Enforcing Regional DRM for Multimedia Broadcasts with and without Trusted Computing

Ulrich Greveler*

Horst Görtz Institute for IT Security
Ruhr University Bochum
Germany
ulrich.greveler@nds.rub.de

This is an extended version of a conference paper presented at
First International Conference on Digital Rights Management:
Technology, Issues, Challenges and Systems
Sydney, Australia, 31 October - 2 November 2005

Abstract. We present the problem of enforcing a Digital Rights Management (DRM) system that needs to consider location-dependent licensing policies and operates on top of existing conditional access standards. A major application for location-dependent DRM is Pay-TV broadcasting as rightsholders require different business models in different regions. A global provider's enduser equipment needs to validate the user location in some way in order to enforce DRM in this scenario. We will depict several solutions to the problem and compare their security qualities. The main result is that trusted computing hardware may not be the most appropriate solution given reasonable conditions.

1 Introduction

In this paper we focus on the problem of enforcing Digital Rights Management (DRM) with location-dependent licenses for multimedia broadcasts (i.e. Pay-per-View television). Today, a Pay-TV provider serves its customers in a dedicated region (e.g., a country). The program offering is tailored to the potential customers in this region (e.g., language, national interest). As the digital rights holders may require different terms regarding distribution and pricing depending on the region in which the content is distributed to the end-customers, every Pay-TV provider will deliver the multimedia content under terms valid for the region it serves. The content is generally scrambled (encrypted) so that only the paying customers can consume the content.

* The author was supported by the European Commission through IST-2002-507932 ECRYPT.

A customer trying to circumvent regional limitations might be able to buy Pay-TV services in a distant region (another country) and move all the equipment needed (smartcard, set-top terminal) to his home region and use it there if signal reception is possible (e.g., satellite coverage). However, the audio streams and subtitles are still tailored to the customers in the distant region so the content might lose some of its value for this traveling pirate customer. Due to this effect, regional Pay-TV providers establish a regional DRM system in the sense that licenses for specific regions are implicitly enforced.

As standard set-top terminals (STTs) and broadcast technologies are becoming a reality, a future Pay-TV provider might want to serve customers in several regions or globally. The broadcast signal might already be received in a super-region when radio or satellite networks cover multiple countries or Internet multicast is used. In these cases, the offering quickly becomes global. Transmissions can incorporate several audio and subtitle streams so that each customer is enabled to choose and consume the content following his preferences.

The digital rights holders may welcome such a global Pay-TV provider when transmission costs are reduced significantly but they will most probably not accept the content being distributed in a way that infringes rules on regional licensing and eases piracy.

	Region 1	Region 2	Region 3
Transmission 1 (**date:** Jan 15) **audio:** E, F, DE **subtitle:** E1, E2, F	per-view 5$ audio: all subtitle: all	per-view 3$ audio: DE subtitle: E1, DE	black out
Transmission 2 (**date:** Feb 12) **audio:** E, F, DE, ES, IT, CH, JP **subtitle:** E1, E2, F, DE1, DE2, ...	per-view 3$ audio: all subtitle: all	black out	per-view 5$ audio: E, JP subtitle: all
Transmission 3 (**date:** Jun 19) **audio:** E, F, DE **subtitle:** E1, E2, F	free for subscribers audio: all subtitle: all	per-view 1$ audio: DE subtitle: E1, DE	free for subscribers audio: E, JP subtitle: all

Fig. 1. Several transmissions of same content, example

We illustrate these different regional distribution or business models with Fig. 1. The rights holder of a certain multimedia content (e.g., a movie production) sells to regional Pay-TV providers. The pricing, release dates and supported

languages (audio and subtitles) depend on the region. Each regional provider is able to diversify the digital content to meet the requirements and transmit the tailored content to his customers. However, if a global provider emerges that wants to serve all regions with *one* transmission covering all regional needs (and reducing transmissions costs) it has to ensure that the customers can only receive (i.e. descramble) the content they are entitled to. For instance, a customer living in *Region 1* of Fig. 1 shall not be able to buy the Pay-Per-View package for *Transmission 1* in *Region 2* and receive it at home for a lower price and with more language options than entitled. Loosely speaking, the equipment shall know where it is located and change its behavior when moved to another region and follow local rules regardless where it was bought.

2 Background and Definitions

Let us first fix what a license in our regional DRM context shall be. A user is entitled to certain content consumable under certain conditions that depend on the region once she bought a subscription and / or a Pay-Per-View product. This consumption right shall be her license and be expressed as a machine-readable license ticket shown in Fig. 2.

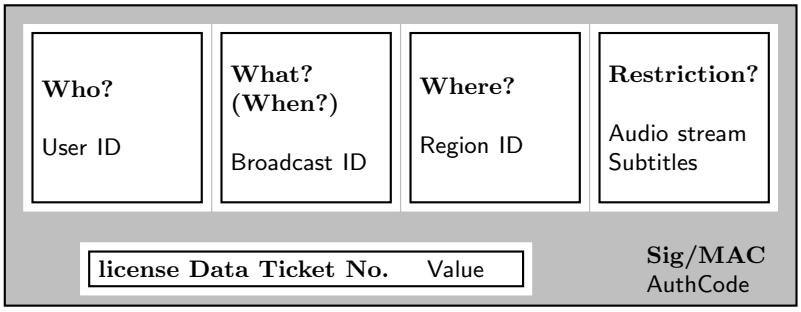

Fig. 2. License ticket

The license ticket is usually sent via the broadcast channel individually to each user and processed by the user equipment (here: smartcard). It carries the User ID so the STT or the smartcard knows whether it shall process the ticket, a Broadcast ID to map it to a transmission and a Region ID to specify the region in its regional licensing model. The restrictions are not necessarily a list of rules but could be a set of one-time keys which allow to decrypt certain parts of a transmission. This broad definition of restrictions allows us to be compatible with established technology standards. The Broadcast ID refers to a certain transmission and will change when a transmission is repeated. The time of the transmission is thus indirectly encoded with this ID. The ticket is authenticated by some cryptographic mechanism (e.g., a MAC function) and may carry a unique number for differentiation.

Multimedia Standards In order to approach practical relevance for our proposed system, we briefly describe the relevant standards regarding Pay-TV and multimedia distribution. The goal is to operate on top of established technology so that security can be achieved without the need to roll out a new infrastructure based on a revised standard.

Our aim is to re-use conventional conditional access technology for securing multimedia transmissions. The content we refer to is coded in MPEG [1] format and encrypted by the DVB encryption standard. DVB can be broadcasted via satellite (DVB-s), terrestrial emitters (DVB-t) and cable (DVB-c).

Currently, most Pay-TV customers own an STT equipped with a *Common Interface* [2], an established standard used in digital video broadcasting. This Common Interface is connected with a *CI module* that is incorporating a smart card reader where the user will put in a smart card issued by his 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 that the Pay-TV service providers use and implement on the module. All STTs are applying the same content descrambler (specified by the *Common Scrambling Algorithm*). During a secured transmission the STTs continuously receive so-called *Control Words* via the Common Interface that they need to descramble the secured content. These Control Words are short-lived session keys only used for small parts of one transmission.

3 Enforcing Regional DRM

3.1 Appropriate Organizational Measures

The DRM enforcement could be based on organizational measures only – or be combined with technical measures described in the next sections.

Regional Smartcards If the distribution of smartcards (as part of the Conditional Access system) could be linked to the regions defined by the DRM policy (and each card stays in a region), it is not a difficult task to enforce the license restrictions. The sender would send the management messages containing the descrambling information to the set of smartcards distributed to a region. Only these cards are then able to descramble the content according to the regional licensing model. This regional licensing approach is not new and was in particular set into practice for DVD media in the nineties (by applying *regional codes*) and did not prove to be successful.

The attacker's task in such a scenario would then be to move the smartcard from one region to another (e.g., from an *inexpensive* region to an expensive one) or to alter the card distribution process. The sender (in the role of the smartcard issuer) could prohibit that cards are moved across borders but this would probably not stop all potential attackers. Moreover, such a regulation might not even be enforceable by law as a violation of the subscription contract

is not necessarily a breach of law in every region. In this case the sender is unable to prosecute traced pirates. Such a situation renders regulations useless.

3.2 Technical Measures: Tamper Resistance / Trusted Computing

In order to technically prevent unauthorized movement of the user's STT (including the CI module and the smartcard), either the network or at least one component has to validate the location when no other technical measures are in place. If the STT is forced to initiate a communication to the sender before a transmission there are several proposed ways to locate the equipment by letting the STT initiate a communication to the broadcast sender [3], but as we aim to operate on top of the established DVB and Conditional Access standards, we cannot expect the STT to have such a convenient call-out feature. The communication is one-way only, hence the sender does not know where the receiver is located.

As the STT itself is standard off-the-shelf hardware being sold across regions with no localization features, either the CI module or the smartcard may be augmented with extra-functionality to validate the user location.

Positioning Systems The CI module delivered by the Pay-TV provider could incorporate a positioning module like a GPS or Galileo signal receiver. If the positioning unit operated in a secure (i.e., tamper resistant) environment it would be able to securely validate the location and check the license against geographical co-ordinates. If a confidential channel to the smartcard is established, the descrambling of content will only be initiated if the correct location is determined.

The positioning module would unlikely be incorporated in a smartcard as the restriction on size and computational power are much higher compared to the CI module. However, this option should be taken into consideration for completeness. Our findings regarding the CI module augmented with a localization module are also valid for smartcards with localization features, so we do not elaborate on an augmented smartcard approach further.

The tamper-resistant device in this scenario needs to validate the license ticket by checking the co-ordinates of the STT against the Region ID in the ticket. If the user (her equipment) is located in the specified region, then the descrambling process is initiated. This process is specified by Algorithm 1.

3.3 Technical Measures: 2nd Radio Network

For this scenario we apply an idea from [4] where an additional radio network for Pay-TV localization purposes is used. This 2nd radio network with low data throughput performance can send small amounts of key information (individually encrypted for a user) to a *radio cell*, which is a rather tiny area (compared to the rather big regions), so that this information would be missing in other regions where only the broadcast signal is available. In order to use established

Algorithm 1 ticket processing and localization

```
repeat
   read ticket
until ticket on User ID is received
get STT co-ordinates
if Region ID matches co-ordinates then
   return keys from ticket restriction field
else
   return license violation error
end if
```

technology, the individual information could be transmitted via the GSM [5] mobile phone network using the service *cell broadcast* [6]. This radio interface does require the CI module device to incorporate a basic non-voice GSM terminal card so that these cell broadcast messages can be received. Regions without GSM coverage can also participate if another local radio network with cell addressability is available (e.g., pager networks or analogue mobile phone networks). This enhanced CI module is called a *DRM device* (in [4]) to distinguish it from an ordinary CI module.

The localization is implicitly performed via the 2nd radio network and there is no need to use clients of positioning systems. In order to apply the second radio network scheme to our ticket based licenses approach each ticket is split up into two parts. The restrictions field containing the cryptographic keys are removed from the ticket that is sent via the broadcast channel. This part, which is represented by a rather small amount of data, is sent via the 2nd radio network to the user location's radio cell if the cell co-ordinates match the Region ID. Note that Algorithm 2 does not contain any conditional statements.

Algorithm 2 ticket assembling using 2nd radio network

```
repeat
   read ticket.part1 (broadcast channel)
until ticket.part1 on User ID is received
read ticket.part2 (2nd radio network)
assemble ticket from both parts
return keys from ticket restriction field
```

3.4 Security Analysis of Measures

Organizational measures: There is no obvious way to compare the strength of the organizational measures named in the preceding section to technical measures, but history shows that selling devices in a certain region and banning export to other regions is not a method to stop users from doing so. The Digital Versatile Disc (DVD) region codes [7] are an example for this strategy. The

DVD world is divided into six regions and DVD players in one region shall only play media with the correct region code embedded. It has not been a successful security mechanism: one problem is that many software players need to be configured for region locking before first use but could be resetted later or patched to be *region-free* while the media are shipped to more regions by mail-order anyway. But apart from that license enforcement weakness, the DVD has been a commercial success.

Small-size devices like smartcards can easily be transported or shipped by mail and it does not require any expertise to remove the smartcard from the card reader and send it to somebody else in another region. Moreover, different national laws might not legally support the system supplier's export regulation and render it useless.

Trusted Computing: While the trusted computing property of the CI module (or a part of it) can be a significant line of defense for an attacker, the positioning radio signals are received outside the TC environment before the secure computation is initiated. A straightforward attack scenario would be to remove the antenna and record the signals at another location in order to replay it. The same result could be reached by generating fake signals and feed them to the positioning unit directly. Regarding the current de-facto standard positioning system (GPS), the latter task is feasible as the positioning satellites' signals are not cryptographically protected at all and fake signals can easily be generated.

A direct attack on the Trusted Computing hardware is generally regarded to be too costly for an average attacker, but it still needs to be considered here as the pivotal machine command executed by the secure hardware is the **if**-statement of Algorithm 1. The attacker only needs to provoke a faulty system state at this computation step in order to circumvent the trusted hardware; he does not need to read any secret keys in the device. This kind of attack on tamper-resistant hardware could be rather inexpensive [8], and special protection concepts against these attacks have to be considered [9].

2nd radio network: Our first observation is that the second radio network (e.g. GSM network) is used as a trusted party in this scenario. A manipulation of a network that makes it possible to re-route a 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 might unlikely be performed by a single Pay-TV pirate user, but it shall be regarded as an attack on the whole global DRM system that could be launched by a group of attackers being organized.

As the key information needed to descramble the content is not available in other regions (by the trusted 2nd radio network), an attacker can not gain anything from manipulating the STT, smartcard or DRM device hardware. If the information is not available in the region the attacker is located in, it could not be derived from other information stored by the user equipment at all.

An attacker might utilize a functional STT together with a license in one region for the purpose of intercepting the Control Words on the slot interface

and use the intercepted data to run a STT in another region where the license is not valid. These Control Words are the secret information continuously issued by the DRM device via the Common Interface that is needed by the STT to descramble the content during a broadcast session.

If this type of attack is feasible (the Control Words need to be transmitted realtime 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). The attack could also be applied for the trusted computing based solution sketched above, so it does not distinguish the measures from each other.

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 standardized Pay-TV technology is the vulnerability in this case the proposed system is at most as secure as the content scrambling standard adopted by it. If the scrambling algorithm is broken, then new STTs have to be rolled out anyway and the system could operate on top of this new standard technology again.

Comparison of technical measures: In order to compare the measures it is reasonable to identify the differences first. The trusted computing solution of the problem does require a trusted hardware framework for the localization device that needs to be issued together with the STT to the enduser. Such a device would increase the cost for the enduser equipment considerably. Moreover it is limited in its suitability for solving the problem as current available positioning systems can be circumvented by feeding a fake signal to the antenna input. The trusted computing device would still store secret information that could be used by an attacker to descramble the content if a successful attack on the secure hardware could be launched. The 2nd radio network solution does not need additional trusted computing hardware (a smartcard would still be used, though) and it would not store secret information that could be used to descramble the content as this information is not available outside a target region. The major difference to the TC solution is that another (trusted) network is needed and the usage of the network services would also add cost to the global content distribution (and some extra hardware is needed as well). The security limitation here is the amount of trust towards the second radio network management. If the cost generated by both solutions is assumed to be comparable or negligible regarding the security considerations, the remaining differentiator is the security limitation of each solution. As the generation of fake positioning signals (or usage of copied signals) is a feasible task for an attacker, while the manipulation of a radio network is considered infeasible, and as the trusted computing hardware can also be subject to successful attacks, we would favor the latter solution under reasonable conditions. Note that this decision is based on theoretical analysis only and might not withstand real-life conditions regarding cost and availability of hardware and radio networks.

4 Conclusion and Outlook

Solutions to the problem of enforcing a DRM system that needs to consider location-dependent licensing policies can be based on very different technical or organizational measures. A global Pay-TV provider being forced to provide the enduser equipment for user location validation can choose between these different options. The options differ in cost and security properties. Trusted computing hardware that is often considered to be a standard instrument for DRM enforcement is not the only option to follow here, depending on the additional conditions to be considered, it might even be inferior to other solutions.

References

1. Jan Bormans, K.H.: Mpeg-21 overview v.5. Technical Report JTC1/SC29/WG11/N5231, ISO/IEC, Requirements Group (2002)
2. CENELEC: Common interface specification for conditional access and other digital video broadcasting decoder applications. Technical Report EN 50221, Technical Committee TC 206 (1997)
3. Gabber, E., Wool, A.: How to prove where you are. Proceedings of the 5th ACM Conference on Computer and Communications Security (1998) 142–149
4. Greveler, U.: How pay-TV becomes e-commerce. Proceedings of the 7th International IEEE Conference on E-Commerce Technology 2005 (2005) 508–511
5. Hillebrand, F.: GSM and UMTS - The Creation of Global Mobile Communication. First edn. Wiley (2002)
6. Harris, I.: Technical realization of short message service cell broadcast (smscb). Technical Report 3GPP TS 03.41, 3rd Generation Partnership Project (3GPP) (1996)
7. Taylor, J.: DVD Demystified. Second edn. McGraw-Hill Professional (2000)
8. Anderson, R., Kuhn, M.: Low cost attacks on tamper resistant devices. IWSP: 5th International Workshop on Security Protocols, LNCS 1361, Springer-Verlag (1997) 125–136
9. Kommerling, O., Kuhn, M.: Design principles for tamper resistant smartcard processors. Proceedings of the USENIX Workshop on Smartcard Technology (1999) 9–20