CONTENT PROTECTION: FROM PAST TO FUTURE

DIEHL Eric
THOMSON R&D France
Corporate Research, Security Laboratory
Rennes, France
Eric.diehl@thomson.net

Key Words

Content protection, Conditional Access, Digital Rights Management, Copy Protection

Introduction

Since about twenty years, the value of audiovisual contents continuously increased. Digitalization of contents has simplified and empowered the creative process, has multiplied the number of delivery channels, and made easier the consumption of contents. Digital contents are easier to distribute. Digital contents are easier to consume. Digital contents are easier to copy. All these factors favoured the hackers.

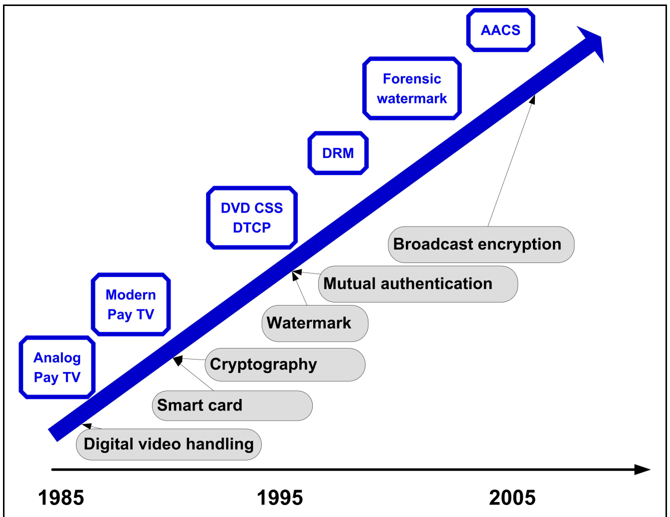

Figure 1: Advances and content protection

Content owners needed their content to be protected against piracy. Fortunately, academic world provided numerous scientific advances that content protection designers used for new schemes. The race was starting.

This document focuses on the protection of audiovisual contents. Nevertheless, many of the described techniques are applicable to other types of content such as games or eBooks. The first sections introduce the history of content protections. It gives a quick overview of the current techniques and some deployed systems. Last section proposes a list of research topics that may influence the design of future content protection systems.

Twenty years ago

Scrambling the content

The history of content protection started with the advent of Pay TV operators. In 1984, French Canal+ launched its first subscription based channel. The video was analog and the transmission was terrestrial. The protection principles were rather simple. Content was scrambled, i.e., the content was modified. Digital technologies allowed more powerful key-based scrambling techniques. For instance, Canal+ added a variable delay after the sync signal of each video line. An algorithm using a key defined the amplitude of the transformation. If the user dialed the same key, then the decoder descrambled the content, i.e., the decoder reversed the applied transformation. The key was changing every month. Quickly, the first schematics of pirate decoders appeared. It was rather easy to find the short monthly key by some trials. In 1985, HBO used Videocipher II to protect its content. Here also, very quickly pirate decoders were available with distribution

Published in Shaping the Future : 10 years of Irisatech, INRIA, 2007

channels for the monthly key. Piracy reached quasi-industrial organizations. The hard lessons were that *a key-based system needs serious scrambling and long enough keys*. This was known for more than a century as Kerckhoffs's law [5].

The rise of cryptography

These first commercial deployments highlighted the need of longer keys and a mean to protect these keys. End of 80s, the first smart cards were available. Two European Conditional Access systems (CA), EuroCrypt and VideoCrypt, draw the foundations of modern content protection. The systems used the "universal" scheme illustrated by Figure 2 [8]. Scrambling applies cryptographic symmetric encryption to the clear content. A primary key protects scrambled content. To retrieve clear content, the device applies the decryption algorithm with the same primary key. Only authorized devices should have the primary key. This is the role of key management. It cryptographically protects the primary key and generates data that we will call the secondary key. Only authorized devices should be able to derive the primary key from the secondary key.

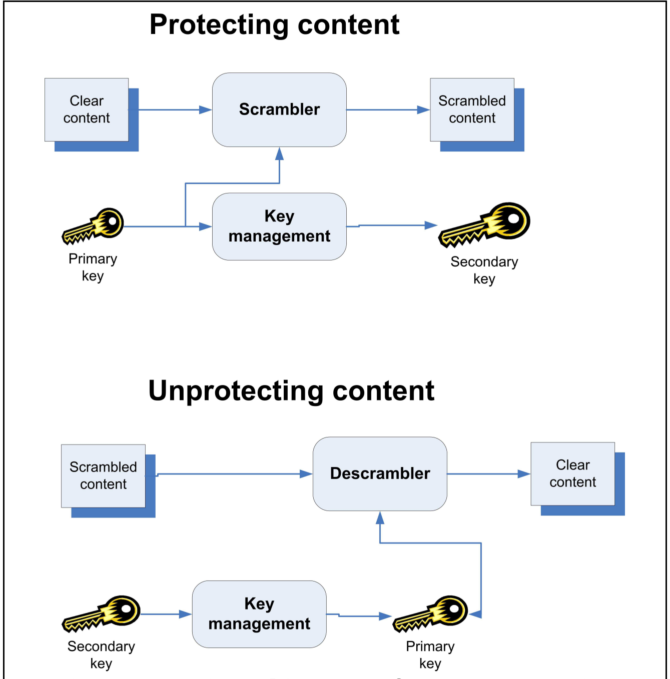

Figure 2: Basic architecture of content protection

Obviously, these new systems used more serious scrambling schemes such as line cut and rotate, or line shuffling. Nevertheless, the major improvement came from the use of smart card. Smart cards allowed:

- The use of modern cryptography for key management
- Tamper resistant hardware to protect the keys; Reverse engineering protected hardware requires far more skills and materials than reverse engineering software.
- Renewability; an initial assumption was that hackers would break the system, but not the scrambling method. Changing the smart cards was a way to answer these future attacks. This approach has proven to be successful.

In 1995, Digital Video Broadcast group (DVB) standardized the way to protect MPEG2 transport streams. It defined a common scrambling algorithm DVB-CSA, and the signalling for proprietary Conditional Access systems (ETR 289). All DVB decoders use the same scrambling algorithm and use smart cards that hold proprietary key management. This system is still successfully in exploitation.

Protecting DVD

The red book, the standard specifying CD audio, does not define any copy prevention system. Audio tracks are in the clear. With the advent of computers, and recordable CD-ROM, it was easy to rip an audio CD. When the movie industry decided to replace the VHS tape by DVD, it wanted to avoid the mistakes of the audio industry.

Thus in 1995, Motion Picture Association of America (MPAA) launched the Copy Protection Working Group (CPTWG) [1]. Since then, every two months, experts from studios, consumer electronics manufacturers, and IT industry meet to design solutions to protect digital content. Very quickly, CPTWG generated three main advances in content protection.

The first outcome was the Content Scramble System (CSS). This standard defines the encryption of DVD. It uses symmetric cryptography to protect the video content. In 1999, John Lech JOHANSEN, also called DVD John, published DeCSS a software that bypassed CSS protection. There was no way to recover from this lethal attack. The hard lesson was that *renewability and revocation were mandatory features for any content protection scheme.*

Quickly CPTWG identified the threat of analog hole [4]. Scrambling protects content while digital. Nevertheless, final rendering converts digital content into analog. Once analog, content is not anymore protected. Therefore, content should carry in a protected way copy control information such as copy never, copy once or copy free. The suitable solution used an emerging technology: digital watermark [1].

As illustrated by Figure 3, digital watermark invisibly embeds a message into the content. The message should survive many transformations such as digital to analog conversion, multiple compressions, or resizing. Analog inputs of recorders would check the presence of eventual watermark and act correspondingly. Ten years later, CPTWG still struggles to select one unique technology. Meanwhile, watermark technologies drastically enhanced and its usage widened.

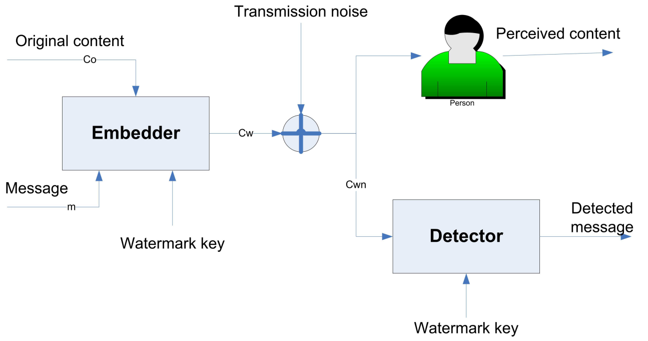

Figure 3: Principle of watermark

The third outcome of CPTWG is the concept of home network. DVD player would have digital output to transfer content to new digital recorders, or TV sets. These home networks should not carry content in the clear. The first candidate was Digital Transmission Copy Protection (DTCP). DTCP provides link encryption between two devices [9]. The system uses more sophisticated cryptography schemes. For instance, DTCP introduces mutual authentication and revocation lists. A source device sends protected content only to an authenticated sink device. Furthermore, it is possible to revoke compromised devices. Today, all current schemes use these concepts.

At the same time, THOMSON introduced a new concept: the domain [10]. A domain is the set of devices belonging to the same family. Within a domain, consumers have seamless access to all their contents. Exchange of content between domains is strictly controlled. Although provocative at its inception, the notion of domain is now accepted and present in many current initiatives such as DVB-CPCM, CORAL or OMA.

The last decade

The birth of DRM

End of 90s, two pioneer companies invented a new concept: Digital Rights Management (DRM). ContentGuard and Intertrust extended notions created by conditional access systems but with different environments and constraints. The main evolutions were:

- More complex usage rights
- Two-way communication
- Software based client

CA used very simple usage rights such as subscription, or Pay Per View. DRM supports more complex schemes such as “view n times”, “view for a given period”, or “copy m times”. These usage rights require a language so called Rights Expression Language (REL). The most known languages are XrML or ODRL.

Pay TV was designed for broadcast environment, i.e. one-way communication. Of course, return channels offered a limited two-way communications. Unfortunately, many Pay TV decoders are never connected to their return channel. DRM assumes that the communication is two-way. For instance, the DRM client loads the secondary key of Figure 2 from a remote license server. Two-way communication offers many advantages to the security designers, e.g. validation of the genuineness of the DRM client.

One of the biggest security challenges is that the DRM client is purely software based. Reverse engineering software is easier than reverse engineering hardware. Thus, they are easier target for hackers than CA smart cards. Currently, most of largely deployed DRM systems have been broken.

DRM uses the same content protection techniques than CA. Furthermore, the difference between DRM and CA is blurring. For instance, next generation of CA will support personal video recorder and offer complex usage rights like DRM. The current trend for IP distribution is cardless CA like DRM.

The growing scope of watermark

Although initially foreseen to carry copy control information, watermark found a new type of application: forensic watermark. Internet provides an easy and cheap distribution channel. Finding movies of excellent quality before their actual launching dates is extremely easy. These movies are often screeners. Screeners are movies distributed to privileged viewers for instance for awards, or critics. Normally, these screeners are for the exclusive use of these recipients. Unfortunately, screeners are sometimes posted on Internet. Watermark embeds the identity of the recipient. Thus, it is possible to identify the leaking source in case of illegal posting to Internet. Forensic watermarks currently protect most of screeners for awards. Forensic watermarks more and more protect content while in post production [11]. Both audio and video can be watermarked.

AACS

In 1993, FIAT and NAOR found a new concept: broadcast encryption [5]. This family of key management is perfect for prerecorded content. A central authority delivers a set of keys for each device. The content provider defines the list of devices authorized to access content. Broadcast encryption builds a data structure called Key Block. A device, pertaining to the authorized list, inds he primary key by applying a mathematical calculation using its set of keys and Key Block. A device, not pertaining to the authorized list, cannot find the primary key using the same calculation. The key management both protects the primary key and manages the revocation. Content defines the devices that can access it. Broadcast encryption eliminates revocation lists.

Since 2006, broadcast encryption is one of the main elements of Advanced Access Content System (AACS). AACS is the copy protection system of HD-DVD and BluRay discs. AACS is currently the most complex copy protection system. AACS embeds many technologies such as broadcast encryption, AES, forensic watermark, encrypted bus for drives. Unfortunately, hackers already exploited weak implementations of players [1]. Nevertheless, AACS has tools to counter these attacks. The lesson is that *a theoretically secure system may be defeated if its actual implementation is weak.*

The future

Content protection will always be a race between designers and hackers. To stay ahead, designers will need new security tools. This section describes some promising techniques that once mature may empower the designer's toolbox.

Formal analysis: Once a security protocol designed, designers have to check that the protocol fulfils the security requirements. Formal proof is a useful tool. Unfortunately, its use currently requires high mathematical skills. Industrial practitioners need simpler tools. The description of the protocol must be simple, and the declaration of the requirements must be even simpler.

Tamper resistant software: In the future, electronic devices will execute secure software. Designers need to be able to trust the executed software. Thus, designers must have tamper resistant software or at least tamper detection software. The tools will have to be parametized to define the level of expected security, the real time constraints, and the assets to protect with different risks.

Validation of implementation: Too often breakdown comes from weak implementation. Designers need tools that coupled with database of known attacks and errors, will automatically challenge the tested implementation. Buffer overflow attack is a typical implementation error. Good software practice could easily eradicate it. Unfortunately, it is not often the case. How can we test this vulnerability? Side channel attacks, such as Differential Timing Attack, Differential Power Attack, or Branch Predictive Attacks [5] are powerful attacks. How can we ensure that implementations are robust against them? With the raise of tamper resistant software, it will be mandatory to know the real level of robustness against different profiles of hackers.

Trust management: more and more secure systems will interoperate. Interoperability requires that different trust models interact. DRM will be acceptable only if interoperable. Tools should identify the point of failures generated by slightly different interacting trust models. Furthermore, there is a need to materialize in a user comprehensive ways the notion of trust. How many people properly handle a message from their browser informing that the certificate of the site is perhaps not trustable?

Processing friendly encryption: More and more, content will be scrambled. While content remains encrypted, it is safe. Unfortunately, contents may have to be modified, e.g., editing, compression in another format or addition of a forensic watermark. With current encryption schemes, it is mandatory to first decrypt, then to apply the expected modifications, and finally to re-encrypt. This transformation in the clear is a vulnerability point. Research should explore new schemes that would not require preliminary decryption for some transformations.

Many other subjects could provide new tools for content protection designers such as white box cryptography, or secure schemes for software renewability.

Conclusions

Digitalization of content and Internet offer many advantages to both content providers and consumers.

It creates also a new playground for hackers. Since about twenty years, designers of content protection systems and hackers of content protection systems compete in a thrilling race. Research has already provided tools to the designers such as cryptography, watermark, or tamper resistance. Many topics will in the future offer new tools for this race.

References

[1] COURTAY O., KARROUMI M., ***AACS under fire,*** in Security Newsletter #5, Spring 2007, THOMSON

[2] COX I., MILLER M., BLOOM J., ***Digital watermark,*** Morgan Kaufmann Publishers, 2001

[3] DELP E., ESKICIOGLU A., ***An overview of multimedia content protection in consumer electronic devices***, in Signal Processing: image communication, 2000

[4] DIEHL E., FURON T., © ***watermark: closing the analog hole***, ICCE 2003

[5] FIAT A., NAOR M., ***Broadcast encryption***, Proceedings of Crypto 93, available at http://www.wisdom.weizmann.ac.il/~naor/PAPERS/broad_abs.html

[6] JOYE M., KOC C., ***Side channel attacks against OpenSSL***, in Security Newsletter #5, Spring 2007, THOMSON

[7] KERCKHOFFS A., ***La cryptologie militaire,*** *Journal des sciences militaires*, vol. IX, Janvier 1883

[8] Mc CORMAC, ***European Scrambling System***, Volume 5, Waterford University Press, 1996

[9] http://www.dtcp.com/

[10] http://www.smartright.org/

[11] http://www.cnc.fr/Site/Template/T8.aspx?SELECTID=2531&ID=1661&t=1

Published in Shaping the Future : 10 years of Irisatech, INRIA, 2007