/* */ /* */

Office documents **can** be made secure without the need to use a password. It seems like an oxymoron: securing documents but **NOT** using a password however it is true.

Information Rights Management (IRM) is a technology built into Office 2007/2010 (and also available for Office 2003) which allows you to both encrypt documents and provide varying levels of access for different users or groups, all without the need to enter a password. To find out more use the link below to read on or contact me for more information about rights management for Office documents.

Introduction

Historically it has been possible to protect Office documents by using the built-in features which require and prompt for a password. However it's widely known that no one should use this option to secure Office documents. David LeBlanc works implementing encryption features in the more recent versions of Office and in his blog he writes Don't Use Office RC4 Encryption. Really. Just don't do it . LeBlanc describes document protection in Office versions up to 2003 as more like obfuscation and writes:

"If you need to encrypt an older file format, then use a 3rd party tool that will do proper encryption. If you merely need obfuscation, perhaps to keep your kids out of the Christmas list, it might suffice for that, but not if you have a really bright kid."

But the poor protection is only one reason for not using password protection of Office documents. Another is the inconvenience when passwords are lost. Fortunately, modern PCs are fast enough to crack passwords used by Office 2003 in a matter of hours so all is not lost but it is an inconvenience. However this reality raises another problem: if you can crack the password, so can anyone else who might have an interest in seeing the document's contents.

Microsoft has long recognized the weakness of document security in Office and since Office 2007 the standard is to use the accredited and robust cryptography baked into Windows. Windows includes many forms of encryption including an algorithm known by the initials AES which has been created by the US and UK governments and which is part of the Federal Information Processing Standard. Office 2007 uses AES to encrypt documents by default. At

least with today's PC's AES can be pretty much unbreakable. That is, if you lose the password protecting an Office 2007/2010 document you've pretty much had it. Which is ironic because users now have a real reason to not use password protection!

So what's the difference between 2003 and 2007 encryption?

There are lots of detailed differences between 2003 and 2007 that cryptographers get hung up on but there are two essential differences: the quality of the encryption algorithm and the length of the 'key' used by the algorithm. The key is really important and assuming the algorithm is robust, the longer the key the better.

In Office 2003 the length of the key is 40 bits so there are 2^40 or 1,099,511,627,776 possible values. One trillion sounds like a big number, and it certainly used to be, but your Desktop PC probably executes this number of instructions every 5 minutes or so and laptop every 6 or 7 minutes.

By contrast, the AES key is 256-bits long or 2^256 or 1.16 x 10^77 (that's 1 followed by 77 zeros). It takes a significant period of time even for the fastest computers to crunch through this number of values and the chance of finding the right key by chance is correspondingly small.

This is why losing the password protecting your Office 2007 document probably means you've lost the document. I say 'probably' because it depends on how hard it is to guess the password. An easy to guess password (like 'password' - you've done it, right?) is no protection no matter how good the encryption!

Where does the key come from?

The key used by AES or the older algorithm used by Office 2003 is generated from the password you enter when prompted by Office. Office 2007 in particular makes it all but impossible to work out the password used from the generated key and I've tried to show above there's no hope of working through all the keys.

But AES, and so Office 2007, share the same Achilles heel as Office 2003: weak passwords. It's much easier (though still potentially hard) to work through likely passwords than it is to guess the key. Most passwords we use are 6-8 characters (letters and/or numbers, maybe an

asterisk or exclamation mark thrown in) so fairly easy to hack because there aren't *that* many combinations. More that you'd want to try by hand but a competitor with a computer looking for secrets?

To offer any protection, passwords have to be long, which are hard to remember, which is another excuse not to use passwords.

So what's the alternative?

The ideal, then, is to use the stong encryption in Office 2007 but not to use passwords. Fortunately, it turns out Office 2007 (and later) support a protocol called Information Rights Management (IRM) which allows just this. Microsoft's IRM implementation is Active Directory Right Management Services (ADRMS).

Using IRM

Using traditional Offic encryption you enter a password. Using IRM you define permission restrictions. The Office options to encrypt a document (read: password protect) and to restrict permissions sit next to each other on the Prepare option of the File menu of Office 2007/2010. The end result of using either option is the same: an encrypted document. However when restricting permissions there's no password to enter or forget so the encryption is no compromised by the limitation of human memory.

The even better thing is that the ability to define permissions rather than encryption using a password is also more powerful. When passwords are used, a document user either knows the password and can access the contents or they do not. With permission restrictions the document author is able to grant different permissions to different users or groups of users.

Another example of the benefit of using permission restrictions is that the document can only be decrypted by individuals whose domain credentials have been authenticated. This means if the document leaves the corporate network, it cannot be opened. Password encrypted documents can be opened if there's inside help to disseminate the password. With IRM, there is no password to compromise.

Even where a document might be shared with third parties (other departments or even other

companies) permissions can be defined to impose limitations on what a user is able to do with the decrypted document such as preventing the copying of cell values.

By enabling restrictions, but not defining any restrctions for yourself, you create an encrypted document no one else can access, which you do not need to enter a password to open but which cannot be opened by anyone else. This is the ideal scenario.

So far so good, but what happens if your domain account is deleted? Isn't that just another way to lose the document's content? OK, not only is it less likely that an administrator will delete your account but IRM has a built-in mechanism to handle the problem of a document owner losing control of a document. I'll touch on this in the next section. But first's it's worth noting that while IRM is baked into Office 2007/2010 the same capability is available to Office 2003 with the installation of an IRM client add-in which is available from Microsoft.

If there's no password, how are documents encrypted?

IRM is a protocol which depends upon a central server to generate and store certificates that are used to encrypt documents. The certificates generated are similar to those used to secure browser sessions when using 'https' . In a Windows environment the IRM server is a component available at no additional cost with Windows 2003 and Windows 2008. As mentioned earlier, Microsoft's IRM implementation is known as Active Directory Rights Management Services (ADRMS). Like any other server the ADRMS server becomes a member of the domain in order to support IRM actions by clients application like Office.

Roughly, when you enable permission restrictions in an Office product for a document, the client software requests that a certificate is generated by the ADRMS server which is stored with the encrypted version of the document. When a subsequent attempt is made to open the document, the IRM capabilities of Office interact with the ADRMS server again to obtain a public certificate for the document. Office determines whether the certificate retrieved grants you permission to open the document and, if so, decrypts the document and applies the implied restrictions.

To me an interesting aspect of the Microsoft IRM implementation is that the ADRMS server supports the concept of one or more nominated 'super user' accounts. These are normal Windows domain accounts or domain groups which are able to take control of all documents encrypted using IRM. Because of super users it is much less likely that circumstances can arise which will result in the permanent loss of document content.

Conclusion

If you would like to secure your Office documents but find it impractical to use passwords, Microsoft's implementation of IRM is a technology worth reviewing. It provides a way to secure documents which does not involve passwords which also allows different levels of document access to be conferred on different users and groups.