CONTENT SUPPLIER'S PERSPECTIVE: HOME NETWORKS AND RIGHTS MANAGEMENT

Robert M. Zitter, Craig D. Cuttner
Home Box Office

Abstract

Copyright Protection, Digital Rights Management, Home Networks and other buzzwords are all swirling around in a frenzy that has seemingly pitted content providers against operators and all seem to make consumers appear to be felons.

This paper defines the scope of the issue and discusses the pro- and con-attributes of a Home Network.

Beginning in the first-steps of initial implementation of "simple" Copy Control Information (CCI) and how that may evolve into sophisticated Digital Rights Management (DRM) systems.

BACKGROUND

Content Value and Cable Value

The 'sale' of access to video content has been a hallmark of the cable television industry since its inception. Technology used in the distribution, securing the distribution and the content itself has evolved over time as has the value of the content being distributed. Cable, and other forms of multichannel distribution (MVPDs), are actually the 'tip of the iceberg' related to a multi-faceted time-value food-chain that impacts all aspects of content.

Time-value of content and distribution are not new concepts. Hard cover books become mass-market paperbacks and later motion pictures. Theatrical movies have subsequent distribution windows such as home video, pay-per-view, etc. – each window and its attendant revenue stream is critical to the total revenue stream that makes theatrical movie production a viable ongoing business.

If video programs are available on the Internet at no charge, once the Internet is connected to a digital home network, consumers will be less likely to pay for the services MVPDs offer.

Distribution Security

Over time, cable distribution technology has evolved to thwart the capabilities of the "consuming public" to circumvent the collection of fees and protect revenues. Non-standard channel ("mid-band" placement for pay channel security in the '70s) was succeeded by block converter devices and, later, by the cable-ready TV, which necessitated trapping. Higher value premium TV led to channel scrambling and fixed (programmed) descrambling STB's. Pay per view required addressability – and the consumer's ability to record high-value content led to analog copy control (a/k/a Macrovision).

Each of these steps was necessitated by an evolutionary requirement to continue to collect revenue to keep growing the cable and content industries.

Likewise, the "robustness" of systems was driven to sophistication requirements by the day's environment. Security evolved from virtually-none (since early TVs did not

generally tune RF non-standard channels), compromised by simple "orange wires" in set-top-boxes, to sync-suppression scrambling – and, in fact, it was not always clear that the consumer electronics products were designed to respect the necessity of cable security – early versions of digital-chassis analog television receivers were able to defeat very sophisticated sync-suppression scrambling.

Although there were limited cases of "redistribution" of video programming (e.g. an apartment building with 'channel-3 sharing'),. the physical audit capabilities of the cable operator, and simple physical limitations of single-premium-channel distribution, were adequate limits on the spreading of content redistribution.

TODAY'S LANDSCAPE

Building on the premise that the "on/off" nature of conditional access (traps, addressability, or other forms of access denial) was appropriate to the consumer's then-current abilities to circumvent those systems. Further building on the ability to use simple analog Macrovision as an appropriate means to prevent analog VCR copies in the PPV window – where does that leave us today?

Digital cable-ready receivers will soon be able to be directly-attached to cable systems; digital VCR and DVD burning devices are growing in popularity, and the fastest-growing segment of the (IT) computer industry, the 'Media Center PC' – promotes a video program guide, Digital Video Recording and DVD-burning.

Clearly, the next evolution in conditional access, content security – and potential new revenue streams are upon us.

Consumers increasingly want all of their home electronics products to integrate and provide a 'greater good' by using common control systems and making content available in different rooms, on different devices – including computers, portable devices, and, perhaps, vehicles.

This need for integration means a network – and the "Home Network" connectivity promise soon available to consumers is both a potential revenue source for enhanced services, provisioning, management, and maintenance – and a threat to the distribution-revenue just as has occurred in decades past.

The stakes today, unfortunately, are much higher.

While a crude 'channel-3 network' might have provided a few like-minded apartment dwellers a single-channel of HBO in the 1970's – one copy of a motion picture on the Internet has devastating impact on the revenue stream before, during and after the cable window. The impact will be more devastating now that the value of cable content has significantly increased – and more of that content is original-to- cable, as its first exhibition window.

First Steps in Security – Basic Conditional Access

The FCC and industry economics have dictated the first steps to continue the evolution of cable security – the one-way digital cable ready television is a reality.

Using contemporary industry-standard digital encryption techniques, the CableCARD™ can take the best-of-breed conditional access systems deployed today and integrate it into a consumer-purchased host device. As required by the Digital

Millennium Copyright Act (DMCA), no consumer-accessible 'in-the-clear' streams are available courtesy of DFAST encryption.

It is important to note that the current implication in the nature of consumer behavior is that "in the clear" is a direct tie to "distributed on the Internet" without recourse. It is the need to encrypt content securely to both maintain its value and retain legal protections under DMCA.

CableCARD, however, is only the first-step evolution of an integrated TV / set top – and it alone does not provide functionality for the Home Network as consumers would deploy it.

In a consumer environment, more connections than cable-to-host / display are envisioned. Modular components (set top to plasma display; recorder to display; media storage to display) begin to form the basis of a series of output to input links – all digital – hence all needing some form of copyright protection to prevent 'unprotected copying and redistribution.' Each type of interface has a defined and approved copy protection system and is a overall part of the 'Plug-and Play Agreement' tied to a set of principles and rules that govern access to and use of cryptographic keys that control system behavior.

Second Step – (Protected Interfaces)

As secure digital interfaces require copyright protection regimes, there are systems appropriate to the major interfaces:

1. The CableCARD itself – although not intended for consumer access, the pins of the card interface could be intercepted during their transport of high-value content – thus, the DFAST encryption system is used to ensure that the host device properly adheres to the PHILA principles.

2. Compressed Firewire (1394) – the '5C' (DTCP) copy protection regime is specifically tailored for high-speed compressed applications.

3. Uncompressed DVI (also HDMI) – the 'HDCP' copy protection regime is specifically tailored for uncompressed digital signals such as might be transported between a host device and display device.

These copyright protection systems protect, generally, a source-to-sink relationship and convey only 'basic' copy control states. (Generally, signals in this context, originate in a "source" device and are consumed in a "sink" device. A set top is an example of a source, a TV display is a sink.)

The ability to separately enable and disable items 2 and 3 (above), is referred to as "selectable output control" which was a point of considerable discussion during the Plug and Play negotiation.

Second Step – (**Un**protected Interfaces)

Analog video, in many contemporary consumer devices today, is routinely converted from analog to digital in a very high-quality manner. Once that conversion has occurred, all of the concerns about copyright protection, Internet redistribution, etc. equally apply to the converted signal. This is the so-called "Analog Hole."

NTSC composite analog video is "protected" only to the extent that Macrovision may be applied as a part of the 'copy never' state. CGMS-A may also be present to signal other copy control states, but may be removed by some consumer

devices, thus it is not, by itself, sufficient for authoritative signaling. Further, the "low-quality" nature of NTSC limits the quality of copies that may be made from either the original analog or digital copies thereof.

Component analog video interfaces are higher quality than NTSC, and can support very-high quality signals up to high-definition. Considering the weaknesses of CGMS-A noted above, and the fact that only certain resolutions and formats of component analog support a vertical blanking interval for carriage of copyright control information, there are concerns about very high-quality analog to digital conversions of component analog. When component interfaces are "unprotected" some content owners necessitate lowering the picture resolution to that of NTSC, so that analog to digital conversion is less effective – thus called "down-resolution" – which is also a point of discussion in the two-way negotiations.

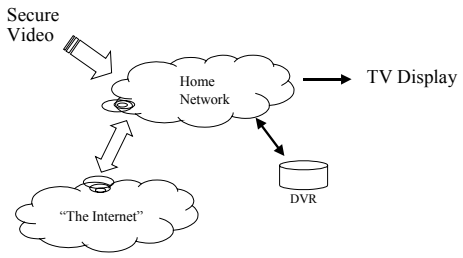
Copy protection states are discussed more fully below.

FUTURE NETWORK FEATURES

Third Step – Protected Home Network

How do we evolve the current secure and revenue-generating MVPD distribution infrastructure into a similarly secure (often called "trusted") part of the content distribution infrastructure? Considering that it is a forgone conclusion that consumer home networks will exist, this is an important task at hand – as will be discussed for the remainder of this paper.

Home Network Topology



There are two other "competitors" that currently are working to be the key providers of that home network:

1. Consumer Electronics (CE) manufacturers that look at device connectivity as an extension of their devices' functionality – and hope to leverage that product benefit into their offerings;

2. Information Technology (IT) manufacturers, recently growing into the traditional CE space by selling entertainment hardware, have looked at home networking as an extension of their data infrastructure – and the increased functionality is also a point of desired benefit.

3. Of course, it is desired that the MVPD be included in this list – as a very key provider with decades of expertise in the transport of high-value content – and a key participant in the revenue chain that benefits from the secure transport of content.

Currently, neither of these two non-cable potential home network providers are involved in the revenue stream nor the protection of the time-value of the content in the food chain.

Although home networks will exist, it is essential that the home network be 'trusted' in the economic sense – and, in the technical realm, 'robust' in implementation – unlike the previous evolution from traps to scrambling, the stakes are much higher.

If three equal home networks were to evolve, content companies need the same level of security – and already have experience with "trusted" cable networks. Content security is a "new" feature to the "other two" home network developers. Thus, MSOs have an advantage because of their participation in the revenue chain – and the attendant concerns to preserve security, and to evolve conditional access as they have before.

COPY PROTECTION BASICS

Access to Content

In the 1970's 'legacy' consumer environment, where "on and off" were sufficient business conditions – and there were no recording or distribution issues of concern – conditional access worked fine at a very simplistic level. As noted, when consumer copying of PPV became a potential threat, copy protection was added.

Today's access to content, if the environment was devoid of redistribution, copying and there was no desire to increase revenue by exploitation of the time value of content, then simple conditional access would be sufficient.

However, the home network implies connectivity, copying for convenience and device portability – and the risk of uncontrolled redistribution of high-quality content beyond the subscriber is too economically devastating to ignore. Copyright protection is necessary to augment conditional access.

Copy Control Modes

Generally, there are but a few business model concerns that need protection:

No uncontrolled redistribution on the Internet – this restriction is mandatory in every copy 'restriction' state – and also a requirement for the 'Retransmission Control Descriptor' (RCD) (also known as "broadcast flag") if the content is not otherwise copy controlled. (Note that the RCD is currently under industry discussion and is not necessarily ratified in standards mentioned below.)

Copy Once – content marked copy once is restricted to one copy (even on removable and archival material), but all playback devices must mark the playback output as "copy no more" to ensure that no subsequent copies are made. A copy on a device such as a Digital Video Recorder (DVR) might be 'moved' to an archive under the rules of Copy Once.

Copy Never – content marked copy never is prohibited from having any recorded copies other than copies that are of short-duration (convenience-type) copies.

These three states are communicated by two binary "bits" in several control messages that are either embedded in content or sent via control streams. Copy control information (CCI) bits can occur in some or all of the following forms:

- Setup in the configuration of set-top boxes, control software and digital interface drivers. In this way permanent modes could be set via programmer (content provider) direction.

- Analog (Copy Generation Management System – Analog (CGMS-A)) bits are sent via Line-20 (International use, standardized by IEC); US VBI standardization of CGMS-A is included in CEA-608-B via Line-21. Note: The intent is not to restrict analog recording but identify copyrighted content to downstream Analog to Digital (A/D) devices or encoders to give instructions regarding redistribution and copying.

- Other signaling such as Program Map Table (PMT) is under discussion and is proposed in some technology licensing agreements.

It is important to note that declaration of copy control mode, the mechanism that sets the mode (whether that control is embedded in the content or 'authoritative' via secure channel such as an encryption system) and the type (category) of content that is copy-controlled is governed by the DMCA, FCC rules, and technology licensing agreements (so-called "Encoding Rules").

Encoding Rules as proposed by the cable and consumer electronics industries (and adopted by the FCC) propose the following **ceiling** levels (less restrictive levels are allowed for a particular content type, but not more restrictive) for copy control:

- Copy Never: PPV, VOD (on-demand PPV), SVOD.

- Copy Once: Linear premium and basic television

- Copy Freely: Over-the-air broadcast television (however, the RCD may be applied).

BASIC COPY CONTROL STATES

Bits	Control Mode	RCD	Redistribution
0 0	Copy Freely	0	Allowed
		1	Prohibited
0 1	Copy Once	x	Prohibited
1 0	Copy Never	x	Prohibited
1 1	Copy No More*	x	Prohibited

(* sometimes copy no more is flagged as copy never)

x = "don't care"

HBO / Cinemax linear content is designated "Copy Once" and HBO / Cinemax on-demand content is designated "Copy Never."

Fourth Step – Digital Rights Management

The next step in the evolution that optimizes the trend in time-value content revenue optimization, secure distribution of content, copy management, portable device management and takes the role of conditional access to its, arguably, ultimate level – is to include digital rights management functionality into a 'traditional' conditional access system.

DRM will be the tool by which MVPDs and content owners will be able to use copyright protection technology to create new consumer offerings rather than simply employing the technology in attempts to preserve the status quo.

Conditional Access systems, generally, are 'trusted' for their security and have evolved from quite simple on/off gates to addressable, VOD-enabled, two-way session-based, transactional systems.

Digital Rights Management (DRM) systems, now deploying for Internet-related content delivery, provide basic security (encryption) technology – but have very

complex on/off rules – sometimes embedded within the content (not necessarily requiring a two-way connection). On/Off rules can be soft descriptions of business cases (such as subscription, copying permission, quantity of viewing (e.g. x-views), duration of viewing (self-destruction of copy after y-days), etc.).

Signaling the DRM control states is an ongoing industry discussion ("Extended CCI") and is not yet embodied in cable standards or other rules.

The integration by a MVPD of an 'trusted' conditional access / DRM system into a whole-home-network environment that exerts authoritative control over content within the network, provides all protected outputs from the network under that control umbrella, is the genesis of a 'Trusted Domain.' Such a secure environment will be necessary to optimize the time-value revenue stream – that has served cable so well since its very first paying subscriber. But, that was a few hundred billion dollars ago, and there are plenty more to go around.