특집

디지털방송과 미디어 보호관리

[redacted]

디지털방송, 특히 HD급 디지털방송이 본격적으로 시작되면 미디어 보호가 심각하고도 시급한 문제로 대두될 것이다. 고화질의 비디오와 뛰어난 품질의 오디오를 근간으로 하는 HD급 미디어를 무단복제해서 배포할 경우 미디어 제작자들이 양질의 미디어 제공을 꺼리게 될 것이고, 이것이 시청자의 피해가 돌아갈 것이라는 주장이 설득력을 얻어가고 있다. 한편 저작권보호 기술이 소비자의 권리를 침해하고 오히려 저작권보호 기술의 발전을 저해한다는 의견도 있다. 그래도 저작권보호 기술이 많이 진보했지만 아직 그 기술들이 쓸만하다고 보여지지는 않는다. 여전히 소비자들은 무료에 익숙해져 있고 P2P (Peer-to-Peer) 기술이 널리 확산되었으며 특히 기존 보호기술이 공격에 취약하다. 그렇더라도 저작권보호 기술은 중요한 기술로 자리잡을 것이고 계속 발전하겠지만 여전히 한계를 지닐 것으로 보인다. 그래서 기술적인 조치와 법률적 조치가 동시에 필요하다. 이미 법률적 조치들만으로는 시장의 질서가 잡히지 않음을 확인한 바 있다. 최근 DMP (Digital Media Project) 표준화가 시도되면서 기술적 측면 외에도 법률적 측면이나 사회적 측면도 고려되고 있다. 그래서 여기서는 저작권보호 현황과 이슈들을 기술적인 관점과 법률적 관점에서 살펴봄으로써 기술적 조치가 고려해야 할 새로운 측면을 도출하고자 한다.

Ⅰ. 저작권보호의 필요성

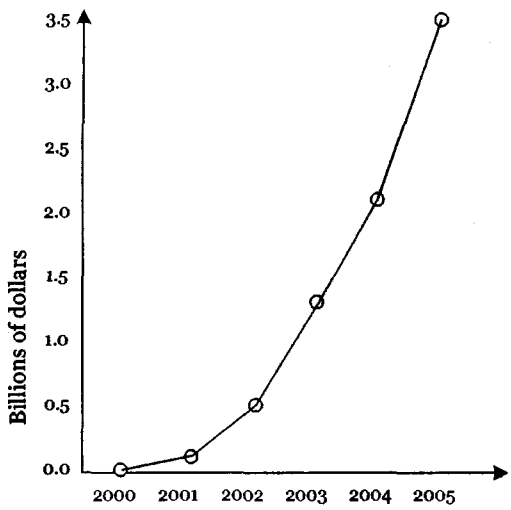
디지털기술이 발전하면서 아날로그 시대에 경험할 수 없었던 여러 현상이 나타나고 있다. 대표적인 예가 질적 저하 없이 얼마든지 미디어를 복제할 수 있다는 것과, 인터넷을 통해 쉽게 대량 배포할 수 있다는 것이 그것이다. 게다가 MP3와 같은 압축기술이 적용되면서 디지털 미디어가 무단복제에 얼마나 무방비상태로 노출되어 있었는지 확인된 셈이다. 즉, 비트 단위의 복제와 복제나 전송 도중 발생하는 오류를 정정할 수 있는 뛰어난 디지털 기술의 장점이 저작권 관점에서는 독이 됨을 알 수 있다. 디지털방송이 시작되면 이런 장점이 오히려 디지털방송의 발목을 잡을 가능성이 높다. 방송되는 디지털 미디어를 질적 열화 없이 대량 복사해서 무단배포하면 미디어 제작자는 수익 창출이 어려워질 수 있고, 이것이 양질의 미디어 제작 열의를 꺾을 것이고, 그러면 방송의 질이 떨어질 수 있다.

디지털세계에서의 불법복제 문제는 디지털방송의 구상단계에서부터 예견되었다. 그래서 이미 오래 전부터 불법복제에 대응하기 위해 다양한 기술을 연구해왔다. 그러나 당시로서는 인터넷 기술이 초보 단계에 있었고 네트워크 속도도 느려 오늘날과 같은 멀티미디어 환경과는 거리가 멀었고 당시로서는 불법복제의 위험성만 예상되었을 뿐이어서 불법복제가 피부에 와 닿지도 않았고 그리 큰 위협으로 느껴지지도 않았다. 그러나 MP3 플레이어가 출현하면서 그 심각성이 표면화되었고 패닉 현상까지 보일 정도로 충격을 받았다. 미국의 경우 대학을 중심으로 CD 판매량이 급감하면서 겨우 미국음반협회에 해당하는 RIAA(Recording Industry Association of America)는 상황의 심각성을 인식하기 시작했다. Napster와 같은 P2P(peer-to-peer) 업체는 더욱 문제를 더욱 복잡하게 만들었다. Napster 가입자들이 음악파일을 공유한다는 명분 아래 무료로 음악 파일을 무료로 주고 받았다. 서버는 단지 누가 어떤 파일을 가지고 있는지 알려줄 뿐이고 그 사이트 가입자들은 그 리스트를 보고 서로 파일을 주고 받았다. 물론 법정에서 Napster가 패소해 최소한 Napster가 불법복제를 방조하게 하는 것은 막았지만 그렇다고 P2P 업체가 모두 사라진 게 아니었다. 오히려 더 많은 P2P 업체가 생겨나 문제가 더 꼬여버렸다. 이것은 저작권보호를 위해 끊임없이 법률적 도움을 받아야 함을 의미한다. 초기에는 미국 음반협회에 해당하는 RIAA가 Napster와 같은 큰 회사를 상대로 재판을 걸면 모든 문제가 해결될 수 있을 것으로 여겼으나 불법복제가 줄어들기는커녕 더 기승을 부리자 최근에는 복제를 많이 한 개인을 상대로도 소송을 걸기에 이르렀다.

법률적인 방법 말고도 기술적으로 불법복제를 막을 방법이 있기는 하지만 기술적으로 완벽한 단계에 도달하지는 못했다. 제한수신이나 워터마킹 등 여러 기술이 있지만 아직 제 자리를 잡지 못하고 있다. 여기에는 여러 원인이 있다. 첫째 이유는 멀티미디어의 특성에서 기인하는 것으로 방송 미디어의 용량이 큰데도 리얼타임 처리가 요구되기 때문이다. 텍스트나 음악 파일에 비해 HD급 미디어는 비교할 수 없을 정도로 용량이 큰다. 예를 들어 MP3 곡이 128 kbps라면 HD급 방송은 약 20 Mbps를 요구한다. 그런데다 방송의 특성상 미디어가 끊기지 않고 리얼타임으로 플레이되어야 한다. 당연히 많은 계산능력이 요구된다. MPEG 디코딩도 계산량을 많이 요구하는데 여기에 저작권보호를 위해 복잡하고 시간이 많이 소요되는 암호기술을 적용하면 리얼타임 처리가 힘들어진다. 그래서 고도의 암호기술을 적용하지 못하는 것이 기술적 애로의 한 원인이 되고 있다.

둘째, PC를 비롯한 대부분의 기기가 고유한 식별체계를 지니고 있지 않다는 점에 주목할 필요가 있다. 즉 이 PC와 저 PC의 다른 점이 있어야 하는데 기존의 PC들은 차이가 없다. 기기가 서로 구별되어야 그것을 기반으로 불법복제에 가담한 기기를 찾아낼 수 있겠지만 현재로서는 그런 일이 원천적으로 불가능하다. 지구상의 모든 사람들이 얼굴이 같고 같은 옷을 입고 있다면 인상착의만으로 범인을 잡을 수 없는 것과 같은 이치이다.

그리고 셋째는 DRM (Digital Rights Management) 기술이 보여준 착시 현상이다. 다시 말해 아직까지 시장은 아날로그 관행이 주류를 이루는데 DRM은 완전히 디지털로 이행한 것처럼 착각함으로써 아날로그 시대에 만들어진 비즈니스 관행을 간과하는 잘못을 저질렀다.



〈그림 1〉 DRM 소프트웨어 및 관련 산업 규모: 2000-2005 (자료: IDC 2001)

예를 들어 저작권 관련 법률만 해도 책이나 음반처럼 손으로 만져지는 형체가 있는 것에 담겨진 창작물을 대상으로 삼고 있다. 그런데 완전한 디지털 미디어는 형체가 없는 숫자들만의 조합이라서 과거의 법률적 잣대나 관행이 적용되기 어렵다. 책을 산 사람은 그 책을 친구에게 빌려줄 수 있지만 그 책은 한 권이므로 늘 한 시점에서 그 책은 한 권일 뿐이다. 그런데 MP3 음악은 한 곡을 사서 복사하면 원본과 동일한 곡이 얼마든지 만들어진다. 그런데 소비자들은 여전히 아날로그적으로 생각하고 있다. 그래서 이런 착시현상에 대한 자성의 목소리가 최근의 DMP (Digital Media Project) 활동에서 제기되었다. 그래서 DMP에서는 기술 외적인 사항을 충분히 고려하면서 기존의 전통적인 비즈니스 모델도 새로운 DRM에 반영하려는 노력을 경주하고 있다. 책은 헌 책으로 팔 수도 있지만 MP3곡은 살 수 있지만 싫증이 났을 때 헐 값에 팔 방법도 없다. 이런 것이 디지털 도메인에서 수용할 수 없는 과거의 관행인 것이다.

그럼에도 불구하고 디지털방송은 이제 막을 올렸고 HD급 방송이 본격적으로 확산되고 있다. 그런데 불행하게도 아직까지 불법복제를 방지할 수 있는 만족할만한 기술적 대책이 마련되지 않았다. 설령 그런 기술이 마련된다고 해도 그 기술은 "선량한 사람을 계속 선량하게 한다 (Keep honest people honest)"는 원칙을 고수하는 선에 머물 것이다. 이것은 아무리 고도의 기술을 개발할지라도 크래커들에게는 여전히 좋은 공격의 대상 가운데 하나일 뿐이고 언젠가는 그 기술이 깨어질 수 밖에 없음을 인식하고 있기 때문이다. 법률적 수단도 같은 한계를 지니고 있음이 밝혀졌다. 그렇다고 그런 법이라도 없으면 불법복제가 기승을 부릴 것이므로 법이 있는 것처럼 기술도 그를 것이다. 또 법이 있으면 그나마 사회가 안전할 것이라는 믿음을 주는 것처럼 기술이 있음으로 미디어 제작자들을 안심시킬 수 있다.

디지털방송은 세계적으로 국가적인 프로젝트로 인식되고 있다. 디지털방송은 국가정보화의 중추를 이루는 골격이자 가전, 반도체, 소프트웨어, 디스플레이, 통신, 디지털 미디어 등 관련 산업과의 연계효과가 매우 크다. 또 방송과 통신의 융합이 가속화되고 있는 시점이라 디지털방송이 통신영역까지 영역을 확장해 사회적 영향력도 커지고 있다. 게다가 양방향통신을 수용하여 시청자의 참여를 유도하고, 대화형 기술을 활용해서 시청자가 바라는 프로그램을 만들려고 하기 때문에 방송이 중요하다. 그래서 한국도 고정수신에 중점을 둔 디지털TV와 이동수신을 강조한 DMB (Digital Multimedia Broadcast) 사업을 본격적으로 추진하고 있다. 따라서 디지털방송을 성장시키기 위한 방안의 하나로 디지털 저작권

보호 기술도 개발하도록 독려할 필요가 있다.

안타깝게도 복제방지 기술은 산업으로 자리잡는데 아직까지는 실패했다. 그것은 전술한 바와 같이 불법복제가 사라지지 않고 있기 때문이며 본격적으로 메이저 방송이 DRM을 채택한 일도 없었다. 당연히 DRM이 수익을 낼 시장이 열리지 않았고 이로 인해 수익을 낼 기회도 없었다. 그러나 방송이 본격적으로 시작되면 상황은 크게 달라질 것이다. 그리고 미디어 시장의 핵심 기술이 될 것으로 보여 꾸준한 관심과 투자가 필요하다. 그림 1이 DRM 산업의 현황과 미래를 보여주고 있다.

II. 저작권보호에 관한 이해

저작권 관련된 용어들에 대한 이해는 앞으로의 논의를 진행시키는데 큰 도움이 된다. 저작권은 특허, 상표, 의장 등들 포함하는 공업소유권과 더불어 지적소유권의 일환을 이루고 있다. 저작권과 공업소유권의 차이점은 공업소유권은 특허 등의 아이디어 자체를 보호하는데 반하여 저작권은 저작권의 아이디어나 사상, 감정 등이 "표현된 것"을 보호하는 것이다. 저작권은 크게 저작재산권과 저작인격권(moral rights)으로 나누어 볼 수 있다.

저작권(copyrights)이란 시, 소설, 음악, 미술, 영화, 연극, 컴퓨터 프로그램 등과 같은 저작물에 대해 창작자가 가지는 권리를 말한다. 예를 들면, 소설가가 소설작품을 창작한 경우에 그는 원고 그대로 출판 및 배포할 수 있는 복제 및 배포권과 함께 그 소설을 영화나 번역물 등과 같이 다른 형태로 저작할 수 있는 2차적 저작물 작성권, 연극 등으로 공연할 수 있는 공연권, 방송물로 만들어 방송할 수 있는 방송권 등 여러 가지의 권리를 가지게 된다.

방송권에 의해 저작권자는 자신의 저작물이 방송에 이용되도록 허락할 권리를 가진다. 방송이 일반공중으로 하여금 수신하게 할 목적으로 무선 또는 유선의 방법에 의해 음성, 음향 또는 영상 등을 송신하는 것을 뜻한다. 따라서, 아마추어 방송은 일반공중으로 하여금 수신하게 하는 것이 목적이 아니므로 방송에 포함되지 않는다. 그러나 재방송이나 중계방송도 모두 저작권자의 방송권의 대상이 되며, 저작권자에게 허락을 얻지 않고 방송한 경우는 저작권 침해가 된다.

전송권은 저작자에게 부여된 전송할 수 있는 권리를 말한다. 이때의 전송이란 "일반공중이 개별적으로 선택한 시간과 장소에서 수신하거나 이용할 수 있도록 저작물을 무선 또는 유선통신의 방법에 의해 송신하거나 이용에 제공하는 것"을 말한다. 인터넷 등을 통해 이용자가 개별적으로 원하는 시간과 장소에 저작물을 전달하는 형태의 자료 이용이 급증함에 따라 만든 것이 전송권이다.

배포권이란 원저작물 또는 그 복제물을 판매, 대여, 대출, 점유, 이전, 기타의 방법으로 일반공중에게 제공하는 권리를 말한다. 배포권은 기본적으로 복제권에서 유래된 권리로 이해된다. 그런데 저작권자가 일단 원저작물 또는 그의 복제물을 공중에게 배포한 때에는 그 배포권이 소멸된다. 배포권의 개념을 오로지 오프라인에 한정하고 온라인에서의 배포는 별도의 전송권이란 개념으로 파악할 수 있다.

또한 저작자, 예를 들면 소설가는 위에서 본 바와 같이 여러 가지 형태로 저작물이 이용되는 과정에서 그 소설의 제목, 내용 등이 바뀌지 않도록 하는 동일성유지권과 함께 출판된 소설책에 자신의 성명을 표시할 수 있는 성명표시권,

그리고 그 소설을 출판할 것인지의 여부를 결정할 수 있는 공표권을 가진다. 이는 저작자의 인격을 보호하고자 하는 측면에서 주어진 권리이므로, 이를 저작인격권이라 하여 저작재산권과 구분한다. 저작재산권이란 제작자가 갖는 재산적 권리를 뜻하며, 저작인격권이란 저작재산권의 소유여부를 불문하고 저작자가 자신의 저작물에 대하여 가지는 인격적인 권리를 뜻하는 것이다.

저작인접권(neighboring rights)이란 저작물의 복제 및 전파기술의 발달로 전통적인 저작권의 보호 외에 저작물의 실연, 녹음 및 방송을 통하여 저작물의 배포, 전파에 기여한 사람들의 권리를 보호해 주기 위해 인정된 권리 개념이다. 저작물은 훌륭한 실연에 의해 그 가치가 보다 증대되며, 음악의 제작이나 방송프로그램의 제작에는 고도의 기술적 또는 정신적 노력이 요구된다고 보아 이와 관련된 정신적 창작성을 인정해주게 된 것이다. 그래서 실연자, 음반제작자, 방송사업자는 저작인접권자로 보호를 받는다. 저작인접권의 보호대상은 실연, 음반, 방송이나 모든 실연, 음반, 방송이 보호되는 것은 아니며, 저작권법에 그 구체적인 적용범위를 정하고 있다. 예를 들면 방송은 한국 국민인 방송사업자의 방송, 한국에 있는 방송설비로부터 행하여지는 방송, 한국이 가입 또는 체결한 조약에 따라 보호되는 방송으로서 그 조약에 가입한 나라의 국민인 방송사업자가 그 나라 내에 있는 방송설비로부터 행하는 방송이 보호대상이 된다. 방송사업자는 그의 방송을 녹음, 녹화, 사진, 그 밖의 이와 유사한 방법으로 복제하거나 동시중계방송할 권리를 가진다. 방송사업자의 복제권은 방송의 녹음 및 녹화뿐만 아니라 그 녹음 및 녹화물을 또다시 복제하는 것에도 미친다. 다시 말하면, TV 연속극을 녹화하여 판매한 비디오테이프를 다른 사람이 임의로 복제하여 이용할 수 없다는 것이다. 다만, 종합유선방송법상 유선방송사업자에게 공중파 방송의 동시재송신 의무를 두고 있어 그 범위 내에서 방송사업자의 동시중계방송권이 제한된다. 저작인접권자의 사용승인을 받아야 하는 권리로는 복제 및 배포권, 음반의 거래제공 및 대여 허락권 등과 방송사업자의 음반제작자에 대한 보상 수혜권이 있다.

일반적으로 저작권에는 최초판매 이론(first sale doctrine)이 적용된다. 이 이론은 저작물을 구매한 사람은 구입한 저작물을 저작자의 허락을 받지 않고 자유롭게 처분할 수 있다는 원칙이다. 기존의 저작권법에서 일반적으로 채택하고 있지만 프로그램 보호법에서는 최초판매이론은 적용되지 않는다. 디지털 환경이 무한 복제가 가능하게 한다는 이유 때문에 복제하지 않은 원본 프로그램이라 할지라도 타인에게 양도하기 위해서는 저작권자의 허락을 받아야 한다. 즉, 이용자가 비용을 지불하고 구입한 정보를 처분할 수 있는 권리는 저작권자에 있게 된다. 좋은 예가 포장약관(shrinkwrap license)인데 프로그램의 경우 포장을 뜯으면 반품이나 환불이 되지 않도록 한 약관을 정하고 있다. 이 경우 포장을 뜯어낸 후에야 약관을 볼 수 있어 제품을 충분히 확인하기 전에 약관의 내용도 알지 못하면서 상품을 구매하므로 소비자 입장에서는 매우 불합리하지만 디지털 도메인에서는 정당한 것으로 받아들여지고 있다.

디지털방송은 디지털 저작물의 전송 그 자체이다. 이런 디지털 저작물을 보호해야 할 저작권의 주요내용이 복제권임을 감안하면, 종래의 아날로그 환경에서와 달리 원본과 복사본이 구별되지 않는 디지털 환경에서의 복제를 막을 적절

한 방법이 필요하다. 물론 할 수만 있다면 아날로그 저작물도 복제를 막을 기술적 보호장치가 필요하다. 그런데 아날로그 저작물에서는 기술적 보호조치가 상대적으로 미흡했다. 아날로그에서는 저작물에 접근하는 것이 바로 복제를 의미하지는 않았고 복제에 상당한 노력이 요구되며 대량배포나 대량복제가 쉽지 않았기 때문이다. 그러나 디지털 환경에서는 디지털 미디어에 접근한 순간 쉽게 복제가 되고 대량으로 배포될 수 있다.

그래서 디지털 기술 발전은 여러 측면에서 저작권과 충돌하고 있다. 그 예가 공정한 이용(fair use) 케이스이다. 공정힌 이용이란 저작권자의 이용허락 없이도 저작물을 이용할 수 있는 제도로 한국 저작권법에서도 저작재산권의 제한이라는 규정을 따로 두어 공정한 이용을 보장하고 있다. 도서관에서 복사하거나 시사보도 또는 교육의 목적으로 저작물을 이용하는 것은 허용되어 왔으며 사적이용을 위한 저작물 복제도 가능하다. 예를 들어 작품의 비평, 해설, 보도, 연구조사 등의 비영리적 목적으로 저작물의 일부를 이용하는 경우 저작권자의 허가를 얻지 않아도 된다는 권리를 말한다. 그런데 공정한 보도를 강조할 경우 디지털 데이터의 특성상 무단복제가 횡행하게 될 것이라는 우려가 높다.

III. 기술적 보호조치

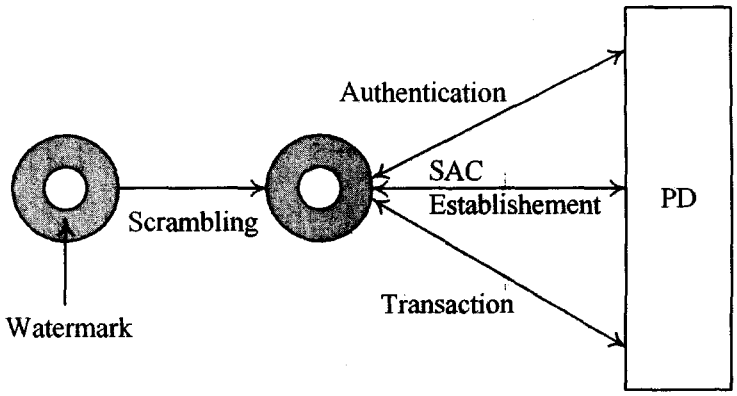
아날로그 시대에도 불법복제는 있었지만 디지털에 비하면 물리적 제약이 많았다. 예를 들어 음반을 복제해서 불법으로 판매한다고 가정하면 최소한 다음 과정을 거친다.

1. 테이프를 구입한다. (물론 돈이 든다)
2. 복제장치를 구입한다. (여기에도 돈이 든다)
3. 복제한다. (시간을 투자해야 한다)
4. 포장한다. (노동력이 필요하다)
5. 판매한다. (붙잡히지 않도록 조심해서 판다)

이 과정을 거치는 동안 각 단계마다 상응하는 비용, 노동력, 시간을 투입해야 한다. 그래서 아날로그 복제는 힘들다. 특히 아날로그 복제에서는 복제할수록 품질이 떨어진다. 요약하자면 아날로그 복제는 그 자체에 복제를 억제하는 내재적 요인이 존재한다.

그런데 디지털에서는 복제를 부추기는 요인이 너무 많다. 첫째 손가락으로 클릭 한 번 하면 원본과 완벽하게 일치하는 복제품이 만들어진다. 시간, 노동력, 비용이 거의 들지 않는다. 인터넷에 연결되어 있기만 하다면 전세계 누구에게라도 순식간에 원본과 동일한 미디어를 보낼 수 있다. 그래서 법률적 보호수단을 써봤지만 그것만으로는 저작권의 침해에 대해 효율적으로 대처할 수가 없다는 것이 이미 잘 알려졌다. 따라서 저작권자는 저작물의 불법적인 이용을 방지하기 위해 기술적인 방법을 사용하여 저작권을 보호하려고 한다. 그러나 이러한 기술적인 보호장치도 대응하는 기술 발전으로 언젠가는 이를 무력화할 수 있어 불법적인 이용을 방지하려는 이러한 기술적 보호장치를 법적으로 보호해야 할 필요성이 생겼다. 그래서 기술적 조치를 무효화, 우회, 제거, 해체 또는 기타 회피하는 것을 주요 목적으로 하는 장치나 상품의 수입, 제조 또는 판매하거나 어떠한 서비스를 제공하는 것도 금지하는 내용을 저작권법에 포함시키는 것이 미국을 비롯한 주요국가의 추세이다.

기술적 보호방법은 주로 접근방지, 복제방지, 전송방지, 사용통제 기술로 분류할 수 있을 것이



〈그림 2〉 통상적인 안전한 채널 연결 절차

다. 접근방지 기술은 그 가운데 가장 개발하기 쉬운 것으로 기존의 CAS (conditional access system) 시스템이 여기에 속한다. 그리고 방송 내용을 저장하는 장치에는, 예를 들면 PVR (personal video recorder) 등에는 인증(authentication), 안전한 세션 채널(secure session channel) 열기, 권리(rights) 전달 등의 순서를 거치도록 권장한다. 그림 2가 이런 내용을 요약해서 보여주고 있다. 미디어에 워터마크를 삽입해서 판매나 다운로드가 가능하도록 한다. 패키징 단계에서 미디어에 대한 내용과 권리에 대한 메타데이터를 작성해서 미디어와 함께 포장한다. 휴대장치인 PD(portable device)는 서버나 STB(set-top box)와 교신한다. 이때 서버 입장에서는 PD를, PD 입장에선 서버를 확실히 신뢰하지 못하므로 인증 단계를 거친다. 이때 X.509 인증서를 이용하며 인증기관의 도움을 받는다. 인증단계 및 세션 키 교환에서는 안전을 위해 보통 공개키 방식을 이용한다. 인증이 끝나고 세션키를 교환하는데 이때 흔히 Diffie-Hellamn 프로토콜이 사용된다. 세션키는 비밀키 방식을 사용하는데 디지털 미디어 암호화 및 복호화에 공개키 방식은 너무 계산시간이 많이 들기 때문이다. SAC(secure authenticated channel)이 열리면 그 채널을 통해 패키지에 담긴 미디어를 주고 받을 수 있다. 그 패키지에는 저작권 관련 메타데이터가 담긴다.

저작권 관련 사용권리(usage rights) 메타데이터는 보통 다음과 같은 양식을 취한다. 사용권리는 그 미디어를 사용할 수 있는 방법을 기술한 것으로 복제 허용 횟수, 사용 기간 등을 명시하고 있다. 예를 들어 아래의 사용권리에 보면 사용기간이 <notAfter>2004-03-13T23:59:59</notAfter>로 명시되어있는데 사용기간이 2004년 3월 13일까지라면 그 이후에는 사용이 불가능하다. 사용권리는 반드시 암호화되어 서버에서 PD로 보내진다.

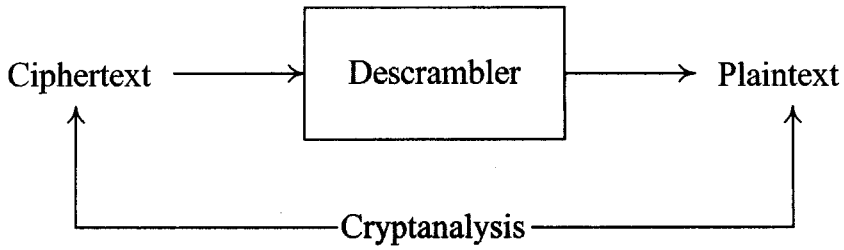
복제방지 기술이나 전송방지 기술은 자체기술로 개발이 쉽지 않은 난점이 있다. 그래서 이런 기술이 스스로 존재할 수 없기 때문에 위에서 인증을 받은 곳에만 전송을 한다거나 사용권리에 표시된 복제허용 횟수와 연계하여 복제를 허용하는 것이 그것이다. 워터마크와 연계시키는 것도 한 방법일 수 있다.

디지털방송 미디어를 보호하려는 기술도 제한접근 (conditional access) 및 워터마크 삽입 등을

```
〈license〉
        〈grant〉
                〈keyHolder〉
                        〈info〉
                                〈dsig:KeyValue〉
                                        〈dsig:RSAKeyValue〉
                                                〈dsig:Modulus〉Fa7wo6NYfmvGqy4ACSWcNm
                                                uQfbejSZx7aCiblgkYswUeTCrmS0h27GJrA15
                                                SS7TYZzSfaS0xR9IZdUEF0ThO4w==
                                                〈/dsig:Modulus〉
                                                〈dsig:Exponent〉AQABAA==〈/dsig:Exponent〉
                                        〈/dsig:RSAKeyValue〉
                                〈/dsig:KeyValue〉
                        〈/info〉
                〈/keyHolder〉
                〈cx:play/〉
                〈cx:digitalWork〉
                        〈cx:locator〉
                        〈nonSecureIndirect URI="http://thisMovie.mpg"/〉
                        〈/cx:locator〉
                〈/cx:digitalWork〉
                〈validityInterval〉
                        〈notAfter〉2004-03-13T23:59:59〈/notAfter〉
                〈/validityInterval〉
        〈/grant〉
〈/license〉
```

사용한다. 그래서 다양한 기술을 개발하고 표준화하려는 움직임이 대두되고 있다. 앞으로 디지털방송 미디어에 스크램블링 기술이 널리 적용될 것이다. 공익을 우선하는 방송은 스크램블링 기술을 적용하지 않을 것이다. 그러나 영리를 목적으로 하는 방송은 대부분 스크램블링 기술을 적용하게 될 것이다. 그런데 디지털방송 스크램블링에서 가장 문제가 되는 것은 이 시스템이 기지평문공격(known plain-text attack) 환경에 고스란히 노출되어 있다는 점이다. 암호를 풀기 전 미디어와 푼 후의 미디어를 모두 가지고 있기 때문에 공격자는 마음만 먹으면 키를 비교적 쉽게 찾을 수 있다. 그림 3이 기지평문공격의 개념을 보여주고 있다. 왼편에 스크램블링 된 미디어가 입력으로 들어와서 원래의 미디어로 복원하자면 키가 필요하다. 이 키가 없기 때문에 미디어를 볼 수 없기 때문에 공격하는 사람 입장에서는 그 키를 알아내는 것이 중요하다. 이 때 어떤 키는 적용해서 원하는 미디어가 나온다면 그게 키가 되는 셈이다. 물론 모든 키를 다 적용해보는 것은 대단히 어리석은 일이지만 어느 키인가가 완벽한 영상을 재현해준다면 더 이상 다른 키를 써볼 필요 없이 그 키가 찾고자 했던 키라고 단정해도 된다.

디지털방송은 비디오 및 오디오를 전송하고 부가서비스로 데이터도 전송하게 된다. 일반적



〈그림 3〉 기지평문공격의 개념

으로 비디오는 데이터 양이 방대해서 전송에 시간이 많이 걸린다. 그래서 불법복제 전문가들도 일단은 양이 적은 오디오를 주로 공격한다. 그리고 비디오 스크램블링은 처리시간 단축을 위해 비교적 시간이 적게 걸리는 단순한 방법을 선호한다. 그런데 궁극적으로는 비디오에서도 공격에 강인하면서 처리속도도 낮은 기술을 채택하게 될 것이다. 데이터는 주로 T-Commerce와 관련된 상품거래 정보들이기 때문에 복제방지보다는 개인의 사생활 정보보호 차원에서 접근해야 한다.

아무튼 크래커들의 공격에 견디기 위해서는 두 가지 접근법이 있다. 하나는 키를 자주 바꾸는 방법이다. DVD를 비롯한 많은 시스템에서 키를 (예를 들면 15초마다 한 번씩) 바꾸는 방법을 적용하고 있다. 둘째는 키를 길게 하는 방법이다. 그런데 이 방법은 계산에 시간이 많이 소요되어 당분간 적용하기 어렵다. 멀티미디어 속성 때문에 키를 다 풀어놓고 나중에 천천히 보고 듣는 것은 상품성이 없다. 멀티미디어는 리얼타임 처리가 가능할 때 상품성이 극대화된다.

디지털전환에 가장 적극적인 미국은 재정적인 문제나 운영 경험의 부족 등을 이유를 들어 디지털 전환의 어려움을 토로하고 있다. 그러나 디지털 전환 이행에 있어서 재정적인 문제는 본질적인 문제가 아니며 오히려 디지털 미디어 보호방안 부재 등 다른 부분들이 방송사업자 및 미디어 사업자의 조속한 디지털 전환 이행을 늦추고 있는 것으로 나타났다 [1]. 이에 FCC는 디지털 전환의 조속한 이행을 위해 몇 가지 방안을 검토해 왔고, 최근에도 디지털 전환의 조속한 이행 완료를 위한 다양한 촉진 정책을 채택하고 있다. 예를 들어 브로드캐스트 플래그(broadcast flag)가 좋은 예이다.

미국의 경우 디지털 미디어를 제공하는 할리우드 영화사들의 입김이 거세 그들의 입맛에 맞는 정책을 펼 수 밖에 없다. 할리우드 영화사들은 디지털방송 프로그램을 무단복사해서 인터넷에서 무제한적으로 배포해 저작권을 심각히 침해할 수 있음을 알고 있어 브로드캐스트 플래그를 요구하고 나섰다. 이 플래그는 디지털방송 프로그램에 삽입되는 한 비트의 정보에 불과한데 이것에 대한 논란은 매우 뜨겁다. 한 비트이므로 이것으로 표현될 수 있는 상태는 온 아니면 오프 가운데 하나이다. 만일 어느 프로그램이 온으로 세팅되어 있다면 그 프로그램은 불법복제와 무단배포가 불가능하게 해야 함을 의미하고, 오프라면 복제와 배포에 제한이 없음을 의미한다.

미국에서 지상파 디지털TV 방송을 개시한 1998년의 시점에서는 지금처럼 브로드밴드 네

트워크의 보급이나 P2P에 의한 음반업계의 타격은 상상도 할 수 없었다. 그래서 복제방지 기술을 미처 도입하지도 않은 상태에서 디지털TV가 판매되기 시작했다. 그래서 이미 팔려버린 디지털TV에서 수용하기 힘든 기술을 채택할 경우 기존의 디지털TV 사용자로부터 반발을 살 수 있다. 예를 들어 디지털 미디어를 암호화해서 방송하면 전혀 시청이 불가능한 상황이 발생한다. 시기를 놓친 것은 분명하지만 그렇다고 새로운 기술을 빨리 도입하지 않으면 우량 미디어가 점차 줄어드는 상황이 발생할 수 있고 브로드밴드 네트워크는 더 널리 보급되어 피해가 커질 수 있다. 그래서 이제라도 보호장치를 도입하도록 해야 한다는 것이 MPAA 등을 통해 주장하는 디지털 미디어 업계의 목소리이다. 그렇다고 더 좋은 기술, 더 완벽한 기술을 채택하게 하자면 시간이 오래 걸려 현재 가용한 기술이면서 소비자의 반발도 최소화할 수 있는 기술로 브로드캐스트 플래그가 채택된 것이다. 예를 들어 디지털 워터마크와 같은 기술은 아직 강인성이 확실히 확보되지도 않았고 그것이 쓸만할 때까지 무작정 기다릴 수도 없다는 것이다. 기다리는 사이에 가전업계는 보호장치가 없는 기기를 대량으로 보급할 수 밖에 없고 그렇게 되면 미디어 업계 관점에서는 상황이 점점 더 악화되기 때문이다.

여기에 아날로그 홀 (analog hole) 같은 복병은 디지털 미디어 보호를 어렵게 만든다. 디지털방송을 수신해서 아날로그 출력으로 수신하고 저장하면 브로드캐스트 플래그는 무력화된다. 디지털 세계와 아날로그 세계가 공존하는데 디지털 세계만 존재하는 것처럼 생각하고 브로드캐스트 플래그를 만든 결과가 아날로그 홀이다. 워터마크 기술은 아날로그 홀에 대응할 수 있는 기술적 대안 가운데 하나로 보인다. 디지털 미디어에 워터마크를 삽입하면 이것을 아날로그 출력으로 만들어도 여전히 워터마크가 검출될 수 있게 할 수 있다.

기술적 보호조치에 대한 무력화 기술에 대해서는 법적으로 대응하려는 것이 일반적인 추세이다. 무력화란 무단으로 기술적 보호조치를 회피, 제거, 손괴하는 등의 행위와 저작권자의 허락도 없이 스크램블된 저작물을 푸는 것, 또는 그 밖에 기술조치를 회피(avoid), 우회(bypass), 제거(remove), 해제(deactivate), 또는 제거(impair)하는 것을 말한다. 무력화 행위는 일반적으로 접근통제 무력화와 이용(복제 등)통제의 무력화로 나눌 수 있다. 이런 규제가 카피레프트(copyleft)를 주장하는 측의 강력한 반발을 사고 있지만 이미 DMCA (Digital Millenium Copyright Act) 등에 입법화되었다.

IV. 방송과 저작권보호

저작권보호의 필요성에 대해서는 이미 충분한 논의가 있었다. 그래서 이제는 방송사업자나 시청자가 만족할 만한 수준의 기술을 구현할 필요가 있다. 그러자면 둘을 만족할 만한 요구사항이 먼저 나와야 한다. 방송용 DRM관 관련해서는 여러 요구사항이 존재한다. 예를 들면 EU에서의 방송사업자의 주요 요구사항은 다음과 같다 [2].

1) 복제방지 기술은 융통성이 있고 인지된 위협의 정도에 비례해서, 그리고 미디어 형태, 미디어의 가치, 미디어가 시청자에게 제공되는 방법에 따라 적절히 대응할 수 있어야 한다. 인터넷에서의 온-디맨드 서비스를 통해 고급 미디어가 무단으로 재전송되는 것을 합리적인 수준에서 효과적으로 대처할 수 있는 방안을 제공하는 것이 DRM의 주

요 목표이다.

2) 달리 상호연동성(interoperability)를 달성할 수 없는 상황이 아니라면 강제규정(mandatory)을 허용하지 않는다. 공개된 하나의 표준에 자발적으로 합의하는 것이 가장 이상적인 방법이다. 그것이 불가능하다면 기술적 규격에서의 완전한 상호연동성과 추가적인 비용의 부담이 없음을 보장해야 한다. 특별히 소비자 관점에서 수평적인 기기 시장을 허용하기 위해 비용부담이 없어야 한다.
3) 이미 시장에 뿌려진 기기들에 대한 적절한 고려가 있어야 한다. 즉, 새로운 기기로의 완전한 이행에 적절한 기간을 허락해야 한다. 그래야 사용자나 생산자도 대비책을 세울 수 있다. 갑자기 기존의 모든 것을 중단하고 새로운 시스템으로 이행하도록 하는 것은 시장질서를 혼란에 빠뜨릴 위험을 지니고 있다.
4) DRM 시스템은 방송 신호와 간섭을 일으켜서는 안된다. 복제방지는 제한수신과 본질적으로 다르다. 따라서 DRM 시스템이 전송할 신호를 스크램블하게 할 것인지 말 것인지는 전적으로 방송56사업의 재량에 달려있다. 복제방지 기술을 적용함으로써 발생하는 시각적, 청각적, 또는 시간지연 효과는 그 신호를 기기에 저장하거나 포착할 때 한 번만 발생해야 한다.
5) DRM 시스템은 비용 관점에서 효율적이라야 한다. DRM 기법이 관리비용 증가나 적법한 디지털 방송과 관련된 다른 비용을 증가시키지 말아야 한다.
6) DRM의 구현 뒤 방송한 미디어가 3자에 의해 깨지더라도 방송사가 책임을 지는 일이 없어야 한다.

CPTWG (Copy Protection Technical Working Group) 산하의 BPDG (Broadcast Protection Discussion Group) 주요 요구사항은 다음과 같다 [3].

1) 인가되지 않은 재전송에 대항하기 위해 복조 시점에 시작하는 것으로 브로드캐스트 플래그에 기반을 둔 접근법은 디지털 형태의 DTV 미디어 시그널링 보호 목적에 기술적으로 충분하다. 이 목적에 적합한 그 브로드캐스트 플래그는 ATSC 표준 A/65 재전송제어 기술자이다. ATSC 표준 A/54을 따르는 데이터 스트림의 8-VSB, 16-VSB, 64-QAM 또는 256-QAM 변조된 신호를 복조하는 시점에서 보호 요구사항이 시작되어야 한다.
2) 브로드캐스트 플래그를 찾아서 그것이 없음이 확인되거나 없을 때까지는 복조된 신호를 보호 모드로 다루어야 한다.
3) 브로드캐스트 플래그가 발견되지 않으면 마크가 없는 미디어에 대한 더 이상의 제한이나 요구사항을 부가하지 말아야 한다.
4) 마크가 있는 미디어나 스크린하지 않은 미디어는 다음과 같은 조건 아래서만 출력이나 레코딩이 가능하다.
   a) 아날로그 방식의 출력이나 레코딩
   b) 8-VSB, 16-VSB와 64-QAM 및 256-QAM 변조기 (조건에 따라)
   c) 보호되지 않는 DVI 출력 (해상도의 제한 아래)
   d) 인가받지 않은 재전송에 대항해서 특정한 수준의 보호가 가능한 디지털 출력과 레코딩 방법
5) 디지털 레코딩을 보호하기 위한 요구사항

은 브로드캐스트 플래그로 표시된 DTV 미디어를 PVR (예를 들면, TiVo나 ReplayTV 같은 하드디스크 기반의 기기) 또는 착탈식 (예를 들면, D-VHS 테이프 또는 DVD-R 디스크) 기기에서 안전하게 복사할 수 있는 소비자의 능력을 훼손하지 말아야 한다. 마찬가지로 디지털 출력을 보호하기 위한 요구사항은 DTV 미디어를 디지털 셋톱박스, 디지털 레코더, 디지털 서버, 디지털 디스플레이 장치 등이 연결된 안전한 홈 네트워크를 통해 전송할 수 있는 소비자의 능력을 훼손하지 말아야 한다.

6) 기기 내에서 사용자들의 접근이 가능한 버스를 압축된 형태로 돌아다니는 마크가 있는 미디어와 스크린되지 않은 미디어는 보호되어야 한다.

이런 요구조건을 기반으로 보다 여러 보호기술이 개발되고 있다. 여기에는 암호기술과 여러 프로토콜이 필요하고 기존의 비즈니스 관행도 포함함으로써 DRM이 제자리를 잡아가도록 해야 한다. 그래서 여전히 새로운 기술이나 아이디어가 필요하다. 이런 관점에서 비교적 최근에 나온 브로드캐스트 암호[4] 개념은 유념할 필요가 있다. 브로드캐스트 암호 기법은 특정 응용분야에서 공개키 암호기법을 대체할 목적으로 사용될 수 있다. 이것은 원래 케이블 TV 등을 위해 단방향으로 개발되었다. 기존의 방법에서는 공통으로 사용할 일단의 키들을 모든 기기가 공유하면서 보호한다. 그런데 이런 방법의 약점은 키를 배정한 다음 철회가 불가능하다. 이것은 모든 기기가 동일한 키를 보유하고 있어서 기기 하나 바꾸는 것으로는 아무 효과가 없기 때문이다. 유일한 해결책은 모든 기기를 바꾸는 것이지만 이것은 너무 비용이 많이 든다. 이런 면에서 브로드캐스트 암호가 유용하지만 실제 적용했을 때 어떤 문제가 생길지는 두고 볼 일이다.

방송분야에서 가장 발전된 기술은 그나마 제한수신 기법이다. 나머지 기법들은 앞으로도 많은 연구가 필요하다.

참고문헌

[1] 김국진, 이찬구, "디지털 전환 정책: 미국 사례 분석," 정보통신정책 제 15 권 23호. 2003.

[2] EBU-EUR, "EBU Memorandum on Digital Rights Management: Impact and Importance of DRM for Broadcasters," 2003.

[3] R. Perry, M. Ripley, and A. Setos, "Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group," http://www.mpaa.org/Press/Broadcast_Flag_BPDG.htm, 2002.

[4] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Crypto 2001, pp. 41-62, 2001.

저자소개

김 형 중

1978년 서울대학교 전기공학과 학사
1986년 서울대학교 제어계측공학과 석사
1989년 서울대학교 제어계측공학과 박사
1992년 USC 방문교수 (~1993)
현 재 강원대학교 제어계측공학과 교수
주관심분야 멀티미디어 미디어보안