INNOVATION REPORT

Content Protection Systems

Piracy of digital content is one of the main concerns of the media and entertainment industry today. But the current situation could become even worse with the advent of digital home networks, thanks to which consumer electronic devices will be able to exchange digital content. The traditional ease of use of those devices could transform any normal user into a potential pirate. Therefore, securing the distribution of digital content within digital home networks has become mandatory and was the subject of the ITEA project COPS (Content Protection System) that finished in late 2005. This document was produced by the COPS team as a contribution to the ITEA programme report 2005 (chapter 'Developments in the programme environment').

The project COPS realised the 'authorised domain' concept being discussed in standardisation bodies. The idea of authorised domain is that devices belonging to a user form a trusted environment where the content protection – conditional access or digital rights management – used by the distribution network is extended and usage rules are enforced. Content may be shared between those devices but not with a neighbour's devices or over the Internet.

The target when designing the COPS system was to define a global solution. This requires a design operating at very abstract layers to remain independent of the lower layers. Various technologies for carrying data are competing in digital home networks: IP/Ethernet, IEEE1394, USB, Bluetooth, 802.11g, etc. And several types of heterogeneous busses are likely to coexist within one digital home network.In the same way, there will not be one unique format of content within a single digital home network. To propose a global solution, COPS made minimal assumptions on the carrying media and on the format of the protected content. The demonstration illustrated the applicability to MPEG-2 TS and JPEG2000/MXF formats over IP/Ethernet, IEEE1394 and also 'sneakernet' – transferring files physically through the use of USB keys.

Furthermore, other currently proposed copy-protection systems define security systems embedded within devices and are non renewable. This approach is very presumptuous: any security system will eventually be broken. This is particularly true in the consumer electronics domain. Embedding fixed security in a device means that once the hacker defeats the system, there is no way to recover. This signifies the content will be available for free until there is a completely new type of device to replace the broken one. The defeat of the Content Scramble System (CSS), which protects DVDs, is a perfect illustration of this. Smart cards have proven their security, their reliability and their ease of use in the consumer world such as in payphones, GSM mobile phones or pay-TV applications. In pay TV, they have demonstrated a perfect fit with the applications requirements in terms of security and the efficiency of their renewability. Renewable means that, if the system is broken, only the smart cards have to be replaced as opposed to replacing expensive devices.

In the COPS solution, usage rules are defined before entering the authorised domain and are still under control of the content owner or provider. These usage rules are then respected by the COPS-compliant devices.

Efficient copy protection should preserve consumers' private-use rights. One of COPS' objectives was to allow the user to make copies and backups for private use on any of his devices, with respect to the usage rules. This means that the user should be able to play his copied content on any of his devices linked to his network, on any of his portable devices including future mobile phones, on any of his devices located in his secondary residence and on his car's devices. But he should not be able to play his copies on a neighbour's devices.

Furthermore, the security model has been proven so that content owners trust the protection for private use.

COPS used results of projects such as HOMENET2RUN (ITEA), ProCredo and CoSIN (both RIAM), as well as current work of the DVB-CPT and TVAnytime standardisation bodies.

The COPS project provided two main results:

- A specification for a copy-protection system for a complete digital home network, independent of the busses used, and supporting the main formats used for multimedia content. It is compatible with major conditional access and digital rights management systems. This specification has been promoted in several standardisation bodies, with the main focus on DVB-CPT and TVAnytime. It has also been presented to, and discussed with, the content owners that trust this system.

- A demonstrator that presents an advanced digital home network protected by COPS. This demonstrator features set-top boxes, home servers and digital TVs, as well as elements of a protected-content distribution chain using existing conditional access and digital rights management. A subset of this demonstrator was shown at the 2005 ITEA symposium in Helsinki, and the complete version was presented during the final project review.

The companies involved in the project were Deutsche Thomson Brandt (D), Nagra France (F), Octalis (B), Philips DSL (NL), Philips STB (F), STMicroelectronics (F), Thomson R&D France (F) and Université Catholique de Louvain (B).