TrueCrypt was a free encryption software widely used in the 90s and early 2000s. It allowed users to encrypt at the operating system level and could be used for any of the main OS - Linux, Windows and Mac OSX. It was discontinued in 2014, due to the discovery of a large number of security vulnerabilities and code quality issues.

The most concerning vulnerability was the “Weak Volume Header key derivation algorithm”(Junestam and Giugo, 2014). The algorithm used to encrypt the volume was not of sufficient complexity and left the encrypted data vulnerable to brute force attacks. The article did not mention how vulnerable, i.e. how long it may take to complete a brute force attack, but suffice to say it was vulnerable enough to contribute to the discontinuation of the software.complexity resulting in an encryption key that could be found using brute force techniques. Another issue with TrueCrypt was that its compiler suppressed warnings within the code.

Would I recommend TrueCrypt to a Friend?

Though using TrueCrypt would definitely be better than using nothing, it has reached end of life and is not being supported, patched or upgraded against newly discovered vulnerabilities, and thus it would not be prudent to recommend to a friend. Other actively maintained tools that fulfil the same need include VeraCrypt (VeraCrypt, 2021).

References

Junestam, A. and Giugo, N. (2014) Open Crypto Audit Project TrueCrypt Security Assessment. Available at: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf (Accessed: 18/5/22).

VeraCrypt (2021) VeraCrypt - Free Open source disk encryption with strong security for the Paranoid: Code. Available at: https://www.veracrypt.fr/code/VeraCrypt/(Accessed: 18/5/22).