



Document DRM: Replacing Encryption as the Standard for Document Protection

Author: DR Stephen Hitchen

Dr Hitchen has designed award winning access control, encryption and DRM devices over the past 20 years

Introduction

Corporate intellectual property and other sensitive information is generally created and maintained in the form of electronic documents. Encryption is routinely used to protect this information against unauthorised access during storage and transfer (*e.g.* by email). While encrypted, the protected information, or content, is essentially immune to unauthorised access. It may seem, therefore, that the application of modern encryption software provides perfectly adequate protection of such information. However, such a view is superficial – in essence it focuses on only one aspect of securing sensitive information.

Out of traditional encryption and DRM techniques has evolved a new generation of DRM software ideally suited to the task of securing the content of documents in a modern business context. This software is known as document DRM (dDRM) or Enterprise Rights Management.

In this article, it is argued that dDRM has rendered traditional encryption, as a method for protecting information in documents, obsolete and that dDRM will become the new standard for protecting electronic documents in general.

Securing Content, NOT Files

The key part of any electronic document or file is the information contained within it, i.e. the *content*. Protecting the content is not the same as protecting the file itself; for example content can be deleted without deleting the file.

Files can be protected against unauthorised access, deletion, *etc*, through access control mechanisms. However, the content of a file is much more difficult to secure, especially while in use by an authorised user.

It is protection of the content of electronic documents that is addressed in this article.

Encryption for Protection of Document Content

Encryption is employed routinely to protect document content during:

- a. Storage. For example: Windows 2000 encrypted file system, virtual drive encryption, *etc*.
- b. Transfer. For example: Email using PGP, Internet using SSL.

From its widespread use it may seem that encryption affords strong protection against unauthorised access to document content. However, in reality, the use of encryption alone presents serious shortcomings for content protection, particularly in a modern business environment:

- Perhaps the main defect of encryption for content protection is that the security issues that it solves are minor compared to those raised by the misuse of content *while it is in use by authorised users*. There is a weight of evidence to support the assertion that most electronic information theft (or accidental leaks) from organisations, arises from internal sources and it can be assumed that at least a substantial proportion of these incidents involve *authorised* users. In other words, this major source of corporate data loss cannot be addressed by the use of encryption alone.
- Encrypted storage only protect information while documents are actually in the store – to maintain protection, movement of documents must be restricted to ensure that they are not moved or copied to unprotected locations. Except, perhaps, for personal documents such limitations may either be impossible to adhere to, or conflict with the requirements of modern business practice, which tends towards collaboration on document content.

With collaboration, especially if this involves users external to the organisation, it will be difficult or impossible to ensure that protected storage is used; this may either inhibit collaboration or lead to the security requirement being opening or tacitly dropped – in which case the original security, applied by the content owner, is redundant.

- Encryption during document transfers (*e.g.* email) only protects content during the transfer itself – once documents have been received, by the authorised recipient, there is no guarantee that the content will remain protected. Also, it is debatable that deliberate interception of emails is a significant security risk to corporate data, owing to the limited opportunities for interception.
- With a shared document, encryption cannot prevent other users of the document from accidentally or deliberately misusing the content, *e.g.* by copying some or all of the content and forwarding to third parties, printing the content for unauthorised use, *etc.*
- Access to content cannot be restricted by date/time.
- Encryption cannot prevent users from making unauthorised modifications to content. Although modifications can be detected through the use of digital signatures, from a user experience perspective it is better to prevent such changes in the first place.

Overall the issues noted above make the use of encryption for content protection very limited in scope. A crucial problem is that encryption affords no control over the content once it is in use – an essential requirement for content security. The use of encryption to secure content may therefore lead to a sense of false security.

It may be considered that the comments noted above are contradicted by the widespread use of encryption to protect document content: why else would the use of encryption for documents be so common? However, encryption is commonly used to protect personal documents and also some other situations where documents are unshared and / or the user can be completely trusted. Another significant factor is that, until recently, there have been no practical alternatives to encryption, and so it has tended to be applied regardless of its suitability.

Document DRM

Document DRM (dDRM) is the application of access and digital rights controls (such as restrictions to copying content, printing, editing, *etc*) to the content of documents (*e.g.* Microsoft Word documents).

Content is encrypted, and digital rights controls are applied on top of this by various means, making dDRM at least as secure, in principle, as encryption for securing content against unauthorised access.

Software with these capabilities have been available for sometime, but these early generation products are of limited practical use for one or more of the following reasons:

- Documents cannot be protected as they are created. Instead a separate protection step is required to convert the document to a protected form, leaving the original content unprotected.
- Editable (in progress) documents cannot be protected – leaving document content unprotected during its creative stages.
- Changes are required to the way in which protected documents are accessed, *e.g.* they must be opened through Internet Explorer or require the use on non-standard commands if opening form within an application.
- Exhibit poor security, with temporary files, the system paging file, *etc* left unencrypted.
- Are not resistant to tampering, *e.g.* the use of system level debuggers to defeat DRM controls.
- Limited access control authentication options, *e.g.* no support for digital certificates.
- Inflexible architecture – generally server based and requiring on-site configuration.
- Complex set-up and management.
- Intrusive, making usability poor.

New Generation DRM Software

Responding to the lack of a practical dDRM solution that addresses the requirement of protecting corporate intellectual property contained in documents during their formative stages, collaborative documents, etc., the latest generation of dDRM software evolved with the following characteristics:

- Protection can be applied as documents are created; ensuring that content is protected at all stages of a document's development.
- Content owners work completely normally with documents containing protected content.
- Other users also work normally with protected content except where access control or digital restrictions are encountered.
- Content is protected with on-the-fly encryption of files holding protected content, temporary files, and the system paging file.
- Complete transparency in operation – users are not required to make any changes in the way they access or use protected content.
- Seamless integration with document sharing and document management systems.
- Corporate document security policies can be used to automatically apply appropriate access and digital rights controls.
- Anti-tampering built in.
- Support for a wide range of access control authentication mechanisms such as X509 digital certificates, Active Directory, *etc.*
- Flexible architecture and no requirement for server.
- Simple flexible management.
- Out-of-the box installation.
- Usable for protection of personal documents.

Misconceptions

A number of misconceptions have been voiced regarding dDRM, principally that dDRM:

- Affords poor security that is easily by-passed.

- Is of limited use.
- Is not needed.

These criticisms have validity when applied to early generation software (on which they are probably based). However, the emergence of the latest generation dDRM software completely negates the first two arguments. The third argument isn't tenable in modern business practice, where constant sharing and collaboration is essential. In this type of environment, encryption alone is clearly inadequate for protecting document content.

Even when considering personal documents or those that are to be shared only with completely trusted parties, dDRM offers considerable advantages over the use of conventional encryption, such as ensuring that content remains protected regardless of the location of the document.

Furthermore, if the deployment of dDRM reduced only part of the leakage of information from internal sources, it would have a considerable beneficial impact.

Conclusions

Encryption alone is a wholly inadequate means of securing document content in a modern business environment. The serious shortcomings of encryption and older generation dDRM software have led to the emergence of dDRM software based on the new approach of protecting content from its inception and throughout its development and use.

The use of modern dDRM software for protection of document content can result in a significant business advantage for companies that embrace this technology. Its use minimises the risk of information leakage and gives content owners control over the use of content and the freedom to collaborate and share content without the associated risks.

With these advantages, dDRM will gradually displace encryption as the standard means of protecting content in the business environment.

 info@avocosecure.com

US: +1 415 839 9433

International: +44 207 851 6070

 www.avocosecure.com