NAGRA
KUDELSKI

CARDLESS WITHOUT COMPROMISE PART 1

The risks of current-generation broadcast cardless CAS technologies and why it's time for a better solution

WHITE PAPER - MAY 2016

SECURE. ENGAGING. EVERYWHERE.
DTV.NAGRA.COM

TABLE OF CONTENTS

04 A SHORT HISTORY OF CARDLESS CONDITIONAL ACCESS SYSTEMS (CAS)

04 Why Conditional Access Systems have historically used smart cards
05 The appearance of cardless solutions in IPTV
05 The adoption of one-way cardless for low-ARPU services
06 Which service providers are using cardless solutions today?

07 THREATS TO CURRENT CARDLESS CAS SYSTEMS

08 Compromises of software obfuscation and white box cryptography
09 Dependence on standard ETSI key ladders
10 Unrecoverable chipset security breaches
10 Excessive bandwidth and complexity required for countermeasures
11 Lack of resource for an effective response to piracy
11 Failure to continue to invest in smart card-based solutions

13 CONCLUSION

EXECUTIVE SUMMARY

As the business of pay television has developed over the last several decades, content protection systems like conditional access (CAS) and digital rights management (DRM) have emerged and evolved to protect it. Because the first digital pay-TV services launched were on satellite, the CAS technology created to secure these services was built to be robust to the most hostile of environments possible: one-way broadcast networks. For this reason, hardware technologies were chosen that were capable of receiving and storing unique secrets that are the basis of most CAS vendors' technologies today. Though there were compromises in these first-generation technologies, the industry quickly learned from them and as a result has produced increasingly sophisticated, hardware-based systems that have successfully withstood the test of time and have protected billions of dollars worth of service provider revenues.

With the advent of IPTV, this paradigm began to change. In order to reduce costs and speed time to market, new market entrants in the CAS/DRM space began to offer alternative technologies that made little or no use of the trusted hardware elements that had so successfully protected the pay-TV industry in the past. IPTV service providers experienced little or no negative impact from using these technologies because their closed networks are by their very nature less vulnerable than broadcast networks, and they also tended not to offer the same exclusive content available from many high-value broadcast services.

But as emerging markets began the process of digital migration, they looked to software-based technologies used in IPTV to protect their broadcast services, and so-called "cardless" technology began being introduced into the broadcast space as well. These first-generation solutions leveraged some of the technologies associated with card-based solutions, but they did so while leaving their systems open to several different types of potentially devastating attacks, while at the same time failing to develop the technologies, services and expertise to effectively recover from these attacks.

This paper will explore the history of one-way cardless CAS technologies, their use in the market, and analyze the potential risks and vulnerabilities of their use.

In Part 2 of this white paper series, we will explore how NAGRA is addressing these threats with a range of technologies and services that give pay-TV service providers the peace of mind that they can adopt cardless solutions to save money on smart card logistics without having to compromise on key aspects of content security that will ultimately cost them unexpected money in the long run.

A SHORT HISTORY OF CARDLESS CONDITIONAL ACCESS SYSTEMS

WHY CONDITIONAL ACCESS SYSTEMS HAVE HISTORICALLY USED SMART CARDS

Since the first DVB-based digital television services began operation in the mid-1990's, hardware-based CAS clients have been used; either embedded in set-top boxes or in the form of smart cards. Because these initial services were predominantly satellite-based – transmitted over an "open" broadcast network that anyone within the footprint could receive - a CAS was required that could store the subscriber identity and their service entitlements within a secure environment. The smart card provided such an environment, and through a process of pirate compromises and subsequent technological advancements and innovations, it continues to be the workhorse of the pay-TV industry more than 20 years after its initial launch.

For large pay-TV operations with high subscriber revenue and exclusive content, hardware-based security continues to be the tool of choice for nearly every pay-TV operator on the planet, because it has a proven ability to provide the protection required. Even as new threats like Control Word Sharing have emerged, smart card-based systems have evolved to effectively combat them. And some next-generation solutions completely eliminate the gap that caused the vulnerability in the first place. Because of this, it is likely that smart cards will continue to be used well into the future for high-value services.

Figure 1: Smart cards have been trusted with high-value content since the launch of digital TV.

THE APPEARANCE OF CARDLESS SOLUTIONS IN IPTV

Since the launch of the first multi-channel IPTV service by Kingston Interactive Television (KIT) in the U.K. in 1999, most IPTV service providers have embraced a different kind of content security solution – one based primarily or exclusively on software.Many of these implementations ignored key security best practices developed by the broadcast pay-TV industry, forsaking things like hardware root of trust, tamper resistant hardware, built-in countermeasures, and extensive device certification in favor of a simpler, lower-cost approach.

Figure 2: The world's first multi-channel IPTV service from Kingston Interactive Television

This reduced approach to security has worked to date for IPTV only for several reasons:

- Most IPTV deployments have fewer subscribers than equivalent satellite/cable services, making them less likely to be attacked.
- With some notable exceptions, satellite and cable operators usually carry more exclusive, high-value content than telcos, making them more subject to piracy.
- The closed nature of IPTV networks provides some protection against content theft by the nature of the network architecture itself, meaning that the IPTV security solutions did not historically need to be as robust as their broadcast counterparts. This is however changing as cyber intrusions into supposedly closed and well-protected systems increase on a daily basis, with high-profile attacks against media companies like Sony and others.

The fact that IPTV security systems have been less subject to attack also means that IPTV security vendors lack many of the anti-piracy resources, skills and experience required by large pay-TV operations; they simply haven't needed to develop them while protecting low-risk networks.As the threats to IPTV increase, they attempt to mitigate these deficiencies through partnerships with small, third-party anti-piracy companies, but this creates an undesirable split between CAS/DRM technology and forensic services that can result in finger-pointing and lack of clarity with regards to roles and responsibilities for solving customer problems.

THE ADOPTION OF ONE-WAY CARDLESS FOR LOW-ARPU SERVICES

Due to the successful adoption of software-based solutions in IPTV, and driven by the need to rationalize the costs of delivering low-ARPU services to subscribers in emerging markets, selected broadcast pay-TV service providers also gradually began to adopt software-based solutions for their one-way networks as well. Though these solutions lacked many of the key security features employed by smart card-based systems, due to the low-value nature of the content being protected, piracy did not represent a significant problem for these companies.

Over time, some cardless solution providers began to add limited hardware security features to their solutions, like leveraging third-party roots of trust in set-top box silicon, and anchoring their solutions to industry-standard ETSI key ladders. They also began leveraging software-based obfuscation to "hide" their software. While these techniques improved on the security of cardless solutions for broadcast, they did not yet bring them up to the level required for premium content protection on large networks.

WHICH SERVICE PROVIDERS ARE USING CARDLESS SOLUTIONS TODAY?

When looking objectively at broadcast-based service providers leveraging cardless solutions, several trends emerge. These service providers are:

- Mostly in emerging markets in India, Asia and Latin America
- Mostly offering low-ARPU and Free-To-View services without exclusive content
- With only a few exceptions, serving on average fewer than 200,000 subscribers, and mostly less than that.

This following graph from ABI Research illustrates the penetration of both one-way and two-way cardless solutions globally, and indeed shows that the penetration of cardless solutions is overwhelmingly in low-cost Asian markets like Indonesia and India.

Despite the efforts of some CAS vendors to spread cardless solutions outside of these markets, they have not yet been successful in doing so in any meaningful way. There are several reasons why operators with higher value content and larger subscriber bases have been unwilling to do this:

- Cardless solutions are not proven in the protection of high-value content.
- Providers of the current generation of cardless have little or no experience battling piracy of these solutions because they have never been used in a high-risk environment that is subject to significant piracy.
- Providers of premium content may not be willing to license their content to cardless systems because they are unproven or provide insufficient protection for content like 4K UHD.
- Perhaps most importantly, these solutions may not provide long-term protection of operator investment in set-top boxes because they lack the ability to recover from a major security compromise once countermeasure are exhausted or the STB chipset is hacked.

For these reasons and more, let us examine what the current threats are to existing cardless systems that make them unsuitable for protecting higher value content for larger service providers

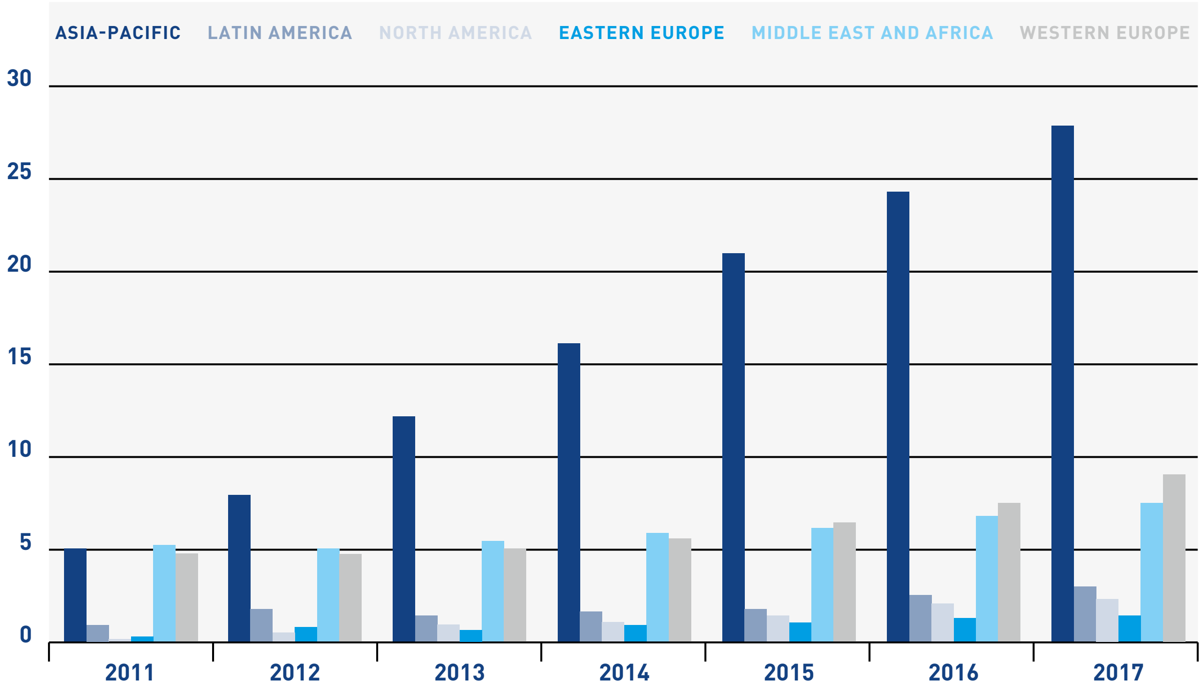
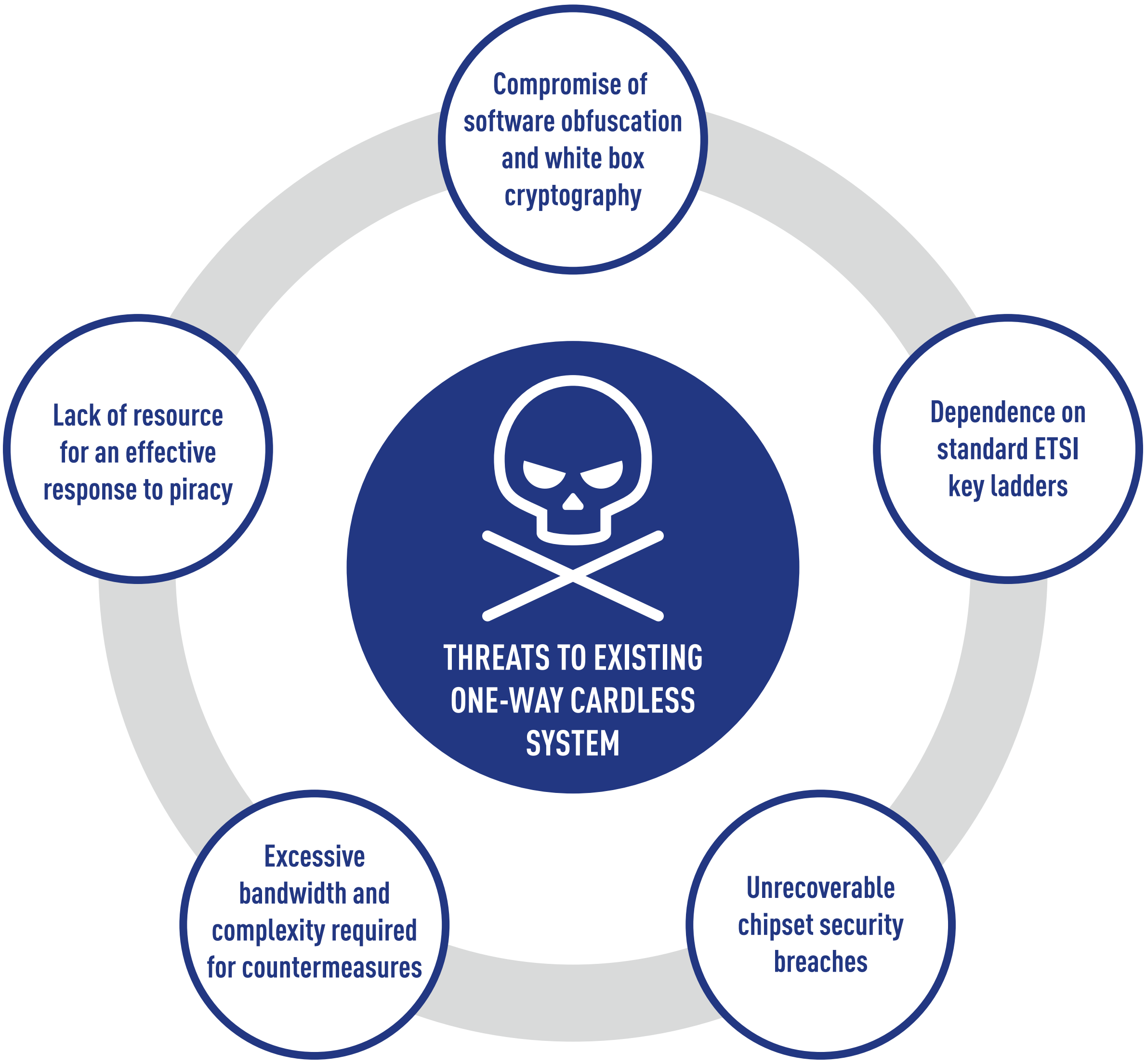


Figure 3 Cardless CAS penetration by geography - historical and forecast. Source: ABI Research

THREATS TO CURRENT CARDLESS CAS SYSTEMS

Current-generation cardless systems were designed in order to cope with the downward pricing pressure put on the traditional smart card products offered by conditional access companies in emerging markets. The companies designing these solutions lacked any expertise in hardware and resorted to using software security techniques and industry-standard security mechanisms to secure their solutions. Though this approach has proven adequate for the protection of low-value content, IT industry security experts consider the techniques used to be fundamentally inferior to the use of hardware-based content protection technologies. Below is a list of the reasons why current generation solutions are at serious risk of compromise.



THREATS TO EXISTING ONE-WAY CARDLESS SYSTEM

Compromise of software obfuscation and white box cryptography

Dependence on standard ETSI key ladders

Unrecoverable chipset security breaches

Excessive bandwidth and complexity required for countermeasures

Lack of resource for an effective response to piracy

COMPROMISES OF SOFTWARE OBFUSCATION AND WHITE BOX CRYPTOGRAPHY

Some cardless solutions rely heavily or exclusively on software obfuscation techniques or "white box cryptography".Obfuscation techniques, while they have been studied for some time in the academic literature, have only recently been exposed to real-world scrutiny, unlike smart card alternatives, whose strengths and weaknesses are well known.

Even those solution providers who rely heavily on it recognize that obfuscation isn't a perfect science and is just as subject to attack as traditional CAS solutions: "Some critics will say that in earlier [generations of white box cryptography] were defeated. And that was the case. There are examples of where white box cryptography has been cracked; for instance, Differential Fault Analysis (DFA)." They claim that they have been able to remedy these problems with next generation solutions, but one leading expert, Harvard Computer Science Professor Boaz Barak, appears to disagree:

"I think that current obfuscators (or fuzzily secure components in general) may have limited uses. These are in cases when security can be tested, and a security breach can not cause catastrophic results. For example, in the setting of copyright protection, it is possible to detect 'interesting' security breaks: If a hacker works alone and breaks the security to copy songs for her own use then this is undetectable, but also causes only negligible damage to the record company. In contrast, to cause some damage, there must be an active 'black market' of copyrighted material, and such a market would be noticed by the studio, which would know that security has been broken. However, in order to be able to use this information, the system must be 'planned to fail' in the sense that it should be easy to redeploy an alternative implementation, upgrade versions, etc. This has not been the case in the past, for example in the DVD CSS algorithm. Thus, fuzzy security should be used only when one understands its inherent limitations. Of course, whenever possible, it is much better to use well-defined (and preferably proven) security."[1]

The same author, in follow-up research presented in March 2016, said that the state of the art had advanced significantly, but that "much additional research will be needed before it reaches sufficient efficiency and security for practice."[2]

Some conditional access vendors have also announced they will move elements of their obfuscated software-based security into secure processing environments on chipsets in the hopes of creating a more secure solution, however there are two problems with this approach:

1) Even though secure processing environments provide a relatively secure space in which to execute software, they are still more vulnerable to attack than hardware IP blocks that are built into the chips themselves because they are unable to withstand state-of-the-art hardware attacks, especially in a one-way environment when protecting higher-value content and services.
2) As a relatively new technology in pay TV, secure processor-based solutions from conditional access providers are only available on a limited range of chipsets and set-top boxes, whereas the most recent generation of advanced SoCs with embedded security IP blocks from leading vendors have been available for many years and are widely available.

The effort to start moving critical CAS security code into a secure environment shows that these parties recognize that obfuscated software alone

[1] http://www.boazbarak.org/Papers/obf_informal.html

[2] http://cacm.acm.org/magazines/2016/3/198855-hopes-fears-and-software-obfuscation/fulltext

is insufficient to fully secure premium content. This step however doesn't go far enough to catch up with solutions implementing full IP-blocks in hardware, because they still remain fundamentally software-based in nature.

It is therefore advisable to use proven and widely available hardware-based systems to protect higher-value content revenues, because the breach of obfuscation- or secure processor-based systems could cause significant commercial damage to the service provider.

DEPENDENCE ON STANDARD ETSI KEY LADDERS

A key requirement for adequately securing a CAS client is to employ a hardware root of trust; a set of hardware keys that are unique to a given device and are used to prevent cloning of the security client and encrypt communications between the security client and the device. The importance of this requirement is evidenced in the Enhanced Content Protection Specification[3] released by MovieLabs, the collective technology interest group of the Hollywood studios.

Some cardless CAS suppliers use this function, and others historically have not. Even the ones that do rely mostly on the industry-standard ETSI key ladder[4], a publicly available standard that is available for all to view, or other third-party solutions not under their direct control. They do this because as primarily software companies, they lack any internal hardware expertise to do otherwise, so they rely fully on silicon vendors to implement it for them. The result of this is that their use of the ETSI key ladder provides a very large attack surface to pirate collectives who seek to defeat the mechanism, because doing so would give them the biggest possible payoff since attacking the ETSI key ladder would directly affect all operators using it.

In addition, in recent times, mistakes made by silicon manufacturers have caused some legacy CAS solutions to be susceptible to forms of piracy like Control Word Sharing, further highlighting the need for CAS solutions to be designed end-to-end by the CAS vendor without reliance on third-party security components.

It is therefore critical to use proprietary key ladders and algorithms from companies like NAGRA who have the hardware expertise in-house to define, produce and test end-to-end solutions that do not have any dependencies on industry-standard security components or third-party manufacturers. That is why all NAGRA security solutions, including cardless ones, use the proprietary NAGRA On-Chip Security 3.0 (NOCS3) block that all major silicon manufacturers integrate directly into their SoCs. By doing this, NAGRA is also able to offer the industry's best guarantees and liabilities.

What do independent security experts say about this approach?

"The use of proprietary algorithms and key ladders, together with proprietary means of rights enforcement, makes an attack on NOCS3 hard to execute in a useful way and less likely than if the system relied on software and the standard ETSI key ladders alone and therefore makes it highly resistant to common forms of attack."
- NAGRA anyCAST PROTECT Review Summary, Farncombe Technology Limited, February 2016

Even first-generation cardless CAS vendors have now started to recognize the importance of using a hardware root of trust because of new Hollywood demands for Enhanced Content Protection and the serious risks linked to using only software-based solutions. But their late attempts to fill the gap by using third party hardware roots of trust like ETSI

[3] http://www.movielabs.com/ngvideo/MovieLabs%20Specification%20for%20Enhanced%20Content%20Protection%20v1.1.pdf

[4] https://www.etsi.org/deliver/etsi_ts/103100_103199/103162/01.01.01_60/ts_103162v010101p.pdf

will ultimately fall short compared to companies that have long invested in an end-to-end approach that leverages long-term investments in proprietary, proven hardware.

UNRECOVERABLE CHIPSET SECURITY BREACHES

As conditional access technology has advanced, so have the capabilities of the pirates who attack them. This includes the ability to leverage potential vulnerabilities in set-top box chipsets as previously mentioned. Cardless solutions that make use of standard chipset key ladders and other functionalities are therefore particularly vulnerable to this type of attack.

Because the descrambling of the DVB transport stream takes place in the chipset, any compromise thereof has the potential to cause catastrophic damages to the service provider by permitting rampant piracy. Should such a breach occur, there is very little that can be done by most conditional access providers to re-secure the system, because if there is a compromise of the chipset, it is highly unlikely that even the deployment of a smart card can aid in its recovery.

Under most circumstances, the only possible remediation of such a breach would be to replace the set-top box with a new-generation chipset, but that represents a tremendous cost to the service provider. Therefore, the ability to re-secure such a set-top box by rerouting transport stream descrambling to a replaceable element like a smart card would represent a huge potential savings to the service provider, but currently only NAGRA offers this option.

EXCESSIVE BANDWIDTH AND COMPLEXITY REQUIRED FOR COUNTERMEASURES

As has historically been the case with most CAS solutions, cardless security solutions using standard, widely available technology like the ETSI key ladder will eventually be broken by pirates. With a software-based CA, however, the best-case response to any pirate exploits of the software (barring the hardware attacks addressed above) is to apply Over-The-Air (OTA) downloads to update the system. Should this be successful, it would likely only help control the level of piracy for a limited period of time, but will most likely ultimately require replacement of the cardless CAS by a smart card.

To allow for an adequate initial response to pirate attacks, sufficient bandwidth must be available for these downloads. A normal anti-piracy scenario should allow for security updates every few months if it is likely that the system will be under attack. If the cardless CAS is deployed in a large system or with high-value content, the required response may require an uneconomic amount of bandwidth, depending on the frequency of updates required. At some point, the CAS provider may not be able to keep up with the pace of updates required in order to re-secure the system due to the cost of the bandwidth required, and the non-negligible amount of time required to create, test and deploy the countermeasures.At some point, the pirates will likely gain the upper hand.

If the outcome of a software-based attack is ultimately the replacement of the cardless CAS by a new, smart card-based system, then service providers are better served by a strategy that anticipates such attacks upon initial implementation of the system. That is why – in addition to providing the possibility to deploy initial anti-piracy countermeasures – a next-generation broadcast cardless CAS must have other "back-up" mechanisms to effectively counter piracy without the logistics and material costs associated with a card swap.

LACK OF RESOURCE FOR AN EFFECTIVE RESPONSE TO PIRACY

Another key success factor in the fight against piracy is the capability of a CAS provider to respond to attacks on the system. The success in creating and applying countermeasures as well as taking legal measures against pirates is directly related to the resources dedicated to undertake these activities in cooperation with the service provider.

CAS vendors can be divided into three different categories in terms of their ability to respond to piracy threats:

+ Smaller, IPTV-focused companies have very little resource or experience in combatting piracy because the closed nature of IPTV networks have not required them to develop this expertise, and because in general these companies are smaller with fewer employees. They are now attempting to source this expertise from third-party partners, but as mentioned previously, this can lead to an undesirable division of responsibilities where technology and services are not working together in harmony to resolve service provider problems.
+ Mid-sized CAS companies generally have a small team of dedicated anti-piracy resources and very limited lab facilities.
+ Large security specialists have large, multi-disciplinary anti-piracy groups that include forensic investigators, legal and engineering resources, and advanced laboratory facilities with state-of-the-art equipment capable of reverse-engineering pirate solutions in order to devise and deploy effective countermeasures.

It may therefore be that, while cardless solutions from small and mid-sized companies might seem initially attractive, their long-term costs are likely to be far higher than expected due to the limited resources and experience they have in fighting piracy. Ultimately, the business case that originally justified the acquisition of such a solution will fail, and the operator risks loss of revenue from piracy, loss of content from providers and loss of brand reputation.

FAILURE TO CONTINUE TO INVEST IN SMART CARD-BASED SOLUTIONS

Most CAS vendors specify smart cards as the proposed "backup plan" should a cardless CAS eventually fail to continue protecting a service provider's content and all other countermeasures have been fully exhausted.But just how much do these vendors invest in such solutions, and how effective will they be in fulfilling their promised role? Again, the response can be divided into three categories:

+ Smaller, IPTV-focused companies have – through acquisition – acquired a limited ability to provide very basic smart card solutions, but these are not widely deployed and are not considered state-of-the-art. They are based on older, industry-standard technologies that are widely used in the telecommunications and banking industries as well, meaning that any successful attack on cards used in those industries may be applicable to pay-TV smart cards as well. Smart cards from these providers have only remained uncompromised due to their extremely limited deployment for low-value services, thus remaining "under the radar" of pirates. But because of their use of standard, widely available technologies, any attacks on those technologies will impact pay-TV operators using these solutions as well.

- Mid-size vendors who used to specialize in smart card-based solutions have fully embraced cardless solutions and have put their smart card development into "maintenance mode", and have stopped making further investments in smart card-based technologies, now that they function primarily as a "backup" solution to their cardless counterparts. In addition, these vendors fully discontinued their expertise in hardware engineering nearly 20 years ago, choosing instead to outsource smart card development and STB chipset expertise to third parties.

- Large CAS vendors, conversely, protect high-value content for large service providers, who continue to prefer the proven track record of smart card-based systems, and therefore still actively develop state-of-the-art and innovative hardware solutions. In addition, these CAS vendors see security as an end-to-end proposition for which they must take full responsibility in order to be able to guarantee the integrity of the CAS. For this reason, companies like NAGRA create custom chipset design elements for SoCs and fully design their own custom smart cards to be able to guarantee the best security technology, services and liabilities in the industry.

The promise of the smart card as a backup scenario to a failed cardless system is only valid if the smart card solution itself is uncompromised. Because of their continued focus on the active development of smart card technology, it is therefore highly advisable to work with larger CAS vendor, because with other vendors, the solution may be no better than the problem.

CONCLUSION

With so many potential problems using first-generation, one-way cardless CAS systems, is there still a way to reduce total cost of CAS ownership without compromising on security? Is it possible to enjoy the logistics savings associated with cardless systems without the fear that the set-top box will ultimately have to be replaced in case of a compromise? Absolutely, but only if the cardless solution meets the following criteria:

1. The solution must rely more on hardware security than on software – even if obfuscated using state-of-the-art techniques – because academic experts agree that software-based systems are not fully robust to tampering and reverse engineering.

2. The solution must rely on systems that use a combination of proprietary key ladders and algorithms, and not on the standard ETSI key ladder, which as an open standard is more vulnerable to attack.

3. The solution must offer a clear and effective strategy for applying countermeasures if the CAS comes under pirate attack, and those countermeasures must be operationally and financially reasonable to execute (e.g. not require excessive bandwidth over an extended period of time).

4. The solution provider must have sufficient expertise in battling pirates and enough resources dedicated to creating and deploying the countermeasures required to keep the solution secure over the long term.

5. The solution must have a credible and reliable strategy for re-securing the STB in case of an unrecoverable breach of the cardless CAS that cannot be remediated by further countermeasures. Ideally, such a strategy should also address compromise of the STB chipset in order to avoid having to replace the entire box.

IF THESE CRITERIA ARE MET, IT IS ENTIRELY FEASIBLE TO IMPLEMENT A CARDLESS SOLUTION TO PROTECT ONE-WAY BROADCAST CONTENT WITHOUT THE INADVISABLE COMPROMISES THAT OTHER SYSTEMS HAVE RELIED ON TO DATE.

NAGRA
KUDELSKI

For more information on this White Paper, please contact the authors:

Nicolas Bovard
VP Product Management CAS & Portfolio Management
nicolas.bovard@nagra.com

Olivier Biot
Product Line Manager CAS & Portfolio Management
olivier.biot@nagra.com

Christopher Schouten
Senior Product Marketing Director
christopher.schouten@nagra.com

All product and application features and specifications are subject to change at the sole discretion of Nagravision SA at any time and without notice.

design: diabolo.com

SECURE. ENGAGING. EVERYWHERE.
DTV.NAGRA.COM