TrueCrypt

Final Release Repository

397,258 views

Yes . . . TrueCrypt is still safe to use.

Although the disappearance of the TrueCrypt site, whose ever-presence the Internet community long ago grew to take for granted, shocked and surprised many, it clearly came as no surprise to the developers who maintained the site and its namesake code for the past ten years. An analysis of the extensive changes made to TrueCrypt's swan song v7.2 release, and to the code's updated v3.1 license, shows that this departure, which was unveiled without preamble, was in fact quite well planned.

For reasons that remain a titillating source of hypothesis, intrigue and paranoia, TrueCrypt's developers chose not to graciously turn their beloved creation over to a wider Internet development community, but rather, as has always been their right granted by TrueCrypt's longstanding license, to attempt to kill it off by creating a dramatically neutered 7.2 version that can only be used to view, but no longer to create new, TrueCrypt volumes.

Then, leveraging the perverse and wrongheaded belief that software whose support was just cancelled renders it immediately untrustworthy, they attempted to foreclose on TrueCrypt's current and continued use by warning the industry that future problems would remain unrepaired. This being said of the latest 7.1a version of the code that has been used by millions, without change, since its release in February of 2012, more than 27 months before. Suddenly, for no disclosed reason, we should no longer trust it?

The mistake these developers made was in believing that
they still “owned” TrueCrypt, and that it was theirs to kill.

But that's not the way the Internet works. Having created something of such enduring value, which inherently requires significant trust and buy-in, they are rightly unable to now take it back. They might be done with it, but the rest of us are not.

The developers' jealousy is perhaps made more understandable by examining the code they have created. It is truly lovely. It is beautifully constructed. It is amazing work to be deeply proud of. Creating something of TrueCrypt's size and complexity, and holding it together as they did across the span of a decade, is a monumental and truly impressive feat of discipline. **So it is entirely understandable** when they imply, as quoted below, that they don't trust anyone else to completely understand and maintain their creation as they have. Indeed, it will not be easy. They might look at the coding nightmare atrocity that OpenSSL became over the same span of time and think: “Better to kill off our perfect creation than turn it over to others and have it become that.”

Those who believe that there is something suddenly “wrong”
with TrueCrypt because its creators have decided they no
longer have so much to give are misguided.

TrueCrypt's creators may well be correct. TrueCrypt may never be as pure and perfect as it is at this moment, today—in the form they created and perfected. Their true final version, 7.1a, may be the pinnacle of this story. So anyone would and should be proud to use and to continue to use this beautiful tool as it is today.

TrueCrypt's formal code audit will continue as planned. Then the code will be forked, the product's license restructured, and it will evolve. The name will be changed because the developers wish to preserve the integrity of the name they have built. They won't allow their name to continue without them. But the world **will** get some future version, that runs on future operating systems, and future mass storage systems.

There will be continuity . . . as an interesting new chapter of Internet lore is born.

Linux Foundation

Tweets from the @OpenCryptoAudit project:

- At 5:40am, 29 May 2014
  We will be making an announcement later today on the TrueCrypt audit and our work ahead.
- 9 hours later at 2:40pm, 29 May 2014
  We are continuing forward with formal cryptanalysis of TrueCrypt 7.1 as committed, and hope to deliver a final audit report in a few months.
- And eight minutes later at 2:48pm, 29 May 2014
  We are considering several scenarios, including potentially supporting a fork under appropriate free license, w/ a fully reproducible build.

So it appears that the unexpected (putting it mildly) disappearance of TrueCrypt.org and the startling disavowal of TrueCrypt's bullet proof security will turn out to be a brief disturbance in the force. We should know much more about a trustworthy TrueCrypt in the late summer of 2014.

Time to panic?

No. The TrueCrypt development team's deliberately alarming and unexpected ***“goodbye and you'd better stop using TrueCrypt”*** posting stating that TrueCrypt is suddenly insecure (for no stated reason) appears only to mean that **if any problems were to be subsequently found**, they would no longer be fixed by the original TrueCrypt developer team **. . .** much like Windows XP after May of 2014. In other words, we're on our own.

But that's okay, since we now know that TrueCrypt is regarded as important enough (see tweets above from the Open Crypto Audit and Linux Foundation projects) to be kept alive by the Internet community as a whole.

So, thanks guys **. . .** we'll take it from here.

Note that once TrueCrypt has been independently audited it will be the **only** mass storage encryption solution to have been audited. This will likely cement TrueCrypt's position as the top, cross-platform, mass storage encryption tool.

My two blog postings on the day, and the day after, TrueCrypt's self-takedown:

- Whither TrueCrypt?
- An Imagined Letter from the TrueCrypt Developer(s)

My third and final posting about this page, in order to allow feedback.
The posting generated many interesting comments:

- Yes **. . .** TrueCrypt is still safe to use.

And then the TrueCrypt developers were heard from **. . .**

Steven Barnhart (@stevebarnhart) wrote to an eMail address he had used before and received several replies from “David.” The following snippets were taken from a twitter conversation which then took place between Steven Barnhart (@stevebarnhart) and Matthew Green (@matthew_d_green):

- TrueCrypt Developer “David”: “We were happy with the audit, it didn't spark anything. We worked hard on this for 10 years, nothing lasts forever.”
- Steven Barnhart (Paraphrasing): Developer “personally” feels that fork is harmful: “The source is still available as a reference though.”
- Steven Barnhart: “I asked and it was clear from the reply that "he" believes forking's harmful because only they are really familiar w/code.”
- Steven Barnhart: “Also said no government contact except one time inquiring about a ‘support contract.’ ”

- TrueCrypt Developer “David” said: “Bitlocker is ‘good enough’ and Windows was original ‘goal of the project.’ ”
- Quoting TrueCrypt Developer David: “There is no longer interest.”

TrueCrypt v7.1a installation packages:

	Downloads
TrueCrypt Setup 7.1a.exe (32/64-bit Windows)	58,677
TrueCrypt 7.1a Mac OS X.dmg	15,735
truecrypt-7.1a-linux-x64.tar.gz	18,153
truecrypt-7.1a-linux-x86.tar.gz	12,800
truecrypt-7.1a-linux-console-x64.tar.gz	9,631
truecrypt-7.1a-linux-console-x86.tar.gz	8,341

The TrueCrypt User's Guide for v7.1a:

TrueCrypt User Guide.pdf	35,823

The TrueCrypt v7.1a source code as a gzipped TAR and a ZIP:

TrueCrypt 7.1a Source.tar.gz	8,856
TrueCrypt 7.1a Source.zip	12,668

Verifying the TrueCrypt v7.1a Files

(Because caution is never foolish.)

Many sites attempt to assert the authenticity of the files they offer by posting their cryptographic hash values. But if bad guys were able to maliciously alter the downloaded files, they could probably also alter the displayed hashes. Until we have secure DNS (DNSSEC, which will create a secured Internet-wide reference for many things besides IP addresses) the best we can do is **host confirmation hashes somewhere else**, under the theory that as unlikely as it is that this primary site was hacked, it's significantly less likely that two unrelated sites were both hacked.

So, for those who double-knot their shoelaces, Taylor Hornby (aka FireXware) of Defuse Security is kindly hosting a page of hash values of every file listed above. And, being the thorough cryptographic code auditor that he is, Taylor first verified the files GRC is offering here against several independent archives:

https://defuse.ca/truecrypt-7.1a-hashes.htm

Additional online TrueCrypt sites and repositories:

- The reconstructed browsable version of the truecrypt.org website. A terrific Canadian web developer, Andrew Y. (who also created the ScriptSafe Chrome browser extension to duplicate the script-disabling of Firefox's NoScript), captured some of the TrueCrypt.org website before it disappeared from the Internet and then reconstructed the missing pieces using the PDF manual. The result is a terrific web-browsable site for TrueCrypt.

- TrueCrypt.ch: A just launched, Swiss-based, possible new home for TrueCrypt. Follow these folks on Twitter: @TrueCryptNext. Given the deliberate continuing licensing encumbrance of the registered TrueCrypt trademark, it seems more likely that the current TrueCrypt code will be forked and subsequently renamed. In other words **. . .** for legal reasons it appears that what TrueCrypt becomes will not be called “TrueCrypt.”

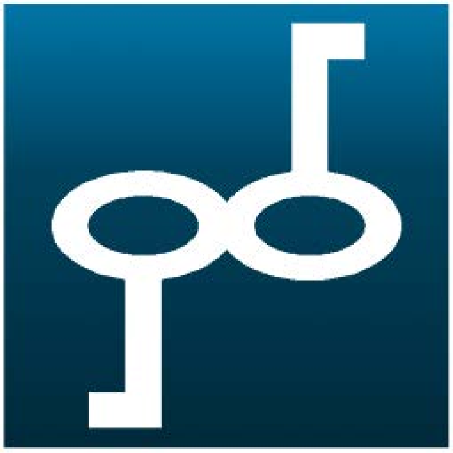
- github.com/DrWhax/truecrypt-archive: This is a frequently cited and trusted archive maintained by Jurre van Bergen (@DrWhax) and Stefan Sundin. It contains a nearly complete, historical repository of previous TrueCrypt versions, tracking its evolution all the way back to when it was previously named “ScramDisk” (which is when we were first using and working with it).

- github.com/syglug/truecrypt: Another TrueCrypt v7.1 archive, though apparently not the latest. But readily browsable if someone wishes to poke around within the source with their web browser.

- IsTrueCryptAuditedYet.com: This is the home of the TrueCrypt auditing project. As the audit moves into its next phase, digging past the startup and boot loader and into the core crypto, updates will be posted and maintained here.

Thoughts about a next-generation encrypted-data logo:

Graphic designer William Culver spend a bit of time thinking about a logo for whatever TrueCrypt becomes in the future. The theme of an infinity symbol is meant to convey the endless lifetime of this terrific data encryption solution. As is made clear on William's page for this, he's releasing all copyright:



256 x 256 pixels

32 x 32 pixels

Additional Miscellany:

- **Amazon uses TrueCrypt** when exporting archived data to users. See the first Q&A of the link. TrueCrypt is a perfect solution for this. We have every reason to believe that it is utterly bulletproof and only TrueCrypt provides the universal Windows/Mac/Linux platform neutrality that this application requires.

Jump To Top

Last Edit: Jun 05, 2014 at 15:28 (102.95 days ago)

Viewed 1,828 times per day