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

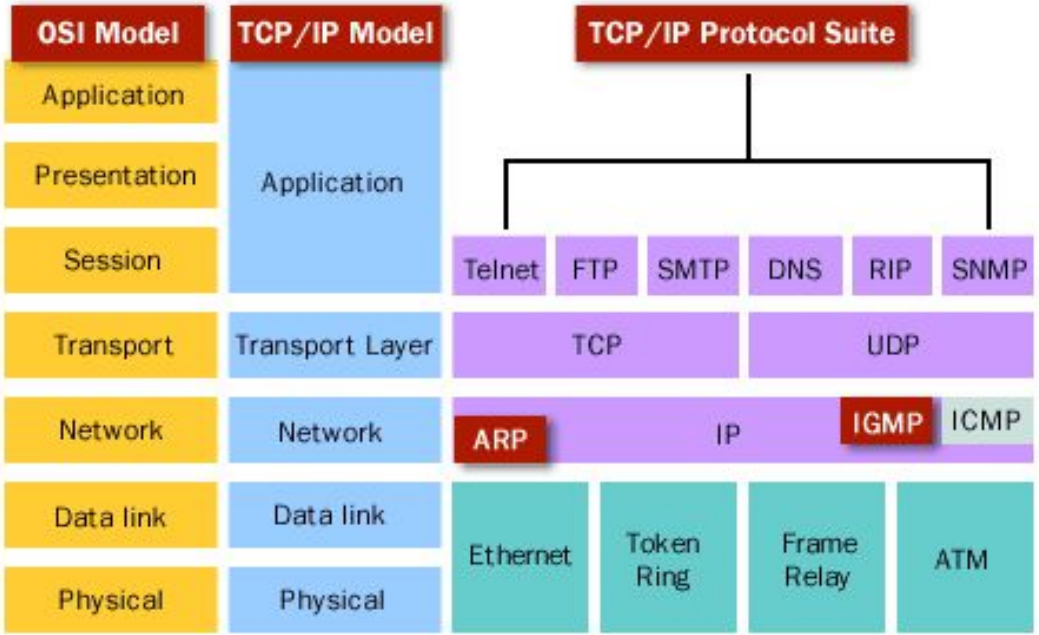
Layering

- 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)

In pratice, we adopt TCP/IP Model/Suite



https://www.dispersednet.com/dhcp-tcp-ip/module3/tcp-ip-protocolSuite.php

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 por 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

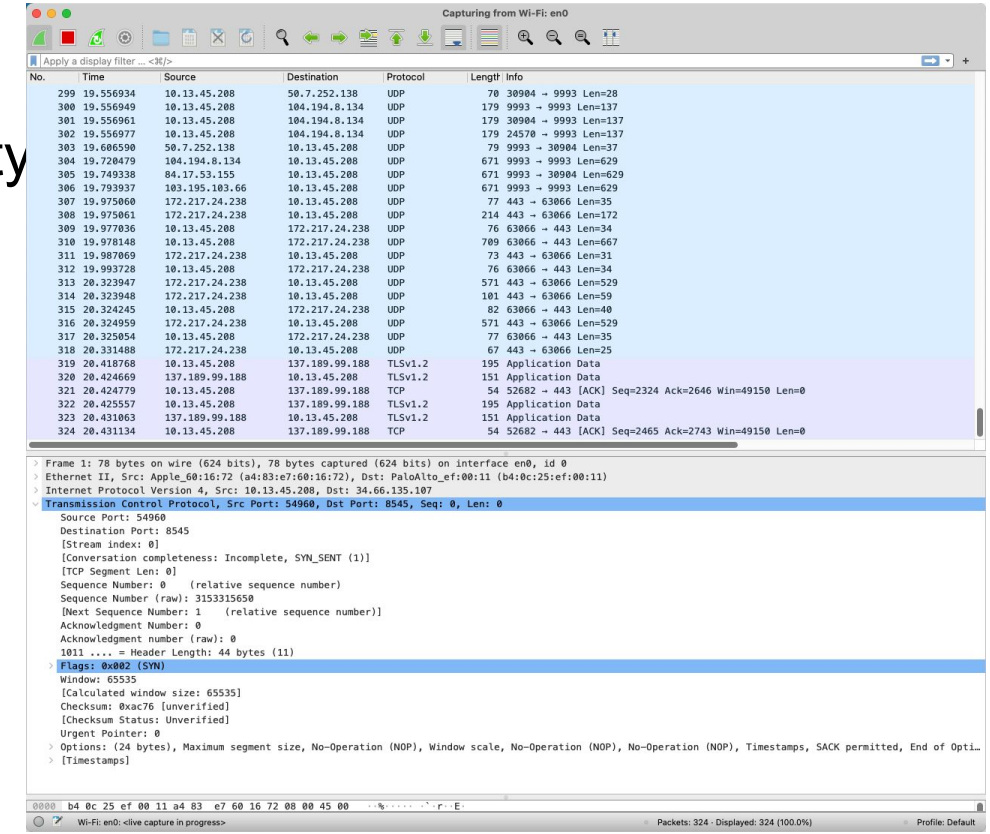
- Attacks can manipulate network traffic in the middle

- Examples:
  - ARP spoofing
  - HTTP MitM

- Why MitM?:
  - Lack of identity authentication
  - Lack of data encryption

Wireshark

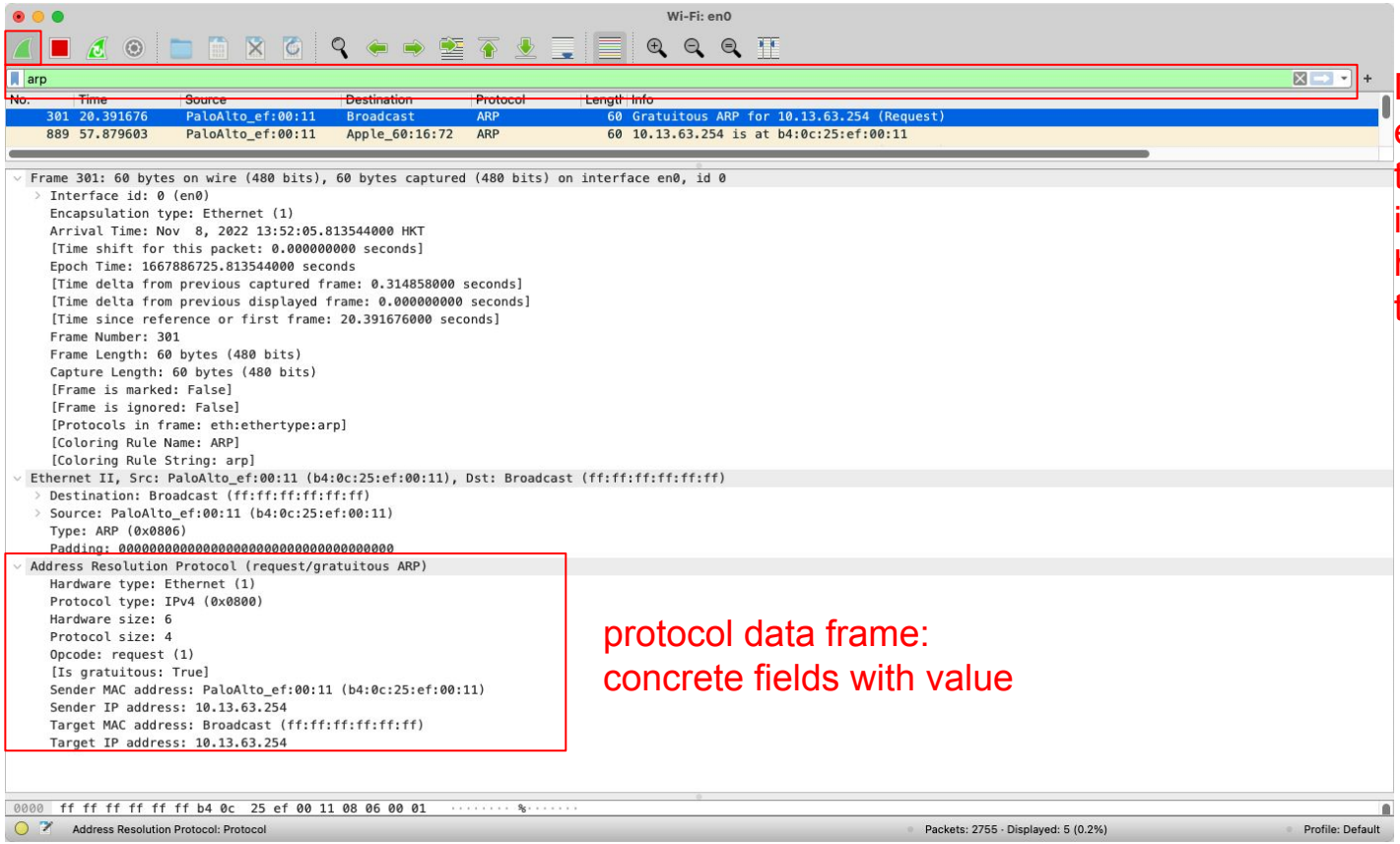
- A network protocol analyzer help us learn network security
- Wireshark: Capturing and analyzing network packetsGUI-based (terminal-based version called TShark)



“工欲善其事，必先利其器”

An example of observing ARP using wireshark

start

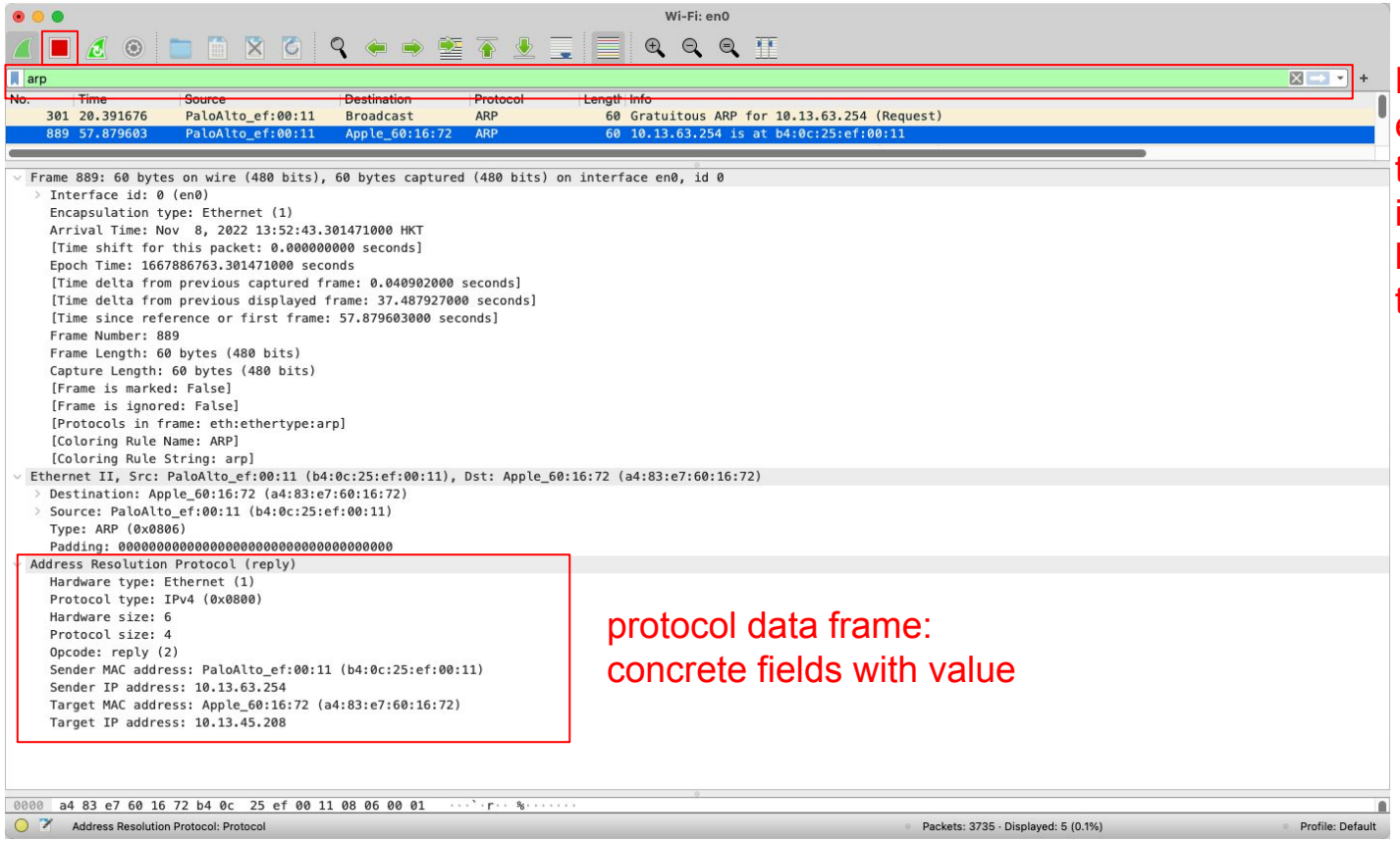


Display filter:
e.g., arp, http, icmp,
tcp.port == 80,
ip.addr == x.x.x.x
http contains “string”
tcp contains “string”

protocol data frame:
concrete fields with value

An example of observing ARP using wireshark

stop



protocol data frame:
concrete fields with value

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