CONTENT PROTECTION CONSIDERATIONS FOR DIGITAL CABLE READY PRODUCTS AND SECURE HOME NETWORKING

Brad Hunt[1] and Jim Williams[2]
[1]Sr. VP, Chief Technology Officer, [2]VP, TV & Video Systems

Abstract

This technical paper highlights several important content protection considerations for Digital Cable Ready products including secure digital outputs, steps to address the "Analog Hole", secure integrated personal digital recorders and secure home networking.

Adding new features in a secure manner will help maintain the viability of cable television in the competitive and expanding market of digital content distribution. It will also better position the cable industry to launch new innovative programming services that can increase revenue, control churn, and expand the subscriber base.

INTRODUCTION

In the recent past, marketplace solutions for content protection and security were developed by Cable MSOs and other MVPDs through independent negotiations and contractual obligations with content providers and receiver manufacturers. As part of its implementation of Section 304 of the Telecommunications Act of 1996, the FCC issued its Second Report and Order in October 2003 that outlined rules and standards for unidirectional digital cable ready products. Through this ruling the FCC committed to the principle of separation of security functions from the base customer premises equipment to support the retail availability of digital cable set-top boxes that consumers could take with them when they move. With the separation of the security functions, content owners and MSOs no longer have a direct relationship or voice in the construction of cable receiving products.

Content owners continue to have a vital interest in ensuring that all content distribution platforms are secure not only for existing services but also for future envisioned service offerings. Their views concerning the security aspects of a content acquisition device should be incorporated into the device's technical specifications and the content protection related licensing terms. In addition, the process for approving new protected digital output and secure recording technologies must also include a role for content owners.

As directed by the FCC, the Cable and Consumer Electronics industries have begun working with content owners to define the content protection requirements for next-generation bidirectional "Digital Cable Ready" products. These ongoing discussions regarding the bidirectional framework have provided content owners with an opportunity to express and discuss their views on content protection. As recognized in the Broadcast Flag regulation, the ability of distribution channels to attract high value content is enhanced by due recognition of the security needs of content owners.

This technical paper will highlight several important content protection

considerations related to Digital Cable Ready products.

APPROVAL OF EFFECTIVE DIGITAL CONTENT PROTECTION TECHNOLOGIES

As important partners in enabling content distribution over cable, content owners have a legitimate interest and should have a meaningful role in approving new digital content protection technologies in digital cable products. These include new protected digital output technologies and secure recording methods.

Currently, CableLabs has the authority to approve or disapprove new digital output protection technologies and secure recording methods for digital cable products manufactured under the CableCARD Host Interface License Agreement (CHILA) and the unidirectional DFAST license. It is not clear what functional criteria CableLabs uses to evaluate a digital content protection technology. In fact, the use of a fixed set of functional criteria may be too restrictive in allowing for innovation of new content protection technologies. A more effective manner of analysis and approval should be based on marketplace criteria where content owners' views and actions can lead to approvals based on the marketplace performance of these technologies. At the very least, CableLabs should incorporate a more formal process that seeks and takes into account input and advice from content owners as an integral part of their decision-making process.

SECURE HOME NETWORKING – EVOLUTION FROM COPY PROTECTION TO CONTENT PROTECTION

The nature of customer premises equipment is changing -- evolving from one or more independent receivers with analog video outputs to a suite of networked digital devices that have access to shared resources including tuners, mass storage devices, optical media burners, computers and Internet connections. With continually increasing processing power, Internet connection speed, compression algorithm performance and storage capacity, the customer premises equipment suite is becoming a digital processing, communications, storage, and consumption powerhouse ripe with new content usage possibilities for consumers.

Digital content protection technologies ensure that a particular usage model or cable service offer that is purchased through a conditional access system is honored by downstream devices. Traditional content protection technologies have focused on copy protection. As customer premises equipment evolves into a suite of home networked devices and even to devices beyond the home, the content protection system must also incorporate redistribution control.

The typical usage rights that might be granted in a cable environment include the right to make copies, the right to electronically move content around one's home (e.g. to another TV set) and the right to make a physical copy that can be carried beyond one's home. However, unrestricted redistribution of content beyond one's home would be inconsistent with the licensing rights negotiated from the content owners and could undermine the subscriber-based

business model of the cable television industry.

OPENCABLE™ MUST BE UPDATED TO PROTECT THE SINGLE HOME CABLE ACCOUNT

The current OpenCable™ specifications do not provide the ability to distinguish a single digital cable subscriber with a home network from a group of separate households "sharing" a single cable account using wide area networking. In addition, the content protection afforded by these specifications should provide the ability to signal redistribution control information and manage content usage in accordance with that signaling.

The current OpenCable™ CableCARD™ Copy Protection System Interface Specification does not provide a means for signaling Redistribution Control. In addition to signaling numeric copy control restrictions of Copy Never and Copy One Generation, this interface specification must have a means to signal Redistribution Control when no numeric copy control restrictions are asserted. For example, this could be the case for programming delivered on the Digital Basic Tier, where a Cable MSO optionally wants to encrypt the service to provide protection against theft of service. In this case, the controlled content would be marked in a manner to signal that there are no numeric constraints on copying within the home or to removable media, but the controlled content must be protected by the host device to restrict redistribution beyond the particular cable subscriber's home, including over the Internet.

IMPLEMENTATION OF A DIGITAL CONTENT PROTECTION DEVICE KEY REVOCATION SYSTEM

The cable distribution system must provide an end-to-end solution for the delivery and processing of digital content protection System Renewability Messages (SRMs). System Renewability Messages are the common name for the messages that contain digital content protection device key revocation information. Device key revocation provides a content protection technology the means to selectively disable the protected digital output of a compromised device (e.g., a non-compliant device created using a cloned device key) without impacting the general functioning of the device. It is therefore a critical component in managing the effective functioning of a digital content protection technology.

Specifically, the cable system must develop a means for efficiently delivering SRMs from the cable head-end to the digital cable receiver. In addition, both the CHILA and the unidirectional DFAST license must contain explicit obligations for the digital cable receiver to perform digital content protection device key revocation processing when validly received SRMs are presented. Since some digital content protection technologies, like High-bandwidth Digital Content Protection (HDCP), do not store revocation lists, the CHILA and DFAST license must explicitly require real-time processing of SRMs. In the specific case of the 5C Digital Transmission Content Protection (DTCP), the CHILA and DFAST license must require that the device implement "Full Authentication" of the DTCP source function, in order to ensure that full SRM processing is done. These are a few of the requirements for insuring digital cable products incorporate digital content

protection technologies that implement an effective device key revocation processing mechanism.

ADDRESSING THE "ANALOG HOLE"

In the process of delivering protected digital content, the content must be converted into an analog video signal in order to support legacy displays that have only analog video inputs. However these analog video signals can be easily converted back to digital without any obligations to preserve and respect the content's usage rights information. The protected digital content is said to escape through the "Analog Hole". The challenge for our industries is to determine the best way to support legacy analog displays without creating an unnatural impediment to the migration to digital.

Several key features of digital cable products are important in addressing the Analog Hole:

- Analog copy control signaling implementation;
- Image constraint on unprotected high definition analog video outputs; and
- Selectable output control capability for new business models.

Each of these features is an important content protection function, and in combination, provides a reasonable approach for addressing the Analog Hole.

ANALOGCOPY CONTROL SIGNALING IMPLEMENTATION

One important component of the solution to the Analog Hole begins with the use of a standardized means for signaling copy control information in the analog video outputs of digital cable receivers. The application of analog copy control signaling, such as analog Copy Generation Management System (CGMS-A) signaling, has been widely implemented for many years in a number of content protection licenses and specifications. This vertical blanking interval signaling allows the conveyance of usage rights in analog video content. Many digital recorders detect CGMS-A in order to manage unauthorized copying. For example, when the CGMS-A state of "Copy Never" (1,1) is detected in the vertical blanking interval of an analog video signal to be recorded, the digital recording is stopped. In order for this signaling to be deployed effectively, it must be generated correctly in the digital cable set top box.

Both the CHILA and unidirectional DFAST license need explicit obligations for the regeneration and the insertion of vertical blanking interval signals for copy and redistribution control. The MPAA has proposed specific language for explicitly defining CGMS-A, Analog Protection System (APS), and Redistribution Control Information (RCI) signaling in these licenses for all analog video format outputs. In order to ensure full protection, analog vertical blanking interval signaling must also be applied both to upconverted standard definition TV programming that is output as a high definition analog video signal and, likewise, to downconverted high definition TV programming output as a standard definition analog video signal. Finally, analog video outputs should not be permitted absent a standardized means for carrying CGMS-A, APS, or RCI vertical blanking interval signaling. This is currently the case for analog RGB VGA computer monitor outputs.

IMAGE CONSTRAINT OF UNPROTECTED HIGH DEFINITION ANALOG VIDEO OUTPUTS

Content owners are very concerned about the introduction of digital recorders that exploit the high definition Analog Hole. The price of high definition analog-to-digital video converter devices is falling and could soon lead to the introduction of consumer devices that digitize and record unprotected analog high definition video content. The use of image constraint on unprotected HD analog video outputs is an important tool in addressing the high definition Analog Hole. The optional use of image constraint on unprotected analog high definition video outputs has not been demonstrated to have any visual impact on legacy HDTV displays having only analog video inputs.

The use of image constraint provides incentives for consumers to use the higher-quality, protected digital interconnects that are becoming available in the marketplace. Since the obligation to implement image constraint is in the DFAST license, all unidirectional CableCARD-equipped host devices being introduced today have image resolution constraint capability. This capability must be implemented in future digital cable products.

SELECTABLE OUTPUT CONTROL CAPABILITY FOR NEW BUSINESS MODELS

Under the unidirectional regulation, the FCC acknowledged that selectable output control could be appropriate for use in the future. Cable is afforded two key benefits by deploying selectable output control capability in Plug and Play products.

First, as suggested by the FCC, selectable output control might enable future applications that are advantageous to consumers, such as new early-window business models. For example, in order to create a more secure environment for an early-window high definition video programming service, an MVPD may find it advantageous to deliver this service with the requirement that unprotected analog high definition video outputs are disabled and only digital outputs protected with HDCP and DTCP are allowed.

Second, selectable output control could also help address unknown problems, such as patent claims and court orders involving a previously-approved content protection technology.

In order to make these future permitted uses possible, manufacturers should be required to incorporate selectable output control capability in all digital cable products.

CONTENT PROTECTION OBLIGATIONS FOR HARD DISK DRIVE INTEGRATED RECORDERS

Integrated Personal Digital Recorders (PDR) in Digital Cable receivers provide many attractive benefits to consumers, such as pause, time-shifting, and the movement of temporarily stored recordings of “Copy One Generation” programming to removable media. But in order for integrated recorders to provide this functionality, the content and associated usage rights information must be securely and persistently protected and content usage must be effectively managed in accordance with those associated usage rights.

In the case of temporary recordings of “Copy Never” programming, the content must be cryptographically bound to the receiving device doing the recording so that

it is not removable and not itself subject to further copying before it is rendered unusable. The temporary copy should be encrypted in a manner that provides no less security than that of the Advanced Encryption Standard (AES) using 128-bit keys. Since rights associated with "Copy Never" content preclude making a permanent copy, the default expiration time of temporary recordings of "Copy Never" content should be 90 minutes. This also requires that the cable system provide a secure source of time to the digital cable receiver/recorder in order for it to securely manage time expiration of bound copies.

In the case of recordings of "Copy Once" programming by integrated PDRs, many of the same requirements for "Copy Never" content are also needed. In addition, these recordings must be remarked to "Copy No More" to prevent further copies from being made by downstream recording devices.

Finally, one of the most important missing features of current Digital Cable Ready products is the provision of a secure time source and a standardized means for signaling time expiration of bound copies. Incorporating this functionality into next-generation digital cable receivers with integrated recording capabilities is critical in supporting a wider range of time-shift, rental, and sell-through programming options for consumers.

LABELING STANDARDS FOR UNIDIRECTIONAL AND BIDIRECTIONAL DIGITAL CABLE PRODUCTS

Based on the bilateral-negotiated DFAST license, a broad array of unidirectional Digital Cable Ready products are beginning to be sold in the marketplace. Even though these devices incorporate a CableCARD slot, they will not be able to access interactive programming services, such as interactive Video-On-Demand (VOD) and impulse Pay-Per-View (PPV) offerings. If a successful conclusion is reached in the cross-industry bidirectional digital cable negotiations, a new bidirectional framework will be created producing a new generation of bidirectional digital cable ready products that incorporate advanced content protection, copy management, and device programmability. These features will better enable cable operators to provide a wide range of new interactive programming services, including early-window content, to cable subscribers purchasing these new bidirectional devices.

However, content owners are concerned that consumers must be properly educated about the more limited set of programming services available to a unidirectional digital cable receiver as compared to the wider range of new, interactive services that will be available to subscribers purchasing bidirectional digital cable products. Although the current market availability of unidirectional devices is helping to facilitate the Digital Television transition, content owners believe that consumer electronics manufactures and consumer electronics retailers must accept the responsibility for clearly labeling digital cable ready products and for educating consumers about the programming and interactive service availability differences. This is critical to help the customer make an informed purchase decision when considering whether to buy a unidirectional or an advanced bidirectional digital cable ready product.

SUMMARY

This technical paper has highlighted several important content protection considerations related to Digital Cable

Ready products. Addressing these issues is a critical step in maintaining the viability of cable television in the competitive and expanding market of digital content distribution. It will also better position the cable industry to launch new innovative programming services that can increase revenue, control churn, and expand the subscriber base. Content owners look forward to continued collaboration with the cable and the consumer electronics industries in addressing these issues that will lead to the introduction of exciting new digital cable products and program service offerings for consumers.