**TrueCrypt is old and dangerously unsecure (Summery Post)**

In my initial post, I have helped point out how dangerously insecure TrueCrypt has become since it ceased development back in 2014. Even the TrueCrypt website states that the software is insecure and should no longer be used. Some of my colleagues argued that it is ok to use the software as long as the data is offline and not available online. However, I have pointed out that even if the data is offline, an attacker can still get ahold of it if someone plugged a malicious USB into the device. In previous posts, I have given examples of such malicious USB devices on what they are cable of doing. For instance, the Rubber Ducky USB drive can be programmed to perform any number of things like infecting the device with a worm, virus or trojan, extracting data from the device, act as a zombie device, install key logging software on the device, and much more.

In this unit, we have learnt a great deal about how software can be insecure. Things like buffer overflow and integer overflow don't seem like much of a security risk at the start. However, once you understand how an attack can utilize buffer overflow, you start to realize how dangerous these can be and such an easy mistake can occur.

According to James Gosling, one of the reasons why Java was created is to remove pointers and help programmers reduce the number of bugs they have in their code. Security was one of the driving pillars of the creation of Java. In C and C++ it is easy to forget to free memory or create a memory leak or have a buffer overflow. On the other hand, language like Java and Python protects the programmer to a certain degree from these issues.

References:

Fridman, L. (2020) Java was created because of pointer bugs in C/C++ | James Gosling and Lex Fridman, YouTube. Available at: https://youtu.be/RrMptmNYkSw?t=636 (Accessed: December 12, 2022).