NDS

Operational Security Group

Piracy in the PayTV environment: The Domino Effect

Nagra vs. NDS

The Domino effect:
Conditional Access systems (such as Irdeto, Nagra and Seca), once hit by Piracy, have suffered from 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.

The Case of Echostar:
Though discussions of Echostar hacks have appeared from time to time on the Internet, Nagra systems remained unhacked for some years.

Echostar, the largest DTH provider using Nagra, has reached a certain 'critical mass' in terms of numbers of subscribers. This made it 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 made 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.

According to hacker web-sites and discussion forums, the pirates were s
discover just how much their initial investment has paid off. According

Operational Security Group

Piracy in the PayTV environment: The Domino Effect

Nagra vs. NDS

The Domino effect:
Conditional Access systems (such as Irdeto, Nagra and Seca), once hit by Piracy, have suffered from 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.

The Case of Echostar:
Though discussions of Echostar hacks have appeared from time to time on the Internet, Nagra systems remained unhacked for some years.

Echostar, the largest DTH provider using Nagra, has reached a certain 'critical mass' in terms of numbers of subscribers. This made it 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 made 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.

According to hacker web-sites and discussion forums, the pirates were surprised to discover just how much their initial investment has paid off. According to their public

postings on the Internet – All PayTV providers using Nagra*CA had the exact same platform.
This meant that:
--A hack for Echostar would work on the other Nagra-CA providers as well.
--All Nagra-CA users had a standard 'off-the-shelf' chip in their smart-card. This meant that it was not necessary to make use of the smart-card provided by the broadcaster as these smart-cards could be obtained openly on the market.
--Since the chip was not unique, reverse-engineering made it possible to implant the smart-card software on any non-smart-card chip.

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. Increased Internet discussions surrounding the European PayTV companies using Nagra (such as Via Digital) indicates that they, too, have been targeted by the hackers.

The situation with the Nagra customers – whereby almost immediately after the hack of one system –other Nagra systems were compromised (an accelerated Domino effect) is apparently because no measures have been put in place to prevent this from happening.

So why is NDS special?

In the unlikely event of piracy, NDS has taken measures to prevent a 'domino effect'. NDS' advantage lies in its technological superiority as well as its operational-security activities.

Technology:
NDS' development process is unique in several aspects.

1. NDS develops custom-made chips, which are available only for NDS-products - and on a per-customer basis. Contrary to other CA-providers, hackers will NOT be able to illicitly gain information about NDS-technology by obtaining an 'off-the-shelf' chips from silicon and chip-vendors. NDS-supplied smart-cards cannot be obtained anywhere except from NDS or its customers. Each PayTV provider who is a customer of NDS receives smart-card technology unlike anything else on the market.

2. NDS integrates an ASIC (Application-specific Integrated Circuit) in its smart-card chips. This added defense makes it prohibitively expensive to reverse-engineer the chip in the NDS smart-card.

3. NDS develops a different platform for each of its customers - so that even if one of its customers may suffer piracy - it will not have any bearing on other NDS-customers.

4. NDS develops software tools inside the architecture of the smart-card for the unlikely event that one of NDS' customers is hit by piracy. These tricks (also known as Electronic Counter Measures) come in many different forms and variations to ensure that even in

our darkest theoretical scenarios, where pirates manage to overcome our Electronic Counter Measures, we are capable of implementing totally new measures which will inflict more damage to these potential pirates.

5. NDS guarantees the security and integrity of its smart-cards for designated periods after which it provides a totally new chip-platform to change over to. This ensures that hackers cannot count on long-term pay-back for a large initial investment as a hacked product will become obsolete within a designated time-frame.

Operational Security

NDS Operational Security has taken pro-active measures to provide an additional defense line – providing the product with a longer life in the field and deterring piracy. Ops-Sec offers a total strategy that covers every stage of design, production, distribution and after-care for the product. It provides for Physical security of facilities and employees, the security of information and knowledge in all their forms, and mostly – it implements counter-piracy measures.

1. NDS has established a proactive intelligence-gathering apparatus worldwide.
2. NDS personnel are engage in covert operations to disrupt hacker activities.
3. NDS has established close ties with law enforcement agencies where piracy is prevalent to assist in bringing hackers to justice.

Comparison table: NDS vs. Nagra Kudelsky

Counter-piracy measure	NDS	Nagra-Kudelsky
1. Chip Design	NDS develops custom-made chips which are available only for NDS-products - and on a per-customer basis.	Uses an identical 'off-the-shelf' chip for all of its customers.
2. Asic	NDS incorporates an ASIC (Application-specific Integrated Circuit) in its smart-card chips.	None.
3. Platform	NDS develops a different platform for each of its customers	Same platform for every customer.
4. Electronic Counter Measure tools.	NDS incorporates several varied ECM tools which, in the unlikely event of piracy, keeps it tightly under control.	Implementation of one identical ECM for over a year. Piracy today is unaffected by these actions.
5. Card Changeover	NDS' customers periodically change over to new smart-card technology – even if there is no piracy (as was the case of the BSkyB P11 card).	No known card changeovers.
6. Intelligence-gathering	Establish proactive intelligence-gathering apparatus worldwide.	No known proactive security-apparatus.
7. Covert operations	NDS regularly Engages in covert operations to disrupt hacker activities.	No known action has been taken against Echostar (or other) hackers.
8. Legal action	NDS has establish close ties with law enforcement agencies around the world and has brought several hackers to justice.	No known legal activities against hackers