**Advanced Security 1 – Assignment**

**C16466214 – Aron O’Neill**

**Part 1:**

In April 2014, the Heartbleed bug was discovered to be a critical bug caused from a serious flaw in OpenSSL which enabled attackers to access sensitive information. OpenSSL is an encryption software providing secure communications between devices connected on the web. A part of the SSL protocol involves one computer sending a heartbeat message to another, to verify that the other computer is still online. The Heartbleed bug is the method of passing a malicious heartbeat message which fools the computer at the other end into sharing sensitive information. The Heartbleed bug arose when it was realized that the computer receiving the heartbeat message failed to check whether the request needed to be as long as it requested, meaning that attackers could make a request for 60KB of memory, only use 20KB and set aside the 40KB for extracting the sensitive data. The bug was discovered on the 1st and got patched by the 7th of April.

Shellshock is a bug, potentially affecting Linux and Unix operating systems. The bug involves the attacker tracking harmful code to the environment variable of a computer through bash, which will then run once received. Attackers could utilize the vulnerability creating a specific HTTP request containing headers including “Referer: () { :;}; echo "NS:" $(</etc/passwd)”. Upon receiving the HTTP request, the target responds by sending the information stored in the file ‘/etc/password’. The shellshock bug was found on the 12th of September, 2014, and got patched up by the 24th of the same month.

These software bugs relate to Cryptography as cryptography involves the studying of encryption techniques used for securing data so that it can be securely communicated between devices. Cryptographers are constantly thinking of possible vulnerabilities in both, the encryption tools used, and the device storing the sensitive data, so that they can avoid any potential attacks. To avoid preventable attacks, cryptographers must be thorough in designing their software, for example, validating the length of requests as discussed within the Heartbleed bug.

The vulnerabilities caused by the Heartbleed bug can be eliminated by updating to the latest version of your server or re-key all your SSL/TLS certificates, install the new certificate and then remove all certificates that have been used with vulnerable versions of OpenSQL.

Ways to mitigate or eliminate vulnerabilities in the Shellshock bug would be to provide policy-based installation of security updates in a company with, closed-loop verification and the ability to manage patches across multiple platforms from a single point of control. It must also reduce patch deployment time to lower the risks associated with Shellshock. IBM have software able to prevent these attacks through its IBM Security Network Intrusion Prevention product which has been offering help to many companies since 2007.

Open source software is less secure than proprietary software as there are usually communities of developers coding open source software over a short period of time and not usually the months spent developing proprietary software. Therefore the chances of finding security issues in open source software are greater. This can be seen through the appearance of these bugs.

**Part 2:**

Cryptocurrency popular has grown substantially over the last number of years, with it now being accepted in some shops, schools and online stores. Bitcoin, Ethereum and Ripple are among the most popular cryptocurrencies used today and in the following passages I will expand on each.

List of Cryptocurrencies:

* Bitcoin
* Ethereum
* Ripple
* LiteCoin
* Dash
* Bitcoin Cash

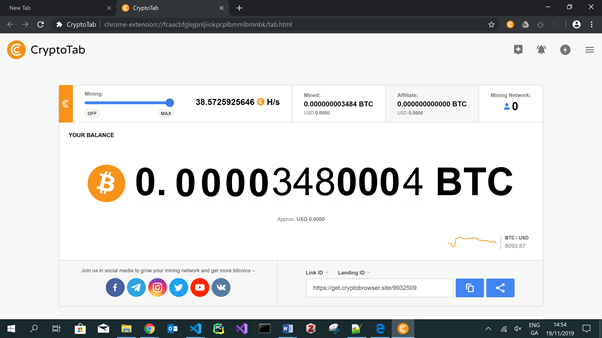
***Ethereum*** is a global, open-sourced platform for decentralized applications. Despite only launching in 2015, Ethereum is the largest open-ended decentralized software platform available.The difference between Bitcoin and Ethereum is that Bitcoin is simply an online currency whereas Ethereum is a ledger technology that companies are using to build new programs. Ethereum comes accompanied with its own programming language which runs on a blockchain, enabling developers to build and run distributed applications.

***Ripple*** is the third largest cryptocurrency by market cap, after both, Bitcoin, and Ethereum. It is a real-time gross settlement system and currency exchange system created by a US based company called Ripple Labs in 2012. It acts as a cryptocurrency as well as a network for financial transactions.

The evolving difficult of the process of bitcoin mining gives the impression that only those with high powered, specialized devices to be able to extract bitcoin. Although, this is in part true, any person with average computing power can still mine bitcoin but the rate of bitcoin mining will take a lot of power to continuously run and will return very little.

Mining Bitcoin on Laptop / Mobile:

To setup a bitcoin mining operation, I first research the different applications available. I decided upon implementing the web application called CryptoTab as it can be used on both, mobile phones and laptops. It is also a very user-friendly application, allowing me to simply sign up with google on my android device. It can ran on either your browser on your phone or your desktop browser and the server dependent mining can be started through the use of a slider which decides on the power to be used by the device. In the screenshot below, we can see the speed at which my laptop is mining as well as my current bitcoin balance.



After I had successfully mined bitcoin for more than 12 hours, I joined a mining network, resulted in 2 being shown instead of 0 in my mining network tab. This to navigate user interface shows that anyone can start mining bitcoins but it is dependent on your computer or phone processing power.

Usage of Bitcoin in Ireland:

The use of bitcoin in Ireland has surged in the last few years with bars, cafes, dentists and even some schools accepting payment in the form of bitcoin. This can even be seen beside out college, on anguier street with Crypto Café now accepting bitcoin. Another example of the now widespread use of bitcoin in Ireland can be seen on the northside of Dublin, where you can now purchase bitcoin using an ATM. The rise in the use of bitcoin in Ireland has seen it become accepted as a payment method in the Berlin Bar on Dame street.

Legality & future of Bitcoins:

Each country has taken their own stance on the legality of bitcoin with some countries deciding to ban it outright and others embracing it. Countries who have embraced bitcoin and legalized it include the US, Australia and the EU. The reason why some countries have said no to bitcoin is that it can be used anonymously to conduct transactions between any account holders, anywhere and anytime across the globe, which makes it attractive to criminals and terror organizations. Countries who have decided against the legalizing of bitcoin are way of its volatility, decentralized nature as well as criminalized activities associated with it. These countries include China and Russia.

There is much debate about the future of bitcoin as it is so volatile, meaning there will continuously be a rise and drop in the price of bitcoin. There is an argument that other cryptocurrencies may surpass bitcoin due to some features such as decentralized application development which can be seen from the Ethereum blockchain. Some people believe that the popularity in bitcoin will drop as it becomes so resource intensive whereas others believe it will only grow in popularity as there are only 21 bitcoins available to be mined. Overall it is hard to gauge where exactly bitcoin and many other cryptocurrencies will be but I feel they will be slowly become more and more accepted as a recognized payment method in society.