ELEC5616 : Assignment 2
SKYNET Design Document
V. Grotte 309193168

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

I implemented a digital signature scheme using PyCrypto. PKCS1_PSS and conjunction with a SHA256 hash (similar to the procedure used in the initial authentication procedure) to sign and verify updates.

"master_sign.py" was edited to allow the master to sign a file on pastebot. The signing procedure involves hashing the file's contents, spawning a signature with the hash and the master rsa key and appending said signature to the file. The file is then renamed to $NAME.signed and pushed to pastebot.

The botnet's "download" functionality was then altered with the implementation of a "verify file" method which checks to see if the document is in such a state as would indicate it had been signed by the master (ie. having a 512 bit *signature* on the end that can be reproduced by combining a SHA hash of the rest of the file and a public rsa key as inputs to a PyCrypto. PKCS1_PSS signature.

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

"Valuables" ie. illegally obtained data are encrypted using the padded stream block cipher PyCrypto. PKCS1_OAEP using a public-key cryptography system. The valuables are encrypted using the master's public key, so that they can only be decrypted using the master's private key.

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

The digital signature that is appended to signed updates is dependent on the contents of the file and is also designed as an integrity check. The key that is used to sign the hash is large, which makes the task of forging (ie. breaking the asymmetric encryption) difficult.

Integrity is ensured due to SHA's 2nd pre-image resistance as it unlikely that an attacker will be able to generate a document of random values that will hash to the same signature, let alone a functioning, executable configuration of code characters.

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

No, the signing scheme in isolation does not become less secure because all the security of the signing scheme rests on the strength and privacy of the master's private key.

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

These protections secure only the information the bots send between each other.
Skynet does not control, secure or obfuscate it's runtime.
Having said that, these schemes are all strong and provide an important element of security for the system.

[1] https://crypto.stackexchange.com/questions/58813/brute-force-attack-on-oaep

[2] https://crypto.stackexchange.com/questions/15174/is-it-true-that-for-rsa-with-no-padding-the-length-of-data-must-be-equal-to-the

[3] https://crypto.stackexchange.com/questions/3581/how-do-i-calculate-the-maximum-plain-text-length-allowable-for-a-certain-cipher

[4] https://stackoverflow.com/questions/35963916/how-to-encrypt-and-decrypt-data-with-pycrypto-and-rsa

[5] https://crypto.stackexchange.com/questions/42097/what-is-the-maximum-size-of-the-plaintext-message-for-rsa-oaep