How Secure Is PDF?

Note: This paper discusses the flaws in the Acrobat Standard Security handler. This paper does not discuss encryption, or the Adobe vs ElcomSoft legal issues, or copyright.

ElcomSoft (www.elcomsoft.com) is marketing a simple software utility, AEBPR*, that claims to be able to effortlessly and almost instantly break most, if not all PDF security.

I can confirm that the claims made by ElcomSoft are true. After running a battery of tests on some of Adobe's own secured documents, with the latest ElcomSoft utility, I was able to remove all security restrictions almost instantly, even with a low powered and outdated Windows based PC. Over 50 secured PDF files were tested and each one failed the test.

The ElcomSoft utility worked flawlessly!

Here is what I was able to easily achieve, in mere seconds, on a regular PC.

1) Remove the Master Password and all the restrictions** it controls.
2) Remove the User Password*** (File Open), 40 and 128-bit RC4 encryption.
3) Remove DRM security from a PDF eBook that was locked**** to my system, and revert this PDF eBook to a regular PDF file that can be viewed and edited in Acrobat.

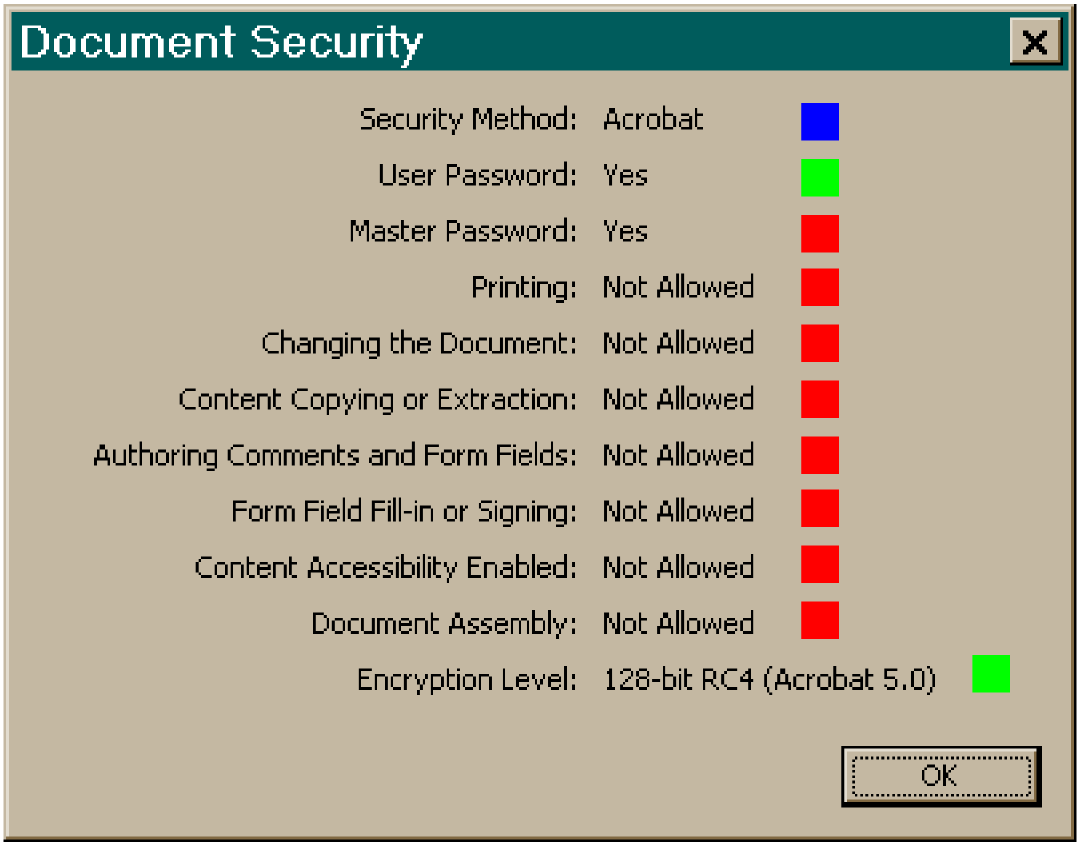
* Advanced Ebook Password Remover (AEBPR) does not crack encryption if you provide it with a valid password. Alladin systems also produces a tool called Ghostscript which can bypass the Master Password and restrictions in a similar way. There may be others.
** See next page for a list of restrictions.
*** You must first provide AEBPR with a valid User Password.
**** Of special interest is the fact that I could not even open this free Adobe supplied eBook with Acrobat, or the Adobe eBook Reader, since it had not been properly registered. This I accomplished by manually bypassing one of the steps in the acquisition of this free eBook from the Adobe eBook website. This should have made things harder for the ElcomSoft utility, but it was able to just as easily remove all DRM security!

A simple analogy of the problem with PDF security would be that of a door knob with a built in lock. Adobe installed this door knob with the screws on the outside of the door. That way anyone with a screwdriver can easily disassemble the lock and get in!

Another simple way of looking at it is as if Adobe locked the front door, but left the backdoor unlocked, and put a sign on the front lawn saying "THE BACK DOOR IS OPEN"!

The bottom line is:
1) Once you distribute a PDF file, the Master Password and restrictions can be removed.
2) Even when encrypted with a User Password, a PDF file can still have the Master Password, all restrictions, the User Password, and encryption removed from it if you give anyone the User Password.
3) PDF eBooks with DRM security (such as, but not limited to Web Buy, EBX, DocBox) offer no additional security at all, and all security can easily be removed.

Screen shot from Adobe Acrobat 5 showing all available standard Acrobat security options.
Colored squares have been added to show how security is affected.



Document Security

Security Method:	Acrobat	🟦
User Password:	Yes	🟩
Master Password:	Yes	🟥
Printing:	Not Allowed	🟥
Changing the Document:	Not Allowed	🟥
Content Copying or Extraction:	Not Allowed	🟥
Authoring Comments and Form Fields:	Not Allowed	🟥
Form Field Fill-in or Signing:	Not Allowed	🟥
Content Accessibility Enabled:	Not Allowed	🟥
Document Assembly:	Not Allowed	🟥
Encryption Level:	128-bit RC4 (Acrobat 5.0)	🟩

🟥 This security can easily be removed with the ElcomSoft utility by exploiting the weakness in the PDF specification. The Master Password is not required

🟩 If a User Password is applied, then it must be provided to the ElcomSoft utility. The utility can then remove the password and all encryption, even 128-bit RC4.

🟦 The ElcomSoft utility can also remove security put in place by some third party (non Acrobat) security handlers, as long as you have the required password, permission, voucher, license, or certificate to successfully open the file. The following can easily be removed:

BPTE_Rot13 (used by New Paradigm Resources Group, Inc.)
FileOpen (by FileOpen Systems)
SoftLock (by SoftLock Services, Inc.)
Internet Standards Australia
Adobe's Web Buy
Adobe's eBook Reader (GlassBook Reader)
InterTrust DocBox (Acrobat 5 only)

Note: Alladin's Ghostscript, a very popular and well respected PostScript and PDF toolset, contains a viewer which also exploits, or disrespects (see next page) the PDF security mechanism.

So what is the real state of PDF security, and where does that leave users in respect to encryption, restrictions and DRM?

The heart of the issue is revealed in the following two brief quotes from the PDF Reference, second edition, Adobe Portable Document Format Version 1.3, (published by Addison-Wesley in paper format, and freely available from www.adobe.com in PDF format). On page 65, first paragraph. Notice the word "expected".

> "PDF specifies a standard security handler that all viewer applications are expected to support, but applications may optionally substitute alternate security handlers of their own."

Then on page 67, second paragraph, there is this revealing note. Notice the words "respect the intent".

> "Note: PDF cannot enforce the document access privileges specified in the encryption dictionary. It is up to the implementors of PDF viewer applications to respect the intent of the document creator by restricting access to an encrypted PDF file according to the passwords and permissions contained in the file."

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".

That may be a nice sentiment, and perhaps even a practical reality a century ago, but in the present reality it is at best, an interesting pleasantry, a poor use of encryption technology, and a completely unreliable way of securing anything that can be contained in a PDF file (including text, graphics, javascripts, annotations, embedded files and more).

Conclusion

The only way your PDF property can be safe is if you keep it to yourself. Because of the "respect" model used by the PDF specification, your encrypted PDF files offer about as much strength as dried eggshells!

Adobe Inc. has not yet offered any indication of what they will do, if anything, to deal with this security flaw.

I also haven't discussed the particular details of how to bypass PDF security. I leave this as an exercise for programmers and developers.

Bryan Guignard

Adobe Adobe® Certified Expert

THE PDF EXPERT