Collaborative Discussion 2 – Cryptography case study: TrueCrypt

TrueCrypt is a software tool used to encrypt disks and even entire OS installations. The software has been discontinued as of 2014, however even during this time, multiple vulnerabilities were detected with this tool. While none of these vulnerabilities were in the 'High Risk' category, they are still significant and render the software susceptible to attack (Junestam & Guigo, 2014).

The weak volume header key derivation algorithm is susceptible to a brute force attack, even more so with today's technological advancements. The bootloader decompressor vulnerability can also be exploited to potentially access the password and therefore bypass the encryption. Aside from the other vulnerabilities, these two alone can be easily exploited to gain access to the encrypted files.

Furthermore, the report also identified low code quality. This would further complicate the process of fixing the current vulnerabilities and to update the software to an acceptable standard.

I would not recommend TrueCrypt to a friend as a secure environment primarily because this Software has not been updated since 2014. Even if the cryptanalysis had discovered zero vulnerabilities, the lack of ongoing support for this software would be reason enough to avoid using it. Vulnerabilities are continuously detected, and Software must be maintained to ensure its continued security and reliability. The security assessment provided was produced in 2014 so it is also significantly outdated and is very unlikely to cover all current vulnerabilities.

References

Junestam, A. & Guigo, N. (2014) Open Crypto Audit Project: TrueCrypt. Available from: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 11/12/22]