디지털 케이블방송 표준에서 콘텐츠 복제방지 기술

김영화 • TTA 디지털유선방송송수신정합표준전담팀 위원
TTA, IT시험연구소 디지털방송시험센터

1. 복제방지 기술의 필요성

현재 우리나라의 방송환경은 지난 수십년간 지속되어온 아날로그 방송시스템에서 디지털방송 시스템으로 변모해가는 과도기를 맞고 있다. 이미 지난 3월부터 디지털 위성 본방송을 시작하였으며, 지상파에서도 일부 프로그램을 고선명(High Definition) 디지털 프로그램으로 송출하고 있다. 또한 케이블방송 역시 연내 디지털 방송체계로의 전환을 목표로 준비하고 있다.

이러한 방송환경의 변화와 더불어 디지털방송 인프라에 담길 각종 디지털방송 콘텐츠 산업의 중요성이 날로 부각되어 가고 있으며, 또한 이와 더불어 중요시 되고 있는 것이 고부가가치의 디지털방송 콘텐츠에 대한 불법복제 방지기술이다.

디지털방송 환경으로 전환됨에 따라 복제방지에 대한 관심이 민감하게 대두되는 데에는 그만한 이유가 있다. 아날로그 방송환경에서는 전송시의 오류를 완벽하게 수신기에서 제거할 수 없으나, 디지털방송 환경의 경우 오류정정 기능에 의해 원본과 동일한 콘텐츠를 수신기에서 복원할 수 있다는 점이 그 첫 번째 이유이다. 두 번째로는 아날로그의 경우 복제를 반복할수록 복사본의 품질이 원본에 비해 열화되어 가지만, 디지털의 경우 원본과 동일한 품질을 유지하면서 복사의 횟수와 상관없이 무수히 많은 복사가 가능하다는 점이다. 그리고 세 번째 요소로는 아날로그와 달리 디지털 콘텐츠의 경우 인터넷의 발달과 더불어 온라인으로 누구에게나 손쉽게 전달이 가능하다는 점이다.

헐리우드 영화와 같은 고급 방송 콘텐츠를 하나 제작하는 데에는 막대한 자금과 노력이 투자되어야 하는데 이렇게 제작된 고급 콘텐츠가 쉽게 복제되고 유통될 수 있다면 이는 정보화사회 발달에 따른 또 하나의 역기능이라 할 수 있으며, 이를 방지하기 위한 각종 기술에 자연스럽게 관심이 집중되고 있는 것이다.

이러한 배경 하에서, 본 기고에서는 2005년부터 미국 차세대 디지털 케이블방송 표준 규격으로 적용하기로 예정되어 있는 오픈케이블(OpenCable^{TM}) 방식을 중심으로 이에 함축되어 있는 콘텐츠 복제방지 기술(Copy Protection)에 관하여 소개한다. 복제방지를 위해 어떤 정보보호 기술요소들이 구성되어 있으며, 이들이 어떻게 표준에 반영되어 있는지에 대해 중점적으로 살펴보고자 한다.

먼저 2장에서는 복제방지와 관련하여 논란이 되어온 도입배경을 소개하며, 제3장에서는 복제방지 기술에 관한 북미 디지털 케이블방송 규격의 변천과정을 소개한다. 제4장에서는 본 기고에서 논하고자 하는 오픈케이블 규격상에서 복제방지 시스템의 구현개념에 관하여 기술한다. 제5장에서는 시스템 구성을 소개하고, 제6장은 복제방지를 위해 적용된 암호화 기술에 대해 소개하며, 제7장은 암호화 키 공유를 위해 적용된 공개키 방식에 관하여 소개하며, 제8장은 인증 시스템에 관하여 소개한다.

2. 복제방지 기술의 도입배경

복제방지 기술의 도입에 관한 논란과 배경은 최근의 일이 아니다. 이에 대한 간략한 역사적 배경을 소개한다.

■ 1975 : 상용 비디오 복사장치 출시

- 일본의 Sony사에서 최초로 일반 사용자용 비디오 카세트 레코더("Betamax")가 출시되었다. Betamax는 공중파 TV 신호를 수신하여 직접 비디오 테이프에 녹화할 수 있도록 되어 있는 현재 비디오 레코더의 초기 상용 모델이다.

■ 1976 : Disney & Universal Studio가 Sony사에 대해서 저작권 침해소송 제기

- 미국 영화 제작사들은 Sony사에서 제작 판매하는 이 비디오 레코더가 자신들이 만든 영화에 대한 저작권을 침해할 수 있는 도구로 사용될 소지가 있다며 소송을 제기하여 법정논쟁의 시작이 되었다.

■ 1979-1981 : 법정 공방

- 1979년 미연방 법원(District Court)은 영화 제작사의 소송제기에 대해 Sony사에 유리하게 전개되어 갔으나, 재심과정에서 결국 1981년 연방법원의 최종 결정이 Sony사에 불리한 쪽으로 결말이 났다. 이에 굴복하지 않고 Sony사는 미 최고 법원(Supreme Court)에 이를 항소하였다.

■ 1984 : 미 최고법원 평결로 Sony사 최종 승리

- 최고 법원은 최종 판결을 통해, 집에서 테이프에 녹화하는 것은 저작권 침해라고 볼 수 없다("private home taping does not constitute a copyright violation")는 평을 내림으로써 오랜 법정 공방은 Sony사의 승리로 결말이 났고 현재까지도 비디오 레코더에 녹화기능의 사용이 허용되고 있다 .

■ 1990 : DAT(Digital Audio Tape) 판매에 관한 논란

- Sony사에서 개발 판매된 DAT recorders와 blank DAT tapes에 대하여 비디오 레코더와 같이 저작권 침해의 소지가 있음을 지적하면서 미국내에서 이들 물품에 대한 판매를 하지 못하도록 해야 한다는 주장이 제기되었다.

■ 1998 : DMCA(Digital Millennium Copyright Act) 법령 통과

- 미국 의회에서는 디지털 콘텐츠에 대한 저작권 보호와 관련하여 포괄적인 법안인 DMCA를 통과시켰다.
- 이 법안은 미국에서는 디지털방송 환경에 대비하여 불법복제에 관한 보다 적극적인 관심과 구체적인 기술개발의 계기가 되었다.
- DMCA의 내용을 요약하면 다음과 같다.
  – 복제방지 기술을 무효화시키는 것을 불법으

로 간주함
- 복제방지 기술을 무용화시키는 장치를 제작, 수입 및 유통을 금지함
- 복제방지를 위한 제어 및 구현에 대한 임의 조작을 금지함
- Macrovision 기술을 아날로그 복제방지 기술로 승인함 등

■ **1999 : EIA-697/NRSS (National Renewable Security Standard) 표준 채택**

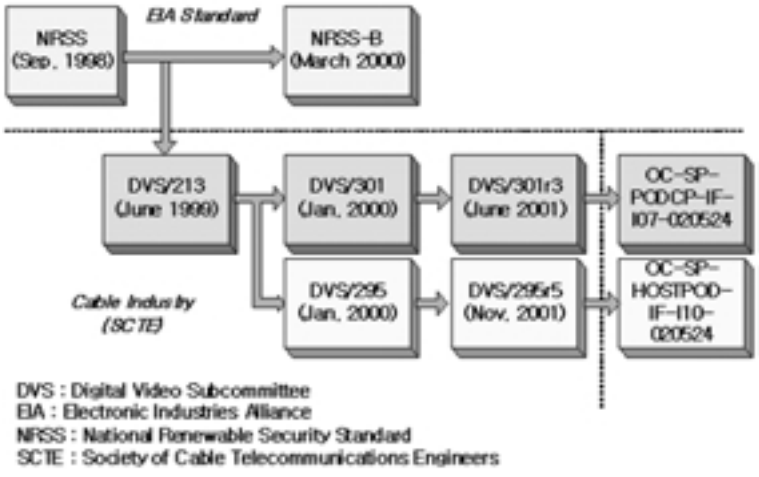
• 미국 의회의 적극적인 복제방지 정책현안을 기술적으로 뒷받침하려는 활동의 결과중 하나로서 미국전자 산업계 기술표준으로 NRSS (National Renewable Security Standard)를 EIA-679 표준으로 공식 채택하게 되었다.

• NRSS 표준 규격에서 담고 있는 기술적 내용은 다음과 같다.
- 장치간 물리적 정합 요구조건 : PCMCIA card interface
- 복제방지 장치와 수신장치의 결합요건 : Host /POD binding
- 복제방지를 위한 암호화 기술과 요건 : DES-ECB
- 복제방지를 위한 자원관리 및 프로토콜과 이에 적용되는 메시지 정의 등

3. 콘텐츠 복제방지 기술규격의 변화

1998년도 9월에 제정된 NRSS 표준규격을 기준으로 하여 이후 디지털 케이블방송 시스템에서의 복제방지 표준 규격들이 새롭게 마련되어 왔고 여러 차례 개정을 통해 현재까지 진행되어 오고 있는데, 이와 같은 복제방지에 관한 표준 규격의 변천과정을 그림으로 나타내면 다음 (그림 1)과 같다.

1998년 9월 초기 NRSS의 제정시에는 PCMCIA 카드를 이용한 복제방지 장치의 물리적 크기와 모양 그리고 연결 커넥터에 대한 정의 등에 중점을 두고 있었으며, 영화 산업계에서 복제방지를 위한 구체적인 요구사항들이 적극 반영된 상태로 진행되지는 않았었다. 이후, 2000년 3월에 개정된 EIA-679-B(NRSS-B) 표준안에서는 복제방지 장치에서 사용할 프로토콜과 기술들에 관하여 구체적으로 언급되었다. 1999년 6월(최초 버전은 2월에 발표)에 미



(그림 1) 복제방지 관련 기술규격의 변천과정

국 케이블방송 산업계에서는 NRSS 표준 규격을 기준으로 하여 디지털 방송분야에 적용할 복제방지 기술 표준 규격으로 SCTE(Society of Cable Telecommunications Engineers) DVS/213(Copy Protection for POD Module Interface)을 미국 표준으로 제정하여 채택하였다. 이 규격이 몇 번의 확장과 개정을 거치면서, 2001년 6월 현재의 미국 디지털 케이블방송에서의 복제방지 규격인 ANSI SCTE 41 2001 Formerly DVS301(POD Copy Protection System) 이 제정되어 현재 미국 표준 규격으로 사용하고 있다.

한편, 현재 미국에서 2005년부터 적용을 목표로 차세대 디지털 케이블방송 규격을 미국 CableLabs™사에서 OpenCable™ 프로젝트를 운용하고 있으며, 상기 SCTE 41 DVS301 표준 규격을 기반으로 하여, 2002년 5월에 제정 공포한 표준 규격 중, 복제방지 기술에 관한 표준 규격이 OC-SP-PODCP-IF-I07-020524(OpenCable™ POD Copy Protection System)이다. 본 기고에서 소개하고자 하는 복제방지 장치기술은 이 기술규격을 근간으로 소개하고자 한다.

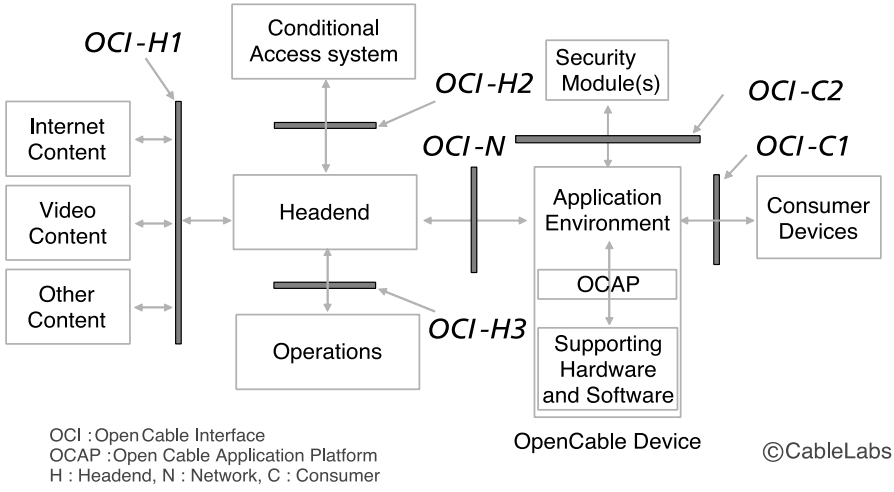
한편, 복제방지 장치에 관한 물리적 정합을 포함하여 각종 레어상의 정합표준을 정의한 것으로서는 2000년 1월에 제정된 SCTE DVS/295 표준 규격이 있으며, 이에 대한 개정을 다섯 차례에 걸쳐 2001년 11월 버전 5(SCTE DVS/295r5)를 기반으로 ANSI SCTE 28 2001 Formerly DVS 295(Host-POD Interface Standard)를 채택하였으며, 이를 기반으로 하여 미국 OpenCable 프로젝트에서는 OC-SP-HOSTPOD-IF-I10-0524 (OpenCable™ HOST-POD Interface Specification) 를 발표하였다.

현재 우리나라에서도 이들 표준 규격을 포함하여 OpenCable™ 방식을 국내 디지털 유선방송 송수신 정합 표준규격으로 채택하여 제정 공포하였다.

4. 수신제한 시스템(CAS)과 복제방지 시스템(CPS)

디지털 케이블방송을 위해 필요한 각 구성요소간의 정합에 관한 오픈케이블 표준의 기본구성을 그림으로 나타내면 다음 (그림 2)와 같다.

이 그림에서 보는 바와 같이 모두 6가지의 정합규



(그림 2) 오픈케이블 표준 정합규격

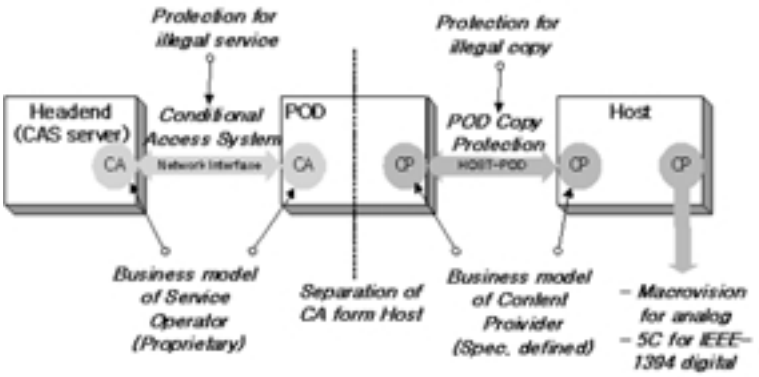
격이 있으며, 여기에 Host(또는 셋탑)가 갖추어야 할 기본 핵심기능을 정의한 HCR(Host Core Functional) 규격과 DOCSIS(Data Over Cable Service Interface Specifications) 케이블모뎀을 적용하기 위해 필요한 DSG(DOCSIS Settop Gateway) 규격이 추가되어 있다. 이들 모든 규격에 관한 각 세부 사항의 소개는 추후에 기회가 있을 경우에 소개하기로 하고, 이 중에서 본 기고에서 관심을 갖고 있는 콘텐츠 복제방지 기술인 OCI-C2 부분에 해당하는 복제방지 시스템에 한정하여 소개한다.

오픈케이블 규격상에서 복제방지 부분만 나타내면 (그림 3)과 같이 표현할 수 있다. (그림 3)에서 보면 두 가지의 복제방지 시스템이 구현되어 있음을 알 수 있다. 하나는 디지털 케이블방송 송출시스템을 중심으로 한 수신제한 시스템(CAS : Conditional Access System)과 다른 하나는 호스트로부터 분리된 POD(Point Of Deployment, 수신제한 장치)와 호스트 사이의 복제방지 시스템(CPS : Copy Protection System)으로 구분되어 있다. 일반적으로 복제방지 시스템은 후자인 CPS를 의미하며 따라서 POD 복제방지 시스템이라고도 불리운다. 이와 같이 CAS와 CPS는 각각 의미하는 바가 다르다.

여기서 POD라는 장치에 관하여 간략히 언급하면, 기존의 디지털방송 수신장치 시스템에서는 송출시스템으로부터 암호화된 콘텐츠를 수신하여 다시 일반영상으로 선택적으로 복원하는 기능이 수신장치 내부에 내장(Imbedded CA System)되어 있었다. 이와 같은 수신제한 장치를 수신장치로부터 분리한 별도의 Security Module을 POD라 한다. 즉, 방송사업자의 비즈니스 모델에 관련한 기능적 요소들을 수신장치에서 분리함으로써 수신장치 역시 하나의 가전제품과 같이 소매시장에서 유통시킬 수 있게 하고자 함이 POD 도입목적 중의 하나이다. 즉, CAS는 방송사업자가 정식으로 방송서비스 가입을 통한 적법한 수신자에게만 디지털방송 서비스를 제공하고자 하는 것이며, CPS는 적법한 사용자인지 아닌지를 떠나서 수신장치에서 복원된 고급 콘텐츠를 임의대로 복제하지 못하도록 방지하는 콘텐츠 복제방지 시스템을 의미한다.

이를 비즈니스 모델의 관점에서 보면 CAS는 방송사업자의 수익모델을 보장하기 위한 기술로서 의미가 있으며, CPS는 이들 방송사업자에게 제공하는 콘텐츠 공급자의 수익모델을 보장하고 콘텐츠의 저작권을 보호하기 위한 기술규격으로 볼 수 있다.

기술규격상에서 CAS에 관한 부분은 방송사업자와 일반 CAS 기술 보유업체에게 많은 부분을 유예하였으나, CPS 부분은 기술규격상에서 엄격하게 정의하고 언급되어 있음을 보면 콘텐츠에 대한 저작권 보호가 그동안 얼마나 첨예한 논란이 되어 왔으며,



(그림 3) 수신제한시스템(CAS)과 복제방지기술(CPS)의 적용개념

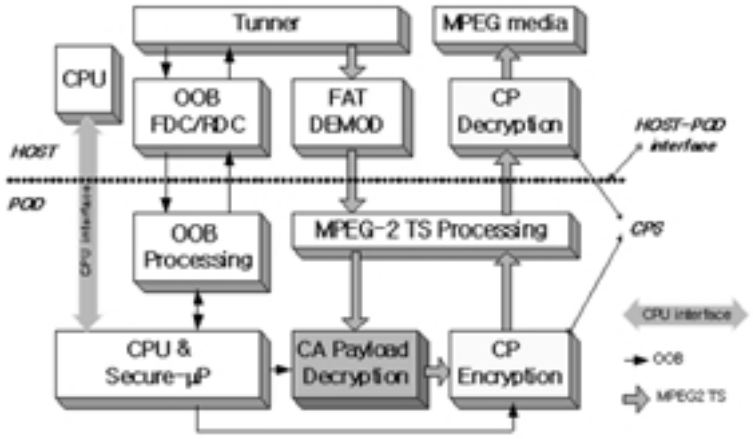
향후의 논란의 소지에 미리 대비하여 전반적인 디지털 방송산업의 발전과 더불어 고급 콘텐츠산업의 발전을 보호하고 이에 대한 논란의 소지를 기술적으로 철저히 대비하고 있는지 볼 수 있다.

5. 제어시스템 구성과 제어정보

복제방지 시스템인 CPS의 기능 블록도를 나타내보면 (그림 4)와 같다. 이 그림에서 보면 먼저 송출 시스템에서 암호화된 디지털 콘텐츠는 가입자 수신제한 장치인 POD에서 복호화(CA Payload Decryption)되어 일단 평문상태의 디지털 콘텐츠로 변경되고, 이 콘텐츠는 다시 복제방지 시스템에 관한 표준 규격에서 요구하는 방식에 의해 암호화(CP Encryption)된 후에 호스트로 전송하도록 되어 있다. 이러한 암호화를 통해 고급 디지털 콘텐츠가 평문상태로 POD에서 호스트로 전송되는 것을 금지하도록 규정하고 있다.

이와같은 CPS는 모든 콘텐츠에 적용되나 모든 콘텐츠가 반드시 암호화해서 전달되는 것을 의미하지는 않는다. 즉, 수신제한 시스템이 관여하지 않는 콘텐츠 예를 들면, 공중파를 통해 수신되는 무료채널 또는 긴급 재해방송 채널 등에 대해서는 암호화하지 않고 전달할 수 있어야 한다고 표준에서 규정하고 있다. 최대한 고급 디지털 콘텐츠에 대해서만 복제로부터 보호하고 나머지 공공의 성격을 띠고 있는 채널에 대해서는 어느 누구도 수신이 가능하도록 하고 있다.

복제방지를 위한 암호화의 적용여부 등을 정하는 데에 있어서 결정적인 기준은 해당 콘텐츠를 제작한 콘텐츠 제작업체에 우선권을 부여하고 있다. 복제방지 시스템의 복제 허용여부를 결정하는 정보를 CCI (Copy Control Information)이라 하여 이를 각 전송되는 디지털 콘텐츠에 대응하여 수신자의 POD에 내려주게 되어 있다. 송출 시스템에서는 CAS 서버 시스템에서 이러한 정보를 포함하여 각 가입자별 또는 장치별로 고급 디지털 콘텐츠에 접근 허용여부를 제어하는 메시지를 MPEG2 TS(Transport Stream)내에 Private Section 형태로 내려주게 되는데 이를 ECM(Entilement Control Massage)이라 한다. ECM에 실려 내려오는 CCI 정보는 POD에 의해 판독되고 이들 정보는 인증된 채널 즉, 전달되는 정보의 무결성을 증명할 수 있는 암호화 프로토콜로 정의된 채널을 이용하여 호스트에 전달되도록 되어 있다.



(그림 4) 복제방지 시스템 기능 블록도

호스트는 이렇게 전달된 CCI에 준해서 해당 콘텐츠에 대한 출력을 제어하도록 규격에서 정의하고 있다. 표준에서 정의하고 있는 CCI는 8bits, 1byte로 구성되어 있으며 그 포맷은 <표 1 >과 같다. CCI에 표현된 각 비트 정보들에 대한 아날로그 콘텐츠에 대한 의미해석과 디지털에 대한 의미해석은 <표 2 >와 같다.

APS bits로 제어되는 아날로그 콘텐츠의 경우, 복제방지를 위해 사용승인된 기술(Macrovison 등)을 적용할 수 있는 포맷(예, NTSC, S-VHS)에 대해서만 그 출력을 허용하고 있으며, 콤포넌트(RGB, YPbPr 등) 출력에 대해서는 이들 출력 포맷에 대해 복제방지 기술적용이 가능할 경우에만 허용하도록 하고 있다. 한편 이들 기술을 적용하지 못할 경우, 출력화면의 분해능을 520,000pixel 이하로 제한된 것만 출력가능하도록 하는 방안을 고려 중이다. 한편, EMI bits로 제어되는 디지털 콘텐츠의 경우, IEEE-1394 및 DVI(Digital Video Interface) 출력에 대해서는 DTLA(Digital Transmission License Agreement)와 HDCP(High-bandwidth Digital Content Protection)를 따르도록 권고하고 있다.

6. MPEG2 전송 스트림 콘텐츠 암호화

POD와 호스트 사이의 MPEG2 전송계층 암호화에 사용될 암호화 알고리즘으로서는 표준 블록암호화 알고리즘인 DES(Data Encryption Standard)를 사용하도록 권고하고 있다. 이 암호 알고리즘에 관한 자세한 소개는 생략하기로 하며, 그 특징에 관해서만 간략하게 소개한다. DES 알고리즘은 1972년 미국 상무성 주도로 개발되어 1977년 미국 표준으로 채택된 이후 매우 광범위하게 적용되어온 블록암호 알고리즘의 표준으로서, UNIX 시스템의 crypt() 명령어에서도 이 방식을 채택하는 등 널리 사용되고 있다. 이 암호 알고리즘은 평문으로 64 bits를 입력받아서 56bits의 암호화 키에 의해 이에 대응되는 64bits의 암호문을 발생하도록 되어 있다. 해킹 기술의 발전과 더불어 이에 대한 암호학적 안전성의 논란에 따라 현재는 Triple-DES, 또는 라운드 수의 변형 등을 통해 여러가지로 변형한 블록암호화 알고리즘을 사용하고 있지만 그 근간은 DES에서 크게 벗어나지 않고 있으며, 최근에는 이보다 더욱 안전한 알고리즘을 대체하여 표준으로 사용하는 추세이다.

이 블록암호 알고리즘을 적용함에 있어서는 몇 가

〈표 1〉 CCI 정보의 구성

CCI Bits #	7	6	5	4	3	2	1	0
POD set to	0	0	0	0	APS1	APS0	EMI1	EMI0
Host interprets as	rsvd	rsvd	rsvd	rsvd	APS1	APS0	EMI1	EMI0

〈표 2〉 CCI 정보에 대한 복제방지 제어의미

Bit values	EMI for Digital content		APS for Analog content
	Copy permission	Value	
00	Copying is permitted	Not high	Copy protection encoding Off
01	No furture copying is permitted	High	AGC process ON, Split burst Off
10	One generation copy is permitted	High	AGC process ON, 2 Line Split burst ON
11	Copying is prohibited	High	AGC process ON, 4 Line Split burst ON

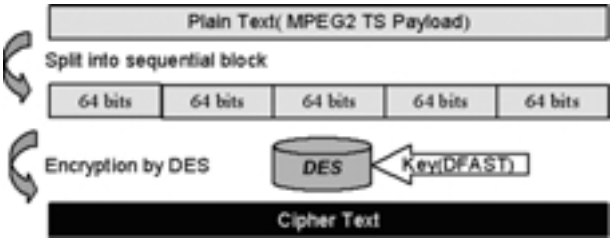
지의 운용모드(Operation Mode)로 구분할 수 있는데, 그 중 복제방지 시스템에서 채택한 운용모드는 (그림 5)와 같이 기본적인 형태인 ECB(Electronic Code Book) 모드로 운영하도록 권고되어 있다.

이 암호화 알고리즘에 암호화와 복호화에 있어 핵심이 되는 암호화 키의 생성을 위해서는 미국 GI (General Instrument)사에서 특허권을 가지고 있는 DFAST(Dynamic Feedback Arrangement Scrambling Technique, US patent 5054067/Oct. 1, 1991 and US patent 4860353/Aug. 22, 1989) 알고리즘을 사용하도록 되어 있다. 현재는 GI사가 모토롤라로 합병되어 DFAST 특허권을 모토롤라가 가지고 있으며, 이에 대한 특허 허여권을 미국 CableLabs사에 실사함으로써, 이 기술을 오픈케이블 규격상에서 사용할 경우, CableLabs사로부터 PHILA(POD-HOST Interface License Agreement)라는 특허 사용계약을 체결하도록 되어 있다.

DFAST 알고리즘은 두 개의 시프트 레지스터로 구성되어 있는데, 그 중에서 하나는 출력 비트 스트림을 예비 키출력 스트림(Pre-key stream)과 논리연산에 의해 나온 결과를 다시 궤환(Feedback)시켜서 키 수열을 동적(Dynamic)으로 발생하도록 구성되어 있으며, 입력으로 128bits를 키 발생 입력정보로 받아들여서 56bits의 출력을 생성하며, 이 출력이 다시 DES 암호화 알고리즘의 POD와 호스트 사이의 전송계층의 암호화 및 복호화 알고리즘에 대한 키로 사용되도록 되어 있다.

MPEG2 TS의 암호화는 188byte의 TS 중에서 Payload 부분에만 적용되며 헤더정보, 적응필드(AF : Adaption Field) 및 Tail block(암호화 블록 단위인 64bits를 기준으로 payload 부분을 분할하다가 보면 64bits가 채 안되는 맨 마지막에 남는 블록)에는 적용하지 않도록 되어 있다. 따라서 AF가 0 byte인 경우, 188 byte MPEG2 TS 중에서 헤더 부분인 4byte를 제외하면 MPEG2 TS의 payload에는 23개의 블록이 DES로 암호화되어 전송하도록 구성되어 있다.

이와 같은 암호화는 앞에서 언급한 바와 같이 모든 콘텐츠에 적용하는 것이 아니라, CCI의 내용과 CAS 시스템에서 암호화된 콘텐츠에 대해서 CPS에서의 암호화 적용을 원칙으로 하며, POD와 호스트



(그림 5) ECB 운영 모드

〈표 3〉 암호키 적용 모드에 따른 암호화 적용제어(CP__Trnasport__scrambling__control__field)

EMI Bit values	For Single CP-Key Mode	For Optional Dual CP-Key mode
00	No scrambling	No scrambling
01	Reserved	Reserved
10	Reserved	TS packet scrambled using EVEN key
11	TS packet scrambled	TS packet scrambled using ODD key

사이에 암호화 및 키 적용에 관한 규약을 표로 정리하면 다음 <표 3>과 같다. 여기서 기본은 단일 키 모드이며, 옵션으로 짝수 번째와 홀수 번째로 두 개의 키를 적용하는 듀얼 키 운용 모드도 가능하다.

7. POD와 Host의 키 공유

DES와 같은 고전적 암호화 방식(또는 대칭키 암호화 방식, Classic or Symetric Cryptographic Algorithm)에서는 암호화에 사용되는 키와 복호화에 사용되는 키가 반드시 일치하여야 한다. 즉, 송신측인 POD에서 사용하는 암호화 키와 수신측인 호스트에서 이들 암호화된 데이터를 다시 원래대로 복원하기 위해서 사용하는 복호화 키는 반드시 정확하게 일치하여야만 한다.

그러면, 여기서 어떻게 안전하지 못하다고 가정된 POD-Host 통신채널을 통해 서로 일치하는 암호화 키를 공유할 수 있을 것인지에 대한 문제를 해결하여야 한다.

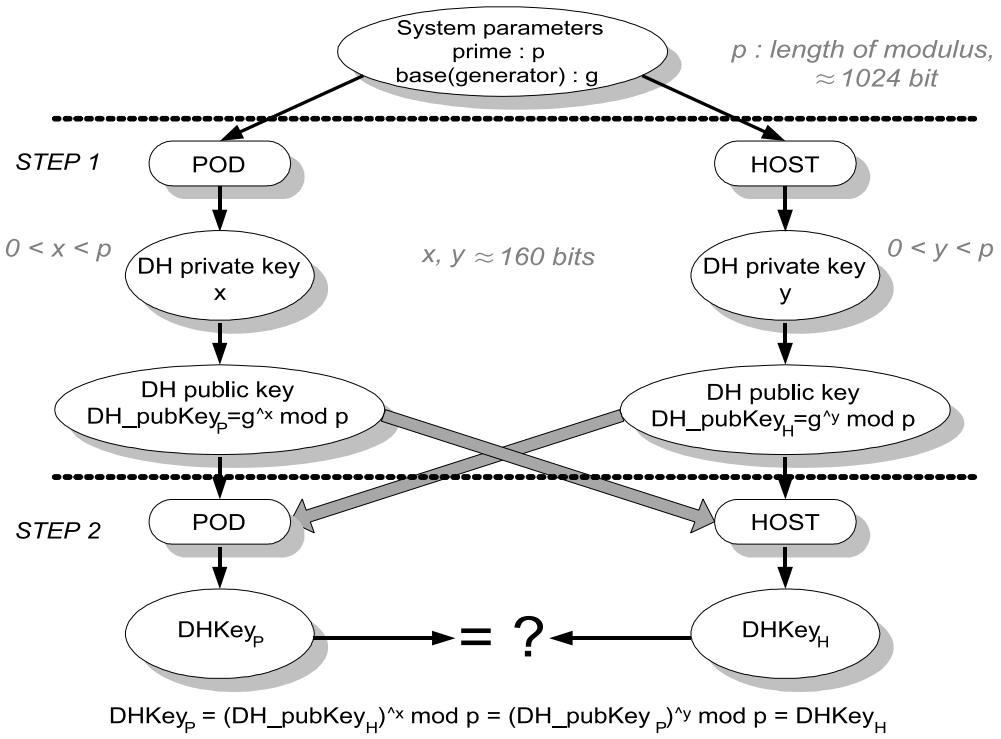
가장 간단하게 생각해볼 수 있는 것은 하나의 객체가 임의로 키를 만들어 다른 하나에게 전달해주면 간단히 해결될 것같이 생각할 수 있지만 실제로 전달하는 채널 자체가 안전하지 못한 채널이라고 가정하기 때문에 가장 안전하게 지켜주어야 할 핵심 데이터인 암호화 키를 이와 같이 전달할 수는 없는 것이다. 즉, 안전하지 못해서 암호화를 적용하여 통신하는데, 그 암호화를 적용하기 위해서는 이 안전하지 못한 채널을 통해서 키를 공유해야 한다는 딜레마에 접하게 되는 것이다.

이와 같은 딜레마를 해결하기에 매우 적절한 기술이 공개키 시스템을 응용한 암호화 프로토콜이다. 복제방지 표준 규격에서도 이와 같은 키 공유문제와 인증에 관한 문제에 대해서 공개키 시스템을 도입하고 있다. 즉, 공개키 시스템 기술의 하나인 Dieffie-Hellman(DH) 키 공유 프로토콜(Key Sharing Secure Protocol)을 채택하고 있다. 이는 두 개의 객채가 서로 안전하지 못한 통신채널을 사이에 두고 있을 경우, Challenge-response 방식과 공개키 방식을 응용하여 둘 만이 가질 수 있는 비밀정보를 공유할 수 있도록 고안된 암호화 프로토콜이다. 이의 안전성은 이산대수(Discrete logarithm)에 있어서 소인수 분해가 수학적으로 매우 어렵다는 특성에 기인하며, 이런 특성을 암호화 프로토콜에서 요구하는 일방향 함수(One way function)의 특성으로 간주하는 데에 있다. 보다 상세한 내용은 생략하기로 하며 복제방지 기술에 적용된 이 암호화 프로토콜을 그림으로 나타내면 다음 (그림 6)과 같이 나타낼 수 있다.

이 알고리즘의 기본 처리과정은 그림에서 보는 바와 같다. 먼저 제1단계로 POD와 호스트는 제작 당시 주어진 시스템 파라미터(Prime number and Base)에 의해 각자 공개키(Public key)와 개인키(Private key)의 키 쌍(Key pair)을 생성한다. 이후 2단계로 이들 중 공개키를 각각 상대방 측에 전송한다. 이 경우 전송되는 채널 상에는 이들 객체들의 공개키만 공개되지만 공캐키 시스템의 안전성에 기인하여 이들 공개키로부터 각자가 가지고 있는 비밀키 정보를 유도하는 것은 실제적으로 불가능하다고 보기 때문에 각자의 비밀정보는 노출되지 않는 것으로 볼 수 있다. 마지막으로 3단계로서 POD와 호스트는 서로 교차하여 주고받은 공개키를 Base로 하여 각자가 가지고 있던 비밀키로 승산한 후, 모듈러 연산을 취하면 그 결과값으로 양측이 동일한 값(DHKey)을 얻게 된다.

DH 공개키 공유 프로토콜 방식에서 POD 측의 공유키 정보의 유도과정은 다음과 같다.

$$DHKey_P = (DH\_pubKey_H)^{\wedge x} \bmod p = (g^{\wedge y} \bmod p)^{\wedge x} \bmod p = g^{\wedge y \wedge x} \bmod p$$



(그림 6) 키 교환 프로토콜

한편, 호스트측에서는 다음과 같다.

$DHKey_H = (DH\_pubKey_p)^{y} \bmod p = (g^{x} \bmod p)^{y} \bmod p = g^{x^{y}} \bmod p$

상기의 두 식의 결과값에서 알 수 있듯이 상기 두 식의 결과값은 동일하게 된다.

이와 같이 계산된 키 값이 POD와 호스트 간에는 둘 만이 공통으로 간직할 수 있는 비밀정보가 되는 것이다. 이 비밀정보는 이후에 유도되는 장비간의 결합(POD/Host binding)의 완성유무를 인증(Auth-key)하고 판단하는 기준이 되며, 또한 MPEG2 TS를 암호화 하는데 적용하는 비밀키(CP-key) 정보를 유도하는데 핵심 기반정보가 된다.

이와 같이 공유된 비밀정보로부터 장비간의 결합을 검증하는 판단기준인 장비인증 키의 생성은 다음과 같이 계산하여 얻는다.

POD 측의 경우 : $AuthKey_P$ = SHA-1[DH_key_P/Host_ID|POD_ID]

호스트 측의 경우 : $AuthKey_H$ = SHA-1[DH_key_H/Host_ID|POD_ID]

여기서 SHA-1[.] 함수는 해쉬함수(Hash function)의 일종으로 512bits 입력을 받아 160bits로 압축된 정보를 생성하는 미국 표준 디지털 서명 알고리즘(DSA : Digital Signature Algorithm)에 사용되는 해쉬 알고리즘이다.

또한 이 키를 근간으로 하여 암호화에 적용할 키(CP-key)는 세션(Session) 개념을 도입하여 임의 난수를 상호교환한 후, 이를 상기에서 유도한 Auth-key 정보와 함께 이용하여 다시 해쉬함수에 의해 얻게 된다. 이들 유도과정에 대한 상세한 내용은 표준 규격을 참조하는 것으로 하고 여기서는 생

략하기로 한다. 표준 규격상에서 사용하는 시스템 파라미터를 표로 정리하면 다음과 같다.

〈표 4〉 키 발생 및 교환을 위한 시스템 파라미터

Keys	Size	용도
Diffie-Hellman keys(DH_pubKeyH, DH_pubKeyP)	1024 bits	인증키 및 공유키 생성
Authentication keys(AuthKeyH, AuthKeyP)	160 bits	복제방지 키 생성
Host_ID(호스트 장치 고유할당 번호)	40 bits	장치 인증
POD_ID(POD 장치 고유할당 번호)	64 bits	장치 인증
Diffie-Hellman prime(DH_p)	1024 bit	공개키 생성
Diffie-Hellman base(DH_g)	1024 bit	공개키 생성
RSA public signing key exponent	40 bits	서명 생성 및 검증

8. 인증 시스템(Authentication System)

상기에서 언급한 공개키 시스템 기반의 DH 알고리즘은 기존 대칭키 시스템에서 안전하지 못한 채널을 통해서 키를 안전하게 전달하는 수단으로서 매우 적합한 공개키 솔루션을 제공하고 있다. 그러나 이러한 공개키 시스템도 모든 종류의 해킹 공격에 항상 안전하다고는 볼 수는 없다. 이 공개키 알고리즘의 가장 취약한 약점 중 하나는 제3자 개입 공격법(Man in a Middle Attack)이다. 즉, 제3자가 두 객체 사이에 위치하여 상호 간의 호스트에 대해서는 자기가 POD인 것처럼 위장하고 POD에 대해서는 자신이 호스트인 것처럼 위장하면서 정보를 중간에서 가로채는 공격법이다. 따라서 이와 같은 공격에 대처하기 위해서는 전달되는 공개키가 정말 해당하는 POD와 호스트의 것인지를 상호 간에 증명할 수 있어야 한다. 이를 위해 일반적으로 사용되는 정보보호 시스템에서는 데이터의 무결성(Integraty) 보장 및 객체 인증(Object authentication)이라는 기술을 사용하며, 이와 같은 요구조건을 만족하도록 시스템을 설계한다. 본 기고에서 관심을 두고 있는 복제방지 기술규격 상에서는 이를 위해 ITU-T X.509 버전 3의 인증서(Certificate) 표준을 도입 적용하여 이러한 안전성을 보장하도록 되어 있다. 이는 CableLabs를 최상위 Root CA(certificate Authority)로 하여 각 장비 제조업체를 이의 하위 CA로 두며, 이들 업체에서 생산하는 장비들에 대하여 각각 장비인증서(Device certificate)를 발급하도록 되어 있어 3단계의 인증 체인(Certificate chain)을 구성하도록 되어 있다. 당연히 Root CA 는 RSA(Ron Rivest, Adi Shamir, Leonardo Adleman) 방식에 의한 자필 디지털 서명(Digital signature)된 인증서와 함께 제조업체에 대한 공개키 인증서에 서명하여 제조업체의 공개키에 대한 무결성과 인증을 보장하며, 이를 근거로 각 장비들은 키 교환시 제조업체에 의해 디지털 서명된 장치 인증서와 제조업체 인증서를 서로 교환함으로써 그들이 교환한 공개키의 무결성과 소유객체의 인증을 X.509 인증 체인을 통해 검증하도록 되어 있다. 또한 이들 장비의 인증유효성 검증과 사후 인증취소 여부를 제어하기 위해서 CRL(Certification revocation List)를 적용하도록 되어 있다. 이러한 장치인증의 의미는 결국 고급 디지털 콘텐츠를 실질적으로 다루는 것은 사람이 아니라 수신장치이므로 이들 장치에 대해 적법성 여부를 인증하여 이들 장치가 고급 콘텐츠를 핸들링할 수 있는 자격이 있는지의 여부를 검증하자는 것이다. 이러한 인증 시스템은 현재 규격상에는 장치인증의 개념에 한정되어

있으며, 데이터방송 표준에서 데이터 콘텐츠에 대한 인증이 일부 포함되어 있으나, 향후 TV Anytime 표준화의 RMP(Right Management and Protection) 규격화 작업 등과도 연계하면서 이 분야의 전반에 확장될 소지가 많이 있는 것으로 생각된다. 본 규격상의 인증 시스템과 프로토콜 그리고 시스템적 구현 방안과 Service Revocation 등에 대해서는 다음 기회가 있을 경우 자세히 소개하기로 한다.

맺음말

본 기고에서는 디지털 케이블방송의 미국 차세대 표준인 동시에 우리나라 디지털 케이블방송 표준으로 채택하고 있는 오픈케이블 표준 규격에 포함되어 있는 복제방지 기술에 대하여 소개하였다.

본 기고에서는 시스템적인 차원에서 세부적인 프로토콜과 구현관점에서의 기술적인 내용들은 대부분 생략하고, 복제방지 기술의 도입배경과 필요성 그리고 복제방지 시스템 규격에 적용된 정보보호기술들이 어떤 것들이 있으며, 어떠한 기술요소에 의해 복제방지 시스템을 구성하는지에 대하여 중점적으로 소개하였다.

이와 같은 복제방지 시스템도 넓은 차원에서 보면 정보보호시스템에 속한 시스템 기술로서 정보화사회의 고도화에 따른 역작용을 최소화하여 보다 풍부하고 다양한 정보의 활용을 위해 반드시 해결되어야 할 문제로 생각된다.

불법 소프트웨어 복제가 소프트웨어 산업발전의 저해요소가 될 수 있듯이, 디지털방송 산업분야에 있어서도 미래의 고부가가치 산업으로 예상되는 디지털방송 콘텐츠 산업에 대한 저작권 보호를 위하여 현재의 디지털방송 시스템 규격은 다양한 정보보호 기술들을 도입하면서 멀지 않은 장래에 있을 것으로 예상되는 불법복제의 문제점에 대해 기술적인 관점에서 그 해법을 접근하며 대비하고 있는 것이다. 이를 위해서는 단순히 어떤 특정 부분에 특정 기술을 적용하는 것으로만 해결할 수는 없으며, 콘텐츠의 생산에서부터 전달과 최종 활용시점까지 시스템 전반적인 차원에서 고려되어야 할 부분이 많은 것으로 생각된다. 실제로 오픈케이블 규격도 이러한 복제방지 기술부분의 반영을 위해 하드웨어 구성을 포함하여 다른 관련된 표준 규격을 몇차례 수정해온 바 있다.

방송환경이 디지털로 전환되어 가면서 보다 양질의 고급 디지털 방송 콘텐츠의 확보여부가 디지털 방송산업의 성패를 좌우하게 될지도 모르며, 따라서 고품질 영화 또는 고급정보의 방송 데이터 등의 콘텐츠 산업의 육성과 보호를 도모하기 위해 반드시 해결해야할 불법복제 문제에 대한 해법으로서, 이와 같이 차세대 디지털 케이블방송 표준에 복제방지 기술을 적극 반영하고 있는 것이다.

참조 문헌

[1] SCTE 41 2001(Formerly DVS 301) POD Copy Protection Standard

[2] SCTE 28 2001(Formerly DVS 295) HOST-POD Interface Standard

[3] OpenCable Specification, OC-SP-PODCP-IF-I07-020524

[4] OpenCable Specification, OC-SP-HOSTPOD-IF-I10-020524

[5] NRSS(National Renewable Security Standard), EIA-679 Part B

[6] NIST FIPS PUB 180-1, Digital Signature Standard

[7] NIST FIPS PUB 140-1, Security Requirements for Cryptographic Modules

[8] NIST FIPS PUB 81, 46-2, DES Modes of Operation, Data Encryption Standard
[9] U.S. Patent No. 4,860,353, DFAST encryption technology
[10] CableLabs, PHILA-POD-Host Interface License Agreement
[11] David Broberg, "COPY PROTECTION IN DIGITAL CABLE TELEVISION SYSTEMS", NCTA 2001.
[12] Doug Jones, "Public Key Infrastructure-Using X.509 Certificates for Device Authentication Here a Cert, There a Cert, Everywhere a Cert", NCTA 2002.

IBM '생각하는 DB' 만든다

'데이터베이스가 사람처럼 인식능력을 가질 수 있을까?' 세계 최대 컴퓨터업체인 IBM이 이에 도전하고 있어 관심을 모으고 있다. 특히 이는 신용카드 번호 등 민감한 개인정보를 담은 데이터 유출을 막을 수 있어 전세계적으로 개인정보 유출이 사회 문제가 되고 있는 것과 관련, 더 호기심을 불러일으키고 있다. IT월드(http://www.itworld.com) 따르면 IBM의 알마덴연구센터에서 근무하는 라케시 애그로월 최고연구원(펠로)은 인식능력을 갖춘 고기능의 데이터베이스 개발 프로젝트를 추진, 향후 1~2년내에 가시적 성과를 내기 위해 연구력을 집중하고 있다. 애그로월은 이와 관련된 연구 논문을 최근 홍콩에서 열린 '2002년 대형 데이터베이스 학술회의(Very Large Database 2002 Conference)'에서 발표, 주목을 받기도 했다. 이 시스템의 작동 방법은 다음과 같다. 우선 데이터가 한 곳으로 집합되기 전에 이 데이터의 정보 유형이 먼저 파악된다. 그리고 이 데이터가 어떻게 사용될지 등의 기본적 규칙이 결정되는데 이 규칙에는 누가 이 데이터에 접속할 수 있는지, 또 이 데이터를 얼마 동안이나 가지고 있는지 등이 포함된다. 이후에는 유저의 애플리케이션이 데이터 베이스와 상호 작용, 데이터 프라이버시 정책이 사용자들에게 제대로 받아들여지고 있는지 체크하게 된다. 이런 과정을 거쳐서야 마침내 데이터는 데이터베이스로 이동하게 된다. 고도의 프라이버시 능력을 갖춘 이러한 데이터베이스를 개발중인 애그로월은 "현재의 데이터베이스는 단순히 기록을 보관하는 데 그치고 있으며 데이터를 가지고 무엇을 해야 할지를 알려주는 지침이 없다"며 개발 배경을 설명했다. 그는 의사인 동생이 "의사들은 히포크라테스 선서로 윤리 능력을 고양하고 있다"는데 힌트를 얻어 연구에 나섰는데 그래서 이름도 '히포크래틱 데이터베이스'(Hippocratic Database)라고 짓고 있다. 즉 그리스 명의인 히포크라테스가 제창한 의사의 기본윤리 처럼 '히포크래틱 데이터베이스'가 개인의 민감한 정보 유출을 막아주는 '윤리적 데이터베이스'가 될 수 있을 것이라는 주장이다. 하지만 이와 비슷한 시스템 개발은 애그로월이 처음은 아니다. 인터넷표준화 국제기구인 W3C(World Wide Web Consortium)가 특정 웹사이트의 프라이버시 정책을 사이트 접속자에 알려주기 위해 올해 초 만든 'P3P'(Platform for Privacy Preferences)도 이와 비슷하게 프라이버시를 보호하고 있다. 애그로월은 "하지만 P3P는 초기에 프라이버시를 체크하지만 제어력이 없다. 우리가 개발하는 데이터베이스는 데이터가 사용되는 시간의 양까지 통제할 수 있다"고 언급하고 있다. 현재 애그로월은 첫 연구 단계를 마치고, 이의 성과를 IBM의 'DB2' 데이터베이스에 구현했는데 데이터의 사용시간까지 통제하는 연구에 나설 예정이다. 애그로월은 "앞으로는 우리가 개발중인 데이터베이스 보유 유무가 기업의 경쟁력을 가늠하는 시대가 올 것"이라고 강조했다.