NDS

Operational Security Group

Nagra piracy situation:
May 2000

I. Introduction:

Nagravision CA of Nagra-Kudelsky provides digital Conditional Access as well as interactive services to various broadcasters around the world. Their main customers are Echostar (Dishnetwork) in the United States, ExpressVu in Canada, Sky-Vista in Hawaii and the Carribeans (being shut down), Via-Digital in Spain, TV-Cabo in Portugal and SpaceTel in Taiwan.

Nagra has also provided Analog CA to cable and satellite companies such as Canal+ France and Premier in Germany however these systems are in the process of being switched off.

Of the current digital broadcasters using Nagra CA, the 3 North-American systems are hacked. Devices can be obtained from commercial pirate-device dealers. The 4th system (Via Digital in Spain) has been targeted by hackers however no commercial hack has yet appeared. In addition, certain cable-companies in the U.S utilizing Nagra CA have also been targeted by pirates.

Of the various Nagra customers, only Echostar has been conducting electronic counter measures. These ECMs were only partially successful – in that it has eliminated the free hack, but boosted the profits of commercial hackers. Recently, hackers on the Internet have noted that ExpressVu has taken steps to initiate ECM-activities.

II. Chronicle of the Nagra hack

In September of 1998, a well-known and 'respectable' hacking website known as 'DR7' (http://www.dr7.com) created an 'Echostar' section which provided a discussion-forum as well as a 'tools' section for other hackers.

By October 1998, the first hacks of Echostar appeared. The initial hacks were complicated to implement and were of interest primarily to those hackers involved 'for the challange'. The commercial value of such a hack however, soon created the incentive to develop a more marketable hack.

The first commercial hack known as AVR was essentially a printed circuit-l chip and a battery. These devices emulated the actions of the original smart-

CASE NO.
SA CV 03-950 DOC (JTLx)
ECHOSTAR SATELLITE CORP., et al.,

vs.

NDS GROUP PLC, et al

PLAINTIFF'S EXHIBIT 74

DATE _____ IDEN.

DATE _____ EVID.

BY _____
Deputy Clerk

E
No. SA CV
DO

NDS

Operational Security Group

Nagra piracy situation:
May 2000

I. Introduction:

Nagravision CA of Nagra-Kudelsky provides digital Conditional Access as well as interactive services to various broadcasters around the world. Their main customers are Echostar (Dishnetwork) in the United States, ExpressVu in Canada, Sky-Vista in Hawaii and the Carribeans (being shut down), Via-Digital in Spain, TV-Cabo in Portugal and SpaceTel in Taiwan.

Nagra has also provided Analog CA to cable and satellite companies such as Canal+ France and Premier in Germany however these systems are in the process of being switched off.

Of the current digital broadcasters using Nagra CA, the 3 North-American systems are hacked. Devices can be obtained from commercial pirate-device dealers. The 4th system (Via Digital in Spain) has been targeted by hackers however no commercial hack has yet appeared. In addition, certain cable-companies in the U.S. utilizing Nagra CA have also been targeted by pirates.

Of the various Nagra customers, only Echostar has been conducting electronic counter measures. These ECMs were only partially successful – in that it has eliminated the free hack, but boosted the profits of commercial hackers. Recently, hackers on the Internet have noted that ExpressVu has taken steps to initiate ECM-activities.

II. Chronicle of the Nagra hack

In September of 1998, a well-known and 'respectable' hacking website known as 'DR7' (http://www.dr7.com) created an 'Echostar' section which provided a discussion-forum as well as a 'tools' section for other hackers.

By October 1998, the first hacks of Echostar appeared. The initial hacks were complicated to implement and were of interest primarily to those hackers involved 'for the challange'. The commercial value of such a hack however, soon created the incentive to develop a more marketable hack.

The first commercial hack known as AVR was essentially a printed circuit-board with a chip and a battery. These devices emulated the actions of the original smart-card provided

by Nagra to Echostar subscribers. These circuit-board type devices were freely and amply available as they were developed originally to hack the DirecTV P1 card.

These 'AVR'-cards (as they were called) were programmed with certain 'keys' which were unique to every pirate-device user. Once programmed, these cards would replace the Echostar-issued smart-card in the IRD-slot, and would enable unlimited free viewing of all channels and services.

These devices are no longer in use because there is no ECM-support from pirate dealers.

In parallel to the AVR device, a ' Blocker '-type device was marketed, which was capable of blocking off the ability of the IRD to record and report 'Pay Per View' events, thus enabling unlimited viewing of Pay-Per-View movies etc.

Until about January of 1999, a large portion of the pirate-devices were built and developed by people motivated by the technological challenge. The information about the hack as well as the hacking methods was freely available on the internet for anyone to develop.

In these Internet chat-forums, several hackers reported that the exact same hardware was effective in decrypting the other Nagra systems in the North America region: namely ExpressVu in Canada and SkyVista in the Caribbean.

Soon websites appeared which specialized in other PayTV providers using Nagra CA.

With the appearance of Electronic Counter Measures by Echostar, Pirate-device dealers soon seized the opportunity for continuous profits from the sale and support of devices, and websites began selling commercial Echostar devices. These devices were called AVR2. They were still battery-card type devices, however the dealers developed them with automatic ECM-support built in- something that the original AVR hacks did not have.

As the customer-base grew, new types of devices were being produced. By the summer of 1999 original Echostar smart cards were hacked and sold by various dealers (these devices were known as E3m).

By September 1999, hackers developed a pirate-device to hack Echostar which was based on an off-the-shelf smart-card with a PIC-chip inside. These cards were also amply available as Pic-chips are very popular for hacking other CA vendors in Europe (such ad Irdeto and Seca).

As stated, Echostar's initiation of Electronic Counter-measures brought an end to the free Echostar hack. Initially, hackers would extract decryption-keys from the system, and post them freely on the internet. However once it was evident that Echostar would ECM whenever keys were posted, the hackers began keeping decryption-keys to themselves.

The only way to obtain a sustainable hack of Echostar was to purchase a hack from a dealer who provided the necessary key-updates whenever Echostar chose to ECM.

These ECMs harassed pirate-device users but Echostar never altered them (for comparison, NDS conducted similar simplistic ECM activities during the early BskyB analog days in the early 1990s).

As these ECMs continued - unaltered - for almost a year, the hackers studied them to the degree that they have developed a card which is unaffected by the ECMs (known as 'auto-roll' cards). These cards would be able to anticipate the ECM which Echostar would fire off, and make the necessary modifications so that the card would not be targeted by the ECM.

Over the past 2 years, the continued work by hackers on the various Nagra systems resulted in entire portions of the Nagra software to be posted on the internet. For example, the Echostar smart-card ROM has been posted - totally disassembled – on the internet. The Eeprom of smart-card used for the Spanish Via-Digital PayTV provider has also been posted in its entirety on the internet (indicating that hackers are showing an interest in other broadcasters using Nagravision.) Every few weeks, 'keys' for decrypting the various systems are posted by various people on the internet.

III. Nagra's anti-piracy efforts:

From about November of 1998, after the first hacks appeared, Echostar began its efforts to counter the pirate-devices by launching electronic counter measures. As these electronic counter-measures were a simple and repetative - far from eliminating piracy - it provided additional information which enabled the hackers at a later stage to develop a more marketable hack.

In desperation, Nagra increased the pace of their ECMs - to the point where they were launching ECMs twice a day. However legitimate customers began being affected by these maneuvers and after some mishaps, the pace of ECMs was moderated.

Nagra's countermeasures had different effects on the hackers. Initially, these ECMs required pirate-device users to re-program their cards after each ECM. To overcome this difficulty, the pirate-dealers have developed various ways to make this process easier. One such method entailed a person to insert his pirate-device into a card-reader which automatically obtains the new keys from the internet.

Other pirates developed yet another product - which was a stand-alone card-programmer with key-pad and screen - which does not require a computer to reprogram a card after ECMs.

Eventually, pirate-devices were developed which are totally unaffected by the Echostar ECMs. This situation persists today.

As early as December 1998, Echostar posted a message in the piracy news-groups which in essence admitted that it was being hacked. the message was a 'warning' to anyone attempting to hack their system. In parallel, Nagra Kudelisky launched an Internet web-site in which they boasted that Nagra CA-systems have acquired a reputation for reliability and security with their resistance to piracy being one of their most prominent features.

In exhibitions, when asked about piracy, Nagra representatives deny they have a piracy problem, yet boast of an Operational Security department tasked with tracking and fighting piracy in the realms of legal action and covert action based on collection of intelligence on piracy activities.

After over 18 months of mostly futile ECM activities, Echostar recently developed a new ECM which, for the first time, targeted the blocker devices. The hackers have yet to overcome this recent attack, however the regular devices still operate as before.

In addition, hackers who have concentrated on the Canadian ExpressVu system have noted recently that new downloads to the Set-top box indicate that they are preparing to begin conducting ECMs as well.

ExpressVu's strong legal offensive against piracy of their systems has caused the ExpressVu piracy to go underground. ExpressVu keys are rarely posted on the internet. There are almost no websites advertising the sale of hacks for ExpressVu. However several dealers are said to sell these devices 'under the counter'.

IV. The Domino effect

The PayTV pirates have followed a common pattern in their efforts to hack PayTV systems around the world. Hackers naturally aim to keep up with all the latest technological security measures, while investing less time and resources and still maintain a good income.

Hackers' business-sense in payTV piracy has driven them to recognize patterns and similarities between various products. Making it easier for them to hack the smart-cards of one payTV operator, and then maximize their profit from this single attack by implementing it on other Pay-TV operators.

This process has been quite visible with the pirate-devices developed to hack Echostar in the United States. Pirates have utilized this product again and again over an extended period of time, to hack other PayTV operators using Nagra Conditional Access such as ExpressVu and SkyVista. This ongoing income from one product enabled hackers to invest their profits in developing better hacks and will eventually enable them to hack newer technologies thus ensuring that they keep up with the latest security developments.

Though discussions of hacking Nagra customers have appeared from time to time on the internet, Nagra systems remained unhacked for some years. Once Echostar, the largest DTH provider using Nagra, has reached a certain 'critical mass' in terms of numbers of subscribers – the situation changed.

Echostar now became a viable business venture for pirate-card dealers to invest in. Once a hack has been developed for the Echostar system, these pirate-card dealers make an effort to maximize their profits.

As the Nagra-CA system has been thoroughly researched in order to hack Echostar, the pirates then pursued other PayTV providers using Nagra Conditional Access. As a result, almost immediately upon the release of the Echostar hack - the two other North American broadcasters using Nagra-CA (SkyVista and ExpressVu) - were hacked as well.

Occasional Internet discussions surrounding the European PayTV companies using Nagra (such as Via Digital) indicates that they, too, have been targeted by the hackers. However to date, no commercial hack for the European sites is being marketed.

Today, Echostar pirate-dealers in North America boast that they are capable of hacking any Nagra-based system worldwide.

As with other Conditional Access systems (such as Irdeto and Seca), we have witnessed a 'domino effect'. This effect portrays the life-cycle of piracy per CA-vendor in the PayTV realm.

First, a PayTV provider reaches a certain 'critical mass' in terms of numbers of subscribers - making it a viable business venture for pirates to invest in.
Once profits have been exhausted from the hack of one system, the global nature of PayTV piracy enables hackers to search out other broadcasters employing the same Conditional Access system.
Hackers maximize their initial investment by modifying the hack to work on other PayTV providers utilizing the same CA.
The success of the pirate will depend to a large extent on the level of similarities between the CA systems implemented in the two PayTV systems and the amount of modification required to get the existing hack to work.
With the steady profit, a hacker can then invest in hacking newer products, thus ensuring that he remains in the forefront of technological and security developments.
In parallel, hackers lower cost of production by utilizing cheaper raw materials (such as an off-the-shelf smart-card).

Thus, Nagra is currently walking in the same path that Seca, and before that Irdeto, walked. The hacking of one system causes the collapse into piracy of other smaller systems utilizing the same CA.
The use of off-the-shelf products such as Pic-chip based smart-cards make production-costs particularly cheap – thus causing an even greater proliferation of the hack.