Chapter V
Discovering the Core Security Requirements of DRM Systems by Means of Objective Trees

Hugo Jonker
University of Luxembourg, Luxembourg
Eindhoven University of Technology, The Netherlands

Sjouke Mauw
University of Luxembourg, Luxembourg

ABSTRACT

The use of Digital Rights Management (DRM) systems involves several stakeholders, such as the content provider, the license provider, and the user, each having their own incentives to use the system. Proper use of the system implies that these incentives can only be met if certain security requirements are fulfilled. Much attention in literature has been devoted to specific security aspects of DRM systems. The contributions of this chapter consist of deriving a systematic overview of core security requirements for DRM systems. This chapter conducts a stakeholder analysis, gives an objective tree for each relevant stakeholder, and develops a simple, generic conceptual model to arrive at the set of core security requirements.

INTRODUCTION

There is a precarious balance between dissemination of information (to the general public) and stimulation of innovation and art. The easier it is to spread new information, the less possibilities to profit there will be for innovators to reap the fruits of their labour. On the other hand, spreading innovation and art is considered beneficial to society.

The introduction of computers has had a profound impact on this balance. With computers,
it is trivial to create a perfect copy of content – a term used to indicate a work of art, such as music, literature, movies, etc. This coupled with the widespread availability of broadband internet connections means that completely new venues for spreading content to the public at large have come into existence. This enables a business model that consists of selling and delivering digital versions of content online. The main point of concern for such a business is to prevent unsanctioned redistribution of the delivered content.

Digital Rights Management (DRM) systems have been created for this goal. The purpose of a DRM system is to protect (digital versions of) content. Content is bound to a license, and the content is only accessible under the terms stated by the license. Since the year 2000, there has been a strong push into the research and development of DRM systems. There has been work on various related security aspects such as secure storage (Shapiro & Vingralek, 2002), traitor-tracing (Kiayias & Yung, 2003; Safavi-Naini & Wang, 2003), watermarking (Cox, Bloom & Miller, 2001), fingerprinting (Haitsma & Kalker, 2002; Prechelt & Typke, 2001) and tamper resistant code (Horne, Matheson, Sheehan & Tarjan, 2002; Chang & Atallah, 2002). There have also been various proposals for models of DRM systems with specific properties (OMA, 2004; Serrão, Naves, Barker, Balestri & Kudumakis, 2003; Guth, 2003; Popescu, Kamperman, Crispa & Tanenbaum, 2004).

These proposals incorporate various security requirements. Some of these requirements assure core DRM functionality, whereas other requirements realise the specific properties for which that architecture was constructed (e.g. interoperability: MOSES (Serrão, Naves, Barker, Balestri & Kudumakis, 2003), Coral (Coral Consortium, 2006)). The emphasis of such proposals is usually on the latter type of requirements. It is not uncommon that the requirements assuring core DRM functionality receive a lesser treatment. These requirements are often not all made explicit, nor is a justification for them provided. Which of these requirements are made explicit varies from proposal to proposal, which means that the set of requirements that assure core DRM security is scattered. There are several reasons to make this core explicit. The first and foremost reason is that security is an enabling factor for DRM systems. DRM systems are designed to provide a solution for a security problem. An understanding of (the justification for) the core security requirements is crucial for fundamental comprehension of the security of DRM systems. Moreover, knowledge of the core security requirements is instrumental in the construction and verification of DRM systems. Such knowledge enables developers to better understand the consequences of security trade offs. In practical systems, such trade offs between desired features and security requirements are not uncommon.

For example, Apple’s iTunes allows the user to create a CD of protected music. Naturally, Apple realised that such a CD could be used to copy music. Nevertheless, this feature was deemed more important than the costs in terms of loss of security. In this case, an informed decision has been made. In other respects, some of the design decisions of iTunes seem less well-informed and have a negative impact on the overall security of the system. A more detailed examination of iTunes follows below.

This chapter uses a structured approach to identify core security requirements and provide a justification for them. The goal of this chapter is focused on the security aspects of the design of DRM systems and our aim is to systematically derive core security requirements for DRM systems. Although there is a wealth of methodologies supporting system analysis and design, the methodologies for deriving security requirements are only at their infancy. Therefore, our research will start by identifying some useful methodologies and combining their strengths.

In order to provide a base for the found security requirements, we describe a model which limits