Collaborative Discussion 2

Initial Post

TrueCrypt was a popular (Ratliff, 2016) data encryption programme, which was compatible with all major operating systems, however its development was discontinued in the light of multiple security issues and end of support for Microsoft XP (TrueCrypt, 2014), however multiple news organisations raised unusual circumstances (Hern, 2014).

Overall, I would not recommend a friend to use TrueCrypt. Firstly, given the developers abandoned the project over ten years ago, this is inherently a major security flaw. Software which is no longer kept up-to-date does not receive security updates, thus becomes vulnerable to new exploits. Additionally, the latest security mitigations are not carried, which results in exploitation being more successful and difficult to detect (NCSC, n.d.). Many organisations already use multiple outdated software packages with multiple vulnerabilities, exposing themselves to cyber attacks (Murciano-Goroff et al., 2024).

Additionally, although the report by Junestam & Guigo (2014) does not highlight any high-level vulnerabilities, only medium and low, a second report released by Balducci et al. (2015) highlights multiple high-severity issues which may cause significant failures in specific circumstances. For example, in one instance the random number generator for master encryption may fail, resulting in poorer encryption. The findings of the reports overall do not necessarily advise people against using TrueCrypt, but given these were produced a significant period of time ago, there is a high level of uncertainty as to their fit with current operating systems.

Figure 1 demonstrates an ontology of the findings based on the initial 2014 report, and adds vulnerabilities recorded in MITRE's CVE. Additional fields have been added to list requirements by users and which are affected by the listed vulnerabilities. The ontology could be expanded for the purposes of comprehensiveness and clarity. Some components of the ontology, such as 'hasVulnerability' has been demonstrated in the paper by Wang & Guo (2009).

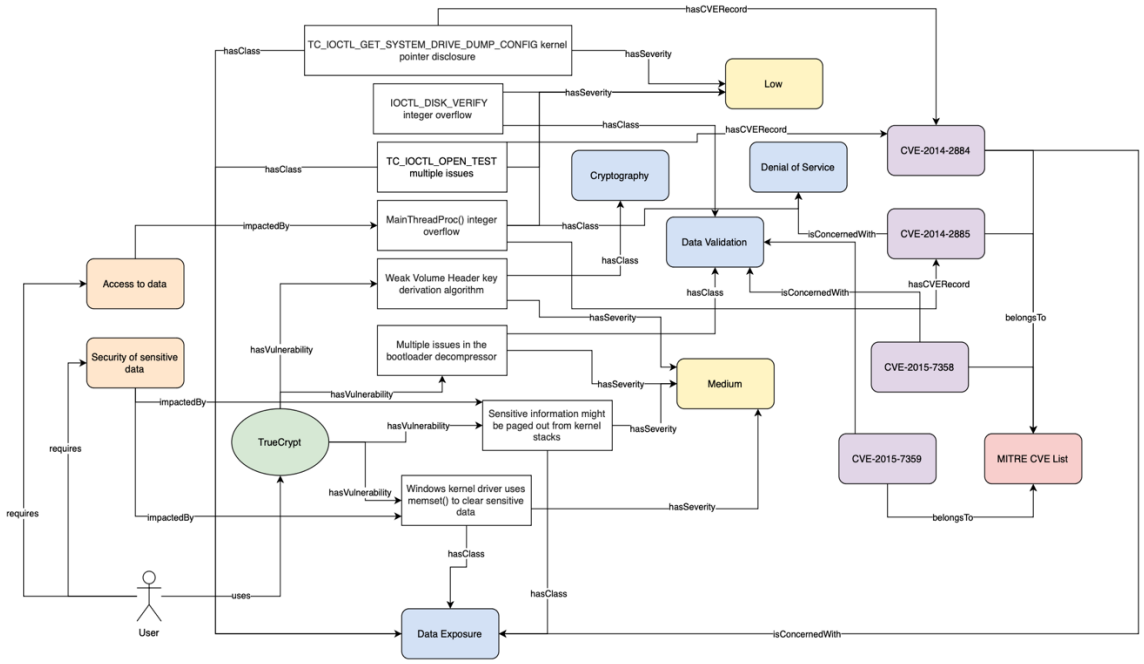

Figure 1. Initial ontology based on findings by Junestam & Guigo (2014).

References:

Balducci, A., Devlin, S. & Ritter, T. (2015) Open Crypto Audit Project: TrueCrypt. *Open Crypto Audit Project*. Available from: https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf [Accessed 11 December 2024]

Hern, A. (2014) Encryption software TrueCrypt closes doors in odd circumstances. *The Guardian*. Available from:

https://www.theguardian.com/technology/2014/may/30/encryption-software-truecrypt-closes-doors [Accessed 15 December 2024]

Murciano-Goroff, R., Zhuo, R. & Greenstein, S. (2024) Navigating Software Vulnerabilities: Eighteen Years of Evidence from Medium and Large US Organizations (No. w32696). *National Bureau of Economic Research*. Available from: https://www.nber.org/papers/w32696 [Accessed 15 December 2024]

NCSC (n.d.) Obsolete products. *National Cyber Security Centre*. Available from: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products [Accessed 15 December 2024]

TrueCrypt (2014) Homepage. *TrueCrypt*. Available from: https://truecrypt.sourceforge.net [Accessed 11 December 2024]

Ratliff, E. (2016) The Strange Origins of TrueCrypt, ISIS's Favored Encryption Tool. *New Yorker*. Available from: https://www.newyorker.com/news/news-desk/the-strange-origins-of-truecrypt-isiss-favored-encryption-tool [Accessed 15 December 2024]

Wang, J.A. & Guo, M. (2009) OVM: an ontology for vulnerability management. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (1-4).