Collaborative Discussion 2

Summary Post

In my initial post, I initiated an overview and analysis of TrueCrypt, a once-popular data encryption program, examining the extent of its security vulnerabilities and discussing why it should not be recommended for use today. The key argument was the halt of TrueCrypt's development and maintenance over a decade ago and the inherent security risks of using software with such state. Despite there being no major high severity issues identified, such as a backdoor vulnerability, it would be ill-advised to recommend outdated software, given how unpredictable its behaviour might be in the context of more modern, up-to-date hardware and software systems. This appears to be the opinion of my fellow peers too.

Following the feedback from my peers, I expanded my understanding of TrueCrypt's vulnerabilities, particularly those identified in the Balducci et al. (2015) audit report. This report revealed several high-severity issues, including potential failures in random number generation and susceptibility to cache-timing attacks in the AES implementation. The feedback helped me better understand the technical aspects of these vulnerabilities and their potential mitigations, such as using the CRYPT_VERIFYCONTEXT flag when calling CryptAcquireContext.

Finally, with tutor's guidance, I simplified my original ontology by removing user/actor information, as this made it more aligned with traditional ontology structures and ensured the focus is specifically on TrueCrypt and its vulnerabilities. To enhance this view, I also added mitigatedBy paths to the identified vulnerabilities to better illustrate how these security issues could be addressed. I hope this modification improved the clarity of the relationships between different components and made it easier to capture the value of the proposed ontology.

The peer discussions also emphasised the importance of considering alternative encryption tools, particularly VeraCrypt, which builds upon TrueCrypt's foundation while addressing many of its weaknesses. This addition of practical alternatives strengthened my original argument against using TrueCrypt and provided constructive solutions for those seeking secure encryption options. The combination of the security audit findings, peer feedback, and ontology improvements has resulted in a more comprehensive and practical analysis of TrueCrypt's security implications.

References:

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