Cryptography

Case Study - TrueCrypt

- The (anonymous) TrueCrypt authors have said "Using TrueCrypt is not secure as it may contain unfixed security issues" (**TrueCrypt**, 2014). Does the cryptanalysis provided above prove or disprove this assumption?
- Would you be prepared to recommend TrueCrypt to a friend as a secure storage environment? What caveats (if any) would you add?

The analysis provided by the Open Crypto Audit Project would suggest that TrueCrypt did have unfixed security issues in 2014 and that this would have been the primary factor in the software being withdrawn. The audit found 8 issues with security which were classified as 4 medium and 4 low. One of the main issues was the lack of comments within the code which makes it difficult to maintain. Given the nature of evolving threats in cyber security, the need to maintain and improve software with regular updates would be an imperative.

The software has been discontinued for over a decade and it would not be recommended that this software should be relied on, even if it carried a perfect bill of health (which it did not) in 2014. Furthermore, TrueCrypt was designed to be compatible with now obsolete versions of Microsoft Windows operating systems. Installing and relying on this software may be unwise given that the operating systems they were designed to work with are now largely unsupported.

Finally, as the world of technology and cyber security is changing at a fast pace, it would be unwise to draw substantial conclusions from a report which is outdated. The report was one reliable source in 2014, but it would be better to review up-to-date software with current industry audits.

References

Junestam, J., & Guigo, M. (2014). *Open Crypto Audit Project: TrueCrypt*. Available from: Deliverable (opencryptoaudit.org) [Accessed 21 October 2024].

TrueCrypt (2014). *Warning:* Using TrueCrypt is not secure as it may contain unfixed security issues. Available from: https://truecrypt.sourceforge.net [Accessed 21 Oct. 2024].