SmartRight**: How smart cards fight video piracy**

Eric Diehl, Sylvain Lelievre

THOMSON multimedia Corporate Research, BP19, 35511 CESSON, FRANCE,
Phone: +33 2 99 27 30 00, Fax: +33 2 99 27 30 01
diehle@thmulti.com;lelievres@thmulti.com

Abstract. ***SmartRight*** system offers an end-to-end protection against illegal copies within a digital home network. On one end, smart cards control the entry to the home network. On the other end, smart cards control the rendering. Furthermore, ***SmartRight*** system introduces the innovative notion of Personal Private Network. This notion offers a high level of flexibility for consumption of contents within the home network. This paper describes the associated key management.

Introduction

Digital world is an emerging reality. It is the result of fantastic new technologies that ease consumers' life. For example, digital technology facilitates transfers of movies between devices in the homes, or between home networks, e.g. through the Internet.

As a consequence, digital world allows copies of a given content (movie, song, video game software…) which remain as pristine as the original one, unlike in analog world where successive copies are degraded in quality. This bears severe consequences for the content industry if no high-level protection is made available.

There are three categories of pirates [1]:

- Organized and well fund pirates; they produce and sell pirated physical goods. No technological answer can stop them. Only the legal answer is efficient.
- Garage pirates; they mainly search the exploit. They provide pirated materials in electronic format on the Internet. Robust technological answers may slow them down. Nevertheless, they will always get rid of the protection.
- Ant pirate; they use simple devices or tools provided by garage pirates. They are mainly consumers of pirated goods and may help to the spreading of the hack. Simple technological answers or cumbersome circumventing processes may rebuke them.

The first category is a serious threat to content owners. Three days after the launch of "Star Wars: Episode 2", the first video CDs were on sale in Asia. The two last categories of pirates represent another threat. The possibility to post or receive content from Internet, especially through peer-to-peer networks is frightening. In 2001, approximately 99% of music files available online were unauthorized [3]. The day that "spider-man" opened in theaters, the online trading population soared to over 9 million simultaneous users, of which more than 2.5 were observable on IRC—about five times the norm [2].

With the advent of digital recorders connected through digital buses, the threat becomes even more serious. Future consumer electronic devices will be connected together through digital home networks and connected to the external world through digital links. ***SmartRight*** system proposes an end-to-end copy protection mechanism within the digital home network.

SmartRight approach

What is a digital home network?

A digital home network is a set of devices connected through digital links that receive, store, and render digital contents. Digital contents may be video, audio, or program files. The links will be either wired (for instance IEEE1394, Ethernet, …) or wireless (for instance 802.11b, Hiperlan2, …). A same network may use different types of digital buses.

Furthermore, a digital home network may link devices located in different geographical locations (for instance summer house), and portable devices that only intermittently connect to the network.

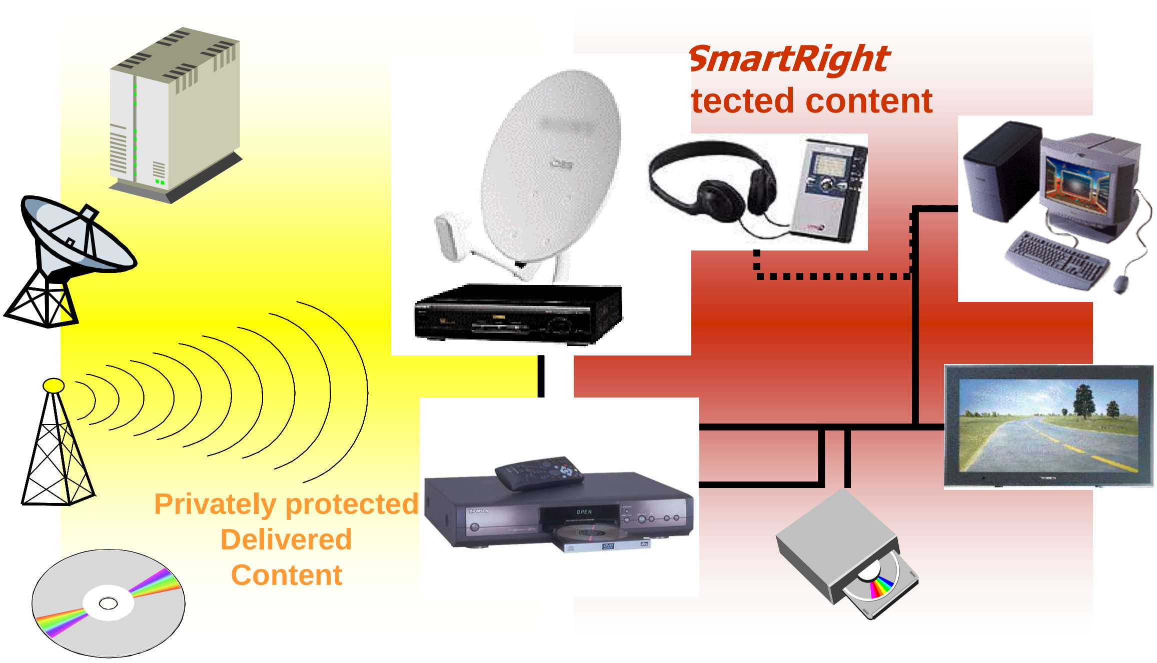
With such a versatile definition of digital home network, assembling device-dedicated security technologies together with link-dedicated security solutions would generate a piecemeal solution. This would be necessarily weak. Only a global copy protection solution common to all the elements of the network can work. ***SmartRight*** system proposes such a global solution.

End-to-end protection

SmartRight system clearly distinguishes the means used to protect the content from the means used to control the rights to access the content. Within the home network, controlling the rights to access the content is the responsibility of Conditional Access (CA), or Digital Rights Management (DRM). Within the home network, protecting the content and controlling copies is the responsibility of ***SmartRight*** system.

In ***SmartRight*** architecture, content providers deliver scrambled content to one end of the home network through access devices. Typical examples of access devices are set top boxes, DVD players, or Internet gateways. CA and DRM control the access to the content. Once the access granted, access devices do not descramble the content but send it scrambled in the home network. They securely package the keys needed to descramble the content together with the usage rules for copying. On the other end of the network, presentation devices unpack the descrambling keys and check the associated rules. If authorized, presentation devices descramble and render the content. Typical examples of presentation devices are digital TV or mp3 players.

Thus, the content is never descrambled within the home network. This limits the points of vulnerability of the system. Furthermore, it solves the issue of storage. Content being self-protected, there is no need for secure storage. Storage units act as simple bit bucket.



Where are the smart cards?

If we assume that the scrambling methods are secure, then security relies on the secrecy of the descrambling keys. Smart cards protect these keys. Access devices package the descrambling keys by smart cards so called converter cards. The keys are in a data structure called Local Entitlement control Message (LECM). In the case of CA, the creation of LECM occurs in the card hosting the CA. Presentation devices unpack LECM and control the copying usage rules by smart cards so called terminal cards. Every ***SmartRight*** TV set has an associated smart card.

The rationales to use smart card are twofold:

- Tamper resistance of smart cards offers a secure environment to handle descrambling keys, and secret keys needed for the key management. Furthermore, it guarantees a trusted behavior of main elements of the system.
- Any system will be hacked one day. Therefore, renewability is mandatory. ***SmartRight*** security is entirely in smart cards. Replacing the smart cards is one potential answer to a serious hack. This is current practice in conditional access domain.

An innovative key management scheme

Introduction

SmartRight system introduces the notion of Personal Private Network (***PPN***). The PPN is the set of devices belonging to a customer and linked by a digital home network. To build such PPN, all terminal cards of a PPN share the same secret called the Network Key (***Kn***). This secret key protects the LECM. Two PPNs cannot interoperate, that is to say that two PPNs cannot share contents.

The problem is to provide every terminal card of a PPN with the same network key. One additional requirement is that there is no connection to a central database. The key distribution is done thanks to a protocol based on messages exchanged between the cards, through the device. The cards check the received messages and eventually send back messages to the other cards.
The ***key management*** is launched at the network initialization, when a new device is detected on the network. First, the network consistency is checked by verifying that all terminal cards have the same ***Kn***. Then, if a new presentation device is present, its terminal card receives ***Kn***.

Description of the cards

Terminal card content

Each terminal card holds the following information:

- One asymmetric key pair called terminal key pair (a private key and a public key); the public key is embedded in a certificate called terminal certificate (***TC***). This key pair is generated and loaded prior to the delivery and is different for each terminal card.
- A certification authority public key, common for all terminal cards; It is used to verify the validity of other terminal certificates.

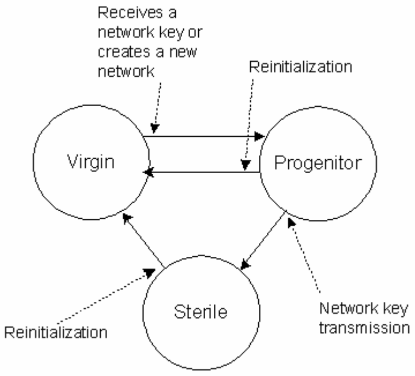
Each terminal card belonging to a PPN holds the additional information:

- The network key (***Kn***). The network key is either picked at random at the network creation or transmitted by another terminal card.
- One public data called network identifier (***Nid***). This identifier is a public value related to the network key (e.g. its hash value).

Terminal card states

A terminal card has three possible states:

- "Virgin", if it possesses no network key. It belongs to no PPN.
- "Progenitor", if it possesses a network key and can transmit it to another terminal card. Only one Progenitor card should be present in a given PPN.
- "Sterile" if it possesses a network key but cannot transmit it to another terminal card.



When delivered, a terminal card is virgin. It becomes progenitor when it receives a network key ***Kn*** from another progenitor terminal card or when it is the first card installed in the PPN. It then creates the Network Key ***Kn***.
A progenitor terminal card becomes sterile once it transmitted the network key to a virgin terminal card.
When disconnected from the network, a terminal card remains in the same state.
The user may reinitialize a non-Virgin terminal card to Virgin.

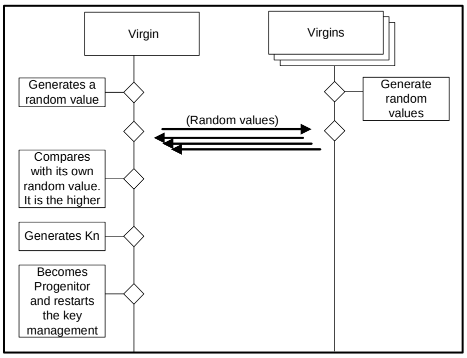
Key management process

Network consistency check

The goal is to check that all progenitor and sterile cards hold the same ***Kn*** and that there is only one Progenitor in the network. Each card broadcasts its ***TC*** along with its ***Nid*** (***Terminal Progenitor*** or ***Terminal Sterile*** message) and checks the messages they received from the other cards. If the check failed, the network cannot be initialized and the devices are blocked.

Network creation

When the first presentation device connects to the network with a virgin card, the network key must be created. The virgin card randomly generates ***Kn*** and becomes progenitor.


Virgin
Virgins
Generates a random value
Generate random values
(Random values)
Compares with its own random value. It is the higher
Generates Kn
Becomes Progenitor and restarts the key management

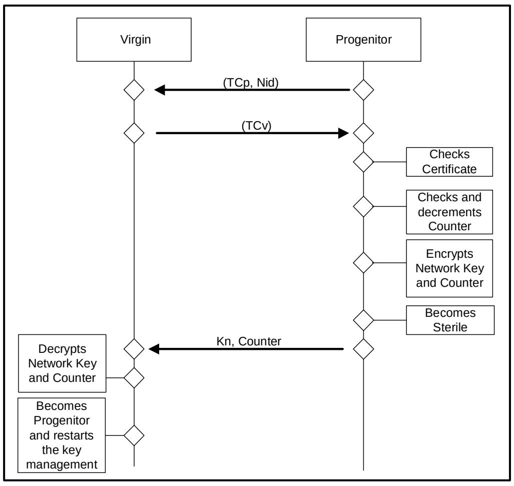
If several virgin cards are present in the network, an election process chooses the card that will become progenitor. Each card broadcasts a random value (***Virgin Random*** message) and the card that sent the higher value wins. The network is then created and the normal key transfer is performed to initialize the other virgin cards.

Network Key transfer

The network key transfer gives the network key to a virgin card. It occurs if there is at least one virgin card in the network and if one and only one progenitor card is present.

When a virgin card receives a ***Terminal Progenitor*** message, it returns its ***TC*** (***Terminal Virgin*** message). Upon reception, the progenitor card encrypts ***Kn*** with the Virgin public key, sends it to the virgin card and becomes Sterile. The Virgin card decrypts ***Kn***, stores it and becomes Progenitor.

If several virgin cards are in the network, the first responding card receives ***Kn*** and then the key management restarts. This is repeated until there are no more virgin cards.


Virgin
Progenitor
(TCp, Nid)
(TCv)
Checks Certificate
Checks and decrements Counter
Encrypts Network Key and Counter
Becomes Sterile
Kn, Counter
Decrypts Network Key and Counter
Becomes Progenitor and restarts the key management

In a network without a progenitor card, **Kn** cannot be transferred and no virgin card can be initialized.

Conclusion

SmartRight system proposes a new concept of copy protection for digital home network based on end-to-end protection. The extensive use of smart cards ensures high level of security and full renewability of the security. Thus, smart cards efficiently fight against video piracy at home.

Furthermore, ***SmartRight*** concepts encompass an innovative method to share a common secret between a set of digitally linked smart cards without the need of a central authority. Other applications may use this scheme.

References

[1] ABRAHAM G., et al., ***Transaction Security System***, IBM systems journal, Vol 30, N° 2, 1991

[2] FRANK A., ***The copyright crusade II***, Viant Media Entertainment, 2002

[3] ***IFPIMusic Piracy report***, IFPI, 2002 available at http://www.ifpi.org/