PDF Encryption and Security

Adobe PDF Encryption and Security History

The Adobe ™ PDF document format has been in development since 1991, and from as early as 1994 included security features that were aimed at preventing users from being able to make changes to a published documents. This involved the use of encryption as the only practical way of protecting information. The basis of PDF encryption is to prevent users viewing the file if they are not authorized, and if they are authorized, to control what they can do with the file (i.e. whether printing is allowed, etc.).

Early PDF document security relied on weak 40 bit encryption and soon after it was released methods of breaking it were freely available on the Internet. In May 2001 128 bit encryption became available to prevent simple hacking of the native mode controls, and degraded printing, was also added.

This did not mean that the hacking/cracking industry had not grown up to break the security measures that were in place.

PDF Password Cracks and Hacks

The early controls relied upon manual entry of either one or two passwords which allowed the user to override the controls initially placed on the document. The commonest method of attacking an encrypted PDF document is to try and break the 40 bit key implementation (the default if security has been selected). Advertisers such as www.crackpassword.com claim to provide a solution for Version 4 products that guarantees to break that level of protection in 4 days or less using an exhaustive attack (if only Manager password was set then the process is instantaneous). Version 5 products claim to be attackable by organizations such as www.lostpassword.com/acrobat.htm or www.popularshareware.com/PDF-Password-Recovery using advanced techniques, although they warn that the 128 bit algorithm itself cannot be practically attacked using brute force.

Fortunately (or unfortunately for some!) most attacks are speeded up significantly by the choice of 'poor' passwords (8 characters or less that are common words). Whilst the 128 bit PDF encryption algorithm may be good, the choice of a poor password, so that users can remember it, defeats all the good technical work. One site www.password-crackers.com will decrypt Adobe PDF files regardless of whether they have user or owner passwords set and regardless of whether they are protected by 40 bit or 128 bit encryption.

Use of passwords for PDF encryption is not the only area open to attack as you can see from the list of password crackers available for literally every common application - http://neworder.box.sk/Password_crackers

Clearly the use of passwords for PDF encryption (or encryption of any other document) is not the way forwards!

PDF encryption security methods since then have moved to using public key technologies. A number of companies have moved into this space, adding their own approaches to PDF encryption but they over-complicate the approach and do not supply any key management making the system impossible to manage. Some older products even had security flaws as in plug-in systems the key required to decrypt the PDF file is handed over to Adobe for processing - www.planetpdf.com/mainpage.asp?webpageid=1654.

Famously, in 2001 a programmer from Elcomsoft was prosecuted in the USA for publishing a program for removing PDF copyright protection on FileOpen products by attacking this weakness in the system.

Locklizard have taken a pragmatic view of the situation

Firstly we do not use plug-ins. Decryption of the document occurs in our own application and only then do we pass the decrypted file over to the secured version of the Adobe Viewer. Decryption only ever occurs in memory and non-encrypted files are never stored to disk (unless you have specifically allowed this to happen).

Secondly, many organizations do not need or wish to purchase cryptographic keys from suppliers. They already have business relationships with their customers and do not need to prove who they are cryptographically or otherwise. They are looking for a simple system to protect PDF files from any kind of password based attack and to ensure that users are not able to compromise the integrity of the system by sharing files, cryptographic keys, passwords or any other materials used to encrypt PDF files.

Thirdly, we use the US Government strength encryption to protect your PDF file – the AES encryption algorithm at its strongest strength, 256 bits.

We have introduced a new, but very simple method for allowing a copyright owner to specify controls that will be enforced on all recipients of a document. It provides for a simple, but cryptographically secure method of customer registration that transfers the true encryption key into the registered product by secure key exchange, and holds the key in a secure form prior to use. There are no passwords to manage or attack so the system cannot be compromised.

Customers, once registered, can receive files and use them seamlessly. However, they cannot transfer their registration to another computer system, and do not have access to the underlying secrets by which their access is authorized, so they cannot give those to other users.

This creates a win-win for both supplier and customers and ensures your IPR and your revenue stream remains protected at all times.