Secure Software Development (Computer Science) March 2022

« Collaborative Discussion 2: Cryptography case study: TrueCrypt

Sathira Padukka

Initial Post

20 days ago

4 replies

Last 3 days ago

TrueCrypt is a disk encryption software. The Open Crypto Audit Project reviewed TrueCrypt 7.1a disk encryption software. This included reviewing the bootloader and Windows kernel driver for any system backdoors as well as any other security related issues (Junestam -Security and Guigo -Security Engineer, 2014).

The findings of iSEC team presented 11 different issues. Four of the issues are medium severity, four low severity and 3 informational severity issues. Some of these issues are in different classes, Cryptography, Data exposure, Data validation, Denial of service and Error reporting.

The source code for both the bootloader and the Windows kernel driver did not meet expected standards for secure code. This includes issues such as lack of comments, use of insecure or deprecated functions, inconsistent variable types, and so forth. (Junestam -Security and Guigo -Security Engineer, 2014).

As the authors of TrueCrypt mention, Using TrueCrypt is not secure as it may contain unfixed security issues (truecrypt.sourceforge.net, n.d.), therefore I would not recommend this software to my family or friends instead I will recommend Bitlocker or Veracrypt (Githinji, n.d.).

References

Junestam -Security, A. and Guigo -Security Engineer, N. (2014). *Open Crypto Audit Project TrueCrypt Security Assessment Prepared for: Prepared by*. [online] Available at: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf.

truecrypt.sourceforge.net. (n.d.). *TrueCrypt*. [online] Available at: **http://truecrypt.sourceforge.net/**.

Githinji, R. (n.d.). *5 best TrueCrypt alternatives to encrypt your data today*. [online] PrivacySavvy. Available at: https://privacysavvy.com/security/safe-browsing/truecrypt-alternatives/ [Accessed 5 May 2022].

Reply

4 replies

1

Post by **Pavendran Wimalendran**
Peer Response

12 days ago

Hi Sathira,

Very useful and well-organised information about TrueCrypt's security flaws, with supporting documentation. This gives the reader an overview of the security vulnerabilities with TrueCrypt and also directs them to an alternative.

However, If I may add, when recommending an alternative solution, a quick comparison between TrueCrypt and the alternative, or a few lines explaining why the alternative is better, could have been helpful to the reader, along with the citation.

Also, I am not sure if you are planning to add an ontology design. If so, then it will be a great addition to your post. Thank you.

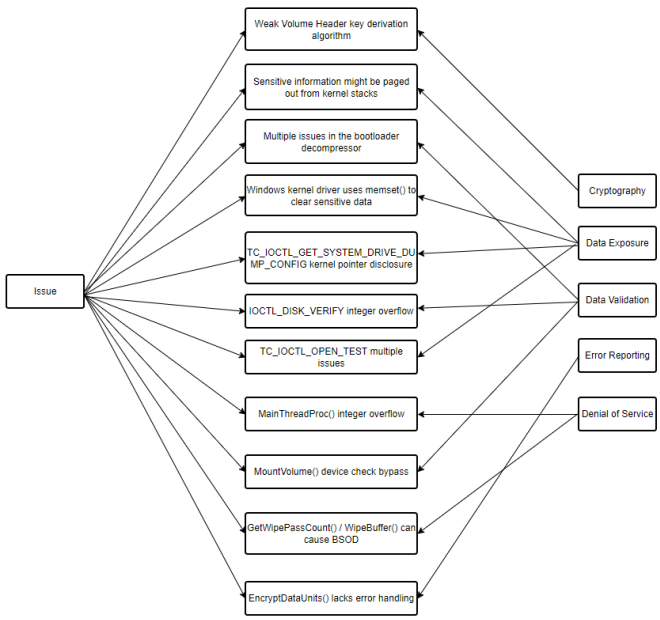
Reply

2

Post by **Sathira Padukka**
Ontology

5 days ago

Sorry there must have been an error and the ontology was not uploaded.



Reply

3 

Post by **Kei Yiu Yvone Chan** 5 days ago

Re: Initial Post

Sathira thank you for the post.
As you mentioned about Bitlocker and it is the first time I get to know this tool, I have surfed on the internet to try to understand more. It seems to me both tools are very popular while the main difference lies in VeraCrypt being mostly open-source while Bitlocker is owned by Microsoft and built in to the OS.

There are some comments mentioning VeraCrypt has a more robust security profile as it supports more encryption methods and types than Bitlocker does. Besides, there are concerns around whether Microsoft has left a backdoor in the software to make it easier for law enforcement and government agencies to access encrypted data (Henry, 2016). It is interesting to see how people's concern differ when we are talking about open-sourced and company owned encryption softwares.

References:

Henry, A. (2016) Windows Encryption Showdown: VeraCrypt vs Bitlocker. Available from: https://lifehacker.com/windows-encryption-showdown-veracrypt-vs-bitlocker-1777855025 [Accessed 24 May 2022]

Reply

4 

Post by **Yin Ping Lai** 3 days ago

Re: Initial Post

Hi Sathira,

Thank you for your sharing.

You organized and summarized the findings of the iSEC team, which was very remarkable for other readers to understand the problem of TrueCrypt flaws quickly.

For the ontology design, If I were you, I would add a sub-column next to each vulnerability and categorize them by their severity. I think adding the severity for each vulnerability could be helpful for readers to realize how important it is. Also, it is better to utilize the ontology design to address the flaws information for the TrueCrypt software intuitively.

In the final section, I saw you were not recommending it to your friends. I also would like to share some alternatives with you. Next time, you can provide an alternative for your friends and assist them in making a better choice on doing the data encryption. For ex-

ample, we can utilize the BitLocker, which is created by Microsoft and free to use on the Windows platform. It also supports advanced encryption standards. It mainly supports full-disk encryption to protect your entire computer and not just individual files. It also works for encrypting a virtual drive or other volumes that you can view and access like other drives on your computer. (Rob G., 2022.)

References:

[1] Rob Githinji, 2022, “5 best TrueCrypt alternatives to encrypt your data today”. [online] Available at: **https://privacysavvy.com/security/safe-browsing/truecrypt-alternatives/**. [Accessed on 26 May 2022].

Reply

Add your reply

Your subject

Type your post

Choose files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Summary Post

NEWER DISCUSSION

Initial Post