Ghiribizzo's Cracking Tutorial

Cracking the PDF format

Cracking the PDF format

Well, you'll notice that my tutorials are in Adobe's Portable Document Format. And why not, it's a nice format, fairly small overhead (compare sizes with HTML) and has some nice features. +ORC has started a project to crack it.

PGP and Signed Tutorials

My tutorials and programs should be signed electronically using PGP. PGP 5 supports DSS/Diffie-Hellman keys. These keys are not supported by previous versions of PGP.
You should check the signature to make sure that the tutorial and especially its program files have not been tampered with. All cracks, tutorials and zip files I release will be signed. This will prevent tampering and will hopefully reduce the chances of viral infection.
My signature will also be the only way you can identify me as my email address will often change.

My Web Site:	http://www.geocities.com/Athens/3407
My Email:	Ghiribizzo@geocities.com
My Backup Email:	Ghiribizzo@hotmail.com

This document is presented with no warranties or guarantees of any kind including fitness for any particular purpose. If you use the information contained herein, you do so at your own risk.

“*As first contribution I'll give you here the very protected files that caused the whole problem in the first time, which are not only "target material" but "study material" as well, since these essays from Ghiribizzo are quite interesting in themselves.*”

- Fravia (29 October 1997)

This document is intended to give those crackers among you who are involved in the PDF cracking project a little helping hand. This document will be published both protected and unprotected and I’ll give you the password for the protected version. Nice of me, eh?

Here’s what Fravia wrote:

PSedit (ghiric1.pdf)
low security, menu and option grayed, Acrobat reader can still close and pass to another file
How to protect better, a strategy (ghiric3.pdf)
higher security, heading still there with the three boxes, reader cannot open another file
NuMega’s BoundsChecker 5.xx (ghiric7.pdf)
higher security, heading still there with the three boxes, reader cannot open another file

I think he has misinterpreted what I have done. The files all have the same security. The difference is that in the later tutorials, I got the viewer to hide the menu and button bar to increase the viewing area. These can be brought back using the hotkeys. The security settings are as follows:

```
Security Method: Standard
Open password: No
Security password: Yes
Printing: Allowed
Changing document: Not allowed
Selecting text and graphics: Not allowed
Adding changing notes and form fields: Not allowed
```

I seem to recall that the file is encrypted using RC4. The difficulty in cracking this will rely on how much forethought Adobe put into the design of not just the PDF format, but also the reader and their other programs. Although RC4 is a respected algorithm, it’s security means nothing if it isn’t implemented properly. With various ‘strong cryptographic’ products being poorly implemented, the chances of serious cryptographic considerations being made when designing PDF format and products is slim.

Anyway, good luck. The password for the encrypted version of this document will be: “Ghiribizzo”.

The files:

Ghiric8.pdf	Security as above
Ghiric8a.pdf	No security
Ghiric8b.pdf	As 8, but with print disabled and ‘Open Document Security’ enabled.

If Adobe implemented the protection in ghiric8b.pdf correctly, then it should be impossible to ‘crack’. The best you could do would be to brute force the password. The implementation of the ‘security’ password is likely to be much weaker and should be easy to bypass.