를 표준 DRM의 분배 방식을 따르는 방법이 있다. 암호화 키의 분배가 쉽고 공인 인증서와 연동이 쉬운 장점이 있지만, 다양한 형태의 접근 제어 기술을 수용하기에는 채널 별로 키를 관리해야 하기 때문에 키 분배 및 관리에 많은 비용이 발생하는 문제점을 가지고 있다.

3. 새로운 암호 이론 기반의 접근 제어 기술

IPTV 방송의 접근 제어를 위해서는 사용자 인증, 시스템 인증, 키 분배, 암호화, 복호화라는 일련의 과정을 거친다. CAS 방식 혹은 DRM 방식은 모두 기존의 서버 시스템과 호환성을 가지는 방식인데 반해 암호 이론 기반의 접근 제어 기법은 다양한 형태로 구성이 가능하다. 하지만 방송 시스템이 가지는 특징을 반영하면 CAS 방식에서 스크램블(Scramble) 방식이나 키 분배를 위해 스마트카드(SmartCard) 인터페이스 부분에서 변형되는 방식이 연구되고 있다. 또한 Group Key Management나 TTP(Trusted Third Party)를 활용한 연구도 진행하고 있다.

IV. IPTV 보안 기술 동향

IPTV 서비스를 위한 보안 서비스는 DVB의 CPCP을 중심으로 하는 DRM 기술 연구와 ATIS 나 DVB를 중심으로 하는 CAS(방송 수신 제한 기술)이 주를 이루고 있다.

전통적인 관점에서 IPTV 서비스는 주문형(VoD) 방송과 실시간(Linear) 방송으로 구분되며 주문형 방송은 DRM 기술을 중심으로 발전하여 왔고, 실시간 방송은 CAS 기술을 중심으로 발전하여 왔다. 최근의 연구는 DRM 기반의 실시간 방송 수신 처리 기능이나 반대로 CAS 기반의 DRM 연구도 진행이 되고 있다.

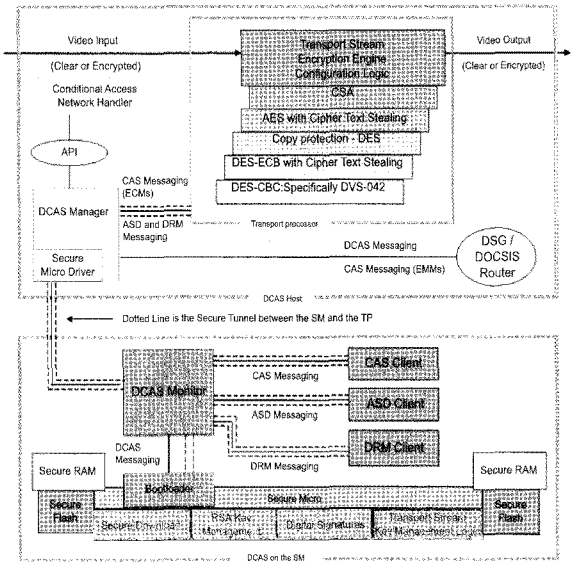
다음은 IPTV 위한 보안 기술의 대표적인 표준화 기술인 OpenCable DCAS, DVB CPCM, ATIS IIF에 대해서 기술하고 각각이 가지고 있는 특징을 정리한다.

1. 다운로드 수신 제한 기술 연구

(그림 2)는 OpenCable 측에서 연구 개발 중에 있는 DCAS 구성도를 보여주고 있다. 먼저 OpenCable 측은 전용 칩을 사용한다. 이 전용 칩은 CAS (Conditional Access System), DRM(Digital Right Management), ASD(Authorized Service Domain) 클라이언트를 다운로드 받을 수 있도록 설계 하였다. 여기서 암호화된 콘텐츠를 복호화하는 기능은 TP(Transport Processor)에서 담당을 하며, CAS Client(다운로드 CAS 코드)에서 전송하는 Control Word를 통해 실시간 복호화하는 과정을 가진다.

2. DVB-CPCM 기술 연구

DVB 측은 방송 수신 제한 기술에서 사업자가 동등한 접근성을 보장하기 위해서 많은 노력을 수행하고 있다. 세부적인 수신 제한 기능보다는 전체적인 시스템에서 사업 간의 동등 접근을 보장하는 것이다. 이를 위해 DVB 측은 MultiCrypt. 와 SimulCrypt 기술을 개발하였다.



(그림 2) OpenCable DCAS 구성도[2]

MultiCrypt는 다수의 방송 수신 제한 프로그램을 동시에 구동되는 특징을 가진다. SimulCrypt는 서로 다른 보안 업체에서 하나의 공통 암호화 알고리즘을 사용하고 업체별로 메시지(EMM, ECM)를 생성하여 전송하는 시스템이다. 이 기술은 하나의 방송 채널에 대해서 다수의 보안 업체가 동시에 서비스를 제공하기 위한 기술을 정의하고 있다.

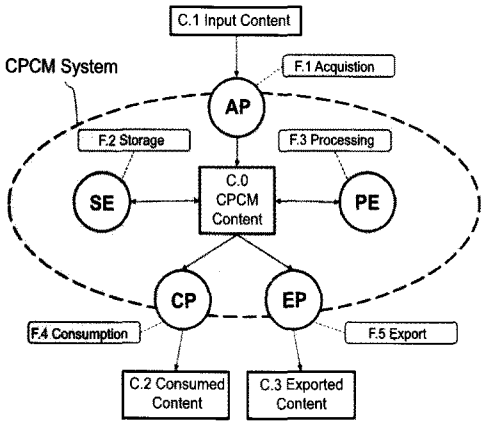
(그림 3)은 DVB의 CPCM 기술을 보여주고 있다. DVB는 댁내로 전달되는 네트워크와 홈 내에서 소비되는 네트워크를 분리하여 정리하고 있다. 그림에서 AP는 실제 방송 스트림을 수신하여 CPCM 콘텐츠로 변환하는 역할을 수행한다. DVB 측에서는 기존의 방송 영역과 별도로 홈 안에서 유통되는 모델을 정의하고 있는 것이다. 즉 홈 내에서는 모든 콘텐츠를 CPCM 콘텐츠로 변환하여 유통하고 외부로 전송하

는 경우에만 다시 변환하는 절차를 거치게 된다.

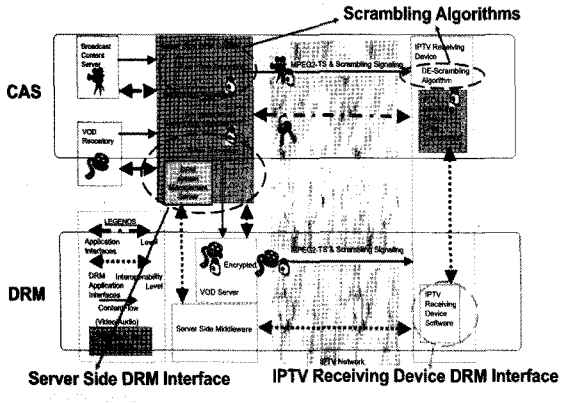
3. ATIS IIF(IPTV Interoperability Forum)

ATIS IIF는 IPTV 서비스의 상호 호환성을 확보하기 위해서 북미 통신 사업자 연합이 설립한 기구이다. 특히 보안 기술의 상호 호환성을 확보하기 위해서 IDSA(IIF Default Scrambling Algorithm)를 제시하고 있다. IDSA는 실시간 방송은 CAS 기술을 이용하고 요구불(On Demand) 방식은 DRM 기술을 이용하는 것이다.

(그림 4)는 ATIS IIF에서 정의하고 있는 구조를 보여준다. 그림에서 상단부는 실시간 방송 서비스에 대한 기술로 Real-Time Encryption이 이루어지고 키 분배 과정을 모두 포함한다.



(그림 3) DVB-CPCM 기술[3]



(그림 4) ATIS IIF의 IPTV 보안 기술[4]

즉 전통적인 CAS 기술을 그대로 수용하고 있다. 반면 하단부는 사용자의 요구에 의해서 제공되는 VoD 서비스 경우로 미리 암호화된 콘텐츠를 이용하여 전송한다.

V. 결 론

IPTV 서비스를 위한 보안 기술은 인터넷이 가지고 있는 양방향성과 방송이 가지고 있는 대중성을 기반으로 하고 있다. 특히 다운로드 가능한 방송 수신 제어 기술은 사용자 혹은 서비스 제공자마다 필요로 하는 수신 제한 기술을 달리 적용할 수 있는 기술로 특정 수신 제한 기술에 종속되지 않는 특징을 가지고 있다.

이들 특징을 반영한 기술이 CAS와 DRM 기술이다. 이들 기술은 상호 배타적이면서 또 보완적인 특징을 가지고 있다. DVB의 경우는 CAS 기술과 DRM 기술의 영역을 구분하여 상호 보완적인 구조를 가지도록 연구가 진행 중에 있다. 북미의 ATSC 경우는 실시간 방송을 위해서는CAS 기술을 적용하고 요구불(On Demand) 서비스에 대해서는 DRM 기술을 적용하고 있다. 이는 CAS와 DRM 기술이 상호 배타적이거나 경쟁적인 기술이 아닌 상호 보완적 기능을 수행하기 때문이다.

따라서 IPTV와 같이 양방향 특징을 가지는 방송 서비스에서는 제공하는 방송의 형태에 따라서 CAS와 DRM 기술이 동시 제공되거나 통합하는 보안 기술이 요구된다.

참 고 문 헌

[1] ATSC Standard, "Conditional Access System for Terrestrial Broadcast Revision A," 2004

[2] Opencable, "DCASTM System Overview Technical Report", OC-TR-DCAS-D01-06-2-6, OpenCable™

[3] DVB, "Support For Use of Scrambling and Conditional Access Within Digital Broadcasting Systems," DVB Document A007, 1997.

[4] ATIS, "IIF Default Scrambling Algorithm(IDSA) IPTV Interoperability Specification," ATIS-0800006, 2007.
[5] CableLabs, "The OpenCable Application Platform", http://www.opencable.com/ocap/
[6] TV-Anytime, "The global TV-Anytime Forum", http://www.tv-anytime.org/
[7] OSGi, "Open Services Gateway Initiative Alliace", http://www.osgi.org/
[8] DVB, "Multimedia Home Platform", http://www.mhp.org/
[9] Cruselles, E., Melus, J.L., Soriano, M., "An overview of security in Eurocrypt conditional access system," Global Telecommunications Conference, 1993, IEEE in Houston. GLOBECOM '93., IEEE Nov. 1993, pp. 188-193
[10] Baofeng Liu; Wenjun Zhang, Tianpu Jiang, "A scalable key distribution scheme for conditional access system in digital pay-TV system," Consumer Electronics, IEEE Transactions on, Vol.50, No.2, May 2004, pp. 632-637
[11] Tianpu Jiang, Shibao Zheng; Baofeng Liu, "Key distribution based on hierarchical access control for conditional access system in DTV broadcast," Consumer Electronics, IEEE Transactions on, Vol.50, No.1, Feb 2004, pp. 225-230
[12] Prasertsatid, N., "Implementation conditional access system for pay TV based on Java card," Computational Electromagnetics and Its Applications, 2004. Proceedings ICCEA 2004. pp.533-536
[13] Angebaud, D., Giachetti, J.L., "Scrambling and controlling access to an all-digital broadcast programme," Broadcasting Convention, 1992. IBC., International, 3-7 Jul 1992, pp.224-228
[14] Kamperman, F., van Rijnsoever, B., "Conditional access system interoperability through software downloading," Consumer Electronics, IEEE Transactions on, Vol.47, No.1, Feb. 2001, pp.47-54
[15] Hongtao Wu, Bocheng Zhu, "Design WDRM in digital TV," Communications and Information Technology, 2005 ISCIT, IEEE International Symposium on, Vol.2, 12-14 Oct. 2005, pp.910-913
[16] Douglas R. Stinson, "Cryptography theory and practice," CRC press, 1995, pp233

약 력

박 종 열

1996년 충남대학교 학사
1999년 광주과학기술원 석사
2004년 광주과학기술원 박사
2001년 ~ 2002년 U. of Utah, 객원연구원
2004년 ~ 현재 ETRI 선임연구원
관심분야 : 방송 수신 제한 시스템, 전자지불, 인증, 분산시스템 등

문 진 영

2000년 경북대학교 학사
2002년 한국과학기술원 석사
2002년 ~ 현재 ETRI 연구원
관심분야 : 방송 수신 제한 시스템, 지바카드, 메타데이타 기술 등

김 정 태

2002년 Charles Sturt U. AUS 학사
2004년 Monash U. AUS 석사
2004년 ~ 현재 ETRI 연구원
관심분야 : 홈네트워크, 유비쿼터스 컴퓨팅, 네트워크 보안, 미들웨어 등

백 의 현

1984년 숭실대학교 학사
1987년 숭실대학교 석사
1997년 숭실대학교 박사
1987년 ~ 현재 ETRI 책임연구원
관심분야 : IPTV, 방송 수신 제한, 개방형 홈네트워크, 상황인지 등