How Pay-TV becomes E-Commerce

This is an extended version of a conference paper presented at 7th International IEEE Conference on E-Commerce Technology 2005 (Munich, July 19-22) IEEE Press P2277, ISBN 0-7695-2277-7

Ulrich Greveler

Horst Görtz Institute for IT Security
Ruhr-Universität Bochum
Germany

ulrich.greveler@nds.rub.de

Abstract

In this paper we highlight the fact that existing Pay-TV schemes operating on countries or world regions could be transformed into a global system as the digital television broadcasting technology offers the possibility to put different regional content (e.g., audio and subtitle information) into one transmission so that each user could decode the content according to his personal needs. As the Internet could be used for selling Pay-Per-View licenses and the digital multimedia content can be played by personal computers the existing Pay-TV systems could become a global electronic commerce solution reducing the transmission cost per content significantly.

We will consider the issue on DRM enforcement that could be a major stumbling block for such a global system as the digital rights holders will probably not support a new system that eases piracy and unauthorized copying of valuable content.

A new global e-commerce Pay-TV scheme will be presented that can be implemented on top of existing technology and that uses GSM mobile phone networks for location validation of the user equipment. This way we will not lower the DRM security baselines of existing regional Pay-TV systems.

1. Introduction

In the recent past we witnessed the quick emergence and growth of electronic commerce (e-commerce) integrating business processes with information technology and Internet based sales channels using the world-wide web and the Internet technology as a bearer [14].

Pay-per-Download or Pay-per-View is nowadays a known concept for e-commerce applications where web-based virtual shops use the web not only for the product offering but also for *shipping* the goods to the customer. The Pay-per-view business model for selling digital goods (e.g., music tracks, e-books, journal articles) via the Internet is well established and it particularly has initiated the ongoing research and development work regarding robust and secure digital rights management (DRM) solutions [1].

Before e-commerce became a commonly used term there was already the world of analogue Pay-TV where the subscription based content distribution of television programs and the Pay-per-View model for single high-value transmissions (e.g., sports events or movie premieres) had been in place for years and had become a successful business model for several broadcasters. Pay-TV in Europe and the US could deliver audiences numbered in millions already in the early 1990s with analogue communication networks (satellite, cable-TV, terrestrial) when e-commerce over the Internet was not yet invented.

As television broadcasting becomes *more digital* and adopts the same standards for multimedia transmissions as Internet-enabled PCs [11, 5] and as these PCs can get access to the data channels used by television broadcasters (DVB-S, DVB-C) as well as to high-bandwidth Internet connections, the question comes up: when do the technologies converge toward a point that any user connected to the Internet could use any pay-per-view television offering? From an Internet user's point-of-view, it would be a similar question: When does Pay-TV become e-commerce? Reasoning that by following e-commerce strategies the Pay-TV broadcasters or the digital rights holders could reduce their costs of delivering the content significantly, we can analyze the barriers that are preventing the Internet access to Pay-TV.

The major barricade to overcome here is DRM enforcement: a new distribution channel will not realize its potential before the digital rights holders are convinced that the new way to deliver their valuable content to the consumer does not technologically facilitate unauthorized copying of content [2].

In this paper we will identify the obstacles which prevent Pay-TV broadcasters or the digital rights holders of television content to use e-commerce mechanisms. We will develop a set of requirements regarding an e-commerce approach to Pay-TV. These requirements are to be honored to make it feasible for Pay-TV broadcasters to follow this approach. We will then describe a technical model for a Pay-TV / e-commerce solution that takes DRM issues into account by showing that it is possible to implement such a solution on top of existing technologies and interfaces without the need to develop and roll out a new multimedia communication or DRM enforcement system first. This way we demonstrate that Pay-TV could *become e-commerce* today.

The rest of the paper is organized as follows. We will give some background information and define the terms in the following section. After that the Pay-TV status quo is examined in detail and the requirements of a new system that can act as an e-commerce application are described. The next section will then sketch the architecture of the new system and describe the standards that are (re-)used in our approach. We will then give properties and a security analysis of the proposed system and eventually draw some conclusions.

2. background and definitions

A pay-per-view system consists of a sender S and a set of users $U = \left\{u_1, u_2, \ldots, u_{|U|}\right\}$. Each user is subscribed or entitled to some content, which is coded in a transmission T. The sender encrypts the content and sends it via the broadcast channel. A user is provided with a user terminal (which we call a set-top terminal, STT), which receives and decodes the broadcasted content. This STT can be a television set-top box as well as a laptop computer with multimedia functionality or a mobile phone that is able to receive broadband broadcasts of digital multimedia data.

Current Pay-TV systems are serving only a sub-region of the signal coverage area. An improved system would cover the whole area (or extend a limited area to all STTs connected to the Internet) and enforce DRM policies to the delivered content.

Digital multimedia content is already suited for cross-border delivery as current standards as MPEG2 [11] do support multiple audio streams and subtitle texts per video stream so that each user can choose the audio language of a transmission.

The commercial scenario we consider in this paper is that of content broadcast transmission where the transmissions are secured (encrypted), so that only authorized users can receive (decrypt) the transmission. An important example is digital Pay-TV, where a digital signal is broadcasted via satellite, cable or a terrestrial radio connection (e.g., DVB-T). But there are also other applications for pay-per-view services such as Internet multicasts for audio, video or data transmissions similar to the Pay-TV situation.

3. Pay-TV status quo

These days, a Pay-TV provider is serving customers in a dedicated region (e.g., a country). Its program offering is tailored for the potential customers in this region (e.g., language, interest).

3.1. Digital Broadcast Issues

The Pay-TV provider often sends the secured transmission to a super-set of the user base already. Considering satellite broadcasting, a transmission intended for one country could be received (but not decrypted) by users in many countries. Transmission costs per user would be lower if these users outside the region could participate in the Pay-TV scheme because the sender bears the cost for using a satellite data channel. The cost of a transmission is independent from the number of users receiving the transmission.

The Pay-TV provider might even send the transmission through several networks (e.g., more than one satellite or cable network) and cover most parts of the world and reduce costs per user further when the transmission is relevant for such a huge user group (e.g. world-class sports events, new movie productions). A good reason to do this is that the transmission needs to be prepared for digital Pay-TV broadcast transmission only once but could then be used for several digital broadcast networks.

A global Pay-TV transmission could be produced with several audio and subtitle text channels so that each user in some part of the world could select the correct channels for his needs and is able to consume the global transmission that is sent to many parts of the world. All this is possible but global broadcasting to end-users is not done today.

If a Pay-TV provider uses the same STT technology in many regions the possibility to send transmission to super-regions will be enabled. There are only few standards for digital television broadcasts that cover major parts of the world, America: ATSC standard, Japan: ISDB-T (similar to DVB-T), Europe, parts of Asia and Australia: DVB-S/T/C. The DVB standard family could easily grow to a globally used standard if global Pay-TV services became a reality.

The e-commerce idea we portray in this context is that transmissions could be sent and received globally; the Internet could be used for selling the pay-per-view licenses. An STT temporarily connected to the Internet and being able to receive constantly broadband digital data via non-Internet sources (e.g., satellite reception) would be the user's equipment in such a scenario.

All these e-commerce enhancements are not in place today and there is no visible move to go in that direction (standard STTs and broadcast technologies are becoming a reality, though [10, 9]). The digital rights holders sell the content on different terms to each regional Pay-TV provider and they enforce DRM differently in the regions. A content can be of different economic value in different regions so the current regional Pay-TV systems reflect these values with the subscription fees.

3.2. Technology and Business Parameters

A Pay-TV system that covers multiple regions needs to be designed in a way that no feasible hardware or software manipulation to the STT does help an attacker to construct a super-terminal showing all transmissions from all regions *for free*. It is unlikely that the rights-owners would accept a global Pay-TV system that can not assure this hard minimum requirement.

Unfortunately to the e-commerce approach, a global Pay-TV system cannot use the Internet for transmitting the (secured) content for performance reasons today. Also in the near future it cannot be expected that a home Internet connection is so stable and swift that a high-quality multimedia transmission (easily exceeding 4GB of data) which requires a stable bit-rate for several hours is transmitted without deferments or connection disruptions. The data size of multimedia transmissions is growing as well as the bandwidth of home Internet connections but it is unforseeable when the gap might be closed. Note that there is a multicast future for IP-based communication [8] but IP multicast is not necessarily the right choice for distributing Pay-TV via Internet [13].

However, while the Internet can be used to perform the Pay-Per-View sales transaction delivering a license to the user equipment the same user equipment could link to other high-bandwidth broadcast data sources (e.g., satellite, cable, digital radio broadcast) in order to receive the multimedia transmission. A global Pay-TV server could use several satellites and cable networks simultaneously to transmit to a user base distributed across different regions.

3.3. Regional Pricing

The rights-owners may require that for every region a different pricing and subscription model for transmissions can be set and also that some regions shall be blacked out for certain transmission but might participate in a later re-transmission when other regions are excluded.

The rights-owners will probably not accept a global system if there is a risk of pirate decoders that could circumvent the whole system and become super-terminals showing all content for free.

Currently, most Pay-TV providers focus on a country and the offering is sold in this country only. A user could export a STT to another country, though, and use a subscription there if signal reception is technically possible. However, the transmission for one country do most likely not contain multiple audio tracks or subtitle information so that users in another country speaking a different mother-tongue will in general be less interested in the offering. This provides implicit DRM enforcement: a user outside a region can not consume the content that is dedicated for the region because this content is simply unavailable outside.

From a rights-holder's point of view a global Pay-TV provider could reduce its costs per transmission compared to a national service provider and Pay-TV as a sales channel for multimedia productions could return higher profits as costs are are cut back. A national Pay-TV provider being forced to go global might not favor globalization of his services and see the need to seek an international alliance or merger as supposably only a few global players will be able to compete on a global market.

3.4. Related Ideas

In the past there was some development to standardize multimedia data formats so that hardware media could be produced and used worldwide while the rights-holders' ideas of regional sales strategies are respected: The Digital Versatile Disc (DVD) region codes [15] are an example for this strategy. The DVD media carry a code that specifies a *region* of the world (one or more regions out of six) where the media can be played. The basic policy is that a DVD player bought in one of such regions will only play media dedicated for this region. This technology can not prevent that a player is exported to another region thus it is not suitable for technically enforcing different media prices in the regions. Moreover, it was quickly rendered useless after computer DVD drives could be used to play DVD content disregarding the region code information or altering the player region code if necessary by applying freely available patches to the player software.

Another development are the Internet video initiatives: *CinemaNow* [4] was founded in 1999 by several companies and headed by Microsoft. Several thousand movies are offered on a Pay-per-View basis. The system does not incorporate the full offering of a Pay-TV provider (e.g., real time transmission of events) and the multimedia content does not meet the established digital television standards (this reduces the media file sizes though). *MovieLink* [12] was launched in 2002 by major digital rights holders (i. e. Hollywood movie studios). Several hundred movies are offered but only US customers can participate in the service so the regional DRM issue was solved in a way that only one region is covered. Both initiatives might give the industries helpful experiences for future Internet based movie distribution channels but they are not intended to take over the role of Pay-TV stations.

3.5. Wish List of Requirements for a new E-Commerce based Global Pay-Per-View System

In order to reflect the technological and business parameters laid out in the above sections we fix a set of requirements for a new global Pay-TV system that follows e-commerce considerations.

- The system shall provide a global offering to Internet users who are able to receive high-bandwidth broadcast data.
- There shall be no theoretical possibility to construct a system pirate device displaying all content of all regions without a license. Moreover, a pirate device shall never display content dedicated for a region it is not located in
- The multimedia coding technology and the STT architecture shall adopt existing standards. There shall be no need to roll out a new broadcasting and set-top technology - e. g., latest-generation STTs already shipped to the user base shall be enabled to participate in a new system
- The STTs may be exported but shall always enforce DRM policies in the region they are located in.
- The STT technology shall adopt the same tamper-proof and system security requirements as existing Pay-TV systems. Established conditional access solutions shall be used.
- An existing state-of-the-art Pay-TV provider shall be able to extend the regional coverage to a global coverage while the legacy user base can still be served with the same technology
- If the system security is compromised in one region the system security in other regions shall not be affected necessarily.

The goal is to construct a scheme meeting all of these requirements.

4. A new Pay-TV System approaching E-Commerce

The new Pay-TV system architecture that we want to sketch in this section shall fulfill the security and DRM requirements we have identified in the preceding section. It shall not be less secure or less efficient than current productive Pay-TV systems that operate in a dedicated region (e.g. country), i.e. the aggregation of several regional systems to one new global system shall not make it easier for an attacker to jeopardize the system security in one region only because the system is compromised in another region.

4.1. Architecture Goals and Definitions

Our proposed system provides multimedia transmissions that are secured by encryption (as it is the case for current Pay-TV systems). Every user $u \in U$ owns a unique user key k_u that is stored on the smartcard inside the device. All content is encrypted at source and decrypted at the STT. To decrypt a transmission T one or more session keys $k_1^S \dots k_n^S$ are needed that are derived by the user's STT by using the individual user key and information sent to the STT in a control message individually encrypted for each user who has obtained a license.

The session key(s) are valid for one transmission only and used to decrypt the video content as well as the audio content a user is entitled to according to his subscription contract and / or pay-per-view payment. We will call this collection of user rights the user's *license*. Note that a user may only be entitled to some subset of the transmitted video or audio content; this subset is dependent not only on the license but also on the location of the user. In our proposed system architecture the STT can only derive the session keys that make it possible to decrypt exactly these subsets.

If a user moves the STT to a different area before or after obtaining a license the STT is not able to decrypt more content than the user is entitled to in this different area. The system enforces the DRM policy with technical measures – we will not rely on a legal environment that prohibits the misappropriation of content by assigning penalties for wrong behavior. Note that such a uniform legal requirement could not be easiliy established across borders.

4.2. A new system on top of existing standards

We use conventional conditional access technology for securing the multimedia transmissions. The content is coded in MPEG [11] format and encrypted by the DVB encryption standard.

The user STTs is equipped with a *Common Interface* [3], an established standard used in digital video broadcasting. This Common Interface is normally connected with a *CI module* that is incorporating a smart card reader where the user will put in a smart card issued by the Pay-TV provider. Most currently available set-top boxes and DVB-cards for Personal Computers provide at least one or more than one Common Interface slot. Different CI modules facilitate different cryptographic protocols and algorithms used by the Pay-TV service providers and implemented on a CI module. All STTs are applying the same content descrambler (the *Common Scrambling Algorithm*), during a secured transmission the STTs continuously receive *control words* via the Common Interface that are needed to descramble the secured content. These Control Words are short-lived session keys only used for a part of one transmission. Our proposed solution will operate on top of this existing technology so today's standard STTs equipped with the common interface could be used in the new solution and the same level of cryptographic security is achieved.

The proposed solution will contain a new component: the *DRM device*. This device takes over the role of today's CI module and but still sends the Control Words to the STT and carries the provider's smart card if a tamper proof key container is required.

The new functionality introduced here is that this device will also receive location dependent information so that the STT needs to be located in the correct region when a license obtained by the user is only valid for a named region. The idea is to utilize a different radio network that can send small amounts of information individually encrypted for a user to a rather small region so that this information would be missing in other regions where the broadcast signal is still available.

In order to use well established technology this location dependent information could be transmitted via the GSM [7] mobile phone network using the service *cell broadcast* [6]. This radio interface does require the DRM device to incorporate a basic non-voice GSM terminal card so that these cell broadcast messages can be received. The Pay-TV smart card can be used to store the GSM network authentication data (IMSI, K_i) so that no further hardware is needed (see fig. 1). In the case where a GSM mobile phone is a STT by itself no extra GSM terminal card is needed. Regions without GSM coverage can also participate if another local radio network with cell addressability is available (e.g., analogue mobile phone networks or pager networks).

The sender will broadcast some of the information that is necessary to derive the Control Words individually encrypted to each user addressing only the GSM cell area the STT is located in. By evaluating the location information given by the user while purchasing his license or obtained through outgoing GSM communication by the device. The exact way to obtain location information about the STT can be chosen according to user privacy regulations. The GSM cell is a rather small area with a diameter of less than 20 kilometers so it sets a sufficient hard limit regarding the mobility of the STT that shall not be moved outside a much greater area (e.g. a country).

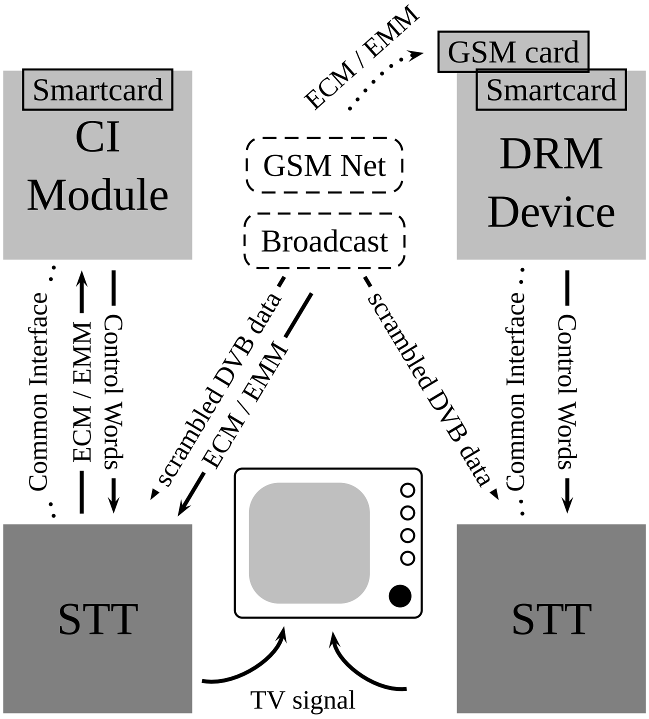

Figure 1. Standard Conditional Access Scheme — Proposed New Scheme

The key feature here is that this location dependent information can not be received when the DRM device (connected to the STT) is moved outside the region. An attacker might be able to simulate localization information (e.g. manipulate the unsigned GPS data signal fed to an STT if GPS technology was used instead) but he will not be able to receive information that is not broadcasted at the STT location GSM radio cell.

A user may obtain a license for a certain transmission in a certain region. The sales channel can be the Internet, e.g., a web-shop selling Pay-Per-View licenses on behalf of a global Pay-TV provider. If the user PC is also the STT (e.g., because a built-in DVB card is used and the DRM device is connected to the CI slot of the card) the consumption of the content could take place directly at the user's desktop.

Before a transmission starts the sender sends *Entitlement Control Messages (ECMs) and En-*

titlement Management Messages (EMMs) to the STT as it is the case in current Pay-TV technology (for details refer to [3]). These messages are required by the CI Module to activate certain subscriptions and to generate the Control Words during the transmission. The difference is that in our proposed system the ECMs / EMMs are not sent via the broadband channel but via the GSM cell broadcast to the specific user location. Hence, the user can only exercise a license if the STT location matches the region attribute of the license so a rather inexpensive license obtained by pretending to be in a different region is useless as the DRM device will not receive the ECM / EMM messages and can not generate the Control Words necessary to descramble the content. Because this location property is not achieved through cryptographic measures but through location dependent information the mechanism cannot be attacked with cryptanalytic strategies or by breaking tamper-resistant devices (i. e. smartcards).

Note that the business model of the digital rights holder might require that the content is received as free-TV in some regions, sent to a set of flat-fee subscribers in another region while in yet another region only Pay-Per-View is offered. All these different regional DRM policies can be honored by our proposed system although only one secured transmission is broadcasted globally.

4.3. Properties and Security Analysis of the Proposed System

The proposed system can assure the same security standard as existing regional Pay-TV systems if the sole technology change in this region is that Pay-TV CI modules are replaced by the proposed DRM devices and if the tamper resistance properties of the modules and the devices is comparable. The feasibility of an implementation depends on the global adoption of conditional access technology and DVB standards.

An attacker might utilize a functional STT together with a license in one region for the purpose to intercept the Control Words on the slot interface and use the intercepted Control Words to run a STT in another region where the license is not valid. If this type of attack is feasible (the Control Words need to be transmitted real-time to another region if the transmission there is to be descrambled in real-time as well) then it could be applied already today for regional Pay-TV systems where the data broadcast is covering a super-region (e.g., satellite Pay-TV, cable networks). A possible counter-measure for this type of attack is to enforce a mutual authentication of the CI module and the STT. As the underlying Pay-TV standardized technology is the vulnerability in this case our proposed system is not more secure than the content scrambling standard adopted by it. If the Scrambling Algorithm is broken then new STTs have to be rolled out anyway and our system could operate on top of this new standard technology again.

If the system is broken in a region so that pirate users could generate their own licenses without the need to pay for the purchase by using other users' cell broadcast messages in that region then these licenses are still useless in other regions as the STTs do not receive matching ECM / EMM messages for the pirate licenses. Hence, a local failure of the system security does not necessarily affect the global security of the system.

Finally we have to take into account that the GSM networks are used as trusted parties in our proposal. A manipulation of a network that makes it possible to re-route a GSM cell broadcast to a different region (in a different country) would threaten the system security as the DRM device could not securely determine the user location anymore. This kind of attack is unlikely performed by a single Pay-TV pirate user but it should be regarded as a potential mechanism to let our proposed global Pay-TV system fail regarding DRM enforcement in some regions.

5. Conclusion

In this paper we presented a concept of transforming existing regional Pay-TV business and technology to an electronic commerce based global realization. We identified the current obstacles regarding DRM enforcement that possibly prevent a global technological offering although such a system could reduce the transmission costs significantly. We sketched a new global Pay-TV scheme that could be implemented on top of existing technology and that would use standard hardware already rolled out in the user space (Set-top Boxes). We also presented evidence that the proposed new scheme will not be less secure than existing state-of-the-art Pay-TV systems.

References

[1] S. M. Bill Rosenblatt, Bill Trippe. *Digital Rights Management: Business and Technology*. Wiley, first edition, Nov. 2001.

[2] D. Brown. Pay-tv business planning. Technical Report www.im-reports.com/PTVBP, International Marketing Reports, June 2003.

[3] CENELEC. Common interface specification for conditional access and other digital video broadcasting decoder applications. Technical Report EN 50221, Technical Committee TC 206, Oct. 1997.

[4] CinemaNow. http://www.cinemanow.com.

[5] K. et al. Mpeg-4 audio v.2. Technical Report JTC1/SC29/WG11/N2670, ISO/IEC,Audio Subgroup, Mar. 1999.

[6] I. Harris. Technical realization of short message service cell broadcast (smscb). Technical Report 3GPP TS 03.41, 3rd Generation Partnership Project (3GPP), June 1996.

[7] F. Hillebrand. *GSM and UMTS - The Creation of Global Mobile Communication*. Wiley, first edition, Jan. 2002.

[8] R. Hinden and S. Deering. IP version 6 addressing architecture. RFC 2373, IETF, July 1998.

[9] D. J. Iles. Operational dvb-t sfn experience in australia. In *IBC online paper http://www.broadcastpapers.com/tvtran/tvtran.htm*, Sept. 2003.

[10] Inter-American Telecommunication Commission. A global digital tv standard for latin america and the caribbean. Information Document 459/04, Organization of American States, July 2004.

[11] K. H. Jan Bormans. Mpeg-21 overview v.5. Technical Report JTC1/SC29/WG11/N5231, ISO/IEC, Requirements Group, Oct. 2002.

[12] MovieLink. http://www.movielink.com.

[13] K. Obraczka. Multicast transport protocols: A survey and taxonomy. *IEEE Communications Magazine*, pages 94–102, Jan. 1998.

[14] F. Riggins and H.-S. Rhee. Toward a unified view of electronic commerce. *Communications of the ACM*, 41(10):88–95, 1976.

[15] J. Taylor. *DVD Demystified*. McGraw-Hill Professional, second edition, Dec. 2000.