NAGRAVISION®
DIGITAL PAY-TV SYSTEMS

Inadequacy of Technology-only Approach to PayTV Piracy

Conditional Access (CA) systems for pay-TV applications are designed to allow legitimate paying subscribers to view and enjoy the programs that they have paid for and to prevent access by other non-paying or undeclared subscribers. Additionally, CA is designed to grant access only to the programs for which a subscriber has paid, denying access to premium or other similar programming unless the subscriber has specifically purchased it. As such the primary goal of the CA system is to protect the business and the revenue of the pay-TV operator.

Historically, cable and satellite pay-TV systems, including those of Nagravision, have been under attack by pirates since their inception. The lessons learned by the industry in North America as a result of this experience have been striking. The figure below presents some highlights of this history. In the mid-1980's HBO became the first channel in the US to scramble its satellite service, using a system known as Videocipher. Two versions of Videocipher were developed by M/A-com, a company later purchased by GI, which was finally acquired by Motorola.

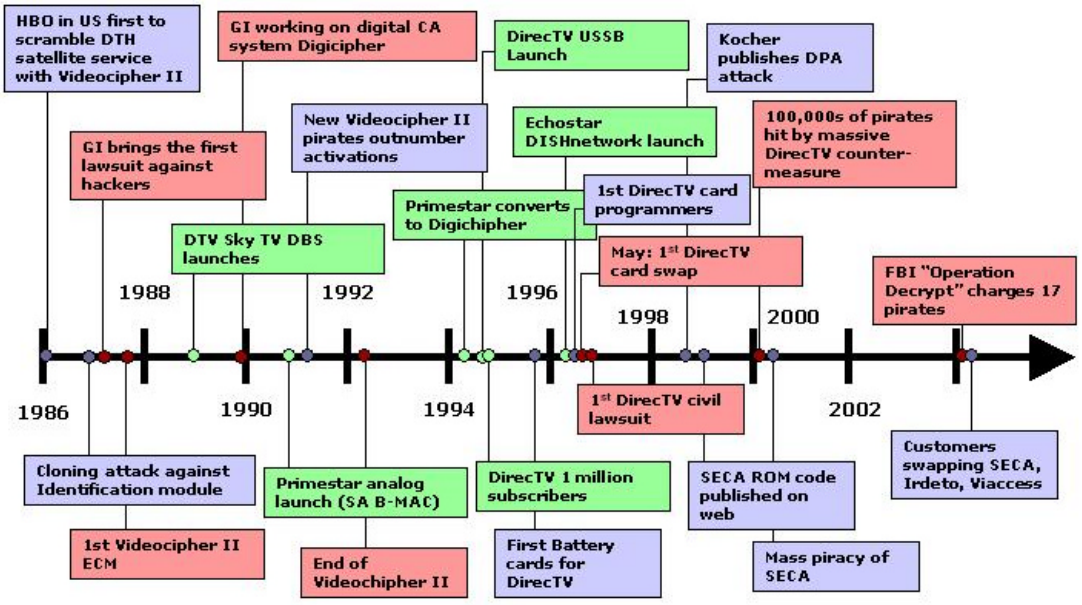

Figure 1 Piracy Time Line

When Videocipher II security modules were introduced in 1986, it was less than a year before the first successful cloning attack appeared against them. The first technical countermeasure, designed to disable the clones appeared just over a year later, thus beginning an attack and counter-attack cycle that continues to this day. Other similar systems such as the B-MAC of Scientific Atlanta suffered a similar fate.

When GI began work on a new digital version of Videocipher, known as Digicipher, almost four years later, the number of pirates on the old system had already reached proportions similar to those of legitimate users.

Because digital conditional access techniques are much more sophisticated than analog ones, and because the encryption of digital signals is more robust than analog scrambling methods, it was believed that once the transition to digital satellite transmission was complete, the pirates would finally be brought under control. This turned out not to be the case, and the history of attacks on analog scrambling systems repeated itself on the digital systems.

In the mid-1990's Primestar converted to Digicipher, and shortly thereafter DirecTV launched its direct to home satellite service. In less than a year DirecTV claimed over 1 million subscribers, but it was also at this time that the first so-called battery cards (pirate devices designed to allow decryption of DirecTV signals without a legitimate subscription) were discovered during a search by US customs officials. Since that time, despite repeated electronic counter-measures (over the air technical upgrades designed to disable pirate devices), DirecTV has replaced the smart card security elements in its STBs at least three times in an attempt to stem piracy of its services.

Other operators and conditional access systems have suffered a similar fate. In 1998 Paul Kocher and his colleagues presented a paper at a conference on advances in cryptography describing how differential power analysis attacks could be used to compromise smart card security elements. [1] By this time, every major conditional access system was under attack worldwide. Pirates communicated, exchanged technical information and in many cases carried out commercial activities on the Internet. Piracy on several systems resulted in the well-publicized swap of smart cards for clients of Canal+ Technologies in 2002 (Canal+ Satellite in France as well as customers in Spain and Italy). [2] Industry sources reported that over 30$ million was spent on the development of the new system, neglecting costs of acquiring and deploying the new technology by the operators. [3] Viaccess, Irdeto and other suppliers have recently suffered a similar experience.

Nagravision's systems have been under attack as well. Nagravision's Security Engineering team includes a world-wide multilingual group devoted to monitoring and intelligence activities, as well as a dedicated team to analyze pirate devices, devise counter-measures to disable these devices and support the engineering and development teams. Nagravision, too, has recently released its next generation security system, Aladin, the successor to its earlier DNASP-2 system, first deployed in 1996.

However, the lessons are evident. Technology has improved for both the industry players and the pirates alike. While our new technology is state of the art today, our intelligence teams are well aware that pirates are starting to study all these technologies to find ways to attack them, and it will only be a matter of time before some new attacks are successful, and the cycle will repeat again.

While continuing technology advances are necessary to stay ahead, it is important to remember that conditional access exists to protect the pay-TV business, and technical security solutions are just one component available to thwart pirates. Equally important are the legal actions that may be taken to curb pirate activities.

Indeed, the European Commission in its recent report on the Conditional Access Directive was clear that technology alone cannot solve the problem. [4] This explains why the Council of Europe is promoting measures to curb audiovisual piracy, including *possession of pirate decoders and smart cards*. The Treaty under which members of the Convention pledge to prohibit these and other activities has been signed by 10 member countries and entered into force on July 1, 2003. [5]

A striking example of the consequences of a technology-only approach comes from the automotive industry. In the 1990's manufacturers began to introduce new anti-theft measures such as coded keys, making cars more difficult to hot-wire. Although this technology effectively reduced the chances that cars with these devices would be stolen from parking lots, a way of defeating the technology was quickly discovered and carjacking soon emerged as a frequently reported violent crime. In addition to the appearance of automotive theft rings, able to obtain coded keys by infiltrating dealerships, the introduction of this technology has changed the face of the still-lucrative car theft business.

Fortunately, pay-TV piracy is not often a question of life-or-death, but the annual losses can be significant for industry players, and the lesson should be well taken.

For this reason, Nagravision supports Hong Kong Cable Television's request to the Hong Kong Legistlative Council to criminalize possession of pirate devices.

References

[1] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis," Advances in Cryptology - Crypto 99 Proceedings, Lecture Notes In Computer Science Vol. 1666, M. Wiener ed., Springer-Verlag, 1999.
http://www.cryptography.com/resources/whitepapers/DPA-technical.html
[2] http://www.skyreport.com/skyreport/oct2002/101502.shtm
[3] http://www.telesatellite.com/articles/complot_pirates/
[4] Report from the Commission of the European Communities on the implementation of Directive 98/84/EC on the legal protection of services based on, and consisting of, conditional access, April, 2003), p. 6.
[5] European Convention on the legal protection of services based on, or consisting of, conditional access (ETS no. 178). http://conventions.coe.int/Treaty/