Everyone reading this story has heard the phrase copy protection (or content protection), but exactly what does it entail? And what do you, as a video producer, need to know about it?

Unlimited digital copying of licensed content is seen as a threat by most content owners. The possibility of widespread distribution of perfect video copies has resulted in content protection mechanisms to restrict copying. Yet to video creators, these restrictions can seem inexplicable and random, depending on the material’s source (i.e., standard or premium content) and the interactions between old and new equipment.

In this article, I’ll focus primarily on what video pros need to know about the aspects of consumer electronics (CE) and the technologies that are being deployed to protect broadcast and recorded video content, most prominently via TV and DVD. I won’t discuss DVD region codes, protecting music and CDs, Web streaming and downloads, or issues of morality, whether “piracy” or “fair use.”

Content Protection System Architecture (CPSA)

Content protection can be a morass of similar-sounding technical acronyms and obscure licensing organizations. Amazingly enough, the consumer electronics, computer, and content companies have developed a fundamental architectural strategy that underlies these approaches. The Content Protection System Architecture (CPSA) was developed by the 4C Entity (www.4centity.com), named after the four founding companies: IBM, Intel, Matsushita, and Toshiba.

CPSA is an overall framework designed to encompass major existing and upcoming entertainment content protection technologies. Its scope covers protecting personal computing and consumer electronics devices, protecting audio and video content in both analog and digital formats, and supporting physical and electronic content distribution methods. The architecture describes how compliant devices handle copy control information (also known as Content Management Information, or CMI), protect content during playback and output, and manage usage rights for recording.

Content Protection Issues

The CPSA framework states three basic requirements:

- protect content at its source (wherever it is stored and whenever it is copied);
CONTENT PROTECTION

- protect content as it is transmitted (e.g., from player to recorder, or player to display);
- protect content from unauthorized copying (i.e., only as permitted by the CMI).

A collection of technologies is needed to support these requirements, including

- digital and watermark copy management information to define usage rules;
- encryption algorithms to protect digital content (and associated CMI);
- encrypted transmission protocols to transfer content (and associated information) among devices;
- content protection mechanisms for unencrypted outputs to address the "analog hole" created during output to analog video displays.

This framework is demonstrated by the technologies developed for DVD, broadcast digital television, and high-definition formats.

DVD-Video Content Protection: Playback and Recording

Let’s start by analyzing DVD discs, which illustrate these content protection technologies. They use encryption to protect the digital content and support copy-management technologies for marking and encrypting. The protection technologies used are

- source protection: CSS for DVD-Video, CPPM for DVD-Audio;
- copy management: CGMS for DVD-Audio;
- output protection: Macrovision ACP (and HDCP, DTCP, etc.);
- content protection: CPRM for DVD-R/-RW, VCPS for DVD+R/+RW.

For replicated discs, the DVD author has the option of enabling one or more of these mechanisms in the disc image sent to the replication facility, with the appropriate licenses for both the title and the facility.

DVD players and recorders that choose to license CSS (in order to play back mass-market movies) also must support Macrovision ACP and CGMS-A analog protection, HDCP for DVI or HDMI digital outputs, and DTCP for IEEE 1394 and USB digital connections. These support requirements also apply to computer DVD drives and burners, and analog and digital computer TV outputs.

Replicated DVD Source Protection

Although replicated DVD-Video discs use CSS encryption, DVD-Audio uses a technology called CPPM. These technologies use a combination of keys as layered protection for unlocking the content: Title Keys to encrypt the content, Disc Keys to encrypt the title key on the disc, and Master Keys to decrypt the disc keys (see image at left). CPPM and CPRM also use a Media Key that uniquely identifies the physical disc. These technologies also include a key-exchange protocol to encrypt and protect the communication between the disc drive and the playback device.

Let’s step through the major technologies I mentioned. For easy reference, we’ve decoded many of these acronyms in a glossary on page 36.

Content Scrambling System (CSS)

CSS is the encryption technology used to protect DVD-Video discs. It’s licensed by the DVD Copy Control Association (DVD CCA; www.dvcca.org/css), and administered by License Management International (LMI; www.lmicp.com).

Content Protection for Prerecorded Media (CPRM/CPPM)

CPRM/CPPM is the corresponding encryption technology used to protect DVD-Audio discs. It’s licensed by the 4C Entity (www.4centity.com/tech/cprm).

Recordable DVD Source Protection

For recordable discs, the "zung" and "ung" formats support different content protection technologies. Besides encrypting the content, these CSS and CPPM
technologies tie the copy to the physical media to prevent bit-by-bit copies by using a unique media ID stored in an inaccessible area of the disc, etched in the lead-in area on the disc before the readable data area.

Although these technologies could potentially be used by consumers to protect home copies, they haven’t been visible in CE products. VCPS (see the definition below) is a recent development that’s showing up in new equipment in response to the FCC Broadcast Flag rules. Some DVD recorders support CPRM, but it hasn’t been required for DVD players. However, once a DVD has been encrypted with one of these technologies, the disc won’t be playable in legacy devices, even if copying is permitted.

**Content Protection for Recordable Media (CPRM)**

CPRM is used for DVD-R/-RW and DVD-RAM discs. It’s used for copy-once VR format recordings (not DVD Video). The RW Compatible logo on many Japanese DVD recorders and players means the device can play VR recordings with CPRM encryption. CPRM also is licensed by the 4C Entity.

**Video Content Protection System (VCPS)**

VCPS is used for DVD+R and DVD+RW recordable media. Developed by HP and Philips (www.licensing.philips.com/vcps), VCPS was designed to protect recordings of digital broadcast according to the FCC Broadcast Flag rules, and also enables direct digital recording of copy-once content from satellite and cable sources.

**DVD Copy Management Information**

DVDs also use technologies to associate content management information with analog and digital content.

**Copy Generation Management System - Analog (CGMS-A)**

CGMS-A embeds copy management information in analog video, carried in the vertical blanking interval. Unlike Macrovision ACP, CGMS-A is only a flag, and depends on downstream equipment to recognize the signal and refuse to make copies. CGMS-A is required for use with CSS and DTCP. The CGMS-A+RC (Redistribution Control) extension requires that the content may not be redistributed over the Internet. Versions of CGMS-A are standardized as IEC 61880/61880-2 and EIA/CEA-608-B, available from Global Engineering Documents (http://global.ihs.com).

**Copy Generation Management System - Digital (CGMS-D)**

CGMS-D defines copy management information for digital connections. It’s used as the basis for technologies such as HDMI and DTCP (see the following sections). However, CGMS is something of an ad hoc standard, without an active licensing or certification entity, so its use has been limited in current DVD devices.

**DVD Output Protection**

As required by the CSS license, DVD players also must actively protect output to displays. For digital outputs, these devices use HDCP and DTCP to encrypt the signal. For analog video output, Macrovision ACP prevents analog copying with devices such as VCRs and DVD recorders.

**Macrovision ACP**

Macrovision ACP analog content protection applies two techniques to the video signal—Automatic Gain Control and Colorstripe—so VCRs can only make distorted copies while televisions, with less strict tolerances, can still display the signal. Macrovision ACP is patented and licensed by Macrovision (www.macrovision.com/products/macrovision_acp).
**Digital Video Content Protection**

The development of digital displays and networked devices introduced a new dimension into content protection. Technologies such as CSS and CPRM/VCPS can protect source digital content when it's stored on DVD. And, as with VCRs before, technologies such as CGMS-A and Macrovision ACP can mark and protect the output analog video signal. But before consumer electronics and computer industries could promote direct digital connections among home devices, content owners demanded additional protection technologies to encrypt the material across digital wires.

**Broadcast Flag**

Thus, the Broadcast Flag was defined to mark content as requiring protection as it enters the home, and technologies such as HDCP and DTCP are used to protect material on high-bandwidth display connections and traditional computer digital interfaces. The Broadcast Flag is a digital broadcast content protection mechanism that was mandated by the U.S. Federal Communications Commission (FCC) in 2003 for the purpose of preventing mass distribution of copies over the Internet (http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-273A1.pdf). The Broadcast Flag was intended to be set at the discretion of the broadcaster as a digital code embedded in ATSC digital TV broadcasts. All digital copies of flagged broadcasts must then be encrypted, and be playable only on devices that don’t permit redistribution. It didn’t prevent analog copying or additional copying to authorized devices.

In order to enforce this requirement, the FCC extended its mandate from communications to encompass the consumer electronics and computer industries. The FCC ruled that after July 1, 2005, any DTV receiver could only pass on flagged content to a digital output if that output is protected by an approved technology. However, in May 2005, the U.S. Court of Appeals for the District of Columbia ruled that the FCC had exceeded the scope of its regulatory authority, and struck down the Broadcast Flag.

Meanwhile, the FCC mandate had already resulted in a new infrastructure required to support the Broadcast Flag in CE and computer equipment. This included the addition of VCPS to DVD recorders and support for the CPRM and VCPS protocols in software like CyberLink PowerDVD in order to permit consumers to play back their recorded discs. The FCC’s intent was that “all existing equipment will remain fully functional.” However, old equipment and software wouldn’t be able to even play back encrypted discs. As an example, if you swapped out an existing DTV demodulator connected to an old DTV recorder, you might find the DVD recorder suddenly can’t understand the encrypted signal that’s passed to it when the new demodulator recognizes the Broadcast Flag.

**Digital Video Display Interfaces: DVD, HDMI, HDCP**

All-digital home entertainment systems introduce a demanding problem: supporting high-bandwidth uncompressed video connections at HDTV resolutions. The creation of the Digital Visual Interface (DVI; www.ddwg.org) and High-Definition Multimedia Interface (HDMI; www.hDMI.org) allows digital devices to generate full-quality outputs on digital displays, using consumer-friendly cabling.

**High-bandwidth Digital Content Protection (HDCP)**

HDCP is designed for protecting audiovisual content from being copied over DVI and HDMI high-bandwidth interfaces. HDCP provides content protection mechanisms for authentication of HDCP-compliant transmitters and receivers, encryption of content over the interface, and revocation of invalid receivers based on assigned private Device Keys. HDCP was developed by Intel and is licensed by Digital Content Protection, LLC. (www.digital-cp.com).
Digital Video Transmission Protection

Besides local display devices, the digital home also offers the opportunity to distribute digital content to other devices through local FireWire and USB connections, and even over a local home network. One computer-based solution for protecting content within this larger scope is to use a digital rights management (DRM) technology that’s supported by the PC and attached devices for situations like downloading a purchased movie or song to a portable device.

Digital Transmission Content Protection (DTCP)

DTCP defines a more general cryptographic protocol for protecting digital A/V content on high-performance digital interfaces, such as FireWire. It includes a device authentication and key exchange protocol to verify connections, copy-control information based on CGMS, and content encryption with optional stronger ciphers. DTCP also supports revocation of unauthorized devices through system-renewability messages delivered with new content. It was defined by the “SC” group—Hitachi, Intel, Matsushita (Panasonic), Sony, and Toshiba—and is administered by the SC / Digital Transmission Licensing Administrator, LLC. (DTLA; www.dtcp.com).

DTCP over Internet Protocol: DTCP-IP

DTCP-IP extends DTCP to protect content transmitted across IP network connections using 128-bit Advanced Encryption Standard (AES) encryption. It’s intended for use within local home networks, including wireless connections (see the image above).

The Next Generation: High-Definition Content

Content protection for DVD has arguably served its purpose of preventing wholesale casual copying. However, sophisticated pirate rings still can produce copies of first-run features within days of their release, captured from videotapes shot in theaters or even the original prints, and released over the Internet or on DVD in surprisingly high quality, complete with packaging and subtitles. In addition, motivated consumers can download DeCSS ripping tools to copy their discs, optionally recompressing from dual-layer DVD-9 to single-layer recordable DVDs, or even to CD.

Given this history, content owners wanted stronger technologies to protect new high-definition digital material, whether delivered by broadcast or on physical media. The result is AACS, which uses stronger technology than CSS to protect source content on optical media and also integrates content management for both replicated and recordable discs.

Advanced Access Content System (AACS)

AACS is designed to encompass content protection, copy control, and key management and revocation for compromised keys. It is being managed by the AACS Licensing Administrator (http://aacsia.org), founded by companies spanning the content, PC, and CE industries: IBM, Intel, Microsoft, Panasonic, Sony, Toshiba, Disney, and Warner Bros. The intent is to provide more flexible copy management and to share and even move content across home networks and onto portable devices.

FURTHER RESEARCH:

BACKGROUNDER

For background on content protection laws and technologies, search for Don Labriola’s detailed Digital Content Protection article on www.extremetech.com.

DVD FORMATS & PROTECTION

For more information on DVD formats, see Jim Taylor’s extensive DVD FAQ for technical details and updates on associated content protection technologies (www.dvddemystified.com/dvdfaq.html).

GLOSSARY

For a recent summary of content protection and DRM technologies, see our glossary on the following page or the glossary from DEG at www.dvdfoundation.com/TechResources/images/DEG%20DRM%20Glossary.pdf.
audiovisual content. AACS also uses a new renewable form of drive authentication that’s not compatible with the CSS protocol used by current drives.

**Content Protection in the Digital Home**

The popularity of online services like iTunes has demonstrated the importance of selling content as digital bits, both as purchased downloads and as licensed streaming.

The corresponding explosion of portable media players has expanded content from the desktop to local devices in the home. Moreover, digital video recorders within the digital home open up the possibility of storing and sharing content among a family of computer and consumer electronics devices throughout the home.

This development has engendered a broad coalition of industries to develop content protection technologies that provide strong enough protection to satisfy content owners, while also allowing controlled copying among computer and CE devices.

However, introducing these technologies in new CE and computer devices can lead to collateral damage—some material can inexplicably become inaccessible or unable to be copied. These new products will need more transparent mechanisms to view and understand authorization information associated with content.

**Conclusion**

We can expect to discover unpleasant surprises as digital content flows among new content technologies and legacy devices, and when computer-based DRM systems interface with consumer electronics equipment.

---

**GLOSSARY**

- **AACS**: Advanced Access Content System, developed and managed by the AACS Licensing Administrator
- **ATSC**: Advanced Television Systems Committee
- **CGMS-A**: Content Generation Management System - Analog
- **CGMS-D**: Content Generation Management System - Digital
- **CMI**: Content Management Information, aka copy control information
- **CPPM**: Content Protection for Prerecorded Media, for DVD audio
- **CPRM**: Content Protection for Recordable Media, for DVD-R/RW
- **CPSA**: Content Protection System Architecture, developed by the 4C Entity
- **CSS**: Content Scrambling System, for DVD video
- **DRM**: Digital Rights Management technology
- **DTCP**: Digital Transmission Content Protection over USB and IEEE 1394
- **DTCP-IP**: Digital Transmission Content Protection over Internet Protocol
- **DTLA**: Digital Transmission Licensing Administrator, LLC.
- **DVD CCA**: DVD Copy Control Association, administers CSS
- **DVI**: Digital Visual Interface, display interconnect
- **HDCP**: High-Bandwidth Digital Content Protection, developed by Intel, licensed by Digital Content Protection, LLC.
- **HDMI**: High-Definition Multimedia Interface
- **LMI**: License Management International
- **Macrovision ACP**: Analog Protection System from Macrovision
- **VCPS**: Video Content Protection System for DVD+R/+RW, developed by HP and Philips

Another industry group, the Coral Consortium, is addressing these usability issues of “interoperability between DRM technologies used in the consumer media market” (www.coral-interop.org). Its voting members are HP, Intertrust, Philips, Matsushita (Panasonic), NBC Universal, Samsung, Sony, and Fox.

The result for professionals is to add another kind of compatibility testing to the workflow: verifying the flow of digital content through computer and CE pipelines, especially when adding new devices or working with new content sources.