

*An Roinn Dlí*

***Department of Law***

**Advanced Security – Cryptographic Applications**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tim Browning\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student I.D. No.: \_\_\_\_\_\_\_\_\_\_\_\_C14519547\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Programme (Course) : \_\_\_\_\_\_\_\_DT211C\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Module (Subject) : \_\_\_\_\_\_\_\_\_\_\_Advanced Security\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lecturer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Aneel Rahim\_\_\_\_\_\_\_\_\_\_\_**

**Date of Submission: \_\_\_\_\_\_\_\_\_\_31st October 2017\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Author’s Declaration:**

I hereby acknowledge that this essay is my own original work. All quotes, references and assistance received are acknowledged.

**Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_Tim Browning\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_31st October 2017\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Q1)

How are these software bugs related to Cryptography?

The Heartbleed Bug is a data leakage in the openSSL ­­open source library. This consists of the Secure Socket Layer and Transport Layer protocols. Encryption is the backbone of Internet Security. It protects users’ data, passwords and financial details. HTTPS is one of the most widely used protocols. The S from HTTPS means its encrypted over SSL/TLS. But Heartbleed has drawn a lot of attention to itself because it raises a lot of flags regarding internet security. OpenSSL is the most popular open source cryptographic library and TLS. TLS (transport layer security) is used to protect your privacy and transactions. You might have software on your computer that could expose your data from your computer if you connect to unsafe services.

The Shellshock bug was found in Linux operating systems. It was widely reported that Yahoo! servers had been compromised in an attack related to the Shellshock issue. Shellshock rates a 10 on the scale of vulnerabilities.

OpenSUSE has provided this fix in the meantime and it has been successfully tested for compatibility with Cryptshare.

List ways in which the vulnerabilities caused by these bugs can be eliminated or mitigated?

The main thing you should do immediately to mitigate the bug is to change your passwords for any of the affected sites for which you have a login account. If you used the same password for multiple sites, one of them may have been compromised, which means they are all compromised. Another method would be to upgrade your openSSL version so that it is not vulnerable to Heartbleed. The openSSL upgrade should fully patch most issues.

Does the appearance of these bugs mean that Open source software is less secure than proprietary software?

Bugs are said to be fixed faster in Open source projects then in proprietary software. Heartbleed was undiscovered for two years which demonstrates that the security is not up to scratch in open source software. I think there are many users using open source software meaning bugs should become easier to discover and rectify. Using open source software comes with drawbacks. Having bugs is one of them. But that does not go to say that proprietary software is less secure. Internet explorer had a security defect for years which went unnoticed. The main advantage of finding bugs in open source software is that there is way more eyes on the software. The more eyes the better chance there is of finding bugs.

Open source is less secure. Some Propriety software should be left to the experts to fix if a bug arises. Proprietary software which uses financial information, personal information and important data shouldn’t be open source as this can lead to hackers finding loop holes in software leaving the software extremely vulnerable.

Q2)

list of other Cryptocurrencies…

**Bitcoin** – Is a cryptocurrency and a digital payment system. The system is peer-to-peer, and transactions take place between users directly. Bitcoins are created as a reward for a process known as mining and can be exchanged for other currencies.

**Litecoin -** is a peer-to-peer cryptocurrency and is open source. It differs from bitcoin as it adopts segregated witness and the lightning network. These allow a greater number of transactions to be processed by a network.

**Emercoin -** is a cryptocurrency that uses both POW (proof of work) and POS (proof of stake)

The level of difficulty involved in mining bitcoins using laptop and mobile phone…

From my experience I have found that Mining Bitcoins has proven to be easy to setup, not much reward and a slow burner. So I chose NiceHash on desktop to mine Bitcoins, at first I found it difficult to understand what it does but when I did, it was fairly straight forward. When I downloaded it and ran it. It told me the specs of my computer and then made me enter in my wallet details. To set up the wallet I used a service called Coinbase. It is a free service which allows you to buy and sell bitcoins but also have addresses. I used an address to link my NiceHash account with my Coinbase. Earnings from NiceHash will be stored in a Coinbase account. And that was it. I was mining bitcoins. My computers graphics card was not in the supported list but my CPU was. After 1 day of mining bitcoins I didn’t receive any bitcoins. I think this is because I didn’t have a computer with good benchmarks. So this meant my results aren’t too exciting.

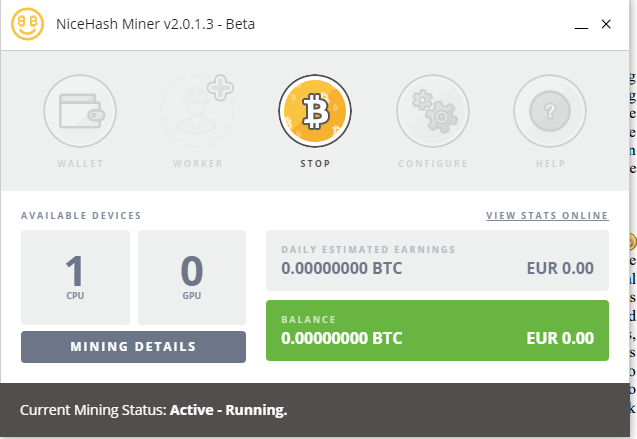


Figure 1

AntMiner is a piece of hardware that accelerates the production of bitcoins when using NiceHash. I have looked at many YouTube tutorials and found out that it works on a basis of the more you invest at the start the more return on investment you will get. AntMiner uses a substantial amount of power. Depending on which AntMiner you purchase you are likely to start making a profit after 4-5 months. This is quite reasonable considering the fact that you don’t have to put that much work into it. An issue with bitcoin mining is that you will have to have your computer on all the time so you might have put up with loud fans and an overheated room. You will have to consider good ventilation in the room which contains the equipment you are using for bitcoin mining.

The app I used for mining bitcoins on mobile device was called BlockChain. This app is only used for buying and selling bitcoins. It is an extremely convenient app to keep track of your earnings. BlockChain is also secure as you require a 2-step authentication, disables access from Tor and disables brute-force attacks on your account. BlockChain make their money from transaction fees.

In terms of difficulty I didn’t find myself pulling my hair out when using these services/application. They are all stress free. However, to become a successful bitcoin miner you will have to spend a lot on hardware.

Usage of Bitcoin in Ireland.

BitEx.ie is Irelands oldest bitcoin provider and it is a member if the official Irish Bitcoin foundation. You are able to buy and sell bitcoins through this company. It eliminates bank and PayPal charges.

Legality of bitcoins

The legality of bitcoins varies substantially from country to country. Its status as money varies. In Ireland bitcoins are deemed legal however the central bank stated that it does not regulate them.

In countries like Kyrgyzstan, Ecuador and Bangladesh they are Illegal. In Bangladesh you could be put in prison for using Bitcoin and in Kyrgyzstan they say it’s a violation of the law of our state.

Future of bitcoins.

The big question with bitcoins is: Is bitcoins profitable or is it a gamble? Bitcoins unique architecture is set up so its gets progressively more resource-intensive and is limited to 21 million Bitcoins. In 2013 Bitcoin was trading between 10 and 15 dollars. Now its trading at around 5,600 dollars. However, huge fluctuations have occurred with this cryptocurrency which has made traders wary whether Bitcoins has a future or not.



Figure 2

Bitcoin enthusiasts suggest that there are substitutes for Bitcoin however they claim that this will never be an issue as Bitcoin was the pioneer and has first-mover privileges. I see bitcoin being the most popular cryptocurrency however I do see that it will peak sooner rather than later.

## **References**

Cryptshare.com. (2017). *Shellshock Bug: Fix available*. [online] Available at: https://www.cryptshare.com/es/blog/shellshock-bug-fix-available/ [Accessed 31 Oct. 2017].

En.wikipedia.org. (2017). *Legality of bitcoin by country or territory*. [online] Available at: https://en.wikipedia.org/wiki/Legality\_of\_bitcoin\_by\_country\_or\_territory [Accessed 31 Oct. 2017].

Q&A (2017). *Heartbleed: Q&A*. [online] Insights.sei.cmu.edu. Available at: https://insights.sei.cmu.edu/sei\_blog/2014/05/heartbleed-qa.html [Accessed 31 Oct. 2017].

TechRepublic. (2017). *Why open source development is getting more secure*. [online] Available at: https://www.techrepublic.com/article/open-source-vs-proprietary/ [Accessed 31 Oct. 2017].

AntMiner:

https://www.youtube.com/watch?v=b3Qbr85Ko-c