Collaborative Discussion 2: Peer Response

Hi Sebastien,

A brief explanation of TrueCrypt is provided in your post, together with information on its historical relevance and the issues with its security and usability. For users of Windows XP, TrueCrypt offered solid solutions for various operating systems, including the ability to encrypt the entire operating system (Biggs, 2014).

However, TrueCrypt's abrupt demise in 2014 and the cryptic warning from its anonymous developers about security flaws caused alarm in the tech world. These worries are given more weight by the analysis by Junestam and Guigo (2014).

While acknowledging TrueCrypt's theoretical shortcomings, your post recognises its solid theoretical underpinnings. However, because of flaws and a lack of support, TrueCrypt is not advised to be used, according to Gujrati & Vasserman (2013). Use of TrueCrypt should come with a notice regarding its deprecated status and potential risks, as it is safer to use modern encryption tools (Messmer, 2014).

Your ontology design classifies weaknesses into three categories: cryptographic vulnerabilities, software stability issues, and user interface and usability issues. This makes it easier to understand TrueCrypt's shortcomings and potential impacts; as Noy and McGuinness (N.D.) explain, categorising ideas hierarchically helps organise them into broader categories and subcategories.

Your post thoroughly analyses TrueCrypt, recognising its historical significance while underlining the security and usability issues that resulted in its termination. Given the changing threat landscape and the absence of continued support for TrueCrypt, it makes sense to adopt more contemporary encryption technologies.

References:

Biggs, J. (2014). *TrueCrypt, An Open-Source Whole-Disk Encryption System, Leaves Users High And Dry*. [online] TechCrunch. Available at: https://techcrunch.com/2014/05/30/truecrypt-an-open-source-whole-disk-encryption-system-leaves-users-high-and-dry/ [Accessed 6 Oct. 2023].

Junestam, A. & Guigo, 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.

Gujrati, S & E. Vasserman (2013). *The usability of TrueCrypt, or how I learned to stop whining and fix an interface*. Conference on Data and Application Security and Privacy. doi:https://doi.org/10.1145/2435349.2435360.

Messmer, E. (2014). *TrueCrypt's abrupt demise 'puzzling, bizarre'*. [online] Network World. Available at: https://www.networkworld.com/article/2358255/truecrypt-s-abrupt-demise-puzzling-bizarre.html [Accessed 6 Oct. 2023].

Noy, N. F. & McGuinness, D. L. (N.D.). *Ontology Development 101: A Guide to Creating Your First Ontology.* [online] Available at: https://protege.stanford.edu/publications/ontology_development/ontology101.pdf.

Hi Liam,

Firstly, your post references TrueCrypt's statement from 2014, which admits there may be unfixed security issues. Federal Office for Information Security (2015) analysis supports this statement, as they identified 11 vulnerabilities and categorised them by severity. Therefore, it is evident that TrueCrypt did indeed have security issues.

The severity of the identified vulnerabilities was also classified, with four rated as medium, four as low, and three as informational by Junestam & Guigo (2014). This classification helps to understand the potential impact of these vulnerabilities on the system's security.

Your post highlighted particular places where vulnerabilities were found. These include the bootloader decompressor and readability, emphasised in the Federal Office for Information Security's (2015) report on the bootloader, Windows kernel driver, and installation procedure for the TrueCrypt project. Your post mentions security issues, access permissions, and information disclosure vulnerabilities. This specificity gives your post more depth and demonstrates that the vulnerabilities weren't simply theoretical but had real-world repercussions.

Your post strongly recommends against using TrueCrypt for secure storage. This is because the identified vulnerabilities relate to critical aspects of data security, such as data exposure and validation. Your post correctly argues that these vulnerabilities could open the system to various attacks, including brute force and denial of service attacks, as GeeksforGeeks (2020) highlights.

Moreover, the creators of TrueCrypt themselves expressed concerns about the system's security (Rashid, 2014). Therefore, trusting their judgment and avoiding using TrueCrypt for storing sensitive data is essential.

Even though your post makes effective use of Junestam & Guigo's (2014) cryptanalysis findings to highlight TrueCrypt's unresolved security issues and that you advise against using it to store sensitive data, it would be helpful to offer alternatives, given the known vulnerabilities and the software's developers' lack of confidence as mentioned by our colleague Sebastien.

References:

Federal Office for Information Security (2015). *Security Analysis of TrueCrypt* Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Truecrypt/Truecrypt.pdf?__blob=publicationFile&v=2.

Junestam, A. & Guigo, 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.

GeeksforGeeks. (2020). *Cryptanalysis and Types of Attacks*. [online] Available at: https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/

Rashid, F. (2014). *TrueCrypt Shut Down; What to Use Now to Encrypt Your Data*. [online] Available at: https://uk.pcmag.com/opinion/32788/truecrypt-shut-down-what-to-use-now-to-encrypt-your-data [Accessed 7 Oct. 2023].