Advanced Security 1 – DT211-4 and DT228-4

Cryptographic Applications (10%)

Part A

There has been a lot of media reports on the security concerns caused by Heartbleed bug (http://heartbleed.com/) and Shellshock bug or Bashdoor bug (http://en.wikipedia.org/wiki/Shellshock_%28software_bug%29). How are these software bugs related to Cryptography? List ways in which the vulnerabilities caused by these bugs can be eliminated or mitigated. Does the appearance of these bugs mean that Open source software is less secure than proprietary software? Write a report of at most one page.

Part B

In the last few years the use of so called cryptocurrency has increased significantly in the world. There are a lot of social, political and economical reasons for this raise of virtual currency. The major attraction to those who use the cyrptocurrency is that it is decentralized, no control from Central banks. One of the most widely used cryptocurrency is called the Bitcoin (https://bitcoin.org/). Unlike traditional currencies, which are issued by central banks, Bitcoin has no central monetary authority. Instead it is underpinned by a peer-to-peer computer network made up of its users' machines, akin to the networks that underpin Bit Torrent, a file-sharing system, and Skype, an audio, video and chat service. Bitcoins are mathematically generated as the computers in this network execute difficult number-crunching tasks, a procedure known as Bitcoin "mining".

In this part of the assignment you will be required to set-up a bitcoin mining operation. Run the bitcoin mining operation for at least 12 hours. Search, install and run mobile apps in your mobile phone that will enable you to take part in Bitcoin mining. You may wish to join a Bitcoin mining pool to experience how computation collaboration works. It may help your research and implementation if you can create a Google Alert on Bitcoin mining. Finally, write a report of at most a two pages detailing your experience. Your report must include a list of other Cryptocurrencies, the level of difficulty involved in mining bitcoins using laptop and mobile phone, usage of Bitcoin in Ireland, legality of bitcoins and the future of bitcoins.

References

http://www.nature.com/news/the-future-of-cryptocurrencies-bitcoin-and-beyond-1.18447#/b3