Discussion Topic

TrueCrypt was a popular and well-respected operating system add-on that could create encrypted volumes on a Windows and/or Linux system. In addition, it was also designed to create a complete, bootable volume that could encrypt the entire operating system and data for a Windows XP system. It was discontinued in 2014.

Case Study: Read the TrueCrypt cryptanalysis by Junestam & Guigo (2014) (link is in the reading list) and then answer the following questions:

- The (anonymous) TrueCrypt authors have said “Using TrueCrypt is not secure as it may contain unfixed security issues” (TrueCrypt, 2014). Does the cryptanalysis provided above prove or disprove this assumption?
- Would you be prepared to recommend TrueCrypt to a friend as a secure storage environment? What caveats (if any) would you add?

Remember to save this to your e-portfolio.

Present an ontology design which captures the weaknesses of TrueCrypt, and organise them according to their severity. Expand the ontology design by considering the factors which will cause each weakness to become an issue from a user's perspective. For example, if a user wishes to encrypt a disk storing bank details using TrueCrypt, which weakness of the software might cause this specific user goal to be negatively impacted?

My post:

TrueCrypt was a popular encryption software with a user-friendly interface and cross-platform support. It faced security concerns and controversies before being discontinued in 2014 (Vaughan, 2023).

The practice of identifying weaknesses in cryptographic techniques to decode ciphertext without the use of a secret key is known as cryptanalysis. In this process, malicious actors may attempt to obtain information about plaintexts or ciphertexts or uncover the private key and other functionally equivalent methods. The attacker's goal will depend on their specific needs within a particular attack context. Despite having access to only a limited amount of unencrypted data, attackers may still be able to meet their objectives (Rezos, N.D.). Hence, Junestam & Guigo (2014) correctly assumed that TrueCrypt is not secure.

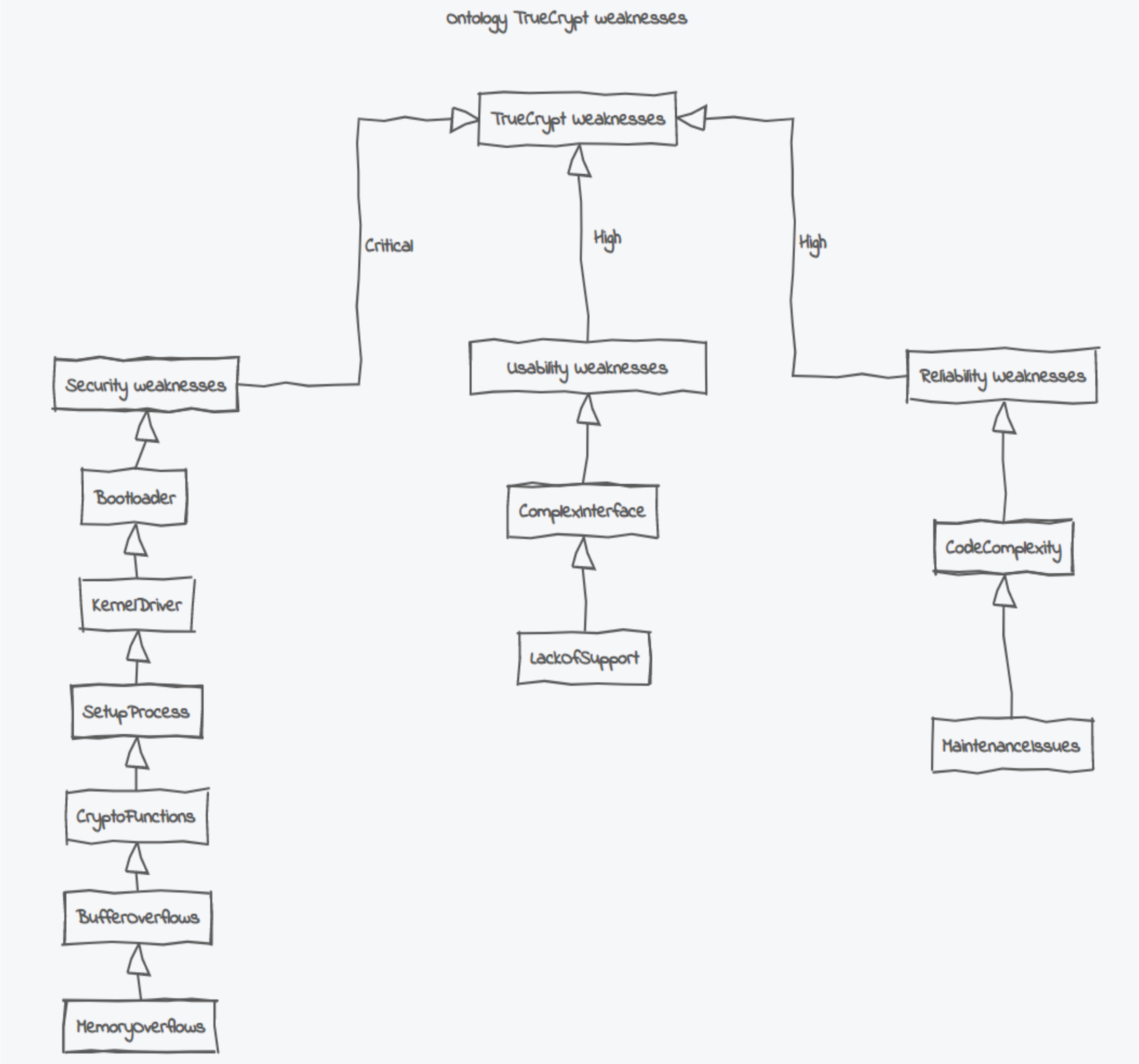
Cryptology involves creating and breaking secret codes through cryptography and cryptanalysis, respectively. Various attacks, such as brute force and differential cryptanalysis, identify weaknesses and enhance security (GeeksforGeeks, 2020). According to Junestam & Guigo (2014), although the web documentation for TrueCrypt was relevant, potential flaws were found in the Volume Header's integrity checks.

Considering the factors above, suggesting TrueCrypt to a friend for secure storage would not be advisable. It is an unsafe option for protecting sensitive data due to the need for development and known flaws.

Ontology design which captures the weaknesses of TrueCrypt:

The TrueCrypt Weakness represents TrueCrypt's vulnerabilities, consisting of three essential categories: security weaknesses, usability weaknesses, and reliability weaknesses, which categorise the various weaknesses. Each category further breaks down into specific sub-attributes.

Weak encryption includes Bootloader, KernelDriver, SetupProcess, CryptoFunctions, BufferOverflows, and MemoryOverflows, while usability weaknesses encompass ComplexInterface and LackOfSupport. On the other hand, reliability weaknesses include CodeComplexity and MaintenanceIssues.



References:

Vaughan, A. (2023). *TrueCrypt Alternatives 2023: The Best Secure Storage Solutions*. [online] TechnologyAdvice. Available at: https://technologyadvice.com/blog/information-technology/truecrypt-alternatives/

Rezos, KristenS, kingthorin (N.D.). *Cryptanalysiss*. Software Attack | OWASP Foundation. [online] Available at: https://owasp.org/www-community/attacks/Cryptanalysis#:~:text=Cryptanalysis%20is%20a%20process%20of.

Junestam, A. & Guigo, N. (2014). *Open Crypto Audit Project TrueCrypt Security Assessment Prepared for: Prepared by*. [online] Available at: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf.

GeeksforGeeks. (2020). *Cryptanalysis and Types of Attacks*. [online] Available at: https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/

Osborne, C. (2015). *TrueCrypt critical flaws revealed: It's time to jump ship*. [online] ZDNet. Available at: https://www.zdnet.com/article/truecrypt-critical-flaws-revealed-its-time-to-jump-ship/.

Federal Office for Information Security (2015). *Security Analysis of TrueCrypt* Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Truecrypt/Truecrypt.pdf?__blob=publicationFile&v=2.

Gujrati, S & E. Vasserman (2013). *The usability of TrueCrypt, or how I learned to stop whining and fix an interface*. Conference on Data and Application Security and Privacy. doi:https://doi.org/10.1145/2435349.2435360.

Unit 8 – Reflection:

Throughout Unit 8, I have delved into the intricate world of cryptographic libraries. My studies also included a comprehensive analysis of the 'Cryptography case study: TrueCrypt discussion', which I thoroughly researched. I have documented my extensive findings and personal insights on this subject matter in great detail within my ePortfolio.

Additionally, I had the opportunity to improve my coding skills in the 'Cryptography Programming Exercise' seminar, which required me to develop a Python program using Codio. The program I created was designed to take a text file and later produce an encrypted version as a file within the user's folder on the Codio system. I successfully demonstrated the program's functionality during the seminar, which was an outstanding achievement.

This week's learning experience has significantly enhanced my understanding of cryptography's vital role in maintaining application security. I am grateful for the opportunity to expand my knowledge and skills in this area.