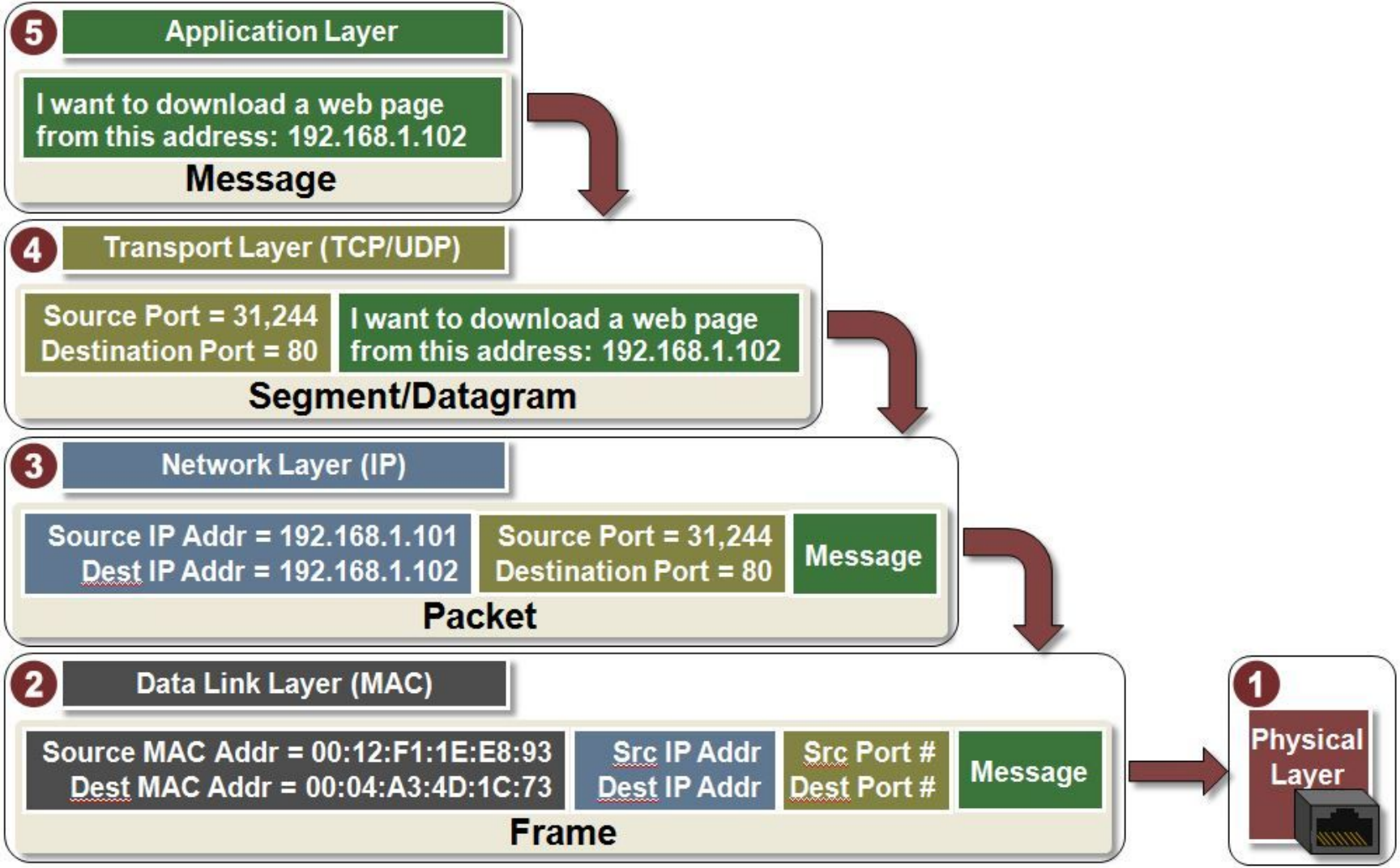
Network Security Overview

2019/04/29 by zolution
@ NASA 1! Training

Agenda

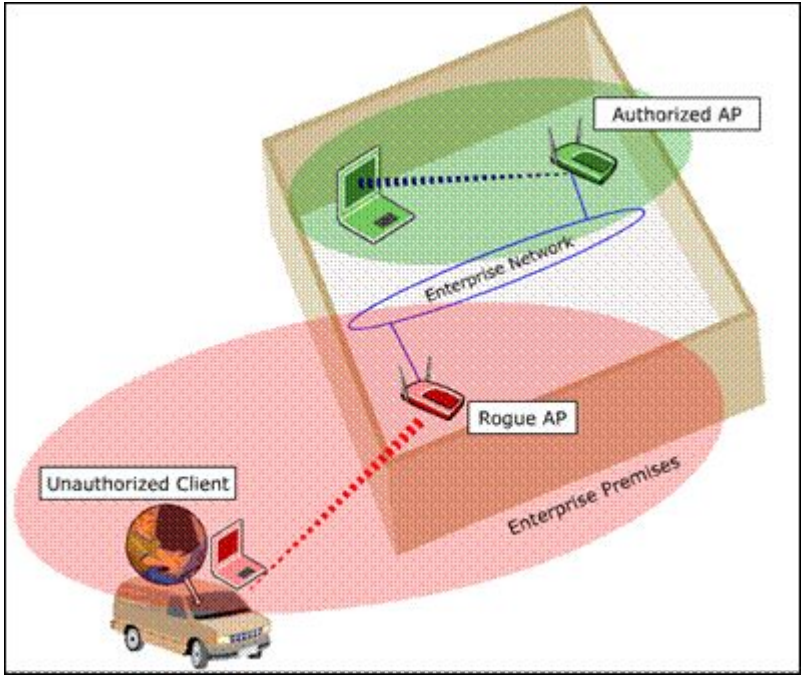
- Physical Layer (L1) Attack
- Link Layer (L2) Attack
- Network Layer (L3/L4) Attack
- Application Layer (L5) Attack
- Lab: SYN Cookie


5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

Physical Layer Attack

Rogue Access Point

- Web login APs
  - NTU, TPE-free, iTaiwan, ...
- Unauthorized Access Leak
- Man-in-the-middle Attack



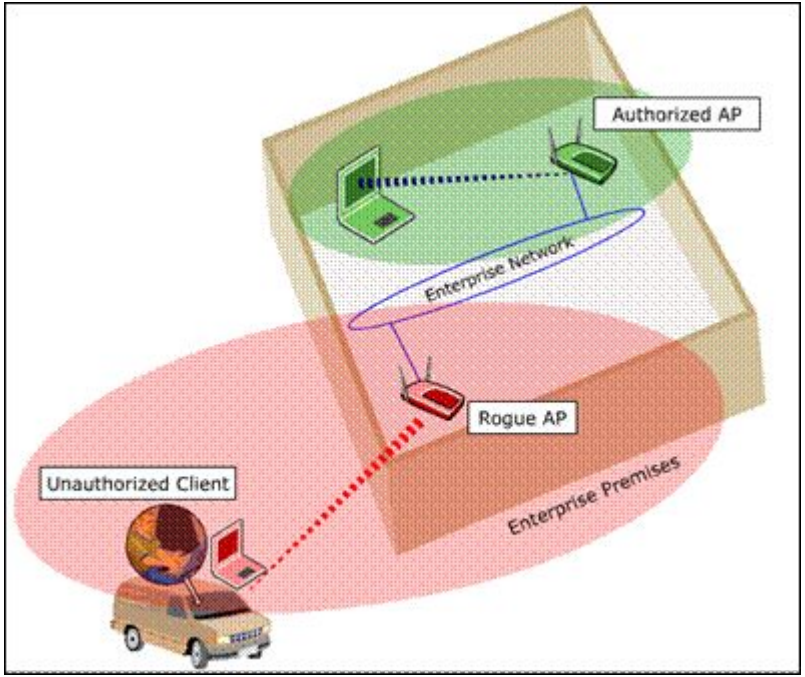
Man-in-the-middle (MitM) Attack

- 中間人攻擊
- Let one user (ex: client) trust the attackers to be another user (ex: server)

- Example: Key Exchange
  - Alice <-> Bob (expected)
  - Alice <-> Mallort <-> Bob (attacked)
  - Alice thought she established a secured channel with Bob, but in fact with Mallory

Rogue Access Point

- Web login APs
  - NTU, TPE-free, iTaiwan, ...
- Unauthorized Access Leak
- Man-in-the-middle Attack (HOW?)



Link Layer Attack

Link Layer Attack

- ARP Spoofing
- MAC Flooding
- DHCP Spoofing
- DHCP Starvation Attack

Address Resolution Protocol (ARP)

- 10.1.1.222 does not know the MAC address of 10.1.1.111
- Broadcast ARP Request
  - “Who is 10.1.1.111? Tell 10.1.1.222”
- ARP Reply
  - “10.1.1.111 is at 01:23:45:67:ab:cd”

ARP Spoofing

- Spoof the ARP Replies
  - “10.1.1.111 is at 01:23:45:67:ab:cd”
  - “10.1.1.111 is at cc:00:dd:00:ee:00”
- Poisoning the ARP cache

- Man-in-the-Middle Attack is possible, how to attack?

ARP Spoofing Mitigation

- Port Security
  - Similar to NTU Dorm (not BOT) network environment
  - Restrict: MAC <-> Physical Port

MAC Flooding

- If the MAC address is not in the MAC address table
  ⇒ Broadcast the packet on all ports
- Keep MAC address <-> Physical Port

- But MAC address table size is limited.

MAC Flooding

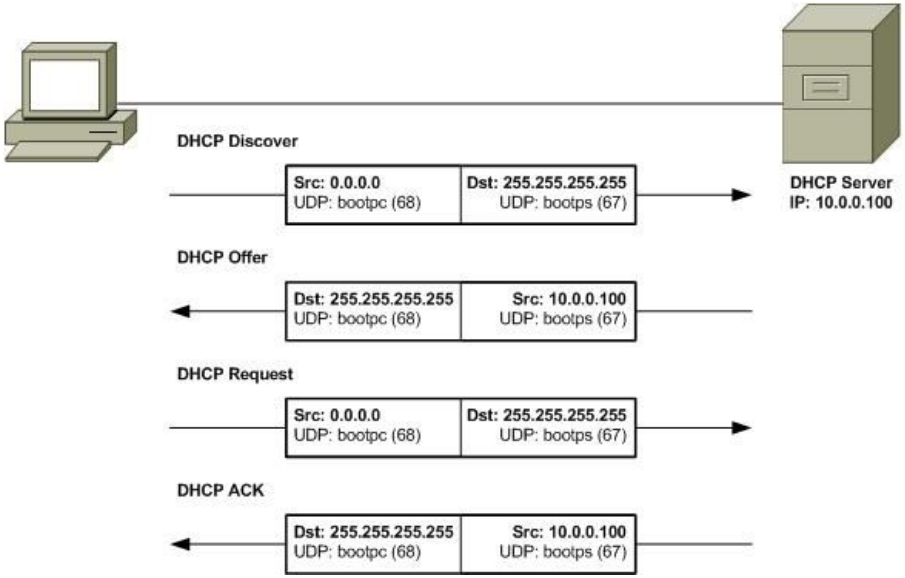
- Spoof MAC Addresses ⇒ Exhausting MAC address table

- Switch will start to **broadcast every packet** on all ports.
  - Eavesdropping the victim's traffic
  - Consume the CPU/Memory of the switch

DHCP Starvation Attack

- DHCP Starvation = DHCP Exhaustion
- Numerous DISCOVERY packets with unique but fake MAC addresses

- DHCP cannot get IP addresses



DHCP Spoofing

- DHCP server provides:
  - IP address
  - Default Gateway
  - DNS Server
- What will happen when there are multiple DHCP spoofing?

- Solution?

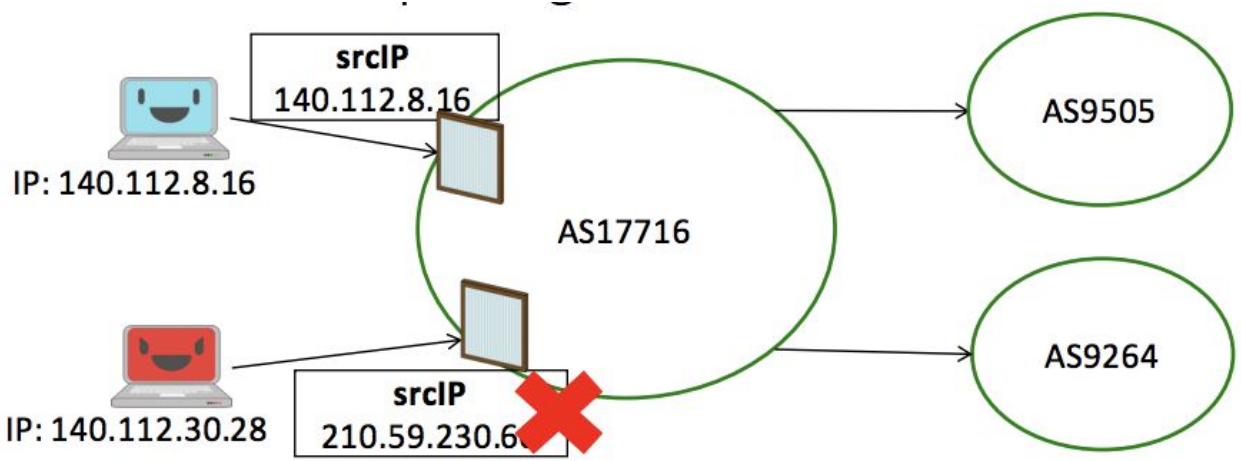
DHCP Spoofing Mitigation

- DHCP snooping
  - You have seen the commands in HW3
  - `ip dhcp snooping trust`
- Allow DHCP ONLY from trusted interfaces.
- Other DHCP packet will be dropped.

Network Layer Attack

IP Spoofing

- Most ISPs will not validate the source IP address
- Widely used in amplification attacks
- Hard to track the real source
- Mentioned in Prof.'s lecture: AS Ingress Filtering



DNS Spoofing

- DNS Poisoning


你
DNS
server
請問 google.com 的
IP 位置是什麼OAO？


0.0.0.0

DNS Spoofing

- DNS Poisoning
- Hijacked by the ISP (ex: China Firewall)

Problem?

- HTTP website hijack / manipulate
- Redirection

Denial-of-Service (DoS)

- Exhaust Resources (Calculation / Network)
  ⇒ Unable the access / provide services
- Overwhelming the victim with a large number of packets
- Flooding
  - TCP SYN
  - ICMP
  - UDP

Denial-of-Service (DoS)

- Distributed Denial-of-Service (DDoS)
- BotNet
- DDoS-as-a-service

Amplification Attack / Reflection Attack

- DNS Reflection attack
  - Request is small
  - Response is large
- Src IP spoofing as victim IP

- NTP/ICMP Reflection Attack

DDoS Attack Types

- By traffic:
  - Service Unavailable
  - Upstream Congestion
  - ISP is affected

- By OSI layer
  - Network Layer (L3/L4) ⇒ Overwhelming Network Interface
  - Application Layer (L7) ⇒ Exhaust the CPU/Memory of the server
    ⇒ Algorithmic Complexity Attack

Mitigation of DDoS

- Difficult
- Cloud-based DDoS Defense
- Proof of Work

Proof of Work

- Ask the user to solve a puzzle first
  ⇒ It takes time and computation cost
  ⇒ Increase the time and cost needed for attack
  ⇒ Attack mitigated

- Ex: Give x s.t. SHA1(x)[-6:] = 123456

Application Layer Attack

Protocols

- Plaintext
  - Http / telnet / ftp/ tftp

- Encrypted
  - Https / ssh / sftp

- 上PTT不要再用telnet啦，密碼滿天飛不好玩的

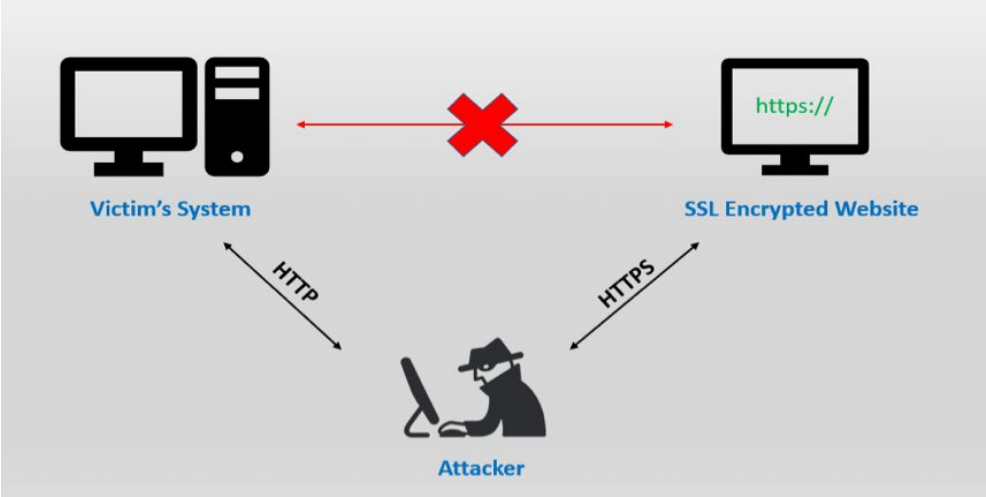
HTTPS

- HTTPS Certificate
  - Self-signed certificate
  - Invalid cert domain
  - Signed by unknown Certificate Authority (CA)
  - Revoked cert

HTTPS

- SSL strip
  - Man in the middle
  - HTTP <-> Hacker <-> HTTPS
- IDN Homograph attack
  - https://apple.com/
  - https://apple.com/

- MitM, Phishing, DNS spoofing?

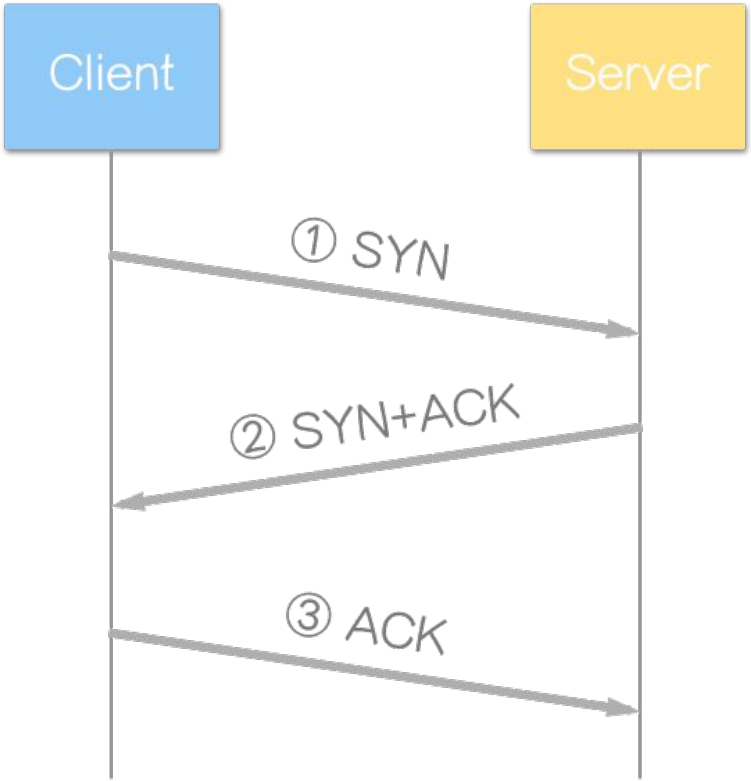


More on Web Security

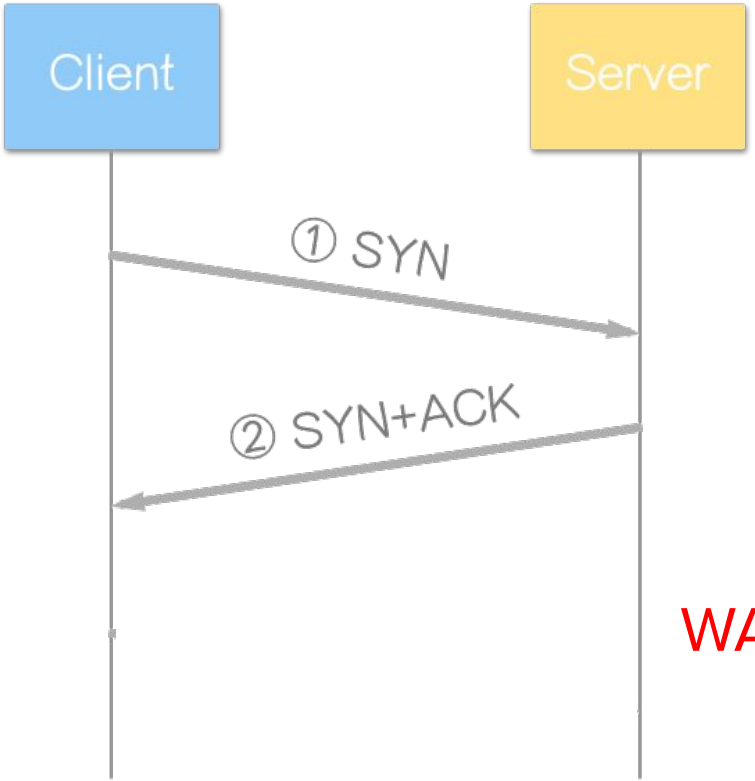
- OWASP Top 10
  - https://www.owasp.org/index.php/Top_10-2017_Top_10

Lab: SYN Cookie

SYN Cookie Review



SYN Cookie Review



WAIT FOR ACK

SYN Cookie Review

- Server keeps the state after sending SYN-ACK
- Table size limited
- Server resource exhausted

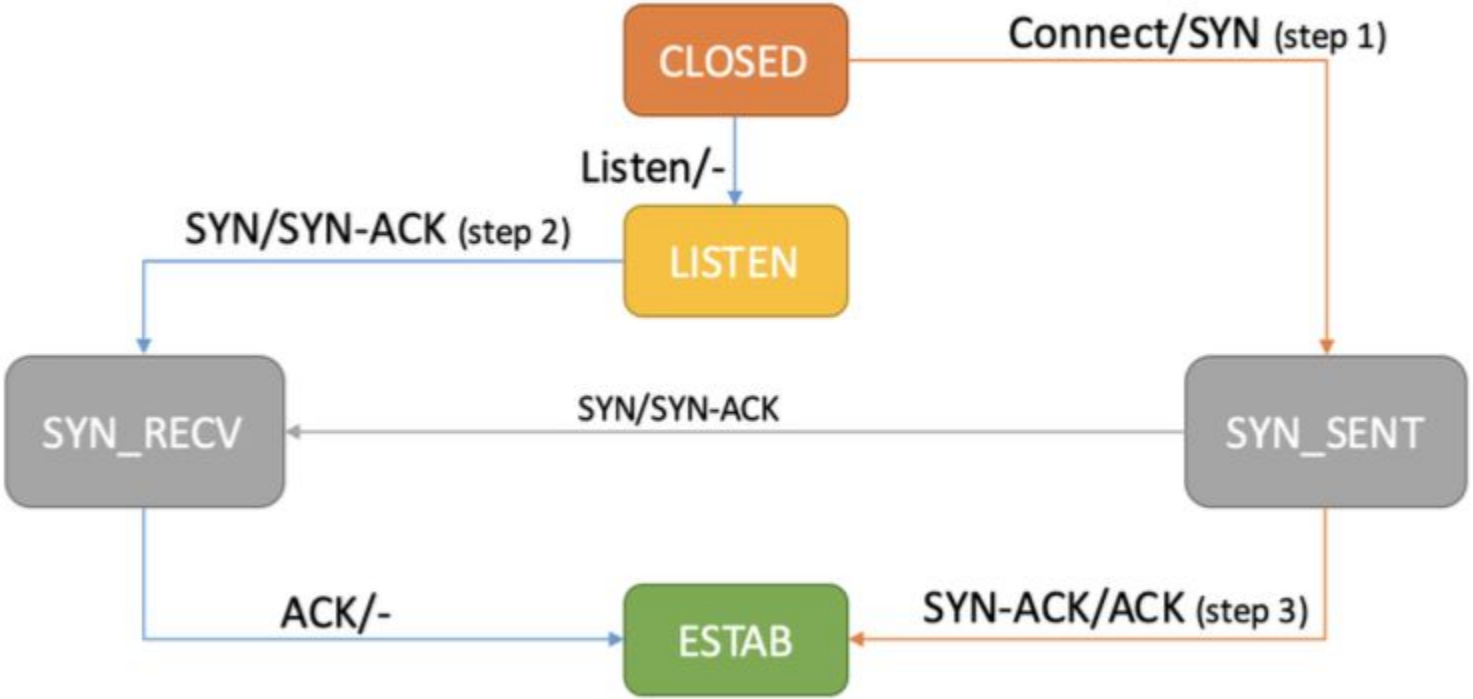
⇒ SYN Cookie ⇒ Stores the state in the cookie and can be verified later

SYN Cookie Review

Cookie = MAC_{key} (Server_IP, Client_IP, Server_port, Client_port, Client_state, time)

Why not H(Server_IP, Client_IP, Server_port, Client_port, Client_state, time)?

TCP Cookie Review - netstat



Lab Requirements

- Implement SYN Flood Attack
- Enable / Disable SYN Cookie on the server
- Compare the differences

Lab Step

1. Download 2 VMs (Same as the previous section, user/pass = nasa/2019)
2. Install hping3 on VM1
3. Install and launch a web server on VM2
   - All kinds of web servers are fine. For example: `python3 -m http.server 8000`
4. Use netstat to monitor the connection state table
   - `netstat -tac`
5. Check if SYN Cookie is enabled
   - `cat /proc/sys/net/ipv4/tcp_syncookies`
   - `sysctl -n net.ipv4.tcp_syncookies`

Lab Step

6. Start SYN Flood on VM1 to VM2
   - `sudo hing3 -i u1 -S -p [port] [ip of VM2]`
7. Observe the returning logs in hping3
8. Check system message
   - `cat /var/log/syslog`
9. Disable SYN Cookie and repeat the steps above.

Lab Discussion and Demo

- Show the system log denoting that SYN Cookie is enabled and distributed.
- Show the congestion / attacking netstat log when SYN Cookie is disabled.

- Bonus: Can you modify the threshold for enabling SYN Cookie defense?