COPY PROTECTION AND CRYPTOGRAPHY: AN EXAMPLE ***SmartRight***™

DIEHL Eric

THOMSON multimedia R&D France
1 Avenue Belle Fontaine
35510 CESSON SEVIGNE CEDEX, FRANCE
diehle@thmulti.com

Abstract

SmartRight system is an innovative renewable copy protection scheme for digital home network. It uses state of the art cryptography tools. Its design highlighted needs for new usable tools for security engineering and new key management schemes.

Introduction

Currently two revolutions are occurring. First, distribution of audio video content becomes fully digital. This offers better quality content with additional features like metadata. Second, computers and consumer electronic devices will be digitally networked. This will offer more flexible consumption modes. These revolutions put copyright protection under a greater threat.

Digital piracy is more dangerous than analogue piracy. Digital world allows pristine pirate copies, whereas analogue world produced degraded copies. Digital world offers convenient ways to disseminate, or to sell pirate copies. Digital world offers fast and easy path to disseminate circumventing methods.

Therefore, the content industry needs robust copy protection schemes

SmartRight™ system

SmartRight system is a copy protection scheme dedicated to digital home networks. A digital home network is a network that links together consumer electronic devices, and eventually computers. A same network may use wired buses such as IEEE1394, and wireless buses such as Hiperlan2.

SmartRight system introduces the new concept of Personal Private Network (PPN). A PPN is the set of devices belonging to one person, or one famiily. A PPN encompasses portable devices, and second household. An original key management defines the boundary of the PPN. All devices of a PPN share a common secret key unique to this network. This key management scheme allows this key sharing without knowing the configuration of the PPN, and without the need of a back channel.

Content providers may deliver content through different means for instance Conditional Access, Digital Rights Management, scrambled pre- recorded media, or free to air broadcast. Within the PPN, content providers decide if the content is

- Free; the content can be distributed to any body.
- View only; the content can be viewed by any device of the PPN but cannot be recorded.
- Private copy; the content can be viewed by any device of the PPN. It can be duplicated without limitation. But the copy cannot be viewed in another PPN.

The view only mode was designed without the assumption that storage units will faithfully collaborate. Furthermore, the protocol does not require a secure communication channel.

SmartRight system is an end-to-end protection. Once entered in the PPN, the content remains scrambled until it is rendered. Storage or duplication do no treatment. They are simple bit to bit copies.

SmartRight system extensively uses smart cards. Smart cards define the perimeter of the PPN. Smart cards protect the descrambling keys. Smart cards ensure the rights enforcement. Two reasons drive the use of smart cards:

- Smart cards are hardware tamper proof devices. This makes the task of pirates more difficult.
- Smart cards are removable. If a serious hack hapens, then we replace the cards.

Renewability is successful with Pay TV operators.

Research topics

Designing ***SmartRight*** system raised many challenges. Although it employs only off the shelf cryptography algorithms, it required the design of new protocols and concepts. Furthermore, ***SmartRight*** system will start an endless race with pirates.
To stay ahead, consumer electronics industry will need new security tools to be able to win this race. Through this design, we learnt many lessons, and identified many areas that would need further enhancement. The following section describes some of these tools.

Threat model and analysis: Successfully designing a protection system requires to know the threats to prevent. Furthermore, an a-posteriori threat analysis is the only way to ensure that the final design effectively prevents the identified threats. Practitioners in the industry need simple to use and practical tools to map and evaluate the threats. These tools should offer the following features:

- Common graphical representation of threats
- Common description of threats
- Method for identifying threats
- Method for evaluating threats, and common presentation of the results

Commonality is very important because it helps designers to efficiently communicate together. The use of common software methodologies increased the quality and reduces the production time of software. The same should occur for security engineering.

Formal analysis: Once the protocols designed, there is a need to check that they fulfil the expected requirements. Formal proof is a useful tool. Unfortunately, its use is limited to highly skilled mathematicians. Once more, industrial practitioners need simple tools helping them in this difficult task. The description of the protocol must be simple, and the declaration of the requirements must be even simpler.

Validation of implementation: We all know that too often breakdown of a system comes from bad implementation. Once more, we need tools that coupled with database of known attacks and errors, will automatically challenge the tested implementation. Following are some examples of such need. Buffer overflow attack is a typical implementation error. Good software practice could easily eradicate it. Unfortunately, we cannot expect this simple remedy to be always applied. How can we test this type of vulnerability? Side channel attacks, such as Differential Timing Attack, or Differential Power Attack, are powerful attacks. How can we ensure that implementations are robust against them?

Optimisation methods: Often academic researchers design secure protocol with very strong security requirements. Real environments may need weaker requirements. It would be useful to have design methods that would allow to securely “downgrade” published protocols to fit less strong requirements.

We described some expected tools that may bring us to a level of maturity similar to software design. We need urgently a concept of Computer Assisted Secure System Engineering (CASSE)

Obviously, industry needs more than tools. We need also new protocols. In the field of copy protection for home network, we identified several interesting research areas.

Innovative key management schemes: Systems will increasingly work in small clusters that need to be secure. People connect and disconnect their devices, especially with mobile devices. The configuration of these clusters will dynamically evolve. New key management schemes must support these constant changes. The schemes will need at least the following requirements:

- It must be distributed rather than centralised.
- It will need to be autonomous.
- There will be no administrator of the network.
- To be accepted by the consumer, it must be fully transparent to him.
- In order to preserve his privacy, there must be no registration phase.

Innovative revocation schemes: Pirates will always successfully reverse engineer devices. Thus, revocation is a mandatory feature. Unfortunately, using a central authority that manages revocation list is not always possible. We need new revocation schemes that work in an off-line hostile environment. This requires taking the smallest set of security hypothesis.

Tamper resistant software: In the future consumer electronic devices will have to execute secure software. Unfortunately, we may not expect to have hardware secure processor to protect the software. To be able to trust these platforms, we need to be able to trust the executed software. Thus we must have tamper resistant software or least tamper detection of software.

Conclusions

We presented a new copy protection scheme: ***SmartRight***. It uses state-of-the-art cryptography and security design. Through this design, we identified some advances in security science that would ease and enhance our work. First area is development of sophisticated tools for security designers. Second area is new key management schemes for distributed networked clusters and new off-line revocation schemes. Third area is development of efficient tamper resistant or tamper detection software.

SmartRight system is designed by Canal + Technologies, Gemplus, Micronas, Nagravision, Pioneer, Schlumberger Sema, SCM Microsystems, ST microelectronics, and THOMSON.