# SENG2250/6250 System and Network Security

# School of Electrical Engineering and Computing

# Semester 2, 2020

## Lab 4: Topic 3 – Key Management and Distribution

### Objectives

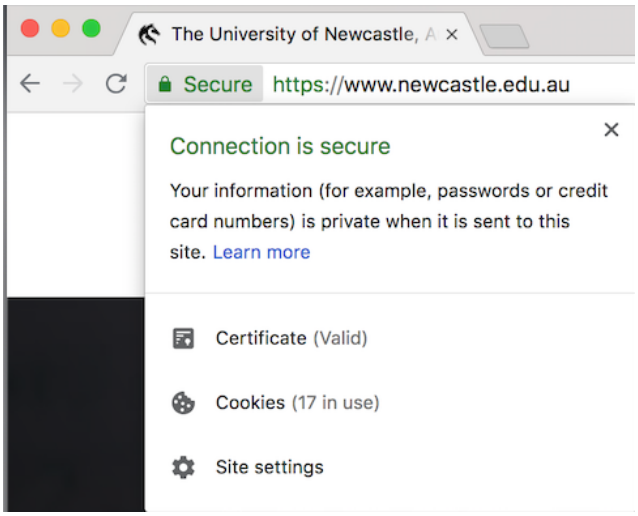
1) Review the knowledge of Topic 3.
2) Analyse and resolve security issues for key management mechanisms.
3) Implement (simulation) the Diffie-Hellman key exchange protocol and the MITM attack.

### Part 1 Review Questions

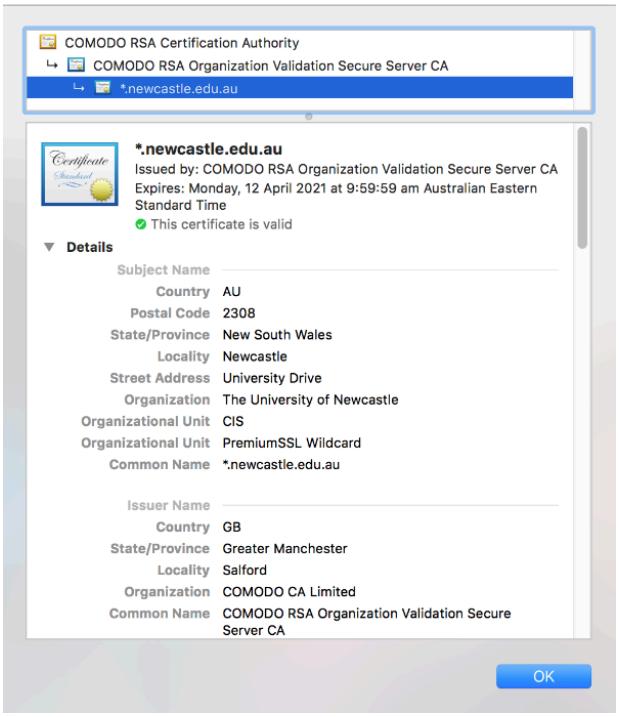
1. What are the key transport and key agreement, respectively?
2. Describe the Diffie-Hellman key exchange protocol.
3. What is a public key certificate? Why is it important for using public key based cryptosystems?
4. What is a public key infrastructure (PKI)?
5. What is the purpose of cross-certification in X.509 Hierarchy?

### Part 2 Exercises

6. **Explore and interpret the public key certificate of The University of Newcastle**.
   - Visit: https://www.newcastle.edu.au and find (as an example in macOS with Chrome)



- Open the certificate of UON and answer the following questions. (as an example in macOS with Chrome)




a. Fill out the following table using the UON's certificate.

| **Item** | **Value** |
|---|---|
| Version | |
| Certificate Serial Number | |
| Signature Algorithm | |
| Issuer Name | |
| Period of Validity | |
| Subject Name | |

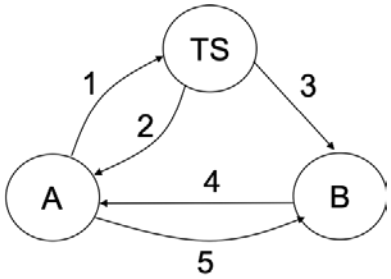
b. Is the UON's public key acceptable for both data encryption and verification?

c. As UON's public key is for RSA encryption, what does it mean by the 2,048 bits key size? Is that the size of the modulus $N$ or $p, q$ of RSA?

7. **Security Analysis of Needham-Schroeder (NS) Protocol**

a. Does the NS protocol provide key freshness in the view of B? (think about it in Message 3). If it doesn't, fix it.

b. Consider the following variant of NS protocol, find the security flaw(s) and fix it (them). Note: a session key could be compromised by an adversary.




1. A → TS: $A, B, N_A$
2. TS→ A: $E_{KA}( N_A, B, K_{AB})$
3. TS → B: $E_{KB}(K_{AB}, A, N_A)$
4. B → A: $E_{KAB}(N_A, N'_B)$
5. A → B: $E_{KAB}(N'_B)$

- TS: trusted server, e.g., key distribution centre (KDC)
- A, B: identities of end-users.
- $K_A$, $K_B$ are long-term shared keys between A and TS, and B and TS, respectively.
- $K_{AB}$ is a session key.
- E is a secure symmetric-key based encryption scheme.
- $N_A$, $N_B$ and $N'_B$ are nonce.

**8. Diffie-Hellman (DH) Key Exchange**

a. Watch the video for Diffie-Hellman key exchange: https://www.youtube.com/watch?v=3QnD2c4Xovk

b. What is the man-in-the-middle (MITM) attack against the DH key exchange?

c. Assume $PK_A$ and $PK_B$ are public keys of A and B, respectively. They both know the other's public key. If they are using their pubic keys to do DH key exchange, will MITM attack be possible? What problem(s) may we have in this case?

d. In practice, a client is usually not required to have a certificate for a DH key exchange. For example, when you use a secure connection (e.g., https://...), you only check the certificate of the website, but not show yours, because you don't have one.
What are the good parts and the bad parts of this method, respectively?

9. **Programming**

a. Implement (simulate using function calls) the Diffie-Hellman key exchange protocol. The program should have at least the following two functions:

- **KeyGen**: for public and private key pair generation.
- **DHex**: for shared session key $K$ computation.

Assume that the system parameters $p$ and $g$ will be given as input so the program does not need to generate them.

b. Implement MITM attack to demonstrate the vulnerability of the original Diffie-Hellman key exchange protocol.

c. Demonstrate the above implementations by using the following parameters.

$$p = 223, g = 79$$