Steve (GRC) Gibson's Blog

Steve's Public Brain Dumping Ground
(watch where you step!)

← Whither TrueCrypt?

Yes... TrueCrypt is still safe to use. →

An Imagined Letter from the TrueCrypt Developer(s)

Posted on May 29, 2014

As I wrote yesterday, we know virtually nothing about the developer(s) behind TrueCrypt. So any speculation we entertain about their feelings, motives, or thought processes can only be a reflection of our own. With that acknowledgement, I'll share the letter I think they might have written:

> TrueCrypt is software. Frankly, it's incredibly great software. It's large, complex and multi-platform. It has been painstakingly designed and implemented to provide the best security available anywhere. And it does. It is the best and most secure software modern computer science has been able to create. It is a miracle, and a gift, and it has been a labor of love we have toiled away, thanklessly for a decade, to provide to the world... for free.
>
> TrueCrypt is open source. Anyone could verify it, trust it, give back, contribute time, talent or money and help it to flourish. But no one has helped. Most just use it, question it and criticize it, while requiring it to be free, and complaining when it doesn't work with this or that new system.
>
> After ten years of this mostly thankless and anonymous work, we're tired. We've done our part. We have what we want. And we feel good about what we have created and freely given. Do we use it? Hell yes. As far as we know, TrueCrypt is utterly uncrackable, and plenty of real world experience, and ruthlessly still-protected drives, back up that belief.
>
> But hard drives have finally exceeded the traditional MBR partition table's 32-bit sector count. 2.2 terabytes is not enough. So the world is moving to the GPT. But we're not. We're done. You're on your own now. No more free lunch.
>
> We're not bitter. Mostly we're just tired and done with TrueCrypt. Like we wrote above, as far as we know today, it is a flawless expression of cryptographic

Search

For GRC Corporate News:
Please see: **blog.grc.com**

Subscribe to eMail Updates
Enter your email address below to receive updates by email:

Join 2,812 other followers

Sign me up!

This Blog's RSS Feed:
RSS - Posts
RSS - Comments

Recent Postings:
- Yes... TrueCrypt is still safe to use.
- An Imagined Letter from the TrueCrypt Developer(s)
- Whither TrueCrypt?
- A quick mitigation for Internet Explorer's new 0-day vulnerability
- The Lesson of Lavabit
- IronMan 3 was "Unbelie… but not in a good way.

Follow

Follow "Steve (GRC) Gibson's Blog"

Get every new post delivered to your Inbox.

Join 2,812 other followers

Enter your email address

Sign me up

> software art. And we're very proud of it. But TrueCrypt, which we love, has been an obligation hanging over our heads for so long that we've decided to not only shut it down, but to shoot it in the head. If you believe we're not shooting blanks you may want to switch to something else. Our point is, now, finally, it's on you, not us.
>
> Good luck with your NSA, CIA, and FBI.

Please also see Brad Kovach's blog posting about this topic. *Very useful*. /Steve.

Rate this:

42 Votes

Like

One blogger likes this.

Related

Whither TrueCrypt?
With 123 comments

Yes... TrueCrypt is still safe to use.
In "GRC"

Why Firesheep's Time Has Come
With 70 comments

This entry was posted in Uncategorized. Bookmark the permalink.

← Whither TrueCrypt?

Yes… TrueCrypt is still safe to use. →

96 Responses to *An Imagined Letter from the TrueCrypt Developer(s)*

James Bertelson *says:*
May 29, 2014 at 7:57 am

I find it highly doubtful that the key reason TrueCrypt shut down is that they didn't want to migrate from MBR to GPT.

Reply

Steve Gibson *says:*
May 29, 2014 at 8:05 am

James,
I hope you read more from that hypothetical letter than that... since the letter said a LOT more. The GPT issue wasn't either a small or huge thing. But it was a discontinuity and presented an opportunity to decide whether they wanted to continue. They decided not to.

- June 2010 (4)
- May 2010 (3)

I Tweet, therefore, I am:

- "Google vs SHA-1" Security Now! podcast #473 show notes: grc.com/sn/SN-473-Note... / 1 hour ago
- "Gotham" - New series on FOX looks FANTASTIC! Check out the preview next Saturday. Then the series begins airing next Monday, Sept. 22nd. / 16 hours ago
- Here's today's TWiT Triangulation with Leo's interview of the fabulous physicist and cosmologist Lawrence Krauss: twit.tv/show/triangula... / 19 hours ago
- OMG! @leolaporte is doing the BEST "Triangulation" interview with Physicist Lawrence Krauss. It's underway now. Grab it once it's posted! / 1 day ago

Eyeball Counter

- 361,157 eyeball pairs

Copyright, Reuse, etc.

Feel free to copy/paste anything here anywhere else. Attribution would be appreciated.

/Steve.

Reply

James Bertelson *says:*
May 29, 2014 at 8:07 am

Reading it again — it does seem I jumped ahead of myself in drawing that conclusion. No more commenting before the morning caffeine sets in!

Reply

CB *says:*
May 29, 2014 at 8:04 am

The “letter” makes a pretty clear point that it is not the real reason.

Reply

passive aggressor *says:*
May 29, 2014 at 8:07 am

So what you mean is they had enough and rather than write something similar to what you wrote, they decided to be EXTREMELY passive aggressive about it? That seems highly unlikely, although knowing lots of geeks personally, definitely a possibility.

Reply

Steve Gibson *says:*
May 29, 2014 at 8:10 am

Yes. When you think about it... how do you really disconnect after a decade of work? You say “Don’t use it anymore, use something else.” That way they can be done. Really.
/Steve.

Reply

Whelan *says:*
May 29, 2014 at 8:11 am

Yes that letter is a fantastic piece of speculation, whose entertainment value is only matched by its irrelevance considering the source. Good grief Steve, are you now dabbling in tabloid journalism for shock value? How about we focus more on the *actual* works of the developers, and less on what one of them may or

may not have said in a parallel universe.

Reply

Steve Gibson *says:*
May 29, 2014 at 8:20 am

Hmmm. Perhaps I was being too subtle? Since you apparently missed the entire point of the letter, even after I carefully set it up. It's what I think. And I'm certainly entitled to think what I choose. And speculating is all we can do. But that doesn't make it useless or a worthless enterprise.

Reply

Donald Hoskins (@Grommish) *says:*
May 29, 2014 at 8:58 am

Besides. When I checked the URL, it was steve.grc.com, not the corporate side. This is YOUR blog, use it as you will. Anyone who wants to stay completely serious all the time makes me wish they really would stick to the Haystacks page.

Reply

Steve Gibson *says:*
May 29, 2014 at 9:24 am

<grin> Right. And the top of the page, since before the first posting here was made, is written: "Steve's Public Brain Dumping Ground (watch where you step!)" This is deliberately and by design a place where I allow myself to relax and play a bit, taking more freedom than I do or would in other more formal venues.

Reply

Max Hallam (@Max_Hallam) *says:*
May 29, 2014 at 1:46 pm

Reply

Rich *says:*
May 29, 2014 at 8:16 am

I think it takes a mindset of people "of an age" to fully grasp what 'tired' means in this context. I think they did a great job, for free, and the audit and other scrutiny is weighing heavy. Life is short. They are, without a doubt, talented developers,

and hope that furthers their career. All the best to them.

Reply

Steve Gibson *says:*
May 29, 2014 at 8:22 am

Amen, and well said, Rich. I hope we know more someday, about this and about “them.”

Reply

Tom Olzak *says:*
May 29, 2014 at 12:13 pm

I agree completely, having been “tired” once or twice myself...

Reply

Alex Santos *says:*
May 29, 2014 at 8:23 am

Is this it? If they had written something like that I would have the following to say: I found the letter from the developer to be rude and arrogant. Quite honestly, if I had been a user of their software I would be offended. Yes, I know it’s free but no one forced them to provide free software, especially when the claims made point to perfection. It’s no one’s fault that they couldn’t attract contributors, who would need contributions when they quite arrogantly announce its’ perfection. If they cared an inkling about the community they relied on, they should have politely warned folks that the timer is ticking and offered a more graceful and gracious shutdown. I would be quite appalled if this were their positioning. The good luck comment would only add salt (not that salt) to the wound.

On a less fictional note (I suppose), I hope we eventually find out what happened and it would be nice to have a substantial reveal.

Reply

Tom *says:*
May 29, 2014 at 9:25 am

I’m not sure whether to even believe that they couldn’t attract contributors. I can recall at least a couple of people over the years who said they were willing to contribute towards Truecrypt, but were turned down. So I got the impression that it was a really tightknit sort of setup that wasn’t particularly open to new contributors.

Reply

The Real Nirv *says:*
May 29, 2014 at 8:24 am

One more thing. I would personally be way more impacted (on my knees) if LastPass would unfold in this way. Yikes!

Reply

Steve Gibson *says:*
May 29, 2014 at 8:31 am

The LastPass problem is different. It's more like the JungleDisk or Hamachi problems: The good products get "acquired" by bigger fish and over time the users get the inevitable squeeze. With TrueCrypt there was never any chance of squeeze... but neither, now, is there any future for TrueCrypt. Of any kind.

Reply

The Real Nirv *says:*
May 29, 2014 at 10:50 am

Steve, just to confirm, that letter is dramatised correct — I mean, you made that up right?

Reply

Tim *says:*
May 29, 2014 at 10:32 am

Unlikely, given that lastpass is profitable company, not an anonymous development project.

Reply

Enigma IT Solutions (@EnigmaITSols) *says:*
May 29, 2014 at 10:38 am

I doubt that would happen for JungleDisk or LastPass – since they have a "paid" option. They're a business, and whilst open source licences do constitute a contract, having a mutual arrangement where money changes hands in exchange for a service means its much more likely that the service will continue.

Reply

The Real Nirv *says:*
May 29, 2014 at 10:49 am

Good thing Tim

I have paid for LastPass on iOS. I completely rely on them and hope they are here for the long of it. All my 100s of passwords lean on their service. Glad to know they have some immunity due to their model.

Reply

r000t (@rootworx) *says:*
May 29, 2014 at 11:40 am

Your entire LastPass database can be exported to LastPass- and KeepPassX-compatible formats, as well as CSV. Mine's exported, ecrypted (With Truecrypt >.<) and put in a secure off-site location once a month.

If someone finds their way into your email account, they can initiate a password reset for Lastpass. While it won't give them access to your passwords (they're encrypted with the "lost" password), it does present the possibility of wiping your account clean.

Either way, those who export their databases are protected from the service going under, or pranksters wiping their accounts clean.

Reply

The Real Nirv *says:*
May 29, 2014 at 1:13 pm

Great idea! Done, but without Truecrypt — I would have but I forget where to source it from now. Used 256bit AES encryption on a disk image. That's the best Apple's Disk Utility will give me. I'll see if Brew offers something better. Thanks for the valuable tip.

Reply

jason *says:*
May 29, 2014 at 8:26 am

I have zero programming skills, but I have a wallet. I contributed and would have continued to do so. It's their product and what they do with it is up to them, but I don't see how you can choose to give something away for free then throw a fit when no one pays for or helps you with it. We don't know if they threw a fit or not- I am really just reacting to your faux letter as a particular pet peeve of mine. I don't mind paying for useful software, and more than the 99 cent per app world we live in today. I don't expect anyone to donate their time and skill to me- no one owes anyone that- but this parasitic notion seems to have strapped itself to the open source movement and I think it's a shame.

Reply

Steve Gibson *says:*

May 29, 2014 at 8:34 am

I agree, Jason. We/I have no idea what they are feeling. And I'd sorely love to know. DO they wish they had more support? If their identities could have been known without repercussion it would have been great to turn it into a commercial product. Most or many would have happily paid for commercial-style support... and a future.

Reply

Pellucid *says:*

May 29, 2014 at 12:47 pm

Copyleft and the whole open source movement came about as a protest against closed and monetarily driven software. I think most open source advocates want exactly the opposite attitude as you're providing. If they simply wanted money or partners, they could've taken their project the business route. Open source folks want FREEDOM. They want away from (as Stallman says) "Masters" and away from intellectual property and away from the monetization of our souls.

Reply

Veer Maharaj *says:*

May 29, 2014 at 2:47 pm

Agreed, I still can't believe i bought Stardock's Objectdock and Start8 applications at full price and quite frankly id pay to have an app to create TC containers and a free app to mound and read/write to them.

Still though, with the audit having been brought up I can only assume that the software creators identities were brought forward and just with lavabit and steve himself, they were more than likely approached and asked to implement a backdoor and once that happened, they wiped their hands of the project totally.

I hope some younger minds pick up the mantle and gear forward and don't give into governmental pressures to compromise their art.

At any rate from a low level code failure to these code gods, I say thank you and for your efforts, the world is a better place.

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

Reply

Stephen Eastmead *says:*

May 29, 2014 at 8:44 am

Steve, The text phraseology, some of the points made and the spelling looks US to me. Stephen UK

Reply

Steve Gibson *says:*

May 29, 2014 at 8:49 am

Well, yeah... because I wrote it and I spell “a synthesized letter” with a ‘z’ not an ‘s’.

Reply

Whelan *says:*

May 29, 2014 at 9:07 am

As you will see above Stephen, this was a somewhat bizarre piece from Steve, at best intended to promote interest in the subject and at worst just a lowbrow trolling attempt (you choose). Either way it’s a generalised snapshot of the open-source problem, where most people get a warm fuzzy feeling from knowing that someone else might have looked at their source code, but they’re not quite sure who signed off on it, or what their qualifications might be. Or to put it another way..

“yay this piece of software is open source!”
“Wait you looked at the source didn’t you?”
“No I thought you did??”.
“No way, most of that code I don’t understand, but I hear there’s some obscure guy in Bulgaria who does”
“Oh well, it’s open source, so yayyyy!”

Reply

Steve Gibson *says:*

May 29, 2014 at 9:19 am

Whelan,
Despite your (mis)characterization of the motivation for this posting, which a great many people have found to be interesting speculation — which was, indeed, it’s intended goal — I very much appreciate and agree with your perfect characterization of the general trouble with the open source model. Nicely done.

Reply

The Real Nirv *says:*

May 29, 2014 at 1:00 pm

Indeed, the short A to B conversation is precisely one of the reason open source is not everything it is dressed up to be. It's a complex problem, on the other side of the equation we have closed source. The latter we also either trust or not. Still, open source has the potential to be very good but it needs persistent expert review by trusted sources to have any real merit. Closed source in today's NSA is subject to scrutiny and secrecy. This is but a drop in the bucket of the issues facing the computing landscape. It's becoming less and less innocent as time goes by.

Reply

Pellucid *says:*

May 29, 2014 at 2:26 pm

Oh as opposed to the:
"yay, it's proprietary!"
"wait, it's a reputable company...right?"
"...and are not working with government agencies...right?"
"Wait, you looked at the source didn't you?"
"No...oh that's right we can't and never will be able to"
"Oh and let's talk to the developers about the direction of the project..."
"Oh wait that's right a corporate master tells them what to write..."
"Oh well, it 'Just Works' right....take mai monies!!!"

Reply

Pellucid *says:*

May 29, 2014 at 4:33 pm

I think I have to clear up this misconception about open source software. Developers are spending their time and money to give something to the community (usually giving the product away for free). The idea of "many eyes on the code" is a SIDE BENEFIT of this collaborative and open model, but it is not a guarantee nor is it an obligation of theirs to ensure ANYTHING. In fact most open source licenses SPECIFICALLY say they provide no warranty and that you accept it "AS IS" (they do this to protect contributors). I must add that despite this, OSS is OFTEN more secure than their proprietary counterparts.

To them it probably feels like this when you complain... (analogy) I give you a 100 dollars and say "this is for improving your life!" You take this 100 dollars and on the

way home you get mugged, stabbed, and they take 50 dollars. Then you spend the remaining 50 dollars on candy bars and develop a huge tummy ache as well as develop diabetes. Then you come to me and say "you said this 100 dollars was to improve my life but it hasn't!" I say, "but I gave you 100 dollars for free and asked for nothing in return, what you do want from me?"

Reply

Pingback: *The death of TrueCrypt: a symptom of a greater problem | @bradkovach.blog()*

Fulcrum *says:*
May 29, 2014 at 10:26 am

I don't doubt this characterization about how they felt pouring their lives into a thankless volunteer effort. This scenario is certainly possible, but given the bizarre phrasing of the front page, I can only read it three ways
1) The Gibson scenario where the webpage text is a sarcastic middle-finger reaction to burnout, full of cynical suggestions and overblown hyperbole.
2) They're Lavabitting instead of revealing what they feel is critical information, such as developer identities, or known unpatched flaws.
3) They, or someone in the team have been coerced into building in a back-door, and are having an attack of conscience.

Number three makes the most sense to me, since the downright odd and confusing message has clearly gotten a lot of attention and inspired a lot of conspiracy scenarios in a community prone to caution, and in the extreme, paranoia.

Reply

Steve Gibson *says:*
May 29, 2014 at 10:47 am

I think your #3 scenario is compelling. We know that crypto is no longer difficult to do right, and that when done right no one — no one — can break it. And we have to presume that an organization such as the US NSA, if it wished to, has the clout and resources to track these developers down regardless of their location on the globe. And how could it not wish to? Nation states don't like any secrets that are not their own. So even a non-US power could be brought into the mix and depending upon where these developers resided, they might well have been under compulsion to subvert TrueCrypt. And, as you suggest, acting a bit like Ladar Levinson did with Lavabit, they chose instead to kill off their creation, thus ending the product's value, terminating interest, and frightening any future users away.

Reply

Adrian *says:*

May 29, 2014 at 3:21 pm

On the bright side, the source code is out there and it looks like the audit process is set to continue. While the program may no longer be supported by its original developers, the program itself isn't going away. Whether future changes by new developers can be trusted or not is, of course, something else entirely.

Perhaps the issue is not that the software has back doors, but that the private keys used by the developers have been compromised and are therefore worthless for preventing in-transit replacement of the binaries?

Reply

Ben Franske *says:*

May 29, 2014 at 10:44 am

The F/OSS community has long had issues with the license that was used for TrueCrypt. TC has been embroiled in controversy because of this issue for a a long time. I think it's less an issue of people not wanting to help the TC developers than the TC developers saying it was their way or the highway. They did not seem to want to develop a community of support for their product. If they wanted help they could have had it but they would have lost some control of the project.

I think it would be unfair to lay the blame on the community for stepping up. I have never been an advocate for TC because of their licensing, secrecy, and attitude toward the community. I find this turn of events interesting and notable but not particularly surprising because of how they chose to run the project. In addition, I think it's unlikely we'll see a real fork of this to continue development. Not due to a lack of interest or ability, but because of the inane licensing choices the devs made. It would probably be better to start all over again or build from something like DiskCryptor which is GPL licensed.

Reply

Tim *says:*

May 29, 2014 at 11:17 am

I'm in the dark on that one – what is the controversy surrounding the TC license?

Reply

@itinsecurity *says:*

May 29, 2014 at 11:59 am

Steve could absolutely be right here. But there's one thing that doesn't make sense in all of that: This spring, TrueCrypt is (finally) getting some overdue attention and help. The code audit initiated by people like Matthew Green would help get TrueCrypt the "stamp of approval" it needs to overcome the suspicions raised against OSS recently. And cases like the OpenSSL vulnerability helps open people's (and companies') eyes to the importance of supporting OSS development.

So if anything, recent developments should be helping TrueCrypt out of that misery Steve suspects could be behind this, shouldn't it?

Reply

Ric *says:*
May 29, 2014 at 12:43 pm

I think the referral to MS is the red herring here.
Everyone knows the cooperation level MS has provided to subvert it's own users.
If I weren't allowed to tell everyone what was going on, I could pick no better flag to use than to refer folks to MS.
No one wishing to maintain their credibility would do so in this community.
Following the "trust no one" mantra, this requires to me that this is a deliberate message of user beware.
I think I'll go back to the xor model with data bytes bit split among multiple devices.
At least I know what that will do and how.

Reply

Donald Burr *says:*
May 29, 2014 at 1:21 pm

If this is indeed the TrueCrypt developers' way of throwing in the towel, then this is pretty damn irresponsible of them. It would be one thing if we're talking about some one-off/useless piece of software, like a screensaver or a wordpress plugin, that either (A) is used by only a handful of people, and/or (B) does not really serve a critical function. But, for better or for worse, TrueCrypt has, in a sense, become part of our computing infrastructure, just like OpenSSL, Apache, Linux, etc. has. It has become a critical part of how many people secure their data, and they depend on it. Doesn't matter if they started out writing it as a hobby or for grins and giggles, it has grown into something big, and I feel that the developers have some sort of responsibility to at least see that it gets handed off properly. Ok, so maybe they don't want to develop it themselves anymore. Fine. So set up a Kickstarter to create a "TrueCrypt Foundation" or some such. Or talk to the TrueCrypt audit people and say "hey, as long as you guys are auditing the code, why not work on it too?" Something! Anything! Don't just shoot it in the head and leave us to deal with the bloody mess.

Reply

The Real Nirv *says:*
May 29, 2014 at 1:31 pm

If Steve's dramatisation is indeed not as far fetched as most of us would like to believe then I could not agree with you more, it would be reckless to say the least.

Reply

Pie Man *says:*
May 29, 2014 at 2:27 pm

Funnily enough a few months ago I was discussing with my wife whole disk encryption options as she needed it for a job. I told her about Truecrypt saying it's great and free, but that no one could rely on it to be continued to be supported as no one knows who has created it and how long they will support it. I also said that in my opinion it would probably continue but that was not a given.
In the end she ended up with a windows 8 computer so rather than jumping through hoops to get it to work I went with bitlocker via windows 8 pro. (shame windows 7 pro doesn't support bitlocker)
Does anyone have any experiance with Symantec Encryption Solutions or cryptic disk by http://www.exlade.com/cryptic-disk Or can someone suggest another whole disk encryption solution...

BTW how come in the last two weeks the big security announcements have happened just after your latest podcast Steve?

Reply

foregon *says:*
May 30, 2014 at 9:50 am

We're just going to have to accept it as part of the nature of the universe: mega big huge security stories will always, and *only*, happen right after after Steve Gibson podcasts...

Reply

PePa *says:*
May 30, 2014 at 7:28 pm

This works great on Windows, and has good reviews:

https://www.diskcryptor.net/

Reply

Michael Samuelle (@Level5Operative) *says:*

May 30, 2014 at 7:30 pm

I am trying this. So far the system encryption is really nice and very configurable.

Reply

Adam Elteto *says:*
May 31, 2014 at 7:08 am

The problem is that right now it is Windows only.

Reply

Pellucid *says:*
May 29, 2014 at 2:39 pm

We'll see how "responsible" you are when you receive a letter from big brother telling you that you are not allowed to say anything publicly and to quietly cooperate. I agree with "Ric" (above), if this is the devs releasing this, I'd take it as a codeword, for "compromised...abandon ship!"

Reply

dburr *says:*
May 29, 2014 at 2:42 pm

If that is the case, then that is of course understandable. If the Feds come a-knockin', then you gotta do what you gotta do to keep yourself out of trouble. But if it's just them throwing up their hands in frustration because they're fed up/tired of it/etc. then my original comment still stands.

Reply

Pingback: *DTNS 2245 – Tales from the TrueCrypt | Daily Tech News Show*

Ray Daac *says:*
May 29, 2014 at 3:33 pm

It kinds of says a lot about us as a society that we were willing to fund a security audit of Truecrypt versus using that money to instead support the developers. I'm of the opinion that maybe half or at least some part of the crowd funding could've have gone to developers as well. This is all speculation on my part since we don't know if lack of support (financial or otherwise) was the reason for the shutdown. I would like to say that I would have purchased a commercial version of Truecrypt, but the donate button has been there this whole time and in the back of my mind I kept saying "I'm going to donate to them eventually". Eventually

never came and now it looks like their gone.

Reply

Steve Wooding *says:*

May 29, 2014 at 3:35 pm

I don't think this fictional letter rings true and is muddying the waters. Money was raised for the audit, showing them that money could be raised to support Truecrypt. Let's just wait awhile for some facts. Hopefully before next week's Security Now. I really hope you won't need to read this fictional letter out on the podcast. Better just to tell us your thoughts Steve, rather than role playing them out in this way.

Reply

morthawt *says:*

May 29, 2014 at 7:23 pm

I remember when you gave them $100. I wish you (+we) could have gotten something more than the same old version after all this time. I am looking into DiskCryptor as an alternative. I hope you can review and check out some free and open source alternatives such as DiskCryptor and VeraCrypt so we can have some actively developed alternatives that have been functionally tested and reviewed by you. It would be nice to be able to get your thoughts on next security now.

Reply

JKAbrams *says:*

May 29, 2014 at 7:44 pm

A likely scenario is that a back door they had been forced to include into the software was about to be discovered in the audit and they knew the game was up. Rather than waiting for the guillotine to fall in the form of the next part of the audit, they decided to pull the trigger themselves.
This hypothesis will be tested when we see the rest of the audit-results (on the assumption that the audit is as good as we hope).

Them referring to Microsoft is indeed strange from a security perspective, but perhaps reflects their own opinions, they might never have set out to protect people from the NSA, and may agree with the sentiment that what the NSA does is warranted. There was no easy to use free solution available for Windows when TrueCrypt started.

For security-minded, freedom loving, trust no one-people, the comment about Microsoft can only read as either an insult or as a way to rely some kind of hidden message.

From what the developers have said earlier, do we have any indication as to what their stance might be? Their license and “we do things our own way”-kind of attitude would rime more with the first, but the fact that they as-far-as-we-know (their own claims to the contrary not withstanding) produced one of the most secure encryption software available (proven useful in court cases), lends credence to the second.

Reply

J K Rowlings *says:*
May 29, 2014 at 10:24 pm

The last line.

“Good luck with ‘your’ NSA, CIA, and FBI.”

US citizen 3rd person statement or Non US resentful sentiment or even clever but subtle Anti US propoganda .

Reply

Steven Wooding *says:*
May 30, 2014 at 1:59 am

Statement of fact: Steve Gibson wrote this letter. No clues can be gleaned from an analysis of words or phrases in a completely fictional work.

Reply

Pingback: *truecrypt unsafe? - SLUniverse Forums*

Nerdo *says:*
May 30, 2014 at 4:59 am

Hey guys,

take a look at this http://truecrypt.ch/

Reply

Ric *says:*
May 30, 2014 at 8:26 am

That looks like the right direction.

Reply

Alexandre Takacs (@alexandretakacs) *says:*

May 30, 2014 at 5:34 am

Well it seems indeed that the devs have given up on the product. Very amateur (to say the least) way to communicate with their community... Thankfully some people (as per previous post) are stepping up.

Reply

Miguel *says:*

May 30, 2014 at 4:20 pm

I would add as another hypothetical reason that the people making the audit are raising funds, and already got a whole lot of money, just to review the sources and "pay bug bounties"? I find it hard to believe that people is paying so much money ("Wed, Oct 24, 2013: (...) To date, we have (...) more than $53.000″ on http://istruecryptauditedyet.com/) to "praise or blame" software and that they may have given no money when they got it. If I were an author of such software, I would not like some other people making bussiness with my software by just claiming they're looking at the sources (and they are taking their sweet time too...) to decide if they can trust me.

Anyway, it's a strange farewell. I don't think they're to lose anything by making their points clear while abandoning the proyect, instead of causing such an alarm as their website is now causing.

Reply

James *says:*

May 31, 2014 at 6:18 am

Ah, more of the open source model being "flawed and out of touch", mo' money marketing.

Greed, greed, greed. The interwebs and the USA are just full of this garbage. But again, what else should be expected. It's the same reason america has politicians who go to college, to become career politicians. Nepotism and greed. You don't spend 10 years on a project to give up because the money wasn't enough. Trying to explain that to someone whose sense of accomplishment is given by how much stuff they can afford to buy or show off on instagram, well anyway, this post is all about me.

A true fact is that for 99% of people, a computer is no longer needed. And truecrypt itself isn't needed because frankly, who and what are you hiding from? If you weren't doing that, you wouldn't need to hide behind TC. For most people now, better to give them a smartphone with whatever app they needed installed, Facebook, Reddit, Twitter where their user experience can be monitored and optimized.

Reply

lol *says:*
June 4, 2014 at 12:45 am

"A true fact is that for 99% of people, a computer is no longer needed"... haha, good lord what a ridiculous comment.

Reply

The Real Nirv *says:*
June 4, 2014 at 2:49 am

I've been itching to say this. Here goes.

If you're on a mac and you want full disk encryption. Use what's built right in to the OS – FileVault 2. End of story.

This will simply end the need to use something like Truecrypt, which technically for the most part, is not completely in question. What bothers me the most is the sudden abandonment — it was a surprise. I understand technology comes and goes but it should have been a little more graceful. There is little point speculating further on the devs methods as it is a futile exercise but alternatives should be sought, the audit should be allowed to conclude before hasty comments are made and someone like the Swiss group at truectypt.ch might be able to keep the torch going.

As Steve Gibson reported on his main site, "...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."
https://www.grc.com/misc/truecrypt/truecrypt.htm

Of course, as far as FileVault is concerned, it's obviously mac centric, not RAID compatible, HFS journaled only, and so on. The audience here is probably very aware of how important full disk encryption is — if you loose your unencrypted computer your data is completely at risk. Considering how much sensitive data lives and breaths on a computer today, full disk encryption is an absolute necessity.

Consider this, an iPhone's contents are completely encrypted until you sign in with your passcode or get in throughTouchID. Your computer's data should be as fiercely locked down.

I would love to here Steve's take on FileVault but if TrueCrypt does remind us of anything, that would be the importance of full disk encryption is.

By the way, I have complete respect for the work of the TrueCrypt devs, I just don't agree with how they pulled the plug. I guess anonymity provided them the 'luxury' of washing their hands of any accountability for their user base and for their beloved software. The least they could do is rethink the software license and open it up for continuity.

Reply

Ric *says:*
June 4, 2014 at 3:12 am

"What bothers me the most is the sudden abandonment — it was a surprise. I understand technology comes and goes but it should have been a little more graceful."

I'm not sure if you are referring to the developers or the user base.

If the developers, I agree it was handled in an odd way especially considering the state of security in these times and how likely a vague message might be interpreted. Especially considering it being from security conscious people who would be aware of that.

If you meant abandonment by the user base, it reminded me of when the feds put their hands on Zimmerman about PGP and everyone was concerned about a secret back door being forced on him. People weren't sure if they should trust it anymore.

Made me feel old just remembering that.

Reply

The Real Nirv *says:*
June 4, 2014 at 3:21 am

Hi Ric,

I meant the developers not the users. Sorry about that.

Reply

fooman *says:*
May 31, 2014 at 7:40 am

If I'd been developing privacy/security product for 10 years and lost my joy,

recklessness and optimism of youth and woke up one morning after my first heart attack and suddenly noticed that the world is turning into a place were a desire for privacy is deemed a crime and punishable in extreme ways and that all seeing, all knowiing entitities are policing the entire planet (and beyond), then I might want to give a clue to my users/supporters as to the situation. In that light I might want to hang up my coat and just walk in the woods my dog, get to know my grandchildren, sit on the porch and rock in the chair looking at the sunset, whilst I'm still able.
I believe that developers of privacy and security software are coming under increasing pressure and scrutiny and the values of open source software dvelopment and supporters of such is being regarded now, as criminally subversive to the 'powers that be'.
Sharing of any resource and empowering oneself or one's community to the benefit of humanity (locally, nationally or globally) is the antithesis to the powermongers agenda of control, accountability and monopoly of all things that walk, crawl, creep, grow, animal vegetable, mineral and other. They want to control every atom, every seed, every river and stream, every cloud in the sky.
These is a very tiring thoughts, I've aged during these last few sentences.
God help our children.

Reply

fooman *says:*
May 31, 2014 at 10:03 am

Please forgive my typos and grammatical slips above. I can't edit it.

Reply

Gonzalo Porcel *says:*
May 31, 2014 at 11:06 am

Please stop posting that Truecrypt is a flawless work of art. Perpetuating a myth for a critical piece of software such as this benefits nobody.

https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf

Read the above report from the open audit project to find out that they were relying on an undocumented build process, deprecated functions, used inconsistent variable naming, had tons of uncommented code and lots of potential issues that arise from all of the above.

In fact, there is no reliable place one can point to me to gather all the build tools necessary to build Truecrypt on Windows. Again, the word here is reliable.

Having said that, Truecrypt can probably be saved if a truly open community takes over the source code, but it will take upwards of a year to have it become something whose build process and binaries can be trusted.

Reply

hazzaxb *says:*
June 3, 2014 at 11:34 pm

I agree that it is unlikely that TrueCrypt is flawless, but which of the issues raised by a source code inspection mean that the code does not do its job perfectly well ?

Reply

The Real Nirv *says:*
June 4, 2014 at 12:40 am

Hi Gonzalo, great link but I am not an expert to review the report. However, a very very brief scan shows what appears to be a concern in section B.4 “Use of deprecated, insecure string APIs”. Section B.3 shows no care was taken to prevent overflow and underflow. I will not go through all the sections but yes there does seem to be some concern over what is called the quality of code. Quality here, from what the sections indicate is not about elegance but focused on technical issues.

I hope Steve Gibson has some time to partially review the PDF and comment on the next Sec Now. Thanks again for the article link hazzaxb

https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.
.

The project’s mission (iSEC Partners Final Report – Open Crypto Audit Project TrueCrypt – Feb 14, 2014, Version 1.1) is highlighted below.

2.2 Project Goals and Scope
The goal of this engagement was to review the TrueCrypt bootloader and Windows kernel driver for security issues that could lead to information disclosure, elevation of privilege, or similar concerns. The assessment included a review of the following areas:
TrueCrypt Bootloader
Setup process
Windows kernel driver specifically including:
Elevation of Privileges from local user to kernel
Information Disclosure during disk operations
Volume parsing as it relates to system and drive partitions
Rescue Disks code paths that do not have the private key
Data Leakage
The assessment explicitly excluded the following areas:
Volume parsing as it relates to a file container
Rescue Disks code paths activated when the disk does contain the private key
Cryptographic Analysis, including
RNG analysis

Algorithm implementation
Security tokens
Keyfile derivation
Hidden Containers
Linux and Mac Components
All other components not explicitly included

This review used a combination of proprietary and public automated tools, manual test tech- niques, and source code review to audit the application.

Reply

TrasMontano *says:*
June 1, 2014 at 6:59 am

Where is the changelog for the alleged lastest version of truecrypt?

Reply

DickTwatCockFace *says:*
June 3, 2014 at 3:36 am

Cool story bro, tell it again.
No seriously Steve, this is utter bullshit, you stupid assclown.

Reply

Pingback: *Security – 31 – TrueCrypt? | inThirty.net*

hazzaxb *says:*
June 3, 2014 at 11:49 pm

I hope I am not defaming anyone, but a long time ago I read a suggestion that the TrueCrypt developers were hoping that Microsoft would buy the rights to their product and that they would thus achieve the unlikely feat of both peer group acclaim and financial reward.
If they are as bright as we suspect, I would imagine that after ten years working on a single piece of software, they might want to do something new.

Reply

Lex Luthermiester *says:*
June 17, 2014 at 6:49 pm

Or perhaps[very likely] they already have, how are we to know?

Reply

Tom *says:*

June 13, 2014 at 8:10 pm

Perhaps their identity was discovered by some government such as the U.S. Which have laws to force compliance with helping it and to never reveal such under law. The developers would have no choice but to walk away and never say why. Such is modern democracy.

Reply

Pingback: *Мистическая история с TrueCrypt | Un-Clouded.Net*

Lex Luthermiester *says:*

June 17, 2014 at 6:47 pm

Um, what with the GPT talk? I have personally used, without ANY problems or complaints from, TC on several GPT drives. Two Western Digital's and a Seagate. Granted, they are not boot drives but the partitions are fully TC'd. So is someone just being silly or am I somehow wasting my time trying to encrypt those particular drives?

Reply

Lex Luthermiester *says:*

June 17, 2014 at 7:02 pm

I'd also like to add that the hypothetical idea of their work being "Thankless" can't be true. They had for a number of years a donation link that I personally used several times. And I KNOW I am not alone. Gratitude was expressed to them in many ways over the years, so the effort could hardly have been thankless. Perhaps I was in the minority, but certainly not alone. They know we that used and understood their wonderful software were grateful for it... So, and no offense to you Steve, that part of this hypothetical letter is little more than nonsense.

Reply

fooman *says:*

June 18, 2014 at 4:01 am

Steve was simply trying to stimulate some debate and I can't believe the level of attack and nasty remarks that he's been exposed to. Some people think that if someone is generous and good willed enough to open their blog to comment then that gives them a green light and free rein to be casually abusive.

Reply

Lex Luthermiester *says:*

June 18, 2014 at 5:41 am

Fooman,

Steve knows who is blasting him with rage and who is offering insight, even if some of it is critical. Stimulating debate is always healthy for working out problems, yet there is always some half-wits who throw a maggot in the ointment. He has never given in to the nasty of the childishness often thrown at him.

Reply

Lex Luthermiester *says:*

June 18, 2014 at 5:42 am

At least in the 13 or so years that I've been following his work...

Reply

Pingback: *Das Bizarrste aus der Securityszene – Truecrypt, der grösste Helfer der digitalen Privatsphäre gibt auf | Upgrade zum Geschäftsmann 2.0*

Pingback: *Tech Mind #66: Dubbi su Fastweb e TrueCrypt | EasyPodcast*

Pingback: *VeraCrypt Rises from the Ashes of TrueCrypt - Percontor*

Pingback: *True crypt не безопасен? | Блог Владимира ТюрюкОва*

www.facebook.com *says:*

July 17, 2014 at 5:02 pm

3% national lead, and historical precedent suggests that the campaign may tighten even further the closer the country moves
to Election Day, especially without significant economic improvement.
I don't know if you are running any business currently. They will show the very best award for the fortunate winner, the top income of past those who win, so to attract more people to take part and buy much more lottery tickets from their store.

Reply

Sakabato Sword *says:*

July 22, 2014 at 6:45 pm

great seller, quick shipper

Reply

Raargh *says:*

August 11, 2014 at 10:57 pm

Good to know Steve G is still active! I miss his original columns, from back in the day.

Reply

Pingback: *TrueCrypt is Still Safe | My great WordPress blog*

twitter.com *says:*

September 3, 2014 at 3:39 am

Gable Fronted: They are also square shaped and have
huge roof windows. Snow and ice can be a real danger for the structure of your home
as well as for you. They are also great looking
and require very little maintenance.

Reply

Federico de León *says:*

September 10, 2014 at 5:11 am

i miss understand some things.. or not!. truecrypt was clearly acquired by Microsoft and implemented in bitlocker. clearly understood this when last month go for his last update and final release. as a programer i decide to support this needed earth app. Does no matter the real reasons for get not involved any more in this project for his developed and owners. they give as a wander-full gif, a needed gif actually, because freedom and privacy has to win more field. i believe that have to gif all knowledge to future generations and have to be FREE.

Reply

Leave a Reply

Enter your comment here...