Digital Rights Management on an IP-based set-top box

by
Erik Hallbäck

LITH-ISY-EX--05/3824--SE

19th December 2005

Digital Rights Management on an IP-based set-top box

by **Erik Hallbäck**

LITH-ISY-EX--05/3824--SE

Supervisor : **Henrik Carlsson**

Examiner : **Viiveke Fåk**
Dept. of Electrical Engineering
at Linköpings universitet

Avdelning, Institution
Division, Department

ISY,
Dept. of Electrical Engineering
581 83 LINKÖPING

LINKÖPINGS UNIVERSITET

Datum
Date

19th December 2005

Språk
Language

☐ Svenska/Swedish
☒ Engelska/English
☐ _____

Rapporttyp
Report category

☐ Licentiatavhandling
☒ Examensarbete
☐ C-uppsats
☐ D-uppsats
☐ Övrig rapport
☐ _____

ISBN
—

ISRN
LITH-ISY-EX--05/3824--SE

Serietitel och serienummer **ISSN**
Title of series, numbering —

URL för elektronisk version
http://www.ep.liu.se/exjobb/isy/2005/dd-d/3824/

Titel Digital Rights Managemnet för en IP-baserad set-top box

Title Digital Rights Management on an IP-based set-top box

Författare Erik Hallbäck
Author

Sammanfattning
Abstract

Digital Rights Management (DRM) is a technology that allows service and content providers to distribute and sell digital content in a secure way. The content is encrypted and packaged with a license that is enforced before playback is allowed.

This thesis covers how a DRM system works and gives some cryptographic background. It also shows how Microsoft DRM for Network Devices can be implemented on an ip-based set-top box.

Nyckelord
Keywords Digital Rights Management, DRM, content protection

Abstract

Digital Rights Management (DRM) is a technology that allows service and content providers to distribute and sell digital content in a secure way. The content is encrypted and packaged with a license that is enforced before playback is allowed.

This thesis covers how a DRM system works and gives some cryptographic background. It also shows how Microsoft DRM for Network Devices can be implemented on an ip-based set-top box.

Keywords : Digital Rights Management, DRM, content protection

Contents

Chapter 1

Introduction

> "Anyone can come up with a security system so clever that he can't see its flaws."
>
> – Schneiers Law

This chapter gives a background to DRM, The goal and limitations is also presented here.

1.1 Background

In the wake of Napster and other music sharing networks there is an emerging market for music stores on the Internet that sell downloadable music. The industry has understood that in order to sell music they need to make the music accessible to the public in a way that is competible with pirated music. Still they want to remain in control of how it is used. The content is served encrypted and it is actually the key together with a license that specifies how the content may be used, that is sold. The intention with this protection is to discourage file sharing between friends and on the Internet. This system has come to be known as Digital Rights Management, or simply the three letter acronym DRM.

On the contrary to Schneiers Law the flaws in DRM are well known and this is also where the challenge is: to make a system usable and hard to break, and once it's broken - easy to patch.

1.2 Problem

Today there is a lot of protected content on the market that the set-top box can't play. This is a problem, but also an opportunity to make more content availible to the users.

The purpose of this thesis is to investigate and compare the DRM systems used today comparing their usage, weaknesses, strengths and relevance for an IP based set-top box.

The thesis shall also include a prototype implementation of a DRM system to be able to show access to commercially available content on the set-top box.

1.3 Limitations

The time for this thesis is limited to 20 weeks and makes a limitation for the work that is to be done. Furthermore since this is quite a new and fast developing technology, there are just a few books yet on the subject (actually I've found two, where the second one turned out to be lecture notes). This makes the sources limited to material found on the Internet. It hasn't been hard to find information but pretty much all information is biased in one way or another since this is a rather controversial subject right now.

1.4 Outline

Introduction This chapter gives an introduction both to the thesis subject and to the report.

Background This chapter presents the problem background and the threats digital content faces today.

Solutions This chapter presents different solutions to the problem given in the background chapter.

DRM This chapter describes the mechanisms of DRM and how the different systems work. It also gives an overview of the security and attacks for extracting the protected content.

REL This chapter describes how a Rights Expression Language works and presents the most commons ones.

Cryptography This chapter describes a few ciphers that are used in DRM systems today.

Implementation In this chapter I describe how the Microsoft Windows Media DRM 10 for Network Devices work and how I got it to work on the set-top box .

Discussion This chapter summarizes the work in this thesis.

Future Work This chapter presents some ideas on what can be done in the future.

1.5 Reading guide

To get a quick understanding for the problem and what possible solutions that exists read chapter two and three. To get a deeper understanding of what DRM is, read chapter four. Chapter six deals with the cryptographic parts that can be found in a DRM system today. To get more technical details and understand how the implementation on the set-top box was done, read chapter seven. Chapter eight and nine summarizes the work and gives a glance at the future.

1.6 Glossary

AES Advanced Encryption Standard is a symmetric block cipher

ASF Advanced Streaming Format is Microsoft's proprietary digital audio/digital video container format, especially meant for streaming media.

API Application Programming Interface is a set of definitions of the ways one piece of computer software communicates with another

ASCII American Standard Code for Information Interchange is a character set and a character encoding based on the Roman alphabet as used in modern English.

Base64 is a data encoding scheme used to represent binary data as 7-bit ASCII characters.

Bittorrent is a peer-to-peer file distribution tool where all connected computers share downloaded bits among themselves in a controlled way to relieve pressure on the initial source.

DES Data Encryption Standard is a symmetric cipher. It became a federal US non-military standard for use on all unclassified data in 1976.

Digital signature is a non-forgeable transformation of data that enables proof of the source (with non-repudiation) and verification of the integrity of that data. Digital signatures are usually created using a public-key algorithm.

DMR Digital Media Receiver may be a computer, but it looks and behaves like an easy-to-use consumer electronics appliance and is usually used to play music and movies in the living room.

DRM Digital Rights Management is an umbrella term referring to any of several technical methods used to control or restrict the use of digital media content on electronic devices with such technologies installed.

DVB Digital Video Broadcasting is a suite of internationally accepted, open standards for digital television maintained by the DVB Project

DVI Digital Visual Interface or Digital Video Interface is a video connector designed to maximize the visual quality of digital display devices such as flat panel LCD computer displays and digital projectors.

ECC Elliptic Curve Cryptography is an approach to public-key cryptography based on the mathematics of elliptic curves. The main benefit of ECC is that under certain situations it uses smaller keys than other methods, such as RSA, while providing an equivalent or higher level of security.

H.263 is a low-bitrate video codec for videoconferencing.

HDMI High-Definition Multimedia Interface is a digital interface for connecting compatible devices such as set-top boxes, DVD players to digital audio and/or video monitor.

HMA Home Media Access is a service in the set-top box that allows the box to access content on a PC in the home network.

IP-STB means IP-based set-top box, it's a regular set-top box but receives its content on the network interface.

MD5 Message Digest algorithm 5 is a widely used cryptographic hash function.

OMA Open Mobile Alliance is a standards body which develops open standards for the mobile industry.

PVR Personal Video Recorder is a consumer electronics device or a functionality in a set-top box with wich TV programs can be recorded to a harddrive.

spoofing A spoofing attack, in computer security terms, refers to a situation in which one person or program is able to masquerade successfully as another.

UPnP Universal Plug and Play is a protocol to allow devices to connect seamlessly and to simplify the implementation of networks in the home.

WMC Windows Media Connect is a media server that can share files with DMR's and IP-STB's (see 7.2 for more details).

Chapter 2

Background

> "Digital files cannot be made uncopyable, any more than water can be made not wet."
>
> – Bruce Schneier

This chapter gives the background to why DRM was invented. It also presents the basic threats to digital content from a content owners perspective.

2.1 Problem background

Back in the days when monks dedicated their lives to copy books, copyright was not a big issue. A lot has changed since then. Today almost all media are digital and can be copied without sweat. This has led to a war between the content owners and the pirates.

2.1.1 Why is this problem greater now than ever before?

In modern times[1] illegal copying has been kept at a tolerable level by a combination of law enforcement, distribution problems and the fact that analog copies usually have a lower quality than the original. Today Internet and high-speed connections has solved the distribution problem and digital content leaves a perfect copy.

2.2 Threats

There are two basic threats to digital content in the eyes of the content owner that I have identified:

1. content is spread in an uncontrolled manner
2. unauthorized users access content

The *first* threat can be a movie that is made availible through a bittorrent tracker or a rip of a DVD passed between friends. An example of the *second* threat is a programmable smart card (see figure 2.1) with the keys to the Canal+ channel.

Most of the time the second threat is a consequence of the first threat, since the fact that content is spread in an uncontrolled manner directly leads to the fact that unauthorized users get access to the content. But the second threat can also be isolated like in the example given above with the programmable smart card.

In the next chapter I will describe the different solutions that are used to deal with these two threats.

[1] By this I refer to the time before the Internet got into every household. Remember, it has only been a little more than ten years ago since Netscape Navigator 1.0 was released.

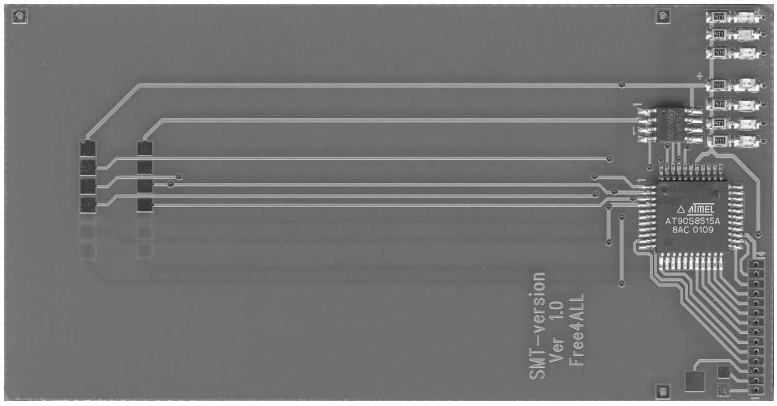

Figure 2.1: Funcard with a programmable microprocessor used to decrypt scrambled TV broadcasts without paying

Chapter 3

Solutions

> "Any solution to a problem changes the problem."
>
> – R. W. Johnson

This chapter presents different solutions to the threats in chapter 2.

3.1 Protection schemes

Different media require different types of protection. There are a few basic ways for protection and then there are a lot of variants and implementations of these.

3.1.1 Conditional access (CA)

Conditional access is used for protection of TV broadcasts. The idea is to encrypt the stream and send session keys encrypted with a master key (that is hidden on a smart card or in the set-top box). The implementations differ mostly in the key management. Some systems use smart cards while others are software only. This is the only system of the ones described here that deals solely with prevention of unauhthorized users gaining access to content. [1]

3.1.2 Digital fingerprinting

In digital fingerprinting you make each copy differ slightly while you keep the content the same throughout the copies. Distributed copies can thus be connected to the person who bought the legal copy from which the illegal copy was made.

This will deter users from making illegal copies, since if they spread the copy to somebody else, they will lose control over it, and it is possible that the copy will arrive at somebody who will identify and prosecute the user for creating and spreading the copy. Thus the greater risk of being identified ought to make it less popular to spread illegal copies. Fingerprinting only makes it possible to tell the copies apart, a database is needed to connect the different copies to the buyers. [2]

3.1.3 Digital watermarking

Digital watermarks are used to add invisible markers to the media. This is achieved by spreading out the bits representing the watermark throughout the file in a way that they cannot be identified and manipulated. It's possible to add the name of the buyer as a watermark, allowing the system to be stand alone i.e. not needing a central database. [3]

3.1.4 Macrovision

Macrovision is a company that creates electronic copy protection schemes. A scheme that has become synonymous with the name of the company that fools most off-the-shelf VCRs has been out for many years now. The protection works like this: a signal is implanted within the offscreen range that does not display on the TV. The automatic tracking in the VCR "feels" these signals and tries to compensate for the strong variation in the brightness and makes the picture unwatchable. This protection scheme has the effect that when a motion picture is seen on a TV, the picture is good, once it is recorded onto a video tape, that video tape is unwatchable. This scheme is implemented in many devices as a small chip that adds these signals in realtime. [3]

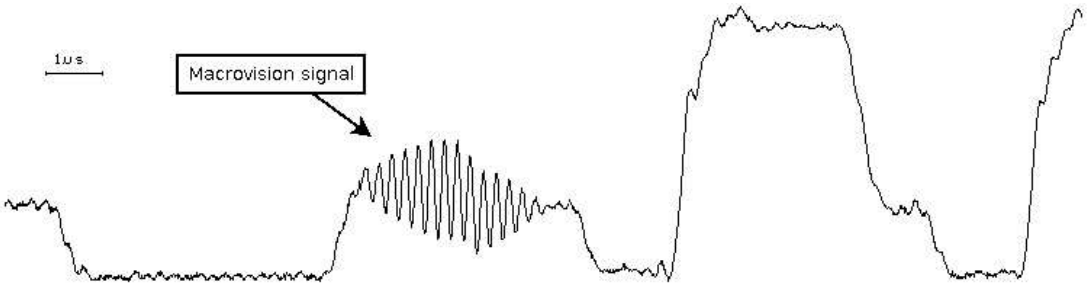

Figure 3.1: Example of what the signal looks like with Macrovision protection.

3.1.5 High-bandwidth Digital Content Protection (HDCP)

HDCP is a specification developed by Intel Corporation to protect digital entertainment content across the DVI/HDMI interface. This is to protect the valuable high resolution digital content from being intercepted on it's way to the presentation device. The content is encrypted before entering the possibly insecure link to the presentation device and then decrypted before presentation (see figure 3.2). [4]

3.1.6 Digital Rights Management (DRM)

This is the technology I will focus on in this thesis

Today everybody talks about DRM, Digital Rights Management or Digital Restrictions Management depending on who you ask.

DRM is a technology that lets content owners safely distribute and sell their content online. Everything that can be represented in a digital form such as audio, video, publications and software can be protected with DRM. It is also possible for the content owners to specify rules for how the content can be used: you can play this song once, you can watch this rented video during 24 hours, you can put this song on portable media and so on.

There is a mature and robust cryptographic theory that can be applied to the problem of securely delivering the digital content. Unfortunately

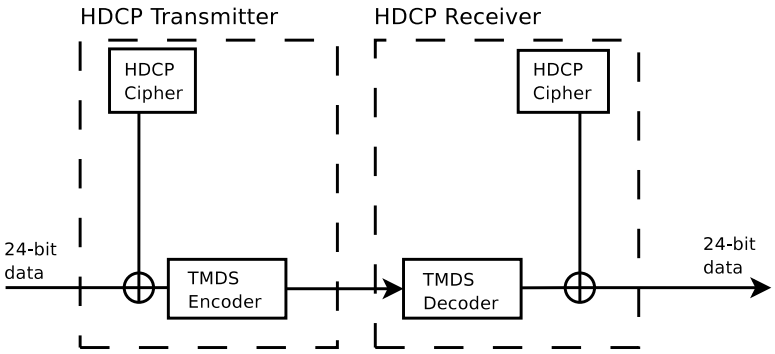

Figure 3.2: HDCP encoding and decoding. TMDS or Transition Minimized Differential Signaling is a technology for transmitting high speed serial data.

there is no comparable theory currently availible for the DRM problem.

The difference from traditional security models is that in DRM, the user is not trusted. How do you send content to someone who you can't trust and make him obey the rules that you specify for this content?

The solution DRM offers to this question is to give the user a "black box" which he has no control over. This box takes the encrypted content, the key and the rules as input and puts out the content in a way that makes it hard for the user to grab. The trend here is to decrypt the content as close to the user as possible because it minimizes the possibilites to get access to the valuable digital content. HDCP (see 3.1.5) is a technology that can be used here. [5]

DRM process

A simple view on the DRM process from the content owners servers to the set-top box can be seen in figure 3.3.

Content distribution server

This server is controlled by the content owner, it stores all media and allows it to be downloaded by the set-top box .

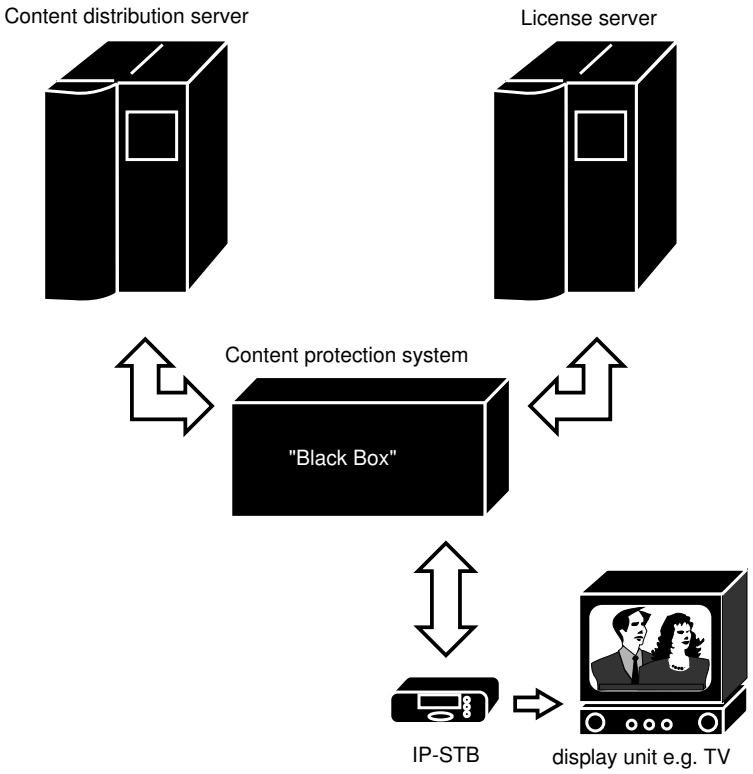

Figure 3.3: A DRM system basically has four software components: content protection software, a content distribution server, a license server and a display unit. The "black box" is actually an application that runs inside the IP-STB.

License server

This server issues licenses for the content on the distribution server. The technical parts will be covered in the next chapter.

Chapter 4

Digital Rights Management

> DRM is acceptable when it's just strong enough to remind you that this isn't freely redistributable content, but not strong enough to actually prevent you from breaking it when you need to. [...] That's why Apple's DRM works. Because it doesn't. If it did, it wouldn't.
>
> – Peter da Silva

This chapter describes the mechanisms of DRM and how the different systems work. It also gives an overview of the security and attacks for extracting the protected content.

4.1 DRM systems

There are several implementations on the market today. Some are specialized in a niche market, like OMA version 1.0 which is only for celluluar phones. Others systems, like Microsoft DRM is intended to work in many fields.

4.1.1 MPEG-21

The MPEG-21 Multimedia Framework is a work in progress by MPEG. Its aim is to enable transparent and extended use of multimedia resources. The framework is based on two essential concepts: the definition of a fundamental unit of distribution and transaction (the Digital Item) and the concept of users interacting with Digital Items. The file format for MP21 will inherit several concepts from MP4 in order to allow a mixed combination of video, audio, graphics and text. There is some reference software for creating and interpreting licenses but the framework is far from mature. There has not been much noise from this project for a long time now. [6],[7]

4.1.2 Microsoft Windows Media DRM 10 for Network Devices

DRM for Network Devices is Microsofts contribution for protecting content in home networks. It allows devices such as set-top boxes and media players to render Windows Media DRM-protected content over a network from a personal computer running Windows XP.

4.1.3 Difference between Portable and Network Devices

There are two systems besides the full implementation of Microsoft DRM, DRM for Portables and DRM for Network Devices. Microsoft DRM for Network Devices does not implement license storage. A device with this DRM system requests a license for every media file it plays and doesn't cache any licenses. It does not need to store licenses because it is always connected to the network and to a computer running Windows Media Connect[1]. DRM for Portable Devices is usually unplugged from the network when in use, typically a portable music player has this system implemented. Portable device licenses have a metered play count and like Network Devices it does not allow content to be copied or edited.

[1] Media server see 7.2

4.1.4 Inside Microsoft DRM

It is interesting to know a little about whats going on inside a DRM system and how the files are protected to discourage crackers from reaching the data.

Thanks to "Beale Screamer"[8] we know a bit about what is going on inside Microsofts DRM. Though this only applies to the older DRM version 2 and only to audio files (.wma) it is still very interesting to see the inner life of a DRM system.

Microsoft DRMv2 uses several cryptographic algorithms for protection of the media, some are standard like DES as a block cipher, RC4 as a stream cipher and SHA-1 as a hash algorithm. Elliptic curves (ECC) are used as a public key cryptosystem and a slightly modified version of Base64 is used as well as their own keyed hash function known as MultiSwap.

The media files are encrypted with a content key. The file is divided in packets and each packet is individually encrypted to allow random access i.e. searching in files. The header of the file contains a DRMV2-object which in turn contains a KID element (Key ID). This element specifies which key to use when deciphering.

When a file is played the DRM first checks if there is a local license with a matching KID. If not, a challenge is sent to a license server. The challenge consists of two ECC points as the session key and a unique "client-id". The response is an XML-encoded license if the challenge is accepted. It is RC4-encrypted with the session key in the challenge. This license contains the key that is used to decrypt the protected file.

4.1.5 Helix DNA

Real Networks are building a DRM solution together with independent developers and other companies which they are licensing under different open source licenses. The platform consists of a producer, a server and a player. The producer converts audio and video into streams that are streamed by the server to the player. [9]

4.1.6 OMA DRM

The Open Mobile Alliance was formed in 2002 to be the center of mobile service enabler specification work, helping the creation of interoperable services across countries, operators and mobile terminals.

One important task has been to specify a standard for DRM on mobile devices so that the operators and content providers can make digital content availible to consumers in a controlled manner.

This is interesting to investigate from a set-top box perspective since the cell phones are getting more and more advanced and the displays are not far away from resolutions comparable to a TV.

The primary target that we can see today is games, applications and music. The set-top box has a similar hardware configuration with a simple input device, the remote, a screen, the TV and good connectivity to the Internet. The set-top box could hence be used as the media device newer cell phones are used as today and take advantage of the rich range of games and music availible.

OMA-DRM v1.0

OMA DRM 1.0 can be used to protect any media object that has a MIME content type defined for it. The standard was designed for low-cost devices with not much memory and no trusted system clocks. It is suitable to protect content like ringtones and wallpapers on cell phones.

The specification consists of three parts

- Forward-lock
- Combined delivery
- Separate delivery

In the case of a simple forward-lock an additional HTTP header is applied to the object:

```
Content-type: application/vnd.oma.drm.message; boundary=boundary-1
Content-Length: 574
–boundary-1
Content-type: image/jpeg
Content-Transfer-Encoding: binary
...jpeg image in binary format...
–boundary-1–
```

The combined and separate delivery are more complex and allows for a rights object to be sent with the media. The rights object specifies what the user can do with the media. The difference between combined and separate delivery is how the rights object is sent. The separete delivery is used when a dedicated DRM agent in the device (a harder to spoof SMS client) is used to pick up the rights object. In combined delivery the content is sent together with the rights object and looks something like this:

```
Content-type: application/vnd.oma.drm.message;boundary=boundary-1
Content-Length: 893
–boundary-1
Content-type: application/vnd.oma.drm.rights+xml
Content-Transfer-Encoding: binary
<o-ex:rights xmlns:o-ex=”http://odrl.net/1.1/ODRL-EX”
xmlns:o-dd=”http://odrl.net/1.1/ODRL-DD” >
<o-ex:context>
<o-dd:version>1.0</o-dd:version>
</o-ex:context>
<o-ex:agreement>
<o-ex:asset>
<o-ex:context>
<o-dd:uid>cid:4567829547@foo.com</o-dd:uid>
</o-ex:context>
</o-ex:asset>
<o-ex:permission>
<o-dd:play/>
</o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
–boundary-1
Content-type: image/jpeg
Content-ID: <45678929547@foo.bar>
Content-Transfer-Encoding: binary
...jpeg image in binary format...
–boundary-1–
```

This is a rights object for a JPEG file. The XML defines the rights for the included file.

Separate delivery is used for superdistribution (see 4.2). For example when you send a wallpaper to your friend, he requests the rights object after receiving the content.

This standard is good to know about because it may be used to protect content such as mobile games and backgrounds. [10]

OMA DRM v2.0

While the main target of OMA v1.0 is mobile phones, v2.0 is broader and can be used on a PC or a set-top box.

A content provider will never trust a device that *says* it is OMA DRM 2.0-compliant. There has to be a control organ that certifies each implementation and makes sure that it does what it is supposed to do, nothing more and nothing less. An organ that all content providers can trust with their valuable content. Content Management License Administrator or CMLA for short is a consortium made up of Intel, Nokia, Samsung, Toshiba and Matshushita. It's primary task is to establish key and digital certificate distribution services, compliance rules and testing tools for vendors to use to ensure that their devices are trustworthy, and legal backstops for devices that are either noncompliant or hacked. [11]

4.1.7 iTunes

iTunes is Apples way of selling music through their musicstore. Everything is tightly integrated with the musicplayer iPod. The music is packaged in AAC format (Advanced Audio Codec). It is based on MPEG4 compression and allows compression of multichannel audio such as surround sound. On top of this they have their own DRM protection, FairPlay, that is added to the file after the file is paid for and downloaded. Apple haven't let anyone license this technology, so for now it's impossible to implement this system on the set-top box .

FairPlay

The audio stream in a FairPlay protected file is encrypted with AES[2] in combination with MD5[3] hashes. The key used to encrypt the stream is encrypted with a user key. Apple keeps track of every user and what keys they have (one key for every downloaded iTune). An iTune can be downloaded to an iPod and recorded to a CD any number of times. The protection is lost when transfered to a CD and it is thus possible to reconvert to mp3 but this will aggravate the sound artifacts of encoding since the resulting file will have been encoded twice.

When a new computer is authorized to the music store, iTunes sends a unique machine identifier to Apple's servers. This identifier is derived from

[2] cryptofunction, see 6.1.3
[3] cryptographic hash function, see 6.1.4

four factors: the serial number of the C: drive, the system BIOS version, the CPU name and the Windows Product ID or the equivalent in a Macintosh environment. A user are allowed to have five computers authorized at the same time. You can also deauthorize a computer whereas iTunes removes all keys from it's encrypted repository and instructs Apple's servers to remove the machine identifier from their database. This is a far more user friendly solution than the system CDON.com offers. Their system is based on Microsoft DRM and you are only allowed to download the license three times, period. [3], [12],

4.2 Superdistribution

Superdistribution is an effect that comes with DRM. It means that the consumer is allowed and even encouraged to share downloaded content with friends. When sent to a friend he too must pay for a license to use the content (see figure 4.1). The consumers actually help the content owners to distribute the content. Many systems support this feature.

4.3 DRM on a set-top box

Digital TV consumers do not only want to watch what is currently on TV, they also want to rent movies online. This is called Video-on-Demand or VoD for short. When payment is registered the movie, protected with DRM, is sent to the box and playback is initiated. The rules in the license determines what the user can and cannot do.

There are also a lot of games and applications developed for mobile devices such as cell phones and PDAs availible. These devices have similar hardware to the set-top box. Modern cell phones are equipped with DRM systems that prevent users from sharing purchased software with friends or on the Internet. A set-top box that wants to be able to run these applications also needs to understand the DRM systems they use.

The implementation that I describe in chapter 7 is for music only and allows a user do buy a song from an Internet music shop that sells music protected with Microsoft DRM 10 (for example CDON.com). After

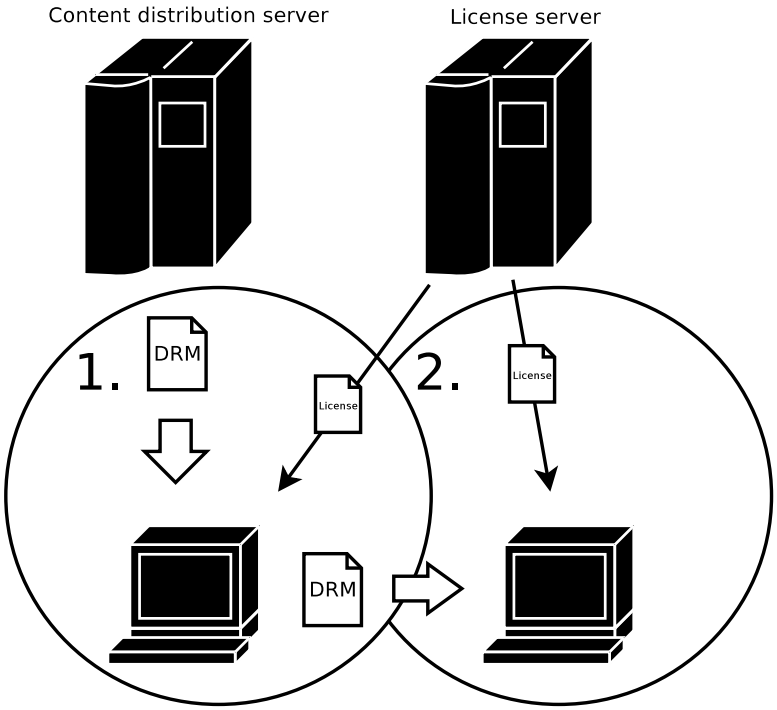

Figure 4.1: Content and license is downloaded to computer 1, then the content is shared with computer 2 wich have to get the license too.

downloading the song to his computer he shares it with Windows Media Connect, and he can play it on his IP-STB (see figure 4.2).

4.4 Security overview

4.4.1 End-to-end security

Every link in the delivery chain has to be secured. A weakness will make it easier for an attacker to reach the data that is not encrypted. To minimize the ways to break the chain you need efforts like encrypting communication between libraries, storing secret keys in linked lists to ensure the key as a whole is not in contiguous memory and even encrypting the communication over the digital link between the computer and the monitor.

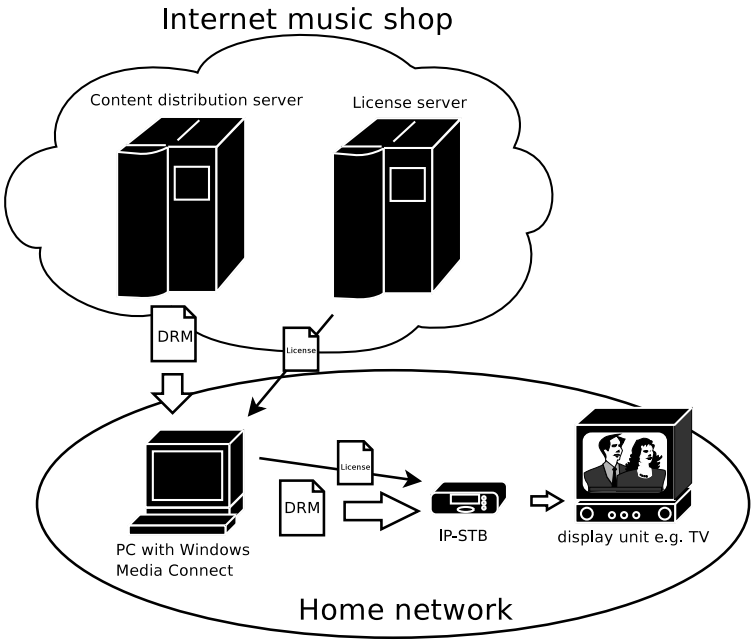

Figure 4.2: Content and license is downloaded to computer and shared with Windows Media Connect. The IP-STB downloads content and license from the PC.

There will of course always be weaknesses at the very end of the chain, where the data is analog in order to interface with us humans. The content owners reason that it's not much to do here and since the data deteriorates going from digital to analog, it also loses much of its value.

4.4.2 Attacks on DRM systems

There are different ways to approach attackers depending on their skill and the resources they have. Microsoft and presumably others too divide the attackers in three groups, naive, skilled and professional attackers. The naive attacker is defined as a person with little knowledge of computers. They can for example change the computers clock to fool expiry dates on rented media. The aim here is to stop this kind of attacker. The DRM system checks that the clock is not tampered with. The skilled attacker

is a person with good knowledge of computers and knows how to handle a debugger. The aim here is to make it more difficult and costly for the attacker to break the system. The code is obfuscated and equipped with software tamper resistance. Holding back a professional attacker with a lot of resources is too expensive so the approach here is to minimize the damage. A revocation list is maintained to block out compromised systems.

Trojans in protected media

In some DRM schemes, the header of a DRM protected file contains information about where to get the license for the content. This is a possible security breach because if this URL is not protected by a signed checksum, anyone can change this information. This has been done in a trojan in version 10 of Windows Media Player. This trojan called WmvDown.A changes the URL thus sending the player to a malicious website from where it downloads malware. [13]

4.4.3 Unprotecting content

There are two ways for an attacker to reach the desired result of unprotecting the content.

Decipher encrypted media

This method will produce an identical file to the original that was once protected. If the encryption methods has a weakness or the key is known it is just a matter of decrypting the file.

Recording of encrypted media

This method does not need any weakness in the software to work, a program intercepts the data on the driver level and records it to a new file. This method has the drawback that it isn't completly lossless like the previous method. Another bad thing is that it takes time, because you need to play the media and record it. This has always been a problem for content owners and there are a number of ways to make it more difficult to do this, and of course as many ways to go around these systems.

4.5 How to use a DRM system on an IP-STB

There are a number of ways that a DRM system can be used in a set-top box. It can be used for protecting content that has been recorded by the box. This could be last nights episode of Simpsons that you recorded on a harddrive with the PVR system. The content owner (the cable company in this case) would not be very happy to find this high quality broadcast availible on the Internet without commercials a few hours later.

A second way to use DRM is to make content like music, movie clips and games intended for the cell phone market availible to users on the set-top box. The mobile phone industry has in a short time come up with specifications on how DRM is supposed to work on a mobile phone. This is done through the Open Mobile Alliance that is a collaborative work among many companies. They have already come out with version 2.0 of their OMA DRM (see 4.1.6).

A third way to use a DRM system is for playing protected music that was bought on one of the Internet music stores that has popped up lately. This is the main focus of this thesis, to find a suitable DRM system that allows for protected music to be played on the STB.

4.6 Selecting what system to implement

I compared the DRM systems above and came up with a clear choice, Microsoft DRM for Network Devices. This system was far more mature than the other systems and integrated well with the existing HMA system. Also the content availible for cell phones and mobile devices are not currently supported by the set-top box . At the time of comparision the PVR technology in the set-top box was in the early stages and there was no need to protect recorded content.

If we were not to protect content ourselves, we need to play protected content. All protected music I've come in contact with on the Internet was either protected with Microsoft DRM or iTunes FairPlay.

	MS DRM-ND	Helix DNA	MPEG-21	OMA 2.0	FairPlay
Content available	√			√	√
Stand alone		√	√	√	√
Implementations availible	√	√		√	
Works with HMA	√				

Explanations to the table:
“Content avalible” means that there is commercial content availible to buy.
“Stand alone” means that the system can handle licenses by itself.

4.7 License revocation and exclusion

A license must be issued with support for revocation lists in order for an issuer to revoke a license. This means that the client has to update the revocation list on a regular basis for the license to be valid. The revocation list contains information about licenses that are not valid anymore. An issuer can through this list end a license prematurely. A member of the license chain can only revoke a license from someone further down in the chain. Each member of a license chain can contain its own revocation point. An end-user license, therefore, could require several revocation lists before being deemed valid.

Exclusion is the process of denying a license to a requesting device because it has been identified as being insecure or compromised. Exclusion is enforced and initiated by license issuers.

Chapter 5

Rights Expression Languages

> "Problem is, to prevent unauthorized users from accessing the data, you need to prevent huge number of scenarios where you access the data - many of them quite legal."
>
> – "insightful" writer on slashdot

This chapter describes how a Rights Expression Language works and presents the most common ones.

To describe licenses governing the access to digital content we use a Rights Expression Language or REL for short. This is a formal language that is machine-readable, unambiguous and secure. The basic component of a REL is the rights expression which describes the permissions granted to a user of protected content. Most RELs are based on XML which is a well established W3C[1] standard.

[1] World Wide Web Consortium

5.1 Security

It is important that the rights cannot be changed by just anyone. The issuer therefore digitally signs the rights expressions so that their authenticity and tamper-resistance can be verified. [14]

5.2 XrML

eXtensible rights Markup Language, XrML, provides a universal method for securely specifying and managing rights and conditions associated with all kinds of resources including digital content as well as services. It is defined using the XML Schema recomendation from W3C.

The basic relationship is defined by the XrML assertion "grant". Structurally, an XrML grant consists of the following:

- The **principal** to whom the grant is issued
- The **right** that the grant specifies
- The **resource** that is the direct object of the right verb
- The **condition** that must be met for the right to be exercised

5.3 MPEG-21 REL

MPEG Rights Expression Language

MPEG-REL, formerly known as XrML, has been selected as the basis for the Moving Picture Expert's Group (MPEG) and the Open eBook Forum (OeBF) Rights Expression Language, and has been contributed to the Organization for the Advancement of Structured Information Systems (OASIS) Rights Language Technical Committee.

5.4 ODRL

Open Digital Rights Language. You'll find it everywhere OMA is. ODRL is an XML schema that supports an extensive language and vocabulary

for the expression of terms and conditions over any content including permissions, constraints, obligations, and offers and agreements with rights holders. ODRL is endorsed by the Open Mobile Alliance for its Digital Rights Management specification.

5.5 XMCL

XMCL or eXtensible Media Commerce Language is an open XML-based rights specification language.

5.6 XMR

eXtensible Media Rights is Microsofts REL. Each license has policies with levels that the set-top box needs to meet to be allowed to play the content. There is not a lot of free information about this scheme.

Chapter 6

Cryptography

> "DRM systems are broken in minutes, sometimes days. Rarely, months. It's not because the people who think them up are stupid. It's not because the people who break them are smart. It's not because there's a flaw in the algorithms. At the end of the day, all DRM systems share a common vulnerability: they provide their attackers with ciphertext, the cipher and the key. At this point, the secret isn't a secret anymore."
>
> – Cory Doctorow

This chapter describes a few ciphers that are used in DRM systems today.

6.1 Background

Cryptography is the fundament that DRM rests on. A DRM protected file is an encrypted file. The key to the file is sold together with a license. The quote above by Cory Doctorow is the truth about DRM systems today and this is also where the effort in improving systems is put in.

The cryptographic algorithms are rarely attacked, but always weaknesses in the DRM scheme.

6.1.1 Public key cryptography

Public key cryptography differs from symmetric cryptography in a fundamental way, it uses two keys instead of one. One public key and one private key. Anyone who wants to send a secret message will use the recipients public key to encrypt it. Once encrypted only the recipients private key can decrypt the message. The most common public key algorithm today is RSA. To break RSA such as derive the private key from the public key, an attacker has to factor a large number. This is computationally infeasible with todays technology. [15]

6.1.2 Optimal Asymmetric Encryption Padding (OAEP)

OAEP is a method for encoding messages developed by Mihir Bellare and Phil Rogaway. The technique of encoding a message with OAEP and then encrypting it with RSA is provably secure in the random oracle model. Informally, this means that if hash functions are truly random, then an adversary who can recover such a message must be able to break RSA.

An OAEP encoded message consists of a "masked data" string concatenated with a "masked random number". In the simplest form of OAEP, the masked data is formed by taking the XOR of the plaintext message M and the hash G of a random string r. The masked random number is the XOR of r with the hash H of the masked data. The input to the RSA encryption function is then

$$[M \oplus G(r)] \parallel [r \oplus H(M \oplus G(r))]$$

Often, OAEP is used to encode small items such as keys. There are other variations on OAEP (differing only slightly from the above) that include a feature called "plaintext-awareness". This means that to construct a valid OAEP encoded message, an adversary must know the original plaintext. To accomplish this, the plaintext message M is first padded (for example, with a string of zeroes) before the masked data is formed. [16]

6.1.3 Symmetric ciphers

Symmetric ciphers use one key in opposite to asymmetric (public key) ciphers. This key is used both for encrypting and decrypting. It is usually a lot faster to encrypt and decrypt with a symmetric cipher than with a public key cipher. Symmetric ciphers such as AES are therefore often used to encrypt audio or video streams in DRM systems.

AES

The cryptographic algorithm Rijndael (named after the creators Vincent Rijmen and Joan Daemen) was announced winner in the Global Information Security Competition held by NIST. The winner got the new name AES as in Advanced Encryption Standard and replaced the old Data Encryption Standard (DES) that had been serving as a federal standard since 1976 and no longer offered sufficient protection. AES is a symmetric cipher like DES.

NIST have issued a recommendation where they specify five modes of operation for symmetric key block cipher algorithms. The five modes – the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes can provide data confidentiality. I will describe the two modes ECB and CTR in more detail since I've used them with AES in this thesis.

Electronic Code Book Mode (ECB)

This mode is a very basic mode. Each plaintext is mapped to a specific ciphertext and vice versa, analogous to the assignment of code words in a code book.

$$ECBEncryption: \quad C_j = CIPH_K(P_j) \quad \text{for } j = 1..n \tag{6.1}$$

$$ECBDecryption: \quad P_j = CIPH_K^{-1}(C_j) \quad \text{for } j = 1..n \tag{6.2}$$

Counter Mode (CTR)

AES in counter mode transforms a set of input blocks called counters to a set of output blocks that are XOR'ed with the ciphertext to produce the

plaintext or vice versa. These three equations together with the text below will make things clear.

$$O_j = CIPH_K(T_j) \text{ for } j = 1, 2..n \tag{6.3}$$
$$P_j = C_j \oplus O_j \text{ for } j = 1, 2..n-1 \tag{6.4}$$
$$P_n = C_n \oplus MSB_u(O_n) \tag{6.5}$$

In equation 6.3 the output blocks (O_j) are produced from encrypting a counter (T_j) with the key (K). This output is then exclusive-ORed with the ciphertext (C_j) to produce the plaintext (P_j) as can be seen in equation 6.4. Equation 6.5 just shows how the last block with only u bits is treated (MSB meaning most significant bits). This only occurs if the ciphertext is not evenly divisible by the blocksize.[17]

6.1.4 Hash functions

MD5

MD5 stands for Message-Digest algorithm 5 and is a cryptographic hash function designed by Ronald Rivest in 1991. It creates a 128-bit hash value and is commonly used to check the integrity of files.[3]

Chapter 7

Implementation

"C++: the power, elegance and simplicity of a hand grenade"

– fortune cookie

In this chapter I describe how the Microsoft Windows Media DRM 10 for Network Devices work and how I got it to work on the set-top box .

7.1 Introduction

7.1.1 The IP-STB

The IP-STB is a special designed piece of hardware running a more or less specialized GNU/Linux distribution. On top of a Hardware Abstraction Layer (HAL) applications and services are running. The applications communicate with the services through an API. A schematic overview of the different layers, both software and hardware can be found in figure 7.1. This picture will help me later on when I describe what parts I have modified and added code to.

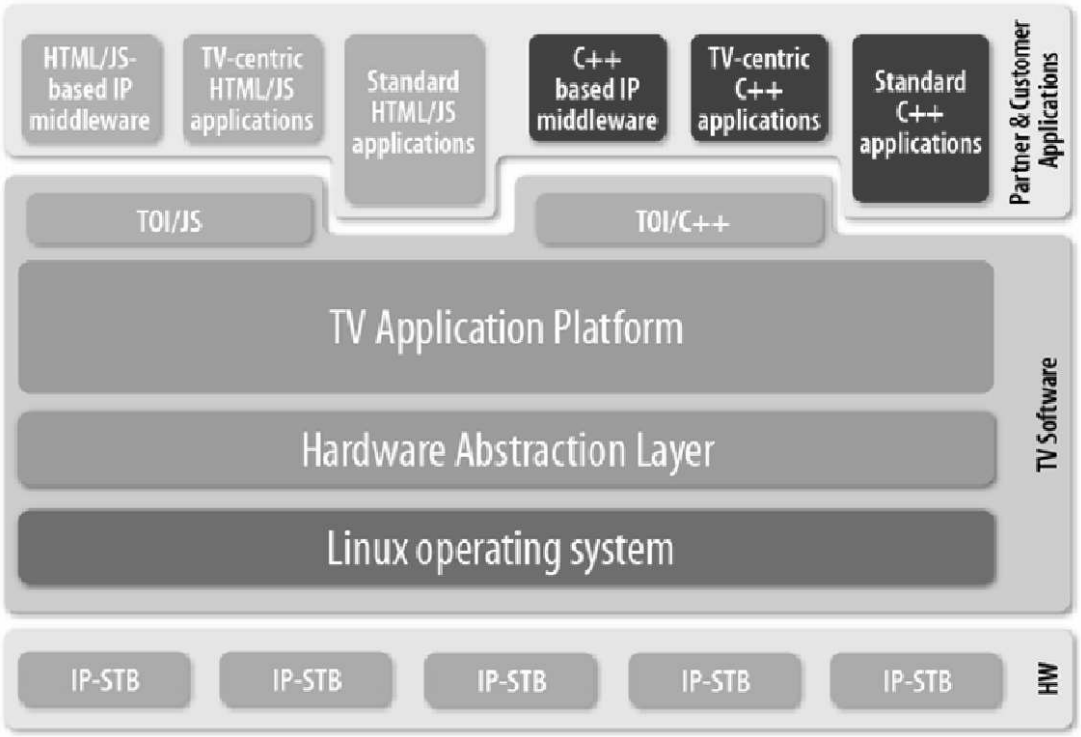

Figure 7.1: Schematic overview of the platform

7.1.2 The first part

The set-top box was already equipped with an application called "Home Media Access" or HMA for short. The presentation part of this application is located in the "TV-centric HTML/JS applications" in figure 7.1, the server part is located in the "TV Application Platform". This application makes a UPnP broadcast to find servers on the network that shares music, movies and pictures. When it finds a server it allows the user to browse the shared files on that server. The server is running a program called Microsoft Windows Media Connect. It is shipped with service pack 2 for Windows XP. HMA was only designed to play content without DRM protection. A part of this thesis work was to make HMA play purchased DRM protected audio files.

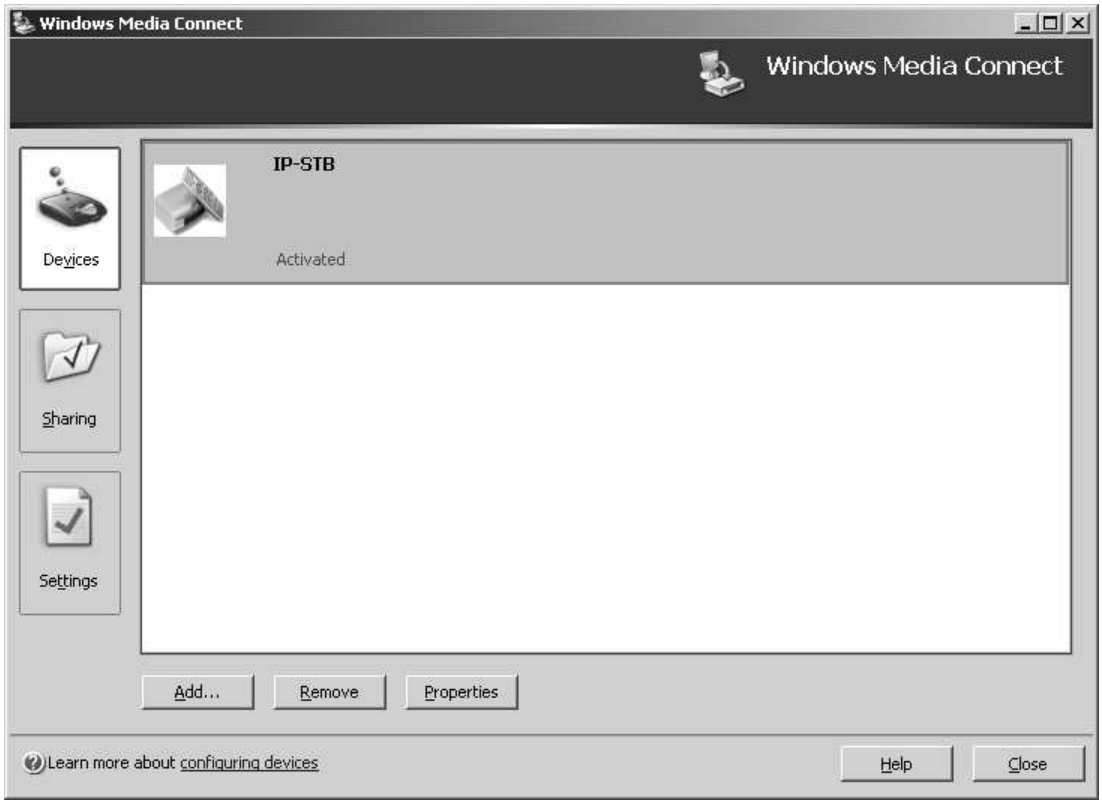

Figure 7.2: Windows Media Connect, mainscreen

7.2 Windows Media Connect

This is the server end of HMA. You can see a screenshot of the user interface in figure 7.2. When a new device is discovered the user is notified by a balloon tip in the Windows UI.

The original behaviour of the HMA was to make a UPnP broadcast to all devices on the network and set up a connection to servers that implemented the "ContentDirectory" service, i.e. servers that share files.

As the first step towards making the DMR able to play protected content I had to write a device description document. This is an XML document that describes the device and the services it provides. This change was necessary because Microsoft has added some tags that Windows Media

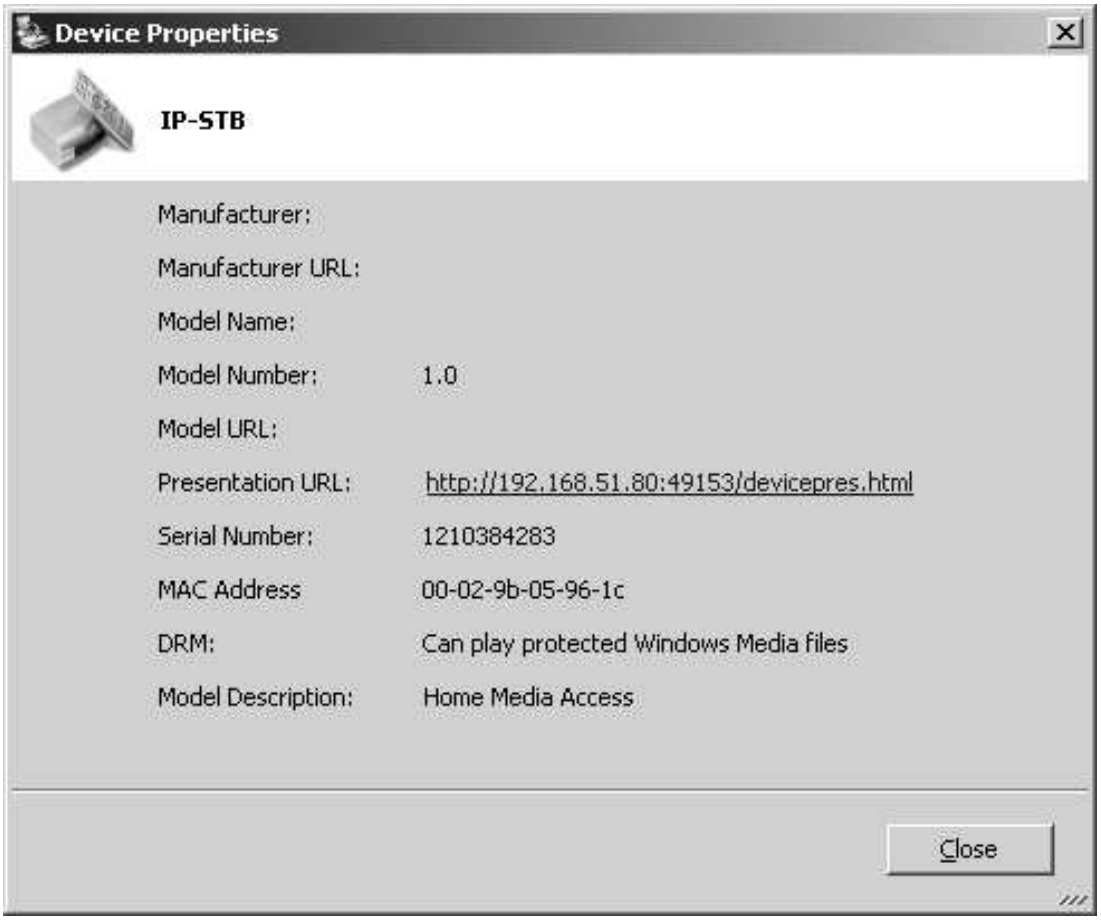

Figure 7.3: Device properties in Windows Media Connect

Connect looks for in the document for the device that tries to register with the server. This document is served with the webserver that is built into the UPnP implementation. In this document I could also specify some tags like “modelDescription” and “manufacturer”, info that shows up in WMC along with an icon of my choice. The document for the set-top box is shown in figure 7.4.

7.3 Authorization

To be able to browse any files at all the DMR has to be authorized by WMC. This was already implemented in HMA and worked fine. When a DMR requests authorization for the first time a balloon tip appears in the Windows UI and the user is asked to authorize the device. The information on who is authorized is stored in the registry and rememberd by WMC.

7.4 Registration

To access protected content, the DMR must register with the DRM service. Registration is done with a UPnP action called “RegisterDevice”. The device certificate wich is signed by Microsoft is here sent to WMC. It includes the public key of the box.

7.5 Proximity detection

Before you can stream encrypted data to a registered device in the Windows Media DRM 10 for Network Devices protocol, you must perform a process called proximity detection. This process involves sending messages to the device and receiving responses. The time it takes to receive a response is used to determine whether the device is “close” enough to the computer on the network to receive secure data. Confirming that the device is physically close to the client computer on the network helps to prevent spoofing and other types of unauthorized access. WMC also checks that the DMR is on the same private network as the sender by simply checking the ip

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0" xmlns:ms="urn:microsoft-com:wmc-1-0">
<specVersion>
<major>1</major>
<minor>0</minor>
</specVersion>
<device ms:X_MS_SupportsWMDRM="true">
<deviceType>urn:schemas-upnp-org:device:MediaRenderer:1</deviceType>
<friendlyName>IP-STB</friendlyName>
<manufacturer></manufacturer>
<manufacturerURL>http://www.manufacturer.se</manufacturerURL>
<modelDescription>Home Media Access</modelDescription>
<modelName>1510</modelName>
<modelNumber>1.0</modelNumber>
<modelURL>http://www.manufacturer.se/products_ipstb.htm</modelURL>
<serialNumber>1210384283</serialNumber>
<UDN>uuid:13141813-3188-6353-314159265358979</UDN>
<UPC>123456789</UPC>
<iconList>
<icon>
<mimetype>image/png</mimetype>
<width>48</width>
<height>48</height>
<depth>24</depth>
<url>/ipstb.png</url>
</icon>
</iconList>
<serviceList>
<service>
<serviceType>urn:schemas-upnp-org:service:RenderingControl:1</serviceType>
<serviceId>urn:upnp-org:serviceId:RenderingControl</serviceId>
<controlURL>/upnp/control/renderingcontrol</controlURL>
<eventSubURL>/upnp/event/renderingcontrol</eventSubURL>
<SCPDURL>/renderingcontrol.xml</SCPDURL>
</service>
<service>
<serviceType>urn:schemas-upnp-org:service:ConnectionManager:1</serviceType>
<serviceId>urn:upnp-org:serviceId:ConnectionManager</serviceId>
<controlURL>/upnp/control/connectionmanager</controlURL>
<eventSubURL>/upnp/event/connectionmanager</eventSubURL>
<SCPDURL>/connectionmanager.xml</SCPDURL>
</service>
</serviceList>
<presentationURL>/devicepres.html</presentationURL>
</device>
</root>
```

Figure 7.4: Device description document

packets. When proximity detection is complete WMC changes the "DRM: Cannot play protected Windows Media files" to "DRM: Can play protected Windows Media files" as can be seen in 7.3. The protocol for proximity detection is confidential and can not be explained in detail here. [18]

7.6 License

The license is a binary XMR policy that needs to be parsed and enforced by the set-top box . XMR is a proprietary binary format. When the license is parsed, information on how the audio may be treated and the keys necessary for decrypting it is obtained. [19]

7.7 Extending the streamer

One central component in the set-top box is the streamer. It's the component that parses all media data that is played. It is designed to be flexible and consists of a minimal core and loadable elements that each have a special task. These elements are chained together at runtime once the streamer knows what type of stream is played and hence what elements to use.

There are three types of elements, source-, intermediate- and sink elements. A simple view of the elements is that source elements injects bits into the stream. Intermediate elements parse data and passes it on to the next element while sink elements extracts bits from the stream.

7.7.1 http-source-element

This element was changed to support license requests and parsing XMR licenses. This is a source element that downloads files with HTTP. A DRM protected file is identified by a HTTP error 400, bad request from WMC. When this error is received we try to request the license with a HTTP POST.

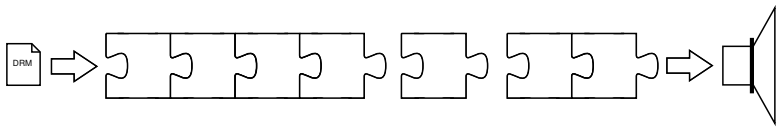

Figure 7.5: This is a simple model of the streamer. Elements (here represented by jigsaw pieces) are put together at runtime, forming a pipe that processes the stream.

7.7.2 wmdrm-nd-decryption-element

This element was created to decrypt the WMA payload with AES in counter mode (see section 6.1.3). It is an intermediate element and is inserted in the streamer as can be seen in figure 7.5.

7.8 Encrypted messages

In the communication diagram in figure 7.6 the communication between the IP-STB and Windows Media Connect is illustrated. The first part, authentication, registration, proximity detection and browsing the media is handled by Home Media Access. The streamer then receives the request to play the file and realizes it's a protected file. It asks for the license and parses it before playback can be initiated. The messages that are sent between the DMR and WMC in the proximity detection phase are encrypted to ensure that only devices that are validated and have certificates signed by Microsoft will be able to download protected content.

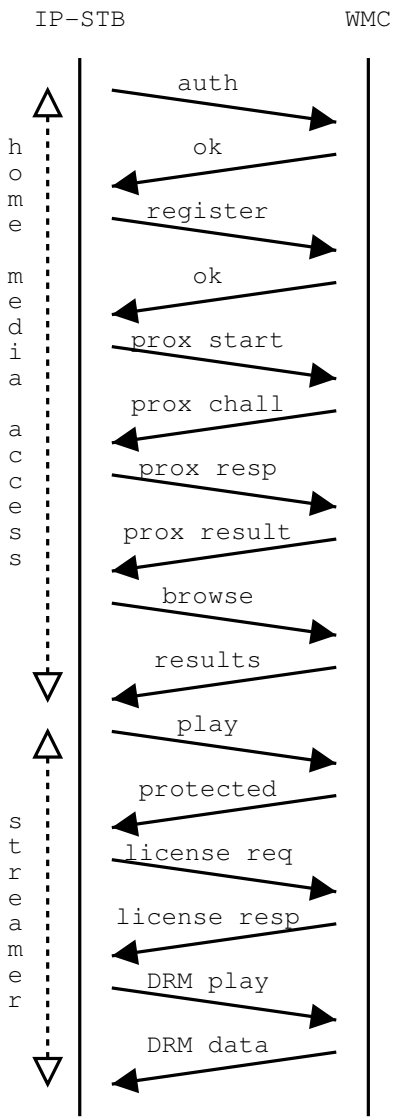

Figure 7.6: Diagram to illustrate the communication between the IP-STB and Windows Media Connect. The first part shows the communication between HMA and WMC. The second part between the streamer and WMC.

Chapter 8

Discussion

This chapter summarizes the work in this thesis.

8.1 Making a set-top box play DRM protected content

The aim for this thesis was to make an IP-based set-top box play DRM protected content.

8.2 Implementational limitations

There are a few limitations in the implementation presented in this thesis work.

- No connection between license parser and decoding element
- No parsing of ASF
- Rewrite of HMA with DRM support in mind

Right now the http-source-element decodes the license but does not pass the keys forward to the wmdrm-nd-decryption-element. Instead the keys

are hardcoded. I left it this way because of time shortage and it does not affect the demonstration of the system since I've only got one test stream and only one license.

A more general parsing of ASF is also needed to play all Windows Media Audio files. The ASF header contains information about how to decrypt the payload data. This information needs to be passed to the wmdrm-nd-decryption-element. This information is hardcoded right now.

HMA is however functional but it was not designed with the DRM extension in mind. It could need a redesign and a rewrite to make it work as well as it once worked, before DRM.

8.3 PVR and DRM

The next generation of set-top boxes has got PVR[1]-functionality. This means that content can not only be viewed on the box but also recorded. This functionality requires that the recorded content is protected in some way.

Since movies and TV-shows are broadcasted to the box in a digital format, it needs to be protected to ensure that pirates do not spread the content on the Internet. At the same time a legitimate user should be able to pause the movie in the livingroom and continue watching in the bedroom.

Also one should not forget that the VCR has set a standard on how people behave with recorded movies and TV-programs. Wouldn't you get frustrated if you no longer could ask your friend to record a TV-show for you because it only would play on his device?

This is a problem and I'm not sure that a DRM solution would solve it to its best. Maybe a solution would be if the box left its fingerprint on the recorded content so that if the content owner was to find a copy on a filesharing service he would know what box once recorded it and take legal actions against the owner of that box.

[1]Personal Video Recorder

Chapter 9

Future Work

> "DRM is a complicated issue and it's not going to go away. As long as there's premium content, there's going to be DRM. There's both good and bad practices here and vendors who adhere to the best practices will find the most customer satisfaction."
>
> – Michael Gartenberg

This chapter deals with how to make DRM into a product and how DRM can be used on a IP-STB in the future.

9.1 How to make DRM for Network Devices into a product

The implementation I've made in this thesis is only a demonstration of how it can be implemented. There are a few steps before this DRM implementation can reach the customers.

- Private key
- Certificate

9.1.1 Hide the private key

In order to send encrypted messages between the IP-STB and WMC a private and a public key is needed. The private key is to be hidden in the set-top box while the public key is published in the certificate.

It's important that the private key is secure and that it can't be read out by an attacker. The IP-STB have a way to download encrypted content and decipher and check the integrity. This mechanism could be used to provide security for the key.

9.1.2 Get a certificate

During development I've been using a test certificate from Microsoft with wich I have only had access to two test streams, one with DRM and one without. In order to play purchased content a real certificate needs to be created.

9.2 The future of DRM on a IP-STB

The next generation of set-top boxes will be equipped with a harddrive that enables the user to download content and *store* it on the box. This changes the need to stream music on the home network and opens for a stand alone DRM solution to play music on the box.

Bibliography

[1] The Digital TV Group Limited. Conditional access (ca). http://www.dtg.org.uk/reference/tutorial_ca.html, 1997-2005. Accessed: 2005-08-08.

[2] Jacob Löfvenberg. Codes for digital fingerprinting, June 2001.

[3] Unknown author. Wikipedia.org. http://en.wikipedia.org. Accessed: 2005-08-08.

[4] Digital Content Protection LLC. Hdcp 1.1 specification. http://www.digital-cp.com/home/HDCPSpecificationRev1_1.pdf, June 2003. Accessed: 2005-08-08.

[5] Mark Stamp. Digital rights management: The technology behind the hype. http://home.earthlink.net/ mstamp1/papers/DRMpaper.pdf, December 2002. Accessed: 2005-08-08.

[6] Keith Hill Jan Bormans. Mpeg-21 overview v.5. http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm, October 2002. Accessed: 2005-08-08.

[7] Information technology Multimedia framework (MPEG-21). Part 1: Vision, technologies and strategy. Technical Report ISO/IEC TR 21000-1.

[8] Beale Screamer (fingered). Microsoft's digital rights manamgement scheme - technical details. http://cryptome.org/beale-sci-crypt.htm, October 2001. Accessed: 2005-02-18.

[9] Helix community. http://helixcommunity.org. Accessed: 2005-08-08.

[10] Open Mobile Alliance. Oma digital rights management v1.0 approved enabler. http://www.openmobilealliance.org/release_program/drm_v10.html. Accessed: 2005-08-08.

[11] Open Mobile Alliance. Oma digital rights management v2.0 candidate enabler. http://www.openmobilealliance.org/release_program/drm_v20.html. Accessed: 2005-08-08.

[12] The hymn project. http://www.hymn-project.org. Accessed: 2005-08-08.

[13] Dan Ilett. Hackers hijack microsoft drm. http://www.zdnet.com.au/news/security/0,2000061744,39177087,00.htm, January 2005. Accessed: 2005-08-09.

[14] The mpeg-21 rights expression language. http://www.contentguard.com/whitepapers/MPEG21_REL_whitepaper_Rightscom.pdf, July 2003. Accessed: 2005-08-09.

[15] RSA Laboratories. What is public-key cryptography? http://www.rsasecurity.com/rsalabs/node.asp?id=2165. Accessed: 2005-08-11.

[16] Crypto faq: What is oaep? http://www.rsasecurity.com/rsalabs/node.asp?id=2346, 2004. Accessed: 2005-08-09.

[17] Morris Dworkin. Recommendation for block cipher modes of operation. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf, December 2001. Accessed: 2005-08-11.

[18] Msdn library: Performing proximity detection. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmform95/htm/performingproximitydetection.asp, 2005. Accessed: 2005-08-11.

[19] Josh Cohen. A general overview of two new technologies for playing protected content on portable or networked devices. http://go.microsoft.com/fwlink/?LinkId=28569, June 2004. Accessed: 2005-08-11.

Index

Copyright

Svenska

English