PRIVACYLOVER.COM

Primary Menu

Privacy Lover

VPN4All Anonymous browsing no logs
PRIVACY STABLE
OFFSHORE
15% OFF! USING CODE: PRIVACYLOVER

ENCRYPTION

ANALYSIS: IS THERE A BACKDOOR IN TRUECRYPT? IS TRUECRYPT A CIA HONEYPOT?

14 AUGUST, 2010 FRANK 5 COMMENTS

Truecrypt domain registed with a false address

The domain name “truecrypt.org” was originally registered to a false address (“NAVAS Station, Antarctica”), and was later concealed behind a Network Solutions private registration.

Truecrypt developers identity hidden

The TrueCrypt developers used the aliases “ennead” and “syncon”, but later replaced all references to these aliases on their website with “The TrueCrypt Foundation” in 2010. The *TrueCrypt* trademark was registered in the Czech Republic under name of “David Tesařík”.

Nobody knows anything about the developers, they do not want to identify themselves. Everyone likes to be known and congratulated for their great work, but apparently not Truecrypt developers, they do not care about the glory and honour and all that comes with it.

Truecrypt developers working for free

Closed source full disk encryption competitors like WinMagic, DriveCrypt (Securstar) and PGP Corporation have a full time team of software developers working in their products, creating such a product is not an easy feat as any of them will tell you.

Meanwhile two unpaid Truecrypt developers manage to work on Linux, MAC and Windows versions, on 32 and 64 versions and support the next Windows 7 as soon as it has been released, at the same time, presumably, these two Truecrypt developers also hold full time jobs that pays them a salary to feed their families and covers their mortgages .

Are closed source full disk encryption software developers overpaid lazy bastards and Truecrypt developers the finest, most hard working and charitable software developers on Earth?

Compiling Truecrypt source code increasingly difficult

Very few people compile the Windows binaries from source; it is exceedingly difficult to generate binaries from source that match the binaries provided by Truecrypt (due to compiler options, etc.)

This would be very convenient for a CIA mole, they are more likely to attack the software implementation other than the algorithm and the best way to do that is to insert some hard to find vulnerability during packaging. If someone else compiled the source code their plan would not work.

Truecrypt license contains distribution restrictions

Truecrypt is released under its own “Truecrypt license”, it is open source but it contains distribution and copyright-liability restrictions, most major Linux distributions do not want to know anything about it, Fedora has included TrueCrypt in its forbidden items list and forked it to RealCrypt instead.

Reference: http://fedoraproject.org/wiki/ForbiddenItems#TrueCrypt

UPDATE 2011: Truecrypt removed from The Amnesic Incognito Live system

The developers of the anonymous live CD called Tails have now decided to remove Truecrypt from their distribution claiming that development is done in a closed fashion, the licensing is restrictive and it is not being reviewed by too many people.

Reference:
https://tails.boum.org/doc/encryption_and_privacy/truecrypt/

Truecrypt open source code has never been reviewed

Truecrypt’s source code has never been the subject of a thorough review, nor is there any reason to rely on the credentials of the developers, since they remain anonymous.

Good thorough code review and testing is hard, tedious and painstaking work, very few people have the skills to do it, and Truecrypt hasn’t been validated through a comprehensive review by any qualified cryptographer.

Censorship at Truecrypt forums

As per Truecrypt forum rule 3 you are not allowed to discuss about other encryption software, as per Truecrypt forum rule 8 you can’t discuss Truecrypt forks, as per Truecrypt forum rule 9 you can’t discuss software that decrypts Truecrypt.

You can't say anything about their competitors and you are not even allowed to say anything about software that decrypts Truecrypt. If you post any criticisms or negative comments about their software, you will find that those posts will mysteriously disappear.

Truecrypt forum rules: http://forums.truecrypt.org/viewtopic.php?t=1651

Can the FBI crack Truecrypt?

The CIA would never share their intelligence with their FBI puppies unless it is a real national security matter, terrorism, et al. And they would not want to kill the cow that produces their milk in a public trial where their capabilities are revealed.

Furthermore, there has been recently a case of a corrupt Brazilian banker who has escaped prosecution after the FBI failed to break his fully encrypted disk, he was using Truecrypt.

Reference: https://en.wikipedia.org/wiki/Daniel_Dantas

Given those news I do not believe the FBI can crack Truecrypt and unless your name is Bin Laden you are probably still safe with Truecrypt, even if it has a backdoor and the FBI seizes your computer.

Alternatives to Truecrypt forums

Computer security and privacy newsgroups such as **alt.privacy.anon-server** ; **alt.security.pgp** , **alt.privacy** and **alt.scramdisk**

Computer and security internet forums such as Wilders Security Forums.

Alternatives to Truecrypt

The only free full disk encryption open source software that I have found and can rival Truecrypt is Diskcryptor.

Conclusion about Truecrypt reliability

Don’t get paranoid, even if you are using Truecrypt I could as well be wrong on my analysis and it is highly unlikely the CIA will ever come after you anyway.

Everyone has something to hide, but take it easy,you will need to trust some encryption product in the end and nobody out there knows 100% sure which one is safe, because what is safe today might not be tomorrow.

Just use the best encryption product according to your opinion and relax, there is no point in keeping in your head what could happen to you if you got it wrong, hopefully you did not, and as long as you did your best research on it, that is all that is needed.

For the record, I still recommend Truecrypt, they are my second choice of full disk encryption software after DiskCryptor. I am just raising what I believe are some fair points, because in security, you **TRUST NOBODY**.

0 Share 2 Share 42 Tweet 11 Share

■ TRUECRYPT ALTERNATIVE ■ TRUECRYPT ARREST

■ TRUECRYPT BACKDOOR ■ TRUECRYPT BROKEN

▪ TRUECRYPT DEVELOPERS IDENTITY ▪ TRUECRYPT ENCRYPTION REVIEW

PREVIOUS POST

Second Perfect Dark “Anonymous” P2P network user arrested

NEXT POST

How to deactivate geolocation tracking in Firefox and Opera browsers

5 THOUGHTS ON “ANALYSIS: IS THERE A BACKDOOR IN TRUECRYPT? IS TRUECRYPT A CIA HONEYPOT?”

ovigia

16 AUGUST, 2010 AT 3:27 AM

it’s an interesting question!

the code could be ok, but a backdoor can be inserted by the compiler.

what compiler are they using?

Anonymouse

16 AUGUST, 2010 AT 10:27 PM

A compiler cannot insert a back door code segment. It is a byte code based executable meaning that if the code doesn’t exist the compiler does not know about it. Any piece of software that is claiming to be open source project and is not under a recognizable license should not be trusted.

Frank

16 AUGUST, 2010 AT 11:05 PM

I never said the compiler inserts a backdoor, I talked about inserting a vulnerability (on the code), it can make a small modification to the actual code while compiling it so that it is breakable.

BTW: DiskCryptor is released under the GPL license, the same license that Linux uses.

Anton

22 APRIL, 2011 AT 5:06 PM

These media guys are masters in creating a big title news from a tin air.That’s an old story and nothing to do with a “backdoor”. It’s more about licence: http://lists.freedesktop.org/archives/distributions/2008-October/000276.html however other less political linux distributions like Gentoo still ok with it.
.
“Compiling Truecrypt source code increasingly difficult” that is completely not true. Gentoo users just type “emerge truecrypt” and it’s compiled in couple minutes.
.
“Truecrypt developers working for free” open source does not mean nobody haven’t paid.Many opensource developers are full time employee. These employers just happy to share the code and open for suggestions.
.
“Truecrypt open source code has never been reviewed” yet another bold statement.You are welcome to hire a “qualified cryptographer” and publish results.
.
“Alternatives is Diskcryptor” – Not true, it is windows only.
.
So far, truecrypt reminds the only cross-platform disk-

encryption software available.

---

couldbe

23 APRIL, 2011 AT 4:45 AM

I think the answer to most of your questions could be that the TC developers remain anonymous for a reason(s). That reason(s) is most likely that if the government or any BAD people (criminal organizations) need help to crack TC encryption, the actual developers/inventors cannot be found or located. There IS risk involved in releasing and developing encryption that even the all mighty US government cannot crack. It doesn't mean that the developers can crack it themselves, but…if you were the government or bad people and you urgently needed to get into this file…where is the first place you would go for help? Probably the people who invented the program.

COMMENTS ARE CLOSED.

ECUR
FAST
S
15% OFF
CODE:
PRIVACYLOVER