Distributed Systems

COMP90015 2023 Semester 1
Tutorial 08

Today’s Agenda

- Assignment 2 Q & A
- Questions on Security (partial)
- Demo on File Transfer

Assignment 2 Q & A

1. What are the different security threats and methods of attacks in a distributed system?

Security Threats

Three broad Classes:

Leakage: Acquisition of information by unauthorised recipients

Tampering: Unauthorised alteration of information

Vandalism: Interference with the proper operation of systems

Method of Attacks

Eavesdropping - A form of leakage obtaining private or secret information or copies of messages without authority.

Masquerading – A form of impersonating assuming the identity of another user/principal – i.e, sending or receiving messages using the identity of another principal without their authority.

Message tampering- altering the content of messages in transit man in the middle attack (tampers with the secure channel mechanism)

Replaying- storing secure messages and sending them at a later date

Denial of service - Vandalism flooding a channel or other resource, denying access to others

2. List and briefly explain some worst case assumptions when designing a secure system.

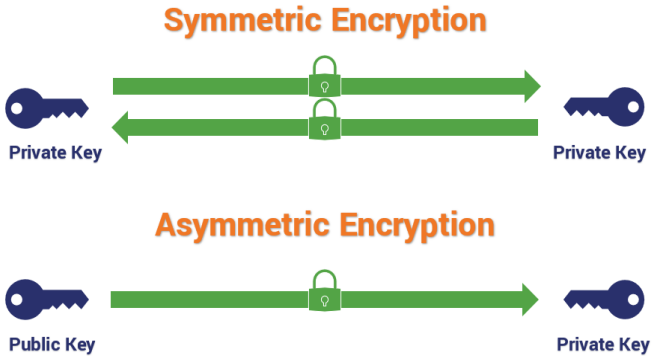
2. List and briefly explain some worst case assumptions when designing a secure system.

- **Networks are insecure.**
  - Messages can be looked at, copied, modified and retransmitted,
  - Attackers can obtain information that they should not and can pretend to be a legitimate party.
- **The source code is known to the attacker.**
  - Knowing the source code can help the attacker discover vulnerabilities.
- **Interfaces are exposed**
  - Communication interfaces are necessarily open to allow clients to access them.
  - Attackers can send messages to any interface.
- **The attacker has unlimited computing resources.**
  - Assume that attackers will have access to the largest and most powerful computers projected in the lifetime of a system.

3. Define encryption and describe the two main types of keys used by encryption algorithms.

3. Define encryption and describe the two main types of keys used by encryption algorithms.

- ***Encryption***
  - process of encoding a message in such a way as to hide its contents.
- ***Shared secret keys*** (symmetric)
  - Sender and recipient share knowledge of the key and it must not be revealed to anyone else.
- ***Public/private key pairs*** (asymmetric)
  - The sender uses a public key to encrypt the message.
  - The recipient uses a corresponding private key to decrypt the message.
  - Only the recipient can decrypt the message, because they have the private key.
  - Typically require 100 to 1000 times as much processing power as secret-key algorithms.



Code Demo

- Sending/Receiving files with Java Sockets