

PDF-COPS

! With PDF-Cops it is possible to distribute encrypted PDF files without modifications to the generic Acrobat Reader program !

Purpose:

PDF-COPS allows you to protect your Acrobat-created PDF files from illegal copying and pirate distribution for maximum PDF security.

The powerful encryption is accomplished using a standard software utility, and it is totally transparent to the end-user. The PDF files can be locked to an original CD-R/CD-ROM/DVD-R/DVD-ROM using our well-known Cops technology, or to the user's machine using WebCops.

How it works:

The Acrobat Reader is monitored, and the PDF files are decrypted in memory on-the-fly. This advanced technique has been implemented to work with modern 32-bit browsers running on 32-bit platforms (Win 95/98/ME, NT 4.0, Win 2000, WIN2003, WinXP/64 and Vista64).

The data files are encrypted using a powerful, proprietary algorithm. Unlocking will take place only when the Crypto loader is running on an authorized machine. The Crypto loader is locked to the CD-ROM using the well-known CD-Cops technology, or to the end-user's machine with either WebCops or CD-Cops Machine Install version.

Any reputable factory can produce the CD-ROMs/DVD-ROMs without the use of special equipment. The CD-R/DVD-R gold-master is made in-house. Distribution on CD-R or DVD-R is easy since these can be made in-house on your existing equipment, using your own media. If you choose to protect with WebCops, distribution can take place over the internet.

Printing and "Copy/Paste" operations can be disabled according to your wishes and specified for each PDF file. "Save as" is always disabled. Other modern Acrobat export options like "Send email", "Save as text" etc. can also be efficiently disabled. ** (see below)

All you have to do is:

- 1) Use our software utility to encrypt the selected PDF files.
- 2) Modify your starting page to start Crypto instead of Acrobat
- 3) If you want users to double-click on PDF files, a registry setting must be created.
- 4) Receive a Crypto loader from us, protected with either CDR-Cops, CD-Cops, DVDR-Cops, DVD-Cops or WebCops.
- 5) Assemble your package and test.
- 6) If CD/DVD-Cops: Burn CD-R, use software tool to establish CD-code and test. Then send CD-R to any CD-plant for normal replication. The finished CD/DVD code must again be established and distributed along with the product.
- 7) If CDR/DVDR-Cops: Make image with your normal burner program. Then burn media with LINK's burner program. The burned disc must be measured to establish the distribution code. When making a batch of similar discs, the code can be embedded on the disc.
- 8) If WebCops: Use the test installation number to test functionality.

Advanced solution:

Using access codes, it is possible to open certain groups of documents for a specified period of time only. New groups can be enabled at any time by using additional codes.

It will require some discussion to outline the best possible PDF security solution. But from past customer projects involving PDF-Cops, a general framework has been established.

Technical details:

Security is a major problem when distributing PDF files. There is a simple mechanism for securing against PRINTING, COPY/PASTE and CHANGING DOCUMENTS built into the PDF format - but since only a

LINK Data Security

www.linkdata.com

few bits are used for encryption, and the format is generic, simple unlocking tools have been spread around long ago ** (see below). Please note that using the powerful encryption made possible with PDF-Cops, these PDF security features can be used, and the generic unlocking tools will no longer work. Future tools are unlikely to overcome this, since each PDF file is individually encrypted and each publisher uses a unique encryption algorithm.

Traditionally, data file protection is done by encrypting the data files and modifying the browser (the program that uses the data) to let it decrypt the data files back to normal.

This approach will not work with PDF files, since the Acrobat Reader is freely distributed under strict license conditions that forbid any such modifications.

Most end-users already have the Reader installed and want to avoid installing special versions, since the Reader is being used for multiple purposes.

Therefore PDF files are normally distributed un-encrypted, maybe with the above-mentioned security settings set - knowing that these limitations can easily be removed.

To overcome this, LINK has used its experience with securing data files on PC platforms and used its advanced Crypto technology to create a dedicated PDF security product: PDF-Cops. It is being used by major companies in high-tech countries like USA and Japan.

The user's normal Acrobat Reader is unchanged. It is started by our protected Crypto loader that monitors the Reader while running and decrypts the PDF files in memory, on-the-fly, and on demand. Both encrypted and non-encrypted PDF files can be used.

Further info:

Please see www.linkdata.com for general info on Cops Crypto, CDR-Cops, CD-Cops, DVD-Cops and WebCops.

There is a good article on www.linkdata.com/theory2.htm about data security.

Send us an email if you are interested in seeing a demonstration of PDF-Cops. Please email to getinfo@linkdata.com.

**** Notes:**

On the market is a simple software utility that claims to be able to break most, if not all PDF security, in a matter of seconds.

A white paper by Bryan Guignard confirms that this is true (www.cs.cmu.edu/~dst/Adobe/Gallery/PDFsecurity.pdf). After many tests, all security restrictions were lifted very fast, even on a slow PC. Many secured PDF files were tested and each one failed the test.

Both Master Password and User Password and all restrictions controlled by these were removed (both 40 and 128-bit RC4 encryption used).

DRM security from a PDF eBook that was locked to a system were removed, and the PDF eBook could be changed into an unprotected, regular PDF file.

Bryans conclusion is that "Adobe makes it clear that it 'expects' software developers to 'respect the intent' of its PDF security system. So as it is clearly seen from Adobe's own specification, PDF security is not based on sound technology, rather, it is based entirely on 'respect'."

Using the encapsulation PDF-Cops offers, this security flaw is overcome.