Collaborative Discussion 2: Cryptography case study: TrueCrypt

TrueCrypt was an open-source software intended for encrypting files or entire HDD volumes. It was developed for usage in the Windows XP operating system (University Information Technology Services, 2018). Eventually, it was disconnected in 2014, around the same time Microsoft stopped supporting the Windows XP operating system. Later, it was replaced by VeraCrypt software.

Following a TrueCrypt security assessment, it was found that the software suffered from eleven vulnerabilities in total, from which four were Medium severity, four were Low severity and three were just Informational (Junestam and Guigo, 2014).
Seven of the vulnerabilities were related to Data (four for Data Exposure and three for Data Validation), which is surprising for software intended to keep data safe. Additional issues related to the source code included lack of comments, insecure usage of functions and erratic variable types (Junestam and Guigo, 2014).

As a result of the security audit assessment, it became clear that the TrueCrypt software did not meet the expected code quality. Additionally, since the software is disconnected, it is not recommended to be used by anybody. I would only recommend its usage for migrating any already encrypted data to another software. For future data encryption, I recommend using the operating system's integrated encrypting software, which ensures compatibility and prompt security updates, or VeraCrypt.

References:

Junestam, A., and 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 03 July 2021].

University Information Technology Services (2018) What is TrueCrypt, and how can I use it to protect sensitive data? Available from: https://kb.iu.edu/d/auhm [Accessed 03 July 2021].