

# IERG4130 Tutorial 9

## Network Security

Yikang CHEN  
cy021@ie.cuhk.edu.hk

# Network Protocols

---

- Set of protocols used to transport data between nodes of a network
- TCP/IP Protocol Suite
  - Link protocols
  - Internet protocols
  - Transport protocols
  - Application protocols

# Layering

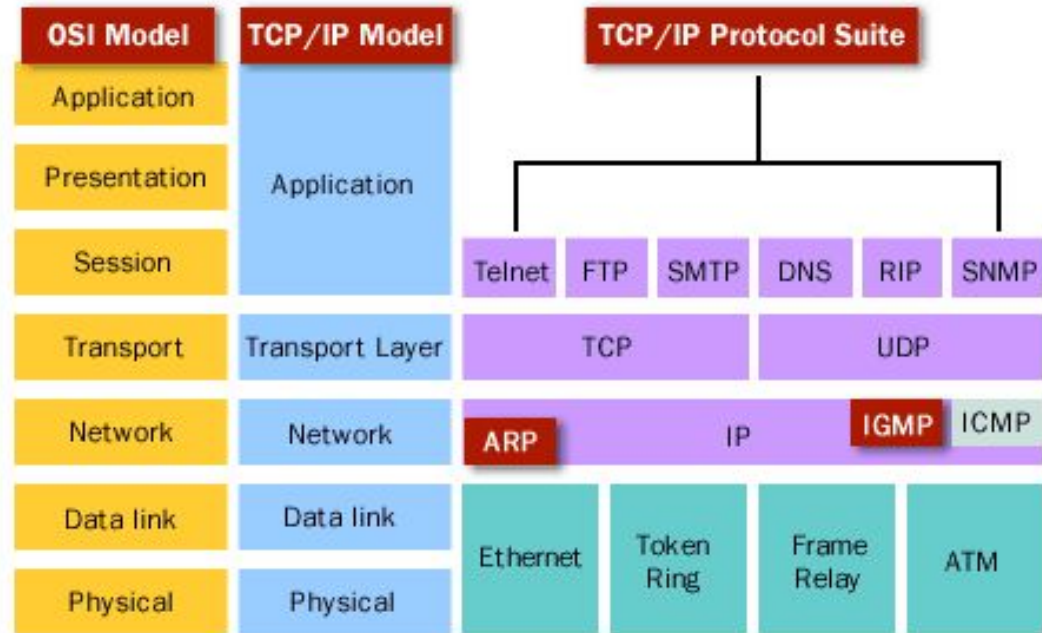
---

- Internet network stack is built on top of multiple protocols at different layers
- Layering allows modularization, which simplifies the designs of protocols for different tasks
- Layering allows encapsulation, which encloses message in different layers' protocols.

# TCP/IP stack

OSI Model is Conceptual model  
([https://en.wikipedia.org/wiki/OSI\\_model](https://en.wikipedia.org/wiki/OSI_model))

In practice, we adopt TCP/IP  
Model/Suite



# IP address and Subnet

---

- 32-bit for IPv4, dotted decimal format of 4 bytes.
  - each byte ranges from 0 to 255. (123.123.123.123)
- Subnets
  - A subnet mask help us divide network space. ( $2^{32}$ )
  - We crystalize some range of IP. (255.255.0.0)
- 128-bit for IPv6, assign an address for every sand on earth

# Special Address

---

- Loopback address: packets will be send back to the host itself
  - 127.0.0.0/8 → 127.0.0.1
- Broadcast address: packet will be sent to all possible destinations
  - 255.255.255.255, in subnet 192.168.0.0/24, 192.168.0.255
- Multicast address: packet will be delivered to a group of interested receivers
  - 224.0.0.0 - 239.255.255.255
- Private address: Routers can handle and forward packets within local network
  - 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12
- Link-local address: Routers will NOT forward packets with these addresses
  - 169.254.0.0/16

# Recap on Protocols

---

- IP (Internet Protocol): a glue of the Internet
- Ethernet: A widely used link-layer protocol
- ARP (Address Resolution Protocol): map the IP address to the link-layer address associated with the peers's hardware interface to be used in direct delivery.
- ICMP (Internet Control Message Protocol): send error messages and operational information indicating success or failure when communicating with another IP address.
- TCP (Transmission Control Protocol): provide reliable, ordered and error-checked delivery of a stream of bytes between applications on hosts communicating via an IP network.
- UDP (User Datagram Protocol): Suitable for where error checking and correction are not necessary and avoid the overhead of reliability.
- FTP, HTTP, HTTPS, SSH, ...

# Network Attacks

---

- Attack goals
  - Impersonation of a host
  - Denial of service
  - Access to information
  - Tampering with delivery mechanisms
- Sniffing
- Spoofing
- DoS
- Man-in-the-Middle



# Sniffing

---

- Sniffing (or eavesdropping) refers to the activity that gathers traffic from the local network
  - Put interface in promiscuous mode, to listen all transmissions even destination address is not mine
  - Can see anything - all data from link layer to application layer
  - If switched Ethernet is used, then the switch must be “convinced” that a copy of the traffic needs to be sent to the port of the sniffing host
- The technique is the basis of many attacks

# Why Sniffing?

---

- Many protocols at different layers transfer data (e.g., authentication/sensitive information, secrets) in the cleartext without encryption to protect **confidentiality**.

# Spoofing

---

- Spoofing means using a fake address to impersonate another host/node
  - Link layer: Spoofing the MAC address (ARP spoofing)
  - Network layer: e.g., build a packet with fake source IP address
  - Transport layer: TCP session Hijacking
  - Application-layer protocol: Domain Name Spoofing by generating a fake reply of DNS request

# Why Spoofing?

---

- Many protocols at different layers do not validate source of their received data.
- It is unknown whether a received data frame from network can be trusted. What can be trusted?

# Denial of Service

---

- Overloading and exhaust the available resources on certain node.
  - cpu resources
  - memory/cache resources
  - storage space resources
  - network connections resources
  - ....
- At different layers:
  - Transport layer: TCP SYN Flood, Smurf Amplification, Reflectors
  - Application layer: DNS Flood

# Why DoS?

---

- A trade-off between availability and security.
- Under limited resources, an overload allocation of resources easily triggered by attacker.
- Threat model is always important for security.

# Man-in-the-Middle

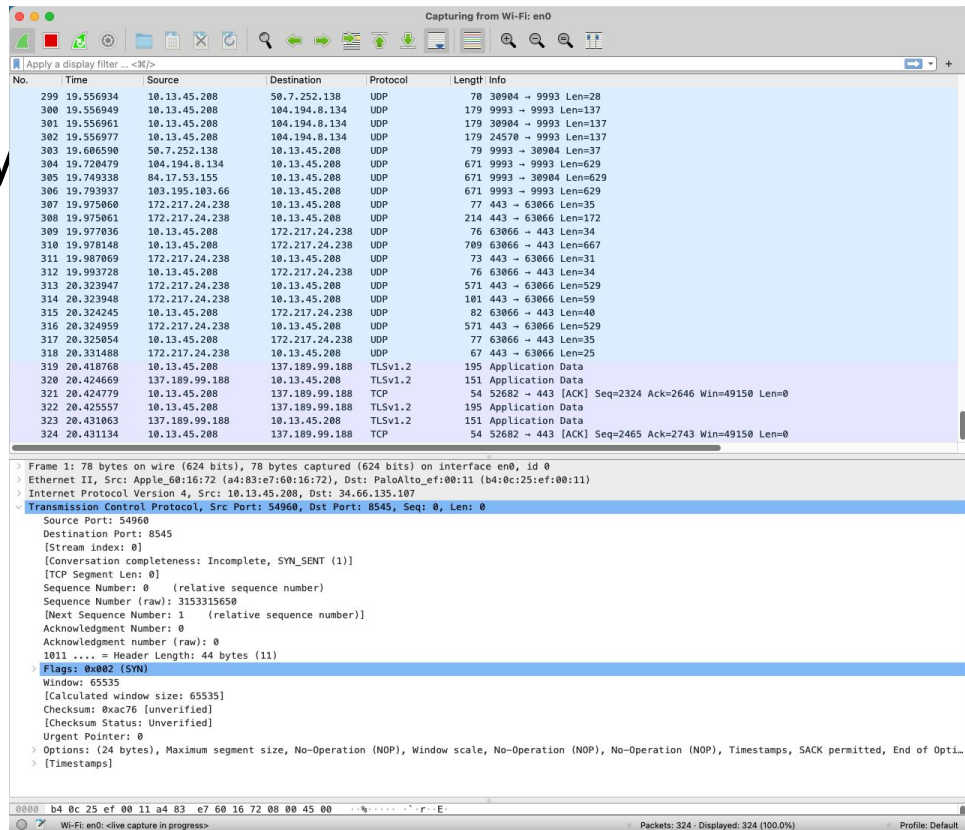
---

- Attacks can manipulate network traffic in the middle
- Examples:
  - ARP spoofing
  - HTTP MitM
- Why MitM?:
  - Lack of identity authentication
  - Lack of data encryption

# Wireshark

- A network protocol analyzer help us learn network security
- Wireshark: Capturing and analyzing network packets GUI-based (terminal-based version called TShark)

“工欲善其事，必先利其器”





# An example of observing ARP using wireshark

start

Wireshark interface showing a packet capture on interface en0. The packet list displays two packets:

No.	Time	Source	Destination	Protocol	Length	Info
301	20.391676	PaloAlto_ef:00:11	Broadcast	ARP	60	Gratuitous ARP for 10.13.63.254 (Request)
889	57.879603	PaloAlto_ef:00:11	Apple_60:16:72	ARP	60	10.13.63.254 is at b4:0c:25:ef:00:11

The packet details pane shows the structure of the selected packet (No. 301):

- Frame 301: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0
  - Interface id: 0 (en0)
    - Encapsulation type: Ethernet (1)
      - Arrival Time: Nov 8, 2022 13:52:05.813544000 HKT
        - [Time shift for this packet: 0.000000000 seconds]
      - Epoch Time: 1667886725.813544000 seconds
        - [Time delta from previous captured frame: 0.314858000 seconds]
        - [Time delta from previous displayed frame: 0.000000000 seconds]
        - [Time since reference or first frame: 20.391676000 seconds]
      - Frame Number: 301
      - Frame Length: 60 bytes (480 bits)
      - Capture Length: 60 bytes (480 bits)
      - [Frame is marked: False]
      - [Frame is ignored: False]
      - [Protocols in frame: eth:ethertype:arp]
      - [Coloring Rule Name: ARP]
      - [Coloring Rule String: arp]
    - Ethernet II, Src: PaloAlto\_ef:00:11 (b4:0c:25:ef:00:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
      - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      - Source: PaloAlto\_ef:00:11 (b4:0c:25:ef:00:11)
      - Type: ARP (0x0806)
      - Padding: 00000000000000000000000000000000
    - Address Resolution Protocol (request/gratuitous ARP)
      - Hardware type: Ethernet (1)
      - Protocol type: IPv4 (0x0800)
      - Hardware size: 6
      - Protocol size: 4
      - Opcode: request (1)
      - [Is gratuitous: True]
      - Sender MAC address: PaloAlto\_ef:00:11 (b4:0c:25:ef:00:11)
      - Sender IP address: 10.13.63.254
      - Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
      - Target IP address: 10.13.63.254

The packet bytes pane shows the raw data: 0000 ff ff ff ff ff b4 0c 25 ef 00 11 08 06 00 01

Display filter:

e.g., arp, http, icmp,

tcp.port == 80,

ip.addr == x.x.x.x

http contains "string"

tcp contains "string"

protocol data frame:  
concrete fields with value

stop



Display filter:  
e.g., arp, http, icmp,  
tcp.port == 80,  
ip.addr == x.x.x.x  
http contains "string"  
tcp contains "string"

# Others

---

- Assignment 3 ddl:
  - Nov. 25 11:59pm
- My office hour
  - Tuesday 4:15PM - 5:15PM, SHB\_826B
  - Ask questions on piazza
  - [cy021@ie.cuhk.edu.hk](mailto:cy021@ie.cuhk.edu.hk)