Agenda

- Public Key Infrastructure (PKI)

Terminology

- `Symmetric Encryption`: Use one key to encrypt information, use the same key to decrpyt information.
- `Asymmetric Encryption`: also known as public key encryption, or public key cryptography. Use a public key to encrypt informaiton, use a private key to decrypt information. Generally more secure than Symmetric Encryption.
- `Man-in-the-middle Attack`: aka. MITM attack, happens when someone else is intercepting the traffic between two devices.

Symmetric encryption vs Asymmetric encryption

Asymmetric encryption - Simply explained
https://www.youtube.com/watch?v=AQDCe585Lnc

Security of Asymmetric Encryption

- Vulnerable to man-in-the-middle attack.
- Solution: Public key infrastructure (PKI).
- Main idea of PKI: introducing the concept of digital certificate and certificate authority (CA).

How PKI defeats the MITM Attack

Attacker has three options, none of them could make the attack succeed, if PKI is used.

- Attacker forwards the authentic certificate
- Attacker creates a fake certificate
- Attacker sends its own certificate

References

A large portion of the material is adapted from:

- Computer Security - A Hands-on Approach by Wenliang Du