**Collaborative Discussion 2: Cryptography case study: TrueCrypt**

#### **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” ([**http://truecrypt.sourceforge.net/**](http://truecrypt.sourceforge.net/), 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?
* 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?

***Summary post with ontology design***

TrueCrypt was published in 2004, although created by anonymous developers, and used by Edward Snowden, a previous contractor of the government of the United States (US) who had leaked secret documents (Miao, 2010). In 2008 in Brazil, a banker, Daniel Dantas, who was accused of being involved in financial crime, was found having hard drives that were encrypted via TrueCrypt (Casey *et al*., 2021). The FBI failed to read the data on those hard drives and returned them to Brazil in 2010 (Casey *et al*., 2021).

Nevertheless, in 2014, TrueCrypt retired, as it had security vulnerabilities that could not be remediated, thus making it unsafe to use (Zhang *et al*., 2019). Despite the “Gibson Research Corporation” and the “Committee To Protect Journalists” claimed that it was still safe to consume TrueCrypt, TrueCrypt’s website provided detailed instructions to use BitLocker instead (Zhang *et al*., 2019). Zhang *et al*. (2019) suggest using TrueCrypt 7.1a from a secure environment, as TrueCrypt 7.2, available on the official website, does not allow to create encrypted volumes.

I would not suggest using TrueCrypt, as it unsafe to store data (Colp *et al*., 2015). However, VeraCrypt, although based on TrueCrypt, could be used, as it is deemed safe to generate encrypted files on either hard or external drives in any of the main operating systems (Windows, MacOS, Linux) (Kedziora *et al*., 2017). VeraCrypt is a viable alternative to Windows’ native encryption due to its user-friendly interface (Kedziora *et al*., 2017). VeraCrypt fixed all serious security vulnerabilities that were identified in TrueCrypt by the “Open Crypto Audit Project”, including buffer overflows and memory leaks (Kedziora *et al*., 2017).

In VeraCrypt, the user can choose an appropriate encryption level and a process to hide the files on the chosen drive (Kedziora *et al*., 2017). Eventually, a strong password is set to protect the drive (Kedziora *et al*., 2017). VeraCrypt enhanced the PBKDF2 algorithm, thus providing further protection against cyber-attacks that were attempting to impact performance negatively (Kedziora *et al*., 2017). Furthermore, VeraCrypt has a size of only 20 MB and is not memory-intensive, except for releasing the encrypted volume (Kedziora *et al*., 2017).

Considering its advanced features but also taking into account its user-friendly interface, VeraCrypt would be more suitable for slightly more advanced users (Kedziora et al., 2017). As BitLocker is not compatible with Mac as default, FileVault 2 is compatible with it and, thus, could be another alternative for 'regular' Mac users; nevertheless, it is worth noting that it does not enable to create encrypted containers. Instead, in VeraCrypt, the user can choose an appropriate encryption level and a process to hide the files on the chosen drive (Kedziora et al., 2017).

As per the attached file ‘Ontology\_design\_TrueCrypt.pptx’, please find an ontology design regarding TrueCrypt, which presents its security vulnerabilities based on their severity and details the factors that cause them from a user’s perspective.

**References**

Casey, E., Fellows, G., Geiger, M., & Stellatos, G. (2011) The growing impact of full disk encryption on digital forensics. *Digital Investigation* 8(2): 129-134.

Colp, P., Zhang, J., Gleeson, J., Suneja, S., De Lara, E., Raj, H., ... & Wolman, A. (2015) Protecting data on smartphones and tablets from memory attacks. In *Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems* (pp. 177-189).

Kedziora, M., Chow, Y. W., & Susilo, W. (2017) Improved threat models for the security of encrypted and deniable file systems. In *International Conference on Mobile and Wireless Technology* (pp. 223-230). Springer, Singapore.

Miao, Q. X. (2010) Research and analysis on encryption principle of TrueCrypt software system. In *The 2nd International Conference on Information Science and Engineering* (pp. 1409-1412). IEEE.

Zhang, L., Deng, X., & Tan, C. (2019) An extensive analysis of TrueCrypt encryption forensics. In *Proceedings of the 3rd International Conference on Computer Science and Application Engineering* (pp. 1-6).