Audio Engineering Society

Convention Paper

Presented at the 118th Convention
2005 May 28–31 Barcelona, Spain

Content Protection for Digital Radio

Skip Pizzi[1]

[1] Microsoft Corporation, Fairfax, VA, 22030, USA
skippiz@windows.microsoft.com

ABSTRACT

The advent of digital radio broadcasting has brought about discussion of possible content protection requirements for the medium. While the issue remains somewhat controversial, a discussion of the technology can and should proceed. The technologies required are already developed and coming to maturity, and beyond their obvious potential application for the content-redistribution control preferred by published music copyright holders, such technologies also can provide new business model opportunities for broadcasters, such as subscription services. The technologies, applications and issues surrounding deployment of content protection in digital radio are briefly covered herein.

1. DEFINING CONTENT PROTECTION

Any discussion of content protection technology must first define a few key terms and illuminate some elementary principles.

Toward that end, consider the following points.

1.1. Conditional Access

The term *Conditional Access* (CA) represents perhaps the most basic form of content protection. It is typically applied on a “channel-specific” rather than a “content-specific” basis, meaning that it is used to simply allow or block access to a given real-time service. This binary approach (i.e., access or no access to the channel) applies encryption to the content at the source, and delivers frequent messages to the authorized receiver on how to decrypt it. Typically these messages are delivered every few seconds, so each single decryption state only applies to a small amount of content. This also implies that the typical CA system can be used only for real-time consumption of a channel’s content. (Some more recent systems have been adapted to accommodate time-shifted playback.)

Such a scheme typically also contains an authentication routine by which the receiver identifies itself as authorized to decrypt the content. This authentication method will vary widely depending on a number of factors, the most obvious of which is whether the receiver has any method of communicating back to the content source (“backchannel”), either permanently or occasionally.

1.2. Digital Rights Management

A different approach to content protection is taken by a newer set of technologies collectively referred to as *Digital Rights Management* (DRM)[1]. While, like CA, DRM also applies encryption to protect content, its processes typically are bound to a specific piece of content rather than applied to a delivery channel.

This implies that DRM can be bound to a given piece of content in advance of delivery (i.e., during production or mastering), rather than at the time of transmission, where CA is typically applied. Thus DRM-encoded content can flow through multiple content delivery paths and retain identical protection.

More importantly, DRM can include far more granularity of control than the simple binary real-time access/no access options of CA. The typical DRM system offers a rich set of usage rights (or perhaps more aptly, "permissions") that can be attached to a given piece of content at the option of the content owner or delivery-system operator.

Because such permissions are permanently attached to the content, the specified usage rights follow the content as it moves throughout the digital media ecosystem.

The rich permission set that can be communicated and enforced by DRM systems incorporates a range of traditional purchase or rental models, but with the ability to add fine-grained specifics to such allowed usage. For example, a given piece of digital media content could be delivered to a user who can then play it back an unlimited number of times for a period of one week, after which the content can no longer be decrypted. Or the usage rights could allow content to be played back only five times, but over an unlimited period of time, and so on.

In some cases, the playback quality of content can be controlled by a DRM system's usage rules. For example, systems may offer *selectable output control* (SOC), via which copying via analog outputs may be allowed, but via digital outputs may be disallowed, for example. Similarly, output for copying or playback may be constrained to lower quality levels than those at which the original file is stored (called *"downresing"*). For example, a stored 24-bit/96 kHz audio file might only be allowed to be copied at 16-bit/44.1 kHz resolution.

1.2.1. Rights Expression Language

Communicating the permissible usage rules associated with a given DRM-encoded content-acquisition transaction is typically performed via a Rights Expression Language (REL). Such a language attempts to communicate all possible usage cases in a consistent and efficient way.

A standardized REL has recently been adopted by ISO/MPEG under the MPEG-21 Multimedia Framework process[2]. This provides a good example of how a content rights holder can communicate the desired set of permissions associated with its content for a given type of transaction.

Of course, the same content could have different permissions associated with different transactional methods of access to it, just as one could either purchase or rent different copies of the same DVD title, for example. But once the transaction takes place, the specified usage permissions will remain with the content throughout its lifespan.

1.2.2. Revocation and Renewal

No content protection system is hackproof, so today's DRM systems typically include methods that make recovery from such inevitable attacks easily and pragmatically possible.

For example, if a particular user's terminal device is found to be compromised or otherwise used in contravention of the desired usage permissions, that device can be *revoked* from further content consumption or transactions by a DRM system.

If the overall encryption algorithm of a DRM system is revealed or otherwise compromised, a *renewable* DRM format allows content distributors to issue updates that return integrity to the system.

[1] In the digital radio environment, this acronym has a problematic collision with that of Digital Radio Mondiale, the digital radio format primarily designed for use at transmission frequencies below 30 MHz. Care should be taken to avoid such confusion in this context.

[2] ISO/IEC 21000-5:2004; see [9]

2. USING CA AND DRM IN DIGITAL RADIO

Much has been done to implement CA in broadcast systems, so these techniques are well known. Applying DRM to broadcasting is more recent practice, and less broadly understood.

It is possible to use either or both technologies in today's digital broadcast systems. CA is more appropriate for subscription services, in which once a user has paid a fee for a service, that user's addressable device is added to the list of authorized receivers and the appropriate messages are communicated to the device to allow it to decrypt transmitted content.

On the other hand, DRM may be useful for stored content, where a user records content via the broadcast service and adds it to a private collection. The attached DRM allows decryption of the content only on authorized devices (as with CA), but also only under defined circumstances, which may include actions performed asynchronously, such as time-shifted playback, possibly including playback on other devices to which the content has been digitally transferred.

The two approaches can even be combined, such that CA is used to allow valid subscriber access to a channel that contains DRM-encoded content, the latter being used to enable consumer recording and reuse under controlled circumstances.

In either case, encryption is applied at the source, so the transmitted content is scrambled, and content cannot be decoded by unauthorized receivers.

In some broadcast environments, however, transmission of encrypted content is not desirable or allowable. Therefore an alternative solution has been proposed for applying content protection without encrypting the broadcast signal or program content.

2.1. The "Broadcast Flag"

Such a system has been created for digital terrestrial television broadcasting in the United States. It is designed to allow free-to-air digital broadcasting to continue "in the clear" (i.e., unencrypted), but enables a system that limits audience usage of certain content.

Specifically, the proscribed usage is Internet redistribution of content, whereas other "fair uses" of the content by consumers are intended to be unaffected. This capability is enabled by the addition of a digital flag in the transmitted bitstream, and the enactment of regulation that all receivers must recognize the flag and prevent any such flagged content from being redistributed by consumers on the Internet. Thus this marker is referred to as the Redistribution Control Descriptor, but it (and the entire process associated with it) is more commonly referred to as the "Broadcast Flag." Transmission of the flag is described in detail in Advanced Television System Committee (ATSC) standards documents[3].

The behavior of consumer equipment that encounters content marked with the Broadcast Flag is specified in regulations issued by the Federal Communications Commission (FCC), the U.S. telecommunications regulatory body.[4]

In short, these behavior requirements are intended to permit fair use of marked content, but disallow "indiscriminate redistribution" of such content by consumers.

This behavior is enabled by the following process: Consumer DTV receivers sold after a given date must recognize the flag and apply content protection. (The protection system used must be selected from a list of FCC-approved technologies.) All other associated equipment sold after this date must also comply with this redistribution restriction, such that the protected content can only be decrypted under acceptable conditions (i.e., "fair usage" only).

Thus the Broadcast Flag process applies content protection at the receiver side, allowing some level of distribution control to be applied to content that is broadcast in the clear.

(Note that the Broadcast Flag rules are currently scheduled to go into effect for U.S. terrestrial DTV equipment sold after July 1, 2005, and at press time there were pending court challenges to these rules[5].)

2.2. Content Protection in the IBOC digital radio system

At press time, a draft standard for In-Band/On-channel (IBOC) digital radio broadcasting was being developed for use in the U.S. by the National Radio Systems

[3] ATSC A/65B; see [2]
[4] FCC 03-273; see [3]
[5] http://www.publicknowledge.org/issues/bfcase

Committee (NRSC). It is expected that FCC rules will subsequently be developed that are based on this standard.

In the meanwhile, current IBOC operations are governed by interim FCC rules, intended to stimulate broadcasters' evaluation and experimentation with early deployment of IBOC transmission equipment. First-generation IBOC receivers are slowly becoming available at relatively small supplies among U.S. retailers.

Neither the current interim FCC regulations on IBOC digital radio, nor the imminent NRSC standard specifies content protection in any form, although proponents of the IBOC system claim that such protection can be technically accommodated if required.

In anticipation of this possibility, the FCC issued a Notice of Inquiry[6] on the subject of digital radio content protection. While most responses to this Notice held that such protection was undesirable or unwarranted, the Recording Industry Association of America (RIAA) responded with comments[7] supporting the addition of a regime similar to the DTV Broadcast Flag for redistribution control of audio content broadcast via IBOC.

At press time the FCC had not yet issued any rulings on this subject or hinted at any upcoming decisions regarding the inclusion of such content protection requirements (or options) for U.S. digital radio broadcasting.

2.3. CA Framework in DAB

In [7], the WorldDAB Forum's Technical Committee is currently considering the addition of a Conditional Access Framework to the Eureka 147 DAB format. While the current DAB format[8] includes an option for CA, it is relatively complex and has never been commercially deployed. The system proposed in [7] is intended to replace the original system in backward compatible manner.

This new CA Framework would allow a standardized mechanism for adding CA to a DAB broadcast, but it would not specify a particular CA algorithm. Any CA vendor could adapt its system to operate within the framework, and thus a broadcaster could selectively add encrypted services for addressable receivers in a relatively cost-effective and predictable manner.

The CA Framework will also accommodate a flexible mix of encrypted and non-encrypted services on a single DAB ensemble or channel, as well as dynamic switching of encryption on any service, without affecting reception of unencrypted services on the same ensemble or channel, on either new or legacy receivers.

This implies that a broadcaster could, for example, keep a DAB audio service in the clear, but add an encrypted data service as a subchannel on the same DAB channel, which would only be receivable on authorized receivers equipped with the updated CA Framework. The encrypted service would remain transparently unavailable to legacy receivers as well as new CA Framework-equipped receivers that were not authorized for the encrypted service's reception, and would in no way affect either type of receiver's ability to receive the unencrypted service(s) on the channel.

It is expected that the new DAB CA Framework will be submitted to ETSI for addition to its suite of DAB standards sometime later in 2005.

Meanwhile, it should be noted that a proprietary CA system has been proposed for subscription DAB in Canada.[9]

3. CONCLUSIONS

While decisions on the appropriateness of adding content protection to digital radio remain business and/or political decisions, an exploration of the technical means for adding content protection to digital radio services is proceeding.

Although a Broadcast Flag-like mechanism can be supported – in which encryption is applied to appropriately signaled content at the receive end – a simpler, more reliable and more easily managed protection performance can likely be delivered by a system that adds encryption at the source.

Such protection can take the form of Conditional Access (which either allows or disallows the real-time reception of a given digital radio channel) or Digital Rights

[6] FCC 04-99; see [5]

[7] http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516213850

[8] ETSI EN 300 401; see [10]

[9] http://www.chumlimited.com/csrc/index.asp

Management (which offers a wide range of usage permissions to specific content items that remain bound to the content throughout its lifespan).

The business models thus enabled can provide expanded opportunities for broadcasters and audio purveyors to deliver high-quality content to consumers. Such technologies could also enhance the user experience of digital radio listeners by allowing richer and more convenient access to the highest quality audio content.

4. REFERENCES

[1] ISO/IEC JTC1/SC29/WG11/N5231: *MPEG-21 Overview v.5*; October 2002.

[2] ATSC Standard A/65B: *Program and System Information Protocol for Terrestrial Broadcast and Cable, Rev. B*; March 18, 2003.

[3] FCC 03-273: In the Matter of Digital Broadcast Content Protection, *Report and Order and Further Notice of Proposed Rulemaking*; November 4, 2003.

[4] NRSC-5: *In-Band/On-Channel (IBOC) Digital Radio Broadcasting Standard, Draft v6* (unpublished Committee Draft); February 2005.

[5] FCC 04-99: In the Matter of Digital Audio Broadcasting Systems And Their Impact on the Terrestrial Radio Broadcast Service, *Further Notice Of Proposed Rulemaking And Notice Of Inquiry*; April 20, 2004.

[6] In the Matter of Digital Audio Broadcasting Systems And Their Impact on the Terrestrial Radio Broadcast Service, *Comments of the Recording Industry Association of America, Inc.*; June 16, 2004.

[7] *Digital Audio Broadcasting (DAB); Conditional Access, v2.1.1* (unpublished Committee Draft); February 2005.

[8] Application Filed in Response to Broadcasting Public Notice CRTC 2003-68: *Supplementary Brief, CHUM Subscription Radio Canada ("CSRC")*; July 2004.

[9] ISO/IEC 21000-5:2004 (Ref. FDIS: SC 29 N 5543), *MPEG-21 Part 5*; April 1, 2004.

[10] ETSI EN 300 401: *Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers*; Second Edition, May 1997.