Digital Rights Management

Reihaneh Safavi-Naini Nicholas Paul Sheppard

Abstract

Digital rights management allows information owners to control the use and dissemination of electronic documents via a machine-readable *licence*. Documents are distributed in a protected form such that they may only be used with trusted environments, and only in accordance with terms and conditions stated in the licence. Digital rights management has found uses in protecting copyrighted audio-visual productions, private personal information, and companies' trade secrets and intellectual property. This chapter describes a general model of digital rights management together with the technologies used to implement each component of a digital rights management system, and desribes how digital rights management can be applied to secure the distribution of electronic information in a variety of contexts.

1 Introduction

Advances in information and communication technologies and in particular digital representation and processing of data together with the vast connectivity of the Internet, has resulted in major challenges to the security of valuable multimedia works, private data and sensitive corporate information. The owners of such information need protection against reproduction and/or distribution and use of the information beyond their immediate control.

Digital representation of data allows perfect reproduction and reliable and efficient storage and transmission. Digital representation of information also provides a unified way of representing content and so possibility of creating high valued complex multimedia objects such as a movie with accompanying sound track and commentaries. Digital representation of data has resulted in a shift from paper based documentation to electronic based documentations. Today electronic documents are the main form of collecting, storing and communicating information within and outside organisations. A particularly useful property of digital documents enhanced with *meta data*, data used to explain data, is classification and search. Using the Internet connectivity digital objects can be instantaneously delivered to users around the world hence providing opportunity for new forms of business and distribution systems.

Traditional access control systems are able to limit access to electronic information for particular individuals or groups, but are limited in their ability to control what those individuals or groups do with that information once they had gained access to it. This approach cannot provide adequate security for valuable contents such as copyrighted multimedia.

Around the middle of the 1990's, systems such as DigiBox [102] and Cryptolope [68] were gradually developed to allow information owners more control over distribution of digital content in a paid form. Digibox is a set-top box that allows television broadcasters to make their content selectively available to subscribers who have paid for the content. Cryptographic envelopes, or "Cryptolopes", were developed by IBM for secure distribution of content. The content together with pricing information and usage rules are transformed into an encrypted parcel which can be super-distributed. The key can be separately obtained by the buyer of a Cryptolope. Mark Stefik of Xerox envisioned an electronic world throughout which the flow of information was controlled by "digital contracts" [105] (called *licences* in this chapter), and developed the Digital Property Rights Language in which these contracts could be written. These technologies came to be known as *digital rights management*.

Digital rights management technology has since become well-known for its role in copyright protection for Internet music and video services, but is also becoming important in the protection of sensitive corporate information [11] and is emerging as a technology for protecting individuals' private information [70].

The commonly used approach used in digital rights management systems is to associate the sensitive information with a *licence*. A licence sets out the rights that have been granted to a user by the information's owner in a machine-readable and (typically) machine-enforceable fashion. The user may only access the information using a combination of hardware and software whose trustworthiness has been proven to the information owner, and which will only permit the user to exercise rights that are granted by a licence. Section 2 presents a reference model for a digital rights management system and its components.

Persistent nature of protection in DRM system implies that a digital object must not leave the system governed by the DRM. This means that all terminals that use the object (e.g. play a music clip) must have the trusted hardware and software and be able to enforce the licence. This makes inter-operability between digital rights management systems created by different vendors a particularly difficult challenge in digital rights management. Section 3 outlines approaches to inter-operability in digital rights management, and describes some of the major specifications in the field.

Section 4 outlines how digital rights management systems can be applied to protecting copyrighted commercial multimedia; sensitive corporate or government information; private personal information; user-generated content; and personal health information.

A complete digital rights management system requires a number of components to be implemented, including a trusted computing base; rights negotiation; a rights interpereter; cryptographic operations and other supporting technology. Approaches to implementing these are discussed in Section 5.

Digital rights management remains a relatively immature and controversial technology, particularly in its application to copyright protection. The "closed world" approach in which every right must be explicitly stated in a licence has drawn much criticism as eroding users' rights under copyright law. We conclude the chapter with a discussion of this and other outstanding issues and challenges in digital rights management in Section 6.

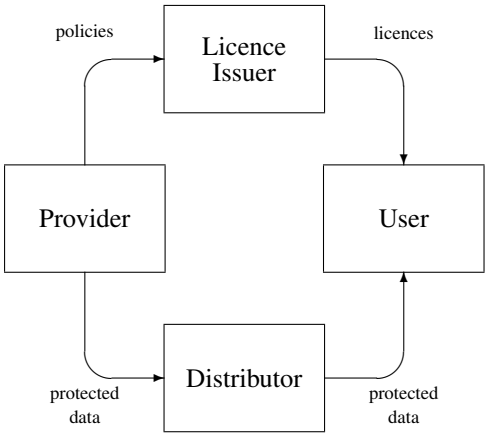

Figure 1: The components of a digital rights management system.

2 The Digital Rights Management Model

Digital rights management has many similarities to traditional access control, but requires that information must remain protected even when transported beyond the boundary of systems controlled by the information owner. Digital rights management can thus be defined as "persistent access control" [13], as distinguished from traditional access control systems that cannot (technologically) compel users to conform to any particular usage policy once they have been granted access to a piece of information.

Digital rights management allows protected information to be transmitted over an insecure channel and stored on an insecure storage device without compromising the integrity and confidentiality of the information. For example, information can be distributed via a direct network connection, a file-sharing network, or by copying it onto transportable media; and stored on a file server, an individual computer's hard drive, or removable media.

2.1 Reference Model

Figure 1 shows our reference model for a digital rights management system. Information is created by a *provider*, and transmitted in a protected (for example, encrypted) form to a *user* via some distribution channel. In order to access the protected data, the user must obtain a *licence* from the *licence issuer*.

Licences are written in a machine-readable *rights expression language* that sets out the terms of use of the data and the information required to access the protected content. We will discuss rights expression languages in more detail in Section 2.4.

The fundamental security requirement for a DRM system is that the hardware and/or software used to access protected data be guaranteed by its manufacturer to behave in accordance with licences; it effectively performs the role of the "reference monitor" in traditional access control systems. For the purposes of this chapter, a *DRM*

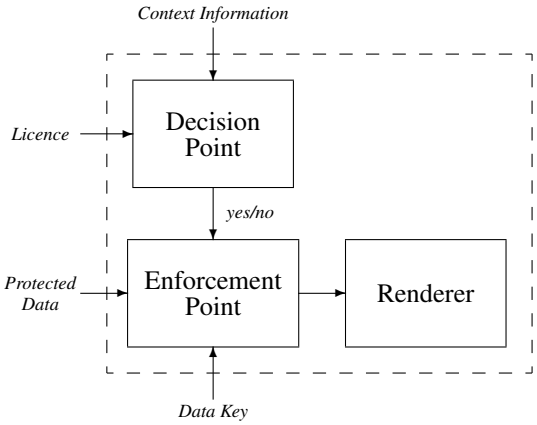

Figure 2: The components of a DRM agent.

agent is an abstract single-user player, editor, or similar that may be implemented as a hardware device, a software application or combination of the two. We will discuss the general form of such devices and applications presently, and discuss their implementation in Section 5.1.

2.2 DRM Agents

Figure 2 shows our reference model for a DRM agent. When a user wishes to perform some particular action on a particular item of data, the *decision point* checks that the user possesses a licence that permits that action. It further checks that the licence has been signed by a recognised licence issuer, and that any conditions associated with the permission are satisfied. If a suitable licence does not exist, or the conditions are not satisfied, the decision point will refuse to carry out the operation. Otherwise, the *enforcement point* will be permitted to retrieve the data key, and the *renderer* enabled to carry out the desired operation.

2.3 Authorised Domains

Early digital rights management systems only allowed licences to be addressed to a single DRM agent, so that a user who bought some multimedia could only access that multimedia on a single device. Most realistic users, however, have more than one device on which they would like to access information.

Newer digital rights management systems support users with multiple devices by way of an *authorised domain*. An authorised domain is a group of DRM agents to which licences to use information can be issued, such that all of the members of a domain can access the information without requiring information to be licensed to each agent individually. DRM agents may join and leave a domain independently of any licences issued to the domain.

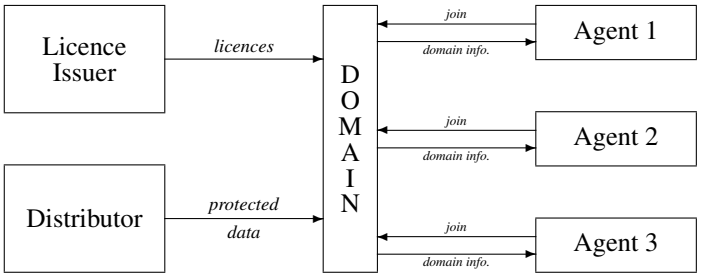

Figure 3: An authorised domain.

In most systems, a device may join a domain by engaging in a cryptographic protocol with a *domain controller* that is responsible for the domain. If the device is accepted into the domain, it will receive some cryptographic information that enables it to decrypt the cryptographic information in a licence awarded to that domain.

The conditions under which a device may join a domain vary from system. Some early systems simply fix an upper bound on the number of devices permitted in a domain [9, 86], with the expectation that this number would be chosen to represent the upper limit of the number of devices owned by a single household. Other systems use the licence issuer as the domain controller [84], so that the rights-holder is able to determine directly what devices should be members of a domain. Some more recent authors have suggested that membership be controlled by some machine-readable policy transmitted from the rights-holder to the domain controller [72, 101, 77].

2.4 Rights Expression Languages

A licence is written in a machine-readable *rights expression language* that describes the conditions under which the associated information may be used.

The rights expression languages most commonly used in the open literature take the form of a series of access control rules, broadly similar to those used in access control languages such as the eXtensible Access Control Markup Language ("XACML") [85].

A licence written in these kinds of languages can be modelled as a contract between a *licensor* (who controls the information to which it refers) and a *licensee* [58, 13]. A licence consists of

- the identitities of the licensor, licensee and any third parties to the agreement;
- the *resources*, that is, items of information, to which the agreement refers; and
- an *agreement* that lists all of the *permissions* that the licensor has granted to the licensee.

Each permission may subject to an arbitrary number of

- *constraints* that must be satisfied before the permission can be exercised, for example, it may only be exercised before a given expiry date; and/or

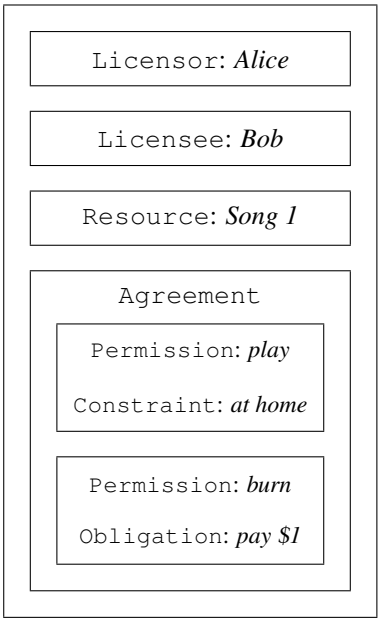

Figure 4: A licence issued by Alice to Bob, in which she has agreed that Bob can play "Song 1" only if he is at home, and that he must pay her $1 for every copy that he burns to CD.

- *obligations* that are incurred by exercising the permission, for example, each exercise must be logged.

Figure 4 shows an example licence set out in this form.

3 Standardisation and Inter-operability

Digital rights management presents a particularly difficult challenge for universal distribution and access to the content. In the following we will focus on technological challenges for inter-operability. Other important aspects are legal and financial implications of allowing content that is protected under one DRM system to be used under a second DRM system. In practice an inter-operability framework addressing these issues must be in place [91].

DRM-protected information is distributed in a protected form that is, by design, inaccessible to any entity that does not conform to the DRM vendor's specification. Therefore, users may not be able to make use of information on DRM agents supporting a different DRM regime, even if they have legitimately acquired the information and the second DRM agent is from a reputable vendor otherwise trusted by the original information provider.

Koenen, et al. [71] suggest three approaches to creating inter-operable DRM systems:

Full-format inter-operability. All protected information conforms to some globally standardised format.

Configuration-driven inter-operability. End-user devices can acquire the ability to process information protected by any DRM regime by downloading appropriate "tools".

Connected inter-operability. On-line third parties are used to translate operations from one DRM regime to another.

Numerous bodies from industry and elsewhere have proposed standards for both complete digital rights management systems, and components of such systems.

3.1 Full-Format Inter-operability

Full-format inter-operability would clearly provide the most convenience for information users, affording them the same convenience that they enjoy when using standardised unprotected formats such as the compact disc. However, it is not easy to define a single standard that is appropriate for all conceivable DRM agents. Furthermore, a breach in the security of the standardised regime could be catastrophic and standards bodies are not typically able to move with the speed required to effectively respond to security breaches.

Full-format specifications include

- the Open Mobile Alliance's Digital Rights Management Specification ("OMA DRM") [84] for mobile phones and similar devices, which provides a simple digital rights management system based on a simplified form of the Open Digital Rights Language;
- the Marlin Developer Community's Core System Specification [77] for consumer electronics devices, which is based on the *Networked Environment for Media Orchestration* ("NEMO") developed by Intertrust [19];
- the Digital Video Broadcasting Project's Content Protection and Copy Management Specification ("DVB-CPCM") [41] for digital television systems;
- the Secure Video Processor ("SVP") Alliance's Open Content Protection System [96] for hardware video decoders that receive protected video from other conditional access or digital rights management systems;
- the security chapter of the Digital Cinema Initiative's Digital Cinema System Specification [37], which defines the measures to be taken to prevent the leakage of digital films from cinemas; and
- Project DReaM [109], an attempt to develop an open-source digital rights management regime sponsored by Sun Microsystems under the name "Open Media Commons".

3.2 Configuration-Driven Inter-operability

Configuration-driven inter-operability attempts to provide flexibility and renewability by allowing DRM agents to dynamically configure themselves with the appropriate digital rights management regime for any protected information that they download. However, it is not clear that all DRM agents will necessarily be capable of accessing all tools (which might only be available for one particular computing platform, for example) or have the resources to store and execute all of the tools required to access all of the protected information accessed by one user.

The MPEG-21 Multimedia Framework (ISO/IEC 21000), for example, includes three parts devoted to a configuration-driven rights management scheme:

- the *Intellectual Property Management and Protection ("IPMP") Components* [63], which describe methods for associating protected resources with *IPMP tools* that implement the specifics of a proprietary digital rights management system;
- the *Rights Expression Language* ("MPEG REL") [64] that will be described in Section 3.4.2 of this chapter; and
- the *Rights Data Dictionary* [65] that provides an ontology for describing rights management activities.

The IPMP Components are the MPEG-21 version of the earlier "IPMP Extensions" developed for MPEG-4 [67], which provide the same functionality for MPEG-4 systems. Variants of the IPMP Components and MPEG REL are also used in the "Inter-operable DRM Platform" promulgated by the Digital Media Project [39].

3.3 Connected Inter-operability

The OMA DRM, Marlin, DVB-CPCM and SVP Alliance specifications all contain ad hoc provisions for importing or exporting protected information to or from other digital rights management systems. The Coral Consortium, however, defines a complete framework for connected inter-operability based on the *Networked Environment for Media Orchestration* ("NEMO") [19] (which is also used by Marlin). Coral's specification defines a series of *roles* such as *rights exporter*, *content mediator*, and so on, in terms of a set of services that a device must implement in order to play that role. If the vendor of a particular digital rights management system implements all of the necessary roles for that system, that system is then able to exchange rights and protected information with other digital rights management systems for which corresponding roles have been implemented.

3.4 Rights Expression Languages

Two widely-known languages of the kind described in Section 2.4 are:

- the Open Digital Rights Language ("ODRL") [83]; and
- the eXtensible Rights Markup Language ("XrML") [29], together with its close descendent the MPEG Rights Expression Language ("MPEG REL") [64].

3.4.1 ODRL

The Open Digital Rights Language is developed and promulgated by the ODRL Initiative as an alternative to proprietary languages. Version 1.1 of the language was released in 2002, and work on Version 2.0 was under way at the time of writing. A highly simplified form of Version 1.1 is used in the Open Mobile Alliance's digital rights management specification.

ODRL is structured as a set of *rights* to perform some *permission* over some *asset*. The rights may represent an *offer* to obtain the rights, or an *agreement* that the rights have been granted to some *party*. The permission may be associated with some *constraints* that restrict the conditions under which the permission is granted, and some *requirements* (re-named *duties* in working drafts of ODRL v2.0) that must be performed if the action is carried out.

In ODRL v1.1, all permissions are assumed to be denied unless they are granted by a rights document. Working drafts of ODRL v2.0, however, do not make this assumption and instead allow rights to contain *prohibitions* that explicitly prohibit actions.

Figure 5 shows an example ODRL v1.1 rights document. This document represents an agreement with Ernie Smith – identified by his X.500 directory entry – and allows him to make use of a resource identified as `doi:1.23456/video/0`, which is a collection of video trailers found at `http://www.sallys.com.au/trailers`. The agreement permits him to play the videos in the collection for a cumulative total of thirty minutes.

3.4.2 XrML and MPEG REL

The eXtensible Rights Markup Language is the direct descendent of the Digital Property Rights Language ("DPRL") [116], developed by Mark Stefik at Xerox very early in the history of digital rights management. Xerox later spun off XrML to a company known as ContentGuard. XrML, with some modifications, was standardised by the Motion Picture Experts Group ("MPEG") as ISO/IEC 21000-5. In this form it is known as the MPEG Rights Expression Language.

An XrML licence is structured as a collection of *grants* issued by some licence issuer. Each grant awards some *right* over some specified *resource* to a specified *principal*, that is, user of a resource. Each grant may be subject to a *condition*, such that the right contained in the grant may not be exercised unless the condition is satisfied. XrML conditions include both constraints that must be satisfied before an action is commenced, and obligations that are incurred by performing the action. All rights are denied unless they are explicitly permitted by a licence.

Figure 6 shows an example XrML grant for a scenario similar to the one we used for our ODRL example earlier. The grant is awarded to the principal who holds a private key corresponding an RSA public key given in the XML Signature format, and permits this principal to play videos identified as `urn:sallys.com.au:trailers` for a cumulative total of thirty minutes.

```
<o-ex:rights>
  <o-ex:agreement>
    <o-ex:party>
      <o-ex:context>
        <o-dd:uid>x500:c=AU;o=Registry;cn=Ernie Smith</o-dd:uid>
      </o-ex:context>
    <o-ex:asset>
      <o-ex:context>
         <o-dd:uid>doi:1.23456/video/0</o-dd:uid>
         <o-dd:dLocation>
           http://www.sallys.com.au/trailers
         </o-dd:dLocation>
      </o-ex:context>
    </o-ex:asset>
    <o-ex:permission>
      <o-dd:play>
        <o-ex:constraint>
          <o-ex:accumulated>30M</o-ex:accumulated>
        </o-ex:constraint>
      </o-dd:play>
    </o-ex:permission>
  </o-ex:agreement>
</o-ex:rights>
```

Figure 5: An ODRL v1.1 agreement.

```
<r:grant>
  <r:keyHolder>
     <r:info>
        <dsig:KeyValue>
          <dsig:RSAKeyValue>
            <dsig:Modulus>d5E73p==</dsig:Modulus>
            <dsig:Exponent>Aw==</dsig:Exponent>
          </dsig:KeyValue>
        </dsig:RSAKeyValue>
     </r:info>
  </r:keyHolder>
  <mx:play/>
  <mx:diReference>
    <mx:identifier>urn:sallys.com.au:trailers</mx:identifier>
  </mx:diReference>
  <sx:validityTimeMetered>30M</sx:validityTimeMetered>
</r:grant>
```

Figure 6: An XrML grant.

3.4.3 Other Approaches

While ODRL, XrML and their relatives are the most prominent rights expression mechanisms in the open literature, a number of other languages following similar principles have been proposed to meet the needs of particular industries, including

- the *Serial Copy Management System* ("SCMS") developed for managing copies of digital audio tapes;
- the *Picture Licensing Universal System* ("PLUS") [111] developed for use in the image licensing industry;
- the Creative Commons' "digital code" [34] for encoding usage and distribution rights for freely distributable works; and
- the *Automated Content Access Protocol* ("ACAP") [2] developed for communicating rights to Internet search engines.

Other approaches have been proposed in which permissions are checked by executing a set of instructions rather than by interpreting a statement of the rights that are available to a beneficiary.

In the *LicenseScript* language proposed by Chong, et al. [25], a licence is expressed as a triple of a resource, a set of *clauses* and a set of *bindings*. The bindings store the state information of the licence, such as the name of the beneficiary, the number of times a particular permission can be exercised, and so on. Each clause is a logical expression that, if true, permits some operation to be performed. When a user wishes to perform an operation, a licence interpreter executes a *query* on the relevent clause and, if the result is true, returns a new licence reflecting any changes to the bindings. For example, the new licence may have the available number of operations reduced by one compared to the original licence. Chong, et al. argue that LicenseScript is more expressive than ODRL and XrML.

The system proposed by the Marlin Joint Development Association uses "control objects" (equivalent to licences in our model) written in an executable bytecode language called *Plankton*. Each DRM agent contains a Plankton virtual machine, and each control object contains a series of Plankton routines that the DRM agent must execute in order to perform actions. For example, a control object for a movie might include a `Control.Actions.PLAY.Perform` routine that determines whether or not the DRM agent has permission to play the movie.

3.5 Other Components

Numerous other industry bodies have developed specifications for some component of a digital rights management system; for example,

- the Content Scrambling System ("CSS") [42] and Advanced Access Content System ("AACS") [5] are used on DVDs and HD-DVDs, respectively, to restrict playback of DVDs to approved DVD players;

- High-bandwidth Digital Content Protection ("HDCP") [38] is used to prevent high-definition signals from being captured between an audio decoder and speakers, or a video decoder and a display;
- Content Protection for Removable Media ("CPRM") [1] specifies a method for binding protected files to removable media; and
- Digital Transmission Content Protection ("DTCP") [40] specifies a method for protecting content transmitted over computer system buses.

4 Applications

4.1 Copyright Protection

Digital rights management was originally developed in order to control the distribution of copyrighted material through electronic channels. Publishing companies foresaw increasing network capacity and improving compression algorithms ushering in an era in which unprotected, high-quality music, video and other commercial publications could be freely distributed without recompense to the publisher.

Digital rights management addresses the problem by making licences the subject of trade, rather than the publication itself. While music, video and text files can be freely distributed in their protected forms, users wishing to make use of these files must purchase a licence enabling their DRM agent or authorised domain to access the file. Since licences cannot be transferred except within an authorised domain, the publisher is able to make sales commensurate with the number of people using their publications.

Publishers and retailers have used a number of different business models supported by digital rights management to varying degrees, and further models have been proposed by academic and other observers.

Pay-per-download. The pay-per-copy model used for physical media such as books, compact discs, etc. can be replicated in an electronic market by having a licence issuer create licences in return for a fee. The buyer must supply the identity of the DRM agent or authorised domain to which the licence is to be issued, together with the identifier of the multimedia work that he or she wishes to buy, and the rights that he or she wishes to obtain. The licence can then create a valid licence matching these identifiers, and transfer it to the buyer in exchange for payment.

Subscription. Subscriptions and compulsory licensing allow users to freely access some pool of multimedia works so long as they are paid members of a service. An obvious way to implement such services in a digital rights management model would be to make service members into the members of an authorised domain that is able to access all of the multimedia on offer. Another approach, which does not require devices to support authorised domains, is to allow the devices to download a licence with every song that they download, and have the licence expire at the end of the subscription period. Renewing the subscription causes the licences to be refreshed. Other proposals include mechanisms by which multimedia owners are compensated according to the

number of times their works are used or transferred within the domain [43], which can be done in a digital rights management model using a licence containing an obligation to report any use or transfer of the accompanying work.

Pay-per-play and rental. Highly-connected devices allow multimedia owners to charge for every individual use of their works (presumably at a considerably lower rate than what they would charge to purchase a copy outright). This can be done without digital rights management by streaming a copy of the work from a central server and using trusted computing techniques (see Section 5.1) to prevent the player from recording the stream to local storage. Digital rights management, however, allows a copy to be stored and used locally while payment is enforced by constraints or obligations in the licence. A strict pay-per-play model can be implemented by associating the licence with a payment obligation, or users can pre-purchase uses in the form of licences that are constrained to a fixed number of uses. Users can also rent works in the form of licences constrained to a fixed time period.

Try-before-you-buy. Multimedia creators often promote their works by allowing some limited access to their works without charge, in the hope that users will decide to purchase works that they like after being exposed to them. Sample items can be created in a digital rights management model in the form of a free licence constrained to a certain number of uses, or a fixed time period. If the user then decides to buy the work, he or she can purchase an unrestricted licence.

4.1.1 Computer Gaming and Copyrighted Software

Copyright protection has a long history in the computer software industry – notably for games – that has developed largely independently from digital rights management systems for music, video and other multimedia. Techniques have included

- providing a unique installation code with each legal copy of a piece of software, which must be entered during installation and registered with an on-line server;
- requiring the original installation media (floppy disk or CD), or a specially-made hardware "dongle", to be inserted into the computer in order to use the software;
- requiring the user to type in words or codes from a printed manual shipped with the game;
- distributing games on specialised hardware modules that are difficult to duplicate and can only be used on gaming consoles; and
- the use of centralised licence servers that require client software to regularly authenticate itself.

Digital rights management approaches of the kind described in this chapter can be applied to computer software in much the same way as they are to general multimedia works. The OMA Digital Rights Management standard for mobile devices [84], for example, can be applied to games on mobile devices. Very little technical information

is publicly available, however, about the proprietry systems used for protecting games on general computing platforms.

4.2 Enterprise DRM

The use of digital rights management to protect and track enterprises' sensitive information – known as "enterprise DRM" – has received considerably less attention than copyright protection in the open literature. Interest in this application is growing rapidly, however, and several enterprise DRM systems are now available on the market.

Enterprise proprietary information includes the intellectual property owned by the company, users' data and a range of documents that are used by employees. Traditional methods of access control, such as file encryption or database access control mechanisms, limit access to authorised employees of the company but do not provide protection against employees' misuse of their rights. An employee may illegally copy a file after it is decrypted, or transfer it outside the organisation or to another employee in the company who is not authorised to access the file, by sending it as an attachment to an email. Enterprise DRM systems address this problem by providing persistent protection of enterprise information.

Arnab and Hutchison [11] give a list of requirements for enterprise DRM based on the three most prominent systems on the market at the time (2005) – Microsoft's Rights Management Services [79], Authentica's Active Rights Management (since bought by EMC and re-named Documentum Information Rights Management [44]) and Adobe's LiveCycle [4]. These products allow users to restrict access to documents to authorised users; place expiry times on documents after which they cannot be accessed; prevent sensitive documents from being e-mailed out of the company; and so on.

Arnab and Hutchison identify

- persistent protection, that is, the fundamental requirement of all digital rights management systems that protected information cannot pass outside an ecosystem of trusted DRM agents;
- support for inter-company transactions; and
- portability, that is, the ability to access protected information in a variety of different locations, formats, and computing platforms.

as the top three requirements for an enterprise DRM system. They also identify requirements over and above those widely used in copyright protection systems, such as

- an "excerpt" right that allows a file to be broken into smaller pieces and inserted into different documents;
- transfer rights that enable companies to share their intellectual property with partner companies; and
- usage tracking to enable auditing and detect illicit activities.

The first two requirements appear to be challenging and have not been widely addressed in the open literature, while the latter is easier to implement but but may present a challenge to employees' privacy.

4.3 Privacy Protection

A number of authors have recognised for some time that there is a duality between protection of private information, and protection of copyrighted material: in both cases, we have a provider who wishes to make some information available to a third party in return for some financial reward or service, but does not wish to make the information publicly available [119, 70].

In a privacy protection context, the provider is a *data subject* whose privacy is at stake should an item of data be misused in some way. A *data user* may require access to the data for some purpose, such as completing a transaction requested by the data subject. In order to gain access to the data, the data user must obtain a licence from the licence issuer. Licences issued by the licence issuer are controlled in some way by the data subject, either directly or by having the issuer act according to a policy supplied by the data subject. The data user can then access the data according to the terms of the licence.

Early systems based on this principle enlisted the policy language defined by the Platform for Privacy Preferences ("P3P") [114] as a rights expression language [23, 24]. P3P is not designed to support automated enforcement, however, and later systems introduced hybrids of P3P and XrML [56, 93] or extended forms of MPEG REL [100]. Other DRM-like systems support very limited rights expressions using their own notation [22, 61].

The digital rights management model provides a straightforward way of implementing the "sticky policy" paradigm [69]. The sticky policy paradigm requires that private information be protected according to the policy that was in force at the time it was collected, even if the organisation that collected the data has since changed its policy, or the data has been transferred to another organisation. In a digital rights management approach, the sticky policy is simply a licence.

4.4 User-Generated Content

"User-generated content", that is, multimedia works produced and made available by non-commercial authors, has gained great prominence in recent years and presents a new environment in which digital rights management might be applied. The need for protection in user-generated content cuts across

- copyright protection for amateur (but possibly would-be professional) authors hoping to maintain some control over commercial use their work; and
- privacy protection for users of social networking sites who wish to maintain some control over the information that they make available on their web pages.

Digital rights management has not yet received much attention in this area, though Conrado, et al. have shown how one copyright-protection digital rights management

system might be extended for user-generated content [28]. The Creative Commons movement has also taken some steps towards introducing (copyright) rights management to non-commercial authors in the form of licences that can be expressed in digital code [34, 32], but little work appears to be done on the issue of enforcement of these licences.

4.5 Healthcare

Petković, et al. examine the potential for digital rights management technology in securing electronic healthcare records [87]. They argue that digital rights management technologies already provide many of the features desired in secure electronic healthcare system, but identify a number of points on which existing digital rights management systems (specifically, those originally designed for enterprise rights management) do not meet these needs, including:

- the parties that access and manipulate documents may come from many different domains and it is difficult to predict in advance who these parties might be;
- the ownership of data is not clearly defined, as it is shared between healthcare workers and patients;
- access rights are highly context-dependent and are difficult to determine automatically (for example, are we in an emergency situation?);
- small fragments of records (and not just whole documents, as is usually the case in copyright and enterprise protection) may be critical;
- the membership of roles can change very quickly;
- healthcare data may be used for research purposes in an anonymised form; and
- healthcare data is prone to numerous inference channels.

5 Implementing Digital Rights Management

5.1 Trusted Computing

The information owner in the digital rights management model wants to deliver information to an end-user who is not necessarily trusted with that information. Since the human user of the information is not trusted to behave in the way desired by the information owner, digital rights management requires some kind of trusted computing environment that prevents users of computer systems from tampering with the rights enforcement mechanism.

5.1.1 Code Obfuscation

Code obfuscation techniques attempt to transform a section of executable code into another section of code, such that the second code performs the same function as the first but cannot be understood by an attacker. A vendor can implement a trusted environment by only distributing the environment's code (or critical sections of it) in an obfuscated form. If attackers are unable to understand and modify this code, it can be trusted to perform the function for which it was designed.

Numerous techniques have been developed for obfuscating code; a comprehensive survey can be found in [118].

Many obfuscated pieces of software have been successfully reverse-engineered by attackers with sufficient time and skill, and in fact Barak, et al. have shown that it is not possible to construct a universal obfuscator in their "virtual black box" model [15]. Nonetheless, some positive results are also available in other settings [75, 115], and code obfuscation forms the basis of many practical digital rights management systems where other techniques are unavailable or too expensive.

5.1.2 Tamper-Resistant Hardware

A wide variety of hardware devices have been designed to provide a physical environment in which sensitive code can be executed without being observed or modified [6]. These kinds of devices are frequently used to implement digital rights management systems in consumer electronics devices, such as mobile phones and DVD players, and may have their security properties specified by the standards body responsible for the digital rights management system.

5.1.3 Operating System Support

While current commodity operating systems for general-purpose computers do not provide trusted computing environments suitable for use by digital rights management systems, researchers have proposed a number of methods by which such trusted computing features could be added to these kinds of systems (not only for the use of digital rights management systems).

Given the difficulty of completely securing a legacy operating system and all of the legacy applications that run upon it, trusted computing environments are typically implemented as a "security kernel" within the host operating system. The security kernel is isolated from the rest of the operating system and insecure applications, and may provide

- a range of primitives with which a trusted application can be built [45, 14]; or
- a complete trusted virtual machine [54, 108, 31].

The security kernel itself must be secured using a tamper-resistant hardware component such as a cryptographic co-processor or Trusted Platform Module, described in the next section.

5.1.4 The Trusted Computing Group

The Trusted Computing Group has proposed specifications for a hardware component known as a trusted platform module that provides support for verifying the integrity of a computer system [112]. The trusted platform module is a computer chip that cannot be easily removed or tampered with, and allows for the integrity of its host computer system to be checked and attested to.

The phrase "digital rights management" is conspicuously absent from the Trusted Computing Group's own literature, and some claim that the chips do not provide adequate physical security in the digital rights management context [92]. Nonetheless, many commentators believe that trusted platform modules are the beginning of a new era of hardware-based digital rights management systems [7, 51]; and a number of authors have proposed and/or implemented actual digital rights management and similar systems based on the trusted platform module [76, 90, 94, 104, 117]. Even if existing trusted platform modules do not provide sufficient levels of physical security for some digital rights management applications, it is easy to see how a secured module with the same functions could be used to produce a secure trusted environment.

The trusted platform module controls the start-up procedure of its host computer system in such a way as to ensure that the configuration of the system cannot be changed without being noted. For every piece of executable code used during start-up, the trusted platform module computes a "metric" that uniquely identifies that code, and stores it inside memory that cannot be accessed by software running on the host computer system. If a component of the host computer system is changed, its metric will also change.

The trusted platform module can attest to the configuration of its host computer system by providing its metrics and a proof that these metrics were computed by a trusted platform module. If a second computer system has access to a set of metrics that it believes to represent a trusted configuration of the first computer system, attestation can be used to check whether or not the first computer system is still in that configuration, or has been altered to be in some possibly malicious configuration.

5.1.5 Certification

The problem of determining whether or not a computing environment is a trusted one appears to have drawn little attention in the open literature. It is possible, in principle, to check the claim of a trusted computing using some public key infrastructure in which every trusted computing device is represented. However, there may be a number challenges in maintaining such an infrastructure [46]:

- By whom and by what procedure are components tested to ensure that they are suitably trustworthy?
- How will this procedure scale to thousands of components in millions of possible combinations?
- Will the need for authentication (possibly deliberately) impede inter-operability between components form different manufacturers?

5.2 Rights Negotiation

Many existing systems (whether based on digital rights management or other technologies) only allow for users to offer or obtain rights to information on a take-or-leave-it basis:

- in electronic commerce, a user can either purchase a given licence for the price offered, or not purchase one at all; or
- in the Platform for Privacy Preferences, a user can supply information to be governed by some given privacy policy, or not supply it at all.

Digital rights management, however, allows for more sophisticated models in which different sets of rights over a work might be offered for sale at different prices, or individual users might negotiate a distribution policy for an item of information according to their particular circumstances.

In the simplest case, a user might be offered a selection of a small number of pre-prepared "instant licences" that describe particular well-known modes of use [62]. In electronic commerce, for example, a work might be offered for sale under three different licences aimed at three different market segments: a basic usage licence for users who want to use the work for their personal enjoyment; a distribution licence for retailers who want to on-sell the work; or a composition licence for authors who want to incorporate the work into larger works.

This approach can be made more flexible by considering a prospective licence as a series of independent "instant grants" that can be accepted or rejected individually using checkboxes or similar mechanisms. In an electronic commerce scenario, each grant may represent some particular use of the object such as "the work may be used in advertising" or "the work may be printed", and be associated with an individual cost [98]. In a privacy scenario, each grant may represent whether or not the information owner wishes to be added to a mailing list, participate in research, etc. [100, 93].

More complex negotiation protocols allow the information provider and user to reach an agreement through several exchanges of offers and counter-offers [36, 10, 12]. The offers and counter-offers may be constructed by human negotiators (presumably using some tool for constructing machine-readable licences), or by automated software agents [106, 35, 53].

Existing rights expression languages do not contain explicit support for negotiation protocols. Arnab and Hutchison propose to extend the Open Digital Rights Language in order for it to express "requests", "offers", "acceptances" and "rejections" for particular sets of rights [12], so that it can be used as part of a negotiation protocol. Jamkhedkar, et al., however, argue that these primitives are better incorporated into an REL-agnostic negotiation protocol [66].

5.3 Rights Interpreters

Whether or not a given licence grants a particular permission in particular circumstances can be checked in a relatively straightforward way by constructing a logical model of the licence at run-time and executing a logical querying on it [58].

Rights expression languages, however, allow for very complex expressions to be built up by making the validity of one licence depend on the validity of another licence or other external piece of information. Authorised domains provide a simple example: a DRM agent that possesses a licence awarded to an authorised domain must check a second licence (or equivalent information) to see that it is a member of that authorised domain prior to using the licence.

Such chains of licences are particularly prominent in XrML and MPEG REL, where they are referred to as *authorisation proofs*. Given a user request to perform an action it is not, in general, obvious how the decision point might construct a valid authorisation proof, if it exists. Wiessman and colleagues argue that the problem of testing for the existence of an authorisation proof for a particular right given a set of licences is, in fact, undecidable for XrML [59] and NP-hard for ODRL [88] though polynomial-time algorithms exist for versions of both languages with some troublesome features removed.

Authorisation proofs can be constructed by inference engines or similar techniques [16, 107, 99]. Licences are represented as statements in some logic and an authorisation request is viewed as a theorem to be proved using those statements. The provers construct a proof in a series of steps in which the engine examines a claim and proceeds by attempting to prove all of the claims on which the current claim depends.

Proponents of the alternative rights expression methods embodied in Marlin and LicenseScript argue that reasoning about the XML-based languages is complex and expensive [25]. In their systems, licences are expressed in a procedural form that can executed by a Plankton (for Marlin) or Prolog (for LicenseScript) interpreter. The creators of LicenseScript, in fact, suggest that LicenseScript could be used as a compiled form of XrML or ODRL that would be more amenable to executation on small devices.

5.4 Supporting Technologies

5.4.1 Cryptography

The primary tools for securing distribution of electronic content are *encryption*, *message authentication codes (MAC)* and *digital signature* [78]. Encryption schemes are transformations applied to the message so that the message is concealed and is accessible only to those who have the correct *decryption key*. In DRM systems the encrypted content can be super-distributed and the decryption key be delivered as part of the license to a specific user.

MACs and digital signatures are two widely used cryptographic primitives that provide guarantee about message integrity and authenticity of origin, respectively. In MAC systems, sender abd receivers share a secret key. The sender uses their key to generate a short *authentication tag* or *cryptographic checksum* to the message. The tag is appended to the message and allows the receiver to verify authenticity of the message. In digital signatures, the signer has a pair of secret and public key and uses their secret key to generate a digital signature, which is a bit string appended to the message. A signed message can be verified by everyone using the public key of the signer. Digital signature guarantee that the message is generated by the signer.

Security of cryptographic systems relies on the security of cryptographic keys. Key distribution protocols are an integral part of all cryptographic systems.

Cryptographic schemes, although essential in securing distribution of content but cannot provide protection against illegal copy and cloning by authorised users.

5.4.2 Digital Watermarking

A *digital watermark* is a subliminal signal embedded into a file such that it can be detected or recovered only by a party in possession of a secret key [33]. In the context of intellectual property protection, there are three main ways in which digital watermarks are used:

- *proof-of-ownership*, in which the presence of an owner's watermark is used as evidence of the owner's claim to the work;
- *fingerprinting*, in which each legitimate copy of a published work is given a distinct watermark, and illicit copies are traced to their source by the presence of the culprit's fingerprint; and
- *captioning*, in which a watermark is used to convey information to a digital rights management system such as "do not copy this file".

Many watermarking algorithms have been proposed for still images, video and audio, in which there is relatively large scope for making small imperceptible changes to the host material. Fewer algorithms, however, are available for media such as text and computer software, where there is much more limited scope for altering the host material.

5.4.3 Content Hashing

A *content hash* (or *robust hash* is a characteristic code computed from an audio or video signal using a function such that (ideally) any two signals will have the same hash if and only if a human observer would identify the two signals as representing the same sound or video [21]. Content hashes are also known as *acoustic fingerints* or *video fingerprints*, but we will use the former term to avoid confusion with the watermark fingerprints described in the previous section.

Content hashes can be computed from a variety of "features" of a signal that vary between two genuinely different signals, but are not altered by routine signal processing operations such as compression, format conversion and filtering. Hashes created by information owners can be used to detect transfers or publications of sensitive signals even if the signals have been modified prior to transmission or publication.

5.4.4 Broadcast Encryption and Traitor Tracing

Broadcast encryption [52] is a cryptographic technique for providing efficient and secure access to content for an authorised group of receivers. The membership of the authorised group may change over time, for example, due to users obtaining or cancelling their subscriptions, or due to user being forcibly ejected from the group for

mis-behaviour. A message is encrypted by a *content key* that can be computed from a group members's private key together with a message broadcast by the group controller.

Broadcast encryption has obvious applications to key distribution in authorised domains and in conditional access systems, and is also widely used to restrict access to stored media (notably DVDs) to a set of approved players.

Traitor tracing systems provide protection against illegal copying and cloning of objects such as software, multimedia content or receiver devices. Protection is usually by "fingerprinting" the object to make it identifiable in such a way that a colluding group of users each having a fingerprinted version of the object cannot construct a new object with the same functionality of the original objects and untraceable to the colluding group [18, 26].

Broadcast encryption combined with traitor tracing allows the content to be delivered to the selected group of user (subscribers) while ensuring that that any illegal copy and redistribution can be traced to the colluding group.

6 Other Issues in Digital Rights Management

6.1 Copyright Exceptions

Copyright regimes typically include exceptions variously known as "copyright exceptions", "fair dealing" or "fair use" that allow users to make copies of a work for limited purposes without first obtaining the permission of the copyright owner. These exceptions include exceptions for making a small number of copies for personal use; making excerpts for a variety of purposes; and converting the work to another format.

Early digital rights management system made no attempt to allow for fair dealing of copyright material. While authorised domains now allow for some degree of personal copying, current digital rights management systems still struggle with fair uses such as excerpting and format-shifting. Some authors have proposed modifications to existing rights expression languages that would enable them to support at least some copyright exceptions [81], but others argue that it is all but impossible to codify legal exceptions into licences [50, 48]. Other authors have proposed systems in which users seeking to exercise an exception can

- appeal to an escrow authority [20, 47];
- negotiate for a special licence covering this use [10, 113]; or
- create a copy from which the user can be identified and prosecuted if the copyright owner deems the use to be unfair [82, 110].

None of these methods appear to have caught on in commercial systems, however.

6.2 Privacy Concerns

Digital rights management systems are inherently more invasive than traditional methods of content distribution [49, 27]. Users are generally required to reveal their identities and/or register their devices in order to access rights-managed content, and business models such as subscription and pay-per-play require users or devices to have an

on-going association with content providers. Although there is a strong security justification for registration and monitoring, but this will also allow the content providers to compile a profile for users' behavior and so breach of users' privacy.

Of course, many of these issues are not unique to digital rights management and apply to a wide variety of electronic commerce and other systems. Numerous "privacy-enhancing technologies" have been developed that attempt to address these issues (see [97], for example), however in practice other aspects and DRM systems such as interoperability and fair use have received wider attention.

6.3 Effectiveness

Opinions on the practical effectiveness of digital rights management systems have ranged from fears that digital rights management will usher in an era of unbreakable security that give vendors absolute control over all uses of digital information [8, 55], to dismissing all attempts at copy protection as doomed to ultimate defeat [95].

Realistically, as in other security systems, developers of digital rights management systems are engaged in a constant struggle with attackers. Developers may create a system that is initially thought to be secure, but after some time attackers may find a method of defeating the system. The developers may find a way of defeating the attack, only to have the new system defeated by another attack at a later date.

Digital rights management and related systems in the copyright protection arena, for example, have been subject to some high-profile defeats [73, 74, 89]. These attacks have generally been defeated by the next version of the system, which itself might be defeated by a another attack.

Several authors have proposed theoretical models that attempt to predict the behaviour of a market for rights-managed content in the presence of digital rights management systems and attackers. Biddle, et al. argue that "darknets" – notional rights-free networks into which rights-managed content is leaked due to a successful attack – are destined to remain a signficant force in content distribution [17]. They conjecture that the ability of a darknet to compete with rights-managed distribution networks depends on the the relative convenience and efficiency of the two networks, the moral behaviour of the networks' customers, and the popularity of the content involved (a darknet will favour more popular content because the incentive to attack such content is higher than it is for less popular content). Acquisti makes a similar argument based on a formal economic analysis [3]. Heileman, et al. use a game-theoretic approach to compare the outcome of various strategies used by content providers, and suggest that giving customers a positive incentive not to share content may be an effective, but currently under-utilised, tool to combat darknets [60].

Singleton uses the history of copy protection in computer games to argue that, even though such schemes have frequently been defeated, such schemes have nonetheless been effective in giving an advantages to protected content over unprotected content [103]. They do this by creating new business models (such as rental models), attracting greater investment than unprotected models, and by being more responsive to customer's needs than critics of digital rights management often contend.

6.4 DRM Patents

In additions to its other difficulties, the uptake of digital rights management systems has been hampered by disputes over the validity and cost of patents in the field. Probably the most prominent example is the stalled deployment of devices supporting the OMA DRM standard due to a dispute over licensing fees between the makers of these devices and the MPEG Licensing Authority, which claims to represent a number of patent owners in the digital rights management space [80].

While the designers of ODRL intend it to be freely available for any use, ContentGuard claims to own patents covering the use of rights expression languages to control the use of digital information [30]. ContentGuard claims they are owed royalties for the use of ODRL in addition to the use of their own rights expression language. The designers of ODRL dispute the validity of ContentGuard's patents [57] but, so far as we aware, ContentGuard's claims have never been tested in court.

7 Conclusion

Digital rights management allows access to an information item to be controlled over the entire lifetime of the item. It has well-established – albeit sometimes controversial – applications in protecting copyrighted multimedia works and corporate intellectual property, as well as promising applications in protecting privacy.

Important requirements of DRM systems are inter-operability and usability. This latter is in particular in the context of fair use and satisfying the need of users in real life application scenarios such as content sharing with friends. Standardisation which is an important step towards implementing inter-operable systems has proved a long, difficult and so far incomplete process. On the other hand designers have found it difficult to marry the rigid protection afforded by technical security systems with the convenience that everyday users expect.

The primary approach approach to DRM, that is using a license to describe the rights of the users and enforcing the license on a DRM agent, is motivated and best suited for traditional distribution models and in particular distribution of multimedia content. More complex content distribution systems may include many players, each having the role of provider and user of content at the same time. The relationship between these players and distribution of cost and financial gains among these players may require a careful re-thinking of DRM systems.

References

[1] 4C Entity. Welcome to 4C Entity. `http://www.4centity.com`, 2008.

[2] ACAP. Automated Content Access Protocol. `http://www.the-acap.org`, 2008.

[3] A. Acquisti. Darknets, DRM, and trusted computing: Economic incentives for platform providers. In *Workshop on Information Systems and Economics*, 2004.

[4] Adobe Corporation. Adobe LiveCycle enterprise suite. http://www.adobe.com/products/livecycle.

[5] Advanced Access Content System. AACS – Advanced Access Content System. http://www.aacsla.com, 2008.

[6] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov. Cryptographic processors – a survey. *Proceedings of the IEEE*, 94(2):357–369, 2006.

[7] R. J. Anderson. Trusted computing and competition policy – issues for computing professionals. *Upgrade*, pages 35–41, 2003.

[8] R. J. Anderson. 'Trusted computing' frequently asked questions. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html, August 2003.

[9] J.-P. Andreaux, A. Durand, T. Furon, and E. Diehl. Copy protection system for digital home networks. *IEEE Signal Processing Magazine*, 21(2):100–108, 2004.

[10] A. Arnab and A. Hutchison. Fairer usage contracts for DRM. In *ACM Workshop on Digital Rights Management*, pages 1–7, Alexandria, Virginia, USA, 2005.

[11] A. Arnab and A. Hutchison. Requirement analysis of enterprise DRM systems. In *Information Security South Africa*, 2005.

[12] A. Arnab and A. Hutchison. DRM use license negotiation using ODRL v2.0. In *Fifth International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*, 2007.

[13] A. Arnab and A. Hutchison. Persistent access control: A formal model for DRM. In *ACM Workshop on Digital Rights Management*, pages 41–53, 2007.

[14] A. Arnab, M. Paulse, D. Bennett, and A. Hutchison. Experiences in implementing a kernel-level DRM controller. In *Third International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution*, pages 39–46, 2007.

[15] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. In *CRYPTO*, pages 1–18, 2001.

[16] L. Bauer, M. A. Schneider, and E. W. Felten. A general and flexible access-control system for the Web. In *USENIX Security Symposium*, pages 93–108, 2002.

[17] P. Biddle, P. England, M. Peinado, and B. Willman. The darknet and the future of content protection. In *ACM Workshop on Digital Rights Management*, pages 155–176, 2002.

[18] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5):1897–1905, 1998.

[19] W. B. Bradley and D. P. Maher. The NEMO P2P service orchestration framework. In *Thirty-seventh Hawaii International Conference on System Sciences*, pages 290–299, 2004.

[20] D. L. Burk and J. E. Cohen. Fair use infrastructure for copyright management systems. *Harvard Journal of Law and Technology*, 15:41–83, 2001.

[21] P. Cano, E. Batlle, T. Kalker, and J. Haitsma. A survey of audio fingerprinting. *The Journal of VLSI Signal Processing*, 41(3):271–284, 2005.

[22] M. Casassa Mont, S. Pearson, and P. Bramhall. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. In *International Conference on Database and Expert Systems Applications*, pages 377–382, 2003.

[23] S.-C. Cha and Y.-J. Joung. Online personal data licensing. In *Third International Conference on Law and Technology*, pages 28–33, 2002.

[24] S.-C. Cha and Y.-J. Joung. From P3P to data licenses. In *Workshop on Privacy Enhancing Technologies*, pages 205–221, 2003.

[25] C. N. Chong, R. Corin, S. Etalle, P. H. Hartel, W. Jonker, and Y. W. Law. LicenseScript: A novel digital rights language and its semantics. In *Third International Conference on the Web Delivery of Music*, pages 122–129, Los Alamitos, USA, 2003.

[26] B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Transactions on Information Theory*, 46(3):893–910, 2000.

[27] J. E. Cohen. Overcoming property: Does copyright trump privacy? *University of Illinois Journal of Law, Technology and Policy*, pages 101–107, 2003.

[28] C. Conrado, M. Petković, M. van der Veen, and W. van der Velde. Controlled sharing of personal content using digital rights management. *Journal of Research and Practice in Information Technology*, (1):85–96, 2006.

[29] ContentGuard. Extensible Rights Markup Language. `http://www.xrml.org`, 2004.

[30] ContentGuard, Inc. Contentguard – licensing programs. `http://www.contentguard.com/licensing.asp`, 2006.

[31] A. Cooper and A. Martin. Towards an open, trusted digital rights management platform. In *ACM Workshop on Digital Rights Management*, pages 79–87, 2006.

[32] Copyright Clearance Center. Copyright clearance center launches Ozmo to help photographers, bloggers and other artists license content for commercial use. Press release, 19 November 2008.

[33] I. J. Cox, M. Miller, and J. Bloom. *Digital Watermarking: Principles and Practice*. Morgan Kaufmann, San Francisco, California, USA, 2001.

[34] Creative Commons. Creative commons. http://creativecommons.org, 2008.

[35] J. Delgado, I. Gallego, García, and R. Gil. An architecture for negotiation with mobile agents. In *Mobile Agents for Telecommunications Applications*, pages 21–31, 2002.

[36] J. Delgado, I. Gallego, and X. Perramon. Broker-based secure negotiation of intellectual property rights. In *Information Security Conference*, pages 486–496, 2001.

[37] Digital Cinema Initiatives, LLC. Digital cinema system specification, 2008.

[38] Digital Content Protection LLC. High-bandwidth Digital Content Protection. http://www.digital-cp.com, 2008.

[39] Digital Media Project. The interoperable DRM platform. http://www.dmpf.org/specs/index.html, 2008.

[40] Digital Transmission Licensing Administrator. Digital Transmission Licensing Administrator. http://www.dtcp.com, 2007.

[41] Digital Video Broadcasting. Copy protection & copy management specification. DVB Document A094 Rev. 2, 2008.

[42] DVD Copy Control Association. Welcome to the DVD CCA website. http://www.dvdcca.org, 2007.

[43] Electronic Frontier Foundation. A better way forward: Voluntary collective licensing of music file sharing. http://www.eff.org/wp/better-way-forward-voluntary-collective-licensing-music-file-sharing, 2008.

[44] EMC. EMC IRM services. http://www.emc.com/products/detail/software/irm-services.htm, 2008.

[45] P. England, B. Lampson, J. Manferdelli, M. Peinado, and B. Willman. A trusted open platform. *IEEE Computer*, pages 55–62, July 2003.

[46] J. S. Erickson. OpenDRM: A standards framework for digital rights expression, messaging and enforcement. In *NSF Middleware Initiative and Digital Rights Management Workshop*, 2002.

[47] J. S. Erickson. Fair use, DRM and trusted computing. *Communications of the ACM*, 46(4):34–39, 2003.

[48] J. S. Erickson and D. K. Mulligan. The technical and legal dangers of code-based fair use enforcement. *Proceedings of the IEEE*, 92:985–996, 2004.

[49] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack. Privacy engineering for digital rights management. In *ACM Workshop on Security and Privacy in Digital Rights Management*, pages 153–163, 2001.

[50] E. W. Felten. A skeptical view of DRM and fair use. *Communications of the ACM*, 46(4):52–56, 2003.

[51] E. W. Felten. Understanding trusted computing – will its benefits outweigh its drawbacks? *IEEE Security and Privacy*, pages 60–62, May-June 2003.

[52] A. Fiat and M. Naor. Broadcast encryption. In *CRYPTO '93*, pages 480–491, 1993.

[53] Y. Gang and T.-Y. Li. A decentralized e-marketplace based on improved Gnutella network. In *International Conference on Intelligent Agents, Web Technology and Internet Commerce*, 2003.

[54] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: a virtual machine-based platform for trusted computing. *ACM SIGOPS Operating Systems Review*, 37(5):193–206, 2003.

[55] J. Gilmore. What's wrong with copy protection. `http://www.toad.com/gnu/whatswrong.html`, 16 February 2001.

[56] C. A. Gunter, M. J. May, and S. G. Stubblebine. A formal privacy system and its application to location based services. In *Workshop on Privacy Enhancing Technologies*, pages 256–282, 2004.

[57] S. Guth and R. Iannella. Critical review of MPEG LA software patent claims. *Indicare Monitor*, 22 March 2005. `http://www.indicare.org/tiki-read_article.php?articleId=90`.

[58] S. Guth, G. Neumann, and M. Strembeck. Experiences with the enforcement of access rights extracted from ODRL-based digital contracts. In *ACM Workshop on Digital Rights Management*, pages 90–102, 2003.

[59] J. Y. Halpern and V. Weissman. A formal foundatinon for XrML. *Journal of the ACM*, 55(1), 2008.

[60] G. L. Heileman, P. A. Jamkhedkar, J. Khoury, and C. J. Hrncir. The DRM game. In *ACM Workshop on Digital Rights Management*, pages 54–62, 2007.

[61] J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *International Conference On Mobile Systems, Applications And Services*, pages 177–189, 2004.

[62] R. Ianella. Supporting the instant licensing model with ODRL. In *Fifth International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*, 2007.

[63] International Standards Organisation. Information technology – multimedia framework (MPEG-21) – part 4: Intellectual property management and protection components. ISO/IEC 21000-4:2006.

[64] International Standards Organisation. Information technology – multimedia framework (MPEG-21) – part 5: Rights expression language. ISO/IEC 21000-5:2004.

[65] International Standards Organisation. Information technology – multimedia framework (MPEG-21) – part 6: Rights data dictionary. ISO/IEC 21000-6:2004.

[66] P. A. Jamkhedkar, G. L. Heileman, and I. Martínez-Ortiz. The problem with rights expression languages. In *ACM Workshop on Digital Rights Management*, pages 59–67, 2006.

[67] M. Ji, S. M. Shen, W. Zeng, T. Senoh, T. Ueno, T. Aoki, Y. Hiroshi, and T. Kogure. MPEG-4 IPMP extension for interoperable protection of multmedia content. *EURASIP Journal on Applied Signal Processing*, 2004(14):2201–2213, 2004.

[68] M. A. Kaplan. IBM Cryptolopes, superdistribution and digital rights management. `http://researchweb.watson.ibm.com/people/k/kaplan/cryptolope-docs/crypap.html`, 1996.

[69] G. Karjoth, M. Schunter, and M. Waidner. The Platform for Enterprise Privacy Practices: Privacy-enabled management of customer data. In *Workshop on Privacy Enhancing Technologies*, pages 69–84, 2002.

[70] S. Kenny and L. Korba. Applying digital rights management systems to privacy rights. *Computers & Security*, 21:648–664, 2002.

[71] R. H. Koenen, J. Lacy, M. Mackay, and S. Mitchell. The long march to interoperable digital rights management. *Proceedings of the IEEE*, 92:883–897, 2004.

[72] P. Koster, F. Kamperman, P. Lenoir, and K. Vrielink. Identity based DRM: Personal entertainment domain. In *IFIP Conference on Communications and Multimedia Security*, pages 42–54, 2005.

[73] Lemuria.org. DeCSS central. `http://www.lemuria.org/DeCSS/main.html`.

[74] J. Leyden. MS preps DRM hack fix. *The Register*, 31 August 2006. `http://www.theregister.co.uk/2006/08/31/wm_drm_crack/`.

[75] B. Lynn, M. Prabhakaran, and A. Sahai. Positive resultsand techniques for obfuscation. In *EUROCRYPT*, pages 20–39, 2004.

[76] J. Marchesini, S. W. Smith, O. Wild, J. Stabiner, and A. Barsamian. Open-source applications of TCPA hardware. In *Annual Computer Security Applications Conference*, Tucson, USA, 2004.

[77] Marlin Developer Community. Marlin – core system specification version 1.2. `http://www.marlin-community.com`, 12 April 2006.

[78] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, Florida, USA, 1997.

[79] Microsoft Corporation. Windows Server 2003 Rights Management Services. `http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx`, 2005.

[80] Mobile Europe. Digital rights management? *Mobile Europe*, 26 April 2005. `http://www.mobileeurope.co.uk/news_analysis/111138/Digital_rights_mismanagement%3F.html`.

[81] D. Mulligan and A. Burstein. Implementing copyright limitations in rights expression languages. In *ACM Workshop on Digital Rights Management*, pages 137–154, 2002.

[82] C. Neubauer, F. Siebenhaar, and K. Brandenburg. Technical aspects of digital rights management systems. In *AES Convention 113*, Los Angeles, California, USA, 2002. Paper 5688.

[83] Open Digital Rights Language Initiative. The Open Digital Rights Language Initiative. `http://odrl.net`, 2004.

[84] Open Mobile Alliance. Digital rights management working group. `http://www.openmobilealliance.org/Technical/DRM.aspx`, 2008.

[85] Organization for the Advancement of Structured Information Standards. OASIS eXtensible Access Control Markup Language TC. `http://www.oasis-open.org/committees/xacml/`, 2004.

[86] F. Pestoni, J. B. Lotspiech, and S. Nusser. xCP: Peer-to-peer content protection. *IEEE Signal Processing Magazine*, 21(2):71–81, 2004.

[87] M. Petković, S. Katzenbeisser, and K. Kursawe. Rights management technologies: A good choice for securing electronic health records? In *Securing Electronic Business Processes*, pages 178–197, 2007.

[88] R. Pucella and V. Weissman. A formal foundation for ODRL. Technical Report arXiv:cs/0601085v1, arXiv, 2006.

[89] B. Rosenblatt. iTunes hacked, then hacked again. *DRMWatch*, 24 March 2005. `http://www.drmwatch.com/drmtech/article.php/3492676`.

[90] A.-R. Sadeghi and C. Stüble. Towards multilateral-secure DRM platforms. In *Information Security Practice and Experience Conference*, pages 326–337, 2005.

[91] R. Safavi-Naini, N. P. Sheppard, and T. Uehara. Import/export in digital rights management. In *ACM Workshop on Digital Rights Management*, pages 99–110, 2004.

[92] D. Safford. The need for TCPA. White paper, IBM, 2002. `http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf`.

[93] F. Salim, N. P. Sheppard, and R. Safavi-Naini. Enforcing P3P policies using a digital rights management system. In *International Workshop on Privacy Enhancing Technologies*, pages 200–217, Ottawa, Ontario, Canada, 2007.

[94] R. Sandhu and X. Zhang. Peer-to-peer access control architecture using trusted computing technology. In *ACM Symposium on Access Control Methods and Technologies*, pages 147–158, 2005.

[95] B. Schneier. The futility of digital copy prevention. *Crypto-Gram Newsletter*, 15 May 2001.

[96] Secure Video Processor Alliance. SVP open content protection system: Technical overview. `http://www.svpalliance.org/docs/e2e_technical_introduction.pdf`, 3 January 2005.

[97] V. Seničar, B. Jerman-Blažič, and T. Klobučar. Privacy-enhancing technologies—approaches and development. *Computer Standards & Interfaces*, 25(2):147–158, 2003.

[98] C. Serrão and J. Guimarães. Protecting intellectual property rights through secure interactive contract negotiation. In *European Conference on Multimedia Applications, Services and Techniques*, pages 493–514, 1999.

[99] N. P. Sheppard. On implementing MPEG-21 intellectual property management and protection. In *ACM Workshop on Digital Rights Management*, pages 10–22, Alexandria, Virginia, USA, 2007.

[100] N. P. Sheppard and R. Safavi-Naini. Protecting privacy with the MPEG-21 IPMP framework. In *International Workshop on Privacy Enhancing Technologies*, pages 152–171, Cambridge, UK, 2006.

[101] N. P. Sheppard and R. Safavi-Naini. Sharing digital rights with domain licensing. In *ACM Workshop on Multimedia Content Protection and Security*, pages 3–12, Santa Barbara, USA, 2006.

[102] O. Sibert, D. Bernstein, and D. van Wie. Digibox: A self-protecting container for information commerce. In *First USENIX Workshop on Electronic Commerce*, 1995.

[103] S. Singleton. Copy protection and games: Lessons for DRM debates and development. Progress on Point 14.2, Progress & Freedom Foundation, February 2007.

[104] S. Stamm, N. P. Sheppard, and R. Safavi-Naini. Implementing trusted terminals with a TPM and SITDRM. *Electronic Notes in Theoretical Computer Science*, 197(1), 2008.

[105] M. Stefik. *The Internet Edge: Social, Legal and Technological Challenges for a Networked World*. MIT Press, 1999.

[106] S. Y. W. Su, C. Huang, J. Hammer, Y. Huang, H. Li, L. Wang, Y. Liu, C. Pluempitiwiriyawej, M. Lee, and H. Lam. An internet-based negotiation server for e-Commerce. *The VLDB Journal*, 10(1):72–90, 2001.

[107] C. H. Suen. Efficient design of interpretation of REL license using expert systems. In *Computer Communications and Networking Conference Workshop on Digital Rights Management Impact on Consumer Communications*, 2007.

[108] G. E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas. AEGIS: Architecture for tamper-evident and tamper-resistant processing. In *Internatioanl Conference on Supercomputing*, pages 160–171, 2003.

[109] Sun Microsystems, Inc. Open Media Commons. `http://www.openmediacommons.org`, 2008.

[110] Sun Microsystems Laboratories. Support for fair use with project DReaM. White Paper Version 1.0 RevA, 2008.

[111] The PLUS Coalition, Inc. PLUS: Picture Licensing Universal System. `http://www.useplus.org`, 2007.

[112] The Trusted Computing Group. Trusted Computing Group: Home. `http://www.trustedcomputinggroup.org`, 2005.

[113] P. Tyrväinen. Concepts and a design for fair use and privacy in DRM. *D-Lib Magazine*, 11(3), 2005.

[114] W3 Consortium. Platform for Privacy Preferences (P3P) project. `http://www.w3.org/P3P`, 2004.

[115] H. Wee. On obfuscating point functions. In *ACM Symposium on Theory of Computing*, pages 523–532, 2005.

[116] Xerox Corporation. The Digital Rights Property Language: Manual and tutorial – XML edition. `http://www.oasis-open.org/cover/DPRLmanual-XML2.html`, 1998.

[117] X. Zhang, J.-P. Seifert, and R. Sandhu. Security enforcement model for distributed usage control. In *IEEE International Conference in Sensor Networks, Ubiquitous and Trustworthy Computing*, pages 10–18, 2008.

[118] W. Zhu. *Concepts and Techniques in Software Watermarking and Obfuscation*. PhD thesis, University of Auckland, New Zealand, 2007.

[119] J. Zittrain. What the publisher can teach the patient: Property and privacy in an era of trusted privication. *Stanford Law Review*, 52, 2000.