

# Usability and Security of DRM architectures

Filip Šuba

Helsinki University of Technology

fsuba@cc.hut.fi

## Abstract

During the last few years, technology research related to Digital Rights Management (DRM) systems has achieved significant progress. Several competing architectures evolved with different mechanisms of DRM enforcement and with different vulnerabilities to various threats and attacks. This paper will discuss major DRM architectures, their vulnerabilities, existing attacks, as well as the impact of using the introduced DRM technologies on a home user.

KEYWORDS: DRM, Architecture, Security, Attack

## 1 Introduction

Upon every purchase of a digital content, users need to be aware of the fact that it is usually protected by a mechanism implementing Digital Rights Management (DRM) attached to the files they're buying, which control the use of the files in various ways, including by restricting usage to a certain number of devices. DRM technology was developed to protect the owners of content from illegal downloads, but it can also lock users into choosing one device, or family of devices.

The motivation behind this paper is to outline direct implications of choosing a particular DRM architecture from the security and usability point of view.

The aim of this paper is to introduce four major DRM architectures, to analyze their vulnerabilities against different attacks and to analyze the impact of these weaknesses along with the actual impact of choosing a particular DRM architecture on a home user.

This document provides an overview of the various ways by which digital content is protected in a DRM system. Several competing DRM architectures are introduced, following by the impact of choosing one of the specified architectures on a home user. Next, the vulnerabilities of introduced architectures are discussed along with the description of various types of attacks against DRM systems.

## 2 DRM architectures

Currently, there is no unified solution available on the field of DRM architectures, and therefore interoperability among devices from different vendors rises new challenges. This paper introduces four major DRM architectures that are most likely to be used in a typical home environment (including devices such as personal computer and various portable media player devices), Microsoft's Windows Media DRM, Apple's FairPlay, Helix's Helix DRM and AACs.

### 2.1 Windows Media DRM

When a consumer acquires an encrypted digital media file from a Web site, he or she must also acquire a license that contains a key to unlock the file before the content can be played.

Windows Media Rights Manager, which is a component of Windows Media Player protects digital media by packaging digital media files. A packaged media file contains a version of a media file that has been encrypted and locked with a "key." This packaged file is also bundled with additional information from the content provider. The result is a packaged media file that can only be played by a person who has obtained a license.

The basic Windows Media Rights Manager process [3] is as follows:

#### 1. Packaging

Windows Media Rights Manager packages the digital media file. The packaged media file has been encrypted and locked with a "key." This key is stored in an encrypted license, which is distributed separately. Other information is added to the media file, such as the URL where the license can be acquired. This packaged digital media file is saved in Windows Media Audio format (with a .wma file name extension) or Windows Media Video format (with a .wmv file name extension).

#### 2. Distribution

The packaged file can be placed on a Web site for

download, placed on a media server for streaming, distributed on a CD, or e-mailed to consumers. Windows Media Rights Manager permits consumers to send copy-protected digital media files to their friends, as well.

### 3. Establishing a License Server

The content provider chooses a license clearing house that stores the specific rights or rules of the license and implements the Windows Media Rights Manager license services. The role of the clearing house is to authenticate the consumer's request for a license. Digital media files and licenses are distributed and stored separately, making it easier to manage the entire system.

### 4. License Acquisition

To play a packaged digital media file, the consumer must first acquire a license key to unlock the file. The process of acquiring a license begins automatically when the consumer attempts to acquire the protected content, acquires a predelivered license, or plays the file for the first time. Windows Media Rights Manager either sends the consumer to a registration page where information is requested or payment is required, or "silently" retrieves a license from a clearing house.

### 5. Playing the Media File

To play the digital media file, the consumer needs a media player that supports Windows Media Rights Manager. The consumer can then play the digital media file according to the rules or rights that are included in the license. Licenses can have different rights, such as start times and dates, duration, and counted operations. For instance, default rights may allow the consumer to play the digital media file on a specific computer and copy the file to a portable device. Licenses, however, are not transferable. If a consumer sends a packaged digital media file to a friend, this friend must acquire his or her own license to play the file. This PC-by-PC licensing scheme ensures that the packaged digital media file can only be played by the computer that has been granted the license key for that file.

## 2.2 FairPlay

The files that are protected with FairPlay are regular MP4 container files which contain an encrypted Advanced Audio Coding (AAC) audio stream. The audio stream itself is encrypted using the Rijndael algorithm combined with MD5 hashes. The master key which is

required to decrypt the encrypted audio stream is stored in encrypted form in the MP4 container file as well. The key required to decrypt the master key is called the "user key."

Each time a track is bought by a customer on iTunes, a new random user key is generated and used to encrypt the master key. The random user key is stored on Apple's servers along with the account information, and also sent to iTunes. On iTunes these keys are stored in iTunes's own encrypted key repository. Using this key repository, iTunes can retrieve the user key required to decrypt the master key. Using the master key, iTunes can decrypt the AAC audio stream and play it. [4]

Every time a track protected by FairPlay is copied onto the iPod, iTunes will copy the user key from its own key repository to the key repository on the iPod.

## 2.3 Helix DRM

Helix DRM is a comprehensive platform for media content delivery of standards-based as well as leading Internet formats, including RealAudio, RealVideo, MP3, MPEG-4, AAC, H.263 and AMR. Helix DRM is part of the RealPlayer and Helix Platform, and thus it enables the users to play the content on a wide array of devices, including mobile phones, home appliances, as well as any personal computer.

Helix DRM [7] comprised of 3 major components:

### 1. Helix DRM Packager

The Helix DRM Packager uses strong encryption algorithms and secure container technology to prevent unauthorized use of content and to prepare digital content for distribution via streaming, download or other delivery methods. The packaged media content and the associated business rules for unlocking and using that content are stored separately, so that multiple sets of business rules can be applied to a single file over time.

### 2. Helix DRM License Server

The Helix DRM License Server verifies content licensing requests, issues content licenses to trusted, authenticated Helix DRM end-user clients, such as RealPlayer, and provides auditing information to facilitate royalty payments. The content owner, in the event of a security breach, can also revoke licenses.

### 3. Helix DRM Client

The Helix DRM client enables download and streaming playback of secure formats in a tamper-resistant environment based on the usage rules specified by the content owners. Customized applications for secure playback can be built on top

of the Helix DRM client. RealPlayer is one example of a customized client application.

Although RealNetworks has recently taken Helix DRM off the market by stopping selling the server software, it will continue to support existing customers such as Vongo and Movielink, as well as its own services such as Rhapsody. [9]

## 2.4 AACSS

Advanced Access Content System (AACSS), the basic encryption present on both Blu-ray and High-Definition (HD) DVD titles, is a successor of the Content Scramble System (CSS) which is used on regular DVD disks.

AACSS relies on the Advanced Encryption Standard (AES) algorithm (with 128-bit keys) to protect the disc data. Similar to DVD players, HD DVD and Blu-ray drives come with a set of Device Keys handed out to the manufacturers by AACSS Licensing Authority. Unlike the CSS encryption used in DVDs, though, AACSS has a built-in method for revoking sets of keys that are compromised and made public. Disks encrypted with AACSS feature a Media Key Block (MKB) that all players need to access in order to get the key needed to decrypt the video files on the disc. The MKB can be updated by AACSS Licensing Authority to prevent certain sets of Device Keys from functioning with future titles.

AACSS also supports a feature called the Image Constraint Token (ICT). When set, the ICT forces video output to be degraded over analog connections.

While AACSS is used by both HD disc formats, the Blu-ray Disc Association (BDA) has added some features of its own to make the Blu-ray format more secure than HD DVD. The additions are BD+ and ROM Mark.

While the generic AACSS specification includes a key revocation mechanism, BD+ allows the BDA to update the entire encryption system once players have already shipped. If the encryption is cracked, new discs will include information that will alter the players' decryption code.

The other new technology, ROM Mark, affects the manufacturing of Blu-ray discs. All Blu-ray mastering equipment must be licensed by the BDA, and they will ensure that all of it carries ROM Mark technology. Whenever a legitimate disc is created, it is given a unique and undetectable identifier. It's not undetectable to the player, though, and players can refuse to play discs without a ROM Mark. [12]

## 3 Impact on Home Users

### 3.1 Interoperability

Microsoft has created a PlaysForSure logo to let users know which devices and files are compatible with Windows Media files that are protected by Windows Media DRM. This way users can play protected files either on their personal computers running Windows operating system or on any device on the market marked with the PlaysForSure logo. However, Microsoft's new Zune media player is not compatible with PlaysForSure.

As for Fairplay, Apple's DRM technology, songs that were purchased at the iTunes Store, can only be played on two devices, such as a computer and an iPod.

Users who have bought for example a Sandisk Sansa e200 series portable music player get RealNetwork's Rhapsody media service bundled inside, and a chance to pay a monthly subscription for music downloads. But if users cancel the subscription, the next time they connect to the Internet, Rhapsody will delete the songs from the music player and their computers. Songs which were purchased individually won't be deleted, but since the content will be protected by RealNetworks' Helix DRM, users will have to ensure that any new music playing software or hardware they buy supports Helix. [8]

### 3.2 Security

From the security point of view, home users do not need to be concerned about practically anything. As the DRM technology was developed to serve the content providers to protect their content from illegal use, if the security is violated, the end users are not endangered in any way.

The only problem might be if the user loses the license, or user keys, so that the content becomes unplayable even if it was purchased legally and the user possesses the actual media file.

## 4 Architectural vulnerabilities

This section analyses possible vulnerabilities of the DRM implementation of leading vendors, such as Apple and Microsoft. Recently, a potential vulnerability was discovered in AACSS, which will be discussed as well. As so far any serious DRM vulnerabilities have not been found in the Helix's architecture, it will not be the subject of this analysis.

## 4.1 Apple

When users buy content, they can authorize up to five devices on which the content can be played. When a new computer is authorized, it also generates a globally unique ID number for itself and sends it to Apple, which stores it as one of the five authorizations in the user account. When a computer is deauthorized, it deletes its local set of user keys and requests Apple to remove the authorization from its records. If the keys are backed up, users can deauthorize their systems, then restore the keys and authorize a new set of computers, resulting in more than five machines that can all play the existing purchased music. However, any new music purchased on the newly authorized systems will create new keys, and the previously de-authorized machines will not be able to play the new purchases because they can't obtain the new keys.

The iPod makes no decisions about which tracks it can play, it simply is given user keys for all the songs it contains by iTunes. If iTunes has songs in its library, but lacks the keys to play them—from another account, or on a deauthorized computer that has dumped its keys—it will simply not copy the protected songs to the iPod. There is no way unplayable protected songs can be copied to the iPod without the user keys to play them, because iTunes will not let this happen. This again delegates the burden of DRM to iTunes. [4]

Because protected AAC songs are scrambled with an encrypted master key, it is practically impossible to unscramble protected song files. Instead, attackers might attempt to steal the user keys so they can simply decrypt songs in the same manner as iTunes does.

There are several known attacks against the FairPlay architecture [5]. Users are able to take advantage of these attacks to decrypt the content that they purchased, and thus they can play this content freely on any other device they possess. However, no attacks have been invented so far that would enable the users to download or decrypt any content they want. This makes the existing attacks rather useless, as the users have always had the possibility to for example burn their content to standard audio CD, which loses DRM protection as well.

## 4.2 Microsoft

When users download content that is protected by Windows Media DRM and try to play it in Windows Media Player, it is possible that they will come across files containing Trojans and other malware. License-protected movie files can be infected with the WmvDownloader-A or WmvDownloader-B Trojans. Normally when a user tries to play a protected Windows

media file, and a valid license is not stored on a computer, the application will look for it on the internet in order for the users to buy access to copyright-protected content. This new technology is part of the latest Windows Media Player 10 update as well as XP SP2. If the user runs a video file that is infected by one of the "DRM Trojans", they pretend to download the corresponding license from the net. In reality users are redirected to sites that take advantage of Windows vulnerabilities to download spyware, adware, premium-rate diallers and other viruses onto victim's machines. [6]

Microsoft's latest operating system includes mechanism called Protected Media Path (PMP), which is a set of technologies enforcing DRM that create a "Protected Environment". The Protected Environment in which DRM content is played contains the media components that play DRM content, so the application operates on very high level of abstraction and provides only remote control (Play, Pause, Stop, etc.), instead of having to process the content data. The Protected Environment is only accessible to the third-party software which has been approved, signed, by Microsoft. Therefore any other applications cannot access the unprotected media content. [11]

In order to prevent the users from copying the protected content during the playback (by approved application), PMP also specifies several hardware requirements on output devices. For example High-bandwidth Digital Content Protection has to be enabled on interfaces such as DVI or HDMI. If the content is played on hardware that does not meet these requirements, the playback quality is significantly decreased (video resolution is rescaled, analog audio outputs are disabled). [10]

In January, a kernel developer for the ReactOS, Alex Ionescu, announced that he had discovered a method that allows end users to bypass Protected Media Path. His idea was to use boot Windows Vista with the /DEBUG flag and then use the internal, undocumented Kernel-Mode Debug API to load executable code in kernel-memory or to overwrite existing code (as well as to disable PatchGuard). The rationale behind this was that PMP wouldn't detect any issues, since no unsigned code was running in the kernel, instead, there would be code hidden in Non Paged Pool or as part of \Driver\Null's IOCTL routine (similarly to how Johanna loaded code using the pagefile.sys). [5]

In March, however, Microsoft announced that this technique would not lead to exploiting the driver signing/DRM model in Windows Vista.

On the other hand, similar to FairPlay, there are several known attacks against Windows Media DRM as well [5]. However, while attacks against FairPlay enable

the users only to retrieve and decrypt the content that they purchased, attacks against Microsoft's Windows Media DRM can be used to terminate the DRM protection on any content the user might come across. This makes Microsoft's DRM architecture more vulnerable and thus more friendly to the users who have the tools to easily decrypt the content and use it with other devices.

### 4.3 AACSS

The AACSS standard is still considered to be secure and no major vulnerabilities have been found so far. Although, in January, a potential weakness of the HD DVD standard was discovered.

AACSS is the content security system, which encrypts the contents on commercial video HD DVD discs in an ideal HD DVD cryptographic ecosystem. Those contents can only be decrypted by trusted devices that will not allow the content to be redirected to a non-secure output. Furthermore, AACSS is designed in such a way that if a known device becomes compromised, it can have its key revoked, making further compromises theoretically impossible.

There is an application called BackupHDDVD, which was built to sidestep this ecosystem by decrypting the content using keys that have been extracted from another compromised player (or obtained using some other method). The decryption process itself is based on AACSS's own publicly available decryption routine, and it would appear as though AACSS has been designed in such a way that if one were to acquire the unencrypted volume key of a specific HD DVD, one can decrypt that disc from the command line using this tool. This exposes a weakness in AACSS design.

However, the question is, how to get the volume keys that might be used with this tool. As BackupHDDVD is not capable of gaining them, the user has to already know what they are and provide them to the tool. As such, BackupHDDVD is a basic decryption utility.

Comments from the tool's author, a programmer known simply as muslix64, imply that software players (such as PowerDVD/PowerHDDVD) actually keep the decrypted volume key in memory, and that the key can be snatched from memory by someone who knows what to look for. There has been no confirmation on this matter, however. [13]

Therefore this method of copying the content in order to be able to play it freely in other players and platforms is not really useful for ordinary home users until someone else makes a list of keys that could be used with the tool and then makes it publicly available.

## 5 Existing Attacks

There are three possible attacks against a DRM system. First one is focused on attacking the DRM protocols, the second one tries to gain access to the secure storage of client devices, and the last one attacks the rendering application. All of them aim for one goal: to get the digital content in an unprotected form.

Despite the fact that DRM technology has existed only for a short period of time, several real life attacks can be found. For example, an earlier version of Apple's FairPlay used an insecure protocol which allowed an emulator *PyMusique* to pretend to be a legitimate iTunes client when downloading music from the iTunes store. This was possible because no mutual authentication between the iTunes client and the iTunes music store existed. There is a similar problem with authentication of the trusted device that enabled another tool, which is provided by the *Hymn* project, to emulate a trusted iTunes client as if it was installed in a different computer, in order to obtain the key of the user from the iTunes server. [1]

Attacks against client devices are usually focused on extracting the content keys or the unencrypted content from the secure storage. Several examples of these types of attacks can be found, such as *Free Me*, *DRM2WMV* or *FairUse4WM* tools against Microsoft's Windows Media DRM system.

Attacks against the rendering application have been found as well, for example authors of a rendering application for the Windows Media DRM system replaced part of their software so that once the content is decrypted, it can be captured and saved. There exist a similar kind of attack against iTunes as well.

## 6 Conclusion

There are many DRM architectures which are provided by different vendors. Most likely to be used in a typical home environment (including devices such as personal computer and various portable media player devices) are Microsoft's Windows Media DRM, Apple's FairPlay, Helix's Helix DRM and AACSS.

Most of these architectures have several more or less significant vulnerabilities, and several attacks were introduced to loose the DRM protection of the media content. The existing attacks can have different forms, such as attacking the DRM protocols, gaining access to the secure storage of client devices, or attacking the rendering application.

The impact on home users is that in many cases the users get trapped with one technology and only can buy devices that are compliant with the DRM mech-

anism that was used to protect the files that they purchased. However, the users can get advantage of existing attacks against DRM architectures, and thus gain full control of their files in order to be able to play them on any device of their choice.

## References

- [1] Gelareh Taban, Alvaro A. Cárdenas, Virgil D. Gligor Towards a secure and interoperable DRM architecture. In *Proceedings of the ACM workshop on Digital rights management DRM '06*, Alexandria, Virginia, USA, October 2006. ACM Press.
- [2] Stefan Bechtold The Present and Future of Digital Rights Management. In *Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS'06)*, pp. 6-7, Max Planck Institute for Research on Collective Goods, Bonn, Germany, December 2006.
- [3] *Architecture of Windows Media Rights Manager*. <http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx>
- [4] *How FairPlay Works: Apple's iTunes DRM Dilemma*. <http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html>
- [5] *Alex Ionescu's Blog: Vista DRM Issue Aftermath*. <http://www.alex-ionescu.com>
- [6] *Trojans exploit Windows DRM loophole*. [http://www.theregister.co.uk/2005/01/13/drm\\_trojan](http://www.theregister.co.uk/2005/01/13/drm_trojan)
- [7] *Helix DRM - Features*. <http://www.realnetworks.com/products/security/drm/features.html>
- [8] *DRM holds key to the digital home*. [http://www.infoworld.com/article/06/09/26/HNmusicdrm\\_1.html](http://www.infoworld.com/article/06/09/26/HNmusicdrm_1.html)
- [9] *DRM Watch: RealNetworks Takes Helix DRM Off the Market*. <http://www.drmwatch.com/drmtech/article.php/3663976>
- [10] *Output Content Protection and Windows Vista*. [http://www.microsoft.com/whdc/device/stream/output\\_protect.msp](http://www.microsoft.com/whdc/device/stream/output_protect.msp)
- [11] *Overview of the Protected Media Path*. <http://msdn2.microsoft.com/en-gb/library/aa376846.aspx>
- [12] *Hacking Digital Rights Management*. <http://arstechnica.com/articles/culture/drmhacks.ars/3>
- [13] *The AAC3 crack that wasn't: BackupHD-DVD*. <http://arstechnica.com/news.ars/post/20070107-8564.html>