TrueCrypt: Initial Post

Course: MSc Computer Science

Module: Secure Software Development (Computer Science)

Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Post:

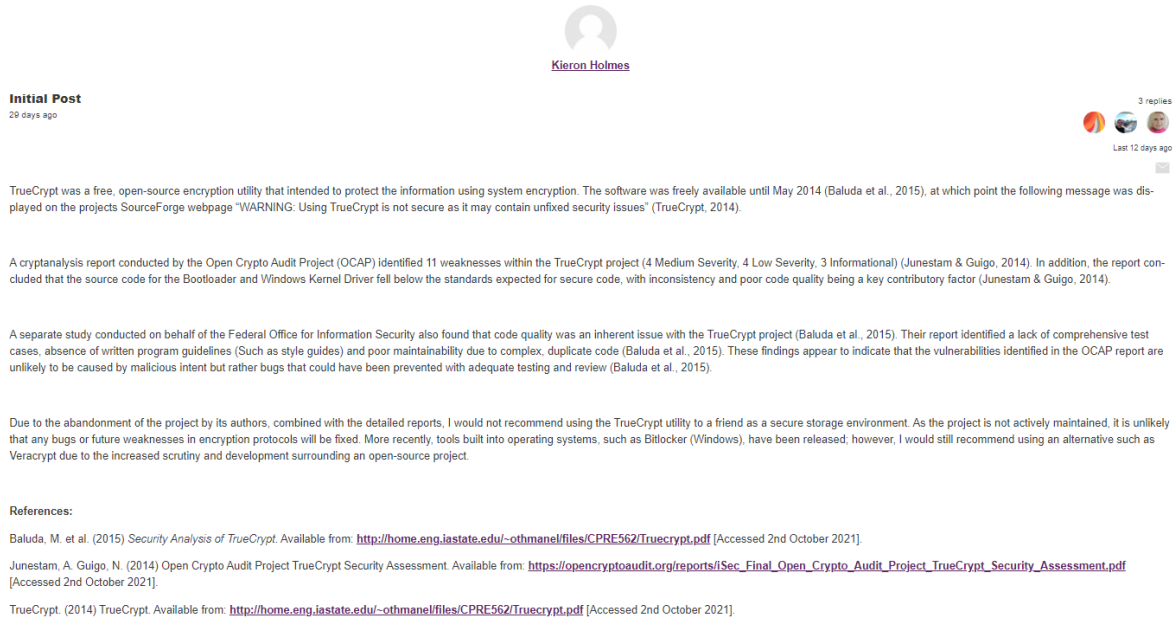
TrueCrypt was a free, open-source encryption utility that intended to protect the information using system encryption. The software was freely available until May 2014 (Baluda et al., 2015), at which point the following message was displayed on the projects SourceForge webpage “WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues” (TrueCrypt, 2014).

A cryptanalysis report conducted by the Open Crypto Audit Project (OCAP) identified 11 weaknesses within the TrueCrypt project (4 Medium Severity, 4 Low Severity, 3 Informational) (Junestam & Guigo, 2014). In addition, the report concluded that the source code for the Bootloader and Windows Kernel Driver fell below the standards expected for secure code, with inconsistency and poor code quality being a key contributory factor (Junestam & Guigo, 2014).

A separate study conducted on behalf of the Federal Office for Information Security also found that code quality was an inherent issue with the TrueCrypt project (Baluda et al., 2015). Their report identified a lack of comprehensive test cases, absence of written program guidelines (Such as style guides) and poor maintainability due to complex, duplicate code (Baluda et al., 2015). These findings appear to indicate that the vulnerabilities identified in the OCAP report are unlikely to be caused by malicious intent but rather bugs that could have been prevented with adequate testing and review (Baluda et al., 2015).

Due to the abandonment of the project by its authors, combined with the detailed reports, I would not recommend using the TrueCrypt utility to a friend as a secure storage environment. As the project is not actively maintained, it is unlikely that any bugs or future weaknesses in encryption protocols will be fixed. More recently, tools built into operating systems, such as Bitlocker (Windows), have been released; however, I would still recommend using an alternative such as Veracrypt due to the increased scrutiny and development surrounding an open-source project.

Screenshot:



Kieron Holmes

Initial Post

29 days ago

3 replies

Last 12 days ago

TrueCrypt was a free, open-source encryption utility that intended to protect the information using system encryption. The software was freely available until May 2014 (Baluda et al., 2015), at which point the following message was displayed on the projects SourceForge webpage "WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues" (TrueCrypt, 2014).

A cryptanalysis report conducted by the Open Crypto Audit Project (OCAP) identified 11 weaknesses within the TrueCrypt project (4 Medium Severity, 4 Low Severity, 3 Informational) (Junestam & Guigo, 2014). In addition, the report concluded that the source code for the Bootloader and Windows Kernel Driver fell below the standards expected for secure code, with inconsistency and poor code quality being a key contributory factor (Junestam & Guigo, 2014).

A separate study conducted on behalf of the Federal Office for Information Security also found that code quality was an inherent issue with the TrueCrypt project (Baluda et al., 2015). Their report identified a lack of comprehensive test cases, absence of written program guidelines (Such as style guides) and poor maintainability due to complex, duplicate code (Baluda et al., 2015). These findings appear to indicate that the vulnerabilities identified in the OCAP report are unlikely to be caused by malicious intent but rather bugs that could have been prevented with adequate testing and review (Baluda et al., 2015).

Due to the abandonment of the project by its authors, combined with the detailed reports, I would not recommend using the TrueCrypt utility to a friend as a secure storage environment. As the project is not actively maintained, it is unlikely that any bugs or future weaknesses in encryption protocols will be fixed. More recently, tools built into operating systems, such as Bitlocker (Windows), have been released; however, I would still recommend using an alternative such as Veracrypt due to the increased scrutiny and development surrounding an open-source project.

References:

Baluda, M. et al. (2015) *Security Analysis of TrueCrypt*. Available from: http://home.eng.iastate.edu/~othmanel/files/CPRE562/Truecrypt.pdf [Accessed 2nd October 2021].

Junestam, A. Guigo, N. (2014) Open Crypto Audit Project TrueCrypt Security Assessment. Available from: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 2nd October 2021].

TrueCrypt. (2014) TrueCrypt. Available from: http://home.eng.iastate.edu/~othmanel/files/CPRE562/Truecrypt.pdf [Accessed 2nd October 2021].

References:

Baluda, M. et al. (2015) Security Analysis of TrueCrypt. Available from: http://home.eng.iastate.edu/~othmanel/files/CPRE562/Truecrypt.pdf [Accessed 2nd October 2021].

Junestam, A. Guigo, N. (2014) Open Crypto Audit Project TrueCrypt Security Assessment. Available from:

https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 2nd October 2021].

TrueCrypt. (2014) TrueCrypt. Available from: http://home.eng.iastate.edu/~othmanel/files/CPRE562/Truecrypt.pdf [Accessed 2nd October 2021].