◆ Network Assisted Content Protection Architectures for a Connected World

Álvaro Villegas, Pablo Pérez, José María Cubero, Enrique Estalayo, and Narciso García

Content protection is a key component for the success of a multimedia services platform, as proven by the plethora of solutions currently on the market. In this paper we analyze a new network scenario where permanent bidirectional connectivity and video-aware encryption technologies allow a trustful operation of ubiquitous end devices. We propose new scalable models for a content protection architecture that may achieve dramatic improvement in robustness, reliability, and scalability. Selective ciphering and countermeasures are included in those models, together with several examples of their application. © 2012 Alcatel-Lucent.

Introduction

Protecting audio/video content to restrict access to it from unauthorized hands is a key principle for monetizing multimedia delivery services over any kind of platform. From the early days of analog television this protection has been based mostly on cryptography, leading to a continuing struggle between piracy attacks and recovery from compromised platforms through the renewal of technology. For almost two decades the scenario has been quite stable, based on unidirectional broadcast networks which pushed virtually all the responsibility for content protection to the client device. Thus there was a tradeoff between the strength of the secure client device (hardware or software based) and its associated cost: platforms delivering high quality content are attractive targets for attack and therefore require stronger and more expensive protection solutions [7].

The scenario in the last few years, however, has changed drastically with the growing availability of bidirectional networks that enable the permanent connection of end devices to the network, and eventually to operator information services [3]. In some cases this connection is the primary vehicle for the delivery of the content itself (e.g., Internet Protocol television (IPTV) platforms [4] or up-and-coming over-the-top (OTT) service providers), while in other cases a hybrid network is deployed, with a bidirectional network complementing the existing broadcast platform. This paper will demonstrate how the availability of this connection, which has already enabled a number of new architectures, has the potential to be of great benefit for improving the efficiency of content protection technologies, introducing new models which maintain or increase the level of security at a much lower cost.

In order to demonstrate how the new connected paradigm can help with content security, we will start by summarizing the existing content protection solutions, from the pure broadcast environments to the first architectures which already leverage a permanent

Bell Labs Technical Journal 16(4), 85–96 (2012) © 2012 Alcatel-Lucent. Published by Wiley Periodicals, Inc.
Published online in Wiley Online Library (wileyonlinelibrary.com) • DOI: 10.1002/bltj.20535

Panel 1. Abbreviations, Acronyms, and Terms

AES—Advanced Encryption Standard
CABAC—Context-adaptive binary arithmetic coding
CAS—Conditional access system
CPE—Customer premises equipment
DTH—Direct to home
ECM—Entitlement control message
EMM—Entitlement management message
HDTV—High-definition television
ID—Identifier
IPTV—Internet Protocol television
IPPV—Impulse pay per view
MPEG—Moving Picture Experts Group
MVC—Multiview video coding
NAL—Network abstraction layer
NALU—Network abstraction layer unit
OTT—Over-the-top
PCMCIA—Personal Computer Memory Card International Association
PVR—Personal video recorder
RDO—Rate-distortion optimization
RTP—Real Time Transport Protocol
SDTV—Standard-definition television
TV—Television
VCL—Video coding layer

connection to the servers. Our first proposal will then be an innovative leak mitigation algorithm which offers a highly efficient and cost-effective means to react to piracy from a new perspective. Next, we will introduce a completely new approach to content protection based on implementing in the network the logic that drives the current smartcard-based solutions. We will then propose a very efficient algorithm for content scrambling that leverages the deep analysis of the content that can be done by specialized servers in the network, leading to very secure results which require a very low computational cost in end devices, which are usually quite resource limited.

Classic Conditional Access Architectures

Conditional access systems (CAS) enable pay television (TV) platforms to deliver content through a shared media which is accessible by more users than the ones paying for it. Satellite direct to home (DTH) is the most evident case, but terrestrial distribution and even more controlled environments such as cable or IPTV platforms make extensive use of CAS technologies [2]. The principle behind CAS operation is cryptography: content is encrypted ("scrambled") before being distributed, and the resources for decrypting it (the "licenses" with the keys, in most cases) are delivered only to authorized client devices, those in which a "secure client" is capable of extracting the key from the data delivered by the CAS and, based on internal rules, deciding if it should be applied to the local descrambler to enable access to the content. The architecture of a conditional access system is depicted in **Figure 1.**

The presence of a secure client with decision capability is a fundamental principle of the traditional CAS architecture: it provides a high degree of flexibility but it also opens a gap for vulnerability in the content protection architecture. If a hacker manages to manipulate this client, keys from devices entitled to access the content may be faked or exposed and then transferred to non-authorized devices which would then enable free access to all content (the well-known "control word sharing" technique is a good example [1, 6]). For this reason, the design and implementation of the secure client is key for the robustness of the solution: pure software implementations on generic hardware are cheap and easy to renew, but are also quite weak, while implementations on specialized hardware (e.g., a smartcard or a PCMCIA card) are stronger but more expensive [15].

An alternative conditional access architecture exists, which is based on a permanent connection between the client devices and the operator servers. We refer to this architecture as "network-based CAS."

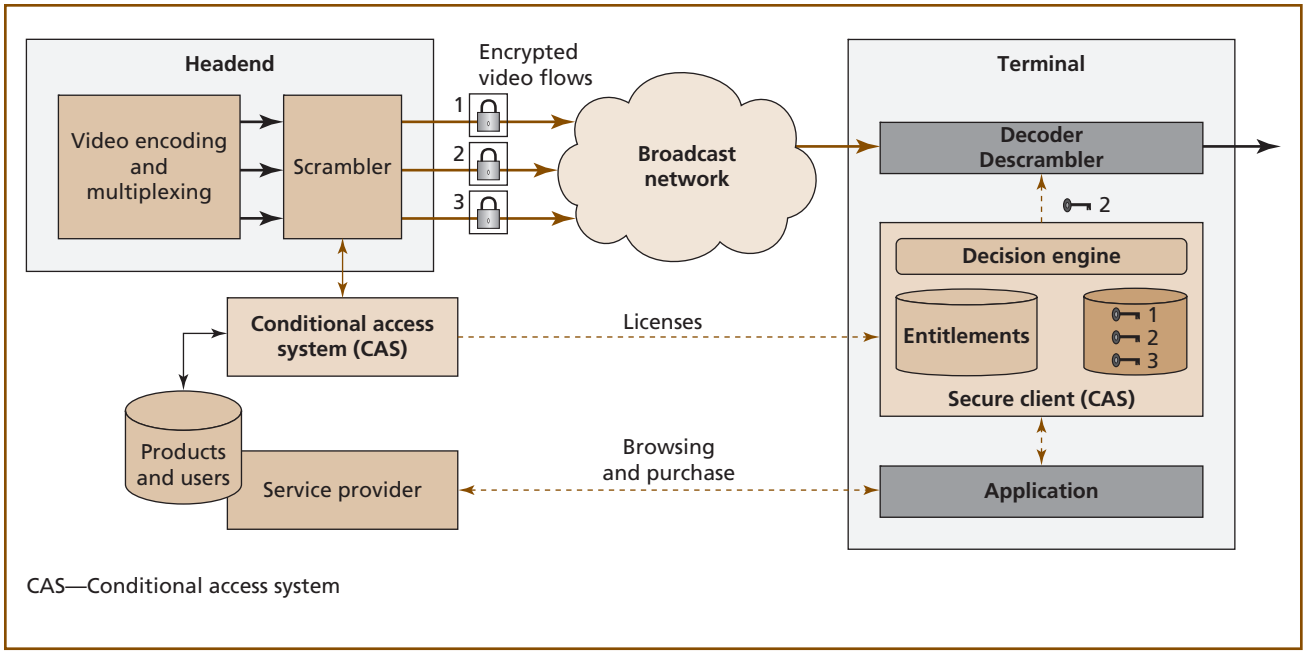

Figure 1.
Architecture of conditional access.

The main concept behind this approach is to shift the intelligence and decision capability from the client device to the network: decryption keys are sent only to client devices which are entitled to receive them, so even if a local application in those devices is hacked, they will not be able to access unauthorized channels, simply because they will not have the keys for decrypting them, as illustrated in **Figure 2**. There is still the risk, however, that the keys sent to a legal device may be extracted and published or transferred to illegal devices. To mitigate this risk, the network-based solution relies on the cryptographic capabilities offered by the latest generation of video chipsets, which include a key decryption hierarchy (the so called "key ladder") within the chipset itself, based on a core unique key stored in each chip, which only the operator or the CAS provider knows. In this way, the decryption keys are already encrypted with the unique secret key of their chipset when they are sent to customers, so when the content is accessed the product decryption key is not exposed in the clear apart from the chipset and therefore cannot be published or communicated to other devices, as illustrated in **Figure 3**. A consequence of this scheme is that a large number of encrypted keys must be sent on a periodic basis, because each key needs to be encrypted and sent as many times as needed. Therefore, this approach is not appropriate for pure broadcast platforms, through it is applicable for connected environments where the client devices can retrieve the keys from specialized servers using unicast connections.

Leak Mitigation Algorithm for Network-Based CAS

We now propose an algorithm to manage the risk of client device manipulation that was previously identified in network-based CAS.

Problem Statement

We described above how network-based CAS avoids the risk that a legal client device may be manipulated to extend its entitlements. We also noted that this model still presents some risk that the keys that are legally sent to the client device may be leaked [2].

The innovative approach that we propose here is a forensic mechanism capable of detecting the source

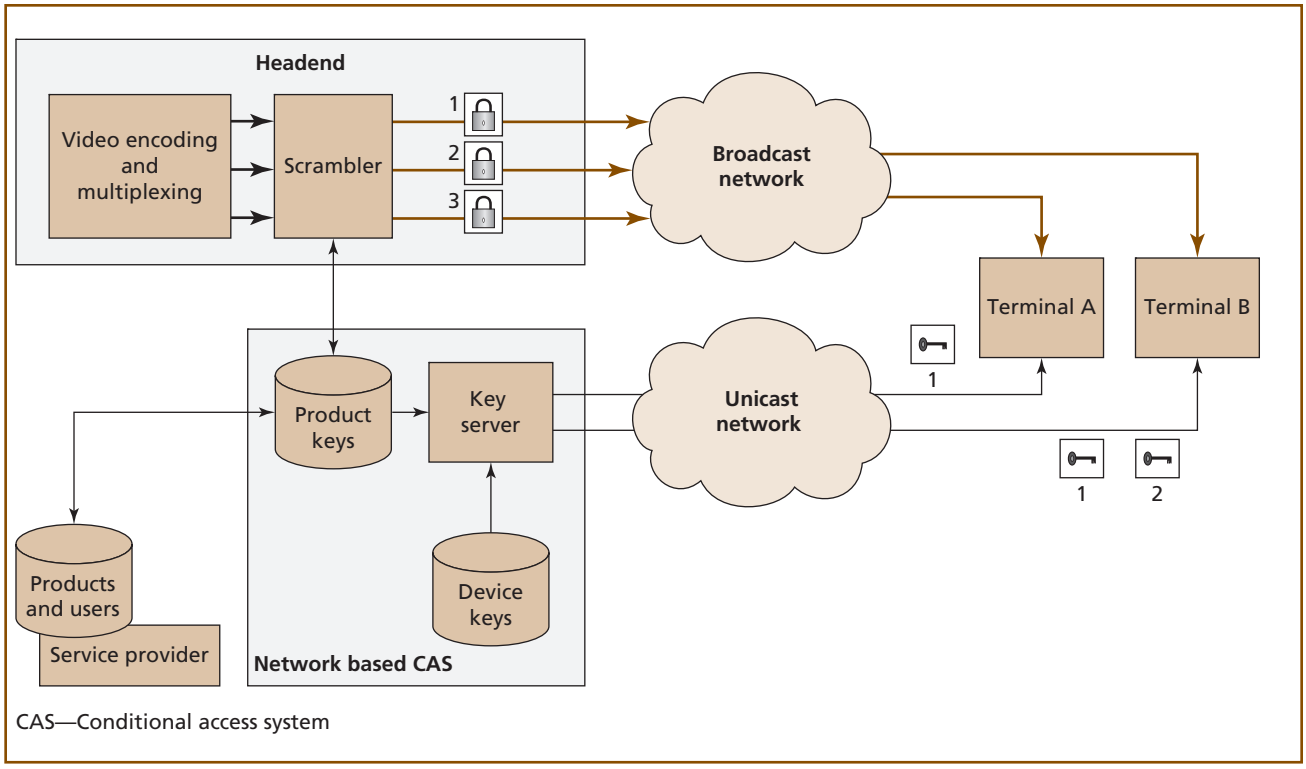

Figure 2.
End to end architecture of network based CAS.

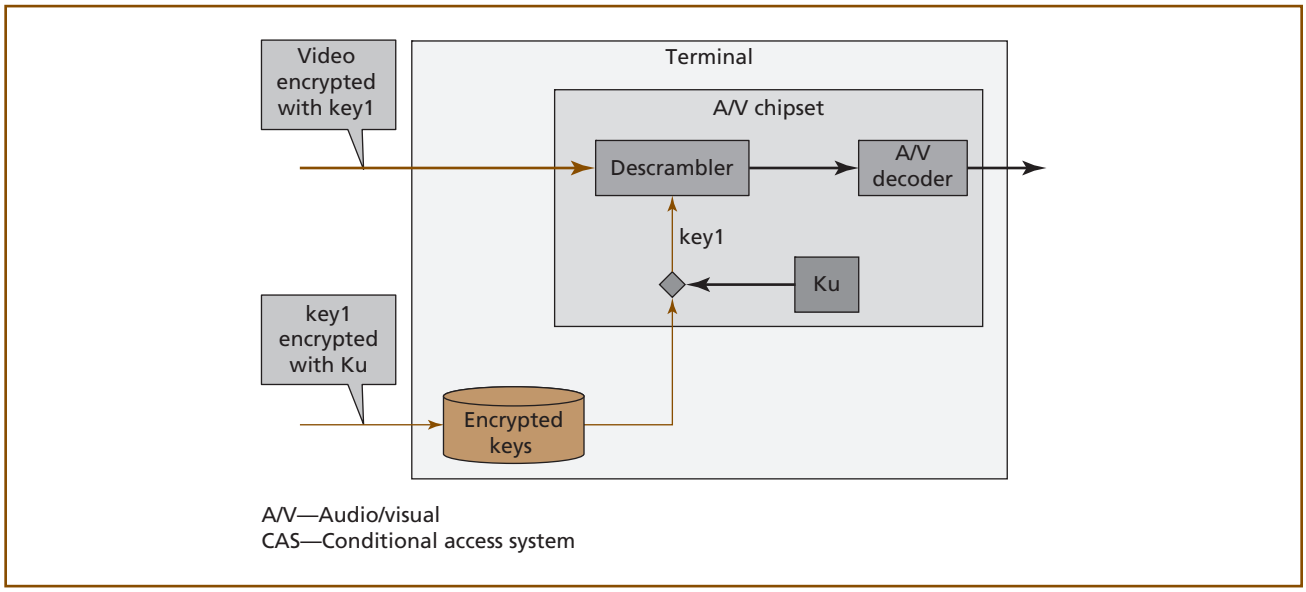

Figure 3.
Key ladder in a network based CAS client.

of the leak when it occurs (i.e., when the key has already been published or transmitted). The algorithm is based on the fact that the source of the leak is always a legal device. With a network-based CAS architecture, a non-legal device would not receive keys, so it cannot leak anything. If a legal device which has been propagating leaks can be identified, it can be banned, thus fixing the security breach.

Proposed Solution

The core idea of the proposed key mitigation algorithm is summarized as follows:

- The content (the audio/video stream) is over-encrypted using two or more different keys, in a way that any of those keys alone is enough for decrypting the content. This scheme can be achieved in different ways: simulcasting small pieces of the content encrypted with different keys, or using a layered key scheme (such as the Moving Picture Experts Group (MPEG) entitlement control message (ECM) mechanism) and sending the low-level key encrypted with several higher-level keys.
- The population of legal terminals is logically divided into as many groups as different keys have been defined in the over-encryption. Each group will receive only one key through the unicast connection.
- If a key leak is detected, the source of the leak (a specific legal device or devices) may be determined by isolating the exact key that has been published or distributed to pirate devices, and it is then assigned to a sub-group.
- The process is iterated with a different distribution of the groups, and the detection is repeated.
- Nevertheless, the algorithm can be challenged by pirates using several hacked devices simultaneously to extract the keys. If several keys are published, it will not be possible to identify the group in that iteration. However, an attempt to defeat the leak mitigation algorithm in this way will only increase the number of iterations required to perform the isolation: the mechanism will eventually work as planned, and all pirate devices will be detected and banned.

Through careful selection of the group distribution algorithm, the isolation of the exact device (or devices) producing the leak can be done in just a few iterations. A basic example: using just two keys per iteration, groups can be defined according to bit N of their device identifier (ID), with N being incremented in each iteration; if there is a device id space of B bits, with just B iterations the source of the leak will be identified.

The architecture of the network-based CAS, which is based on a high key rotation and a massive unicast delivery of keys, is very appropriate for this algorithm.

Smartcard in the Network

In this section, we propose an architecture that will mitigate the weaknesses of network-based CAS without requiring expensive hardware in the client device, as already identified in previous sections.

Problem Statement

We demonstrated previously that content protection solutions which rely on a secure client are highly flexible as a result of the local decision capability, however, they also present a weakness from the security point of view unless expensive hardware such a smartcard is used. On the other hand, network-based CAS provides robust security without a need for expensive hardware in the client device, but does so at the cost of lower flexibility. Commercial models, which require massive simultaneous decision capability at the client side, would not be possible with pure network-based CAS. Examples of such commercial models include:

- *Pay-per-time.* The end user pays for a specific amount of time which can be consumed at intervals of arbitrary length ("slots") on any channel or subset of channels. The slots consumed by each customer are typically controlled locally by the secure client. The secure client tracks usage and stops granting access to the content when the time credit has expired. It is not possible to do the same from a centralized server because it would require permanent bidirectional communication with each client device. On the other hand, it's not possible to use the key delivery mechanism

used in network-based CAS either, because keys would need to be provisioned in advance and there would not be a reliable mechanism to check if they have been used by the client or not. Moreover, the number of keys in such a scenario would be extremely high (one per slot).

- *Impulse pay-per-view (IPPV).* When access to a highly promoted live event can be purchased on a pay-per-view basis, it is quite common to see thousands or even millions of purchase attempts in a very short period of time just before the event starts. (A good example is a soccer match). The most scalable implementation for this scenario is a complete "local" purchase in the secure client which is later logged securely on the service provider backend.

Proposed Solution

To keep the high flexibility from client-side decision power while still leveraging the security and cost savings of the connected scenario, we present new concept: the network smartcard [14]. A server in the cloud, located close to the end device, implements the same functionality as a traditional smartcard: it stores all cryptographic information required to access any content provided by the operator, but it will provide the corresponding keys to the client device only if the user is entitled to receive it.

The key design principle for this solution is the distributed nature of the network smartcard servers which, like physical smartcards, do not require a permanent connection to the operator's core servers to execute their daily work: delivering keys to the descrambler hardware. This also enables a business model which does not require a connection to the core server at peak times of usage.

Of course, once the network smartcard decides to grant access to an asset, the key must be delivered securely. The most appropriate mechanism for this is by leveraging the same key ladder described for the network CAS: the key is encrypted with the chipset's unique key and then delivered via a regular channel (not necessarily secure) to the end device. Data distributed in this way cannot be used by a different device, and the key itself is not exposed in the clear anywhere in the authorized device. Moreover, the volatile nature of distributing the key in this way is also a plus for security: once used, the key (in memory) is not stored in the device.

Figure 4 shows the end-to-end architecture of the network smartcard solution: the critical link is now the connection between the network smartcard server and the end device. The connection between the core servers and the network smartcard servers is only used sporadically: to download new entitlements (as entitlement management messages (EMMs) in the classic CAS environment) when users purchase new products, and to download cryptographic information (which can now be done on a very infrequent basis).

This solution is extremely secure, even more secure than a smartcard-based scheme, because the servers where all the critical information is stored are not physically accessible to hackers. Communication of the key to the chipset is as secure as when using a smartcard (which usually also implement a secure channel based on embedded chipset security).

In terms of scalability, the number of network smartcard servers grows linearly with the number of connected end devices. The cost per user, however, is estimated to be an order of magnitude lower than a smartcard due to economies of scale:

- The traffic from the smartcard servers to the end devices will be unicast, as in the network CAS architecture. The volume of data required will now be higher, because the granularity of the access control will in most cases be finer: for instance, the usual practice of changing the encryption key at regular intervals during the transmission of linear channels (cryptoperiod) will require the communication of such key every time it is changed. In addition, even with cryptoperiods on the order of tens of seconds, this leads to negligible bandwidth. For example, transmitting 1024 bits (enough room for a 128 bit key, metadata and transmission overhead) in a cryptoperiod of 10 seconds (an extreme case) results in 0.1 kb/s. From the server perspective, if a single server is connected to, e.g., 50,000 users, the aggregated bandwidth used to communicate the keys would be just 5 Mb/s.
- The computing power required at the smartcard server is mainly driven by the encryption that has

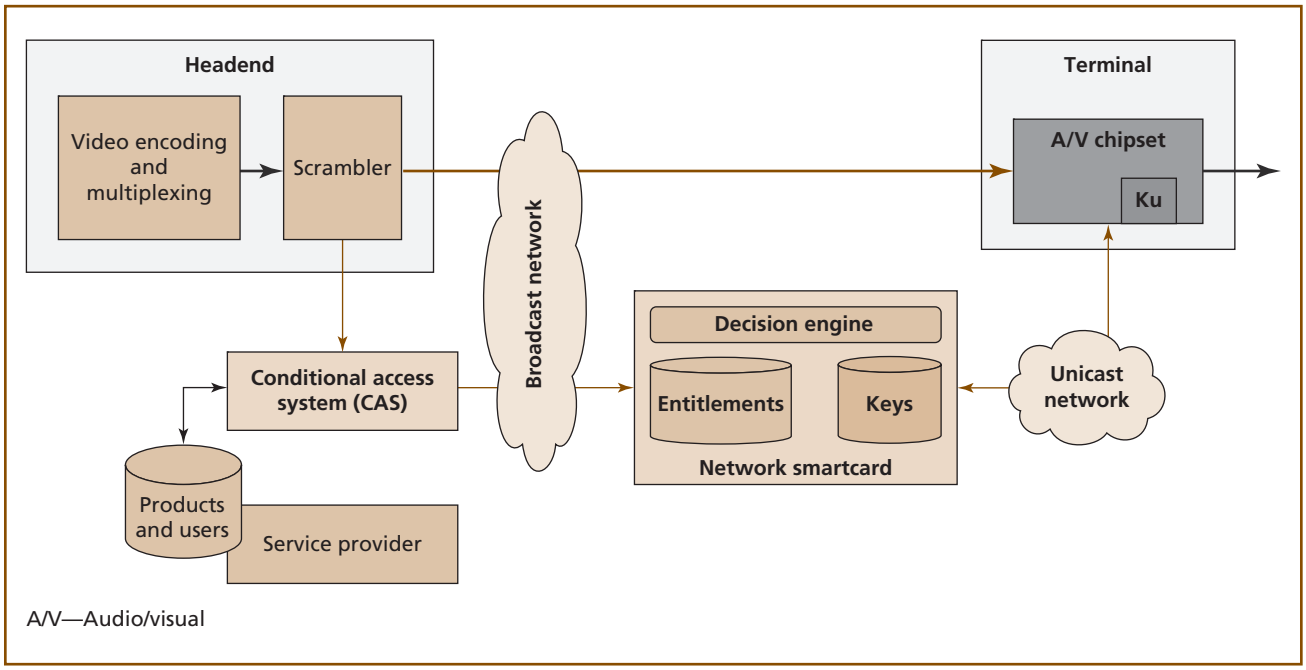

Figure 4.
Network smartcard architecture.

to be done for every product or cryptoperiod for every user when the global encryption key is encrypted with the chipset's unique key. Using the example described above, in the worst-case scenario, 50,000 users would require 5,000 symmetric encryptions (Advanced Encryption Standard 128 (AES 128)), per second, or a peak encryption performance of 640 kb/s, something easily achievable with off-the-shelf available hardware (or even software).

- Latency is in this case an important factor, especially when decrypting linear channels during the cryptoperiod, since the key for the new period should be ready in the chipset on time. However, with cryptoperiods on the order of tens of seconds this is not expected to be a problem.

Content-Aware Content Protection

The traditional approach to CAS systems assumes that from a cryptographic point of view, the whole media stream being processed can be considered as a homogeneous set of data. However, prior knowledge about the media data structure allows enhancing the functionality of a content protection system, adding features such as partial decoding of the video stream (required for network processing systems, like a network-based personal video recorder (PVR)), more efficient scrambling schemes, or free preview of parts of the content.

Selective Scrambling

The concept of selective scrambling means that, when cryptographically protecting a multimedia asset or stream, only a (typically reduced) fraction of the data is scrambled, while the remainder is distributed in the clear. There are two main reasons for this approach: on one hand, by leaving some specific information unscrambled, intermediate video-processing systems can access the part of the data which is required for them to work correctly; on the other, keeping a reduced bit rate of scrambled packets can be the only possible solution for decoding devices with limited computing power, such as customer premises equipment (CPE). The former problem is relatively simple, as the specific data headers required by the network processors are typically known. The latter

is more interesting, as it is necessary to find a good balance point between the scrambling rate and protection effectiveness.

Problem statement. Let us consider a client that is not entitled to receive an asset and which therefore lacks the appropriate keys to descramble it. Any user watching this asset will experience the same effect as a user that loses exactly the same packets that are scrambled in the stream. From this point of view, selective scrambling can be seen as a reverse rate-distortion optimization (RDO) problem. Unlike the typical RDO problem, however, the aim here is *maximizing* the final distortion for a specific rate of scrambled packets [10]. In an ideal case, the resulting distortion should be high enough that no useful data can be extracted from the content. However, for many practical applications, a suitable solution could involve producing video with a quality bad enough to discourage any potential user from watching it. Therefore, in order to find a good selective scrambling algorithm, we use techniques for quality of experience analysis.

Notwithstanding, in designing a selective scrambling scheme, one must remember why the algorithm is required: the scrambled video is processed in the network and the descrambler has limited computing power. In addition, using a lightweight scheme in the scrambler as well as the descrambler would broaden the applicability of the scheme. Thus the requirements for the selective scrambling algorithm include:

1. To be transparent to video servers,
2. To scramble only a (low) percentage of the video packets,
3. To be implementable with low computational cost, and
4. To maximize the distortion introduced by the encrypted packets (i.e., do not allow the video sequence to be recovered from the unscrambled packets without heavy impairment).

Proposed solution. Most existing commercial CAS solutions support fulfilling requirement 1. However, they typically rely on full-stream encryption. There are several solutions in the literature that address the partial encryption of the video stream. A state-of-the-art can be found in [8], which describes a set of encryption techniques that allow good visual degradation of encrypted video while scrambling only a portion of the packets. However, all of them either require deep analysis of the video stream (thus not satisfying requirement 3) or scrambling the video headers to make video undecodable (not meeting condition 1).

In [5], the authors propose encoding the most important data at a higher level of security than the less important data, which also reduces complexity. In [13], H.264 video elements are divided into different classes, which are provided with different protection. In [16] different encryption levels can be reached by analyzing the entropy coding of the H.264 stream. These methods satisfy condition 2, but require analyzing H.264 up to at least macroblock level, which might be computationally expensive, especially when context-adaptive binary arithmetic coding (CABAC) entropy coding is used, as in most IPTV streams.

The approach we propose is exploiting the error resilience characteristics of video coding standards such as, but not limited to, H.264, where video frames are divided into *slices*. It has been shown that when a fragment of the video slice is lost, the rest of the slice becomes almost undecodable [10]. Therefore video can be degraded to an acceptable level for safe transmission by scrambling only a small set of data in each slice.

This solution is especially suitable for multimedia deployments because:

- Commercial encoders use a low number of slices per frame (typically 1 in standard-definition television (SDTV), and 4 to 8 in high-definition television (HDTV). Thus the fraction of video packets to encrypt (scrambling rate) is kept low.
- The information required to process video in a video server (i.e., stream and picture-level information) is contained in other H.264 syntax elements called network abstraction layer units (NALUs). NALUs are not slices, but reside in the slice header.
- The only video stream analysis required for this solution is detecting the type of NAL units, detecting slices and slice headers, and reading the coding type of each frame. This can be performed in the H.264 network abstraction layer, and thus does not require analyzing anything beyond the

Table I. Minimum scrambling rate required to completely loss the video signal, as subjectively assessed by expert viewers in laboratory, for several content assets. Selective scrambling algorithm is compared with random packet scrambling.

Content	Resolution	Bit rate	Scrambling rate (selective)	Scrambling rate (uniform)
Advertising	676i	2.7 Mb/s	1%	15%
News	576i	2.7 Mb/s	1.5%	15%
Movie	1080i	8.5 Mb/s	0.8%	10%
Movie	1080i	15.0 Mb/s	0.3%	5%

slice header level. Therefore, the processing required is much simpler than any other selective scrambling algorithm.

With these premises, we propose a scrambling scheme based on two layers [11] working within each slice of the encoded stream:

1. The first layer would scramble a small set of data just after each slice header. This protects the video from real-time decoding with a very low scrambling rate.
2. The second layer would randomly scramble some sets of data in the rest of the video coding layer (VCL) units, as well as other streams (e.g., audio) following a simple to implement rate-distortion model. With this second layer, two aims are met: first of all, audio streams are also scrambled so that they are heavily impaired to non-descrambling receivers; second, destroying the structure of the video stream makes it impossible to decode even using sophisticated offline error concealment methods.

Results. We tested the algorithm with different scrambling rates and several types of content encoded in H.264. The processed video then was played without correctly descrambling the packets, which results in packet loss. In the laboratory, expert viewers watched the video in order to assess the minimum scrambling rate at which it is impossible to extract any information from it (i.e., the point at which the image was completely impaired). This value was compared with the minimum scrambling rate required to obtain an equivalent result by randomly encrypting video packets. **Table I** presents the results of the tests, and even with the limitations of the experiment it can be shown that by encrypting only up to two percent of the transport packets, it is possible to impair video quality to the point that the resulting video is useless.

All the video samples under study used only one slice per frame. For video sequences with N slices per frame, these values would have to be multiplied by a factor $K \leq N$. Even in that case, for most typical scenarios, the required scrambling rate would be relatively low.

Scalable Scrambling

Scalable scrambling offers another possibility for selectively encrypting part of the multimedia stream. The approach here is scrambling part of the stream in such a way that the part that has been left in clear is a correctly decodable stream, but with lower quality than the original one. The underlying idea is that the user is provided with the same video stream at two levels of quality, the lower in the clear and the higher encrypted. In this way, users can have a free preview of the desired content, but they only can watch the higher-quality version if they have obtained the rights. This idea can be generalized by dividing the stream into a number of layers of differing quality, and encrypting each of them with a different control word (or leaving them in the clear).

The only limitation is the ability to divide the coded stream into two or more different layers. In most coding standards it is possible in one way or another. For example, in MPEG-2 or H.264, this can be achieved by scrambling part of the frames (typically,

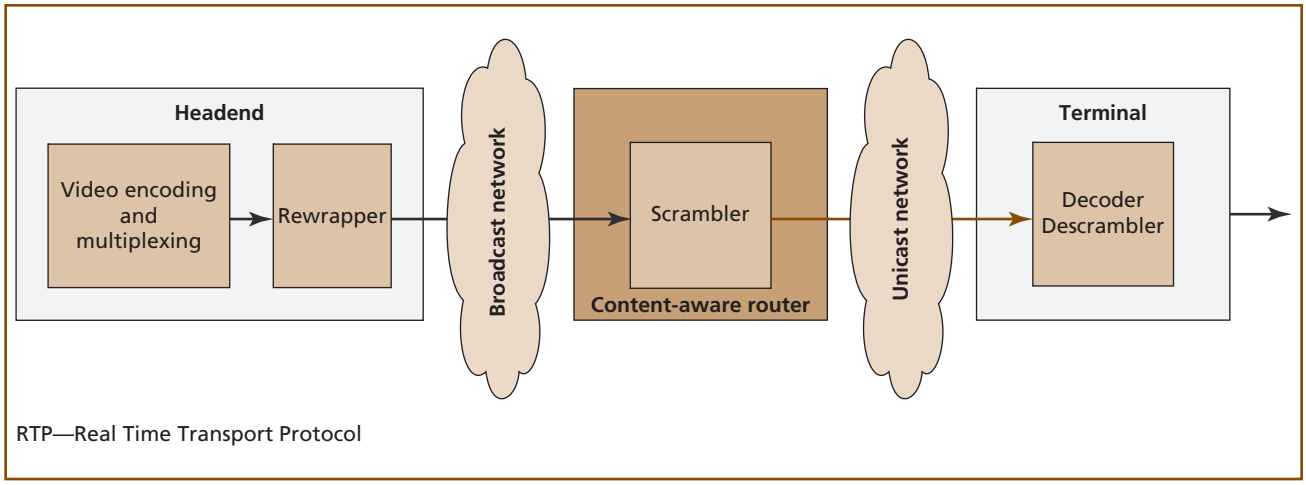

Figure 5.
Efficient RTP scrambling architecture.

the no-reference ones): the base layer (in the clear) would be a version of the original stream, but with a lower frame rate. With more complex coding standards, such as scalable video coding, quality layers are already provided, so scalable scrambling is straightforward. Depending on the coding scheme, other options are possible, such as scrambling different views in multiview video coding (MVC) or different audio components in multi-channel audio.

The ideas mentioned in the section on selective scrambling are also applicable here, in two different ways. First, the scrambling of the desired frames can also be done selectively (i.e., by only ciphering part of the slices, not the whole frames). Second, because the problem of scalable scrambling is again similar to an RDO, the effect of each scrambling strategy can be evaluated by using prediction techniques for packet loss effects. In this way, it is possible to adapt the target quality of each layer with a finer granularity, provided by the packet loss effect estimation algorithm.

Efficient Real Time Architectures

The use of selective scrambling can help to improve not only the performance of lightweight client devices, but also the scalability of encrypting elements in the network. An architecture showing this scalability is depicted in **Figure 5**, tailored for an environment of multicast Real Time Transport Protocol (RTP) distribution. The element in the video headend does not perform the encryption itself, but simply separates video from audio, and labels video frame boundaries appropriately [12]. This network element is called a *rewrapper* and is already deployed in commercial services. With the information provided by the rewrapper, it is possible to predict the main properties of the stream structure, and roughly predict the effect of the loss of an RTP packet [9].

With this data, a content-aware smart router, acting as the media delivery node to the end user, scrambles only the packets required to reach the desired impact in perceived quality. In this case, the encryption occurs at the RTP level, and in this way, the content-aware router only needs to process a few RTP packets in each stream, without the need for deep packet inspection. The required processing power is relatively small, and it is also possible to personalize scrambling per user or per session, hence making the system more robust against piracy.

Conclusions

We have analyzed a set of new approaches for content protection in a connected scenario, where there is a permanent link between the client devices

and the servers in the network. This permanent connectivity opens new and interesting opportunities for improving the security, reliability, and scalability of the solutions.

We first analyzed the existing architectures and the inherent limitations of the currently established CAS technologies. Then we demonstrated how a network-based CAS can be enhanced with a leak mitigation algorithm capable of detecting and fixing important security breaches. We proposed a completely new CAS model based on a smartcard-like server close to the end device (network smartcard) able to achieve dramatic improvement in security and a significant reduction in the cost of the solution. Next, we also introduced a content-aware encryption scheme which again leverages the capabilities of the servers in the network to provide a protection architecture. It achieves the same level of resistance to brute force attacks as a full encryption solution, but requires dramatically less resources at the client side, and hence enables the use of low cost devices while maintaining the same level of security. Finally, we included examples of the application of the proposed schemes allowing improvements in robustness, reliability, and scalability.

References

[1] ABA DSS, "What Is Card Sharing," <http://www.abadss.com/forum/102-faq-how/89484-what-card-sharing-explained.html>.

[2] B. L. Candelore, L. M. Pedlow, S. Richman, and F. J. Zustak, "Antipiracy Key Segmentation for HFC Multicast Distribution from Master Headend to Cable Hubs," U.S. Patent Application 20110096924 (2011).

[3] P. E. Chaudhry, S. S. Chaudhry, S. A. Stumpf, and H. Sudler, "Piracy in Cyber Space: Consumer Complicity, Pirates and Enterprise Enforcement," Enterprise Inform. Syst., 5:2 (2011), 255–271.

[4] European Telecommunications Standards Institute, "Digital Video Broadcasting (DVB), Transport of MPEG-2 TS Based DVB Services over IP Based Networks," ETSI TS 102 034, v1.4.1, Aug. 2009.

[5] Y. Fan, J. Wang, T. Ikenaga, Y. Tsunoo, and S. Goto, "An Unequal Secure Encryption Scheme for H.264/AVC Video Compression Standard," IEICE Trans. Fundamentals Electron., Commun., Comput. Sci., E91-A:1 (2008), 12–21.

[6] Farncombe Consulting Group, "Towards a Replacement for the DVB Common Scrambling Algorithm," White Paper, Oct. 2009.

[7] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in Digital Video Content Protection," Proc. IEEE, 93:1 (2005), 171–183.

[8] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives," EURASIP J. Inform. Security, 2008 (2008), Article ID 179290.

[9] P. Pérez and N. García, "Lightweight Multimedia Packet Prioritization Model for Unequal Error Protection," IEEE Trans. Consumer Electron., 57:1 (2011), 132–138.

[10] P. Pérez, J. Macías, J. J. Ruiz, and N. García, "Effect of Packet Loss in Video Quality of Experience," Bell Labs Tech. J., 16:1 (2011), 91–104.

[11] P. Pérez and J. J. Ruiz, "Encryption Procedure and Device for an Audiovisual Data Stream," European Patent Application 09169825.8 (2009).

[12] D. C. Robinson and A. Villegas, "Intelligent Wrapping of Video Content to Lighten Downstream Processing of Video Streams," European Patent EP 2071850 (2009).

[13] T. Shi, B. King, and P. Salama, "Selective Encryption for H.264/AVC Video Coding," Proc. IS&T/SPIE 18th Annual Symp. on Electron. Imaging: Sci. and Technol. (IE '06) (San Jose, CA, 2006), Program on Multimedia Processing and Applications, Conf. on Security, Steganography, and Watermarking of Multimedia Contents VIII, SPIE vol. 6072, pp. 461–469.

[14] A. Villegas and D.C. Robinson, "Method and Device for Authorising Access to Data," European Patent Application 08305647.3 (2008).

[15] X. Yu and B. L. Candelore, "IP TV with DRM," U.S. Patent Application 20110113443 (2011).

[16] Y. Zou, T. Huang, W. Gao, and L. Huo, "H.264 Video Encryption Scheme Adaptive to DRM," IEEE Trans. Consumer Electron., 52:4 (2006), 1289–1297.

(Manuscript approved October 2011)

ÁLVARO VILLEGAS is a distinguished member of technical staff at Alcatel-Lucent in Madrid, Spain. He received a six-year telecommunications engineering degree at Universidad Politécnica de Madrid, Spain. For the last five years, he has worked as an innovation architect for Alcatel-Lucent. He is also a member of the Alcatel-Lucent Technical Academy. His work focuses on innovative solutions and technologies for the provision of multimedia services on Internet Protocol (IP) and hybrid networks. His prior professional experience, always in the digital video field, was developed in Telefónica Research & Development (R&D); Auna, a digital cable operator; Motorola; and Nagravision.

PABLO PÉREZ is an IPTV solutions system architect in the Multimedia Integration Practice at Alcatel-Lucent's Network and Systems Integration division in Madrid, Spain. He received the ingeniero de telecomunicación degree, a five-year telecommunications engineering program from the Universidad Politécnica de Madrid (UPM), Madrid, Spain and was first in his year. He currently leads the technical design for the Alcatel-Lucent 5910 Video Services Appliance (VSA) product and has a key role in several public co-funded research and development (R&D) projects. His professional and research interests are in the area of multimedia quality of experience modeling and management, as well as video services enablement.

JOSÉ MARÍA CUBERO is an IPTV and multimedia engineer in the Multimedia Integration Practice at Alcatel-Lucent's Video & Networking Competence Center in Madrid, Spain. He received the ingeniero de telecomunicación degree, a five-year telecommunications engineering program from the Universidad Politécnica de Madrid (UPM), Spain. He is part of the Alcatel-Lucent 5910 Video Services Appliance (VSA) product team and has a key role in several public co-funded national and European research and development (R&D) projects. His professional and research interests are in the area of multimedia, particularly advanced video services, video processing, and stereoscopic three dimensional (S3D) content delivery.

ENRIQUE ESTALAYO was an IPTV development engineer in the Multimedia Integration Practice at Alcatel-Lucent's Video & Networking Competence Center in Madrid, Spain when this paper was written. He received a five-year telecommunications engineering degree at Universidad Politécnica de Madrid, Spain. He is part of the Alcatel-Lucent 5910 Video Services Appliance (VSA) core team and actively participates in several public co-funded research and development (R&D) projects. His professional interests are focused in the areas of enhanced video services, computer vision, and three dimensional (3D) graphics.

NARCISO GARCÍA is professor of signal theory and communications at the Universidad Politécnica de Madrid (UPM), Madrid, Spain. He received the ingeniero de telecomunicación degree, a five-year engineering program (Spanish National Graduation Award), and the doctor ingeniero de telecomunicación degree, or Ph.D. in communications (Doctoral Graduation Award), both from the Universidad Politécnica de Madrid (UPM), Madrid, Spain. He has been a member of the faculty of at UPM for almost 25 years. He leads the Grupo de Tratamiento de Imágenes (Image Processing Group) at UPM. He served as coordinator for the Spanish Evaluation Agency from 1990 to 1992 and evaluator, reviewer, and auditor of European programs since 1990. His professional and research interests are in the areas of digital image and video compression and of computer vision. ◆