

Introduction to Digital Rights Management

by: LockLizard, 07/13/2005

<http://www.securitydocs.com/library/3461>

Introduction

Most people have heard of software licensing and pay per view television, but possibly not connected it with a development in technology called Digital Rights Management (DRM). To understand what DRM is trying to achieve you first of all need to understand intellectual property.

Intellectual property

To understand digital rights you need to remember that books, plays, pictures, films and so on (including this paper) are subject to copyright or intellectual property rights. By international agreements such as the Berne Convention countries recognize these rights and provide a framework that allows copyright holders to have uniform rights in different countries and to be able to enforce them. Whenever you buy a book, hear a modern recording played on television or see a film a payment is being made to the copyright holders of the work.

You will find significantly more detail on intellectual property rights (IPR) on the web site <http://www.wipo.int/>. The site provides a comprehensive information resource about the work of the World Intellectual Property Organization (WIPO).

Now intellectual property rights were important in the book and film trades, but television, DVD, computer software and computer games have had such a significant effect on world trade that the World Trade Organization (WTO) has a special section of its activities devoted to dealing with intellectual property rights called Trade-Related aspects of Intellectual Property Rights (TRIPS) and more information on the world negotiations are at http://www.wto.org/english/tratop_e/trips_e/trips_e.htm.

You can gather from this that several industries consider intellectual property to a very big deal indeed.

Demand for digital rights management

So now when we talk about digital rights management we are talking about works of intellectual property that are processed by digital computers (or even analogue ones).

There are many many industries producing copyright works that are held on and processed by computers. That includes anything processing cassette tapes, VCR, CD-ROM, DVD, flash cards and so on. There are even laws that create rights in databases as collections of information.

The copyright holders (owners) found that the original computer systems, broadcast television and cassette tapes, records and VCR machines made no attempt to stop people from copying their work and even selling it on with the owner getting paid the royalty that IPR law gave them. This started in the late 1980's, and grew significantly with the introduction of music standards such as MP3 which did not prevent copying, but did make mass market copying very easy.

Other owners selling 'expensive' works such as financial analyses of companies or markets found that people would purchase one copy and then make copies of it to pass on to their friends for free. When the reports were printed they were photocopied, but making them digital made the copying easier and faster.

The IT industry saw a massive opportunity to be able to make significant amounts of money if they could find one or more ways to control what the person who had licensed a digital work (when you buy a book in theory you license it, and the same goes with a picture or a photograph) did with it.

DRM controls as against IT controls

Obviously the things that you would want to control were any form of access and use, and particularly to prevent any attempt to remove the controls.

So controls often provided are:

- reading the item
 - number of times
 - start and end dates for reading
- printing the item
 - at all
 - poor quality printing
 - number of copies
- altering the item
 - changing information content
 - removing copyright marks
- copying the item
 - making copies others can use
 - copying parts of the work
 - taking screen dumps as copies
- running the item as a program
 - running the item on one computer
 - only allowing one user to run the item
 - limiting the number of CPUs the item may use

These controls are a long way from the original IT type controls on files which (for those not instantly familiar with them) still are:

- read
- write
- append
- delete
- execute

Now as you can see, it's quite a different list of controls with quite a significant impact.

DRM and charging mechanisms

When DRM systems first came out there was a strong move to be able to license significant amounts of the information found on the Internet, and to charge for every conceivable use of an item, as well be able to pass on enforceable rights from one rights holder to another.

Original owners were also to be recompensed through micro-payments mechanisms that would transfer their proportion due each time an aspect of their work was sold/licensed. This was proposed so that owners would receive an accurate payment for use.

Did that make it work?

Well, this is where the detail gets a bit more complicated.

The only mechanism that computer systems have for enforcing controls when the computer operating system is not in control (which is almost all the time with the Internet) is encryption. If you don't encrypt (make secret) the thing you are trying to protect then your (lack of) protection mechanism will soon be detected and either all the works you were trying to protect will suddenly become freely available on the web (as happens more often than you might think) or they will be shared amongst private groups of users freely.

Now encryption requires a number of disciplines if it is going to be successful. It also imposes quite an overhead on a system. For instance, whilst the user would not worry about the time it takes to decrypt a file (say a document, spreadsheet, .pdf file) because the amount of information is in reality quite small, but if they are waiting for the decryption of streaming video or voice the heavy encryption currently used can harm performance. Certainly the average DVD would not perform well using a PC to decrypt all its information using, say triple DES.

Encryption also requires the control of cryptographic keys. Some people who have installed or re-installed Microsoft Windows will have typed in a long series of letters and numbers (a.k.a. a cryptographic key). But DRM system often require you to be in contact with a server that is monitoring user requests and comparing them with dynamically imposed controls (such as continuing to subscribe to a service).

Cryptography allows strong controls, but it also imposes overheads and technical difficulties.

The early DRM systems failed simply because they were too expensive for the amount of money they could reasonably collect. This idea of cost may sound rather strange, but the cost of mounting the servers, the processing overhead and the amount of connectivity required to operate those systems was simply too much compared to the amount of money they could realistically collect.

Can you make it work?

Cryptography can work effectively in a number of situations. But at the moment, micro-payments simply isn't one of them. Using cryptography to control the actions of a user who has paid a substantial amount of money for the product will work where micro-payments will not.

Cryptography will let you control a number of events. But it depends upon how effective your cryptography is. A number of disasters have already overtaken those who either chose to implement poor algorithms or failed to understand that you have to do something significantly better than password protection if you are going to protect something that has significant value for your business. It is not necessary for this paper to do more than state that many of the 'industry standard' solutions failed to recognize the real management issues of cryptography and therefore failed to provide the protection that they seemed to claim.

Later solutions to DRM implementation have been more successful. Although it is fair to note that right owners need to think through what it is that they are licensing their customers for. And to make sure that their licensing is consistent with current international agreements. (Issues of international rights are the subject of a separate paper.)

Moving forwards

Decoupling DRM from micro-payments has enabled a more effective control suite to be provided that on the one hand supports industry objectives and on the other hand is acceptable to users. Users were not willing to work on the basis of micro-payments, but are more willing to buy a service that is delivered over a period of time.

It seems, from current market feedback, that whilst users do not like restrictions on their ability to share information with others, and to have it locked down to a specific computer, they will accept those kinds of limitations. What they are not happy about are situations where they have to be online to remote servers before they are able to use information that, as far as they are concerned, they have purchased, and should be able to access at any time, and for all time.

These requirements are at odds with the ideas of the 'pay per view' community from the record and film industries, who see a massive market opportunity if they can charge for each and every use of an item as against having sold it to a customer for permanent use. (In other words they may prefer the model of the DVD/Video shop to that of the customer buying a the item and being able to use it forever thereafter.)

Conclusion

DRM offers industry information providers, which include the financial industries, analysts, consultants, programmers (applications, games) database owners and so on, as well as the record and film industries, with significant potential. DRM significantly extends the old IT controls and provides a much finer grained control over the ability of the user to make use of an item.

Attempts to link finer grained control to micro-payments controls has not been successful so far, and may prove to be unattainable in the longer term because the cost of operating the mechanism exceeds the possible income per transaction. Speculation that web costs are zero may be correct for the end user, but studies have demonstrated that information service providers actually pay to have their information made available on the web.

The correct mechanism to implement DRM will vary significantly with the delivery requirement. Services that require high speed decryption still need to be implemented in hardware if they are to work in an online situation. Realtime services can only be delivered using dedicated hardware, and owners requiring this service should be aware of this limitation.

About LockLizard

[LockLizard](#) produces high quality, US government strength content encryption products with digital rights management controls that protect your intellectual property from unauthorized use and misuse.