Advances In Content Management And Protection

Wim Mooij
Mindport

Abstract

With the accelerating adoption of digital formats in multiple application domains, it becomes possible to transfer content from one domain to another. Especially with the emerging home entertainment environment with digital storage devices, content can flow between a large variety of electronic devices. Protecting the interests of all value chain participants is the challenge of a new set of technologies called Content Management and Protection. This includes security solution from multiple application domains. Content Management and Protection is critical to the industry growth in the digital content and information era.

INTRODUCTION

Digital Broadcasting is now supported by a wide range of globally adopted specifications for consumer and professional Television equipment. With the migration of broadcast signals to the digital domain, the traditional distinction between various media applications disappears. After all, who can tell the difference between an audio, video and data bits? With the advent of internet, digital television and digital telephony many networks now carry only digital data streams. It then becomes possible to transport the same bits over new distribution infrastructures creating new potential value propositions for network operators, consumers and intellectual property creators. The digital intellectual property in the digital content may represent significant (future) commercial value to participants in the value chain. Content management and protection system aim to enforce the copyrights and/or other intellectual property contained in the content. Such systems need to operate in a rapidly changing environment, and no longer can ignore the move of broadcasting into the "e-Environment".

COMMERCIAL ANALYSIS

Content in digital form can be transported over a wide variety of distribution and communication media. This facility also is available to the consumer. The same content thus may appear in a variety of infrastructures and consumer equipment. This great flexibility allows greater freedom, but with that freedom also comes a vast increase in unintended commercial side effects. Especially the ability to make perfect copies of digital content in any of the domains and the capability to introduce such copies into another player infrastructure completely changes the underlying assumptions of many distribution regimes. Often such implications are only discovered after the fact. It thus is necessary in many cases to re-visit the complete application and determine the basic commercial rules that make it a viable business proposition to all value chain participants. With these basic rules established, it becomes possible to devise a suitable content management and protection regime.

A key observation is that any content management and protection regime takes away some freedom of use from the consumer. In many cases this freedom would allow the consumer to seriously violate the commercial rules driving the application. The

capability of copying and distributing amongst friends without some form of compensation to the intellectual property creators is one such limitation. In all cases the chosen content management and protection system should consider the capabilities of equipment in other domains. So, it is a fallacy to assume that copying is not possible because all copying devices in one application domain, have some build in copy restriction mechanism. If such a mechanism is not implemented in another application domain, it may be possible to make unrestricted copies.

Content in the digital domain may have a substantial value associated with it. The easy copying and distribution of digital information requires that the content itself is protected in a persistent manner. Copies of protected content then are not a problem, as the intellectual property is safe in the protected form. The consumer can play the protected content on any rendering device as long as that device is capable of dealing with the protection layer for the protected content. As the rendering quality of content continuously improves, it becomes increasingly relevant to extend the content protection into the "analog" domain. This aims to prevent the removal of the protection layer through a re-encoding process.

In some CMP systems a removable element such as a smartcard may be used to implement some or all functions of the content management and protection (CMP) system. Other CMP systems utilize periodic on-line communications to implement some protection system functions. Although implementations of CMP systems vary widely, they all share the basic function to enforce the business rules associated with the use of the content.

In an e-Environment where all content is digital and all networks are digital, content can flow very easily between networks and devices. It is unlikely that a single CMP system will be able to deal with all existing and future applications. Hence, CMP systems have to find a way to work with other CMP systems in order to facilitate this natural flow of content.

The main challenge is to make this protection framework easy for the most frequent types of consumer usage of the content. It is a widely held belief that consumers only will accept content protection if this is realized in an interoperable fashion and permitting horizontal market structures. Consumer interests are protected by commercial interests of the industries involved and by possible regulatory involvement. As the need for content protection increases due to a rapidly growing abuse of intellectual property in content, a substantial effort is required to create and implement an open content management and protection system infrastructure. Several standards setting initiatives are now dealing with (aspects of) the content management and protection issues facing a wide range of application platforms.

TECHNICAL ANALYSIS

A content management and protection system architecture operates in an environment where multiple content players are interconnected through an in-home distribution network. An example diagram of such a network is shown in Figure 1.

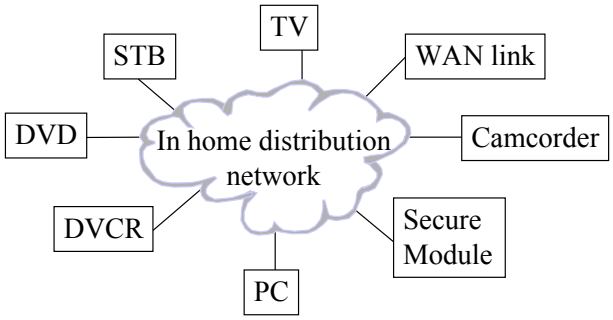

Figure 1 Diagram of the in-home distribution network.

It is desirable in such an environment that content can be shared between content players. During content move and/or copy operations, the material should remain protected. The enforcement of the business rules associated with the content is the task of the CMP System.

APPLICATIONS

There is a continuously expanding range of applications that distribute content. Most of these applications are under control of some form of CMP System. Several distribution infrastructures can be identified.

- Broadband (broadcast)
- Internet
- Wireless networks
- Pre-packaged media

In all of these networks a rich variety of media types can be identified such as real time stock price information, premium movies, archived newspaper articles. In all cases the current and future value of the content differ substantially. Hence the CMP System features also have corresponding differences. Similar differences exist in the payment structure. In the broadcast domain the following different payment structures exist.

- Free TV
- Subscription TV
- Pay per use
- Near Video on Demand
- Video on Demand
- Services that add value to those mentioned above, e.g. paid-for Electronic Program Guides and other such services

Similar differences in service types and payment structures apply to other content delivery structures, further increasing the range of options that CMP Systems need to support.

The threat model for each commercial application also varies significantly. Early releases of premium movies have an entirely different value compared to highly volatile stock price information. Hence the required security features of the CMP System can differ some orders of magnitude. Thus, it is not surprising that all attempts at defining a single CMP System for a reasonable range of applications is impossible.

INTEROPERABILITY

There is a world of proprietary application domains that each have their own governance structures defined by a set of CMP systems. An example of a such a set of CMP Systems is traditional Conditional Access Systems for broadcasting applications. Interoperability among such CMP systems creates a structure where operators and consumers benefit from new commerce structures.

An early attempts at interoperability of CMP Systems is the SimulCrypt concept developed in the European Digital Video Broadcasting project. SimulCrypt is a mechanism where multiple business rule sets are linked to the

same broadcast material. Although this works within a broadcast environment, it does not facilitate interoperability with other digital content application domains.

A multiple application domain interoperability between CMP Systems can be based on the specifications developed in the Open Platform Initiative for Multimedia Access (OPIMA). OPIMA provides tools to exchange a set of authenticated identifiers, called OPIMA Credentials, to enable Protected Content to flow within and between application domains. When OPIMA peers have an on-line connection, the OPIMA Credentials can be exchanged prior to the delivery of the Protected Content. OPIMA Credentials and CMP Systems can be combined with the Protected Content when the delivery infrastructure does not support on-line connections (e.g. storage media, broadcast media). The OPIMA Credentials contain necessary information that may be used to enable Protected Content flow between application domains. For a given instance of Protected Content that is intended for consumption in two application domains, a Broadcast conditional access domain and an Internet music delivery domain, OPIMA Credentials from both domains are associated with the Protected Content.

OPIMA enables generic interoperability between different applications, devices and CMP systems belonging to different *compartments*. A compartment is a class of OPIMA enabled devices that share some common elements in their CMP interfaces and/or architectural components. For example, digital TV broadcasting can be considered as a compartment, which in turn contains other compartments defined by specific CMP system. Content does not necessarily flow between all compartments, however, OPIMA provides a schema for facilitating content flow between compartments.

The OPIMA architecture is peer-to-peer. The core OPIMA element is a peer called the *OPIMA Virtual Machine* (OVM). OPIMA provides protocols and infrastructure components that enable secure (trusted) inter-operation amongst these elements.

This section describes an in terms of. Figure 2 depicts the functional units of the OPIMA Peer.

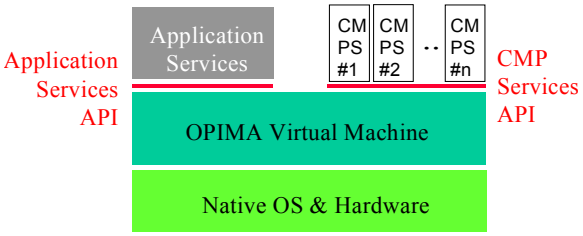

Figure 2 Diagram of the OPIMA peer

The OPIMA peer contains a group of basic functional elements that implement the backbone of trust. This is called the OVM. The basic functionality of the OVM allows for application-specific extensions. The OVM is responsible for establishing authenticated, secure channels amongst OPIMA compliant devices. The OPIMA Application Services API allows services to communicate with the OVM and the CMP system installed in the OVM. CMP Systems can access the OVM functions through the CMP Services API.

The OPIMA specification alone is not sufficient to achieve horizontal markets. This requires further specifications to be defined in a particular application domain. OPIMA solves the problem of permitting content to flow across domain boundaries and thus solves a major problem in the digital content environment.

RENEWABILITY

One of the fundamental assumptions for any CMP System is that eventually someone will compromise the system. This follows directly from the observation that it is possible to copy any system implementation given sufficient resources (time, money and skills). If the eventual breach of a CMP System is an integral part of its design and implementation, it will handle such situations more efficiently. In most cases, the CMP System has some flexible response strategy to deal with such security breach eventualities. This strategy allows the renewal of part(s) of the CMP System with minimal impact to operations and the consumer. This section analyses various implementation options for CMP Systems and describes how these impact the renewability of the system.

The general structure of a Content Management and Protection (CMP) System is assumed to use classic cryptography. Other techniques such as watermarking possess similar security threats and implementation principles. For the sake of simplicity this analysis only deals with the case of cryptographic technology CMP Systems. The key components of such a system are shown in the following diagram.

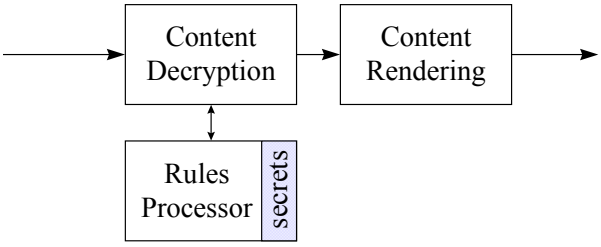

Figure 3 Diagram of a CMP System

Before the content can be rendered (decompressed, D/A converted etc.), the CMP System needs to remove the protective encryption layer around the content. This is based upon some decryption function. The keys to the decryption process are provided by the rules processing engine, which decodes the business rules associated with the content. These business rules can be enforced by the rules processing engine as it uses secrets to decrypt the keys that will unlock the content. Obviously, these secrets need to be protected using tamper resistance techniques. The key issue is the implementation of the CMP System. There are three main trends:

1. Integrate all three elements onto a single silicon device.
2. Integrate content decryption and content rendering onto a single device and use a separate rules processor.
3. As option 1, but make provision for a separate rules processor

The arguments in favor of the first implementation is that this makes it the most difficult (and expensive) for an attacker to find the relevant secrets to compromise the player infrastructure. And even when an attacker manages to find the secrets, it is not possible to introduce a breach into the system without breaking into the integrated device at the chip level. Oddly, the complexity of distribution of a breach introduces a weakness in this implementation. As soon as the secret has been obtained, it becomes necessary to build a modified player that bypasses all security features to distribute the security breach As technology progresses at such high speed, such solutions become increasingly feasible over time. It is thus inevitable that such devices will become available. The pricing of illegal devices can be low as no licenses are paid. The main attraction is that these illegal devices play legitimate content. Thus, the CMP system implementation forces the security breach to be distributed using a alternate (illegal) device infrastructure. As these new devices

are outside the scope of the legitimate content distributors, only legal counter measures are possible. Note that counter measures such as software downloads and revocation don't work when the security system is completely known. Market dynamics at some point will cause the illegal players to grow very rapidly, encouraging manufacturers to also cut corners where security measures are concerned. Over time, the complete device infrastructure is lost to legitimate content distributors. Note that this process accelerates where software receivers are possible.

The second CMP system implementation method offers a slightly lower cost to the attacker as only the replaceable rules processor needs to be reverse broken into. And even worse, the implementation provides an easy way for a security breach to be distributed to the legitimate player infrastructure. It would seem that this is a worse situation than the first implementation. Again, appearances deceive. The distributor of legitimate content now can upgrade the rules processor, driving out the security breached version as this cannot process new content. This will quickly reduce the level of illegal rules processors. The attackers then are forced to break the legitimate rules processor and the cycle repeats itself. Obviously, there is a cost involved in the replacement of rules processors. The important effect of this implementation is that the infrastructure of players always remains legitimate. Only the rules processor can become illegal from time to time, but also can be recovered as a legal content player. This way the security breaches can be contained and controlled without losing the entire device infrastructure.

The third implementation form is a combination of the first two. It pairs a slightly higher burden for the first attack and still allows the infrastructure to recover from a security breach, if implemented through the rules processor interface. If the security breach is distributed through the method described in the first implementation method, the recovery through a rules processor upgrade no longer is possible. This depends upon the discovery of existence of this interface by the attackers.

CONCLUSION

This article describes the challenges placed on CMP Systems in the converging world of digital content and networks. It describes the environment were perfect copies are just one mouse click or a remote control button push away. Supporting the consumer reasonable demand for novel uses of the new network and content possibilities, places strong demands on CMP Systems. They now also need to consider how they can work with competing systems in other application domains. They need to consider how they can deal with security infringements. CMP Systems also need to be flexible to support new business options and new commerce structures. The article describes these problems and shows some recent advances in the CMP Systems that address these important issues for a bright digital content future.

REFERENCES

1. ISO/IEC 13818 part 1, MPEG-2 Systems.
2. IPMP FAQ, MPEG-4 IPMP
3. http://www.cselt.it/ufv/leonardo/opima
4. http://www.dvb.org

ACKNOWLEDGEMENTS

The author would like to thank his colleagues for their contributions to this work. Many of the described concepts are from discussions in standardization activities. This work is supported by beautiful girls in Amsterdam.