ICP-3011 Computer & Network Security

Reflect And Relate

PRIFYSGOL
BANGOR
UNIVERSITY

Max Petts - *eeub35*

📅 - 04.10.2020

Week 1 - SSH Remote Access

Concepts learnt:

- SSH (Secure SHell)
- Authentication
- Cryptography (RSA Cryptosystem)

This weeks lab detailed the steps that must be taken in order to remotely connect to another machine via SSH, provided it's connected to the internet, or the same local network.

Once an SSH connection had been established I used the command *ssh-keygen* to generate an RSA key. This is used to circumvent the transmission of passwords, which can be cracked using brute force attacks, phishing scams or network analysers(if transmitting in plain text). However, a password is used to authenticate the user, but this doesn't leave the computer.

I use git to track changes to my projects, which requires a public key before any changes can be pushed to the repository; if this repo contained sensitive information then the key should use ECDSA, as RSA is vulnerable to timing attacks[1].

References

[1] http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf