Unit 8 – Summary

In unit 8 we worked on a case study regarding the safety of the discontinued TrueCrypt software.

TrueCrypt was an open-source operating system add-on intended for encrypting files or entire HDD volumes in Windows XP or Linux platforms. It was discontinued in 2014 (along with the termination of support for Windows XP) because it suffered from various vulnerabilities.

Most of my fellow students identified that using TrueCrypt would not be sensible, considering that there are dozens of supported and secure software available for usage such as VeraCrypt (David, Anrich, Yohay) or Microsoft's Bit locker (Uzayr). I would only recommend using TrueCrypt to migrate any already encrypted data to another software.

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].