**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/, 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?

**Answer:**

Based on the authors finding regarding the severity of the issues, it makes sense that in 2014 and before, the TrueCryptic was in use, because the technology anyway had not been as advanced as today. Besides that, anyone who considered conducting any malicious activity would have needed a solid amount of knowledge. The authors reported that there were not any severe issues detected regarding TrueCrypt, however, a few weaknesses appeared to be medium severe. Moreover, as stated by the authors, the otherwise potential malicious code was not created intentionally and it is more like a result of so-called bugs in the code (Junesten & Guigo, 2014).

The cryptanalysis provided in the paper aligns with the statement that the TrueCrypt is not safe for use, because the analysis tackles pretty much every aspect of the software, together with the code design patterns, memory management, possible bootloader issues, etc.

Overall I would probably suggest a friend to use the TrueCryptic in 2014, however at the present it appears to be too risky for the use. The biggest issue that I've seen is the outdated components, moreover, the systems that ran the software were built differently in the past, hence installing the software on a modern computer/system is questionable by itself, as regards system compatibilities.

**References:**

Junestam, A., Guigo, N. (2014) Open Crypto Audit Project Truecrypt Security Assessment. Available from: https://opencryptoaudit.org/reports/iSec\_Final\_Open\_Crypto\_Audit\_Project\_TrueCrypt\_Security\_Assessment.pdf [Accessed 21 June 2023].