Security of Digital Entertainment Content from Creation to Consumption

by A Eskicioglu, J Town, E Delp
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Security of digital entertainment content from creation to consumption

Ahmet M. Eskicioglu[*], John Town[§], and Edward J. Delp

[*]Thomson multimedia
101 W. 103rd Street
Indianapolis, Indiana 46290

[§]Technicolor
P. O. Box 7427
Charlottesville, VA 22906

Video and Image Processing Laboratory (*VIPER*)
School of Electrical and Computer Engineering
Purdue University
West Lafayette, Indiana 47907-1285

ABSTRACT

With the advent of digital technologies, many new market opportunities have emerged for content owners, content distributors, and consumer electronics/information technology industries. An essential requirement for developing a thriving marketplace is the protection of copyrighted content in digital form. There are four major stages in the delivery of content to the consumer: (1) capturing on digital media, (2) packaging, (3) distribution to home networks, and (4) transfer to the final audio/visual device within the home network. Entertainment content is of particular importance as it will be in high demand for many years to come. If an end-to-end security cannot be provided in a digital market, there would be no incentive for content creation. Lack of new supplies would result in detrimental effects for all the industries involved in the delivery chain. In this paper, we present the primary means of securing the entertainment content from creation to consumption in an attempt to understand the overall complexity of the problem.

1. INTRODUCTION

In recent years, advances in digital technologies have created significant changes in the way we reproduce, distribute and market intellectual property (IP). Digital media can now be exploited by the IP owners to develop new and innovative business models for their products and services. The lowered cost of reproduction, storage and distribution, however, also invite much motivation for large-scale commercial infringement. In a world where piracy is a growing potential threat, three complimentary weapons are in reserve to defend the rights of the IP owners: Technology, legislation and business models.

Intellectual property is created as a result of intellectual activities in the industrial, scientific, literary and artistic fields[1]. It is divided into two general categories:

- Industrial property: Includes inventions (patents), trademarks, industrial designs, and geographic indications of source;
- Copyright: Includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs.

---

[*] Email addresses for the author are: eskicioglua@tce.com, john.town@technicolor.com, ace@ecn.purdue.edu

Because of its high economic value, copyrighted entertainment content needs to be protected as long as the consumer demand is present in the market.

Creation includes all the activities in developing a new product such as a movie, a TV program, a book or a song. In making a movie, for example, the studio, producer, director and actors all work together to create an IP that is fixed on a 35-mm film for commercialization. Depending on the release window, several distribution channels exist, ranging from theatrical performances to duplication on magnetic or optical media to broadcasting off-the-air. Whatever the form of presentation, the consumer should have the necessary equipment and/or the rights to receive and consume the requested product.

The need for commodity protection has not changed over the years. Every commercial item needs some type of protection until it is introduced to the relevant market for consumption. Let's take the example of a farmer in a small village, who makes a living by selling eggs. His hens live securely in a coop that keeps the predators away. Every Saturday, the farmer puts his eggs in a basket with a bed of straw, and takes them to the local market at the town square, looking out for the thieves on his way. At the market, he makes certain that every customer pays before taking some eggs from the basket. If the commodity is digital entertainment content, we observe similar concepts and rules, but use different protection tools.

End-to-end security is the most critical requirement for the creation of new digital markets where copyrighted entertainment is a major product. After a brief overview of copyright and copyright industries, we will examine how the technological, legal and business solutions help maintain the incentive to supply the lifeblood of the markets.

2. WHAT IS COPYRIGHT?

In order to put our discussion into the right context, we will begin with the definition of "copyright," and summarize the important aspects of the copyright law. Copyright is a *form of protection provided by the laws of the United States (title 17, U.S. Code) to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works*[2]. Although copyright literally means "right to copy," the term is now used to cover a number of exclusive rights granted to the authors for the protection of their work. According to Section 106 of the 1976 Copyright Act[3], the owner of copyright is given the exclusive right to do, and to authorize others to do, any of the following:

- to *reproduce the copyrighted work* in copies or phonorecords;
- to prepare *derivative works* based upon the copyrighted work;
- to *distribute copies or phonorecords* of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
- to *perform the copyrighted work publicly*, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works;
- to *display the copyrighted work publicly*, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work; and
- to *perform the copyrighted work publicly* by means of a digital audio transmission, in the case of sound recordings.

It is illegal to violate the rights provided by the copyright law to the owner of the copyright. There are, however, limitations on these rights as established in several sections of the 1976 Copyright Act. One important limitation, the doctrine of "fair use," has been the subject of a major discussion on content protection. Section 107 states that the use of a copyrighted work by reproduction in copies or phonorecords or by any other means specified by the law, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In any particular case, the following criteria, among others, may be considered in determining whether fair use applies or not:

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes,
2. the nature of the copyrighted work,
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and
4. the effect of the use upon the potential market for, or value of, the copyrighted work.

For copyright protection, the original work of authorship needs to be fixed in a tangible medium of expression from which it can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. This

language incorporates three fundamental concepts[4] of the law: fixation, originality and expression. *Fixation*, i.e., the process of rendering a creation in some tangible form, may be achieved in a number of ways depending on the category of the work. *Originality* is a necessary (but not a sufficient) condition for a work produced by the human mind to be copyrightable. Scientific discoveries, for example, are not copyrightable as they are regarded as the common property of all people (however, an inventor may apply for a patent, which is another form of protection). Finally, it is the *expression* of an idea, and not idea itself, that is copyrightable. Ideas, like facts, are in the public domain without a need for protection. Nevertheless, the separation of an idea from an expression is not always clear, and can only be studied on a case-by-case basis. When the three basic requirements of fixation, originality and expression are met, the law provides a highly broad protection. Table 1 summarizes the range of copyrightable works.

Table 1. Main categories of copyrightable and not copyrightable items

Copyrightable	Not Copyrightable
• Literary works,	• Works that have not been fixed in a tangible form,
• Musical works (including any accompanying words),	• Titles, names, short phrases, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; mere listings of ingredients or contents,
• Dramatic works (including any accompanying music),	
• Pantomimes and choreographic works,	• Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices, as distinguished from a description, explanation, or illustration,
• Pictorial, graphic, and sculptural works,	
• Motion pictures and other audiovisual works,	
• Sound recordings,	• Works consisting entirely of information that is common property and containing no original authorship.
• Architectural works.	

It is interesting to note that copyright is secured as soon as the work is created by the author in some fixed form. No action, including publication and registration, is needed in the Copyright Office. "*Publication*" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. "*Registration*" is a legal process to create a public record of the basic facts of a particular copyright. Although neither publication nor registration is a requirement for protection, they provide certain advantages to the copyright owner.

The copyright law has different clauses for the protection of published and unpublished works. All unpublished works are subject to protection, regardless of the nationality or domicile of the author. The published works are protected if certain conditions are met regarding the type of work, citizenship, residency, and publication date and place.

International copyright laws do not exist for the protection of works throughout the entire world. The national laws of individual countries may include different measures to prevent unauthorized use of copyrighted works. Fortunately, many countries offer protection to foreign works under certain conditions through membership in international treaties and conventions. Two important international conventions are the Berne Convention and the Universal Copyright Convention[3].

A work created on or after January 1, 1978 is given copyright protection that endures seventy years after the author's death. If more than one author is involved in the creation, the term ends seventy years after the last surviving author's death. For works predating January 1, 1978, the duration of copyright depends on whether the work was published or registered by that date.

A law enacted by the US Congress in 1870 centralized the copyright system in the Library of Congress. Today, the US Copyright Office is a major service unit of the Library, providing services to the Congress and other institutions in the US and abroad. It administers the copyright law, creates and maintains public records, and serves as a resource to the domestic and international copyright communities. Table 2 shows some of the copyright milestones in the US for the last two centuries[5,6,7]:

Table 2. Notable dates in the US history of copyright

Date	Event
May 31, 1790	First copyright law, derived from the English copyright law (Statute of Anne) and common law, enacted under the new constitution.
April 29, 1802	Prints added to protected works.
February 3, 1831	First general revision of the copyright law.
August 18, 1856	Dramatic compositions added protected works.
March 3, 1865	Photographs added to protected works.
July 8, 1870	Second general revision of the copyright law.
January 6, 1897	Music protected against unauthorized public performance.
July 1, 1909	Third general revision of the copyright law.
August 24, 1912	Motion pictures, previously registered as photographs, added to classes of protected works.
July 30, 1947	Copyright law codified as Title 17 of the US Code.
October 19, 1976	Fourth general revision of the copyright law.
December 12, 1980	Copyright law amended regarding computer programs.
March 1, 1989	US joined the Berne Convention.
December 1, 1990	Copyright protection extended to architectural works.
October 28, 1992	Digital Audio Home recording Act required serial copy management systems in digital audio recorders.
October 28, 1998	The Digital Millennium Copyright Law (DCMA) was signed into law.

3. US COPYRIGHT INDUSTRIES

The primary domestic source of entertainment content is the US copyright industries[8] which produce and distribute materials protected by national and international copyright laws. The products include the following categories:

a. all types of computer software (including business applications and entertainment software);
b. motion pictures, TV programs, home videocassettes and DVDs;
c. music, records, audio cassettes, audio DVDs and CDs;
d. textbooks, tradebooks and other publications (both in print and electronic media).

Depending on the type of activity, the US copyright industries can be studied in two groups: "core" and "total." The core industries are those that create copyrighted works as their primary product. The total copyright industries include the core industries and portions of many other industries that create, distribute or depend upon copyrighted works. Examples are retail trade (with sales of video, audio, books and software) and the toy industry.

The International Intellectual Property Alliance (IIPA)[8] is a private sector coalition that represents the US copyright-based industries in bilateral and multilateral efforts to improve international protection of copyrighted materials. Formed in 1984, IIPA is composed of seven trade associations, each representing a different section of the US copyright industry. The activities of the member associations are summarized in Table 3.

Table 3. IIPA members

Member	Foundation Year	Type of member activity
AAP	1970	The Association of American Publishers (AAP) is the principal trade association of the book publishing industry. AAP members publish hardcover and paperback books in every field — fiction, general non-fiction, poetry, children's literature, textbooks, reference works, Bibles and other religious books, and scientific, medical, technical, professional and scholarly books and journals. AAP members also publish audio and video tapes, computer software, looseleaf services, electronic products and services including online databases, CD-ROM and a range of educational materials including classroom periodicals, maps, globes, filmstrips, and testing materials.
AFMA	1980	The American Film Marketing Association (AFMA) is a trade association whose members produce, distribute and license the international rights to independent English language films, TV programs and home videos. The American Film market (AFM), the largest international motion picture trade market, is sponsored and owned by AFMA.
BSA	1988	The Business Software Alliance (BSA) is an international organization representing leading software and e-commerce developers in 65 countries around the world. BSA educates computer users on software copyrights; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy.
IDSA	1994	The Interactive Digital Software Association (IDSA) is a U.S. association exclusively dedicated to serving the business and public affairs needs of companies that publish video and computer games for video game consoles, personal computers, and the Internet. IDSA offers services to interactive entertainment software publishers including a global anti-piracy program, the Electronic Entertainment Expo trade show, business and consumer research, government relations and guidance in privacy protection.
MPAA	1922	The Motion Picture Association of America (MPAA) and its international counterpart, the Motion Picture Association (MPA), serve as the voice and advocate of the American motion picture, home video and television industries, domestically through the MPAA and internationally through the MPA. Its members include Walt Disney Company, Sony Pictures Entertainment Inc., Metro-Goldwyn-Mayer Inc., Paramount Pictures Corp., Twentieth Century Fox Film Corp., Universal Studios Inc., and Warner Bros.
NMPA	1917	The National Music Publishers' Association (NMPA) is a trade association representing businesses that own, protect and administer copyrights in musical works. It is dedicated to the protection of music copyright across all media and across all national boundaries. The Harry Fox Agency, Inc. (HFA) was established in 1927 by NMPA to provide an information source, clearinghouse and monitoring service for licensing musical copyrights. The Agency licenses a large percentage of the uses of music in the United States on records, tapes, CDs and imported phonorecords. It also licenses music on a worldwide basis on behalf of its publisher principals for use in films, commercials, television programs, and all other types of audio-visual media.
RIAA	1952	The Recording Industry Association of America (RIAA) is the trade group that represents the U.S. recording industry. Its members create, manufacture and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States.

According to the figures published by the IIPA members and other trade associations, the US copyright industries continue to be one of the fastest growing segments of the US economy. The 1999 statistics in Table 4 provides an indication of the weight of the copyright industries in the US economy[9].

Table 4. The copyright industries in 1999

Factor	Core	Total
Estimated contribution to economy	$457.2 billion (4.94% of GDP)	$677.9 billion (7.33% of GDP)
Number of workers	4.3 million (3.24% of US workforce)	7.6 million (5.7% of US workforce)
Increase in value added to GDP between '77 & '99	360%	303%
Foreign sales and exports		
Industry	**Amount (in billions of US dollars)**	
Core copyright industries	$79.65	
Chemicals and Allied products	$67.74	
Electronic Components and Equipment	$63.76	
Aircraft and Aircraft Part Manufacturing	$60.75	
Motor vehicles and Automotive Parts and Accessories	$58.81	
Computers and Peripherals	$48.00	

Although the estimated growth of the copyright industries is impressive, other reports demonstrate huge losses due to the domestic and foreign piracy of copyrighted materials. The IIPA and its member associations work with both US and foreign government and private sector representatives to track copyright issues in over 80 countries. The data compiled for trade losses due to piracy between 1995 and 2000 is given in Table 5. These figures were taken from the annual "Special 301" reports which normally include 40-50 countries excluding Japan and Western Europe. The annual losses due to piracy of US copyrighted materials around the world are estimated to be $20-$22 billion[8].

Table 5. Estimated partial foreign trade losses due to piracy between 1995 and 2000 (in millions of US dollars)

Content / period	1995	1996	1997	1998	1999	2000
Motion pictures	1813.3	1735.0	1584.0	1406.5	1268.0	1242.5
Records & music	1087.1	1112.3	1331.8	1634.1	1723.5	1835.6
Business applications	4131.1	3905.9	3964.4	3307.1	2761.9	2490.9
Entertainment software	2880.6	3171.5	3249.2	2966.7	2906.8	1658.4
Books	678.0	695.2	669.6	633.2	685.4	675.1
TOTAL	**10590.1**	**10619.9**	**10799.0**	**9947.6**	**9345.6**	**7902.5**

In a recent study, the reliability of the figures attempting to measure the size of the economic impact of piracy was found questionable for two reasons[10]:

- The IIPA reports may imply that the copyrights industries' contribution to the GDP depends on copyright policy and protection measures, pointing to a need for greater levels of protection in the digital world. However, from an economics viewpoint, the specific relation between the level of protection and revenue of a business in the copyright industries is not clear.
- The accuracy of the estimates of the cost of piracy is problematic.

At any rate, there is real evidence of illegal copying, and we need to have a better understanding of its complex economic and social implications.

4. HOW IS CONTENT REPRESENTED

As entertainment content became available in high quality digital form for the professional market in the 1970s and 1980s, new digital packaged media formats were explored and developed to act as carriers for the digital content to the consumer market. Digital media promised not only higher quality for consumers and potentially lower manufacturing and distribution costs for content owners but also the potential for copyright owners to resell their library or catalog of products to the same customers in a new high quality format.

Computer software, including entertainment-oriented software, spawned the first wave of packaged digital media in the 1970s. The computer industry required a medium that would hold a few hundred kilobytes of data in a convenient, portable

format and magnetic media in the form of floppy discs met this requirement. In the 1970s, by far the largest market for entertainment content sold direct to the consumer was audio in the form of analog audiocassettes and vinyl albums. The home video market emerged in the late 1970s using analog VHS videocassettes and Laserdisc (the first optical disc digital storage format) that featured an analog FM video signal using.

It was not until the advent of the Compact Disc in 1982 that the music industry was presented with a digital medium that met all its future requirements for quality and cost. The same technology, in the form of CD-ROM, later became the content distribution medium that replaced floppy discs in the computer software market now dominated by the Personal Computer. Throughout the 1980s, home video grew into a market equal to home audio. It was not until the mid-1990s that a packaged digital distribution medium in the form of DVD-Video was developed to provide the home video industry with the potential benefits the CD offered the music industry. DVD-Video made optical media the leader in quality, cost and performance over all the magnetic media formats.

The 120mm polycarbonate disc in the form of CDs and DVDs has come to dominate digital content distribution as packaged media. The Compact Disc began supplanting all other distribution media it competed with in the mid-1980s, and now fifteen years later, the DVD is set to conquer the videocassette.

At this time, physical media used to distribute digital entertainment content is dominated by:

- Compact Disc
- DVD

Any successful media format requires support of content providers, consumer electronics manufacturers, media manufacturers and, of course, consumers. Launching a new digital format involves substantial risk and investment; new formats are typically supported when significant cost, performance and value benefits are visible for all parties. In the case of digital tape formats versus CD and DVD, no digital tape format has been developed or proposed which provides the perceived value and quality of CD and DVD to the consumer at a competitive manufacturing and retail cost for both hardware and software. Digital Tapes are inherently more costly to manufacture than a DVD, and the associated tape hardware cannot compete with the cost of manufacturing DVD drives. Coupled with this fact is the inherent reluctance of consumers to adopt new formats in the consumer electronics field; consumers have historically chosen standardized formats and supported them for many years. The strength of the CD, and now the DVD, in the consumer market suggests there is less opportunity to launch a successful Digital Tape format to compete.

Such has been the success of the CD and the DVD that other digital packaged media formats exist only in niche markets. These include:

- MiniDisc (optical disc, audio)
- Digital Tape (8mm, D-VHS)

4.1. Digitization and Compression

Before analog content (music or video) can be stored on physical media it must be converted to a digital representation. This process is generally referred to as "digitizing" or A/D conversion. It involves several principal steps including temporal sampling, quantization and binary encoding. The temporal sampling must be done at a high enough rate to satisfy the Nyquist sampling criterion so that content can be converted back to analog form (D/A conversion) without introducing aliasing errors. For audio, the sampling rate is usually 44,100 samples/second/channel (other sampling rates are used).

The "quantization and binary encoding" steps are the source coding steps that convert the signal into a binary representation. While binary representations do not perfectly reproduce the original content, it is customary to differentiate between "uncompressed" and "compressed" binary representations of the content. For example, audio content that is sampled at 44,100 samples/second/channel and then quantized to 20 or 24 bits is referred to as "uncompressed digital audio." Similarly, the CCIR 601 standard definition digital video standard is thought of as "uncompressed digital video".[1]

The problem with uncompressed content is that the data rate or the amount of space needed to store the content is too large for a given use or application. For example, uncompressed CCIR 601 video has a data rate that is larger than 160 Mb/s and

uncompressed digital audio has a data rate that is larger than 1.5 Mb/s. To reduce the data rate, the binary representation is changed by a process known as compression or source coding.[*] The compression scheme usually preprocesses the sampled data with a linear transform before it is quantized. Much work has been done in this area and the Discrete Cosine Transform (DCT) has had broad acceptance as the transform of choice. This is particularly true in the MPEG video compression standards[12] although newer approaches have been proposed[13] particularly in the new H.26L standard[14] and in the use of wavelets in JPEG-2000.[15] For audio, usually one combines the use of filter banks and the DCT to compress the content.[12]

After compression using MPEG-2, typical data rates for standard definition video are 2-8 Mb/s and for high definition video 12-20 Mb/s. For digital audio using MP3[16] the data rates are 96-384 Kb/s.

In recent years we have seen two new standards evolve for video compression: MPEG-4[17] and H.26X.[† 18] Initially, both of these standards were to address low bit rate video compression (data rates less than 64 Kb/s) that could not be handled by MPEG-1 or MPEG-2. H.26X are motion compensated block-based DCT methods that work extremely well in video streaming applications over wired and wireless networks. We are now starting to see H.26X used at higher data rates for encoding standard definition video. The new MPEG-4[17] standard has evolved into a set of techniques for compressing and representation of multimedia content. It allows individuals parts of a scene, for example objects in the scene such as people and the background, to be compressed and represented separately. These video objects can then be rendered independently when the video sequence is de-compressed. MPEG-4 is a very complicated standard with many parameters. In its "base" version, MPEG-4 is very much identical to H.263. Initial results show that at 0.8-2 Mb/s MPEG-4 and H.26X provides better quality video than MPEG-2. The performance gain is attributed to advanced coding options such as overlapped motion compensation and loop filters.[18] It is still too early to determine how MPEG-4 and H.26X will be used in consumer electronics applications. One interesting application, known as DivX[19] or Project Mayo, has been developed by the open-source community and uses a variant of MPEG-4 to transcode MPEG-2 DVD movies to DivX video. It is possible that by using the DivX encoder one can store a two hour movie on a CD-ROM with very good quality.

4.2. Digital Representation of Content on Physical Media

Presently, there are three main forms of entertainment content: audio, home video (movies) and computer software.

4.2.1. Audio

CD-Audio

Audio is recorded in either the analog or digital domain using professional recording equipment. Recording studios and mobile recording units typically have the capability to record up to 24 or 32 individual tracks. The recording system then creates a mix in the form of a 2-track master that is recorded either analog or digital on a professional tape format. These master studio tape recordings are then handed off to a post production unit to perform the (usually) digital engineering and mastering process. After being digitized at high definition sampling rates and quantization (e.g. 20- or 24-bit, 48 or 96 kHz), the sound is "engineered" to meet the artists' and producers' requirements. Mastering for CD involves preparing the recorded work to ensure optimum sound at the 16-bit quantization and 44.1kHz sampling rate inherent to the CD format. This requires down-converting from the digital sampling rate used in the mastering system to the native CD sampling rate.

Digital Audio Mastering has evolved to the point where most processing is performed on Digital Audio Workstations (DAWs). These items are relatively inexpensive computer workstations that give audio engineers a high level of control over their recorded program material. DAWs are usually PC-based or have recordable CD (CD-R) burners available to automatically create a CD output of the edited program. CD-R discs allow the recording engineers to qualify and approve their own work, and act as the input medium to the disc replication process.

DVD-Audio

The DVD Forum has recently specified the DVD-Audio format to co-exist with and compliment the DVD-Video format. Utilizing much of the same technology as DVD-video but requiring new combination DVD-Video/DVD-Audio players, hardware and software products started being offered in late 2000. DVD-Audio offers several features to the publisher

---

[*] Any method of converting an analog signal to a digital representation is source coding.
[†] In H.26X we include H.263, H.263+, and H.26L. These standards were developed by ISO.

including higher fidelity, multi-channel options, on-screen supplementary menus and video to accompany the audio program. DVD-Audio is intended to be the evolutionary successor to CD-Audio, offering better digital quality sound and the same consumer-friendly features found on DVD-Video.

DVD-Audio titles are engineered and mastered from the same master recordings as CD-Audio. However, the engineering and mastering processes create five or six discrete channels for surround mixes from up-to-48 channel master recordings. The sampling rate and quantization are also enhanced up to 96 kHz and 24-bits, respectively. The authoring of the DVD-Audio title from the digital audio streams follows a similar procedure to DVD-Video titles.

4.2.2. Home Video (DVD-Video)

Motion pictures are captured using film or video. Cameras work primarily in the analog domain recording directly to film or magnetic tape (video). Digital camera technology for recording movies is beginning to emerge with notable movie releases expected in 2001 and 2002. Whatever the source for the motion pictures, the digital carrier, DVD-Video, determines the requirements for the video and audio streams necessary to make the final disc. The DVD-Video specifies MPEG2 video with either uncompressed PCM audio (rare) or compressed 2- or multi-channel Dolby Digital audio. The DVD-Video format further allows additional compressed audio streams such as Digital Theater Systems (DTS) to accompany the specified audio streams.

DVD-Video titles are authored from compressed video and audio streams. Post-production houses serving the motion picture industry are employed by the studios to take the original master film format and create MPEG2 video and Dolby Digital audio streams used as inputs to the DVD-Video disc authoring process. DVD-Video uses the concept of variable bit-rate (VBR) in which the degree of digital compression can be varied to optimize data storage space. Custom VBR MPEG2 compression systems have been developed to compress source material from analog or digital video tape masters into usable DVD MPEG2 streams. Similarly, DAWs have been developed to create DVD-ready Dolby Digital audio streams.

The DVD-Video authoring system is a custom workstation designed to combine the various video, audio and still image "assets" that make up a DVD-Video project into a single digital image that satisfies the DVD-Video specification issued by the DVD Forum. The authoring systems create the navigation and menu features around the video and audio assets, and output digital tape masters on Digital Linear Tape (DLT) that are used as input media to the disc replication facility.

4.2.3. Computer Software

Computer software intended for mass-distribution on CD-ROM is developed on PC-based systems and the content providers similarly produce their own "one-off" CD-R discs which act as internal test and qualification masters and as input media to the disc replication.

4.3. Disc Mastering, Replication and Packaging

Pre-recorded CDs and DVDs are produced in disc replication facilities. Content providers typically provide the facilities with the following:

- Digital master data (input media)
- Graphics files for printed labels on disc
- Print collateral for the packaging

Given these three items, the disc replication facility produces a fully packaged item that can be shipped direct-to-retail, direct-to-warehouse or direct-to-consumer. The disc production process consists of three discrete operations:

i. Mastering
ii. Replication
iii. Packaging and Fulfillment

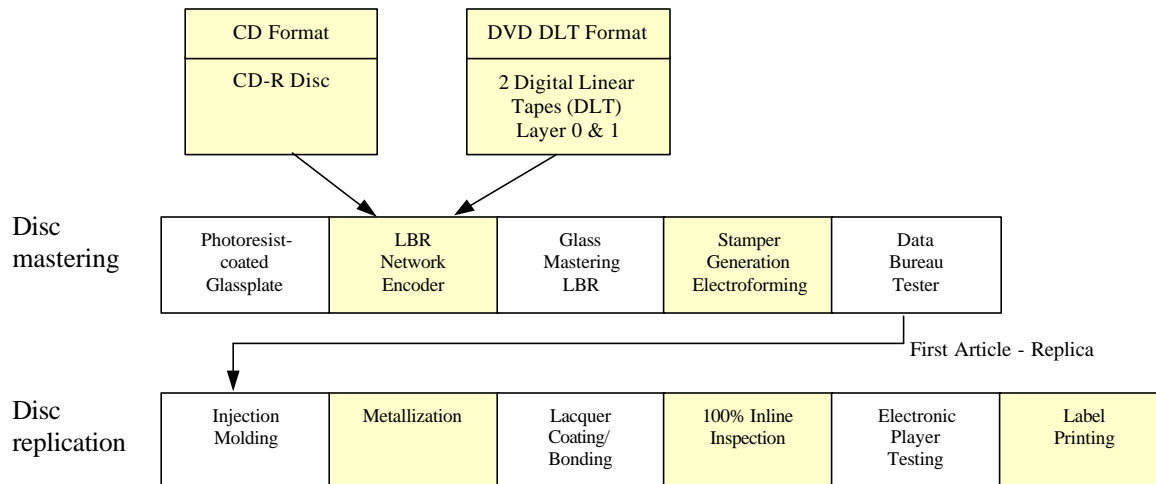The details of mastering and replication are shown in Figure 1.

Figure 1. CD and DVD Manufacturing Process Block Diagram

4.3.1. Disc Mastering

Polycarbonate CDs and DVDs are injection molded from a mold cavity insert called a "stamper." The end product of the mastering process, a stamper is a facsimile of a compact disc that exists as a thin nickel plate encoded with the CD or DVD data features.

The Disc Mastering process is the stage at which the content provider's data is recorded onto the familiar 120mm round disc format. The input media supplied by the content provider is typically uploaded to a mastering computer network allowing the data to be accessed by a Laser Beam Recorder (LBR). The LBR records the customer data onto a large glass plate coated with a photo sensitive material known as photoresist. A laser beam is then focused on the glass plate as it revolves on the LBR, and a data formatter modulates the beam to expose discrete pits or features along a spiral path. In keeping with other photolithographic processes, the features are etched to produce the image of a compact disc within the photoresist coating on the glass. The resulting glass master is subsequently coated with a thin film of nickel and passed to a traditional electroforming process: the disc image is transferred to a nickel part which can be used to form a family of negative and double-negative images in a nickel plating solution thereby duplicating the image of the disc in discrete nickel discs or stampers. The nickel discs are mechanically punched to ensure precise fit in an injection-molding machine for mass replication; literally, the making of replicas of the stamper image.

An important consideration in CD Mastering is that every CD serves as its own master image from which perfect digital copies can be made by consumers and professionals alike. Any disc available at retail can be used as a master image for legal (or *illegal!*) replication at a disc manufacturing facility. This is not possible for DVD-Video or DVD-Audio where the title is encrypted with a proprietary algorithm. The licensing of the related technology prohibits the secure disc keys from being accessed by a playback device and thereby transferred to a disc copy.

4.3.2. Disc Replication

CDs and DVDs are mass-replicated using polycarbonate injection molding machines. Stampers encoded with the customer data are mounted in the injection molding machines which typically produce a replica disc every 4 seconds. The clear polycarbonate discs are subsequently coated with a thin film of aluminum and hard-coated with a protective layer of acrylic lacquer. In the case of DVDs, two discs of half CD thickness are produced simultaneously and later bonded together with a hard coat lacquer.

Approximately 1 disc in 1000 is tested electronically on a player-based test system. The remaining discs are 100% tested physically and mechanically by vision systems. The disc replication processes are typically conducted inline by automating and integrating four processes; molding, metallizing, coating/bonding and inspection. The disc is finished by applying a printed label using UV inks in a screen-printing or offset-printing process.

Replicated discs are collected on spindles of 100-200 discs for packaging and order fulfillment to retail stores, warehouses or direct to consumer. Various automated equipment enables high-speed packaging of media into retail distribution packages. A large facility may have a capacity of 500,000 DVD and/or CD discs per day; facilities with outputs as small as 30,000 discs per day also service niche markets.

Many retailers require custom packaging services such as regional price stickers, promotional marking, and unique packing such as point-of-sale displays. These types of services do not lend themselves to automation due to the dynamic requirement and therefore add cost and decrease manufacturing throughput.

4.4. Fulfillment and Distribution Mechanisms

Digital Tapes

Digital Tapes are not widely used for the distribution of entertainment content. Small niche markets exist for certain semi-professional applications such as 8mm tapes used for airline movie distribution. Duplicated on a small scale at tape duplication facilities, these tapes are usually shipped direct-to-client and not to retail or consumer.

CDs and DVDs

CDs and DVDs are distributed through traditional distribution networks for direct-to-retail, direct-to-warehouse or direct-to-consumer markets. There are roughly one hundred CD replication facilities in North America, a quarter of which also offering DVD replication services. Typically, disc replication plants will ship fully packaged media to distribution centers employed by the content provider or retailer.

Large CD and DVD releases can total in the millions of disc units. The distribution centers are very large order fulfillment centers located at geographically advantageous locations to best service the retail industry. These are able to warehouse and stage a broad variety of stock keeping units (SKUs) for immediate picking, packing, and shipment via parcel, truck and air carriers. Content providers work with retailers to forecast demand for their products and place initial orders for the release of new titles that are then scheduled for replication and distribution to meet a desired street date. Immediate product shortages are replenished through the distribution network while system-wide replenishment orders are placed at the disc replication plant.

As the demand for individual titles weakens, retailers are typically allowed to return unsold product to a returns-processing center associated with a distribution center. These products are often warehoused or reworked, and then marketed through alternate channels.

As manufacturing and retailing models evolve, advances in technology enable efficiencies in the supply chain. Capture of point-of-sale data lets retailers pass sales data back through the distribution and manufacturing processes, thus affecting replenishment of finished goods and ordering of raw materials. Such efficiencies avoid stock-outs, leverage buying opportunities, and reduce overall costs.

4.5. Security in Replication, Distribution and Retail

Security within the replication facilities is of paramount importance to the content providers' business model. Large replication facilities produce media on a daily basis with a street value of many millions of dollars. Prevention of new products from "leaking out" to market before their release date and theft of products within the manufacturing and distribution chain is a major security challenge. The leading disc replication facilities feature sealed buildings with magnetic and physical body searches to prevent media leaving via employees; 24-hour camera surveillance of disc manufacturing areas is standard. Similarly, warehousing and distribution facilities control movement of products through guarded, monitored exits.

Media is typically transported by surface carriers. The high retail value of the media coupled with its small size means that a single tractor-trailer load of digital media might have a street value of over $1 million. Truck shipments of media are typically tracked by GPS, and content providers choose entrusted freight carriers.

The responsibility for security of the digital media eventually passes to the retailer. As the products lost or stolen at retail is at the retailer's cost, physical measures are taken to prevent pilferage. Shipping containers with minimal markings and retail boxes are designed to maximize in-store security. A typical retail package for a CD or DVD may contain any or all of the following physical security devices aimed at protecting the content from counterfeiting and theft:

- Electro-magnetic sensors glued inside the box (e.g. Sensormatic™)
- Shrink-wrap
- Holographic security stickers
- Side-spine and top-spine tamper-proof stickers
- Tamper-proof "clamshells" designed to encase the unit

Recently we have seen the use of digital watermarking techniques[20] to protect the package material from forgery.[21] A fragile watermark is embedded in the packaging material that is easily damaged or destroyed if the material is duplicated. Hence the package is labeled as a forgery or tampered if the watermark is missing.

All the above add cost and complexity to the retail packaging of digital media but are considered essential to maintaining the security of the product.

5. CONDITIONAL ACCESS AND DIGITAL RIGHTS MANAGEMENT

In an end-to-end protection system, a fundamental problem is to determine whether the consumer is authorized to access the requested content. The traditional concept of controlling physical access to places (e.g., cities, buildings, rooms, highways) has been extended to the digital world in order to deal with information in binary form. A familiar example is the access control mechanism used in computer operating systems to manage data, programs and other system resources. Such systems can be effective in "bounded" communities[7] (e.g., a corporation or a college campus) where the emphasis is placed on the original access to information rather than how the information is used once it is in the possession of the user. In contrast, the conditional access systems for digital entertainment content in "open" communities need to provide reliable services for long periods of time (up to several decades) and be capable of controlling the use of content after access.

We will look at two approaches for restricting access to content. The first approach has been used by the satellite/terrestrial broadcasters and cable operators in the last few decades (for both analog and digital content). The second approach has been adopted by the developers of emerging technologies for protecting Internet content.

5.1. Conditional Access Systems

A conditional access (CA) system[22,23,24,25,26,27,28,29,30] allows access to services based on payment or other requirements such as identification, authorization, authentication, registration or a combination of these. Using satellite, terrestrial or cable transmissions, the service providers deliver different types of multimedia content ranging from free access programs to services such as PayTV, Pay-Per-View and Video-on-Demand.

CA systems are developed by companies, commonly called the CA providers, that specialize in the protection of A/V signals and secure processing environments. A typical architecture of a CA system and its major components are shown in Figure 2. The common activities in this general model are:

1. Digital content (called an "event" or a "program") is compressed to minimize bandwidth requirements. MPEG2 is a well-known industry standard for coding A/V streams. Other MPEG variations (MPEG4, MPEG7 and MPEG21) are being considered for new applications.
2. The program is sent to the CA head-end to be protected and packaged with entitlements indicating the access conditions.

3. The A/V stream is scrambled[*] and multiplexed with the entitlement messages. There are two types of entitlement messages[31] associated with each program: The Entitlement Control Messages (ECMs) carry the decryption keys (called the "control words") and a short description of the program (number, title, date, time, price, rating, etc.) while the Entitlement Management Messages (EMMs) specify the authorization levels related to services. In most CA systems, the EMMs can also be sent via other means such as telephone networks. The services are usually encrypted using a symmetric cipher such as the Data Encryption Standard (DES) or any other public domain or private algorithm. The lifetime and the length of the scrambling keys are two important system parameters. For security reasons, the protection of the ECMs is often privately defined by the CA providers, but public-key cryptography and one-way functions are useful tools for secure key delivery.

4. If the customer has received authorization to watch the protected program, the A/V stream is descrambled by the receiver (also called a "decoder"), and sent to the display unit for viewing. A removable security module (e.g., a smartcard) provides a safe environment for the processing of ECMs, EMMs and other sensitive functions such as user authorization and temporary storage of purchase records.

5. The back office is an essential component of every CA system, handling billings and payments, transmission of EMMs, and interactive TV applications. A one-to-one link is established between the back office and the decoder (or the removable security module, if it exists) using a "return channel," which is basically a telephone connection via a modem. As with other details of the CA system, the security of this channel may be privately defined by the CA providers. At certain times, the back office collects the purchase history and other usage information for processing.

6. Authorizations (e.g., EMMs) and other messages (system and security updates, etc.) are delivered to the customer's receiver.

7. Payments and usage information are sent to the appropriate parties (content providers, service operators, CA providers, etc.).

---

[*] In the context of CA systems, *scrambling* is the process of content encryption. This term is inherited from the analog protection systems where the analog video was manipulated using methods such as line shuffling. It is now being used to distinguish the process from the protection of *descrambling* keys.
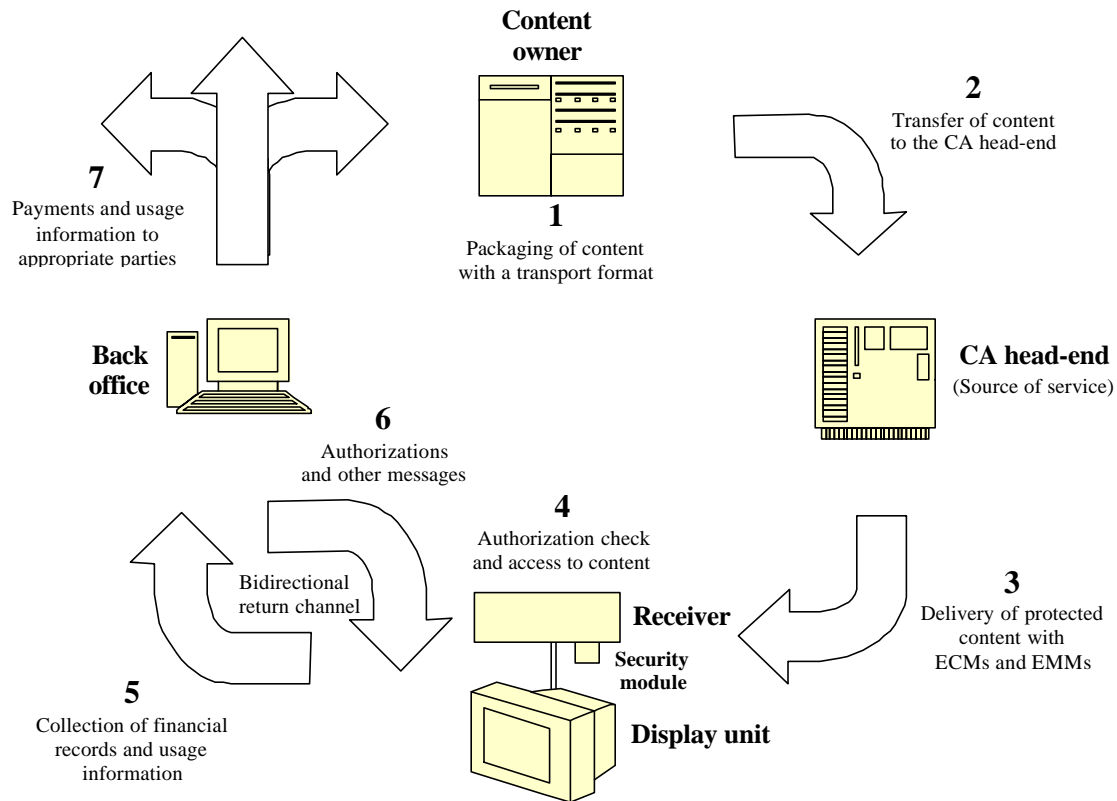
Figure 2. CA system architecture

In today's CA systems, the security module is assigned the critical task of recovering the descramling keys. These keys are then passed to the receiver for decrypting the A/V streams. The workload is therefore shared between the security module and its host. More recently, two separate standards have evolved to remove all the security functionality from navigation devices. In the US, the National Renewable Security Standard (NRSS)[32] defines a renewable and replaceable security element for use in consumer electronics devices such as digital set-top boxes and digital TVs. In Europe, the Digital Video Broadcasting (DVB)[33] project has specified a standard for a common interface (CI) between a host device and a security module.

The CA systems currently in operation support several purchase methods including subscription, pay-per-view and impulsive pay-per-view. Other models are also being considered to provide more user convenience and to facilitate payments. One such model uses pre-paid "cash cards" to store credits which may be obtained from authorized dealers or ATM-like machines.

Note that the model described in Figure 2 has been traditionally used to provide conditional access for viewing purposes. Recording control depends on the type of the signal output from the receiver. If the device has NTSC, PAL or SECAM output (which is the case for almost all devices in the field today), protection can be provided by a Macrovision[34] system which modifies the video in such a way it that it does not appreciably distort the display quality of the video but results in noticeable degradation in recording. For higher definition analog or digital outputs, however, the model is drastically changing, requiring solutions that are more complex and relatively more expensive.

The Digital Video Broadcasting (DVB) organization, a consortium of companies for establishing common international standards for digital broadcasting, has envisaged two basic CA approaches: "Simulcrypt" and "Multicrypt.[27, 35]"

- *Simulcrypt*: Each program is transmitted with the entitlement messages for multiple CA systems, enabling different CA decoders to receive and correctly descramble the program.

- *Multicrypt*: Each decoder is built with a common interface for multiple CA systems. Security modules from different CA system operators can be plugged into different slots in the same decoder to allow switching between CA systems.

These architectures can be used for satellite, cable, and terrestrial transmission of digital television. The Advanced Television Systems Committee (ATSC)[36] has recently adopted the Simulcrypt approach.

5.2. Digital Rights Management Systems

Digital Rights Management (DRM) refers to the protection, distribution, modification and enforcement of the rights associated with the use of digital content. In general, the primary responsibilities of a DRM system are:

- secure delivery of content to users,
- prevention of unauthorized access,
- enforcement of usage rules, and
- monitoring of the use of content.

Although such systems can, in principle, be deployed for any type of distribution media, the present discussions weigh more heavily on the Internet.

The unprecedented explosion of the Internet has opened potentially limitless distribution channels for the electronic commerce of content. Selling goods directly to consumers over an open and public network, without the presence of a clerk at the point of sale, has significant advantages. It allows the businesses to expand their market reach, reduce operating costs, and enhance customer satisfaction by offering personalized experience. While inspiring new business opportunities, this electronic delivery model raises challenging questions about the traditional models of ownership. The lessons learned from the MP3 phenomenon, combined with the lack of reliable payment mechanisms, have shown the need for protecting the ownership rights of copyrighted digital material.

A DRM system uses cryptography (symmetric key ciphers, public-key ciphers and digital signatures) as the centerpiece for security related functions, which generally include secure delivery of content, secure delivery of the content key and the usage rights, and client authentication.

Figure 3 shows the fundamentals of an electronic delivery system with DRM: A publisher, a server (streaming or Web), a client device and a financial clearing house. Although details may vary among DRM systems, the following steps summarize typical activities in a DRM-supported e-commerce system:

1. The publisher packages the media file (i.e., the content) and encrypts it with a symmetric cipher. The package may include information about the content provider, retailer or the Web address to contact for the rights.
2. The protected media file is placed on a server for download or streaming. It can be located with a search engine using the proper content index.
3. The customer requests the media file from the server.
4. The file is sent after the client device is authenticated. The customer may also be required to complete a purchase transaction. Authentication based on public key certificates is commonly used for this purpose. Depending on the DRM system, the usage rules and the key to unlock the file may either be attached to the file or need to be separately obtained (e.g., in the form of a license) from the clearing house or any other registration server. The attachment or the license are protected in such a way that only the client is able to retrieve the information. Public key ciphers are appropriately used here.
5. The customer purchases the content, and uses it according to the rights and rules.
6. At certain times, the clearing house collects financial records and usage information from the clients.
7. Payment confirmation and other messages (system and security updates, etc.) are delivered to the client.
8. Payments and usage information are sent to the appropriate parties (content providers, publishers, distributors, authors, artists, etc.).
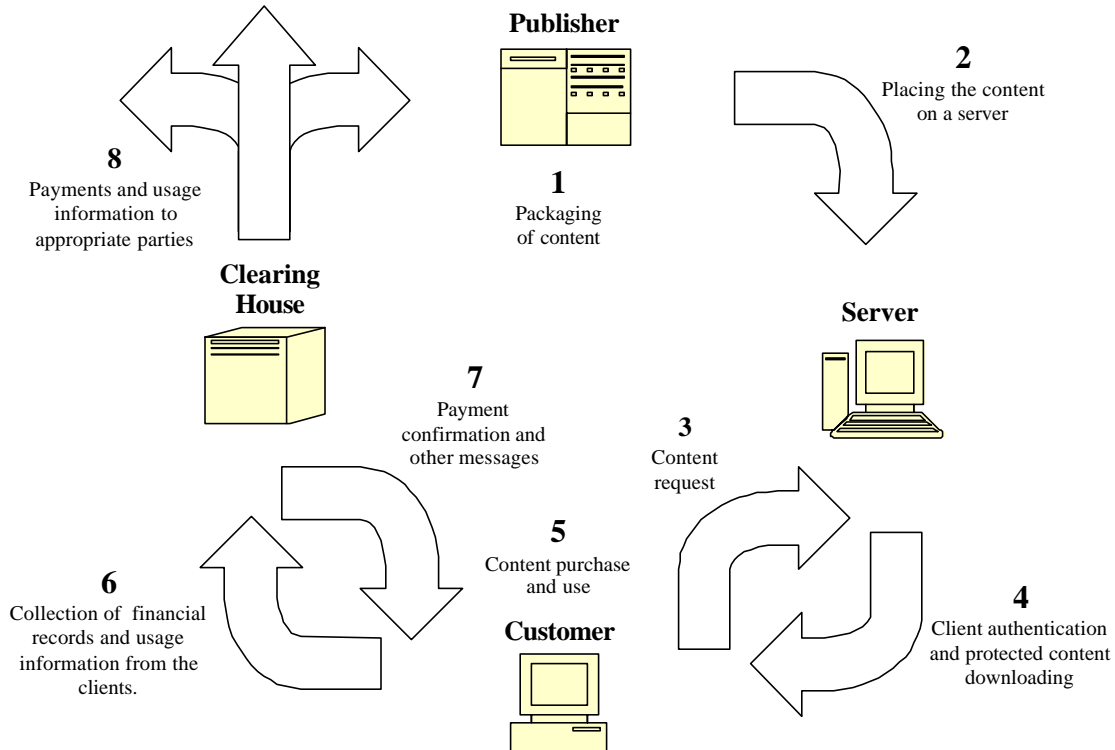
Figure 3. Electronic e-commerce with DRM

Renewability is achieved by upgrading DRM system components and preventing the compromised devices from receiving content. New security software may be released as a regular enhancement or in response to a threat or hack. Revocation lists allow the servers to refuse service to revoked clients (multimedia applications software can also be revoked if it can be authenticated by the DRM component that resides in the client).

DRM enables the content owners to specify their own business models in managing the use of content. A wide range of sales models can be supported, including subscription, pay-per-use, and superdistribution. Time-limited reading of an e-book, multiple viewings of a movie, transfer of a song to a portable music player are all possible scenarios.

Superdistribution is a relatively new concept for re-distributing content across the Internet. It is a process that allows the consumers to forward a content that they have acquired to other consumers (friends, relatives and associates) in the market. The content forwarded to a potential buyer cannot be accessed until the new rights are obtained. This approach has important advantages and drawbacks:

1. It is an efficient way of using a DRM-supported e-commerce system since repeated content downloads are avoided.
2. From an economic point of view, superdistribution may help widen the market penetration. Once a particular content is downloaded to a client, the customer, with sufficient encouragement, can act as an agent of the retailer with minimal effort and cost.
3. From a security point of view, if the content, encrypted with a particular key, becomes available in the market in large quantities, it may increase the likelihood of the key being compromised. For increased security, different copies of a media file need to be encrypted with different keys. This, of course, requires new downloads from the server.

5.3. The Efforts of MPEG

5.3.1. MPEG-7

As more and more content becomes available, there is a need for indexing or a description as to what is in the material and how it is represented. This has been addressed by MPEG and has involved into the MPEG-7 standard. MPEG-7, formally named "Multimedia Content Description Interface," *"aims to create a standard for describing the multimedia content data that will support some degree of interpretation of the information's meaning, which can be passed onto, or accessed by, a device or a computer code. MPEG-7 is not aimed at any one application in particular; rather, the elements that MPEG-7 standardises shall support as broad a range of applications as possible.*[37]*"* MPEG-7 provides a set of descriptors that can be used to describe content; it does not include tools or methods for extracting the content or its meaning. Some of the MPEG-7 descriptors are very simple (for example color descriptors) whereas description schemes specify the structure and semantics of the relationships between simple descriptors[38]. MPEG-7 will use the XML Schema[39] as its "Description Definition Language" to represent the descriptors and description schemes.

One interesting application of content description is the TV Anytime[40] Forum which is developing specifications to enable audio-visual and other services based on mass-market high volume digital storage in consumer electronics applications. The objectives of the Forum are to enable the ability "to search, select, acquire and rightfully utilize material on a local storage device from both broadcast and on-line sources" and "to transfer material between local storage devices using home networks and exchangeable media, and to 'micro-navigate' around rich content." These goals require that the content descriptions are available. TV Anytime has agreed to "harmonize" its descriptors and description schemes with MPEG-7. TV Anytime is also addressing the problem of rights management and protection of both the content and its description.[41] In fact, one could treat the "rights management" information as another content descriptor.*MPEG IPMP and MPEG-21*

In recent years, MPEG has began to address the problem of how to manage intellectual property rights in the development of the MPEG-4 IPMP (Intellectual Property Management Protocol)[42] and MPEG-21.[43] MPEG is moving from defining hooks to proprietary systems (ECMs and EMMs in MPEG-2) to a more encompassing standardization in rights management and protection. Presently, MPEG is examining:

1. Identification of content
2. Automated monitoring and tracking of creations
3. Prevention of illegal copying
4. Tracking object manipulation and modification history
5. Supporting transactions between Users Media Distributors and Rights Holders

The intention is to look at the issue from all sides, and take into account the requirements from authors, broadcasters, collection societies, consumers, creation providers, creators, rights management agencies, media companies, media distributors, performers, producers, publishers, retailers, rights holders, telecom companies and trusted third parties. Everything from watermarking to complete DRM systems has been proposed. It is expected that IPMP protocol will go through several refinement processes in MPEG-21.

5.4. Streaming Content

Video or audio streaming, or the real-time delivery of content over a wired or wireless data network, is the underlying technology behind many applications including video-on-demand and the delivery of educational and entertainment content. In many applications, particularly those involving entertainment content, security issues such as conditional access and copy protection must be addressed.[44] To resolve these security issues, techniques that include encryption and watermarking need to be developed. Since the content (particular the video) will often be compressed using a scalable compression technique and transported over a lossy packet network using the Internet Protocol (IP), the security measures must not only be compatible with the compression technique and data transport but be robust to errors as well. The underlying problems here are that a user may not receive the entire stream due to errors, the network transport (e.g. IP Multicast), or scalable compression (e.g. if MPEG-4 FGS[45] is used). Some of the issues can be resolved by developing error resilient security techniques (encryption and watermarking) and protocols (beyond the DRM protocols now being used).[46]

A fundamental problem in content streaming is that the network errors can cause the bit stream to be de-synchronized from the receiver. This introduces serious problems for encryption and watermarking:

- In the case of block encryption, any losses in the ciphertext will result in the sequence not being properly decrypted. The use of stream ciphers eliminates this problem but synchronization still needs to be maintained. Even if these problems are addressed, the receiver may still not "see" the entire bit stream by design because scalable compression may have been used. Here the receiver only receives or uses the part of the bit stream that it needs.

- A similar problem exists with watermarking where the receiver must process the bit stream to extract the watermark. If part of the bit stream is missing, then the watermark detector will be de-synchronized and may not be able to detect the presence of the watermark.

Designing a DRM system for streaming content is very daunting and much different than systems that are used in less noisy environments.

6. COPY PROTECTION IN HOME NETWORKS

The digital home network is the last stop in the "journey" of entertainment content. After an introduction of the architecture, we will review the approaches and solutions developed for protection.

A digital home network (DHN) is a cluster of digital audio/visual (A/V) devices including set-top boxes, TVs, VCRs, DVD players, and general-purpose computing devices such as personal computers.[47] Figure 4 shows a typical digital home network with several sources of content feeding the A/V devices.
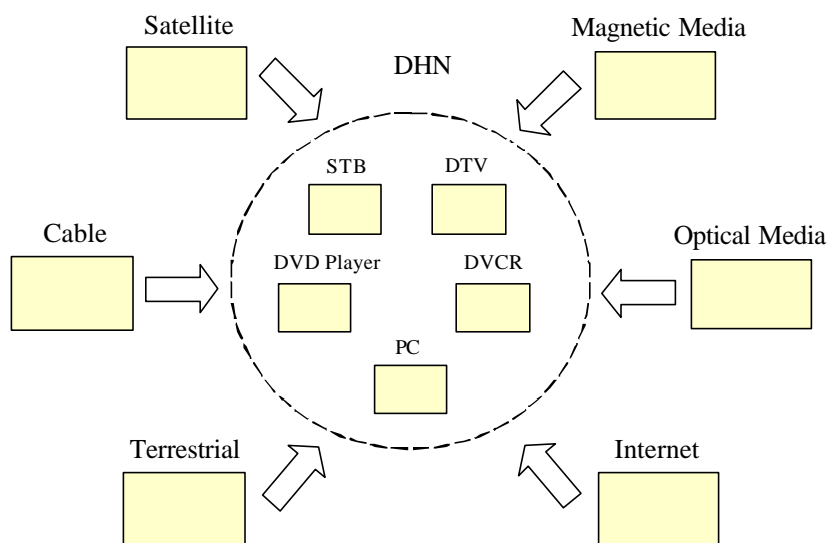

Figure 4. A digital home network with its content sources

The problem of content protection in home networks has the following dimensions:

- Protection of content across digital interfaces
- Protection of content on storage media, and
- Management of rights associated with content.

This problem, it is believed, turns out to be the most difficult problem to solve for a number of technical, legal and economic reasons:

1. Private CA systems are, by definition, proprietary, and can be defined and operated using the strictest possible security means and methods. In comparison, the protection systems needed for the devices and interfaces in home networks have to be developed with a consensus among the stakeholders, making the determination of requirements very difficult.

2. Renewability of a protection system needs to be properly defined and implemented. Important parameters are the cost, user convenience and liabilities resulting from copyright infringements.
3. The new copyright legislation introduces controversial prohibitions subject to different interpretations.
4. The payer of the bill for the cost of protection in home networks is unclear. Several business models are under consideration.

6.1. Technical Solutions

Two groups of technologies are believed to be useful in designing technical solutions: Encryption-based and watermark-based. The potential value of these technologies has been the subject of endless, and sometimes fruitless, discussions in the last decade. As each group presents strengths and weaknesses, some are of the opinion that both types of solutions should be implemented to increase the robustness to possible attacks.

Encryption and watermarking each provide a different "line of defense" in protecting content. The former makes the content unintelligible through a reversible mathematical transformation based on a key whereas the latter inserts data directly into the content. In the digital domain, the value of watermarking appears to be incremental since the fall of the first line of defense (encryption) would make the content totally vulnerable. It is therefore argued that watermarking is indispensable as it is the only surviving protection mechanism when the digital content is transformed to analog form.

The technical solutions developed in the last five years are listed in Table 6. All are encryption-based systems although watermarking is still being considered as a complimentary technology. Because of a number of technical and legal reasons, the selection of a watermark-based system has not yet been finalized.

Table 6. Content protection solutions for digital home networks

Solution	What is protected?	Brief description
CSS[48]	Video on DVD-ROM	CSS-protected video is decrypted during playback on the DVD player or drive.
CPPM [49]	Audio on DVD-ROM	CPPM-protected audio is decrypted during playback on the DVD player or drive.
DTCP[50]	IEEE 1394 serial bus	The source device and the sink device authenticate each other, and establish shared secrets. A/V content is encrypted across the interface. The encryption key is renewed periodically.
CPRM[27]	Video or audio on DVD-R/RW/RAM	A/V content is re-encrypted before recording on a DVD recordable disc. During playback, the player derives the decryption key.
HDCP[51]	Digital Visual Interface (DVI)	Video transmitter authenticates the receiver and establishes shared secrets with it. A/V content is encrypted across the interface. The encryption key is renewed frequently.

In the CSS system, each manufacturer is assigned a distinct master key. If a particular master is key compromised, it is replaced by a key which is used in the subsequent manufacturing of DVD players. With the new key assignment, future releases of DVDs cannot be played on the players manufactured with the compromised key. The CSS system was hacked in 1999 because a company neglected to protect its master key during the software implementation for a DVD drive. In the rest of the protection systems, renewability is defined as device revocation. Updated versions of the revocation lists are distributed on new prerecorded media or through external connections (Internet, cable, satellite, and terrestrial).

Each solution in Table 6 defines a means of associating the Copy Control Information (CCI) with the digital content it protects. The CCI communicates the conditions under which a consumer is authorized to make a copy. An important subset of CCI is the two Copy Generation Management System (CGMS) bits for digital copy control: "11" (copy-never), "10" (copy-once), "01" (no-more-copies), and "00" (copy-free).

A CPRM-compliant recording device refuses the make a copy of content labeled as "copy-never" or "no-more-copies." It is authorized to create a copy of "copy-once" content, and label the new copy as "no-more-copies." The DTCP carries the CGMS bits in the isochronous packet header defined by the interface specification. A sink device that receives content from

a DTCP-protected interface is obliged to check the CGMS bits, and respond accordingly. As the DVI is an interface between a content source and a display device, no CCI transmission is involved.

In addition to those listed in Table 6, private DRM systems may also be considered to be content protection solutions in home networks. However, interoperability of devices supporting different DRM systems is an unresolved issue today.

Other efforts of security in home network environments are worth mentioning here. Two significant projects have recently been initiated within the VHN and UPnP working groups. The Video Electronics Standards Association (VESA)[52] is the international non-profit organization that develops and supports industry-wide display and display interface standards for the electronics marketplace. The Universal Plug and Play (UPnP)[53] Forum is an industry initiative designed to enable easy and robust connectivity among stand-alone devices and PCs from many different vendors. Having completed their specifications for a network architecture, both groups are now focusing on security issues such as authentication, data integrity and confidentiality.

6.2. Legal solutions

The legal means of protecting copyrighted digital content can be classified into two categories:

- National laws (copyright laws and contract laws), and
- International treaties and conventions

The most important legislative development in the recent years was the Digital Millennium Copyright Act. Signed into a law on October 28, 1998, this Act implements two 1996 World Intellectual Property Organization (WIPO) treaties – the WIPO Copyright Treaty and the WIPO performances and Phonograms Treaty. Each of these treaties obligate the member states (1) to prevent circumvention of technological measures used to protect copyrighted works, and (2) to prevent tampering with the integrity of copyright management information.

Section 103 of the DMCA amends Title 17 of the US Code by adding a new chapter 12. Section 1201 makes it illegal to circumvent technological measures that prevent unauthorized access and copying, and Section 1202 introduces prohibitions to ensure the integrity of copyright management information. The DCMA has received earnest criticism with regard to the ambiguity and inconsistency in expressing the anticircumvention provisions[10],[54].

In every country, legally binding agreements between parties would also be effective in copyright protection. All technological measures, without any exception, must include intellectual property (mostly protected by patents) to be licensable. Before a particular technology is implemented in A/V devices, the licensee signs an agreement with the owner of the technology agreeing with the terms and conditions of the license. Contract laws deal with the violations of the license agreements in the event of litigations.

The international treaties that have been signed for the worldwide protection of copyrighted works include:[1],[55]

- The Berne Convention, formally the International Convention For The Protection Of Literary And Artistic Works (1886).
- The Universal Copyright Convention (1952).
- Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (1961).
- Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms (1971).
- Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite (1974).
- TRIPS Agreement (1995).

6.3. Business solutions

In addition to technical and legal means, owners of digital entertainment content can also make use of new, creative ways to bring their works to the market. A good understanding of the complexity and cost of protection is probably a prerequisite to be on the right track. With the wide availability of digital A/V devices and networks in the near future, it will become

increasingly difficult to control individual behavior and detect infringements of copyright. Would it then be possible to develop business models that are not closely tied to the inherent qualities of digital content? The current business models,[10] old and new, for selling copyrighted works are summarized in Table 7.

Table 7. Business Models for Copyrighted Works

TRADITIONAL		
Type	**Examples**	**Relevance to copyright protection**
Models based on fees		
Single transaction purchase	Books, videos, CDs, photocopies	High sensitivity to unauthorized use.
Subscription purchase	Newsletter and journal subscriptions	
Single transaction license	Software	
Serial transaction license	Electronic subscription to a single title	
Site license	Software for a whole company	
Payment per electronic use	Information resource paid per article	
Models relying on advertising		
Combined subscription and advertising	Web sites for newspapers	Low sensitivity to unauthorized access. Concern for reproduction and framing.
Advertising only	Web sites	
Models with free distribution		
Free distribution	Scholarly papers on preprint servers	Low concern for reproduction. Sensitivity for information integrity.
Free samples	Demo version of a software	
Free goods with purchases	Free browser software to on an income-producing Web site	
Information in the public domain	Standards, regulations	
RECENT		
Give away the product and sell an auxiliary product or service	Free distribution of music because it enhances the market for concerts, t-shirts, posters, etc.	Services or products not subject to replication difficulties of the digital content.
Give away the product and sell upgrades	Antivirus software	Products have short shelf life.
Extreme customization of the product	Personalized CDs	No demand from others.
Provide a large product in small pieces	Online databases	Difficulty in copying.
Give away content to increase the demand for the actual product	Full text of a book online to increase demand for hard copies	Need for protecting the actual product sold.
Give away one piece of content to create a market for another	Adobe's Acrobat Reader	
Allow free distribution of the product but request payment	Shareware	Cost of buying converges with cost of stealing.
Position the product for low-priced, mass market distribution	Microsoft 98	

Most, if not all, of these models are relevant for the marketing of digital entertainment content. In general, the selection of a business model depends on a number of factors including:

- type of content,
- duration of the economic value of content,
- fixation method,
- distribution channel,
- purchase mechanism,
- technology available for protection, and
- extent of related legislation.

A good case study to explore the opportunities in a digital market is superdistribution. Figure 5 shows the players in a DRM-supported e-commerce system: A content owner, a clearing house, several retailers and many customers. Let's suppose the media files requested by the customers are hosted by the content owner or the retailers, and the licenses are downloaded from the clearing house.
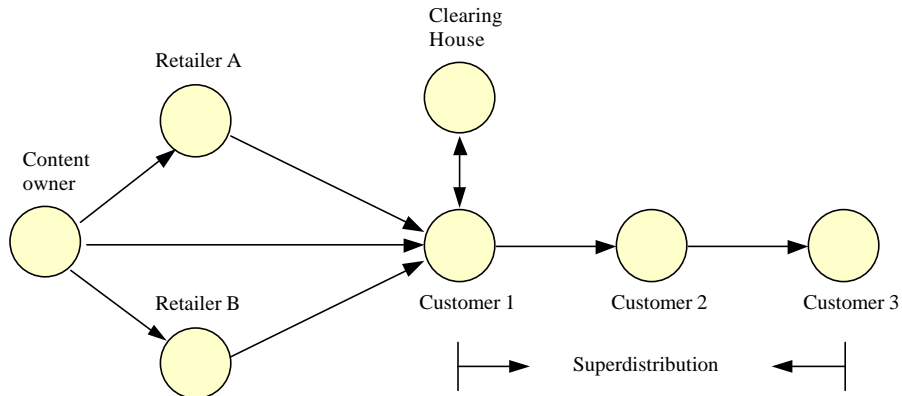
Figure 5. E-commerce with superdistribution

The following are a few of the possible ideas for encouraging file sharing and creating a competitive market[56]:

Promotions: The media file can be integrated with one or more promotions for retail offerings. Examples are a bonus track or a concert ticket for the purchase of an album, or a discount coupon for the local music store. Attractive promotions may result in more file sharing.

Packaged media with a unique Retailer ID: During the packaging of the media file, a unique retailer ID is added.   The file is shared among customers. When a customer in the distribution chain is directed to the clearing house to get his license, the clearing house credits the original retailer. This may be an incentive for a retailer to offer the best possible deal for a content.

Packaged media with a unique Customer ID: During the packaging of the media file, a unique customer ID is added. The file is shared among customers. When a customer in the distribution chain is directed to the clearing house to get his license, the clearing house credits the customer who initiated the distribution. This may be a good motivation for a customer to be the "first" in the chain.

7.   CONCLUSIONS

We have reviewed the security of entertainment content from creation to consumption. Our observations and conclusions are summarized as follows:

- Three complimentary and interacting mechanisms are available to protect intellectual property in digital form: technical tools, legal measures and business models.
- End-to-end-security is a key requirement for the growth of digital markets. Digital entertainment content needs to be protected in every stage of its lifecycle in order to prevent piracy losses, and encourage continued supply of products and services.
- The copyright industries, a segment of the US economy with a high growth rate, are the primary source of digital entertainment content. A better estimate of the economic impact of piracy on these industries is needed. Appropriate copyright policies can only be developed by understanding the complex social, cultural, legal and ethical factors that influence the consumer behavior.
- Digital media offers certain advantages:
    - o Perfect reproduction: Copies produced are indistinguishable from the original.
    - o Reduced costs for storage and distribution: Because of efficient compression methods, high quality content can be stored on lower-capacity media, and transmitted through lower-bandwidth channels.
    - o New business models: Content owners (artists, authors, musicians, etc.) can have direct access to consumers, specify and dynamically change their business rules, and regularly obtain customer information. Superdistribution is a promising model for quick and inexpensive distribution of products and promotions.
- Irrespective of the model used, the following elements interact in a commerce cycle for the management of digital rights:

- o Content owner (or its agent): packages content according to certain business rules.
- o Content distributor: makes content available to consumers through retail stores or other delivery channels.
- o Customer (with a compliant-receiver): purchases and consumes content according to usage rules.
- o Clearing house: keeps track of financial information and collects usage information.

- In every type of content protection system (conditional access, copy protection, digital rights management) based on secrets, key management (i.e., generation, distribution and destruction of keys) is an extremely critical issue. System renewability should be defined with the right balance between economic, social and legal factors.

- The US copyright law has been evolving in the last 200 years in response to technological developments. The recent obligations introduced by the DCMA will most likely need future revision for clarity and consistency.

- Worldwide coordination for copyright protection is a challenging task. In spite of international treaties, there are significant differences among countries, making it difficult to track national laws and enforcement policies.

8. ACKNOWLEDGMENT

9. REFERENCES

[1] http://www.wipo.org

[2] http://www.loc.gov/copyright/circs/circ1.html

[3] http://www.loc.gov/copyright/title17/92chap1.html#107

[4] William S. Strong, The Copyright Book, The MIT Press, 1999.

[5] http://www.loc.gov/copyright/docs/circ1a.html

[6] http://arl.cni.org/info/frn/copy/timeline.html

[7] P. Goldstein, *Copyright's Highway*, Hill and Wang, 1994.

[8] http://www.iipa.com

[9] Executive Summary of the *Copyright Industries in the US Economy – The 2000 Report*, International Intellectual Property Alliance, December 12, 2000.

[10] *The Digital Dilemma: Intellectual Property in the Information Age*, National Research Council, the National Academy Press, 2000.

[11] K. Jack, *Video Demystified*, Solana Beach, California: HighText Publications, second edition, 1996.

[12] B. G. Haskell, A. Puri, and A. N. Netravali, *Digital Video: An Introduction to MPEG-2*, New York: Chapman and Hall, 1997.

[13] L. Torres and E. J. Delp, "New trends in image and video compression," *Proceedings of the 10th European Signal Processing Conference (EUSIPCO)*, Tampere, Finland, September 5-8, 2000.

[14] S. Wenger, "A High Level Syntax for H.26L: First Results," *Proceedings of the SPIE Conference of Visual Communication and Image Processing*, San Jose, California, 2000.

[15] C. Christopoulos, A. Skodras, and T. Ebrahimi, "The JPEG2000 Still Image Coding System: An Overview," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 1103-1127, November 2000.

[16] K. Brandenburg, "MP3 and ACC Explained," *Proceedings of the AES 17th International Conference on High Quality Audio Coding*, Florence Italy, September 1999.

[17] F. Pereira, "MPEG-4: Why, What, How and When?," *Signal Processing: Image Communication*, Vol. 15, no 4-5, January 2000, (Special Issue on MPEG-4).

[18] B. Erol, M. Gallant, G. Cote, F. Kossentini, "H.263+: video coding at low bit rates," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.8, no.7, pp.849-866, November 1998.

[19] See http://www.divx.com, http://www.divxnetworks.com/, and http://www.projectmayo.com/

[20] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, Vol. 87, Issue 7, pp. 1079 – 1107, July 1999.

21 A. M. Alattar, "Smart Images Using Digimarc's Watermarking Technology," *Proceedings of the SPIE Conference on Security and Watermarking of Multimedia Contents II*, San Jose, California, 2000.

22 R. de Bruin and J. Smits, *Digital Video Broadcasting: Technology, Standards and Regulations*, Artech House, Inc., 1999.

23 H. Benoit, *Digital Television: MPEG-1, MPEG-2 and Principles of the DVB System*, Arnold, 1997.

24 L. C. Guillou, J. L. Giachetti, "Encipherment and Conditional Access," *SMPTE Journal*, Vol. 103, No. 6, pp. 398-406, June 1994.

25 W. Mooij, "Conditional Access Systems for Digital Television," *International Broadcasting Convention*, IEE Conference Publication, No. 397, pp. 489-491, September 16-20, 1994.

26 B. M. Macq, and J. J. Quisquater, "Cryptology for Digital TV Broadcasting," *Proceedings of the IEEE*, Vol. 83, No. 6, June 1995.

27 G. Rossi, "Conditional Access to Television Broadcast Programs: Technical Solutions," *ABU Technical Review*, No. 166, pp. 3-12, September-October 1996.

28 D. Cutts, "DVB Conditional Access," *Electronics and Communication Engineering Journal*, Vol. 9, No.1, pp. 21-27, February 1997.

29 W. Mooij, "Advances in Conditional Access Technology," *International Broadcasting Convention*, IEE Conference Publication, No. 447, September 12-16, pp. 461-464, 1997.

30 A. M. Eskicioglu, "A Key Transport Protocol for Conditional Access Systems," *Proceedings of the SPIE Conference on Security and Watermarking of Multimedia Contents III*, San Jose, California, USA, January 2001.

31 International Standard ISO-IEC 13818-1 *Information technology – Generic coding of moving pictures and associated audio information: Systems*, First Edition, 1996.

32 *EIA-679B National Renewable Security Standard*, September 1998.

33 http://www.dvb.org

34 http://www.macrovision.com

35 "Functional model of a conditional access system," *EBU Technical Review*, No. 266, Winter 1995/6.

36 http://www.atsc.org

37 J. M. Martinez (editor), "Overview of the MPEG-7 Standard," *ISO/IEC JTC1/SC29/WG11 N4031*, available at http://www.cselt.it/mpeg/standards/mpeg-7/mpeg-7.htm.

38 http://mpeg-7.com/

39 C. F. Goldfarb and P. Prescod, *The XML handbook*, Prentice Hall, 2001.

40 http://www.tv-anytime.org/

41 *Requirements Series: R-5 on Rights Management and Protection Requirements*, Document: TV039r7, December 15, 2000, available at http://www.tv-anytime.org/

42 *Intellectual Property Management and Protection in MPEG Standards*, ISO/IEC JTC1/SC29/WG11 N3943, January 2001, available at http://www.cselt.it/mpeg/.

43 *MPEG-21 Overview*, ISO/IEC JTC1/SC29/WG11/N4041, January 2001, available at http://www.cselt.it/mpeg/.

44 E. T. Lin, C. I. Podilchuk, T. Kalker, and E. J. Delp, "Streaming Video And Rate Scalable Compression: What Are The Challenges For Watermarking?" *Proceedings of the SPIE Conference on Security and Watermarking of Multimedia Contents III*, San Jose, California, 2001.

45 W. Li, "Scalable video coding with fine granularity scalability," *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, Los Angeles, California, pp 306-307, 1999.

46 E. Lin, G. Cook, P. Salama, and E. J. Delp, "An Overview of Security Issues in Streaming Video," *Proceedings of the International Conference on Information Technology: Coding and Computing*, Las Vegas, Nevada, April 2001.

47 A. M. Eskicioglu and E. J. Delp, "Overview of Multimedia Content Protection in Consumer Electronics Devices," *Signal Processing: Image Communication*, Vol. 16, No. 7, pp. 681-699, April 2001.

48 Content Scramble System, available at http://www.4centity.com/dvdcca

49 Content Protection for Prerecorded Media, available at http://www.4centity.com/4centity

50 Digital Transmission Content Protection, available at http://www.dtcp.com

51 High-bandwidth Digital Content Protection, available at http://www.digital-cp.com

52 http://www.vesa.org

53 http://www.upnp.org

54 P. Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised," *Berkeley Technology Law Journal*, Volume 14, 1999.

55 http://www.wto.org

56 Windows Media Rights Manager, available at http://msdn.microsoft.com