Secure Software Development (Computer Science) March 2022

« Collaborative Discussion 2: Cryptography case study: TrueCrypt

Sathira Padukka

Initial Post

8 days ago

1 reply

Last 7 hours 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

1 reply

1

Post by **Pavendran Wimalendran**
Peer Response

7 hours 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

Add your reply

Your subject

Type your post

Choose files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial Post

NEWER DISCUSSION

Summary Post