Advanced Security Assignment

A. These software bugs Heartbleed and Shellshock are related Cryptography in the following ways. Cryptography is the study of encryption and decryption but the encryption protocols in both cases can be easily compromised therefore there is week security. The Heartbleed bug is a serious bug in the OpenSSL cryptographic library. This is a security weakness that lets people steal protected information. This is information that is protected by the SSL/TLS encryption used to secure the internet. SSL/TSL provides communication security and privacy over the internet for email, instant messaging and VPNs. This bug allows anyone on the internet to read the memory of the systems that have been protected by the OpenSSL software. Names, passwords and secret keys can all be seen. Attackers can eavesdrop on communications and steal data from the user. To eliminate the Heartbleed bug the OpenSSL team released version 1.0.1g in the initial stages to fix it. Now any version higher will also work like 1.0.2. If for some reason, you can't get upgrade your version you can recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS this will also remove the bug.

   The Shellshock bug allows remote attackers to execute code in certain conditions by passing strings of code with environment variables. Many computers are vulnerable to Shellshock as all unpatched Bash versions from 1.14 to 4.3 are at risk. This means the Shellshock bug can be exploited on systems that are running applications and services that allow unauthorized users to assign Bash environment variables. Some of these application and services are Apache HTTP Servers, Certain DHCP clients, OpenSSH servers and Various network services that use Bash. This bug is very widespread even more the Heartbleed bug and it is very easy to exploit. It is recommend that all affected systems are properly updated to fix bug as soon as possible. To check if your system is at risk run the command below:

   ```
   env 'VAR=() { :;}; echo Bash is vulnerable!' 'FUNCTION()=() { :;}; echo Bash is vulnerable!' bash -c "echo Bash Test"
   ```

   This echo command shows where an attacker could but his or her code to cause harm. If you get an output "Bash is vulnerable!" you are at risk. If the only thing that is outputted is "Bash Test" your Bash is safe from shellshock. The best way to fix this bug is to use the default package manager to update the version of bash on your system

   The term open source means software whose source code is available freely on the internet. Proprietary software on the other hand is a closely guarded secret. Because of this Proprietary software is more secure as it not open to the public you are garneted a high standard of software developed by qualified programmers. This means code will have gone through extensive testing and will have less of a chance of getting bugs. In the same breath, Open source software can be seen by many people, so bugs can be caught and reported quicker. They both have their pros and cons but in most case Proprietary is more secure.

B. Bitcoin operates as a peer to peer network this means that everyone who uses bitcoin is a tiny fraction of the bank. Bitcoin mining is a process by which transactions are verified and added to the public ledger aka the block chain and this is how new bitcoins are released. Anyone who has the sufficient hardware and access to the internet can take part in bitcoin mining. How bitcoin mining works is it compiles recent transactions into blocks and tries to solve computationally puzzles that get harder as you complete them. The person who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The math problems are change by the bitcoin network depending how fast they are being solved. Miners are required to approve bitcoin transactions, so this means the more miners there are the more secure transactions are. To set up bitcoin mining one must acquire bitcoin mining hardware. When bitcoin first started people use to mine with their computer CPU or video card if it was capable. Today there are special chips used to mine bitcoin they are called ASIC chips. ASIC stand for Application-Specific Integrated Circuit Chips and these chips now preform a lot better than old systems and are the current leader in the bitcoin mining industry. If one was to use anything less than this, it would likely consume more electricity than you would earn solving bitcoin problems thus losing money. Instead of getting hardware a miner could purchase a bitcoin mining cloud contract. This will make the process a lot simpler but increases the risk as you do not control the hardware. There has been a lot of cloud mining scams. The next step in setting up your mine is to get the free bitcoin mining software. There are lots of programs to mine bitcoin but the two most popular are GCminer and BFGminer. These programs are both run on the command line. Easy miner has a GUI for people who don't like to use the command line. The next step is highly recommended by bitcoin miners everywhere, this is to join a mining pool. A bitcoin mining pool are groups of bitcoin miners all working together to solve a block and share the rewards. The rewards are split based on the amount of computationally work done by you. If you didn't go to a pool they could be stuck mining for up to a year and not make any bitcoin. It works better for everyone if they all share the work load and split the rewards. p2pool is one of these mining pools. The last and final step is to set up a bitcoin wallet or one could use an existing wallet. Copay is the most used bitcoin wallet and can be used on many different operating systems. You can also buy bitcoin hardware wallets instead. The bitcoins you have mind are sent to your bitcoin wallet using an address that only belongs to you. As this is on the internet there are many threats and bitcoin wallets could be attacked by hackers. The most important step in setting up your bitcoin wallet is securing it by having a two-factor authentication or keeping it offline away from the internet. My bitcoin mining experience was strange as it is very hardware extensive and pushed the limits of my laptop. Mining bitcoin can really damage you GPU as it so power hungry one must be very careful while mining on their laptop. I feel the only way you can properly make use of bitcoin mining is joining a pool, there is no way you could make a profit mining on your own. Even with a massive bitcoin mining rig it is still not going to generate much a profit vs how much you are spending on electricity. People who mined bitcoin when it first started would have seen the benefits but in today's market you are best off buying bitcoin and hoping the value continues to grow.

An important part of bitcoin mining is Hash Functions. These are used in the bitcoin protocol and for information security. A hash function is a mathematical process that takes input and preforms and operation on it and returns an output of a fixed size. The most common use of these hash keys is in passwords. In the bitcoin protocol hash functions are part of the block hashing algorithm which is used to write new transactions into the block chain through the mining process. The inputs for the hash function in bitcoin mining are the most recent and not yet confirmed transactions. Changing a small part of the input for a hash function results in a completely different output. This is needed for the 'proof of work' algorithm involved in mining. To successfully solve a block the miners, try to combine all the inputs with their own piece of input data. There is a real problem when mining bitcoin on your mobile phone. Mining is such and hardware-intensive task. This means you will need the most cutting-edge phone to keep up. Some mining applications are available on mobile phones but only on android phones Apple do not allow these apps on their store. The energy requirements to run these apps is monumental and produces little to no profit. The difficulty with mining bitcoin on a laptop is the time. If you mine one block the reward is 12.5 BTC so if you are in a pool of miners, you will be rewarded your fraction of computational problems solved meaning if you $1/12.5^{th}$ of the work you will make one bitcoin. Bitcoin per block was originally 50 when it was created it was then halved to 25, every four years bitcoin is halved. The time it takes to mine bitcoin and the cost of the energy to perform the problems in most cases isn't worth it. There are other forms of cryptocurrency another big one like bitcoin is litecoin. This is said to be the silver to bitcoins gold. Where the differences come in is the bitcoin mining and transactions. In mining litecoin calculations are a lot more serialised then bitcoins and lite coin favours large amounts of high-speed RAM rather than processing power. When preforming transactions litecoin can confirm these transactions much faster than bitcoin, litecoin can do it in half the time. Another form of cryptocurrency is Primecoin. This cryptocurrency uses the proof of work algorithm however it uses prime numbers. Miners must find the Cunningham chains which are sequences of prime numbers. This cryptocurrency not only provides security to the network but also generates a special form of prime number chain that is useful to mathematical research. In Ireland, you are eligible to be taxed on profits made when buying or selling bitcoin. Some business do accept cryptocurrency but not many due to the fact that they are not regulated by the central bank and are not considered legal tender. A lack of regulation also means the cryptocurrencies are volatile in nature. In most countries bitcoin is not illegal expect in Bangladesh or Bolivia, some countries have allowed its use in trade. An example of this is the US treasury classified bitcoin as a convertible decentralized virtual currency in 2013. The IRS tax bitcoin as a property. There are many advantages to bitcoin, so I feel it will remain a relevant currency. The largest BTC transitions are in made in China thus the two will stay connected for the foreseen future. The biggest risk to bitcoin is another cryptocurrency but die-hard Bitcoin fans don't think this will be a problem as it was the first cryptocurrency. This argument is does not make sense BTC payments are very few and its primary use is being stored as it increases in value so other cryptocurrency can always step in.