Project 2

Hanli Zhang 470348789

Zhong Shen 460293080

1. How do you ensure the only one who can send updates to Skynet is the botnet master?

To ensure the authenticity of the updates, we build a digital signature scheme by using the asymmetric cryptography system(PKCS1_PSS) and SHA hash function. After the bot found the Bitcoin, bot should upload the document of Bitcoin to pastebot.net. When the document is in pastebot.net, master can choose a file to sign by hashing it, signing the hash and adding the signed hash to the original file. Create the signature by using the 2048-bit private key, and build the signature which is 256 bytes long, then append the signature to the original file which will has a suffix called ". signed".

Bots must ensure that all download files are signed by the master (download from the pastebot.net and other bots). To do this, bots should decrypt the signature attached at the original file by using the master's public key. The resulting value is the proclaimed hash value of the file. Then bots will hash the part of file which exclude the signature by the same hash function. If these two hash values are same, we can ensure the authenticity of the master, else this file won't be stored and read.

2. How do you protect the valuable information to ensure it can only be read by the botnet master?

Because anyone can read the information uploaded onto pastebot.net, if we want to ensure the confidential of these valuable information, it's necessary to make sure that master is the only recipient authorised to read the files.

Before bots upload the valuable information onto pastebot.net, they must encrypt the packet by using PKCS1_OAEP method from Crypto.Cipher. The encryption is executed by public key from the master. Because the encryption process always uses one-way function which is hard to crack without the key. Thus, only the bots who have the private key of the master can decrypt the documents in pastebot.net folder. By this way, we can make sure the master is the only one who can read the valuable information in pastebot.net.

3. How do you ensure the botnet updates signed by the botnet master cannot be forged or modified?

Because the signature of a digital signature represents the character of the file, if the file changes, the value of the digital digest will also change. Different files will get different numerical features. On the other side, the digital signature is hard to forge, due to the large key which is used to sign file. If enemy wants to break asymmetric encryption involved in the signature, this process will take a lot of time and a great number of money.

It's difficult to modify the uploaded file in pastebot.net. If someone want to modify the file be signed, he must hash the file which has been modified to get the same value with the authentic file. This task is admittedly very difficult to achieve due to the property of SHA hash function.

4. If SkyNet's botnet code is dismantled and/or the source code for it stolen, does your scheme become less secure?

Stolen or dismantled the source code of Skynet's botnet will not significantly reduce the security of using this scheme, because the security relies mostly on the strength and confidentiality of master's private key. If the private key is confidential, there is no use to steal the source code. However, the private key is generated by RSA which is hard to break.

5. Give an indication of how difficult it would be for an adversary to take control of SkyNet when your protections are used.

As we discussed at part 4, the only way for an adversary to take control of Skynet is that find out the private key of master. Because it will take an adversary for years to find the same hashed value with the authentic files. What's more, digital signature ensures that there is no opportunity to execute or store any unauthentic file. Thus, the security of the master's private key is the most important factor when analysing the possibility of Skynet to be token control by adversary.