Oct 2009

Towards a Replacement for the DVB Common Scrambling Algorithm

Farncombe White Paper

Farncombe Consulting Group
Belvedere, Basing View, Basingstoke, RG21 4HG, UK
Phone: +44 1256 844161 Fax: +44 1256 844162
www.farncombe.eu / info@farncombe.eu

© Copyright Farncombe Consulting Group 2009

Table of Contents

© Copyright Farncombe Consulting Group 2009

Introduction

After many years of hype, TV/Internet convergence is finally with us, at both the service and device level.

As consumers seek to receive video from multiple providers in any place, at any time and on any device, they routinely consume video over the Internet on PCs and on smart-phones, as well as through traditional digital set-top boxes.

Operators have responded to this demand by providing their premium content to their subscribers via broadband through over-the-top streamed video services, and – in both the pay-TV and free-to-air environments – hybrid DTV/IP receivers are being commissioned which seek to bring the Internet online video experience to the TV screen alongside conventional one-to-many broadcasts.

In this context, Farncombe believes that the technology at the heart of the DVB's conditional access system – the Common Scrambling Algorithm (CSA) – has, despite the laudable motives behind its creation, become a liability for pay-TV operators.

As we explained in our previous White Paper, the way it is used contains a flaw which creates a piracy risk (so-called control-word sharing) which is exacerbated by the growing ubiquity of residential always-on fast Internet access.

For as long as most ordinary consumers found it difficult to physically link their digital TV and broadband networks, this weakness has tended to be exploited only by dedicated hackers. However, convergence in the form of IP-capable STBs and IDTVs, supported by user-friendly in-home wireless networks, increases its potential.

Many operators are aware of this, and are swapping out their installed receiver bases as a result. However, they risk losing their investment, because the inherent weaknesses of the CSA are being replicated in their new STBs.

Indeed, Farncombe believes we are now at a possible tipping-point, where control-word sharing could explode and threaten the pay-TV industry with the same illegal downloading practices which have undermined the music sector.

We also believe the CSA is distorting the market, through the fact that it is, to one degree or another, a mandated technology within the DVB system.

In our view IPTV players often do not feel obliged to include such a hardware-based encryption system in their devices. This leaves their 'traditional' DVB-based rivals facing increased costs, not least because it is expensive to implement in-home distribution to different devices when the starting-point is an embedded hardware device. These are not issues faced by IPTV operators using software-based CA.

For these and other reasons, Farncombe believes it's time the CSA was replaced. It was designed for an era when operators were keen to avoid their content being distributed to what they perceived as

© Copyright Farncombe Consulting Group 2009

the insecure environment of a personal computer, and where broadband did not exist as a distribution medium, for either legitimate or pirated content.

This White Paper lays out in more detail the arguments for replacing it, and sketches out a toolkit-based approach which we think could reconcile regulatory and competition requirements with operators' business and technology needs.

For those who are not interested in the niceties of control-word sharing and why the CSA allows it, the 'technical aspects' may be skipped. For those who wish for a more elaborate explanation or want to understand how operators might protect their investment in future STB generations, contact us (see Annexe 2 for contact details and more about us).

© Copyright Farncombe Consulting Group 2009

The CSA and Simulcrypt: business aspects

Distribution to PCs

Fifteen years ago, the CSA – and the Simulcrypt system it was designed to enable (see Annexe 1) – were conceived in an environment where PCs were regarded by the DVB membership as inherently insecure devices, to which it was undesirable to distribute premium TV content. In any case, at the time their processing-power, memory and storage capacity were such that they were unable to render long-form high-quality broadcast video in a user-friendly or viewable manner. The CSA was accordingly engineered in such a way – that is, as a hardware-based encryption algorithm (see Technical Aspects section) – as to seek to confine its implementation to set-top boxes (whether standalone or integrated into digital TV sets).

Today, the PC security issue has arguably been addressed: although some concerns remain, the Hollywood majors now allow their premium content to be conveyed by pay-TV operators such as Canal+ (and many others) over broadband to their subscribers' PCs, using software-based DRM systems such as embedded in the Microsoft Windows Media Player[1].

In the circumstances, an entirely understandable, if not praiseworthy, decision to bar DVB content from PCs now seems increasingly perverse. Surely, European operators required to use DVB-compliant equipment should be free to choose a technology approach which facilitates their business objectives – and this now includes Internet distribution to the PC and in-home distribution of content to different devices. This is all the more important given the need to accustom consumers to paying for video content on the Web rather than illegally downloading it.

Regulation and competition

Again, 15 years ago, there were sound regulatory and competitive reasons for creating a unitary algorithm as part of the DVB ecosystem (see Annexe 1): it promoted interoperability and the idea that consumers only needed to buy one set-top box. Regulators could use it to enforce the adoption of a Simulcrypt approach to promote competition between rival pay-TV operators; or pay-TV operators themselves could adopt Simulcrypt to allow different populations of pay-TV boxes to access the same content – for example, following a merger.

From an industry point of view, providing a common CA hardware element in receivers which was independent of individual CA technologies was also of considerable benefit: it prevented (and still does) CA vendor 'lock-in' – the process by which a CA vendor would prevent a particular set-top box hardware configuration working with another CA system, hence limiting competition.

A common algorithm also lowers the entry-barrier for new CA vendors, and allows operators to swap between different CA systems relatively easily – for instance, if their existing system becomes hacked.

[1] Canal+'s Canalplay service even claims to offer its premium movies in this way in HD quality: http://www.canalplay.com/pages/aide/hd/telecharger-hd-haute-definition.aspx

© Copyright Farncombe Consulting Group 2009

The CSA is a system that is mandated under European law for 'digital television' (see Annexe 1), but exactly what this means in practice is unclear. For instance, it is the implementation of the CSA in receivers that is mandated, not its actual use. Moreover, as the DVB itself recognizes, "the wording of the Directive is open to interpretation", with different Member States enforcing its provisions in different ways. Thus in many EU territories there is no requirement to implement the CSA in IPTV systems (which, as already noted, mainly rely on software-based content security technologies). Even where there exists such a requirement, it is often ignored.

This favours the interests of the IPTV operators. Not only do their set-top boxes (in most cases) omit the cost of a hardware element that is compulsory for their cable, satellite and terrestrial competitors, but their software-based approach means they can distribute content much more easily around networked homes. This means they can target PCs with video content which – even if multicast rather than broadcast – represents by any other name what European legislation describes as a 'digital television signal' (the trigger for inclusion of the CSA within a set-top box).

In a cable context, for instance, content-owners would not allow an encrypted broadcast signal to be received and decrypted by a set-top box, and then passed in the clear to other devices around the home. It would first have to be distributed in its protected form and then pushed through a hardware device or hub containing the CSA before being rescrambled or transcrypted for other devices. In effect, use of the CSA in this situation forces multiple decryptions (and at least one re-encryption) in order to pass content around the home. This not only increases the cost and complexity of the in-home customer premises equipment (CPE), but it creates more attack-points and thereby an increased piracy risk.

Such a process is also fundamentally illogical, in that it initially uses a hardware-based algorithm designed to stop content being made available to a PC before re-scrambling that same content to make it available ... on a PC. It also means the cable operator incurs additional CPE costs and security system costs compared to its IPTV competitor, and is forced to use two separate systems (a DVB one and a non-DVB one) for in-home content distribution.[2]

One of the consequences of this situation is that if the operator were to decide not to implement such a DVB CA system conversion inside the CPE because of its expense and complexity (if not its vulnerability), this would have the undesirable effect of frustrating those early adopters within its subscriber base who were keen to play back content on their PCs, portable media players or smartphones. In such a situation, it is increasingly common for such users to seek access to equivalent premium content through illegitimate means – for instance through illegal file-sharing.

The DCB CSA gives rise to two other market distortions, in our view. It is possible, for instance, to address the control-word sharing risk implicit in the use of the DVB CSA system by persuading STB chipset suppliers to make hardware modifications to their standard lines so as to render them more secure – for instance by allowing secret information to be stored in hardware.

However, the majority of CA vendors do not have the market power to be able to commission such modifications, and therefore generally have to rely on off-the-shelf hardware solutions. By their very

[2] Such burdens apply to other types of DVB broadcast service, too.

© Copyright Farncombe Consulting Group 2009

nature, then, their CA solutions are more prone to the type of control word-based piracy attack we have described.

On the other hand, the market leaders are able to 'harden' STBs in precisely this way, simply because they control most of the global CA market between them, allowing them to dictate more secure bespoke hardware solutions. This is a significant differentiator between their CA products and those of the smaller players, and reinforces their market dominance.

Ironically, a system set up to encourage vendor competition by preventing 'lock-in' actually serves to diminish it in practice.

The second, unintended anti-competitive implication of the use of the DVB CSA relates to the Simulcrypt approach itself. Yes, it allows regulators (or the players themselves) to impose interoperability. But what if there is no regulatory or commercial pressure for the adoption of such a model? Given the security weaknesses already described, the operator is effectively being forced to adopt a less secure solution than a competitor who – for whatever reason – is not implementing the CSA.

In such a situation, content owners would be better off if pay-TV operators were free to use their own proprietary scrambling algorithms rather than the CSA. Their content would not only be less exposed to attack (since these proprietary scrambling technologies would by definition not be ubiquitous) but this would not lead to piracy on any other operator's decoders (see Technical Aspects section for the explanation).

The market is in any case moving away from a model which concentrates on securing the delivery mechanism, as DVB CSA does, to one which secures the content (whether in transmission or whilst it is being stored within consumer equipment) and controls access to that secured content. This is, indeed, what the various Digital Rights Management (DRM) systems used by IPTV operators claim to do.

While the DVB standard can be viewed as offering short-term protection (assuming content is viewed in real time and not stored), a properly-implemented DRM solution will offer long-term content protection. The rapidly-increasing penetration of the PVR, and the growing requirement by consumers that they should be able to play back recorded content from any display in the home, underlies the way in which the world is shifting to a content-focused model.

In order to address this development, what is needed is a system which *facilitates* the operator's ability to distribute content around the home (via the Internet if necessary) rather than impedes it, so that the industry can create a legal, user-friendly way of accessing paid-for premium content. Apple has shown the way with iTunes, but the CSA is – to a certain extent – preventing the evolution of a similar system for video.

To sum up, the CSA/Simulcrypt approach – which managed to reconcile supporting and protecting pay-TV operator's businesses with the promotion of vendor competition and the possibility of regulatory intervention – is, in today's radically changed technology environment, having precisely the opposite effects.

© Copyright Farncombe Consulting Group 2009

The CSA and Simulcrypt: technical aspects

Simplified account of a typical DVB CA system

Typically, in a DVB environment the digital data making up the broadcast signal is encrypted (which is to say, made unreadable) just before transmission using an 8-byte secret key, known as a control word. This is changed frequently, with successive values being derived automatically and randomly, so as to be unpredictable.

In a smartcard-based CA system, a secure smartcard acts as the STB's security processor – and in order for it to decrypt the broadcast, it needs to be kept up-to-date in real time about the changing values of these control words. This is done by broadcasting data to the STB.

However, since this data could be modified, or – if secret data is used – be discovered, it must be protected: this is done by a combination of signing messages and encrypting data where necessary, in a manner which is specific and private to the CA system. Extra information is also added to these secured messages telling the STB what authorisations it requires in order to be allowed to view the broadcast. The resulting bundles of data are known as entitlement control messages (ECMs).

Separate chunks of protected information called entitlement management messages (EMMs) are sent out in parallel. These tell the STB what authorisations it currently has (as opposed to the ECMs, which tell the STB what authorisations it needs to access a given program), and thus control what programmes can be watched (i.e. unscrambled). Both the ECMs and EMMs are transmitted as part of the broadcast signal, and on reception are processed by the smartcard.

The mechanisms used by the smartcard to process these messages, and to manage the cryptographic algorithms and/or keys, are proprietary and specific to each CA system.

Concepts underlying the DVB CSA system

The final part of this process is, with reference to this White Paper, the critical one: the market assumption at the time the CSA was created was that it didn't matter if a hacker managed to discover a control word at the point where it was passed without any protection from the smartcard through the set-top box to the descrambler. Since control words are continually being changed, by the time the hacker was in a position to apply the control word to the descrambler in an unauthorised box, it would be too late.

There is therefore no requirement for control words to be protected under the DVB scheme – indeed this issue was deliberately left open to allow a given set-top box hardware configuration to work with any CA system. CA vendors may choose to protect control words within the proprietary parts of their CA systems, but they are not able to do so in a way which creates 'lock-in' – with all the competitive market benefits described in the previous section.

This approach was underpinned by another technology decision: the deliberate choice and design of a scrambling algorithm for the CSA that required so much processing-power that it would be very

© Copyright Farncombe Consulting Group 2009

difficult to carry out in software – only a dedicated chipset could do the job. This theoretically added a further beneficial aspect: it made the CSA hard to reverse-engineer.

Finally, the algorithm itself was kept secret in order to increase the level of security offered, only being provided to bona fide digital TV companies who signed up and agreed to abide by a rigorous set of non-disclosure conditions administered by the European standardisation body, ETSI.

The threats posed by the CSA today

Today, none of the above assumptions – made in the light of what was known about the technology environment at the time, and for the best possible motives – hold true. The nature of the CSA is now known[3,4] and although it has not been broken, Farncombe is aware of websites claiming that open-source implementations of it are available on the Internet.

Of most significance, however, as we noted in our previous White Paper, is the fact that the DVB CSA approach now makes piracy attacks possible through 'control-word sharing', historically known as the 'Wizard' or 'McCormack' hack. A single, modified STB is used to feed a stream of in-the-clear control words across the Internet to a large population of pirate devices – which only need to contain a hardware or software DVB-standard descrambling system to be able illegally to access premium content.

This technique is used in many ways, for both private use and commercial gain. In the former case, users may distribute control words informally within their home, or friends may share control words between homes and across small networks. Until relatively recently, these were the most prevalent modes, and were confined to a minority of hackers with the means to access a pay-TV operator's decrypted stream of control words, and apply them to a DVB set-top box.

Latterly, however, the practice has spread to so-called 'card-sharing' networks, who – in the most extreme cases – run large-scale websites with servers spread across the globe, offering services covering every major market, and charging fees which are not passed on to the pay-TV operators. We have found at least one brazen but unverified example of a site which is targeted at reception of European satellite-based pay-TV services using a Dreambox DTH receiver, with prices starting at £20/month.[5]

[3] Ralf-Philipp Weimann and Kai Wirt Analysis of the DVB Common Scrambling Algorithm, 8th IFIP TC-6, TC-11 Conference on Communications and Multimedia Security, CMS 2004

[4] Wei Li and Dawu Gu Security Analysis of the DVB Common Scrambling Algorithm, The First International Symposium on Data, Privacy and E-commerce, ISPDE 2007, 1-3 Nov 2007.

[5] The site is surprisingly open about what it is doing, explaining that: "Card sharing is a method by which independent receivers obtain simultaneous access to a pay television network, using one legitimate conditional access subscription card. Typically, the legitimate card is attached to a personal computer or Dreambox which is connected to the Internet, and is configured to provide the legitimately decrypted control word to other receivers who request the information. This decrypted control word is then used to decode an encrypted conditional access service, as though each other receiver were using its own subscription card." We do not wish to give publicity to this site or other similar ones, but please contact Farncombe if you want more details about this growing threat to pay-TV operators.

© Copyright Farncombe Consulting Group 2009

One can, of course, use both technical and legal means to confront and take down such operations. But while combating smartcard piracy in this way may work in the initial stages of a hack, the interest-levels generated by viral distribution across the Internet of the details of such breaches, and the rate at which new sites then spring up, soon overwhelms any anti-piracy operation until the underlying security breach is closed. Thus even if the card-sharing sites known about today were closed down, we believe many others would follow, with increasing market penetration. Such exponential growth has been a common characteristic of other security breaches.

In Farncombe's view, the growing ubiquity of always-on, fast Internet access, and its convergence with set-top boxes at the TV receiver, greatly exacerbates this threat. Such a stream of control-words can now potentially be distributed in real-time over the Internet to DVB receivers around the world, which increasingly (whether as a hybrid DVB/IP STB or a 'connected TV') now embed an Ethernet interface. Even where such hybrid devices are not present, operators increasingly facilitate the linkage of DVB broadcast networks and broadband networks by providing their subscribers with wireless hubs or powerline adapters. Piracy can now take place under the TV set in a manner which wasn't possible before.

Many operators are aware of the control-word sharing risks, and are swapping out their installed receiver bases for more secure models as a result. However, although there are acknowledged methods for making it more difficult for control words to be intercepted, ultimately there will always be an interface to the CSA which a dedicated hacker could uncover.

The critical problem here is that the CSA is replicated across all DVB boxes. Only *one* of the pay-TV operator's new set-top boxes has to be hacked into in such a way as to make the stream of control words visible. That pirated stream can then – in principle – be applied in real time to *any* of its set-top boxes, potentially putting all of the operator's premium content in the clear. Indeed, since *all* DVB set-top boxes contain the CSA, the same hacked control word stream can then be applied to the boxes of a different pay-TV operator, or indeed a retail STB, since these would not be able to distinguish an illegitimate control word stream from a legitimate one.

The DVB common interface (DVB-CI) provides another potential security flaw. As part of the original strategy for avoiding 'lock-in', this interface is mandated in all European IDTVs, and was designed to allow a digital TV set to receive different pay-TV operators' offerings simply by plugging a CA module or CAM containing the appropriate CA system into the DVB-CI slot.

The DVB CI was specifically designed to allow CAMs to descramble MPEG-2 transport streams: thus control-word sharing could in principle be used to allow rogue CAMs to decrypt all the broadcast services capable of reception by today's (mainly) MPEG-2-based IDTVs.

It may be thought that MPEG-4 services are not vulnerable to this attack: in fact, the use of a CAM which converts MPEG-4 to MPEG-2 would allow the same IDTVs to receive (and pirate) new MPEG-4 services (HD as well as SD) as well. This is significant, in that it underlines the point that the upgrade to MPEG-4 and the associated use of more secure set-top boxes in an MPEG-4 environment do not fully address the DVB CSA security flaw.

© Copyright Farncombe Consulting Group 2009

While there have been attempts to make the CSA more secure, we believe these have been mis-directed. The DVB Project did specify a more robust version of the CSA in 2008 known as DVB-CSA3, which Farncombe understands from an industry presentation[6] is based on elements of the Advanced Encryption Standard (AES), to increase the algorithm's resistance to more sophisticated attacks in the future.

But, since the existing CSA has not so far been broken, this misses the point. CSA3 has hardly reached the latest chipsets and all decoders would have to implement it for it to be effective. It is usually very difficult for operators to roll out new technologies given their legacy installed bases, and it is likely that by the time a major operator had managed to upgrade all of its set-top boxes to CSA3, the pirates would have figured out how to distribute CSA3-compatible devices *en masse*.

It is the CSA approach itself, with its reliance on a single mandated algorithm using control words transported in the clear between devices that do not authenticate each other and do not ensure a secure communications channel, which is the problem. Using a card-sharing service, as we have seen, a non-subscriber may watch a pay-TV operator's programming without paying for it on a Dreambox. This is not because the CA system used by that operator is insecure, but because the DVB approach created 15 years ago allows a device like the Dreambox to be built without breaking the law.

To sum up, the CSA no longer offers the degree of content security that it used to. Indeed, we would argue that TV/Internet convergence is creating an imminent risk that it will no longer offer an acceptable degree of content security at all.

In the past, where piracy was only viable on the key management system, the industry reacted by making the key management system renewable and placing it within the smartcard. That way, when the system was hacked, the smartcard could be replaced. Today, as we have argued above, the pirate attacks have now moved towards the descrambler architecture and the content flow in the device. The industry now needs to look at how to make these components as renewable as possible.

Clearly, such renewability cannot be achieved for a hardware-based system such as the CSA.

[6] http://www.zetacast.com/Assets/DVB%20World%202008.pdf

© Copyright Farncombe Consulting Group 2009

Next steps

Given the technical and competitive deficiencies outlined above, how might one go about designing a replacement for the CSA?

Clearly, any solution needs to reinforce the use-case and business objectives of stakeholders – be they operators, content-owners, regulatory authorities (at EU and national level) or consumers.

1) First, the advantages that the CSA gained for regulators and consumers in terms of interoperability must not be lost. The CSA's ubiquity underpins the Simulcrypt concept: it was necessary for every DVB device to include the CSA, in case Simulcrypt needed to be implemented in a particular territory or context – it could not be 'retro-fitted.' Thus any solution that is found should achieve the same objectives originally set out by the DVB – viz. "to enable the concept of the single receiver in the home of the consumer."[7] To put it another way, while the issues we have described in this White Paper are not dependent on the Simulcrypt concept, its replacement must address some similar structural requirements.

2) Second, the competitive supply of CA systems must be ensured, in order to allow both large and small operators to deploy secure systems at a reasonable cost.

3) Third, any solution should be platform-neutral, allowing pay-TV operators to access the PC, the STB, and any other 'TV-capable' devices, regardless of their network infrastructure.

These considerations imply that making it possible for everyone to choose the algorithm they wanted would represent a backwards step: every box would be locked to a particular CA vendor, making the market less rather than more competitive, and all the other benefits we have described would be lost.

Conversely, we cannot envisage a mandated solution which requires everyone to use identical technology – this takes us back to the core problem with the CSA. CSA3, then, is – on its own – not fit for purpose.

Logically, rather than CSA3's component approach, we need a system approach which considers the DVB ecosystem as a single, holistic entity, with the home environment and consumer devices being part of it. Commercial and business considerations effectively demand that this new technology operate in software – since operators today want their content to be received on any device, including PCs, and mobile devices[8]. However, simply to replace a hardware-based common algorithm with a software-based one does not address the issues we have outlined in this White Paper.

[7] DVB press release issued 9 March 1995: http://www.dvb.org/documents/press-releases/pr008_Final%20Elements%20of%20Conditional%20Access%20Package%20Agreed.950307.pdf

[8] This is not a particularly original proposal: in the US, Simulcrypt-type approaches use AES or DES, which can both be implemented in software.

© Copyright Farncombe Consulting Group 2009

Farncombe accordingly proposes that the technology should be replaced by a CSA 'toolkit' incorporating the following ideas:

1) Instead of a single, immutable, algorithm, Farncombe proposes a 'toolkit' that should be standardised and present in all DVB-compliant devices, but where the system's configuration is under operator or CA-supplier control. This would mean, for instance, that two operators could choose to configure their systems in the same way, but still in a different way to the rest of the world.

2) In addition, we propose that any such configuration should be secured and kept secret, in the sense that it cannot be trivial to replicate that configuration.

3) To secure such a configuration, an optimal system would require that control-word emitting devices authenticate themselves to scrambling devices and vice versa – so that no legitimate DVB-compliant device would be able to accept control words from a pirate device and vice versa. This would, we believe, require national or international certificate management[9].

Some readers will argue that a hardware algorithm must be implemented to increase security. However, as we have argued above, given what is happening with control-word sharing today and the business needs of operators, it is not certain that any additional security would be delivered in practice: it takes time to implement a new hardware solution since it cannot be used until everyone has got it (one reason, indeed, why CSA3 is not in use today).

A DVB proprietary hardware-based approach is thus very difficult to change. If a software- or 'toolkit'-based approach had originally been approved by DVB, operators suffering piracy would now be able to implement modifications to their existing CA systems. Even if it proved impossible to prevent control-word leakage, they would at least be in a position to prevent control-word usage by every other set-top box.

Ironically, the DVB CM-IPTV Content Security Task Force is currently working on a toolkit approach to conditional access – but for the IPTV sector only – which could incorporate software-based algorithms. If implemented, this would further reinforce the competitive disadvantage being experienced by 'traditional' DVB players.

In any case, we believe that techniques such as white box cryptography[10] used in DRM solutions could provide a possible solution to security concerns. The white box approach (the term originates from the software testing community) assumes everything static is known about a software system and its implementation (decryption algorithms, compiled code) and a hacker can monitor execution of the code, but that the implementation complexity does not allow easy extraction of secret information.

The approach is to transform the algorithms which decrypt secret information, and those which use that information to 'unscramble' content, into an implementation which obfuscates the process. The

[9] Some vendors we have contacted have suggested that there is no need for such a certificate authority. We think this should be discussed in an appropriate forum.

[10] Please contact us if you want to know more about white box cryptography

© Copyright Farncombe Consulting Group 2009

number of internal states in a white box implementation is so large, and internal data distributed so widely across those states, that observation of any secrets in the clear is for all practical purposes unachievable (no control-word observation, no control-word sharing).

We also understand from some in the industry that it should be possible to create a secure link between the white box software descrambler and a smartcard independently of the rest of the set top box software. This is important; otherwise software release management would become very difficult.

This proposed toolbox approach would enable a 'Simulcrypt group specific' common scrambling algorithm, allowing two different CA vendors to supply two different implementations of the descrambler, which could then be downloaded into two different populations of STBs.

Moreover, with a software-configurable system, operators would be free to join or leave the Simulcrypt group.

If the software toolkit were based around a cipher like AES, one could not only change the implementation of the cipher but also the cipher itself. Indeed, it's possible that it could even be white-boxed and implemented in next-generation DVB chipsets shipping in the very near future (which could well be ahead of any CSA3 algorithm implementation). This is because a toolkit software-based approach is much quicker to implement than one based on DVB proprietary hardware.

The approach outlined above directly addresses the requirement for hybrid DVB-IP boxes, and the issue of a DVB home hub.

© Copyright Farncombe Consulting Group 2009

Conclusion

If the issues of illegal content distribution and piracy in the pay-TV sector are to be addressed, the DVB Common Scrambling Algorithm needs to be replaced.

In this White Paper, Farncombe suggests a 'toolkit' approach incorporating both hardware and software-based elements to provide maximum flexibility for operators.

The need for such a replacement is overdue. Operators currently thinking about replacing their set-top boxes – either because they are aware of the control-word sharing risk, or because they are poised to introduce new HD-capable receivers – risk wasting their investment: even where the best security techniques are used, it only takes one hacked receiver to allow control words to be fed over broadband to any legacy DVB STB and enable pay-TV content to be pirated.

In the worst-case scenario, operators could even end up not being able to access premium content any more, as their platforms begin to be perceived as a pirates' playground.

This would provide content providers with a good reason to transition towards an over-the-top distribution model, with potentially dramatic consequences for the pay-TV industry as a whole.

© Copyright Farncombe Consulting Group 2009

Annexe 1 – The genesis of the DVB CSA

The DVB Common Scrambling Algorithm (CSA) had its genesis in 1993, when a group calling itself the European Launching Group for Digital Video Broadcasting was seeking to define a new European digital TV system.

This body, which was later to spawn what we know today simply as 'DVB', had amongst its aims the establishment of common scrambling standards. The original idea was that this, together with the use of defined MPEG-2 compression and transmission profiles, and specified cable, satellite and terrestrial modulation schemes, would enable European digital TV decoders to be standardised in almost every respect – except for a module containing the pay-TV operator's proprietary conditional access system.

Despite opposition from some pay-TV operators, the notion proved to be a surprisingly resilient one, with the CSA emerging initially from within the DVB Consortium in early 1995 as the technology underpinning Simulcrypt. This was the system that allowed two different conditional access (CA) streams to be embedded in a single broadcast, allowing separate populations of decoders using different CA systems to decode it. The CSA provided the common element: indeed, it was necessary for every device to include the CSA even where it was not used for Simulcrypt.

As the DVB said at the time:

> *"Two routes to develop the market for digital television reception should be encouraged:*
> - *Receivers incorporating a single conditional access system (the Simulcrypt route), and Receivers with a common interface, allowing for the use of multiple conditional access systems (the Multicrypt route).*
> - *The definition of a Common Scrambling Algorithm and its inclusion, in Europe, in all receivers able to descramble digital signals. This enables the concept of the single receiver in the home of the consumer."* [11]

By implication, the CSA's implementation in hardware was designed to side-line the PC as a potentially insecure 'user-programmable' device. The CSA was subsequently enshrined in European Law, first within the EC's so-called 'Digital Directive'[12] in 1995, and later as Annex VI of the Universal Service Directive[13] in 2002 as part of a series of measures designed to maximise interoperability of digital TV equipment across the European Union. With respect to the CSA, the latter provides that:

> *"All consumer equipment intended for the reception of digital television signals, for sale or rent or otherwise made available in the Community, capable of descrambling digital television signals, is to possess the capability to […] allow the descrambling of such signals according to the common European scrambling algorithm as administered by a recognised European standards organisation, currently ETSI […]."*

[11] DVB press release issued 9 March 1995, *ibid.*

[12] See Article 4 of Directive 95/47/EC of the European Parliament and of the Council of 24 October 1995 on the use of standards for the transmission of television signals

[13] See article 23 of Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, which references Annex VI

© Copyright Farncombe Consulting Group 2009

Today, the CSA is present in every DVB-standard digital receiver, and can be found as the default scrambling system embedded in most MPEG-2 and MPEG 4 chipsets. For the technically-minded, it may be viewed as a cascade of block and stream ciphers, using the same 8-byte common key.

© Copyright Farncombe Consulting Group 2009

Annexe 2 – About Farncombe Consulting Group

www.farncombe.eu

The Farncombe Consulting Group is a specialised professional services firm operating in the broad digital video technology, telecoms and digital media sectors. Initially focused on pay-TV and digital TV technology through founder company Farncombe Technology, it has since grown into a globally-recognized television consultancy, servicing a large international client roster that includes broadcasters, operators, telcos, hardware and software suppliers and a variety of government, regulatory bodies and private equity companies.

High-profile engagements that can currently be disclosed include helping green support services company eaga to deliver the UK's £500m Digital Switchover Help Scheme (DSHS) on behalf of the BBC, and supporting public service broadcaster SABC's DTT transition in South Africa.

The Farncombe Consulting Group's current focus is on the increased opportunities made available by a converging market which extends from cable, satellite and terrestrial delivery to telco-managed IPTV, video-over-Internet and mobile TV offerings.

The Group comprises a number of separate practices covering a wide range of core competencies. These include:

- Strategy
- Technology Consulting
- Programme Management
- Content Security
- System Integration
- Engineering Services
- Test & Certification
- Design Practice

We apply these competencies to the planning, management, transport and secure delivery of video and other new content services.

For more details, visit www.farncombe.eu; or ring Mrs Georgina Saunders on +44 1256 844161 or email at: Georgina.Saunders@ftl.co.uk.

Basingstoke Office	London Office	Paris Office	Düsseldorf Office
Belvedere	Liberty House	17 rue de l'Echiquier	Grafenberger Allee 363
Basing View	222 Regent Street	75010 Paris	40235 Düsseldorf
Basingstoke	London	France	Germany
RG21 4HG	W1B 5TR		
United Kingdom	United Kingdom		
T: +44 1256 844161	T: +44 20 7297 2367	T: +33 1 71 18 29 86	T: +49 211 1655118
farncombe@ftl.co.uk	farncombe@farncombestrategy.com	farncombe@farncombe.eu	farncombe@farncombe.de

© Copyright Farncombe Consulting Group 2009

About Farncombe's content security practice

Farncombe Consulting Group's founder company, Farncombe Technology, launched in 1991 on the basis of its expertise in pay-TV technology, and since then our content security practice has built up an impressive track-record in this field. Our accumulated know-how can be applied to any broadcast network, including satellite, cable, terrestrial, mobile, and IP-based or on-demand networks.

Farncombe's thought-leadership in this area is demonstrated by the fact that our staff have provided representation on various cross-industry working groups including:

- Chairing the DVB Simulcrypt Technical Group that developed DVB Simulcrypt interface standards that are now in widespread use.
- Representing the ITV companies on the Conditional Access Specialists Group in the European Digital Video Broadcasting (DVB) project

Latterly, our Content Security Practice has also been responsible for publishing a well-received industry White Paper on Conditional Access in Two-Way environments.

Accordingly, our content security practice is frequently approached to carry out security audits of conditional access and DRM systems. These audits have typically been commissioned by broadcasters who wish to have an independent view as to the likely risks to their revenue streams posed by the choice of a particular CA system. Indeed, one pan-European pay-TV content-owner routinely refers operators seeking to distribute its material to us so that we can ensure its premium programming is appropriately protected.

Our core content security competencies include:

- Security Audit
- RFP and Contract Negotiation Support For Security Systems
- Fraud Management
- Secure System Design
- Conditional Access System Evaluation
- Card Swap and Conditional Access Swap Programmes
- Simulcrypt Design and Operations
- Training Services and Thematic Workshops

For further details please contact Andrew Glasspool at our Basingstoke office on Andrew.Glasspool@ftl.co.uk or Jean-Marc Racine in our Paris office on jmracine@farncombe.eu

© Copyright Farncombe Consulting Group 2009