THE FUTURE OF BROADCAST CARDLESS SECURITY REVISITED

Updated survey reveals the latest perceptions in piracy threats and technologies to address them

A white paper by Cartesian in collaboration with Verimatrix

TABLE OF CONTENTS

INTRODUCTION

Aims of This Paper

In this paper, we look at how changes in the last five years in piracy and technology have affected the implementation of conditional access (CA) systems in the one-way broadcast network, and how this landscape is expected to develop in the future.

To answer these questions, Cartesian has looked at the following issues:

- What are the leading forms of piracy in today's market?
- What's the new state-of-the-art for smartcard and cardless technologies?
- What device security features are now seen as important in the fight against piracy?
- How has the industry changed in the last 5 years, and how will it continue to evolve over the next 5 years?

Recap of 2012 White Paper

In 2012, Cartesian conducted an industry survey and authored a white paper exploring the future of cardless broadcast security.

The 2012 white paper looked at how changes in piracy and technology were affecting the implementation of CA systems in the one-way broadcast network and, more specifically, how the relevance of cardless security to one-way service operators was changing.

The takeaways from the previous white paper were:

Takeaway #1: New security technologies lift the barriers to hacking CA cardless systems as high as those to hacking card-based systems, as long as they are implemented correctly.

Takeaway #2: Operators with a low volume of premium content or a low reach should have expected the frequency with which their CA system was attacked to decrease as piracy focus turns to content re-distribution.

Takeaway #3: Cardless CA systems are appropriate for operators with a low volume of premium content or a low reach, although we recommended the inclusion of a smartcard slot as a precaution to mitigate the risk of having to replace all devices.

Takeaway #4: We recommended that operators must implement technologies that enable the direct fighting of content re-distribution and control-word sharing, such as watermarking, fingerprinting and monitoring.

2017 SURVEY

In the summer of 2017, Cartesian conducted a survey on one-way CA systems targeting key stakeholders in the TV industry. One hundred and fifteen professionals from countries across the globe participated in the survey. Service providers, who are the final decision makers in deployment, were a significant proportion of our survey responses.

Figure 1 - Our survey respondents

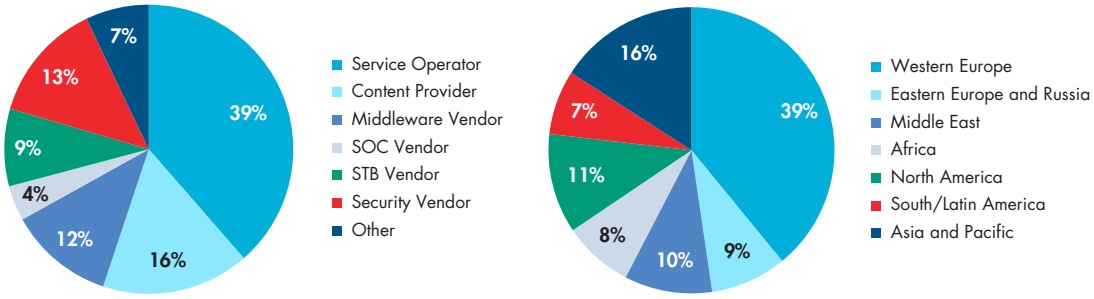
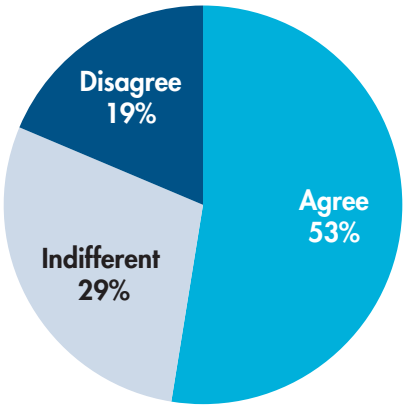


Figure 1 shows the type of companies that responded to our survey, and where they are located. Note that respondents could select multiple options if they had multiple functions, or operated in multiple regions.

Smartcard vs. Cardless CA Systems

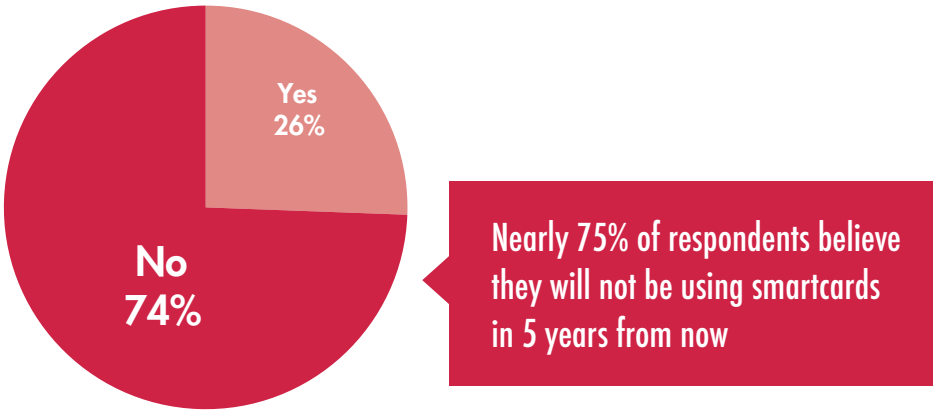
The primary aim of our survey was to capture the current view of cardless technology versus smartcard technology. Figure 2 asks the simple question "is the security offered by cardless now comparable to smartcards?". 53% of our respondents agree that it does, with only 19% disagreeing. One respondent provided their insight - "The goal of any protection is not to be "the best", but to make it too expensive for a pirate to bypass. On this subject, smartcard or cardless solutions are similar". We will revisit this later.

Figure 2 - Do you agree that the security offered by cardless CA system is now comparable to smartcard-based CAS?



For some, there is an inevitability that the industry is moving towards cardless solutions. For others, the need to maintain legacy bases and the maturity of smartcard technology means that smartcards will remain relevant for many more years. Figure 3 shows how respondents think they will view smartcard deployments in 5 years from now.

Figure 3 - Do you feel you will be using smartcards in 5 years from now?

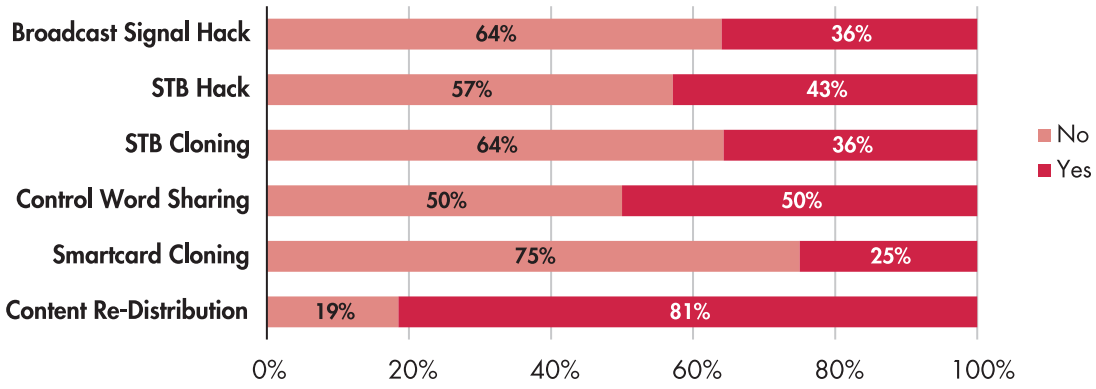


A common message from the survey is that devices are increasingly connected. Although the target of this survey is a one-way CA system, many devices are nevertheless connected, and are predicted to become increasingly connected in the next few years. Connectivity was seen as important for cardless CA systems, with one respondent confidently noting "with 2-way connectivity and embedded security, cardless is superior to card-based for 90% of the cases".

Evolving Threat Landscape

One key factor for some is the evolving threat environment. Figure 4 shows the biggest concerns as presented by our respondents, with the threat of content re-distribution over the internet as the top concern.

Figure 4 - Are you concerned by the following in your deployment?



Control word sharing remains a concern for half of our respondents. As we shall see later, state-of-the-art cardless and smartcard solutions have helped close the weaknesses in earlier smartcard solutions which were targeted by control word sharers.

We can compare these concerns with our earlier survey. Table 1 shows the top-rated piracy concerns raised by the respondents of our 2012 survey, together with those from our 2017 survey.

Table 1 - 2012 vs 2017 survey concerns - "% of operators whose #1 piracy concern is …"

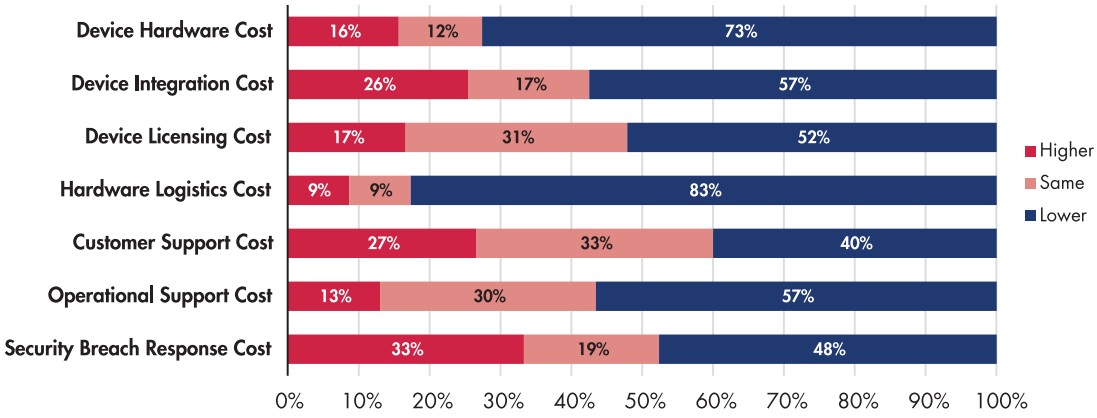
#1 Piracy Concern	2012	2012 5-Year Prediction	2017
Content re-distribution over internet	42%	63%	58%
Control word sharing	35%	21%	8%
Smartcard distribution/cloning	18%	10%	6%
Set-top box cloning	6%	6%	9%

In 2012, content re-distribution was the number one concern for many operators, closely followed by control word sharing. **We predicted that content re-distribution would grow further as the biggest concern, which has proven correct, though the threat of control word sharing has fallen even more sharply than we predicted.**

Costs of Piracy

In terms of cost, Figure 5 shows that cardless is viewed by most as a lower or equal cost to smartcards; although breach response cost clearly remains a concern for many (overall 79% of respondents said breach response cost was a concern for them).

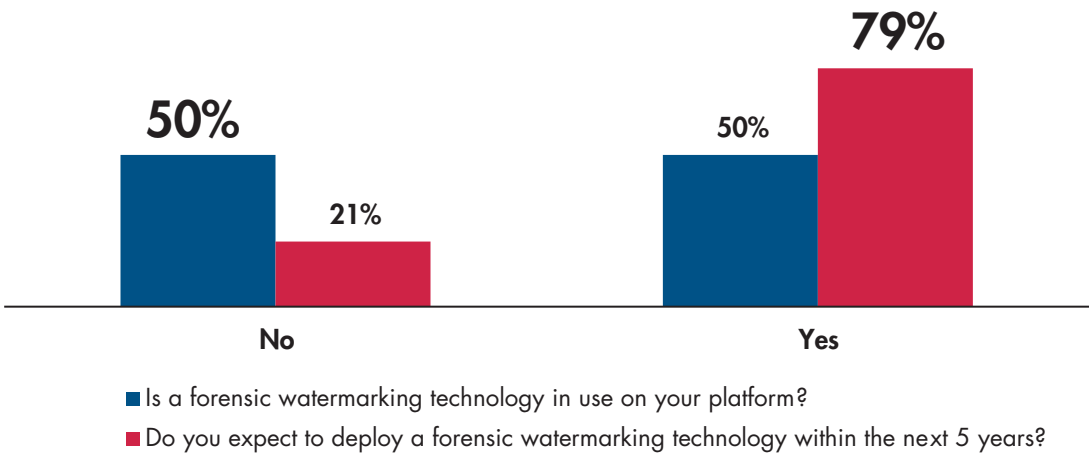
Figure 5 - With respect to CAS costs, how do you think cardless CA systems compare to smartcard-based CA systems in the following areas?



Anti-Piracy

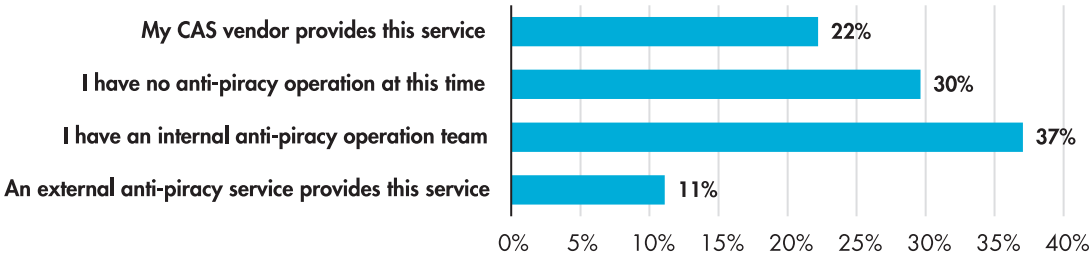
As noted above, content re-distribution is a concern for most in our survey. Forensic watermarking is a technology that can be used to trace the source of illegal streams. Figure 6 shows the current state of forensic watermarking deployment among our respondents. Of those who responded, 50% currently have a solution in place, and 79% expect to deploy in the next 5 years.

Figure 6 - Forensic watermarking



To tackle the challenge of content re-distribution, organisations must deploy an anti-piracy operations capability. Figure 7 shows the current state of anti-piracy operations within our respondents.

Figure 7 - Do you have an anti-piracy operations team to monitor for piracy of your content, and take remedial action?



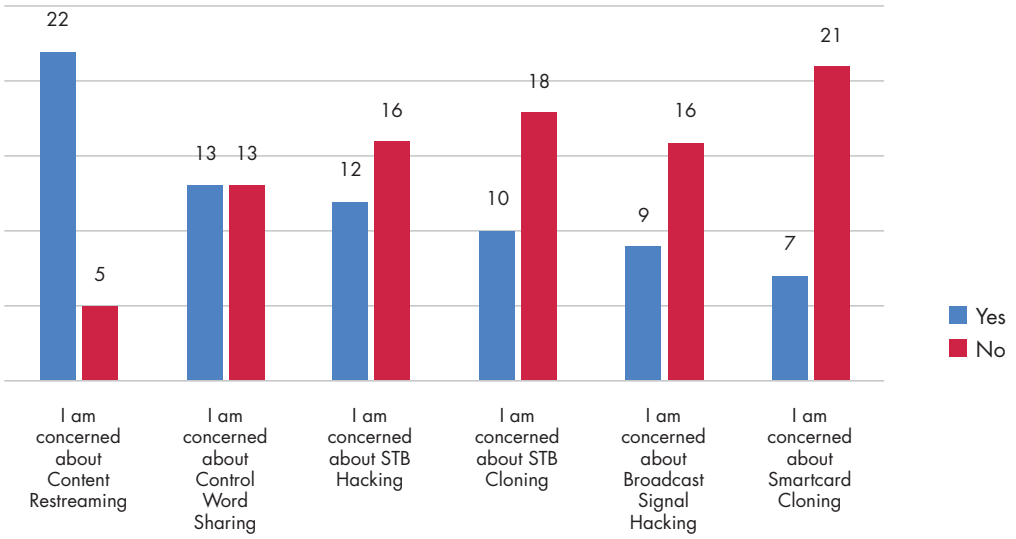
TODAY'S THREAT MODEL

Survey Response

Our survey respondents provided insight into the threats that concerned them, as shown in Figure 8.

We will analyze the top four concerns in more detail in the following sections. Smartcard cloning and broadcast signal hacks (modification of the CA system messages in the broadcast stream to enable access to content) are of lowest concern to our respondents, so will not be discussed in detail.

Figure 8 – Respondent concerns from our survey



As we explore the top four concerns, we will take the view of the pirate. Pirates can be professional or amateur, well-funded or just hobbyists 'in it for the kudos'. In the past, there has been evidence that the groups that operate card-sharing services have links with organised crime syndicates and other criminal activities such as credit card fraud.

When launching a new service, a pirate will consider:

- Cost (time and money) of hacking a device.
- Cost of distributing hacks/devices.
- Ability to reliably reproduce hacks/devices on an ongoing basis.
- Ongoing need for cable access/satellite dish by the end user.
- Enabling of new revenue streams – subscriptions, advertising, etc.
- Risk of being identified (subscriber fingerprint, IP address, etc.) and subsequent prosecution.

These will all be balanced against any potential revenue from the service.

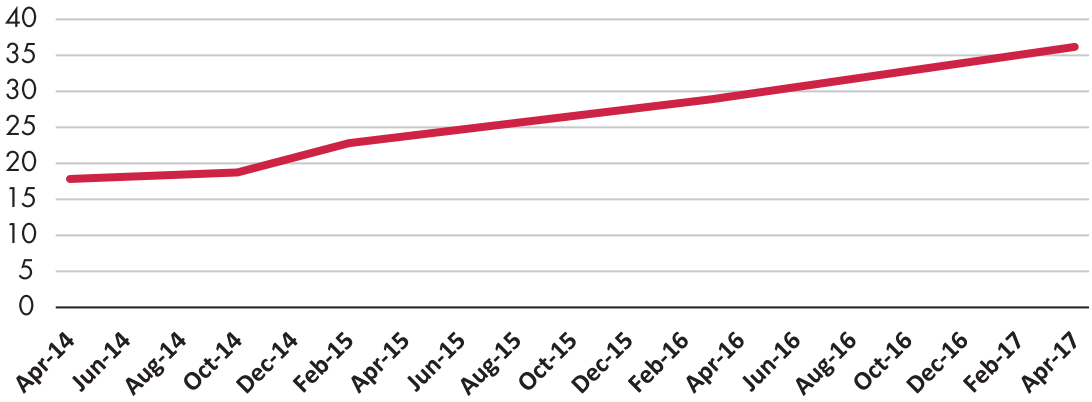
Content Re-Distribution

PIRATE VIEW: A pirate intercepts the video output and re-distributes over the internet.

The rollout of high speed broadband across the globe has continued to grow over the last 5 years. In the UK, we have seen average download speeds double in the last 3 years.

Higher broadband speeds mean that the ability to share video over the internet has grown substantially, and continues to grow[2]. For the pirate building a re-streaming service, the technical barriers to video sharing are much lower than 5 years ago, with the continued growth of easily accessible cloud-based technology making re-distribution at scale practical and cost-effective.

Figure 9 - UK average download speeds[1]



To obtain content, the pirate is likely to attack the weakest link in the chain – the display device (or the link to it). The pirate has several methods available to acquire the content from an authorized device:

- Capture a high quality copy of video from a legitimate display – the 'analogue hole' (e.g. camcorder from TV).
- Capture the content from a PC-based VoD service using screen capture technology.
- Capture the content from the HDMI link using an HDCP stripper. Devices are available that can take HDCP-protected content from the baseband HDMI set-top box (STB) output and be used to then stream into a PC video capture card, where the stream can be re-encoded.

These methods are simpler to execute than alternatives such as hacking a STB to obtain encoded 'bit perfect' video from memory buffers. For many 'consumers' of these pirated services, quality may not be the most pressing reason for using pirated content. They seek access to content when they want it, wherever they want it. The ability to view content on-the-go provides an attractive consumer experience.

Live Re-Distribution

This type of piracy is increasingly pervasive as one only needs an off-the-shelf device with a web-browser to view the content. This covers the whole spectrum of devices, from smartphones and laptops, to media streaming devices. There are paid services with high quality content, down to free services with web pages often infected with malware links, adverts, etc. These services tend to host live content.

Peer-to-Peer Sharing

Peer-to-peer (P2P) file sharing (usually via the torrent file format) has been commonplace for many years. The rise of high speed broadband has enabled very large files to be shared quickly (e.g. a 700MB HD re-encode of a movie can be downloaded in a few minutes on a 20Mbps connection). P2P sharing is generally still the major threat for long form movie/box set content. Some titles are so popular and the means to share so organised that it is possible to watch a P2P-received title in real time (e.g. using Popcorn Time – a multi-platform integrated torrent client and media player).

Apps

Legal media streamers are available at retail, preloaded with applications such as Kodi, with dedicated software plugins that give a semi-professional electronic programme guide (EPG) 'look and feel'. Whilst there has been some clampdown[3] on sales of 'pre-loaded' Kodi media streamers, the plugins are readily available for after-market install by the user. Other apps such as Showbox and Mobdro are alternates to Kodi, and offer simple access to pirate content.

Key (Card) Sharing

PIRATE VIEW: Pirates distribute keys from a hacked device to generic DVB devices.

Key sharing involves intercepting the descrambling key at some point in the device (smartcard, smartcard link, STB chip software and/or hardware), and serving these keys out to users over the internet in real-time. Users obtain STBs containing the descrambling algorithm (which is commonly defined by the DVB) and the means to load the software to receive and load the descrambling

keys. Key sharing was widespread with older systems not using hardware-based key encryption mechanisms, and had the advantage that only a single hacked client device is required to extract the keys.

In the last few years, smartcard systems introduced hardware-based, strongly encrypted key transfer mechanisms to prevent key extraction from the smartcard to system-on-chip (SoC) link. As these mechanisms are rolled out, key sharing attacks have become less common, although many operators have legacy devices that cannot be upgraded. Cardless systems do not expose the control word at any point external to the SoC, making extracting complex. To our knowledge, this type of attack has never been successful against a hardware-based cardless system.

Another even more dangerous form of key sharing is where the 'session key' is distributed. The session key is used to encrypt the final descrambling keys and is changed infrequently (say monthly), whereas the descrambling key changes every few seconds. A hacker has only to distribute the session key meaning a real-time server infrastructure, and a reliable internet connection from the user, is not required. Users use the session key to decrypt descrambling keys as they are received in the stream, and subsequently the content itself.

Descrambling keys are commonly extracted by intercepting unprotected keys on the link from the smartcard to the SoC. Session keys cannot be extracted in this manner, and a reverse engineering of the CA system is required to extract session keys. This is a considerably more complex attack, although the session key is a more valuable target.

STB Hacking

PIRATE VIEW: Pirates distribute a reproducible attack on a legitimate STB.
This type of attack targets a legitimate STB, smartcard, or entitlement messages to give 'free' entitlements to services, sometimes on a genuine device.

If a hardware modification is needed to reproduce this type of attack, it either requires a highly skilled end-user or a custom STB (both may be costly). The need for the user to have a legitimate device and possibly a genuine (basic) subscription to the service as a starting point, could act as a deterrent.

This type of attack used to be possible to execute on older generation smartcards, but is generally not seen today. It is increasingly impractical with modern SoC security, as it requires expensive software and hardware techniques to execute reliably.

STB Cloning

PIRATE VIEW: Pirates manufacture and distribute STB clones.
In this type of attack, the pirate would reverse-engineer a legitimate STB with full entitlements, extract its key material, then load the keys into a clone device. The clone would have the same unique key material as the original[4].

Reverse engineering the device to extract keys and CA system algorithms is very hard but not impossible. Even with expert knowledge and tools this remains costly and time-consuming, impacting a pirate's return-on-investment.

This type of attack is arguably the hardest for the pirate to execute, but the rewards are great. It does however have two large deterrents for the pirate. Firstly, the pirate needs to manufacture a physical device and only distribute to those with access to the required reception equipment (satellite dish or cable access). Secondly, should the identity of the donor device be found, a single revocation message from the service operator could disable all clones simultaneously.

Summarising the Threat

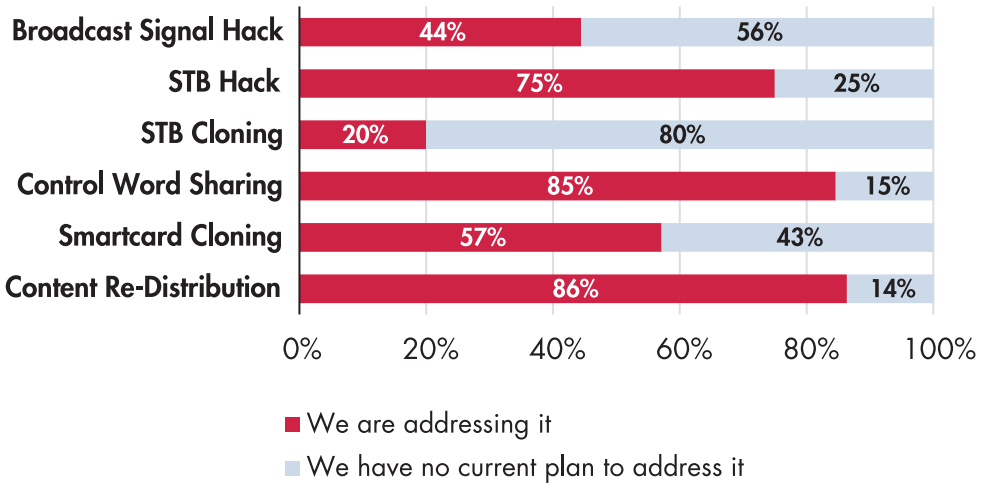
Returning to our 2012 whitepaper, we observed:

- We expect the focus of piracy to shift away from the hacking of broadcast networks, except in the case of operators that continue to provide a high-value opportunity to the pirate.
- Operators with a low volume of premium content or a low reach should expect the frequency with which their CA system is attacked to decrease as piracy focus turns to content re-distribution.
- The desire of pirates to attempt a perfect clone attack on a cardless CA system (which would force STB replacement) will drop, as the benefits to pirates reduce.

The respondents to our 2017 survey confirm that the shift to re-distribution as the primary threat has indeed happened. This shift is further confirmed when we look at the areas of concern that are actively being addressed by our respondents (see Figure 10). Organisational resources are being allocated to address key concerns such as re-distribution and control word sharing, but other areas such as STB cloning are not attracting remedial action. In particular, 86% of our

respondents are actively addressing content re-distribution, and 85% are actively addressing control word sharing. This reflects our observations from 2012 – organisations will only invest in areas of genuine perceived threat.

Figure 10 - For areas marked as a concern, are our respondents actively addressing the issue?



STATE-OF-THE-ART IN CONTEMPORARY SYSTEMS – CARDED

Smartcards are used in many industries, most notably bank cards, for their high security. A contemporary high security smartcard will have an array of anti-tampering measures such as:

- Shield protection against physical attack and light exposure
- Redundant/dummy logic
- Scrambled memory buses
- Detection of voltage, clock frequency, temperature and glitch attacks
- Obfuscated chip layout
- Obfuscated/scrambled non-volatile storage
- Side Channel Attack (SCA) resistance for security critical functions

Smartcards have been in common use for many years, and the technology is very mature. Indeed, our survey results show that respondents regard smartcard cloning as a low risk. The Common Criteria for Information Technology Security Evaluation (CC) Evaluation Assurance Level (EAL) regime provides a framework for security review and analysis of smartcard designs. Smartcard security remains very good, but there has been little significant innovation in smartcards over the last 5 years.

The Changing Role of the Smartcard

In a smartcard-based CA system, the smartcard carries out all of the broadcast message cryptographic processing (i.e. decryption and verification) and entitlement checking and management. When a user changes the channel and is deemed to be entitled to that channel by the smartcard logic, the control word is decrypted and sent to the SoC, where it is loaded into the content descrambler and viewing can commence.

The last 5 years has seen the introduction of very high value UHD content which has driven an increase in security measures across the whole STB environment. The MovieLabs Enhanced Content Protection (ECP) Spec[5] provides guidance for the industry developing secure devices for UHD consumption. This specification introduces security requirements that are beyond the control of the smartcard, including:

- Secure Video Path (i.e. no path from main CPU software to video path processors)
- Output control (i.e. instrumentation of (and ongoing trust in) HDCP configuration by fully trusted software only)
- Session-based forensic watermarking

As such, the smartcard functionality is now one component of a wider STB security environment.

Output control and watermarking are examples of functions which are executed within the SoC, and must be implemented in the same secure manner in both smartcard and cardless CA systems. If output control can be disabled by an attacker, content can be easily captured for illegal re-distribution. If watermarking can be disabled, the source of the content cannot be identified.

Control of these features is managed using CA system messages. In a smartcard CA system, the CA system messages are either decrypted within the smartcard which requires the vendor to

ensure that the smartcard to SoC link is secured against tampering, or are decrypted within the SoC, eroding the usefulness of the smartcard. In a best-in-class system, the final control of the feature within the SoC should be managed/verified from a secure environment, rather than just the STB middleware.

Whilst smartcards are highly trusted secure processing environments, they generally do not allow for major code replacement in the event of a breach. Countermeasures can be deployed to mitigate against security breaches, but these generally take the form of 'sleeper code' or minor patches to smartcard software; a smartcard replacement is of course possible, but this has significant cost and logistical impact.

SoC Security

The SoC provides a range of security functions including decryption of the content itself. The SoC also provides other features that have formed the backbone of typical CA systems, and includes:

- Secure boot chain for STB software, using hardware root of trust
- OTP hardware root secret(s)
- Hardware key ladder for CW decryption
- DRAM scrambling (to protect content in external memory from external snooping)
- Secure STB software upgrade
- Trusted Execution Environment and Secure Video Path (explored in more detail in the next section)

For over a decade, new smartcard systems have provided a hardware encryption mechanism between the smartcard and the SoC to prevent the extraction of control words for use by card sharing services.

STATE-OF-THE-ART IN CONTEMPORARY SYSTEMS – CARDLESS

Cardless CA systems take all of the functionality that would be resident in a smartcard and move it into the main SoC. We have already seen that smartcards provide a highly secure processing environment, so how is this trust maintained in the SoC?

Since the release of the first cardless systems, we have observed continuous innovation in the technology that supports it. Table 2 highlights the growing maturity of this technology.

Table 2 - Advances in cardless technology

Timescale	State of Cardless Technology
First cardless systems	• Software only running on main CPU. • Limited protection of keys and software against exposure.
5 years ago	• CA system client runs on main CPU, but uses hardware key ladders for control word decryption. • Decryption keys protected by hardware from key sharing attacks. • Hardware-based secure boot prevents software tampering. • CA system client remains a weakness, as it executed in same environment as other untrusted software.
Current state-of-the-art	• CA system client functionality split so that critical functions are executed with a Trusted Execution Environment, separated from the main CPU. • Hardware key ladders used for decryption. • Hardware-based secure boot prevents software tampering. • Critical functions protected against Side Channel Attacks. • Secure Video Path for premium content.

Trusted Execution Environment (TEE) for CA Client Execution

The most important development that has brought cardless CA systems to realisation is the appearance of a secure processing environment for the main CA message processing. This Trusted Execution Environment (TEE) provides a processing space that is logically or physically isolated from the main SoC CPU and hence the rest of the STB software. A well designed cardless solution will use this environment for critical CA system functions.

A TEE would typically feature:

- Exclusive access to off-chip RAM areas
- Privileged access to SoC hardware cryptographic resource/key ladders
- Private on-chip RAM resource (if TEE implemented as separate CPU)
- Run time integrity checking of TEE software processes
- TEE inter-process isolation

At the time of the 2012 report, TEEs were not available. The first TEEs appeared in high-end SoCs only, but as the market has matured these features have trickled down and have started to become standard across some ranges of SoC families. Now, all leading SoC vendors offer a solution.

The software executing within the TEE is protected from inspection and tampering, and can be upgraded alongside any other software component in the device. For connected devices, this gives operators great flexibility to keep software versions up to date, and to respond to breaches. Our survey respondents clearly saw the advantages gained from network connectivity when using cardless CA systems.

The TEE offers an execution environment for trusted applications, and may contain applications from multiple vendors. As with any software solution, vulnerabilities may exist within the trusted applications or within the TEE operating system itself which may leak sensitive material from the TEE environment. Good software development practice is essential. For some cardless solutions, some of the functions of a TEE can be executed by proprietary hardware cores. These solutions allow these vendors to adopt their own strategies for security and upgradability.

Side Channel Attack Resistance

The last few years have seen a concerted effort by SoC vendors to improve the performance of their embedded hardware cryptographic engines (e.g. TDES and AES) against Side Channel Attacks (SCA). A SCA extracts key material from hardware algorithms by gathering data from non-invasive monitoring of the SoC during operation. SCAs may involve monitoring of voltage levels or electromagnetic radiation. The lower cost of the equipment required to carry out these types of attacks and dissemination of instructions over the internet has brought it into the realm of the 'advanced amateur'.

Over the last 5 years, these 'hardened' algorithms are disseminating throughout SoC families and lower tier vendors. SoC vendors are increasingly using specialised penetration testing labs to test their devices against these types of attack.

Secure Video Path

A Secure Video Path (SVP) is generally understood to mean a video decrypt, decode, render and display path in the SoC that is implemented using secure firmware and hardware only, not accessible by the main CPU. Configuring an SVP is not without its challenges, but if done correctly it gives trust in the content path. Additionally, it allows a highly trusted means of instrumenting the video path for traitor-tracing mechanisms such as subscriber ID display and content watermarking technologies.

Secure Output Control

To protect video output over HDMI, HDCP encryption is used. There are several versions of HDCP, but only version 2.2 is considered secure enough for UHD content, due to compromises of previous versions. A device must enable HDCP when required, guarantee a minimum HDCP version, and ensure its ongoing enablement during content viewing.

A robust implementation of HDCP is essential to prevent an attacker disabling or down-versioning HDCP and capturing the unencrypted HDMI output for re-distribution. Solutions which control HDCP from the main CPU/middleware are potentially at risk of attack. Implementation within the trusted environment of the TEE ensures HDCP is enabled within a secure environment, and remains enabled over time.

COMPARING CARDED AND CARDLESS

The risks faced by carded and cardless systems are compared in tabulated form in Table 3.

Table 3 – Comparing smartcard and cardless CA systems

Pirate View	Attack	Smartcard	Cardless
Key (card) sharing	Session key sharing	Very low, assuming robust SoC and smartcard	Very low, assuming robust SoC
	Control word sharing	Low, assuming robust SoC and smartcard	Very low, assuming robust SoC (keys not exposed on public bus)
Enable free entitlements on a legitimate STB	Entitlement escalation (single device)	Low, assuming contemporary smartcard	Low, assuming good implementation, TEE and SCA resistance
Sell pirate STBs giving free entitlements to channels	Clone (OTP copy)	Very low, assuming robust SoC and smartcard	Very low, assuming robust SoC
Content sharing	Access content (copy from memory buffer)	Medium, SoC and software dependent	No difference to carded
	Access content for re-distribution (HDCP disable/ down-version)	Medium, SoC and software dependent	No difference to carded
	Access content for re-distribution (HDCP strip)	High,outside of SoC/ STB control	No difference to carded

Carded

For smartcard CA systems, the weakest link is the bus between the smartcard and SoC, as confidential descrambling keys are exposed on external buses. As we have seen, modern systems now encrypt the keys on this bus. A cryptographic brute force attack on the encrypted

control words is possible in theory, but a good choice of encryption algorithm and key length makes this attack impractical.

Smartcards are designed and constructed with a focus on security, and are regarded as very secure. Should an attack be created which acts on the smartcard alone, and such an attack is identified by the operator, then the smartcard can be replaced without a STB swap. With high levels of security within smartcards, pirates are less likely to attack them directly if other components of the system are easier targets.

As we have seen, the SoC has a critical role in the security of the device, even when a smartcard solution is used. A smartcard solution must provide a security solution within the SoC to the same standard as a cardless solution to ensure content is fully protected.

Cardless

For cardless systems, the overall robustness is predicated only on the robustness of the SoC and the environment within, which hosts the CA client. The SoC should ensure that the unencrypted descrambling keys are never exposed outside the SoC, and are not visible to untrusted components within the SoC. Similarly, the SoC and CA system should together ensure that all confidential information does not exit the boundary of the TEE.

Dependence on the SoC

Unlike the Common Criteria certification in place for smartcards, there is no 'pan-industry' certification scheme for SoCs. As such, whilst vendors may boast of having a slew of security features, a thorough review and testing activity is required to build confidence, to include:

- Analysis and review of SoC security architecture (detail of implementation, maturity, etc.)
- Detailed definition and review of particular SoC configuration
- Penetration test of SoC hardware by specialist labs
- Test of CA client as hosted in the production SoC environment

For both carded and cardless, the SoC is the least common denominator. It makes no sense to have an unbreakable smartcard if the pirate successfully attacks the SoC/STB. Of course,

security can always be beaten, due to either a poor design or an innocent bug in an otherwise complex design. As our survey respondents commented, the aim is to raise the bar high enough to stop people attacking the devices, which is why thorough testing by specialised parties is so important.

With the SoC as the common factor in a modern CA system, we see the difference between cardless and smartcard CA systems has closed.

CONCLUSIONS

We conclude this white paper by summarising our key technology takeaways, offering our predictions for the next 5 years, and revisiting the takeaways from our 2012 whitepaper.

Our Key Technology Takeaways

We have reviewed the technology used in cardless and smartcard CA systems in this white paper. Here are the two most important messages from our review:

1. Modern high quality cardless CA systems leverage TEEs, hardware key ladders and other security features in the SoC. These features isolate and protect critical CA system functions, and deliver solutions of comparable security to smartcards.

2. The security of the SoC is critical in both cardless and smartcard CA systems. Many of the security requirements from content owners must execute within the SoC, including output control, watermarking, and Secure Video Path. Poor SoC implementation makes devices an easy target for pirates, even if a highly secure smartcard is in use.

Our Predictions for the Future

We will now turn our attention to the future. Firstly, let's consider the two leading concerns highlighted in our survey and how they will evolve over the next 5 years:

- **Content re-distribution.** We predict that re-distribution of content on the internet will continue to grow. As consumers increasingly view content on-the-go, streaming will remain a massive threat. Content rights owners will encourage and enable further cross-industry collaboration to continue the fight against this form of piracy.

- **Control word sharing**. Control word sharing will continue to decline over the next few years as older devices are gradually replaced with smartcard solutions which encrypt control words, or are replaced with cardless solutions. The rate of decline is driven by operator upgrade timescales rather than technology limitations, and ultimately it may be content owners who drive operator upgrade cycles.

Secondly, let's offer our predictions for technology change in the next 5 years:

- **Cardless technology.** Innovation will continue in cardless technology to meet the growing needs of very high value content. As we have seen, the quality of the SoC is critical to the security of the CA system. Over the next few years we will see current state-of-the-art SoC security features being deployed throughout SoC product ranges, giving CA vendors more choice and lowering costs. Increasing standardisation of TEE environments will ease deployments for both CA system and SoC vendors.

- **Cardless deployments.** Cardless deployments will continue to grow as operators seek to manage operational costs where they can. However, smartcard solutions will continue to be deployed, although this likely to be increasingly limited to markets with existing smartcard devices and head-end systems.

- **Watermarking.** Watermarking deployments will continue to grow, as UHD and premium sports content owners start mandating its usage across all devices. Over the next few years, watermarking will increasingly become mandated by content owners, with premium live sports content leading the way.

- **Connected devices.** Devices are increasingly connected, giving operators more options for in-field management, and for anti-piracy operations. This trend will continue.

Revisiting our 2012 Takeaways

In this final section, let's look back at our original 2012 white paper and revisit our four takeaways.

2012 Takeaway #1: **New security technologies lift the barriers to hacking cardless systems as high as those to hacking card-based systems, as long as they are implemented correctly.**

Our survey results show that more than half of our respondents now agree that the security offered by cardless CA is now comparable to smartcard-based CA systems, with less than one fifth of respondents disagreeing.

As we've shown, modern SoCs offer security capabilities that make them ideal platforms for delivering advanced cardless CA systems. The introduction and increasing deployment of TEEs in the SoC give a very secure environment for the execution of a cardless CA system software, which can be quickly and easily upgraded without the need for a smartcard replacement.

Further, new content requirements introduced by the MovieLabs ECP Spec demand an increasing role for the SoC itself. Secure Video Path, output control and watermarking are examples of functions that require SoC implementation, eroding the role of the smartcard in device security.

A modern SoC, with a robust cardless implementation, is secure enough to deter most from a direct attack on the device.

2012 Takeaway #2: **Operators with a low volume of premium content or a low reach should have expected the frequency with which their CA system was attacked to decrease as piracy focus turns to content re-distribution.**

Our survey shows that the focus of concern in the industry has moved further towards content re-distribution.

The threat of content re-distribution is present in both cardless and carded solutions—both must implement the same level of robustness in the SoC to countermeasure this threat.

2012 Takeaway #3: **Cardless CA systems are appropriate for operators with a low volume of premium content or a low reach, although we recommended the inclusion of a smartcard slot as a precaution to mitigate the risk of having to replace all devices.**

A modern smartcard solution has functionality in the SoC as well as the smartcard itself. Smartcard replacement can only mitigate attacks of smartcard functionality. Attacks to the SoC which target functions such as descrambling, video decoding, watermarking and output protection enforcement cannot be mitigated by smartcard replacement.

Further, there is no standard method available for control word encryption on the smartcard to SoC link – all implementations are vendor specific. This means that migrating from a cardless to a smartcard solution from the same vendor can be planned for during design, but migrating to a smartcard vendor who was not identified during design may not be possible.

Since today's SoCs are optimized for delivering advanced cardless security, cardless CA systems are suitable for large subscriber deployments and major service offers of premium content.

A spare smartcard slot is only suitable for switching from a cardless to a smartcard solution from the same vendor, and cannot be used to manage breaches of SoC resident functions. A spare smartcard slot may therefore be of limited value and may simply carry additional cost for operators.

Cardless CA systems are now suitable for all deployment sizes, and are no longer limited to smaller deployments.

2012 Takeaway #4: We recommended that operators must implement technologies that enable the direct fighting of content re-distribution and control-word sharing, such as watermarking, fingerprinting and monitoring.

As we have seen from our survey, content re-distribution and control word sharing are the biggest threats in our survey. Regardless of the piracy method, tracing the source of the leak is critical. We continue to recommend the inclusion of session-based forensic watermarking in any CA system deployment, and indeed it is increasingly considered a must-have for very high value content (live sports, UHD, etc.).

Watermarking has no value without a monitoring solution in place. 70% of our survey respondents have an anti-piracy operation in place, either internal or external.

Again, we recommend that anti-piracy operations are put in place, and encourage cross industry collaboration where possible.

[1] http://www.ispreview.co.uk/index.php/2017/04/ofcom-2017-study-average-uk-home-broadband-speeds-rise-362mbps.html

[2] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

[3] http://www.digitaltveurope.net/658391/five-arrested-in-uk-clampdown-on-illegal-tv-set-top-boxes/

[4] The concept of a 'minimal' clone is slightly different, and describes a device that does not require the same CA system processing software as the original. A minimal clone would in fact be akin to a client making use of shared session keys)

[5] http://www.movielabs.org/ngvideo/MovieLabs%20Specification%20for%20Enhanced%20Content%20Protection%2v1.1.pdf

Verimatrix specializes in securing and enhancing revenue for multi-network, multi-screen digital TV services around the globe and is recognized as the global number one in revenue security for connected video devices. The award-winning and independently audited Verimatrix Video Content Authority System (VCAS™) family of solutions enables next-generation video service providers to cost-effectively extend their networks and enable new business models. The company has continued its technical innovation by offering the world's only globally interconnected revenue security platform, Verspective™ Intelligence Center, for automated system optimization and data collection/analytics.

Its unmatched partner ecosystem and close relationship with major studios, broadcasters and standards organizations enables Verimatrix to provide a unique advantage to video business issues beyond content security as operators introduce new services to leverage the proliferation of connected devices. Verimatrix is an ISO 9001:2008 certified company. For more information, visit **www.verimatrix.com**.

Cartesian, Inc. (NASDAQ: CRTN) is a specialist provider of consulting services and managed solutions to leaders in the telecoms, digital media, and technology industries. For 25 years, we have helped clients worldwide build and execute strategies that transform the products, services, and organizations that shape the industries in which they operate. Cartesian's security consulting team supports service providers and content owners deliver secure solutions to meet the needs of today's demanding premium content. Our company has offices in Boston, Kansas City, London, New York, Paris, Philadelphia and Washington. For more information: **www.cartesian.com**.