Location Dependent Digital Rights Management

Thomas Mundt
University of Rostock
Albert-Einstein-Str. 21, 18059 Rostock, Germany
thm@informatik.uni-rostock.de

Abstract

In this paper we present a concept and an architecture for a location dependent Digital Rights Management system. The solution is based on a trusted hardware which incorporates the decryption of digital data, a precise secure clock, and a GPS position receiver. A prototype is currently being developed in cooperation with a hardware manufacturer.

1. Introduction

Within the academic community and the general public Digital Rights Management (DRM) is discussed very controversial. Beside all ethical and practical disadvantages DRM has eligibilities where copyrighted or classified material has to be protected. Usually this protection is realized by binding a resource to a certain context such as a single computer or a single person. There is an obvious need for DRM with location as arbitrative credential to gain access to a resource.

1.1. Scenarios

The idea of authenticated positioning and location driven DRM has been developed after finding a vast variety of scenarios where location is essential for controlling access to resources. A small fraction of those scenarios is presented here:

- A company wants to make sure that secret material remains within the company's ground.
- An Oscar nominated movie shall be only viewable at the referee's home only.
- TV shows or DVD movies are licensed to a single country only.
- An amoured car for money transport can be opened next to the bank only.
- A harddisc of the Los Alamos National Lab containing the blueprint of a nuclear bomb can only be read when the harddisc is on the premises of the lab.

1.2. Idea

Digital Rights Management plays a vital role whenever classified or copyrighted material shall be restricted to be used on certain computers, by certain persons or within a certain timeframe. With our idea it is possible to use authenticated position information delivered by Galileo [13] to enable access to restricted digital material or to restricted devices. A secret key can only be utilized to decrypt the digital material or to enable any other process when the device is in the specified area. The major component of our idea is a trusted device analogous to TCPA hardware. The decryption process is controlled by the position which will be determined within the same trusted device. It further includes a trusted time source. To describe the area where access is granted it uses an authenticated dataset (shape). This dataset can be part of the digital material or for some purposes be permanently integrated into the TCPA device.

The TCPA device can be manufactured as a chipset to be integrated into a variety of devices. Examples are:

- TV set top boxes or satellite receivers
- Data viewers / Data storage devices
- Mobile computers

The system uses plausibility checks to ensure the received signal has not been tampered with - for instance has not be reradiated on a different location or replayed. The internal time source is necessary to deal with reradiated signals. Whenever a signal is reradiated, there will be a time difference. Additional hints that the signal is authentic can be permanent monitoring of signal strength, position, speed, and accelaration. In case there are reasons to believe that the satellite signal is not authentic the user can be asked to move a little bit in a given direction. This reduces the risk of having many users connected to one static receiver that distributes the signal.

1.3. Structure of this paper

In section 2 we discuss existing technology in the fields of authenticated positioning, Digital Rights Management, satellite based location providers, and authenticated clock synchronization. Section 3 introduces our new approach on a conceptional level. We report about first experiences with the system in section 4. A short conclusion is presented in section 5.

2. Technological basis

In this section all major technologies needed to implement the proposed solution for authenticated positioning and position dependent rights management are presented in a very short way. Those technologies include DRM which is obviously necessary, satellite based positioning systems as a possible location provider, highly precise clocks needed to work offline and to prevent rerouting attacks, and a secure time synchronization protocol needed to set the internal clock. At the beginning fundamentals of authenticated positioning are discussed. An overview of the current patent situation is also given.

2.1. Authenticated positioning

To the best of our knowledge there is no working system for authenticated positioning with the existing GPS [9]. There are a few patents in this area but no known application. This section gives an overview about authenticated positioning.

In ”An authenticated Camera” [10] Kelsey, Schneier and Hall present how an image taken by a camera can be bound in space. They explain possible attacks such as ”rerouting” GPS signals and state that these kinds of attacks are very difficult to inhibit.

An article named ”GPS Spoofing Countermeasures” which gives a general overview about methods to make GPS more secure against spoofing attacks can be found in [20]. US patent 5,922,073 [16] named ”System and method for controlling access to subject data using location data associated with the subject data and a requesting device” claims to provide a method similar to the idea described in this paper. It does not satisfactory explain how this will be achieved.

2.2. Digital rights management (DRM)

In order to understand how location can be used as input for a Digital Rights Management system we would like to give a very brief overview about DRM. Our example scenarios mention the limitation of TV broadcasts to certain areas. Therefore we also give a brief introduction how Conditional Access in Digital Video Broadcasts (DVB) is realized today.

Digital Rights Management [6] allows the copyright owners of multimedia content to decide under which circumstances they want to allow users to access documents. Access can be restricted to read, write, change, update, and other operations. A wide variety of payment methods such as pay per view, pay per copy, and pay per instance are implementable. A more comprehensive overview about DRM technologies can be found in [19].

Managed material is secured by cryptographic methods such as encryption, watermarking, and signing. For our proposed solution encryption will be necessary to protect the digital material from being read outside the enabled area. Encryption can be done by several algorithms depending on the nature of the digital material. In case of broadcasted material a stream cipher such as RC4 [1] must be used whereas for material in files block ciphers such as AES [5] can be used as well. Algorithms which require more than one key to decrypt are also available [7]. Further information about relevant cryptography for DRM is available in [3].

A simple form of Digital Rights Management is used for encrypted satellite TV broadcasts. A non-public section of the Digital Video Broadcast (DAB) [14] standard defines a scrambling and encryption mechanism which prevents unauthorized persons from watching the protected broadcast. The standard calls this Conditional Access (CA). The TV station uses a Subscriber Management System (SMS) to grant access for registered paying viewers. This is realized by sending an Entitlement Management Message (EMM) to the receiver. An Entitlement Control Message (ECM) which is also being sent is used to decrypt the Control Word (CW) necessary to descramble the digital content. The actual cryptographic process is realized in a smart card. The smart card is unique for each customer. Its inputs are ECM and EMM and its output is the CW. The standard does not define the concrete implementation of the cipher algorithm. Frequently used systems are SECA, Irdeto, and VIACRYPT [14]. Decryption is implemented on the smart card, descrambling runs on the receiver.

2.3. Satellite based location provider

Most of the scenarios backing our ideas are playing in larger areas such as countries or cities where the content should be enabled. For this purpose a regional location system would be insufficient. We concentrate on satellite based location providers. For our purpose it does not matter whether the US operated GPS or the announced European Galileo will be used. As most of the features are identical we use Galileo [13] as example.

Galileo is the new European global navigation satellite system. Its orbital components comprises of up to 40 satellites. The satellites are equipped with highly precise clocks. The time signal and signals describing the ephemeris (trajectory parameters) are constantly transmitted. A portable unit receives the signal and computes its position by using the time difference of signal arrival and the information about the satellites position. The entire system offers several local services. For instance Galileo could additionally transmit shaping information which define areas for the DRM system. A system in which Galileo transmits the shapes on country size levels is suitable for most broadcast scenarios. Bundling these information with the positioning information would simplify receivers. On an independent broadcast channel the already distributed shaping information can be referred to as an area code for instance.

Galileo provides several service levels [17, 8]. These are ”Open Service” (OS), ”Safety of Life” (SoL), ”Commercial Service” (CS), ”Public Regulated Service” (PRS), and ”Search and Rescue” (SAR). The OS service level uses un-encrypted signals and is free of charge. Receivers can use single or dual frequency measurements. There is no integrity check on this level. Signals in the CS and PRS levels are encrypted and integrity can be checked which will necessary for our concept. CS level services can be bought from licensed companies. SoL applications are also free of charge, have equivalent precision as OS (with dual frequency measurements) and use integrity checks as well as authentication of the satellite signal. For this purpose the signal is digitally signed with the private key. The public key is distributed. Further details can be found at [17].

2.4. Precise clocks

The suggested system works offline most of the time. In order to prevent the system from rerouting attacks while being offline (without return channel) it is necessary to implement a precise clock within the system. This clock must be secured against manipulation. Secure protocols for the initial synchronization are discussed later. Depending on the clock drift the times between subsequent recalibrations can be adjusted. High stability quartz based clocks at reasonable prices suitable for integration into consumer electronics have a precision of about 5*10E-7 [18]. The drift caused by temperature changes is less than 10E-12. Long time aging processes do not have much influence as they are predictable and very constant over time. This makes it possible to build clocks with less than 15 seconds time error per year. We will show later how often time synchronization is needed with this clocks to avoid rerouting attacks.

2.5. Authenticated clock synchronization

In order to synchronize the clock of the proposed DRM system it is necessary to exchange timestamps with a trusted device. In his PhD thesis of 2004 [11] Mykhailo Lyubich presents a method for secure time-stamping which can be used to synchronize clocks between two devices. He discusses a variety of threats against such a system such as impersonation and replay. For our needs it is sufficient to authenticate the trustworthy, external clock against the DRM module. This can be ensured by establishing a challenge-response-scheme.

3. Concept, architecture and security threats

In this section we briefly introduce the basic idea and motivate the chosen architecture. The architecture depends very much on a threat analysis. The relationship between threat and design decision is figured out.

Our approach exceeds existing ideas by the following:

- We facilitate precise clocks as a time reference to detect time differences arising of rerouting or replay attacks.
- We introduce a trusted hardware device to prevent manipulation of signals between components of the system.
- We use an authenticated method for regular time synchronization of the internal clock.

3.1. Overview about the proposed architecture

In order to use position information to enable access to DRM material it is necessary to find a way to authenticate the received satellite signals.

Furthermore the TCPA chip needs information about the shape where the material shall be accessible inside. This data must be protected against manipulation. It does not matter whether the protected material is broadcasted or distributed on a hardware medium such as a DVD.

Figure 1 shows an overview about the general functionality of the proposed chipset.

3.2. Threats and countermeasures

Relevant for this idea are situations where neither a permanent response channel is available which can be used for authenticated time synchronization or delay measurements nor an external tracking device can be used to authenticate the current position of a device. The device must be able to autonomously decide whether it is inside the enabled area

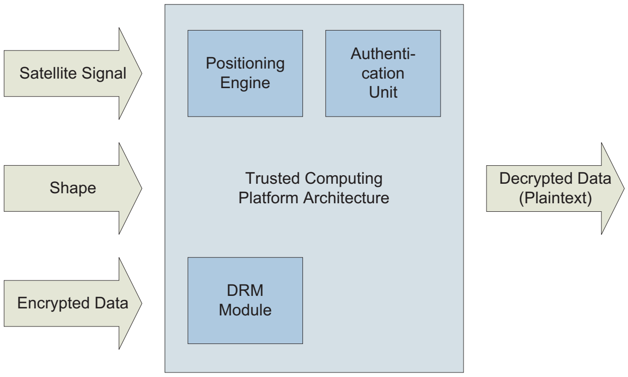

Figure 1. General function of the TCPA chip.

or not. Two attacks are obviously applicable to delude the device.

A highly possible **rerouting attack** against the system works by having a fixed receiver station within the allowed area and to distribute its signal across an entire network as shown in Figure 2.

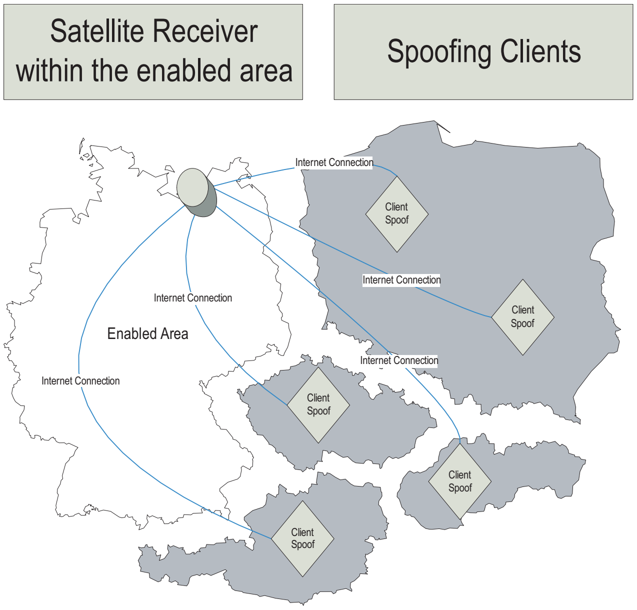

Figure 2. Illegal distribution of non-authenticated satellite signals.

Because the positioning engine is integrated into the TCPA module the fake transmission has to include the entire Galileo spectrum or - more advanced - the integrated signals of all satellites in sight which than can be re-radiated near the receiver. When there is an online connection between receiver and re-transmitter we call this a rerouting attack. When the signals are stored we speak of a replay attack. The main difference between these attacks is the time between receiving and re-transmitting which is in the range of milliseconds for rerouting and in the range of hours for replaying.

A possible countermeasure against this threat is to have a precise clock inside the TCPA package that allows the system to detect time delays of the satellite signal. The satellite signal contains a very precise time information which can be compared with this independent time source in order to detect the redirection of signals. This internal clock must be protected against external manipulation. The clock has to be integrated into the device since there is no constantly usable response channel for synchronization with external time sources. As analyzed in this paper in section 2 current state-of-the-art clocks have a typical error of less than 15 seconds per year. Assuming that an internet connection is used to distribute the satellite signal there will be a delay of at least 5 milliseconds caused by active network components. An ISDN connection would generate at least the same latency values. Connections with less latency will be much more expensive and require a dedicated leased line. They are practically impossible. Assuming the clock error of 15 seconds per year - which is a reasonable value for inexpensive quartz driven clocks as shown in the last section - the clock will pickup an error of 5 milliseconds in about 3 hours time. This means the clock has to be synchronized every 3 hours in order to enable detection of rerouting attacks.

This time can be further increased when the clock drift is known and constant and can be calculated in advance. Each time the clock is synchronized with an external source the drift can be determined and stored inside the chipset.

The rerouting attack could be improved - seen from the attacker's point of view - by manipulating the timestamps of the satellite signal before it is re-radiated at the receivers site. This would imply the need for full decoding of signals. Galileo for instance includes signed timestamps. An anti spoofing mechanism is also included in current GPS signals for governmental purposes. Signed timestamps make it possible to detect every kind of manipulations executed by the attacker to conceal delays caused by rerouting attacks.

The internal clock inside the device itself can only be set up in a trusted environment. This prevents it from being manipulated Algorithms to perform authenticated time synchronization are described in section 2. The time between mandatory time synchronization depends on the precision of the clock. It is impossible to use a data stream such as a TV program for time synchronization since the data signal is subject to the same rerouting attack. A dial in connection can be used for that purpose. When the device fails to synchronize time for a grace period it will disable access to the

DRM protected material.

A **replay attack** can be performed very similar. The satellite signals will be recorded at a position inside the shape. Later the signals can be broadcasted at every other location. This fraud can be fought by the same methods as against the rerouting attack.

Another threat regards the use of **simulated satellites**. This can relatively easily be solved when the positioning signal is signed itself. Galileo will use public key cryptography for this purpose. So called ”certified receivers” will be able to check the digital signature. For GPS this is currently only available for governmental users.

The Galileo system will be secured against manipulation of the satellites which might another threat - although very unlikely.

The transmitted shape data which define the area where the DRM protected material is accessible inside can be protected by signing them with a private key and thus using public key cryptography.

3.3. Risk estimation

The purpose of every cryptographic process is to raise the costs for breaking into a system well above the price of the data to be protected. The costs for a rerouting attack comprises of the following:

- Costs for the data connection (either analogue or digital)
- Costs for the reference receiver (including A/D converter when using a digital connection)
- Costs for the transmitter which re-radiates the signal

We estimate the overall costs of about 1000 EUR or less. This is very inexpensive compared with the possible result. Therefore the proposed architecture must reflect this and increase security significantly. We do not currently see a method to attack the system except assaulting the cryptographic parts. Increasing cryptographic security is beyond the scope of this paper.

3.4. Data flows and data formats

The following data is relevant for the function of the location based DRM system:

- The system receives the **copyrighted material** or already contains it on storage media.
- The location is provided by a **satellite signal**.
- Furthermore the **shape information** is necessary for the DRM system to decide where it enables access to the copyrighted material.

The copyrighted material is encrypted. The key will be generated by the DRM system when access is granted. The format is defined by the copyright holder. As the TCPA chipset is a trusted device of the copyright holder it can either contain a general key or a user-dependent key. In the latter case the protected material can be encrypted in a way that it can be decrypted by several keys [7].

The satellite signal does not have to be encrypted but has to be signed to prevent the signal from being manipulated or faked by an attacker. The TCPA device must be able to decide whether the signal is a genuine location provider for the relevant kind of copyrighted material. The inherent timestamps will also be authenticated by signing the entire data. This is necessary as shown above to prevent rerouting attacks.

Shape information has to be signed as well but does not have to be encrypted. This prevents them from being manipulated. Manipulation of shape data will obviously result in the total ineffectiveness of the entire system.

4. First realization of the concept

In order to show the feasibility of our approach we have implemented a prototype on a Linux driven TV satellite receiver [2] with an in-built harddisk.

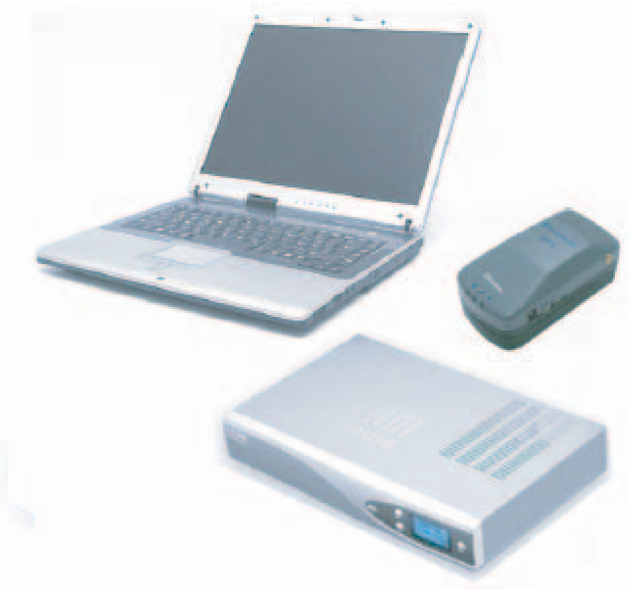

Figure 3. Prototype. The notebook emulates a connection with arbitrary delays.

We have implemented an AES [5] decryption on the set top box itself. Key generation is performed on the Linux receiver as well. In the first implementation we are using a high end GPS received connected via a native serial protocol to a notebook PC. Traditional methods to connect the GPS receiver such as NMEA [12] are unfeasible since NMEA sentences are sent asynchronously by the GPS receiver and the time provided within NMEA is only precise in the second. The notebook signs the data stream using SHA-1 [4] and can be set to delay all messages in order to simulate a rerouting attack. The satellite receiver contains a precise and independent clock. The receiver determines whether the location is authentic. In this case the key to decrypt the file on the harddisk is provided to the Access Module.

Shape information is provided in form of an XML file which contains the corners of the enabled area as geographical coordinates. The file is digitally signed. The public key to check this signature is stored on the smart card. A public key infrastructure which allows a better distribution of keys is to be implemented soon.

This implementation allowed us to verify the general design. The system is working well as software. The time between two re-synchronization cycles depends very much on the accuracy of the in-built timer. With our device exemplar re-synchronization was needed every five hours. Since software can be easily manipulated a hardware chipset is currently in the process of design and will be available at the beginning of 2005.

5. Conclusions and further research

We have introduced our idea of authenticated positioning used for location based Digital Rights Management. The system dramatically increases the efforts needed to break the DRM system. For home usage scenarios it is very secure. The limitation is that short delays in the satellite signal must be detected. This requires precise clocks. The clock must be more exact when delays become shorter. For our calculations we have chosen 5 milliseconds as a reasonable time. Shorter allowed delays would require more precise clocks or shorter re-synchronization cycles.

Since the concept and system described in this paper works with satellite navigation which is not necessarily available indoors we are researching on a solution based upon a different location providers. Currently location providers using Bayesian methods to determine the most likely position according to received signal strengths of stationary nodes in a Wireless LAN [15] seem to be most useful for indoor location. A concept has been finished, a prototype for this approach is in the process of final development.

References

[1] RC4 License. A general introduction is availble at http://en.wikipedia.org/wiki/RC4.

[2] Dream multimedia. ”http://www.dream-multimedia-tv.de/”, 2004.

[3] T. Barr. *Invitation to Cryptology*. Prentice Hall, Upper Saddle River (NJ), 2002.

[4] D. Eastlake, 3rd. RFC 3174: US Secure Hash Algorithm 1 (SHA1), 2001.

[5] J. Daemen and V. Rijmen. *The Design of Rijndael. The Wide Trail Strategy (Information Security and Cryptography)*. Springer, Heidelberg, 2001.

[6] J. Feigenbaum. *Security and Privacy in Digital Rights Management*. Springer, Heidelberg, 2003.

[7] N. Ferguson and B. Schneier. *Practical Cryptography*. John Wiley and Sons, New York, 2003.

[8] G. W. Hein, J. Godet, J.-L. Issler, J.-C. Martin, P. Erhard, R. Lucas-Rodriguez, and T. Pratt. Status of galileo frequency and signal design, 2002. http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_stf_ion2002.pdf.

[9] E. D. Kaplan. *Understanding GPS: Principles and Applications*. Artech House Publishers, Norwood, 1996.

[10] J. Kelsey, B. Schneier, and C. Hall. An authenticated camera. In *Proc. of the 12th Annual Computer Society Applications Conference (ACSAC)*. ACM Press, december 1996.

[11] M. Ljubich. *Methods for Enhancing the Security of Java Card based Payment Protocols*. PhD thesis, University of Rostock, Rostock, Germany, 2004.

[12] National Marine Electronics Association. Nmea 0183 interface standard, 2002.

[13] O. Onidi. Galileo is launched, 2002. http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_is_launched.pdf.

[14] U. Reimers. *Digital Video Broadcasting (DVB). The International Standard for Digital Television*. Springer, Heidelberg, 2000.

[15] T. Roos, P. Myllymaki, H. Tirri, P. Misikangas, and J. Sievanen. A probabilistic approach to wlan user location estimation. *International Journal of Wireless Information Networks*, 9, 2002.

[16] K. Shimada. Patent US 5,922,073: System and method for controlling access to subject data using location data associated with the subject data and a requesting device, 1999.

[17] The European Commission. Mission high level definition, 2002. http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_hld_v3_23_09_02.pdf.

[18] J. R. Vig. Introduction to quartz frequency standards. Technical report, Army Research Laboratory, Oct. 2002.

[19] W. Rosenblatt et.al. *Digital Rights Management: Business and Technology*. John Wiley and Sons, New York, 2001.

[20] J. S. Warner and R. G. Johnston. GPS Spoofing Countermeasures. http://www.homelandsecurity.org/bulletin/Dual Benefit/warner_gps_spoofing.html, 2003.