Encryption is not enough for DRM

Now, let's be clear right from the start that if you want to have any kind of control over the content of an electronic document you have first of all got to use encryption. But encryption is only the start of implementing a DRM service. Poorly packaged encryption, badly thought out licensing, integration that exposes weaknesses in the packaging of the method for displaying the document, are all ways in which even the most powerful encryption system can be made useless.

And, of course, there is the very important question about what is actually encrypted, and what, if anything, is not.

If you examine the ordinary PDF file you will find that a large amount of control information can clearly be seen. In other words, not everything is actually encrypted. That is a weakness since there should be no reliance upon information that has not been protected. Many document protection systems have been attacked successfully using that external control information. It may also allow others to see information that you did not want to be known. So check that all your information is encrypted, and not just the visible content.

So what are the other critical issues once you have found an encryption system that is strong enough to resist attack of the algorithm?

Well actually there are several things that you ought to be bothered by:

- How are you going to manage the decryption key:
- Creating it;
- Transferring it to the customer;
- Enforcing any time limitations;
- Changing user rights;
- Preventing theft or transfer of the key.

Creating a key

In the simplest systems the key used is a password which the publisher sends to the customer. This has the big failing that once the customer knows what the password is not only can they use the document, anyone else they send the document to can use it. Password controls on documents should be avoided as being insecure.

Transferring keys to customers

In more complex systems a random cryptographic key is generated when the document is encrypted, but now this must be made available to the customer so that they can use the

document. So if this is just sent as a file, the customer has only to copy the file and send it to anyone they would like to use the document.

You could try hiding a key in the user's registry, but there are so many programs available to tell even a novice user what has changed that they can easily find the location and the value.
In both the above methods it really doesn't matter if the key is encrypted or not because the key value is available to the DRM protection system.

A better solution is to tie the presence of the key to the customer's PC, so that even when they find out how the key arrives, giving it to someone else won't work.

Enforcing time limitations

There are many different time limiting concepts being pushed by different manufacturers, but they come down to two basic approaches:

- The controls are in the document;
- The controls are in a server that the customer must connect to.

Putting time controls in the document is a good model if you are selling the document 'forever' so the control is present if you sell shorter time periods using the same system.

You can set a time that is shorter than forever, but you must then include a method of checking that the customer does not alter their system clock to pretend the document is still in date. This can be done by using multiple control files with time synchronization, but you need to remember that changes to daylight savings are a valid change.

Having a control server is technically easier as an approach since you will always rely on server time, but it comes with the disadvantage that the customer has got to be online to the control server in order to use the documents. If you do use this approach then other controls can be implemented.

However, you need to choose a business model that also works for your customers. If it is too demanding they may not buy the publications because there isn't enough perceived value. On the other hand, very expensive items going to tightly controlled communities may be perceived as having greater exclusivity if a serious control system is in place.

A compromise position that might be acceptable is to have the reader check with the control server if it is accessible, but not to demand a connection. This is less obviously invasive, but does not allow rigid enforcement of controls or monitoring.

Changing customer rights

This kind of control can only meaningfully happen if customers are required to be in regular contact with a control server. If this approach is used then keys for documents can be brought down at the moment of use instead of being stored locally, where they may become exposed. Secure key exchange mechanisms are well developed to prevent key theft. Such an approach means that you can change user rights and document rights online, taking effect next time the user connects.

Preventing theft or transfer of a key

Some methods for preventing key theft have been discussed as part of other controls, but essential approaches include:

- Don't use passwords;
- Don't allow the user immediate access to the key or a key file where the key is readily identifiable;
- Use a secure key exchange mechanism or use a more complex key access mechanism requiring additional parameters;
- Lock the key to the machine being used.

So in summary, encryption is the technology that underpins electronic document management and control, however great care needs to be taken in its implementation if it is to be anything more than a fictional control. Obviously the strength of any encryption system still has a significant bearing on the ability of an attacker to circumvent it and you should be careful to make sure that your mechanism is going to be successful, assuming it has been properly implemented.

About LockLizard

LockLizard is a DRM (digital rights management) company that specializes in document security and copy protection. We protect information with US Government strength encryption and drm controls to ensure complete protection against copyright piracy. Use our DRM software to stop copying, prevent printing, disable print screen, expire content, and instantly revoke access to information.

We provide copyright protection without the use of passwords to ensure maximum security and usability, and to protect information, documents and web content from unauthorized use and misuse no matter where it resides. Control who uses your content, what they can do with it, and how long they can use it for. http://www.locklizard.com