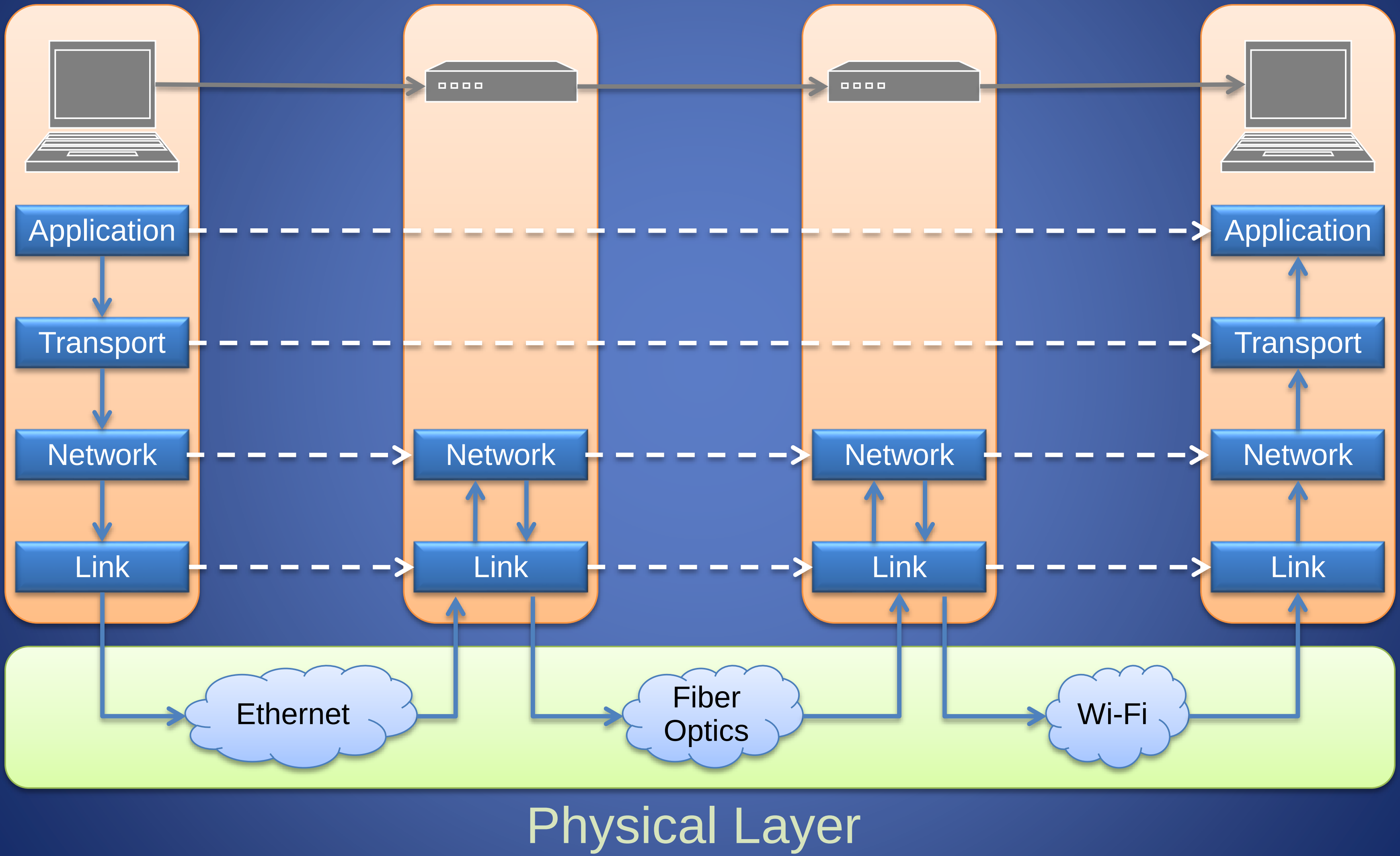
Network Security I

TCP/IP Attacks

Original slides by M. Goodrich and R. Tamassia

Modifications for IV1013 by Markus Hidell

Internet Layers



Link Layer Attacks

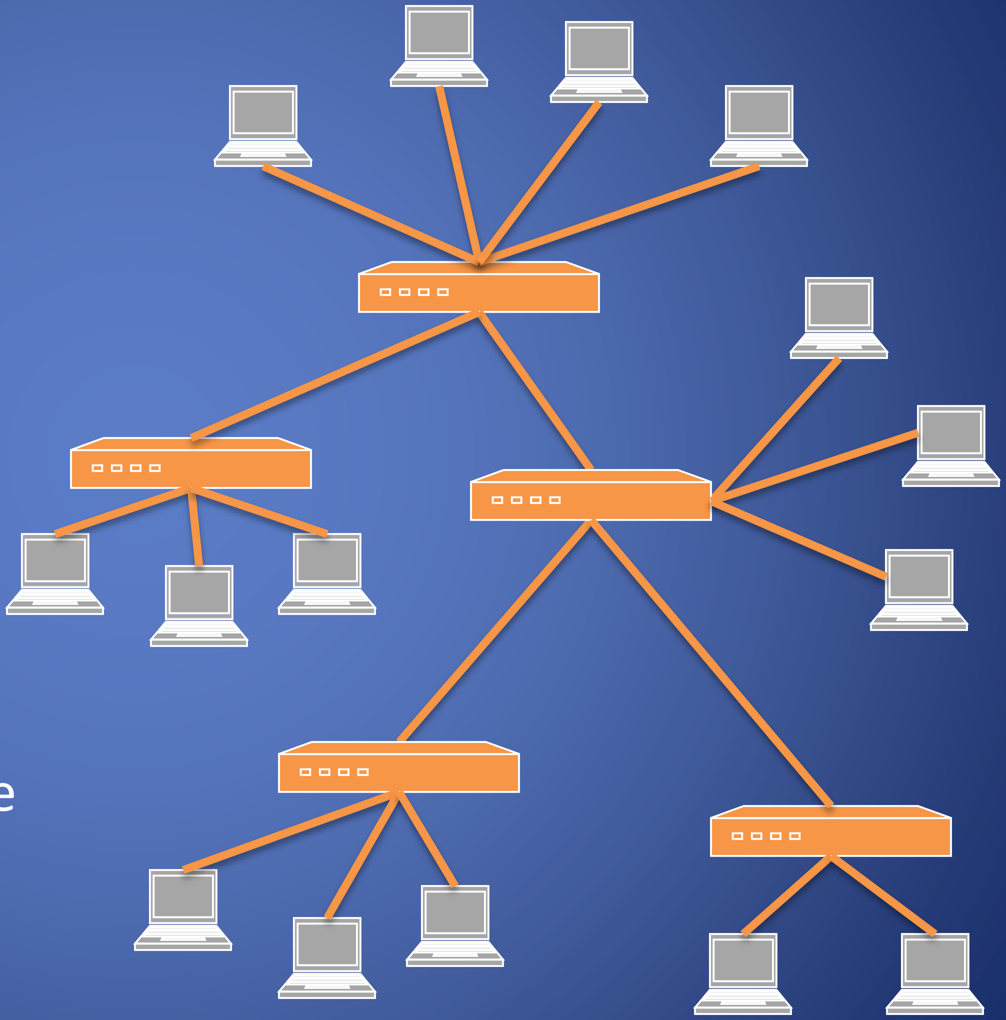
ARP

MAC Addresses

- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92
- The next three can be assigned by organizations as they please, with uniqueness being the only constraint
- Organizations can utilize MAC addresses to identify computers on their network
- MAC address can be reconfigured by network interface driver software

Switched LAN

- Switches can be arranged into a tree
- Each port learns the MAC addresses of the machines in the segment (subtree) connected to it
- Frames to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored



MAC Address Filtering

- A switch can be configured to provide service only to machines with specific MAC addresses
- Allowed MAC addresses need to be registered with a network administrator
- A MAC spoofing attack impersonates another machine
  - Find out MAC address of target machine
  - Reconfigure MAC address of rogue machine
  - Try to turn off or unplug target machine
- Countermeasure
  - Disable duplicate MAC addresses

Viewing and Changing MAC Addresses

- Viewing the MAC addresses of the interfaces of a machine
  - Linux: ifconfig
  - Windows: ipconfig /all
- Changing a MAC address in Linux
  - Stop the networking service: /etc/init.d/network stop
  - Change the MAC address: ifconfig eth0 hw ether <MAC-address>
  - Start the networking service: /etc/init.d/network start
- Changing a MAC address in Windows
  - Open the Network Connections applet
  - Access the properties for the network interface
  - Click “Configure …”
  - In the advanced tab, change the network address to the desired value
- Changing a MAC address requires administrator privileges

ARP

- The address resolution protocol (ARP) connects the network layer to the data layer by converting IP addresses to MAC addresses
- ARP works by broadcasting requests and caching responses for future use
- The protocol begins with a computer broadcasting a message of the form

who has <IP address1> tell <IP address2>

- When the machine with <IP address1> or an ARP server receives this message, its broadcasts the response

<IP address1> is <MAC address>

- The requestor’s IP address <IP address2> is contained in the link header
- The Linux and Windows command arp - a displays the ARP table

```
Internet Address      Physical Address      Type
128.148.31.1          00-00-0c-07-ac-00     dynamic
128.148.31.15         00-0c-76-b2-d7-1d     dynamic
128.148.31.71         00-0c-76-b2-d0-d2     dynamic
128.148.31.75         00-0c-76-b2-d7-1d     dynamic
128.148.31.102        00-22-0c-a3-e4-00     dynamic
128.148.31.137        00-1d-92-b6-f1-a9     dynamic
```

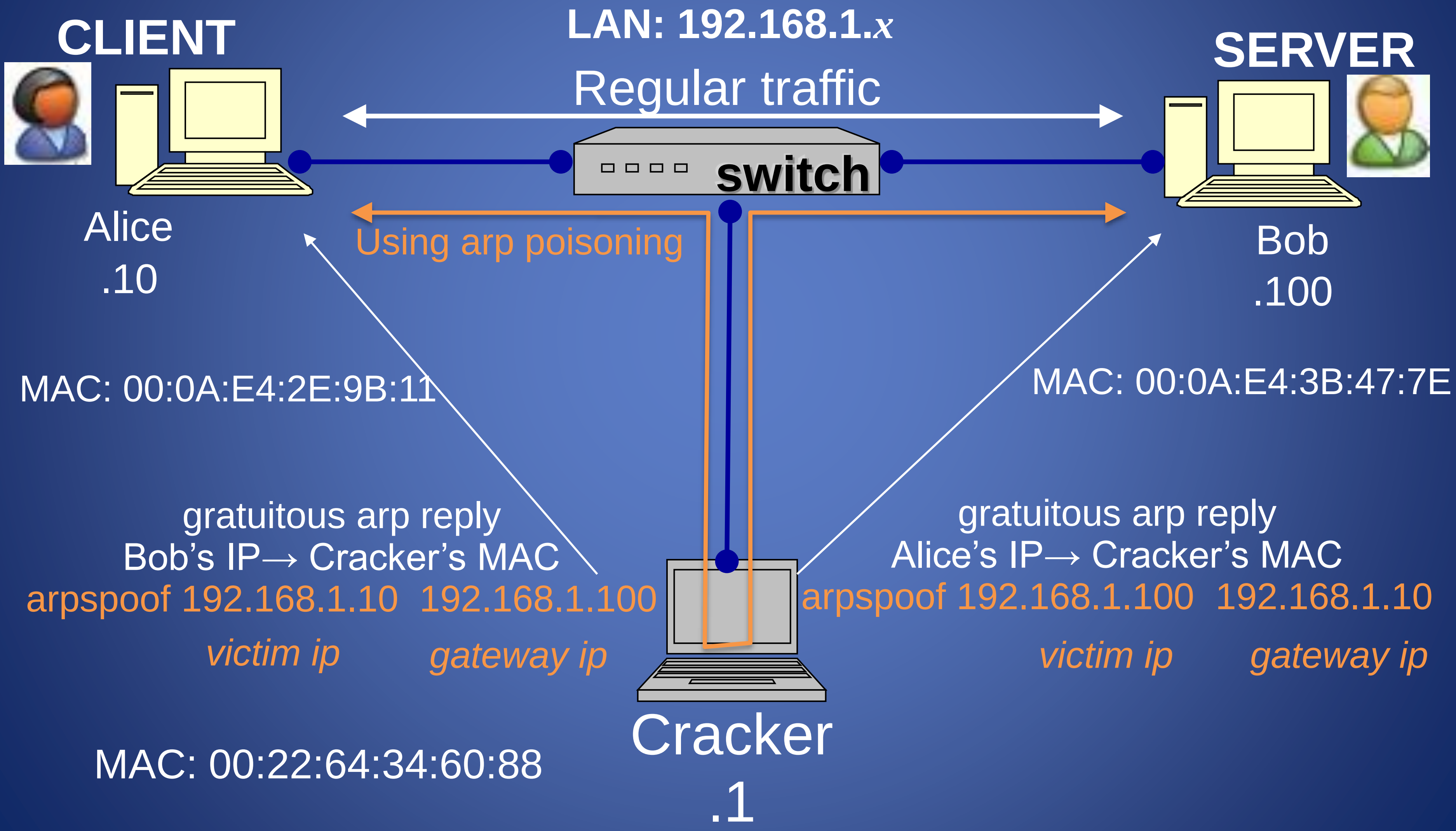
ARP Spoofing

- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

ARP Poisoning (ARP Spoofing)

- According to the standard, almost all ARP implementations are stateless
- An ARP cache updates every time that it receives an ARP reply… even if it did not send any ARP request!
- It is possible to "poison" an ARP cache by sending gratuitous ARP replies
- Using static entries solves the problem but it is almost impossible to manage!

DEMO 1: ARP Spoofing



CLIENT

LAN: 192.168.1.*x*

SERVER

Regular traffic

switch

Alice
.10

Using arp poisoning

Bob
.100

MAC: 00:0A:E4:2E:9B:11

MAC: 00:0A:E4:3B:47:7E

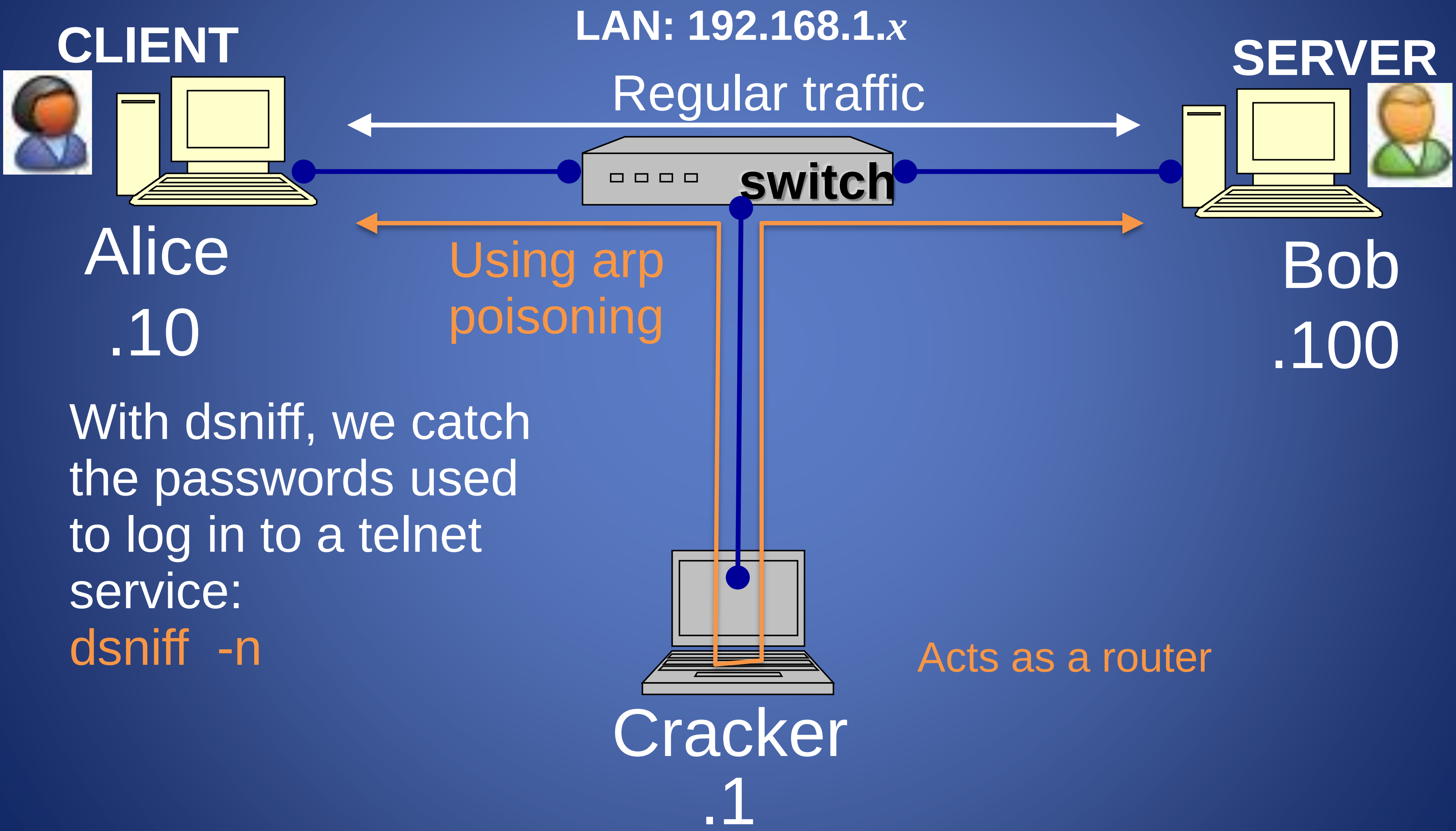
gratuitous arp reply
Bob’s IP→ Cracker’s MAC
arpspoof 192.168.1.10 192.168.1.100
victim ip *gateway ip*

gratuitous arp reply
Alice’s IP→ Cracker’s MAC
arpspoof 192.168.1.100 192.168.1.10
victim ip *gateway ip*

MAC: 00:22:64:34:60:88

Cracker
.1

DEMO 1: catch telnet password



LAN: 192.168.1.*x*

CLIENT

Regular traffic

SERVER

switch

Alice
.10

Using arp poisoning

Bob
.100

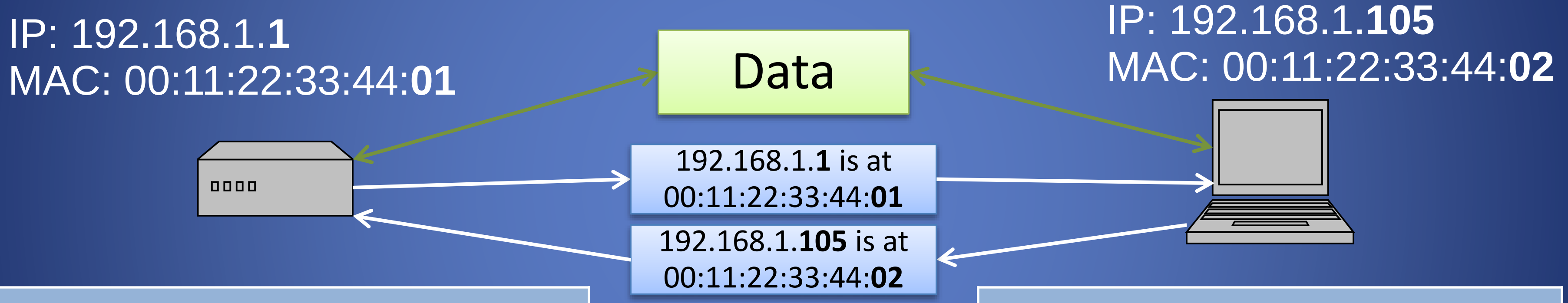
Cracker
.1

Acts as a router

With dsniff, we catch the passwords used to log in to a telnet service:

dsniff -n

ARP Caches



IP: 192.168.1.**1**
MAC: 00:11:22:33:44:**01**

Data

192.168.1.**1** is at
00:11:22:33:44:**01**

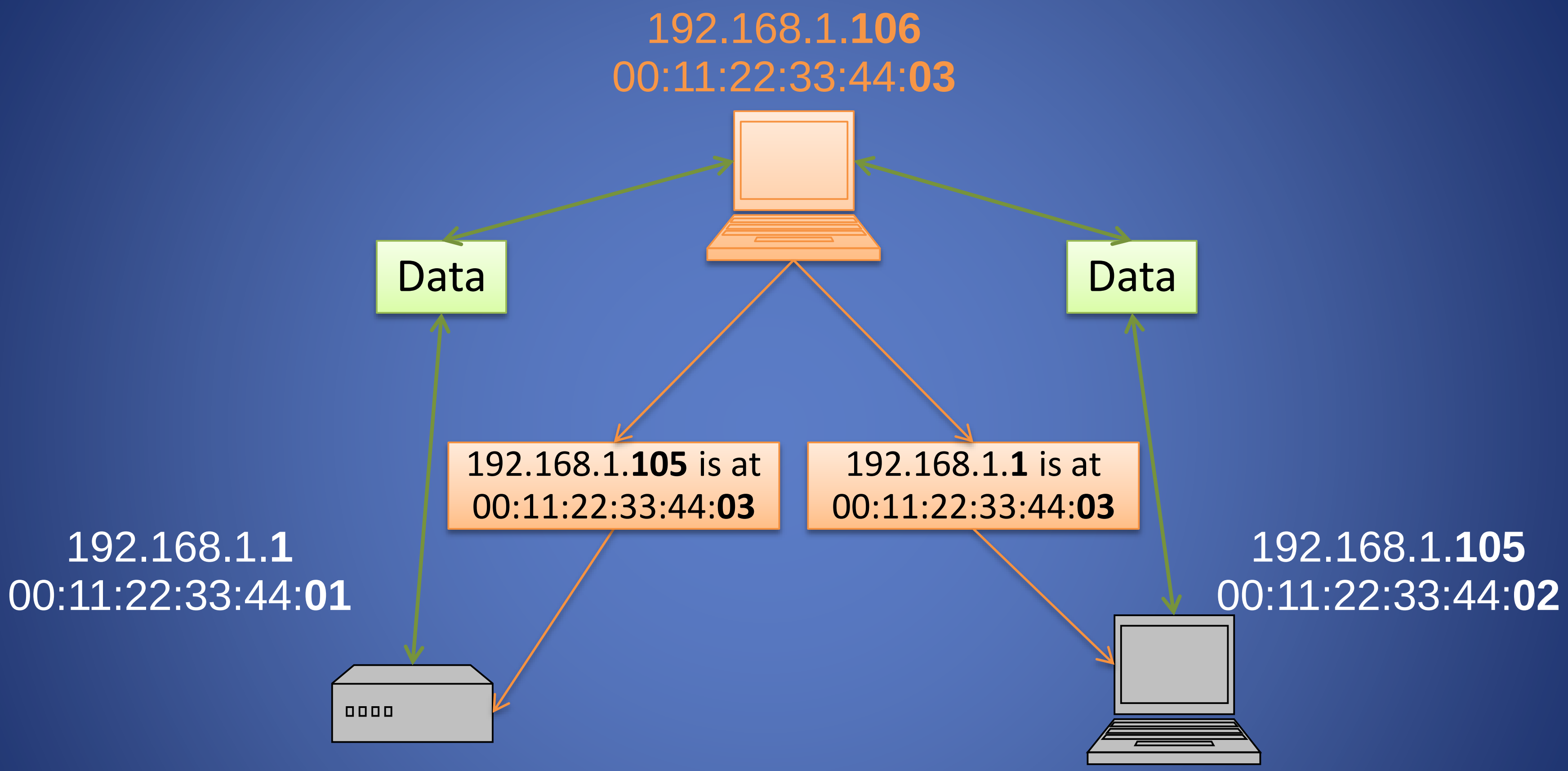
192.168.1.**105** is at
00:11:22:33:44:**02**

IP: 192.168.1.**105**
MAC: 00:11:22:33:44:**02**

ARP Cache	
192.168.1.**105**	00:11:22:33:44:**02**

ARP Cache	
192.168.1.**1**	00:11:22:33:44:**01**

Poisoned ARP Caches



192.168.1.**106**
00:11:22:33:44:**03**

Data

Data

192.168.1.**105** is at
00:11:22:33:44:**03**

192.168.1.**1** is at
00:11:22:33:44:**03**

192.168.1.**1**
00:11:22:33:44:**01**

192.168.1.**105**
00:11:22:33:44:**02**

Poisoned ARP Cache	
192.168.1.**105**	00:11:22:33:44:**03**

Poisoned ARP Cache	
192.168.1.**1**	00:11:22:33:44:**03**

Network Layer Attacks

ICMP and IP

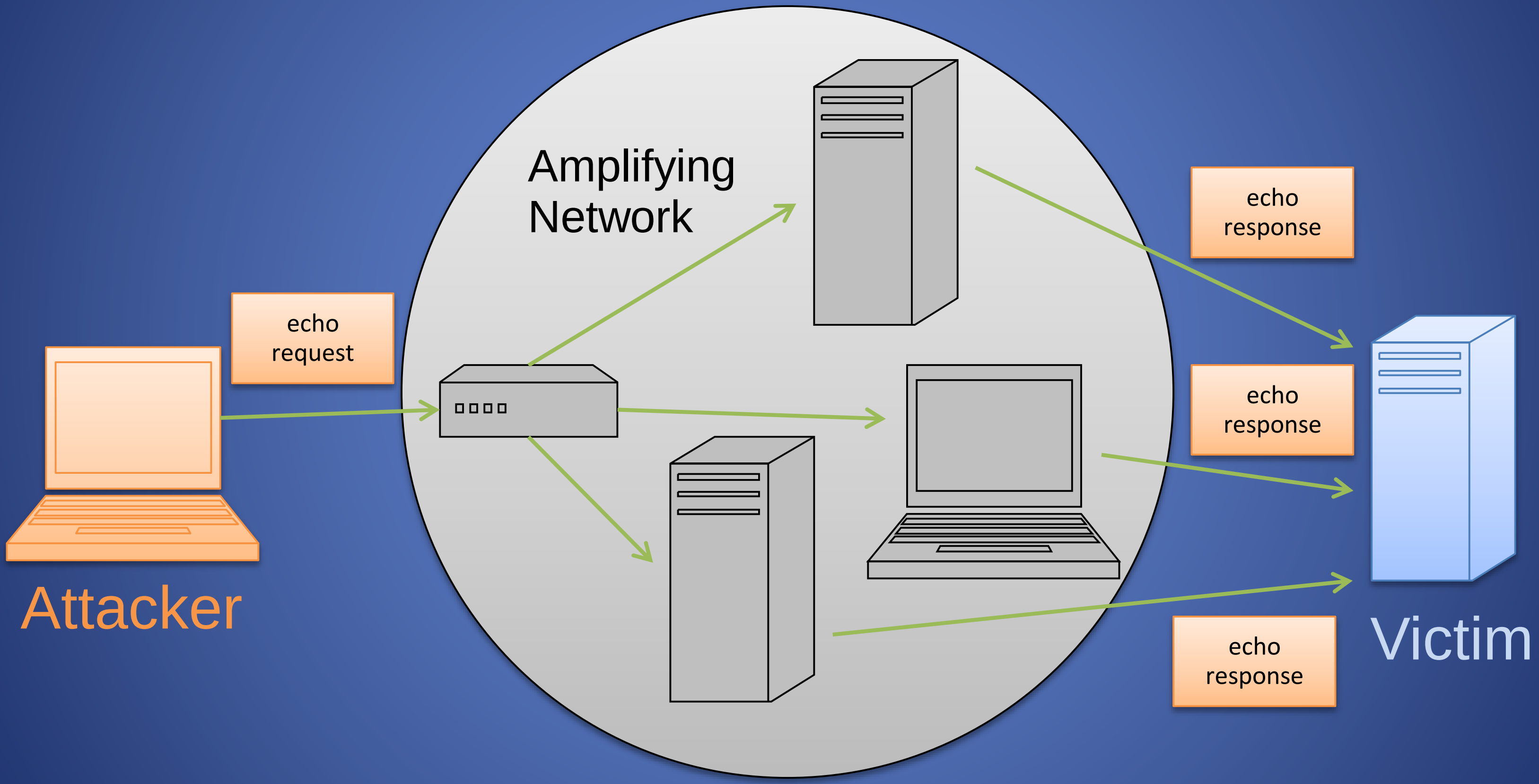
ICMP

- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Simple messages encapsulated in single IP packets
  - Considered a network layer protocol
- Tools based on ICMP
  - Ping: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  - Traceroute: sends series of UDP packets with increasing TTL value to discover routes based on received ICMP error messages

ICMP Attacks

- Ping flooding
  - Powerful machine overwhelms a weaker host with ping requests
- Ping of death
  - ICMP specifies messages must fit a single IP packet (64KB)
  - Send a ping packet that exceeds MTU –> IP fragmentation
  - IP fragment with max offset can be crafted to exceed maximum IP packet size (64 KB)
  - Reassembled packet caused several operating systems to crash due to a buffer overflow
- Smurf
  - Ping a broadcast address using a spoofed source address

Smurf Attack



IP Vulnerabilities

- Unencrypted transmission
  - Eavesdropping possible at any intermediate host during routing
- No source authentication
  - Sender can spoof source address, making it difficult to trace packet back to attacker
- No integrity checking
  - Entire packet, header and payload, can be modified while en route to destination, enabling content forgeries, redirections, and man-in-the-middle attacks
- No bandwidth constraints
  - Large number of packets can be injected into network to launch a denial-of-service attack
  - Broadcast addresses provide additional leverage

IP Spoofing

- IP Spoofing is an attempt by an intruder to send packets from one IP address that appear to originate at another
- If the server thinks it is receiving messages from the real source after authenticating a session, it could inadvertently behave maliciously
- There are two basic forms of IP Spoofing
    - Blind Spoofing
        - Attack from any source—attacker won’t see responses
    - Non-Blind Spoofing
        - Attack from the same subnet (can sniff packets)

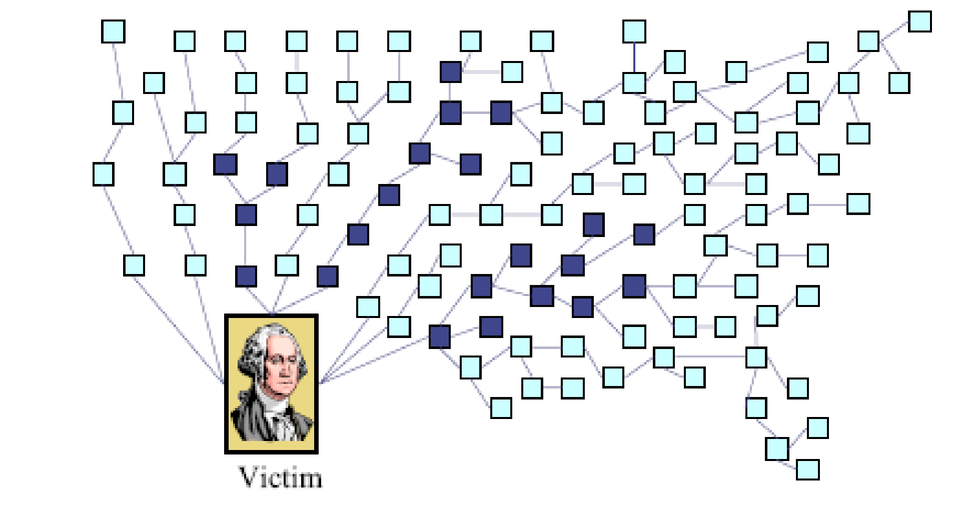
Non-Blind IP Spoofing

- IP Spoofing without inherently knowing the acknowledgment sequence pattern (of higher-level protocols like TCP)
  - Done on the same subnet
  - Use a packet sniffer to analyze the sequence pattern
    - Packet sniffers intercept network packets
    - Eventually decodes and analyzes the packets sent across the network
    - Determine the acknowledgment sequence pattern from the packets
    - Send messages to server with actual client's IP address and with validly sequenced acknowledgment number

Denial of Service Attack

- Send large number of packets to host providing service
  - Slows down or crashes host
  - Often executed by botnet
- Attack propagation
  - Starts at zombies
  - Travels through tree of internet routers rooted
  - Ends at victim
- IP source spoofing
  - Hides attacker
  - Scatters return traffic from victim

Source:
M.T. Goodrich, Probabalistic Packet Marking for Large-Scale IP Traceback, IEEE/ACM Transactions on Networking 16:1, 2008.



Dealing with IP Spoofing

- Block packets from outside administrative domain in case it has a source address from inside that domain
- Block outgoing traffic with source addresses from outside the domain
- Use IP traceback techniques

IP Traceback

- Problem
  - How to identify leaves of DoS propagation tree
  - Routers next to attacker
- Issue
  - There are millions of Internet routers
  - Attacker can spoof source address
  - Attacker knows that traceback is being performed
- Approaches
  - Filtering and tracing (immediate reaction)
  - Messaging (additional traffic)
  - Logging (additional storage)
  - Probabilistic marking

Probabilistic Packet Marking

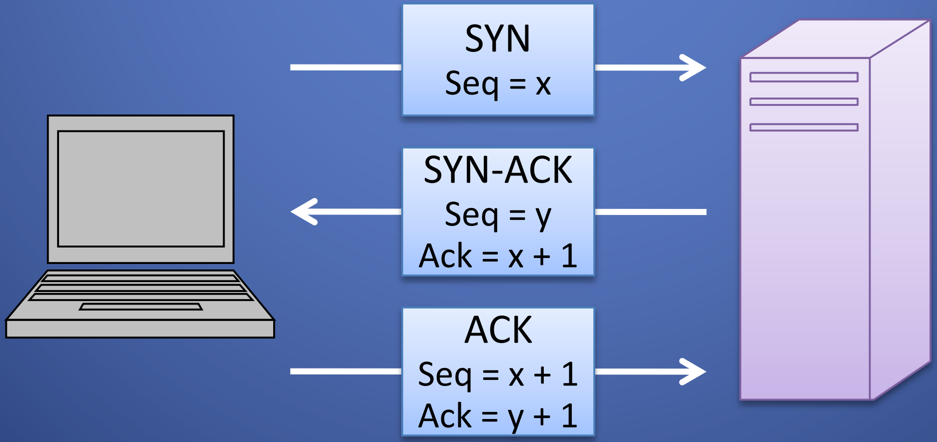
- Method
  - Random injection of information into packet header
  - Changes seldom used bits (use e.g. 16-bit fragmentation ID field)
  - Forward routing information to victim
  - Redundancy to survive packet losses
- Benefits
  - No additional traffic
  - No router storage
  - No packet size increase

Transport Layer Attacks

TCP

Establishing TCP Connections

- TCP connections are established through a three way handshake.
- The server generally has a passive listener, waiting for a connection request
- The client requests a connection by sending out a SYN packet
- The server responds by sending a SYN/ACK packet, indicating an acknowledgment for the connection
- The client responds by sending an ACK to the server thus establishing connection



SYN Flood

- Typically DOS attack, though can be combined with other attack such as TCP hijacking
- Rely on sending TCP connection requests faster than the server can process them
- Attacker creates a large number of packets with spoofed source addresses and setting the SYN flag on these
- The server responds with a SYN/ACK for which it never gets a response (waits for about 3 minutes each)
- Eventually the server stops accepting connection requests, thus triggering a denial of service.
- Can be solved in multiple ways
- One of the common way to do this is to use SYN cookies

TCP SYN Cookies

- Server sends specially crafted SYN/ACK segments back to client, without creating data structures and preparing TCP connection
  - Encode information in the TCP sequence number
    - Time stamp (5 bits), MSS value (3 bits), MAC (24-bit message authentication code)
  - Check the response from client
    - Make sure the received sequence number make sense
  - If OK, Initiate TCP session

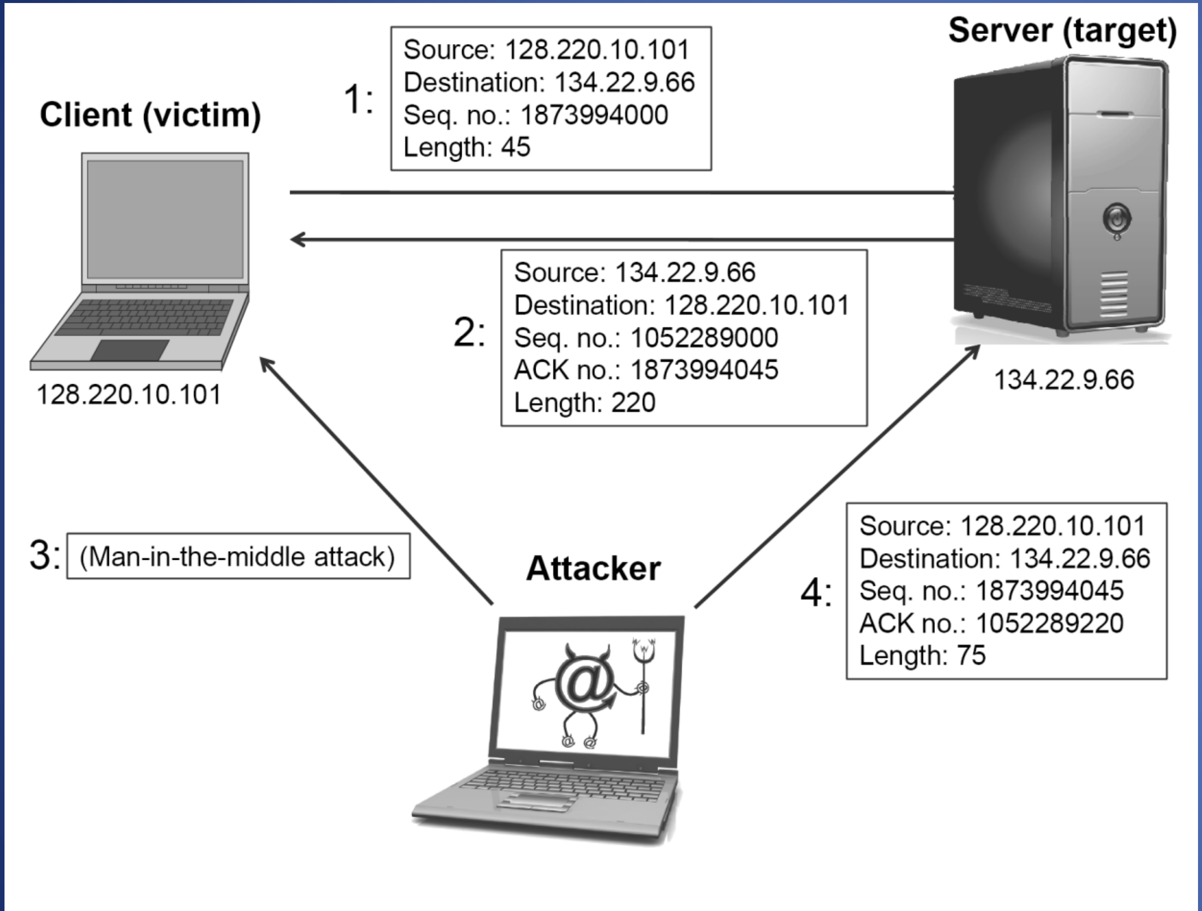
TCP Sequence Prediction (blind injection)

1. Attacker launches denial-of-service attack against client victim
2. Attacker sends a TCP SYN to server to get ISN from it
3. Attacker sends TCP SYN to server, spoofing source IP address to be that of the client victim
4. After waiting short time for server to send reply to client (not visible to attacker, not acted upon by client due to DOS attack), attacker sends ACK packet with predicted expected sequence number, spoofing the victim’s IP address
5. Attacker can now send requests to server as if he/she is the client victim

Session Hijacking

- Also commonly known as TCP Session Hijacking
- A security attack over the same subnet as the target server and/or client in attempt to take control of a TCP session
- Use packet sniffing to see the sequence numbers when client-server connection is established
- Inject a packet with a well-chosen sequence number to the server using a spoofed source IP address
- Can be performed in combination with ARP spoofing to let the attacker also intercept messages from both sides
- Countermeasures: use IPsec to encrypt communication

TCP Session Hijacking Attack



1: Source: 128.220.10.101
Destination: 134.22.9.66
Seq. no.: 1873994000
Length: 45

2: Source: 134.22.9.66
Destination: 128.220.10.101
Seq. no.: 1052289000
ACK no.: 1873994045
Length: 220

3: (Man-in-the-middle attack)

4: Source: 128.220.10.101
Destination: 134.22.9.66
Seq. no.: 1873994045
ACK no.: 1052289220
Length: 75

Figure 5.18: A TCP session hijacking attack.

Problem Solving

Network Security I, C-11

Describe how to configure a NAT router to prevent packets with spoofed IP addresses from exiting a private network.

Network Security I, C-14

Johnny just set up a TCP connection with a web server in Chicago, Illinois, claiming he is coming in with a source IP address that clearly belongs to a network in Copenhagen, Denmark. In examining the session logs, you notice that he was able to complete the three-way handshake for this connection in 10 milliseconds. How can you use this information to prove Johnny is lying?

Network Security I, C-6

Most modern TCP implementations use pseudo-random number generators (PRNG) to determine starting sequence numbers for TCP sessions. With such generators, it is difficult to compute the *i*th number generated, given only the (*i* − 1)st number generated. Explain what network security risks are created if an attacker is able to break such a PRNG so that he can in fact easily compute the *i*th number generated, given only the (*i* − 1)st number generated.