Summary Post:

In summary, I would like to point out that TrueCrypt is not a secure option for safeguarding sensitive data. Rezos (N.D.) highlights that cryptanalysis can decode ciphertext without the secret key, leaving it vulnerable to attackers who aim to uncover private keys or equivalent methods to obtain information. Even limited access to unencrypted data can still allow attackers to achieve their objectives.

Based on its need for development and known vulnerabilities, I would not recommend using TrueCrypt to a friend. While cryptology involves creating and breaking secret codes through cryptography and cryptanalysis, security can be enhanced by identifying weaknesses through attacks such as brute force and differential cryptanalysis (GeeksforGeeks, 2020). Unfortunately, TrueCrypt's web documentation mentions potential flaws in the Volume Header's integrity checks (Junestam & Guigo, 2014).

To further illustrate TrueCrypt's weaknesses, I have presented an Ontology design outlining its three essential categories: security, usability, and reliability. Each class is further classified into specific sub-attributes.

I have also commented on Sebastien's and Liam's posts. Sebastien's post highlights TrueCrypt's security and usability issues, which led to its termination. Given the changing threat landscape and the absence of continued support for TrueCrypt, Sebastien suggests adopting more contemporary encryption technologies makes sense. Furthermore, Liam's post highlights TrueCrypt's unresolved security issues and identifies vulnerabilities that could open the system to various attacks. The severity of these vulnerabilities was classified, with four rated as medium, four as low, and three as informational (Junestam & Guigo, 2014). Given the software developers' lack of confidence and the known vulnerabilities, I suggested that offering alternatives for safeguarding sensitive data would be helpful.

References:

Rezos, KristenS, kingthorin (N.D.). *Cryptanalysiss*. Software Attack | OWASP Foundation. [online] Available at: https://owasp.org/www-community/attacks/Cryptanalysis.

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

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.

Unit 10 – Reflection:

During the studies of this week, I had the opportunity to delve deeper into the topic of Distributed Computing to Microarchitectures, which was the subject of my study in Unit 10. I found this subject to be particularly intriguing and insightful, as it helped me understand some of the key concepts, vulnerabilities, and security attacks that impact modern-day technologies.

I also had the pleasure of participating in collaborative discussions with my peers, where I was able to contribute by sharing my own summary post. In my post, I highlighted the significance of ontologies in describing the relationships between concepts, which in turn facilitate automated reasoning about data. I learned that such reasoning can be easily implemented in semantic graph databases that use ontologies as their semantic schemata.

In addition, the ePortfolio component that focused on facet data was a great learning experience for me. I gained valuable knowledge about the importance of protecting systems against data leakage, and I was able to engage in creating the best approach to implementing the facet system in Python.

This week's learning activities have been both informative and engaging, and I look forward to continuing my exploration of these topics.