SECURITY ASPECTS OF DRM SYSTEMS

H.L. Jonker[1], S. Mauw[1], J.H.S. Verschuren[1,2] and A.T.S.C. Schoonen[2]

[1] Eindhoven University of Technology, Department of Mathematics and Computer Science
E-mail: h.l.jonker@stud.tue.nl, s.mauw@tue.nl

[2] TNO ITSEF BV, Stieltjesweg 1, Delft,
E-mail: {verschuren, schoonen}@tpd.tno.nl

INTRODUCTION

Acquiring digital media over the Internet has become commonplace in recent years. Companies are looking into ways to sell their content (music, movies, etc.) over the Internet without the buyer being able to further distribute the work. Digital Rights Management (DRM) systems address this; their main goal is to enable authorised users to access a version of digital content on the terms for which they are authorised whilst preventing all other access to digital content. This is of course not always possible, therefore the field of DRM is also interested in practical security, i.e. security that may theoretically be breakable, but in practice will not be (because the costs outweigh the benefits).

So DRM systems aim to achieve a security goal. How well they achieve this goal is unclear. Although various security techniques are being used by DRM systems and being researched for use in DRM systems, there seems to be little research into evaluating the security of an entire DRM system. As security of the individual components of a system does not guarantee security of the system as a whole, this means that currently it is hard to understand what level of security is offered by a DRM system.

TNO ITSEF performs security evaluations of both hardware and software products. This paper is a preliminary and condensed report of research into evaluating the security of DRM systems. The main goal of this research is to devise a security evaluation method that has consistent, reciprocal comparable results.

DIGITAL RIGHTS MANAGEMENT

This section describes DRM systems in a generic sense. First, their goals are mentioned, followed by a technical description of DRM systems. The design of a DRM system is of course influenced by the context in which it is deployed. Therefore, the next subsection takes a closer look at that context.

In the last subsection, various techniques are examined which are used to strengthen the security of DRM systems.

Generic break-down of DRM systems

DRM systems operate in a client-server context. A distributor offers content (e.g. audio (music), video (movies), text (books), images (photos)) to customers. Generally speaking, it is far easier to implement stringent security measurements on the distributor's side than on the user's side. Therefore, this side can be considered "secure" and the user's side can be considered "insecure". A network serves as a communication medium. For purposes of security evaluation, the network can be considered insecure.

Distributor's side

To protect the content from access outside the system, the content is stored inside a "secure container". To access the content, a valid license is needed (which can be included in the container or delivered seperately). Licenses are expressed in Rights Expression Languages [4] (RELs). These languages (mostly XML-based) allow only the rights granted in the license and deny any other access. To ensure interoperability, the semantics of a REL can be defined in a Rights Data Dictionary (RDD) – another XML-based language.

To ensure that the content stays secret and is received correctly, secure communication is used. This assures that attackers cannot obtain a secure container and the accompanying license when these are sent to a legitimate user, and ensures that the user receives them correctly.

User's side

In almost all cases, the content provider who uses a DRM system requires a secure environment at the user's side. The content provider wishes to execute DRM components on the user's side. These components consist of code, data and state. Since the user's side is considered hostile territory, these components execute in hostile environment. Measures must be taken to assure correct execution of code, data integrity and state integrity. A tamperproof environment can provide this. This tamperproof environment is referred to as a Trusted Computing Base (TCB). A TCB functions as a trusted third party for computing.

A DRM system assures that all steps from opening the secure container up to and including conversion into an analogue format operate as required by the license. Without a TCB at the user's side, there is no way of guaranteeing that the terms under which the user is allowed to access the content are met.

A TCB is not needed on the user's side, when the DRM system only sends versions of the digital content to the user, which need not (or cannot) be protected (e.g. analogue versions or low-quality versions).

Influence of networks on DRM

DRM systems operate on a network. This could be the Internet or a cell phone network. Other networks are possible (e.g. a cable TV network), but not considered in this paper. A DRM system needs to take into account the constraints of the device which acts as the user's side. An important question is how powerful and secure a TCB implemented on the device is. For the mentioned networks, these devices would typically be a computer and a cell phone. Each of these networks is examined below.

Internet

As computers can emulate computers, they can emulate a computer which is allowed to access the content. So, if a user can access the content once, it is hard to prevent the user from accessing the content as he pleases. This means that it is hard to realise a TCB on computers without additional, tamperproof hardware components.

However, DRM is concerned with practical security: making it too hard to acquire the digital contents illegally. As long as the above attack is too difficult (or time-consuming) to execute, the security of the DRM system can be acceptable for content-providers.

cell phone network (see [5])

Cellular phones have a short life cycle – which means that introducing hardware support for DRM can happen (relatively) quickly. Add to this hardware secrets (the SIM-card) and the closed aspect of the hard- and software (in stark contrast to computers), and it is clear that the technological requirements of DRM systems are more easily provided by the mobile phones industry (when compared to the PC market).

However, cell phones are limited devices. They are not ideal devices for portraying either audio or video (although improvements are being made). This means that the content that can be accessed on cell phones will be limited in scope. It is hardly imaginable to watch a complete movie on a cell phone.

Security supporting techniques of DRM

DRM systems can use various techniques to attain (sub)goals. In this section, the following techniques are discussed: Cryptography, ID techniques, tracing techniques, TCB and finally Updatability & interoperability.

Cryptography secure container

Cryptography is used to protect the content from access and to secure communications between the user and the distributor.

To protect content, the content is hidden in a “secure container”. This container is encrypted to protect it from all access except via the DRM system.

ID techniques

Content owners can use content identification (for example) to detect theft, whilst users could use this to find content which they have seen or heard but which they have not yet acquired. DRM systems can employ a variety of techniques to identify content: a Digital Object Id can be added, the digital content can be fingerprinted or a watermark can be added.

The Digital Object Identification (DOI) scheme works similar to a bar code – given a cryptic identifier, a server looks up the current location of the content and redirects you there [DOI].

A fingerprint is a small sample of the content. This can be sent to a fingerprinting service, which identifies the content and redirects the user accordingly.

Watermarks consist of information embedded in digital content. They are not detectable by humans on playback of the content (if correctly embedded), but a watermark detector finds the watermark, even after conversion to analogue.

Tracing

The information embedded by a watermark could also identify the user who legally acquired the content. If the content is found “in the wild”, the watermark can still be extracted and the user identified.

Trusted Computing Base

A Trusted Computing Base (TCB) assures others that the owner (of the TCB) can execute computations faithfully inside the TCB without exposing secrets to the owner. An example of a TCB is the Dutch “chipknip”.

Updatability & interoperability

Both updatability and interoperability ensure robustness of the DRM system. It is unlikely that DRM systems would achieve perfect security from the outset – but by providing updates the system might be able to remain secure enough.

As there are currently many DRM initiatives, it makes sense to ensure that any DRM system can work with most other DRM systems. This is done by standardising the language of the license (REL and RDD).

EVALUATION TECHNIQUES

In order to get an understanding of the level of security offered by a product, several security evaluation methods have been developed. Among those are the Common Criteria [7] (CC), Attack Trees [8] and OCTAVE [1] . These methods all have drawbacks: the CC use a lengthy and costly process to evaluate, attack trees will differ depending on whom does the evaluation and OCTAVE is more concerned with evaluating organisations than products. It is desirable to use a method which delivers consistent, reciprocal comparable results for technically evaluating DRM systems.

EVALUATING DRM SECURITY

In order to be able to evaluate the security of DRM systems, their security goals need to be clearly stated. A threat model is needed to reason about possible threats. To study the security goals DRM systems aim to achieve, a model of the user side will help determine security issues all DRM systems need to address.

As the design of DRM systems is influenced by the network on which they are deployed, so is the threat model:

For the internet we use a powerful threat model. The attacker can break weak cryptography, exploit weak keys, knows the communication protocol, controls the network, can break into servers with security flaws, has complete control over the user side and can hack the playback software on the user side.

For cell phone networks we use a less powerful threat model. The attacker can break weak cryptography, exploit weak keys, knows the communication protocol, does not control the network, cannot break into servers, has no special control over the user side and cannot hack the playback software.

The security goal DRM systems aim to achieve is to prevent all access to the content that does not comply with a valid license obtained from a valid source for said content. There can be secondary goals (e.g. the ability to trace illegally accessible content back to the buyer or the ability to prove authorship of content). This paper will not concern itself with secondary security goals.

Security issues of the client side

The flow of content through the user side of a DRM system is shown in Figure 1. The content is received over a "connection" (e.g. a modem). It can be stored or streamed to the player. The player generates audio and video output as needed to render the content to the user. This output is converted by drivers into a format understood by hardware. The hardware can either give analogue output, or stream digital output to external hardware capable of handling this.

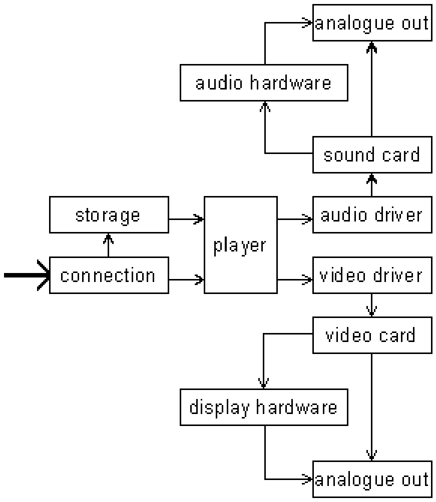

Figure 1: The flow of content at the user side.

To protect the content, the content must remain inaccessible until "analogue out" is reached. Otherwise, the digital, high quality content could be retrieved from an intermediate point.

However, this is not enough. DRM systems require memory (persistent state, see [9], [6]) at the user side, as a license can specify a number of times the content may be accessed.

Security issues of the server side

A DRM system can be modelled in various ways (e.g. [2], [3]). There are some generic security riscs applicable to all models:

Communication Interception Any time the content is sent unprotected over a communication channel, this channel can be intercepted. Using secure channels prevents this.

Analogue out It is possible to make an analogue copy of the output (e.g. taping the output). This cannot be prevented by any DRM system.

Server hacking If a hacker obtains control over one of the servers on the server side, he can provide the server with false information and he might be able to obtain content. To help prevent this, few machines should be used (fewer machines means fewer security hazards) and these servers should be kept as secure as possible. On the other hand, the different servers have different security needs and that would make it more logical not to group them. Ideally, the services offered all operate inside a TCB.

Communication Protocol Hacking The communication protocols used to send data between the various components might have security flaws. Depending on the nature of the flaws, an attacker might learn information, which was meant to be secret (such as decryption keys), or might be able to pose himself as a legitimate communication partner.

Key Acquisition Should an attacker acquire a private key used by a component in the system, that attacker can pose as that component. Exposed keys on the user side can be used to emulate components and so defeat the system.

Evaluation criteria

There are several criteria which can be applied to the evaluation of the security of DRM systems. More research will clarify the impact of these criteria on the overall security of DRM systems. To name a few:

Single Point Of Failures should be avoided as much as possible. The more there are, the harder it is to secure the DRM system.

The ability to update (parts of) a system means that it can cope with security errors. The ease with which updates can be created and integrated is important.

The interoperability of a system poses a security risc. External components (players, secure containers) are introduced into the system, or internal components (secure containers) are exposed to other systems. The influence such components have in the system is important.

Dependencies on other systems (such as an operating system) may introduce weaknesses into an otherwise secure system.

CONCLUSION

Evaluating the security of DRM systems is a complex task. The issue is not solvable, i.e. there is not one definite technical solution that satisfies all security needs - amongst other reasons, the contexts in which DRM systems operate varies too greatly.

Therefore, it is crucial to understand the security a DRM system offers. Unfortunately, current evaluation methods are ill-equipped to produce consistent and reciprocally comparable evaluations of DRM systems. Therefore, more research into this topic is needed.

REFERENCES

[1] CERT. http://www.cert.org/octave/.

[2] Serrão et al. Open SDRM - an open and secure digital rights management solution. Research note, IADIS, June 2003.

[3] S. Guth. *Digital Rights Management*, pages 150–161. Number 2770 in LNCS. Springer-Verlag Heidelberg, November 2003.

[4] S. Guth. *Rights Expression Languages*, pages 101–112. Number 2770 in LNCS. Springer-Verlag Heidelberg, November 2003.

[5] F. Hartung. *Mobile Digital Rights Management*, pages 138–149. Number 2770 in LNCS. Springer-Verlag Heidelberg, November 2003.

[6] B. Horne, L.R. Matheson, C. Sheehan, and R.E. Tarjan. Dynamic self-checking techniques for improved tamper resistance. In *Digital Rights Management Workshop*, pages 141–159, 2001.

[7] TNO ITSEF. http://www.commoncriteria.nl/.

[8] B. Schneier. http://www.schneier.com/paper-attacktrees-ddj-ft.html.

[9] W. Shapiro and R. Vingralek. How to manage persistent state in DRM systems. In *Digital Rights Management Workshop*, pages 176–191, 2001.