# SENG2250/6250 System and Network Security

# School of Electrical Engineering and Computing

# Semester 2, 2020

## Lab 11: IPSec, Wireless Security and Email Security

## Objectives

1) Review essential knowledge of IPSec, wireless security and email security.
2) Use PGP for email security protection.

## Part 1 Lab Environment

1. This lab should be conducted under the **Windows 10** VM. To access your virtual lab:

   https://cybersec-vra.newcastle.edu.au/vcac/org/cybersec

   **Username: student**

   **Password: $tud3nt**

## Part 2 Exercise 1: IPSec and Wireless Security Review

1. What are the two security protocols defined in IPSec?
2. What are the security services provided in IPSec?
3. Can we use IPSec to protect the MAC information of a user?
4. What are the IPSec transport mode and tunnel mode, what are the differences?
5. Why does ESP include a padding field?
6. What is a security association?
7. Explain the entries of the following table.

| Protocol | Source IP | Source Port | Destination IP | Destination Port | Action | Comments |
|---|---|---|---|---|---|---|
| TCP | 10.1.2.156 | * | 10.1.2.132 | 80 | Bypass | Unprotected traffic |
| TCP | 10.1.2.156 | * | 10.1.2.133 | 443 | Bypass | - |
| ICMP | 10.1.2.156 | * | * | * | Bypass | Error messages |
| * | 10.1.2.156 | * | * | * | Protected: ESP transport-mode | Encrypted traffic |
| * | 10.1.2.156 | * | 10.1.2.10 | * | Discard | - |

8. What information should be contained in an ISAKMP SA?
9. What is about the IEEE 802.11i standard?
10. What security issues of WEP are addressed in TKIP.

## Part 3 Exercise 2: PGP

In this exercise, you will use PGP to improve email security.

### Task 1: Installation

In this lab, we use "gpg4win" to do exercises of PGP. We need to firstly install the software in the Windows VM. Follow the instructions to accomplish this task.

1. Login your Windows VM.
2. Open "File Explorer" from the task bar. Browse to \\cybsec-teachfs\data

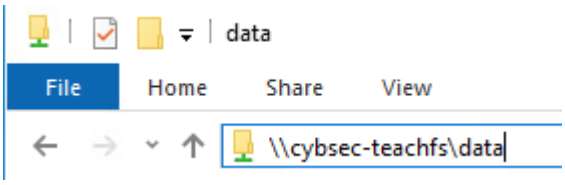


Figure 1. Access the file server.

3. If prompted, enter the username (student) and/or password ($tud3nt).

4. Copy and paste the file "gpg4win-3.1.10.exe" to your desktop.
5. Install gpg4win-3.1.10, keep the default settings. The application "Kleopatra" (a manager) should have been executed. If not, run it from the desktop.

**Task 2: Create Public/Private Key Pair for PGP.**

PGP needs to preform public-based encryption and digital signature for data security. To enable the public-key based cryptographic algorithms, it is required to create your public and private keys. In PGP, you will have different key generation options which depend on the different cryptographic algorithms. In this task, we will create RSA keys for yourself.

1. Click “New Key Pair”. Enter a name and email address of yourself (Figure 2).

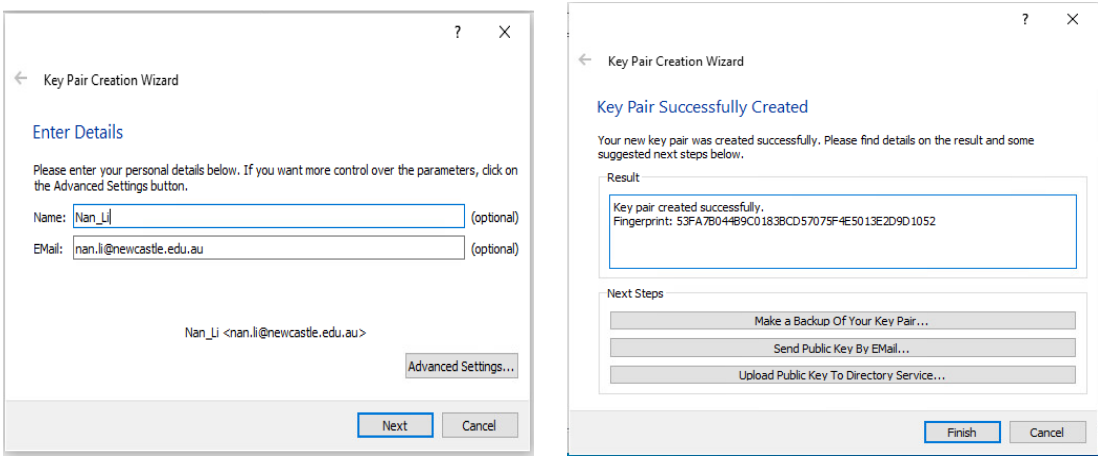


Figure 2. Public and private key generation.

2. Click “Advanced Settings…” and check if the 3072-bit RSA is selected. If not, select 3072 bits, then click “OK”.
3. Click “Next”.
4. Click “Create”. You will be asked to create a passphrase. The passphrase is optional, but it is strongly suggested to create a high-quality password. Create one for yourself and click “OK”. Your RSA public and private key pair will be created (Figure 2).

   **Why do we need a passphrase? Where will it be used?**

   This step also creates a “certificate” of your public key. **In theory, what are the differences between this certificate and X.509 certificate of PKI?**

5. Export the public key (certificate). Select the created certificate and click “Export…”. Save the “.asc” file to the Desktop.

**Task 3: Generate Public and Private Keys for a Dummy User.**

To use PGP for email transmission, you need to have the sender/recipient public key (certificate). In practice, public key information is exchanged before the sending/receiving. In this lab, we create a dummy user to demonstrate it locally.

1. Delete the created certificate and the keys generated in Task 2. Because we have exported the certificate, we can recover it later.
2. Repeat Task 2 to generate a new public/private key pair. It is important to note that you should use a different name and email address.

3. Import the previously exported (in Task 2) certificate. Click “Import…” and import the certificate. Note that PGP certificate is certified by yourself rather than the trusted authority (Figure 3). Tick both boxes then click Next.

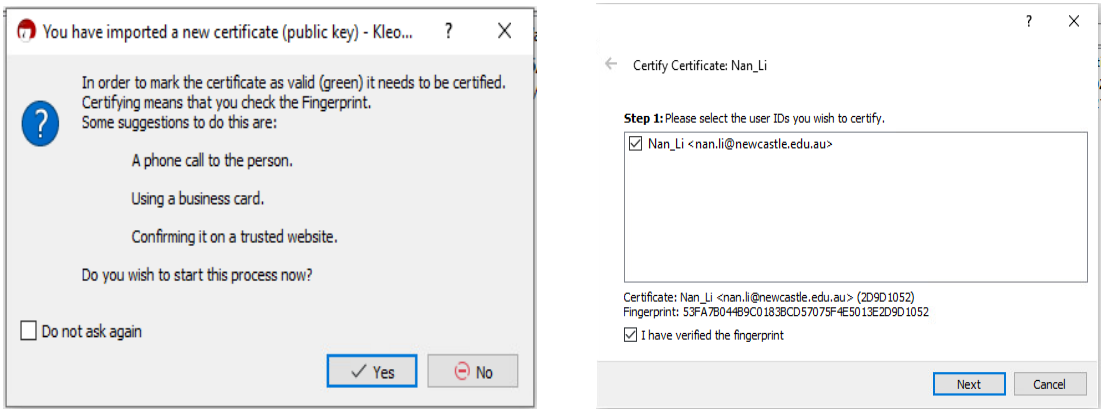


Figure 3. Certify a new public key certificate.

4. Certify the certificate with your passphrase.

   **What is this passphrase used for?**

5. Double-click the listed two certificates respectively.

   **What is the trust level of each certificate? Why? What are the other trust levels in PGP? Explain.**

**Task 4: Encrypt and Sign a Message.**

1. Create a text file “t4sec.txt” on the Desktop. Enter any message then save the file.
2. In the Kleopatra main window, click “Sign/Encrypt…”, select “t4sec.txt”. Then, in the prompt window, add a user for “Encrypt for others”. In this task, you should choose the user you created in Task 2 (Figure 4). Then, click “Sign/Encrypt”.

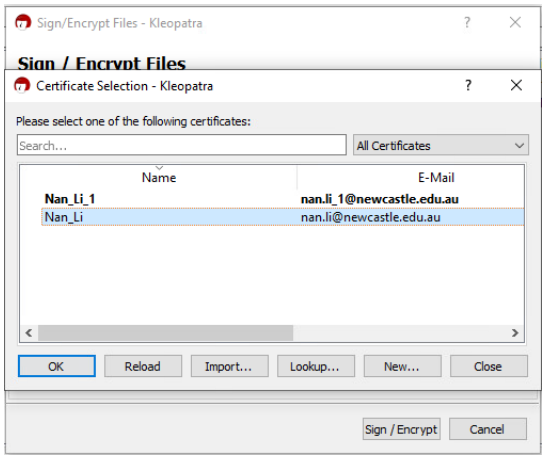

Figure 4. Sign and encrypt a message.

**In theory, what has been done for this sign/encryption process? Draw a diagram to demonstrate the details of PGP sign/encryption.**

### Task 5: Encrypted Email

In Task 4, the file "t4sec.txt" has been encrypted and signed. The protected file "t4sec.txt.gpg" can be sent as an attachment of an email for security protection. In this case, the sender has to write email content to the file. Alternatively, you can copy the PGP message block (Figure 5) to your email content, then send the email as normal.

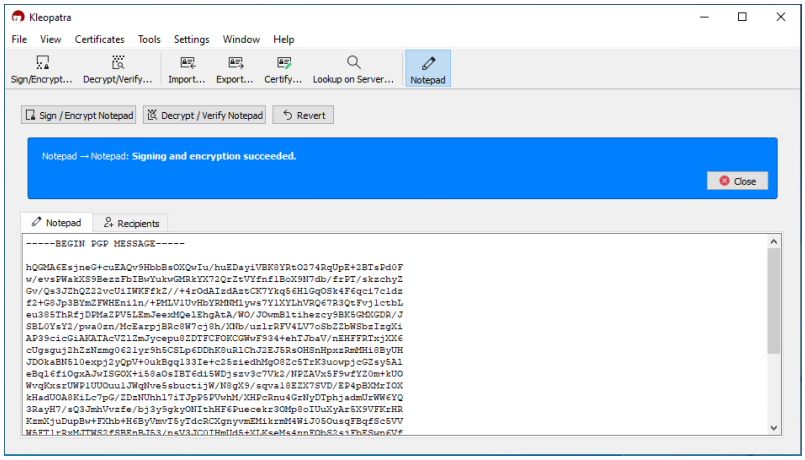


Figure 5. PGP message block.

**Decrypt and verify the "t4sec.txt.gpg" file to recover the text message.**