Models and Languages for Digital Rights

Carl A. Gunter  
University of Pennsylvania  
gunter@cis.upenn.edu

Stephen T. Weeks  
InterTrust Technologies Inc.  
sweeks@intertrust.com

Andrew K. Wright  
InterTrust Technologies Inc.  
wright@intertrust.com

Abstract

Digital Rights Management (DRM) devices provide persistent protection, the means to control the rendering of digital content to users. This enables new kinds of agreements between parties involved in trading intangible goods such as digital music. In this paper we propose a language and model capable of expressing a range of licenses of the kind that DRMs may be expected to support.

1. Introduction

A Digital Rights Management (DRM) system governs rendering of content. DRMs enable sellers of digital content to move beyond current distribution models. Currently a physical medium like a CD is sold to a consumer who receives the right to render all of the works on the CD for his or her own enjoyment as often as desired. This approach is limited in many ways now that media capable of carrying greater content are becoming available, and the Internet can be used to distribute content in bulk transfers or via streaming applications. The sale of a CD is similar to the sale of a good, whereas an ongoing service model may better fit the new distribution techniques. For instance, it may be better to sell a user the right to hear songs from a digital library at a low fixed price per rendering rather than selling the library as a set of hundreds of CDs at a high fixed price. Payments for the service could occur periodically, like paying for using electricity or a cell phone. However, digital goods have some different characteristics than these other services: some experimentation will be required to derive appropriate service models.

The aim of this paper is to make progress on this problem by developing a model and a language for describing licenses to digital works. We focus on licenses likely to be feasible using new DRM technologies such as those developed by InterTrust (http://www.intertrust.com/drm/index.html). While a full-fledged DRM system will allow content providers to make rendering contingent on a variety of events and conditions, such as payment, time and date, identity of the user, membership in a club, identity of the device, return of usage reports, recent contact with a clearinghouse, etc., we begin by studying simple licenses that consist only of payment and rendering events. We develop a mathematical model capable of capturing the meanings of a wide variety of such licenses with precision. We then develop a language of licenses whose semantics is defined by reference to the model. This insures that every license has a completely clear and unambiguous interpretation that is defined without reference to any particular implementation of a DRM system.

2. A Semantic Model for DRM

Our model consists of a domain of sequences of events called realities, and a domain of sets of realities called licenses. Then, in a manner similar to that of denotational semantics for general-purpose programming languages [1], we can express the semantics of a rights management language as a function that maps terms of the language to elements of our domain of licenses. The character of our semantics is similar to those used for concurrency [2] where language constructs are modeled as traces of allowed events.

Our abstract model represents an event, \( e \in \text{Event} \), as a pair of a \( e \in \text{Event} \), and an action, \( a \in \text{Action} \):

\[
e := t : a
\]

Time is totally ordered by \(<\), and the function \( +: \text{Time} \times \text{Period} \rightarrow \text{Time} \) adds a period, \( p \in \text{Period} \), to a time. There are two kinds of actions:

\[
a := \text{render}[w, d] \mid \text{pay}[x]
\]

where \( w \in \text{Work} \) denotes a rights-managed work, \( d \in \text{Device} \) represents a DRM-enabled device, and \( x \) is a decimal. Action \( \text{render}[w, d] \) represents rendering of work \( w \) by rights-enabled device \( d \). Action \( \text{pay}[x] \) represents a payment of amount \( x \) of some currency from a licensee to