

# COMPSCI4062/COMPSCI5063

# Cyber Security Fundamentals

# (CSF)

## Lecture 2

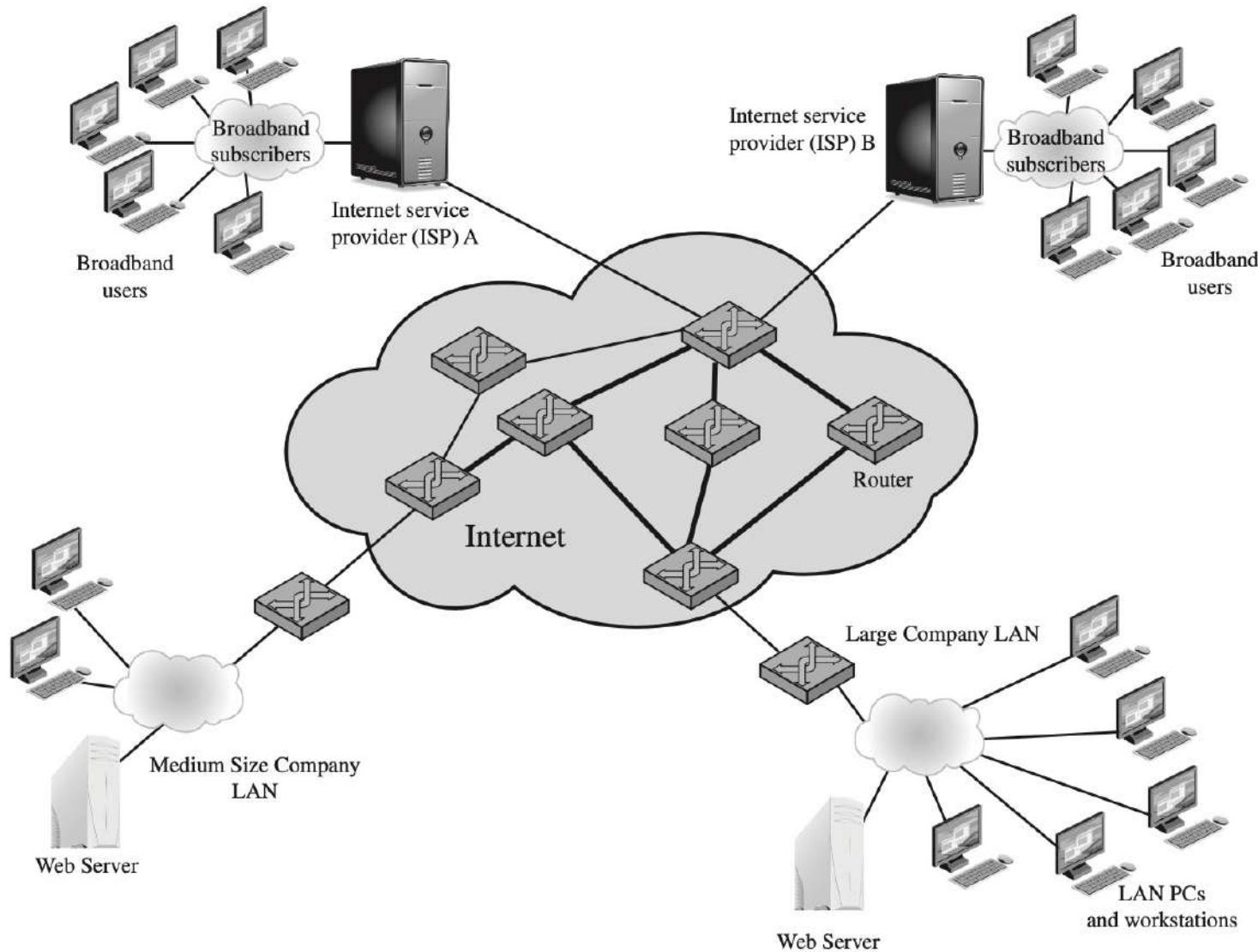
### Cyber Attacks and Security Protocols

# **NETWORK STRUCTURES**

# Network Types

- Local Area Network (LAN)
  - Wireless Local Area Network (WLAN)
- Personal Area Network (PAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Virtual Private Network (VPN)

# A Typical Network



# Open Systems Interconnection model (OSI model)

## 7. Application

Serves as a window for users and application processes to access network service.

## 6. Presentation

Concerned with the syntax and semantics of the information exchanged between the two systems.

## 5. Session

Establish, maintain and synchronizes the interaction between communicating devices (authentication & Authorization)

## 4. Transport

Reliable transmission of data segments between points on a network (TCP, UDP protocols)

## 3. Network

Structuring and managing a multi-node network, including addressing, routing and traffic control

## 2. Data link

Transmission of data frames between two nodes connected by a physical layer (media access control)

## 1. Physical

Transmission and reception of raw bit streams over a physical medium (e.g., optical fibre, cable, wireless radio)

# CYBERATTACKS

# Defination

- A cyberattack is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices

# Types of attack

- Active attack
  - attempts to alter system resources or affect their operation, e.g., Denial-of-service attack, Spoofing, Man-in-the-middle attack, ARP poisoning (Layer 2)
- Passive attack
  - attempts to learn or make use of information from the system but does not affect system resources, e.g., wiretapping, fiber tapping

# Forms of Cyber Threats

- Environmental
  - Break-in, physical damage, natural disaster, etc.
- Unintentional
  - Human error, poor training, insufficient documentation, etc.
- Intentional
  - Internal, e.g., Staff
- External
  - Intelligence agencies, hackers, terrorists, crackers, criminals, industrial intelligence, etc.

# Common Security Problems

- Snooping
  - Unauthorized reading or interception of information
- Modification
  - Unauthorized change of information
- Masquerading or spoofing
  - Impersonation of one entity by another

# Common Security Problems

- Repudiation
  - False denial of sending or creating information
- Denial of receipt
  - False denial of receiving information
- Delay
  - Temporary inhibition of access to services or information
- Denial of service
  - Long-term or permanent inhibition of access to services or information

# Denial-of-service attack

- A **denial-of-service (DoS)** attack is an attempt to compromise availability by hindering or blocking completely the provision of some service
  - Exhaust some critical resources associated with the service
  - Example: flooding a Web server with so many spurious requests that it is unable to respond to valid requests from users in a timely manner

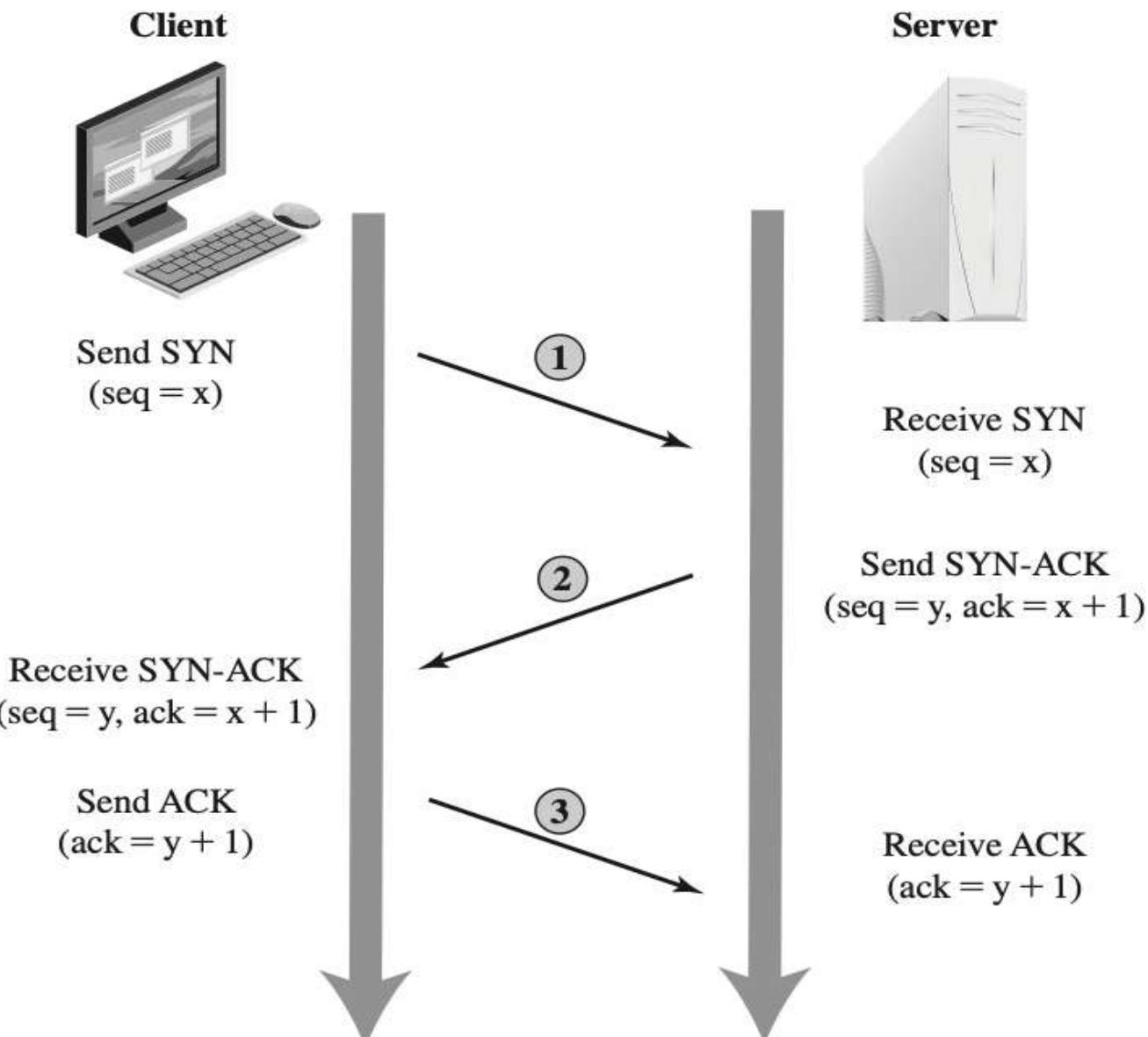
- The resources could be attacked:
  - Network bandwidth
  - System resources
  - Application resources
- A typical Network

# SYN Spoofing-1

- **SYN spoofing** attack targets the table of TCP connections on the server (Layer 4)
- A type of DoS attack

# SYN Spoofing-2

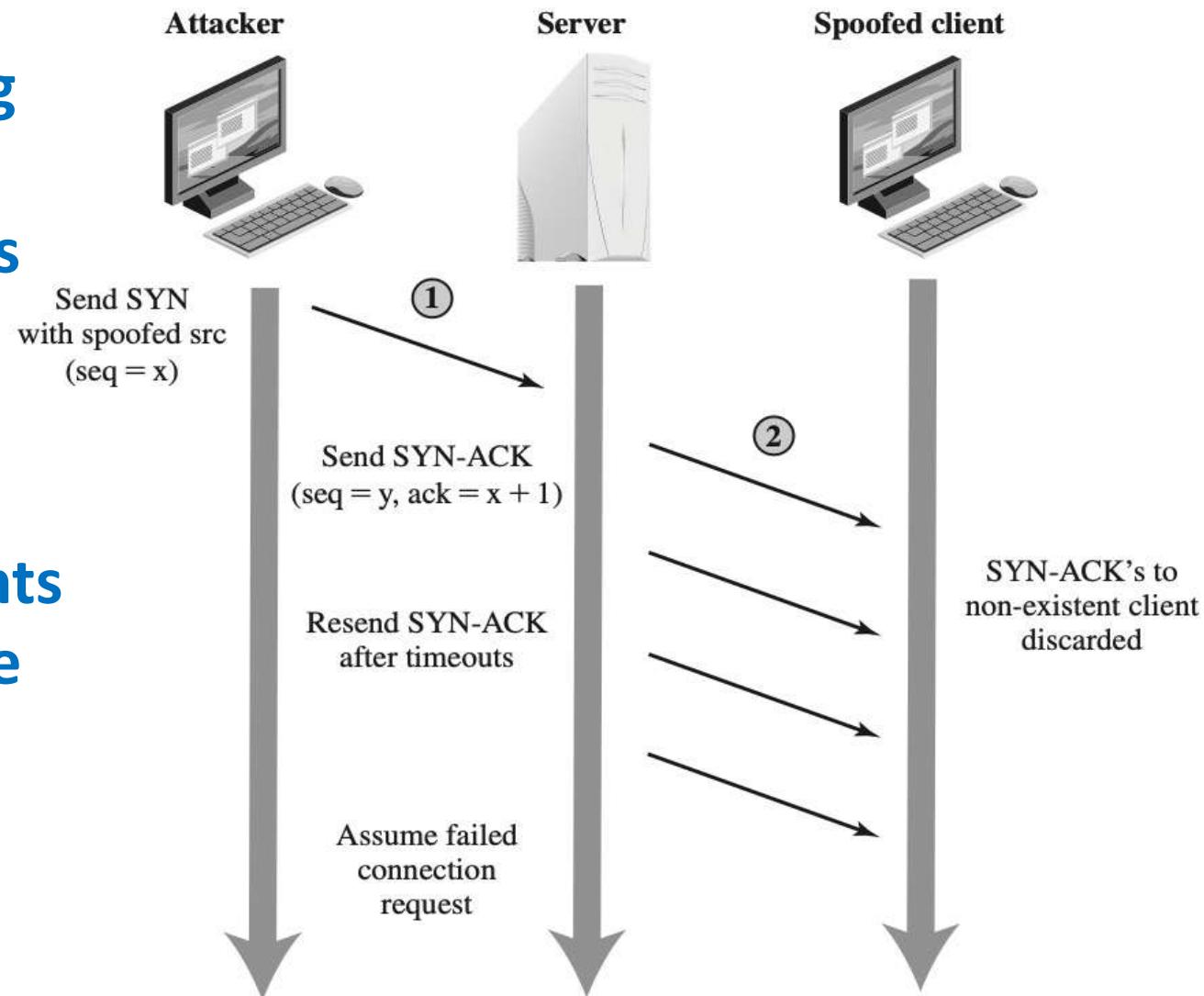
**TCP's three-way handshake used to establish a connection**



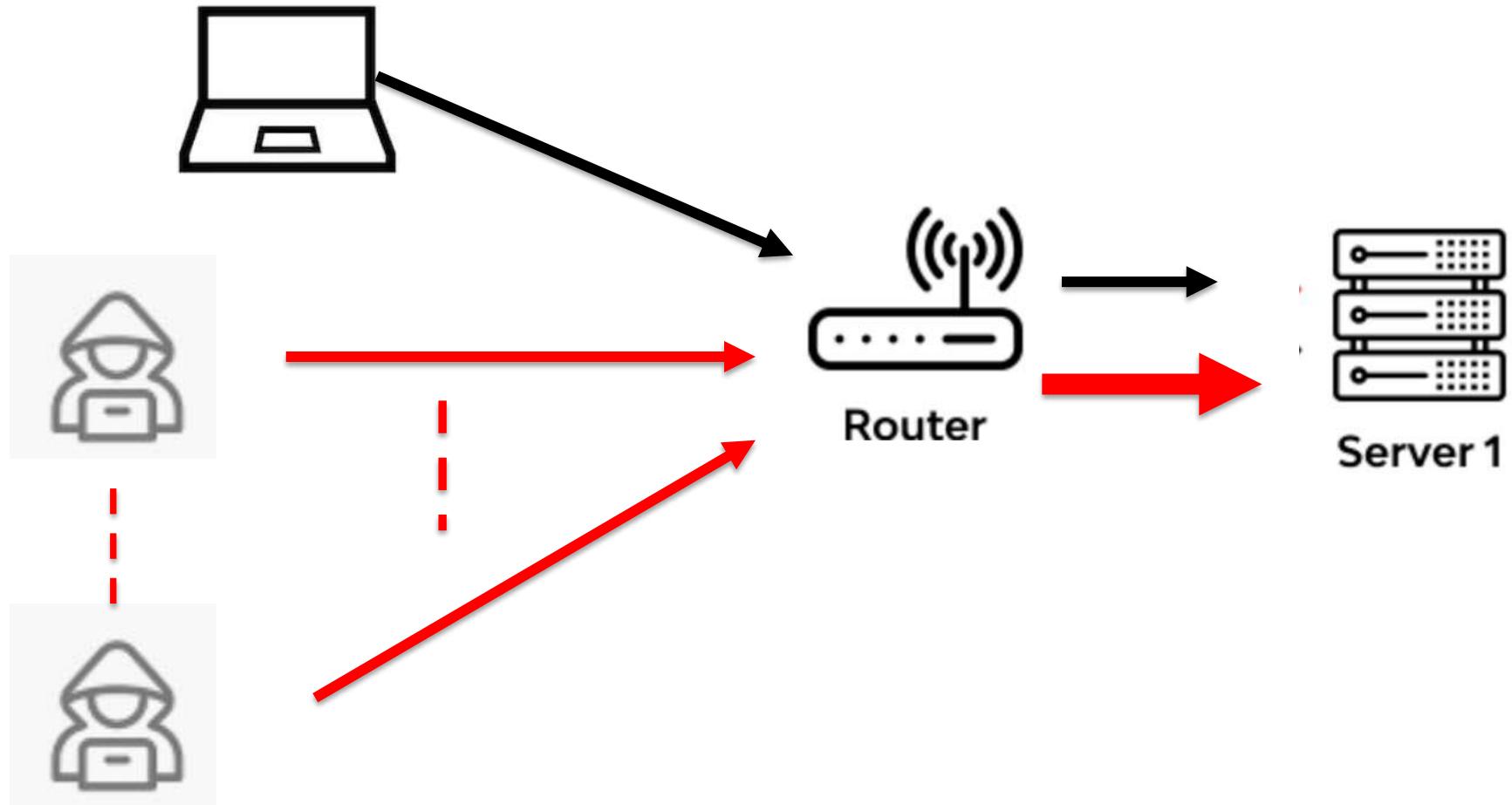
# SYN Spoofing -3

## TCP's SYN Spoofing Attack

- Cause resources on the server binding on the malicious use
- Legitimate clients couldn't use the resource



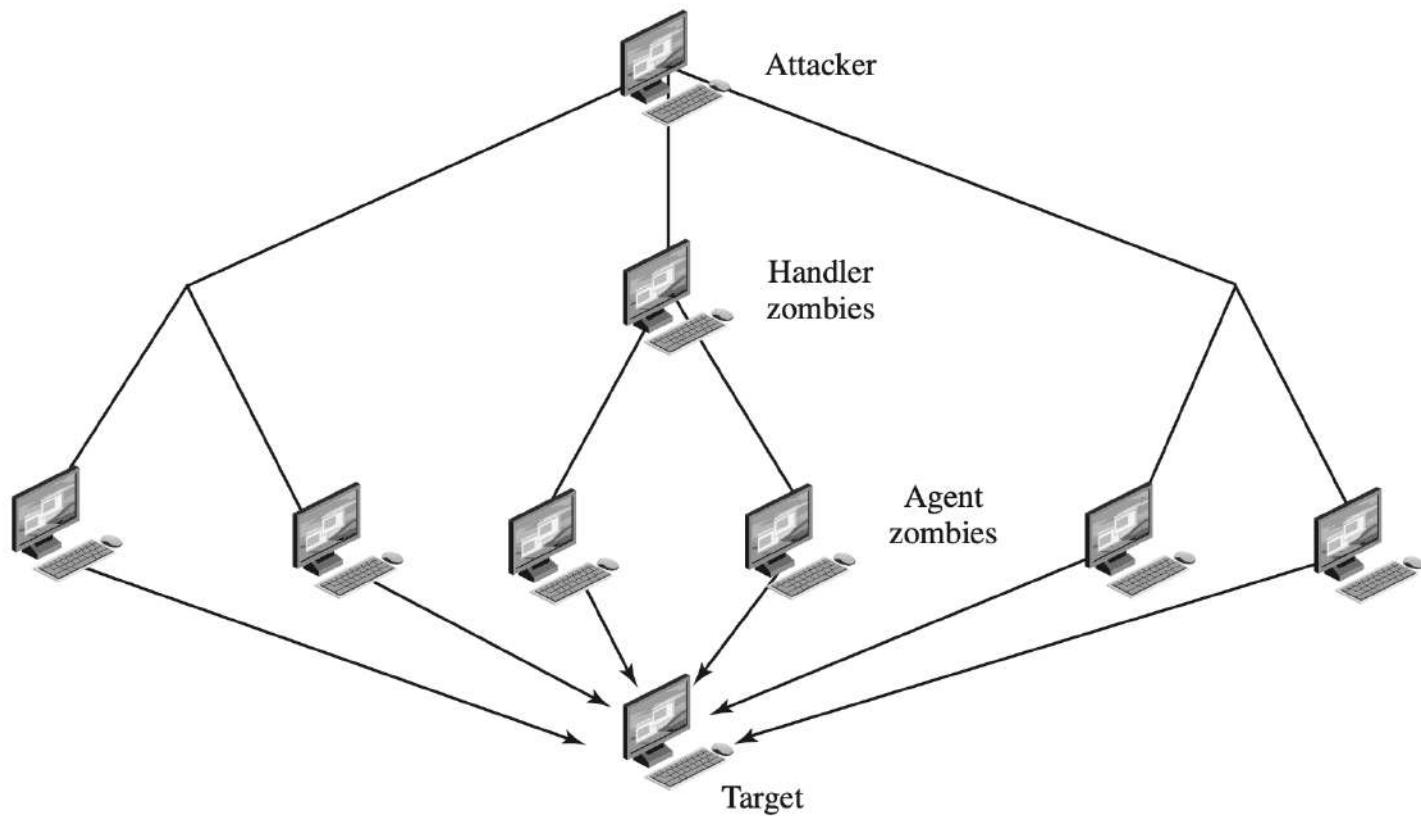
# UDP Flood



\* A type of DoS

# Distributed DoS

1. Application layer attacks
2. Protocol attacks
3. Volumetric attacks

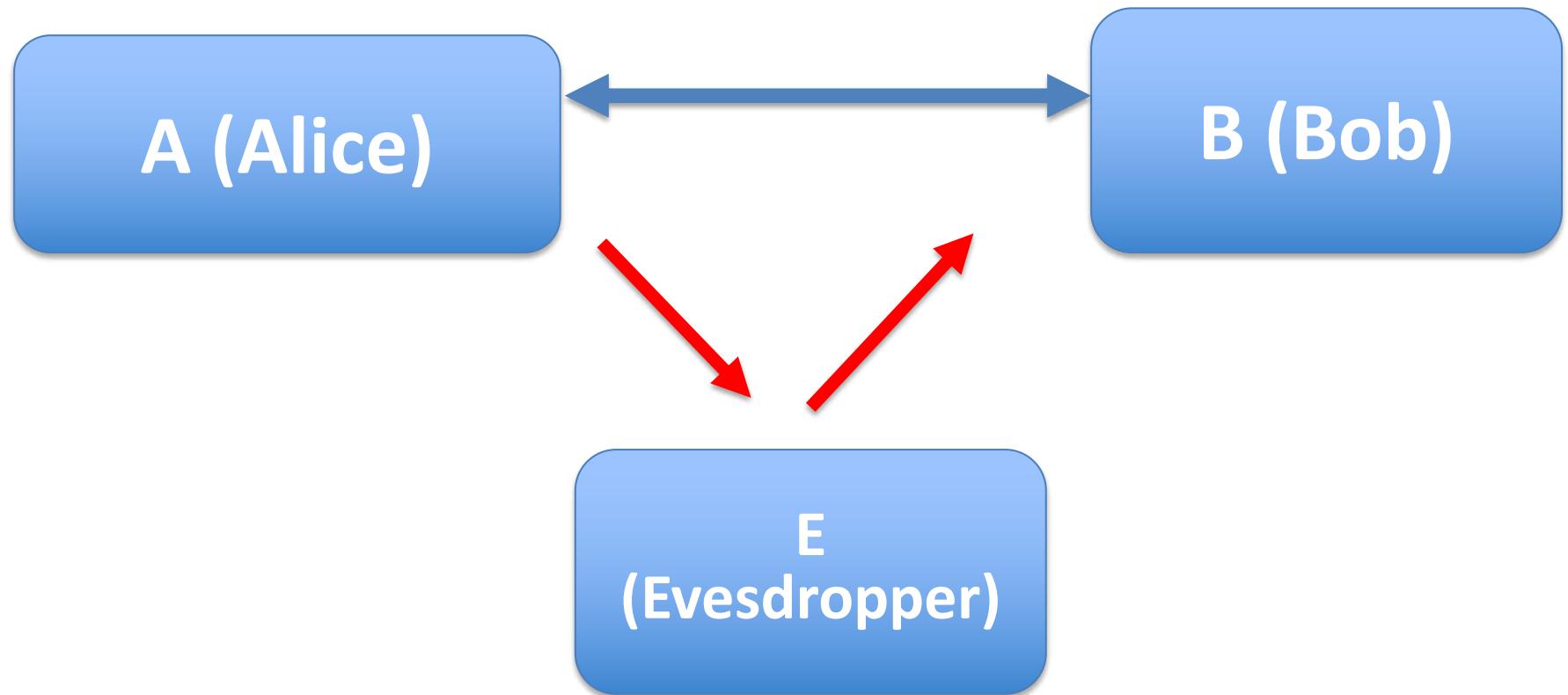


# Defense Against DOS Attacks

- Anticipate the potential attacks in different situations and prepared enough resource
  - High traffic situation, e.g. sporting events like the Olympics or Soccer World Cup match
- Attack prevention and preemption (Before the attack)
- Attack detection and filtering (during the attack)
- Attack resource traceback and identification (during and after the attack)
- Attack reaction (after the attack)

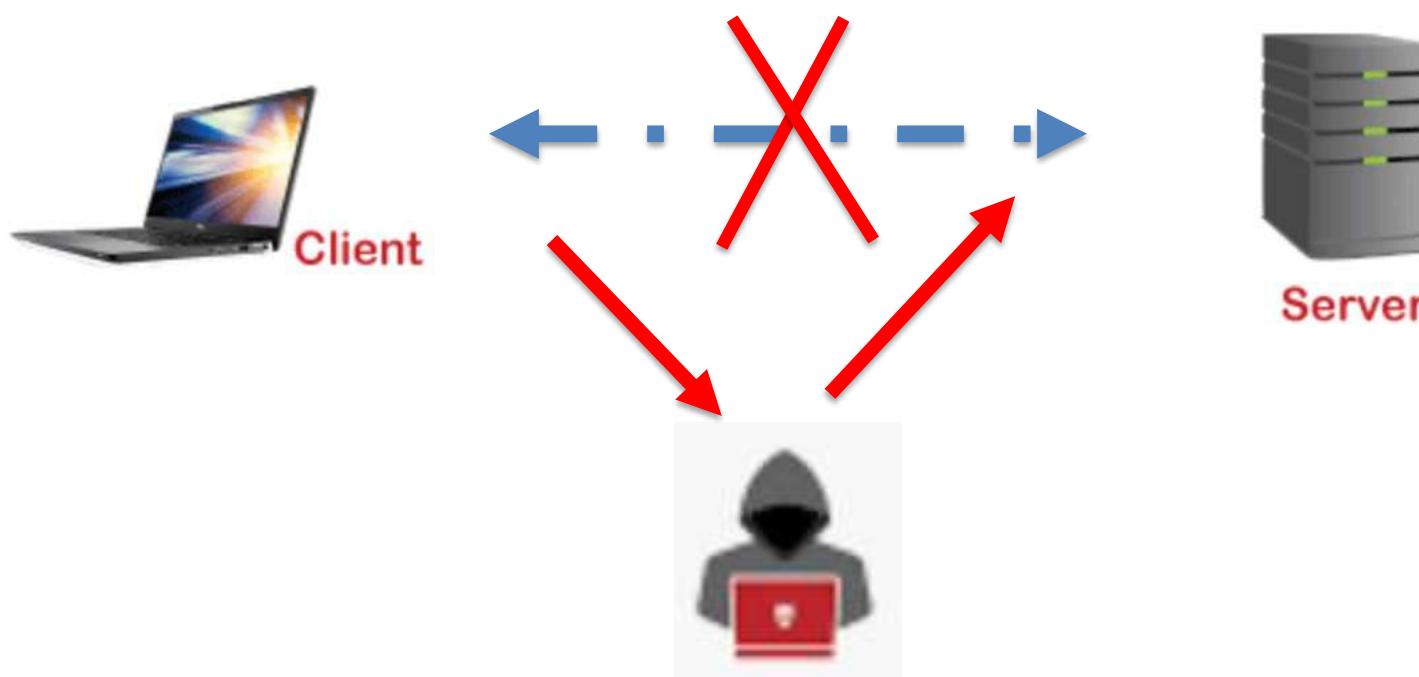
\* These attacks cannot be prevented entirely.

# Man-in-the middle Attack



**Man-in-the-Middle (MITM)**

# MITM Attack

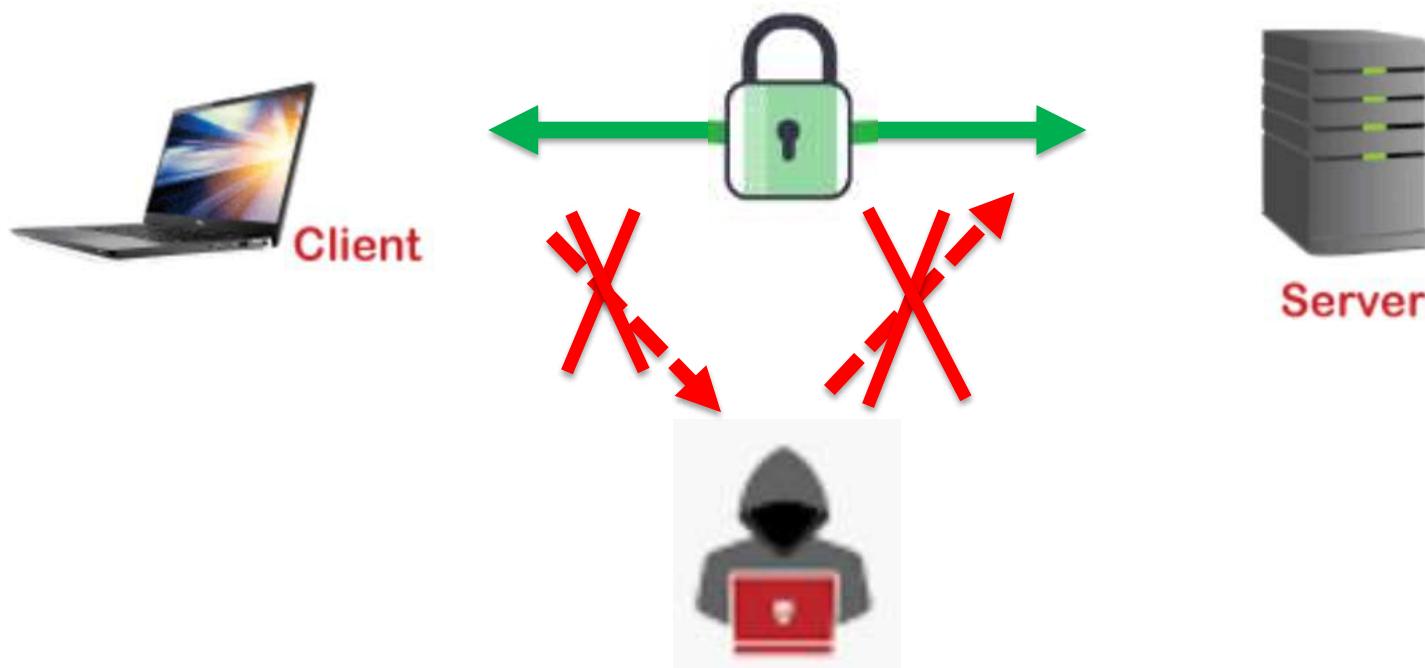


# Types of MITM Attack

- Wifi Eavesdropping
  - Public wifi
- DNS Spoofing
  - A Fraudulent web server, redirect a targeted user to a malicious website under attacker control
- IP spoofing
  - The attackers imitate an approved console's IP address
- ARP spoofing
  - fraudulent response, usually happens to a LAN with ARP protocol
- E-mail Hacking

# Defending MITM

- Wireless Access Point Encryption
- Use a VPN
- Strong user Credentials
- Public Key Pair Authentication



# **SECURITY PROTOCOLS**

## **-KEEPING A SECRET**

# Keeping A Secret: Memorise

- We will start with the simplest cyber security problem, keeping a secret.
- Our first protocol is to memorise the secret.
- This is only appropriate if the secret is fairly short and easy to remember.
  - It could be a password or an encryption key.
  - It should not be a BitCoin ID!

# Keeping A Secret: Paper

- If the secret is too long to remember, the next protocol is to write it down on a piece of paper
  - There is a limit to how long the secret can be.
  - It can be inconvenient to use if it has to be entered into a computer.
- The confidentiality threat relies on the attacker having physical access.
  - They can search our home or office.
- An availability threat is losing the piece of paper.
  - This can be mitigated by backups, making a copy.
  - All copies now need to be secured.
  - We must keep track of all copies
  - destroy all copies when they are no longer needed

# Keeping A Secret: Computer File

- Most documents are prepared on a computer, which introduces a number of **vulnerabilities** that can be exploited by attackers.
- The program used to create the document may make periodic backups, and so there are many different versions of the file that need to be protected.
- It is easy to create copies of the file.
- Deleted files can be recovered.

# Computer File: Encryption

- An encryption program takes plaintext as input and produces ciphertext as output.
- A decryption program takes ciphertext as input and produces plaintext as output.
- Decryption must undo encryption.
- Encryption followed by decryption must produce the same output as the original input.
- The original plaintext document must be erased.
  - Including all copies and backups.
- This protocol has a time limited vulnerability.
  - While the plaintext document is in the file system.

# Protocol: Secret Encryption Algorithm

- The details of the encryption and decryption algorithms are kept secret.
- Threat: finding the algorithms.
  - The algorithms will be computer programs.
  - They cannot be encrypted because they must be run on the computer.

Alice's  
digital file

# **SECURITY PROTOCOLS**

## **-COMMUNICATING A SECRET**

# Problem: Communicating a Secret

- Alice wants to send secret information to Bob without Eve finding out.
- This is usually a confidentiality problem.
- It can also be an integrity problem.
  - If Eve changes the message before forwarding it to Bob.
- It can also be an availability problem.
  - If Eve prevents Bob from receiving the message.
  - How does Bob know that Alice has sent a message?

# Protocol: Secure Transmission Medium

- Alice and Bob meet in a secure room or location.
  - The only secure transmission medium.
- Electronic transmissions are easy to intercept.
  - Transponders can be attached to Ethernet cables and the traffic analysed.
  - Email is stored and can be analysed later.

# Protocol: Secure Preparation

- Alice encrypts the message in a secure area.
- It is transmitted by an insecure medium
  - We assume that Eve can intercept, see and replace it.
- Bob decrypts the message in a secure area.
- Encryption followed by decryption cancel each other out.

# Using Encryption



Alice: Secure

$P$  = plaintext

$E$  = encryption algorithm

Secret

Bob: Secure

Eve

$C$  = ciphertext

$D$  = decryption algorithm

Public

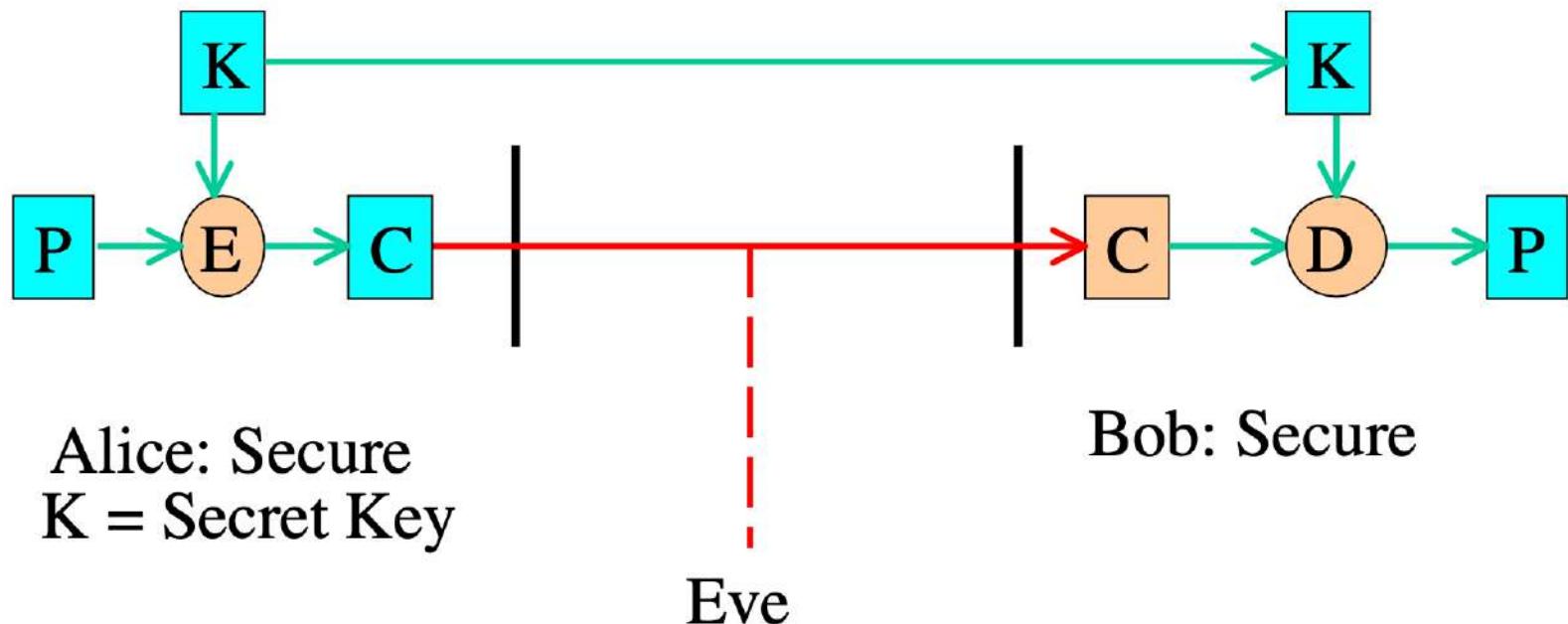
# Protocol: Use a Secret Algorithm

- Keep the details of the algorithm secret.
- This is bad for two reasons.
  - The algorithm designers know the secret and may be physically at risk.
    - Threat of coercion.
- Peer review of a public algorithm reduces flaws.
  - It is easy to fool oneself that an algorithm is more secure than it really is.

# Protocol: Public Algorithm, Secret Key (Private Key)

- Details of the encryption and decryption algorithms are public.
- They have a parameter, the key, which is kept secret.
- Knowledge of the algorithm is useless without the key.
- Also called a ***one key*** system.
- Also called ***symmetric encryption***.

# Using a Secret Key



# Reference Book

- Book: Computer Security Principles and Practice, by William Stallings and Lawrie Brown, 2014