Did you know that DRM is a security mechanism?

Introduction

Mention DRM in the airport lounge or on a commuter train, and you get the kind of look usually reserved for people that don't clean up after their dog. And maybe that's no surprise. But there's more to the use of DRM than commonly meets the eye.

Historical development

Now I know that people tend to follow Henry Ford and say that "History is bunk," but reality is that if you don't understand how it is we got here then you are faced with having to invent something totally new, and whilst the IT industry has specialised in doing that, the magic is wearing thin and customers are increasingly unwilling to jump into a whole new technology when they have not even begun to eat what is on their plate right now.

So, a bit of history.

The DRM agenda has been both set and dominated by the music and film industries for as long as CD technology has been available (arguably since 1978 when Philips released the first video disk player, although the standard was not sorted out until 1981 and mass sales only started in 1983).

The reason those industries were interested was because their anticipated profits had been burned by the cassette tape recorder (readily available in the mid 1960s) that made copying music and sound trivial (although, from my memory, the sound quality left only hi-fidelity to be desired).

Personal Computers of the IBM type had only just been invented (1981) and that type of computing did not become available to the mass markets until around 1985 with the Amstrad, Sinclair, Apple and so on joining the fray. For the new boys on the block, the wonder was to make it work at all - certainly not to worry about some theoretical loss of revenue from failing to collect the royalty on a song or an orchestral work.

So DRM technology was relegated in the minds of both consumers and IT designers as some strange delusion of the music industry that was really all about increasing profits from record, and later film sales.

Access controls and DRM

And that is where the misunderstanding began.

If you look back at access control mechanisms in the days of the mainframe computer you just had a few: read (includes copy), write (includes create), append (includes add to and alter), execute, delete. That was because there was an administrator on the mainframe who probably knew who you actually were, set up your identity and password and 'decided' which rights you had over which files.

Now that was fine at the time, because life was simple, very few people actually got to be able to get to anything and the systems programmers could always fix the errors because mainly nobody except them had serious access to anything at all. The only 'stuff' to leave the mainframe would likely be printed on paper, or maybe on a magnetic tape, and both were controlled physically. Your chance of making copies was about the same as winning the lottery.

Enter the personal computer era.

The real selling point of the PC was the fact that the user was king – they did not have to bow and scrape with the systems programmers, they could do anything they wanted. In fact, each one became the equivalent of a systems programmer.

And PC users had just the same access controls as were on the mainframe, with all the power that went with them. And basically nothing has changed since. The PC is bigger, faster, more interconnected than we ever thought possible in 1981, but the development of access controls has not kept pace with everything else.

And finally governments, industry and users are waking up to the fact that they need more powers to control how information is disseminated and used. Because the original access controls just don't cut it. In some cases they want to allow recipients to read information, but not to be able to copy it. In some cases they want to limit the ability to copy, perhaps allowing only printed copies and not digital. In other cases they may want to be able to track if people are re-distributing their information in a printed form.

If you were to think of it as updating access controls you might get a table something like the following:

Original Control	**Added controls**
Read	Read but not copy
	Read for a number of times
	Read and make printed copy(ies)
	Read showing ownership
	Print showing ownership
Write	Write but not as original author

Append	Allow original to be altered Allow additions that are shown separately
Delete	Delete
Execute	Execute if on an authorised location

Now these additional controls are identical to those used to achieve DRM management of information. The only addition needed, is a more sophisticated method for being able to check that the entity (person, machine and so on) using the information has a tick in the box for the control(s) for them and that it is valid.

Now that's not much of a step on from ticket granting systems that were designed and developed using a technology called Kerberos, which started back in the late 1980s.

So DRM technology, rather than being some evil regime, turns out to be an extension of access control technologies that were developed back in the 1960s, and are just starting to be understood as necessary extensions in order to address the now extended controls required for Internet based computing.