

Re: Disk encryption tools...?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-11/1371.html>

From: WinTerMiNator (*me_at_privacy.net*)

Date: 11/27/04

Date: Sat, 27 Nov 2004 21:52:30 +0100

"Patrick" <Anonymous-Remailer@See.Comment.Header> a écrit dans le message de news: VJ66MY2D38318.8992708333@anonymous.poster...

- > *In article <30rjbjF33q19hU1@uni-berlin.de>*
- > *"WinTerMiNator" <me@privacy.net> wrote:*
- >> *- TrueCrypt [...] also uses*
- >> *some part of OpenSSL code which is today outdated (old versions, while*
- >> *OpenSSL uses today newer ones).*
- >
- > *Are Truecrypt developers aware of this problem ?*
- > *There is no mention of it on their website nor the user forum.*
- > *Perhaps the future version will fix it.*

Yes, they are aware (this point has been discussed in "alt.security.scramdisk") but apparently don't want to change it (note that Truecrypt developers are anonymous, and I can only guess that I have discussed with them).

- >> *- Cross-Crypt, very "basical", without bells and whistles (command line*
- >> *program), can be used with Sarah Dean's dedicated GUI. Robust, compatible*
- >> *with Linux aes-loop.*
- >
- > *very basical indeed.*
- >

It's based on a robust system file driver, FileDisk from Bo Barten, plus crypto from loop-aes and libtomcrypt. Less bells and whistles, less bugs or uncompatibilities than TrueCrypt.

--

Michel Nallino aka WinTerMiNator
<http://www.winterminator.fr.st> (Internet et sécurité)
<http://www.gnupgwin.fr.st> (GnuPG pour Windows)
Adresse e-mail invalide; pour me contacter:
<http://www.cerbermail.com/?vqU5HHs5WG>