The secret TrueCrypt security audit

Hanno Böck

hboeck.de

@hanno

And now for something completely different

hanno, CC0

I wanted to show you this so you can reflect whether it is really a good idea to develop technology that is based on wasting as much electricity as possible

The dire Reality of the Climate Crisis, Day 4, 13:00 Chaos-West Stage

Let's star the real talk

TrueCrypt

A file and disk encryption software first released in 2004

There is a lot of mystery in the TrueCrypt history


E4M
Encryption for the Masses
E4M is an on-the-fly disk encryption product

One of the developers of E4M was Paul Le Roux, who is currently in jail and has been involved in drug deals, illegal arms trade and other criminal activity

TrueCrypt contains lots of the previous E4M code

TrueCrypt developers were anonymous

Is TrueCrypt Free Software / Open Source?

The code is not under any standard license and the license contains some very unusual conditions

The Free Software Foundation does not consider the TrueCrypt license to be free and various Linux distributions think the same

Still TrueCrypt was very popular

2013: Edward Snowden publishes NSA documents

This raised a lot of questions about the trustworthiness of cryptographic software

In late 2013 cryptographer Matthew Green started the Open Crypto Audit Project and collected donations to fund a security audit of TrueCrypt

The donations came in quickly, the audit started

Then something unexpected happened

A message appeared on the TrueCrypt web page:

WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

It is still unclear what unfixed security issues they were referring to

Of course speculation is running wild

TrueCrypt is not developed any more, but there are forks, the most popular being VeraCrypt

The Open Crypto Audit Project reports published in 2015 did not find any severe vulnerabilities, but some smaller ones

In late 2015 James Forshaw from Google's Project Zero found some further vulnerabilities affecting the Windows version of TrueCrypt

In late 2015 BSI published an audit report of TrueCrypt

(a different one from the one we're going to talk about)

VeraCrypt fixed the known vulnerabilities

In 2016 OSTIF and Quarkslab published another audit of VeraCrypt

The BSI

The BSI is the German IT security agency

In theory the BSI has a defensive role in IT security

When government agencies have a defensive role in IT security, but have close ties to other agencies with an offensive role - there's an obvious conflict of interest

BSI is under the control of the BMI (ministry of interior)
- so are BND, VS, BKA, ...

National Cyber Security Centre

a part of GCHQ

Australian Government

Australian Signals Directorate

ACSC

Australian Cyber Security Centre

Recently I learned that BSI had created a TrueCrypt audit that was not public for nine years

In 2010 the companies Sirrix and Escrypt performed a very detailed audit of TrueCrypt on behalf of the BSI

According to BSI they tried to communicate these results to the TrueCrypt Foundation, but they were not interested

Despite all the discussions about TrueCrypt's security
the BSI decided to keep this audit secret

There is a web project called "Frag den Staat" that allows users to send request according to the German freedom of information law (Informationsfreiheitsgesetz)

The German freedom of information law says everyone can request documents from government entities without any justification and they have to provide them (with a number of exceptions)

A user on "Frag den Staat" sent a generic request to the BSI asking for investigations on TrueCrypt and whether they knew about a backdoor

True Crypt (Unterlagen und Backdoor) - Frag Den Staat

The BSI sent parts of the 2010 audit (AP2 - AP6), but said they must not be made public (copyright)

AP2 - AP6 - where is AP1?

Ist *keine FDE* aktiv, so scheint TrueCrypt in seiner Standardeinstellung nicht zu verhindern, dass durch das Wechseln in den Ruhezustand sensible Daten auf die unverschlüsselte Festplatte geschrieben werden. Es besteht jedoch die Möglichkeit, vor der Aktivierung des Ruhezustands alle offenen Volumes automatisch zu schließen. Genauere Analysen und Angriffe hierzu werden in AP3 und AP7 betrachtet.

AP4 mentions AP7

Where is AP7?

After several further requests I (hopefully) got all documents

I found bugs that were never fixed in TrueCrypt or VeraCrypt

I was not aware of the existence of the BSI 2010 audit report on TrueCrypt. I have never been contacted by BSI for anything related to TrueCrypt or VeraCrypt.

Mounir Idrassi, VeraCrypt developer

```
  string Process::Execute (const string &processName,
    const list <string> &arguments, int timeOut, ProcessExecFunctor *execFunctor, const Buffer *inputData)
  {
    char *args[32];
    if (array_capacity (args) <= arguments.size())
      throw ParameterTooLarge (SRC_POS);
[...]
          int argIndex = 0;
          if (!execFunctor)
            args[argIndex++] = const_cast <char*> (processName.c_str());

          for (list<string>::const_iterator it = arguments.begin(); it != arguments.end(); it++)
          {
            args[argIndex++] = const_cast <char*> (it->c_str());
          }
          args[argIndex] = nullptr;
```

Off by one overflow with 31 arguments

B 9.1.1.1.2.2.2.2 Codeschwächen

Hier können mangels einer vollständigen Codeanalyse nur Beispiele aufgezählt werden.

B 9.1.1.1.2.2.2.2.1 Unsichere Stringfunktionen

B 9.1.1.1.2.2.2.2.2 Off-by-One Overflows

B 9.1.1.1.2.2.2.2.3 ...

We can only list examples for these vulnerabilities -

and then we forgot to list the examples

Privilege escalation

In Linux it is possible to run TrueCrypt / VeraCrypt as a user and mount volumes with sudo

You can give users the permission to execute the so-called "Core Service" via sudo

(this is not officially supported or endorsed by VeraCrypt)

This opens up various ways for privilege escalation

Put a suid root binary that opens a shell with root permissions on a volume, mount it with user permissions, execute it and be root

Memory Wiping

It is good practice to wipe memory that has been used for cryptographic keys or passwords in secure software

This is tricky due to compiler optimizations

(there was a talk at 35C3 explaining this)

35C3: Memsad, Ilja van Sprundel

TrueCrypt / VeraCrypt has a macro *burn()* for this that seems to be fine

But it is not always used where it should be used

```
AES_RETURN aes_decrypt_key256(const unsigned char *key, aes_decrypt_c
{   uint_32t    ss[9];
#if defined( d_vars )
        d_vars;
#endif
    cx->ks[v(56,(0))] = ss[0] = word_in(key, 0);
    cx->ks[v(56,(1))] = ss[1] = word_in(key, 1);
    cx->ks[v(56,(2))] = ss[2] = word_in(key, 2);
    cx->ks[v(56,(3))] = ss[3] = word_in(key, 3);

#if DEC_UNROLL == NONE
    cx->ks[v(56,(4))] = ss[4] = word_in(key, 4);
    cx->ks[v(56,(5))] = ss[5] = word_in(key, 5);
    cx->ks[v(56,(6))] = ss[6] = word_in(key, 6);
    cx->ks[v(56,(7))] = ss[7] = word_in(key, 7);
[...]
}
```

Temporary variable ss not burn'ed

The audit contains many such examples, plenty of them still unfixed

If you want to improve VeraCrypt go through the list, check if the problem still exists and send pull requests

(AP5 starting page 26)

Trusted Disk

One of the auditing companies, Sirrix (today Rohde&Schwarz), created a fork of TrueCrypt under the name Trusted Disk

They announced that they will publish the source code, but they never did

Rohde & Schwarz still sells Trusted Disk

This is probably a license violation

The complete source code of Your Product must be freely and publicly available at least until You cease to distribute Your Product. (TrueCrypt license)

Summary

Stories like this tend to fuel wild speculation

(*BSI gave the 0days to their friends at BKA/VS/BND and that is why they did not publish them*)

I do not think that this is very plausible or likely

I do think BSI is a very problematic institution

They have a mentality of being secretive, which I believe is inherently harmful in IT security

Get the documents:

https://fragdenstaat.de/anfrage/untersuchungen-zum-verschlusselungsprogramm-truecrypt/