CISC 3325 – INFORMATION SECURITY

Network Attacks

Rise of the Hackers

- Rise of the Hackers

NETWORK ATTACKS

DOMAIN NAME SERVER (DNS)

- A DNS server is used to resolve a particular domain **to its IP equivalent**
  - Takes time since once a new website request is made,
    - Client asks the resolver
    - Resolver asks the root server for information.
  - Client must wait to receive a response.

DOMAIN NAME SERVER (DNS) Cache

- To save time, DNS cache is created
  - Temporary storage of information about previous DNS lookups on a machine's OS or web browser
  - Keeping a local copy of a DNS lookup allows OS or browser to quickly retrieve it
    - thus a website's URL can be resolved to its corresponding IP much more efficiently

Domain Name Service (DNS) Cache

- A temporary database, maintained by a computer's operating system
- contains records of all the recent visits to websites and other internet domains.
  - A DNS cache is just a memory of recent DNS lookups
    - computer uses when trying to figure out how to load a website

DNS Cache

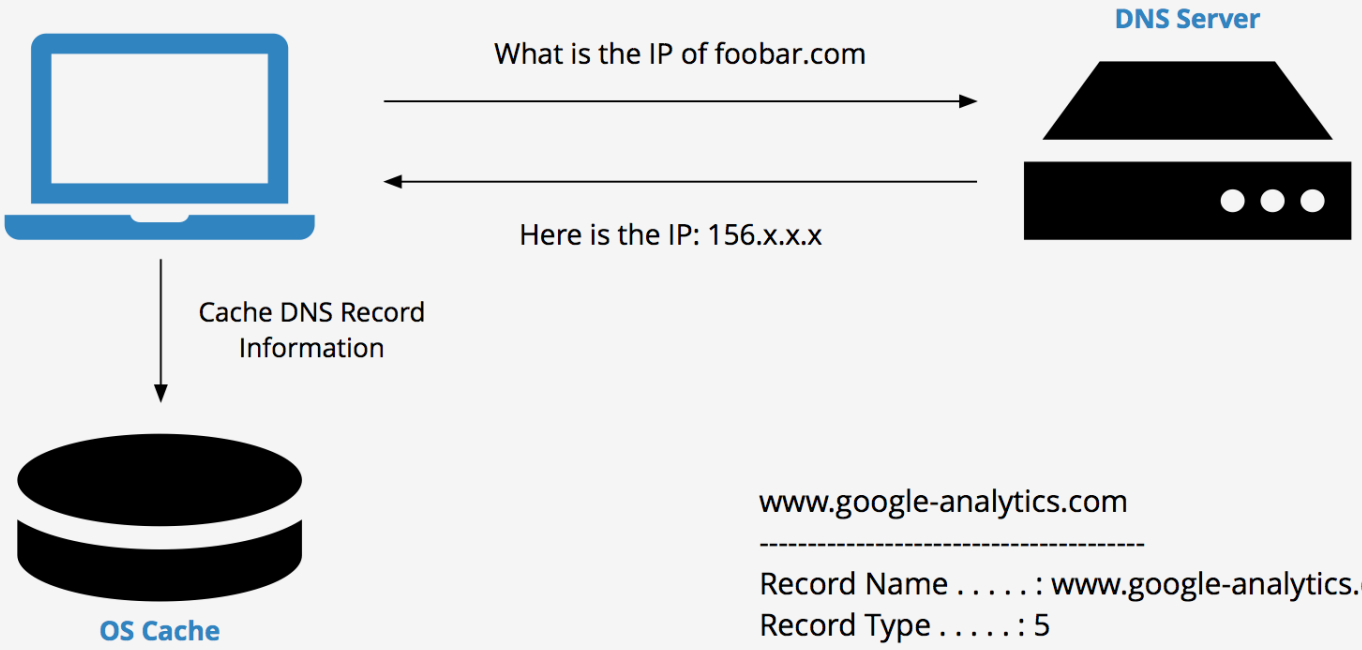
- DNS maintains an index of all public websites and their corresponding IP addresses
  - Analogous to a phone book
    - With a phone book, we can find everyone's phone number
      - Phones need number to communicate
    - Similarly, DNS is used to find website's IP address
      - Needed so network equipment can communicate with websites
      - Occurs when you ask your web browser to load a website.

DNS Cache Example

- You type in a URL like google.com
- your web browser asks your router for the IP address
- The router has a DNS server address stored
  - it asks the DNS server for the IP address of that hostname
- The DNS server finds the IP address that belongs to google.com
  - Enables your browser to load the appropriate page

DNS Cache Example

- Occurs every time user asks to view a website
  - the web browser initiates a request out to the internet
  - site's name is converted into an IP address
    - Only then request can be completed



DNS Cache

www.google-analytics.com

Record Name . . . . . : www.google-analytics.com
Record Type . . . . . : 5
Time To Live . . . . : 104
Data Length . . . . . : 4
Section . . . . . : Answer
CNAME Record . . . . : www-google-analytics.l.google.com

DNS Cache Poisoning Attack

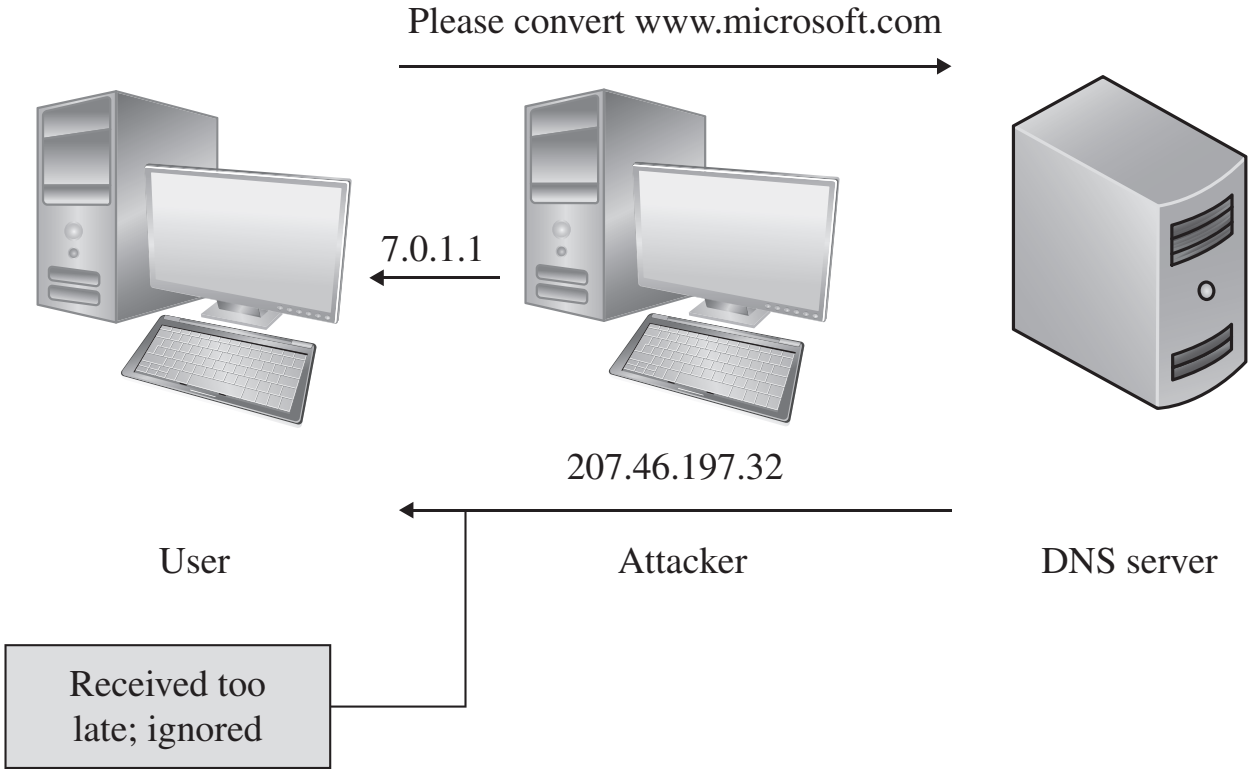
- DNS works by getting information about IP's and names
- **DNS cache poisoning:** a pharming attack directed at changing a host's DNS cache
  - to create a falsified domain-name/IP-address association
  - Feeds you fake DNS addresses when you try to access a legitimate website

DNS Cache Poisoning Attack

- Can spread to other networks:
  - If other servers can get their information from a compromised server
    - Serve this information to other hosts

DoS Attack: DNS Spoofing

- The attacker acts as the DNS server in order to redirect the user to malicious sites



DNS Cache poisoning attacks

- DNS cache poisoning attacks

DNS Cache Poisoning Attack

- Occurred in Brazil, 2018
- Attackers installed fake DNS addresses for popular websites
  - Google, Hotmail, etc.
- Victims were sent to a server that the attacker controlled
  - Installed a malicious applet on their system
    - Banking trojan designed to steal banking information

How Hackers Hijacked a Bank's Entire Online Operation

https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/

IoT Hackers Trick Brazilian Bank Customers into Providing Sensitive Information

August 10, 2018 — by Pascal Geenens — 85

Radware Threat Research Center has identified a hijacking campaign aimed at Brazilian Bank customers through their IoT devices, attempting to gain their bank credentials.

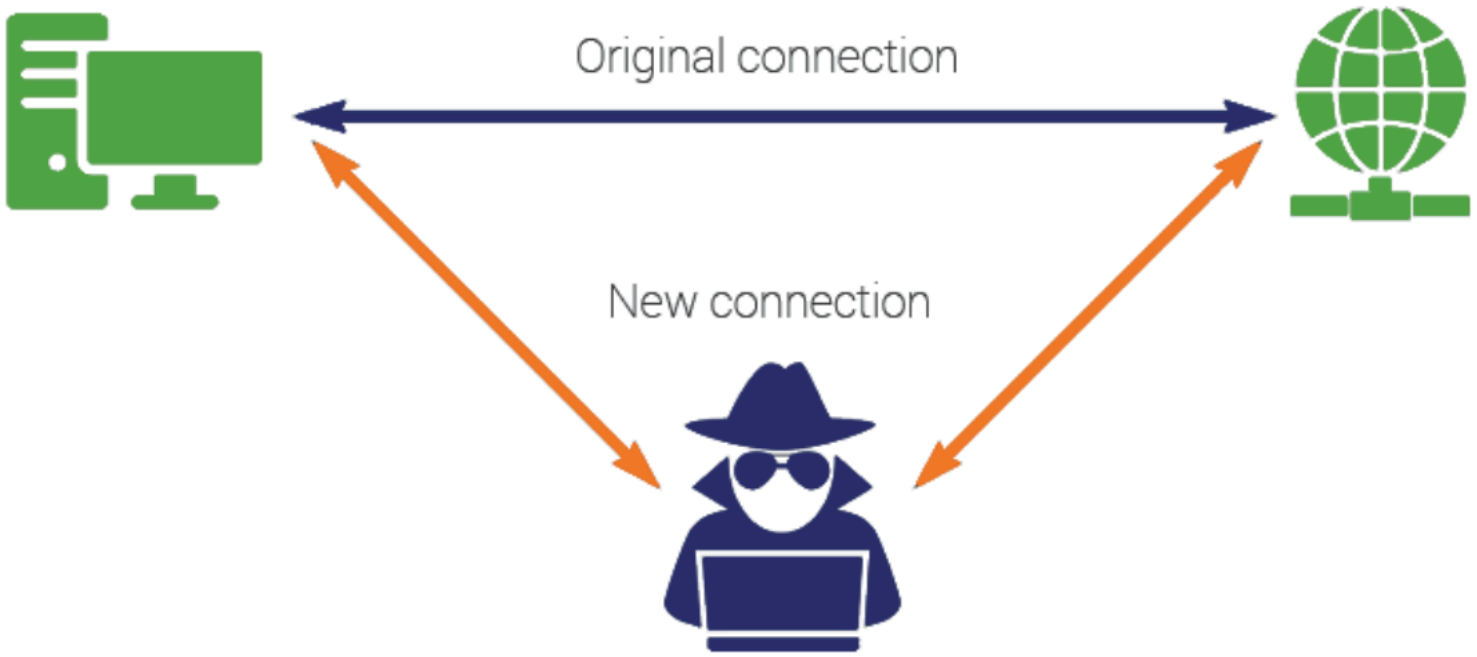
The research center has been tracking malicious activity targeting DLink DSL modem routers in Brazil since June 8th. Through known old exploits dating from 2015, a malicious agent is attempting to modify the DNS server settings in the routers of Brazilian residents, redirecting all their DNS requests through a malicious DNS server. The malicious DNS server is hijacking requests for the hostname of Banco de Brasil (www.bb.com.br) and redirecting to a **fake**, **cloned** website hosted on the same malicious DNS server, which has no connection whatsoever to the legitimate Banco de Brasil website.

https://blog.radware.com/security/2018/08/iot-hackers-trick-brazilian-bank-customers/

Man-In-The-Middle Attack

- Attacker monitors information between two hosts
  - Potentially modifies it in transit

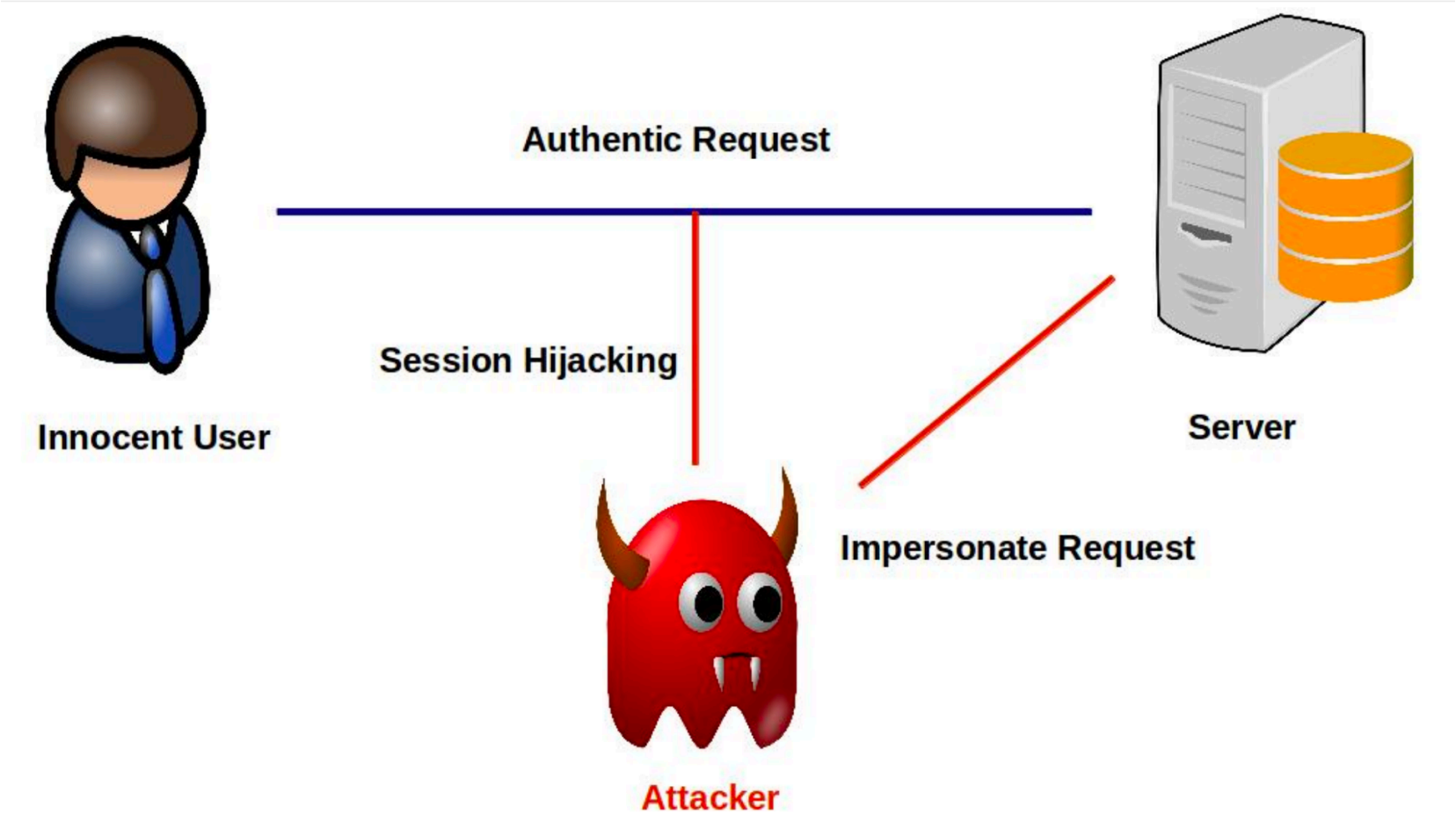
Man-In-The-Middle Attack



https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

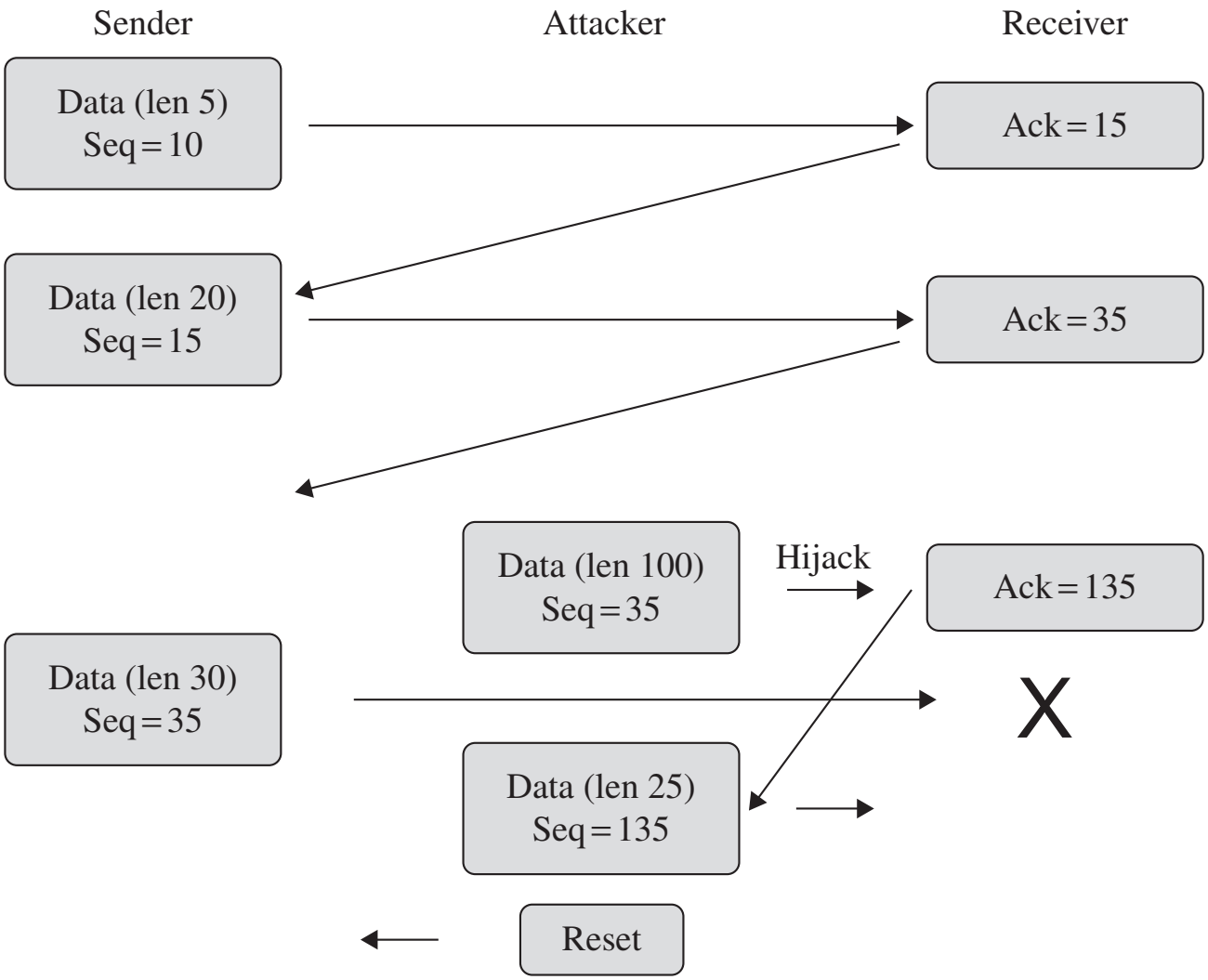
Session Hijacking/Cookies Hijacking

- User already authenticated itself to the website
  - Generated a session token that enables access to that website
  - The hijacker steals the token and impersonates the original user on that website



https://hakin9.org/how-does-one-defend-against-session-hijacking/

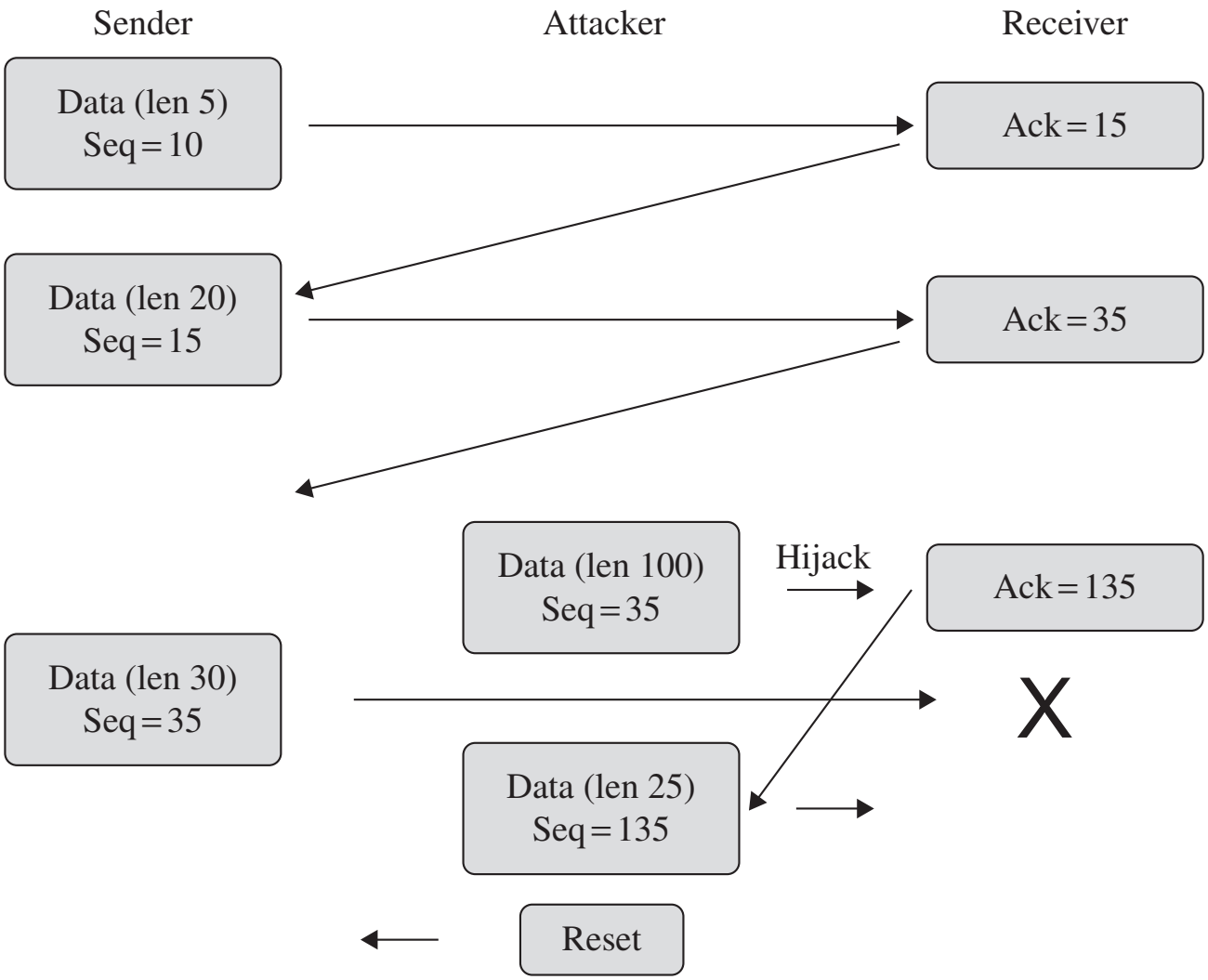
Session Hijacking Example



Session Hijacking Example

- An attacker is able to:
  - synchronize with a receiver
  - break synchronization with the sender
  - reset sender's connection.
- The attacker continues the TCP session while the sender thinks the connection just broke off

Session Hijacking



Session Hijacking

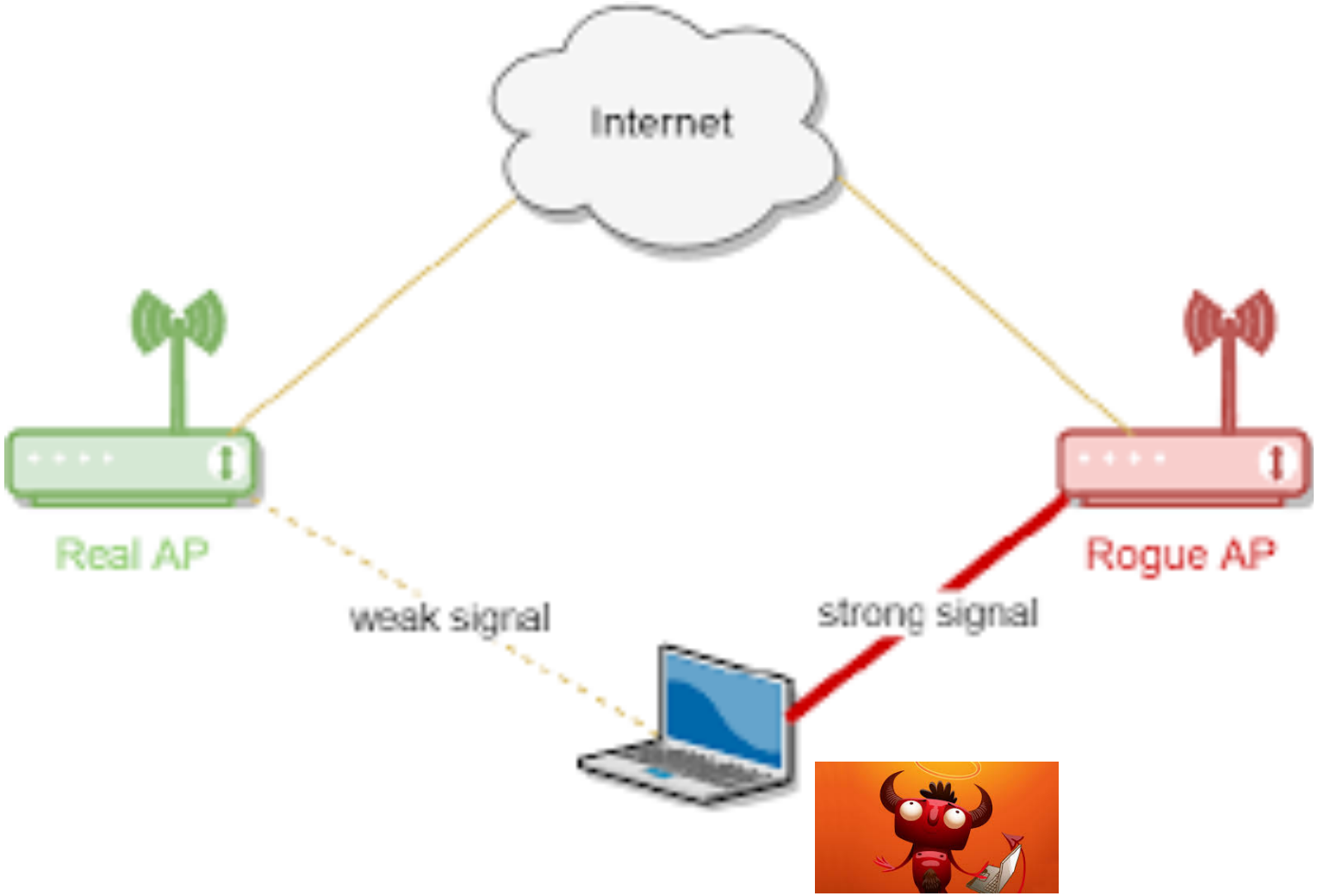
- How is the token compromised?
  - Predictable session token
  - Session Sniffing
  - Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc)
  - Etc.

Network Attack: Rogue Access Point

- Another form of man-in-the-middle attack
- A wireless access point is installed on the network
  - Without network administrator's knowledge or authorization
  - Added by an employee
    - Or a malicious attacker

Rogue Access Point

- Example:
  - In a corporate network, a user may plug a router into a corporate network
    - Creating a simple wireless network
      - With poor security
  - An attacker may login into this wireless network
    - Instead of having to attack the corporate network
      - Which may have more security measures
    - Install an access point
      - May eavesdrop from a distance



https://www.scmagazine.com/home/security-news/sc-security-ops-center/deception-pointe/

Rogue Access Point

- How to detect a rogue access point?
  - Organizations can install wireless prevention systems
    - Monitor radio spectrum through authorized access points
    - For each access point detected, need to check
      - Is it in the managed access point list?
      - Is it connected to the secure network?
    - If not, needs to be disabled

Evil Twin Attack

- Connect to a network identical to yours
  - Controlled by the attacker
- equivalent of the phishing scam
  - For wireless LAN
- Can be used to Steal the passwords of unsuspecting users by either:
  - monitoring their connections
  - Phishing - setting up a fraudulent web site and luring people there

Evil Twin Attack Steps

- Attacker scans the air for the target access point information
  - SSID name, Channel number, MAC Address.
- Attacker uses information to create an access point
  - with same characteristics, hence Evil Twin Attack
- Clients on the legitimate AP are repeatedly disconnected
  - forcing them to connect to the fraudulent access point

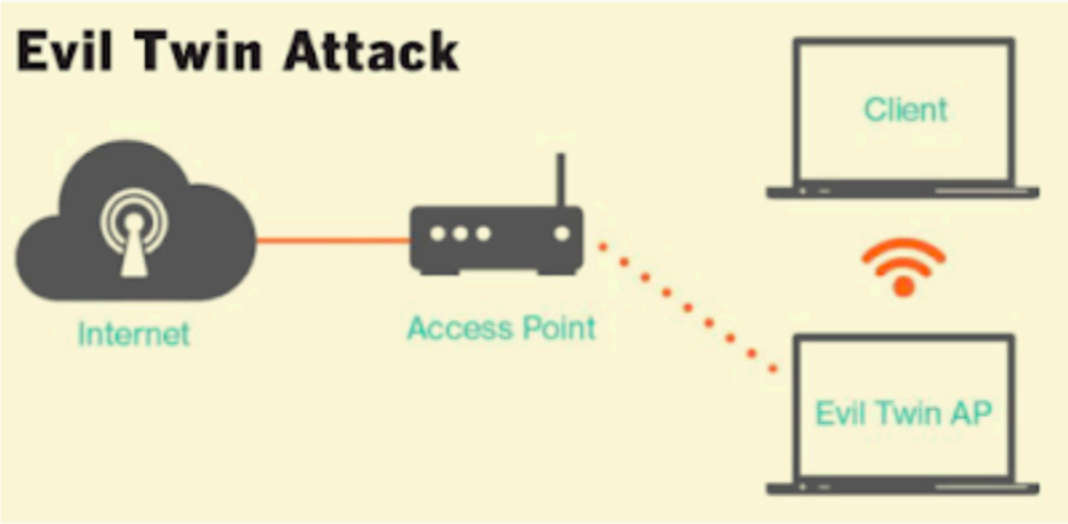
Evil Twin Attack Steps

- Client unknowingly connected to the fake access point
  - May start browsing the Internet
- Client opens up a browser window and sees a web administrator warning
  - "**Enter WPA password to download and upgrade the router firmware**"

Evil Twin Attack Steps

- Client enters the password
  - Password stored in the MySQL database of the attacker machine.
  - Client redirected to a loading page
    - Which looks like authentic page
  - Evil Twin attack automated
    - Making it feasible to attack multiple clients
- An attacker can also simply change the webpage
  - Creating a DOS attack

Evil Twin Attack



Denial of Service (DoS)

- An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server
- A website has capacity to serve a limited number of users
  - Usually millions
  - All hosting has bottlenecks

Denial of Service (DoS)

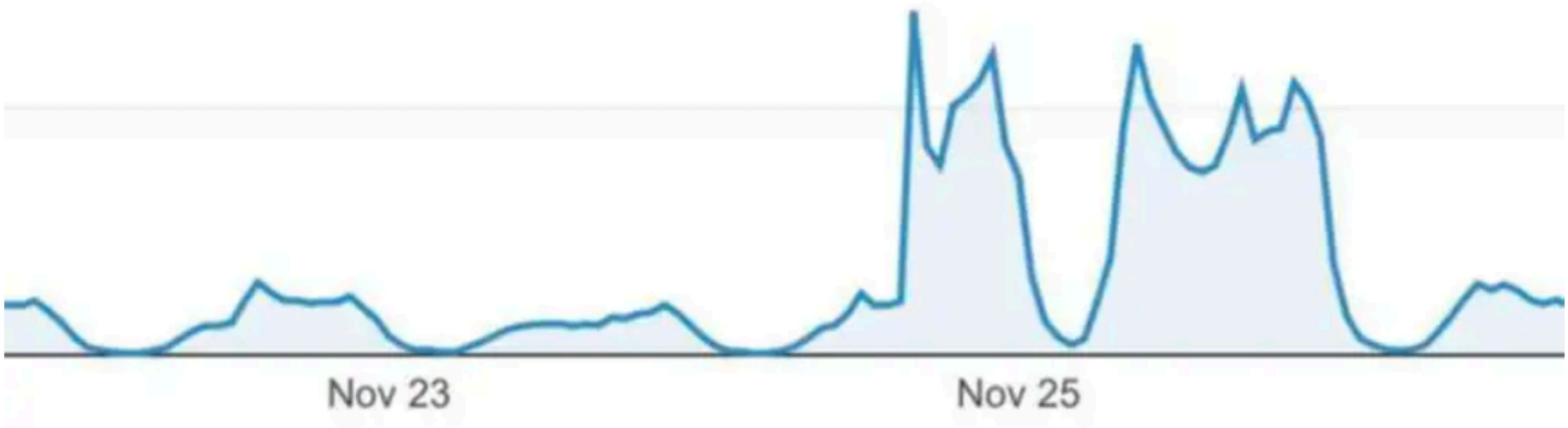
- DoS attacks are attempts to defeat a system's availability
- Volumetric attacks
- Application-based attacks
- May result in disabled communications
- Hardware or software failure

PERFORMANCE

How to estimate how many website visitors your hosting can deal with

Erlend Eide
CEO, Servebolt

Published: May 17, 2018 12:00 am
Last edited: April 20, 2019 1:44 pm

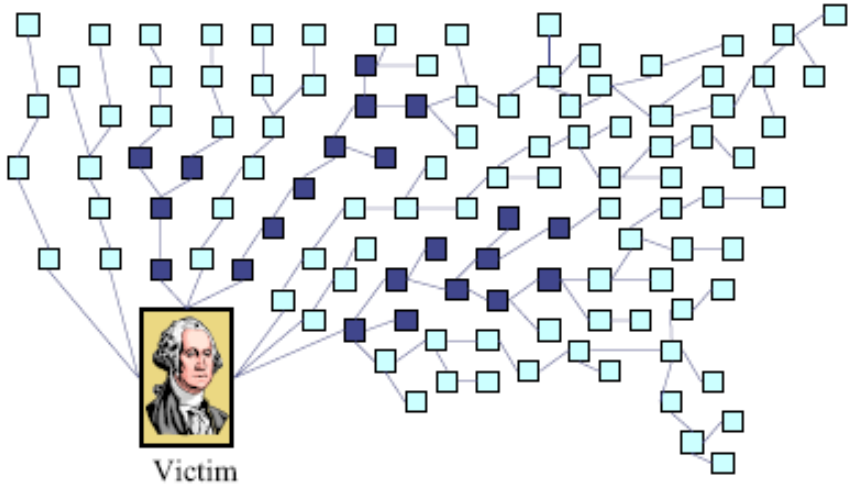


https://servebolt.com/articles/calculate-how-many-simultaneous-website-visitors/

Denial of Service (DOS) 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.



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DOS Attacks - Examples

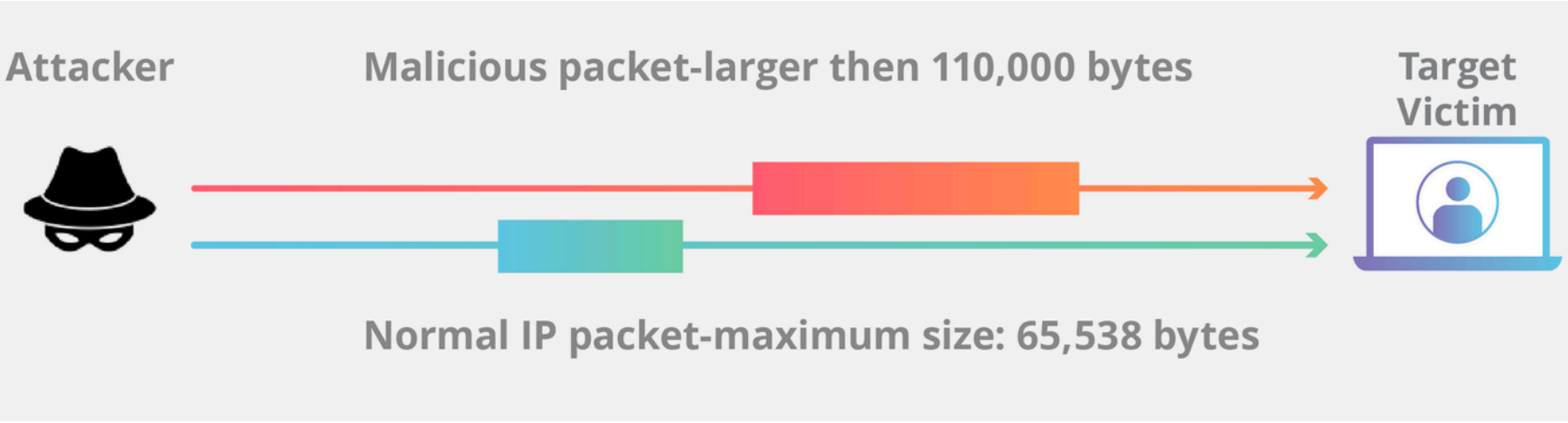
- Ping of death (PoD) attack
- SYN(PING) flood
- Smurf Attack
- Teardrop attack

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Ping of Death Attack

- Attacker sends a large ping
  - Larger than the protocol made to handle
- Results in buffer overflow
- Results from attack:
  - System may crash
    - Or execute malicious code

Ping of Death Attack



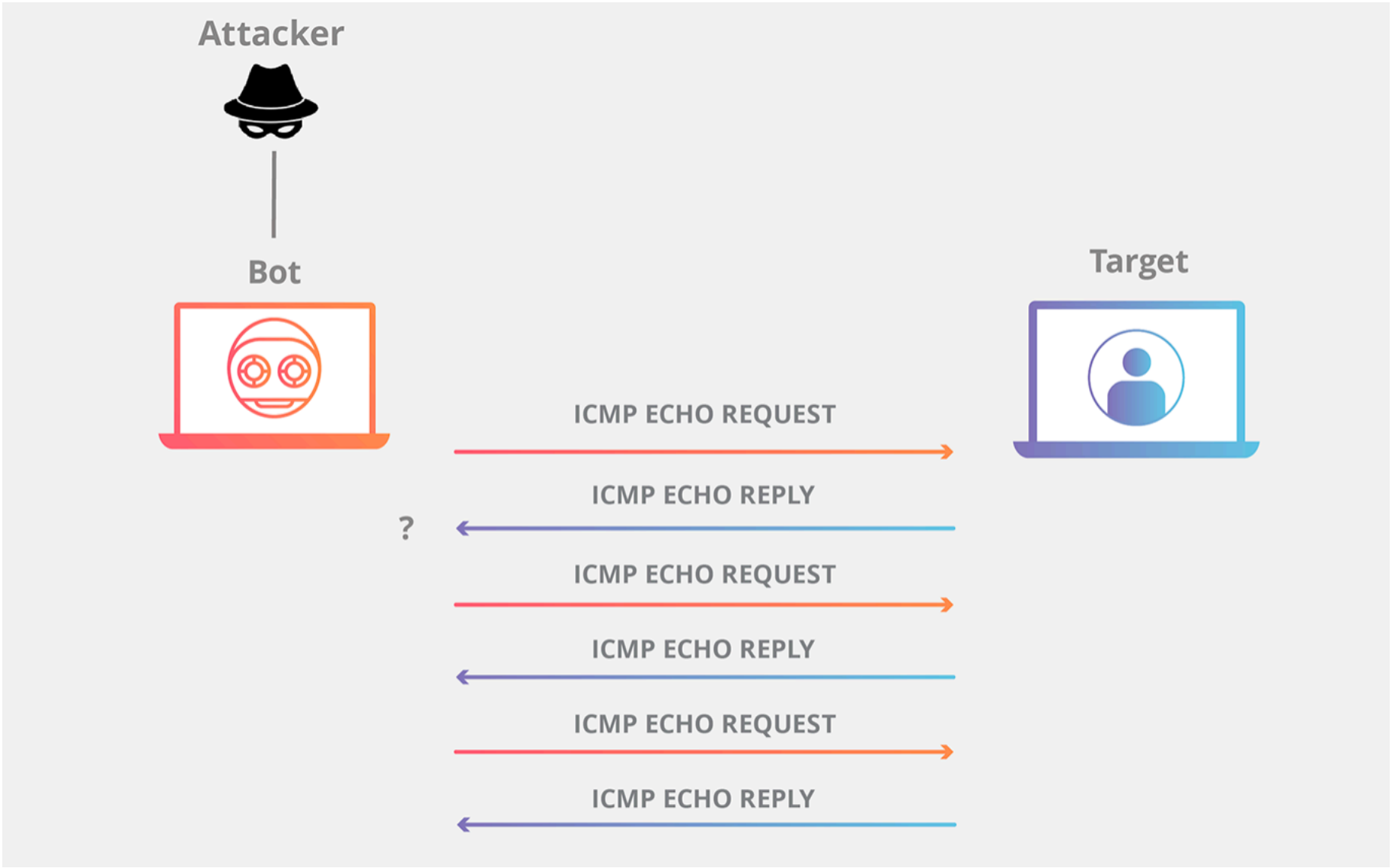
https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

Internet Control Message Protocol (ICMP)

- Networking protocol
- Used by network devices, including routers
- Sends error messages or operational information
  - Indicating success or failure when communicating with another IP address
- Messages include ICMP “echo request”
  - Receiver generates an ICMP "echo reply" in response

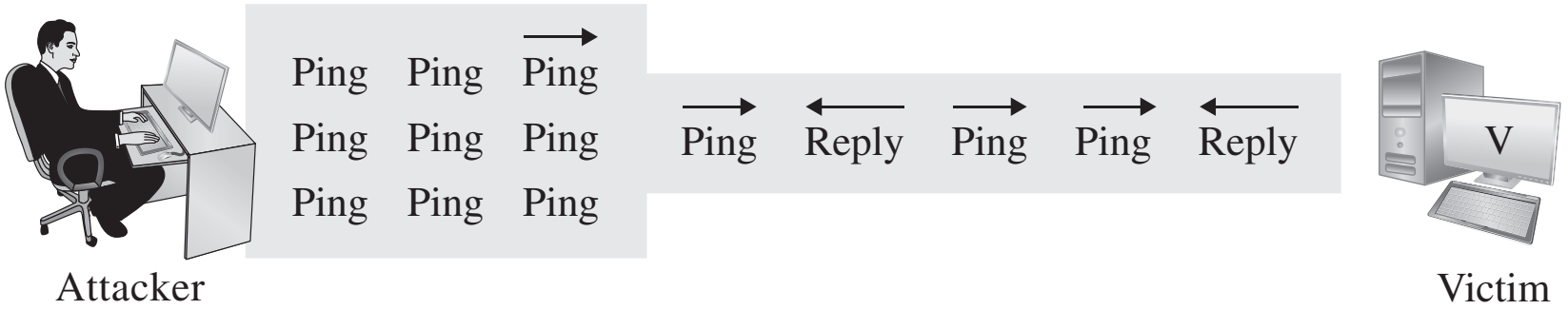
PING (ICMP) Flood Attack

- Send ICMP-echo request ping messages
- Expects ICMP echo reply
- If frequency is too high, computer can not keep up with this

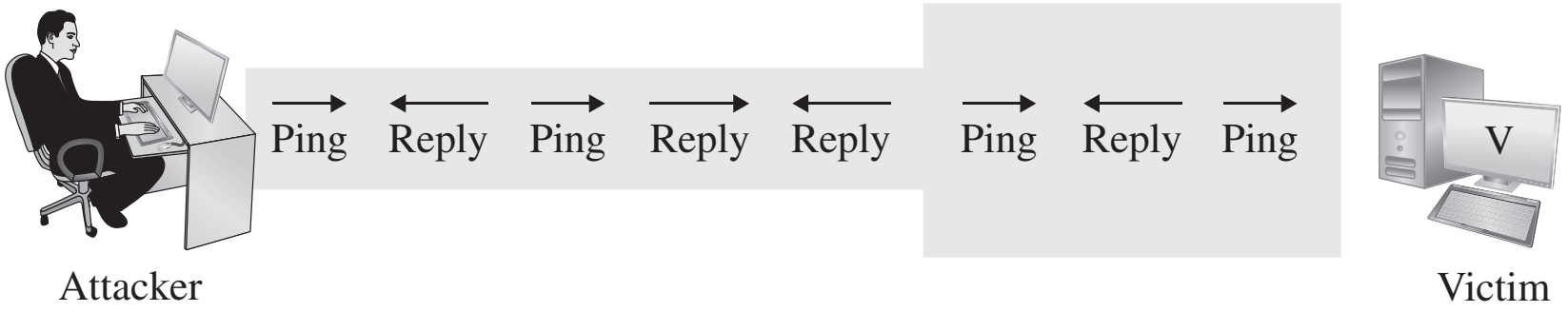


https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/

DoS Attack: Ping Flood



(a) Attacker has greater bandwidth



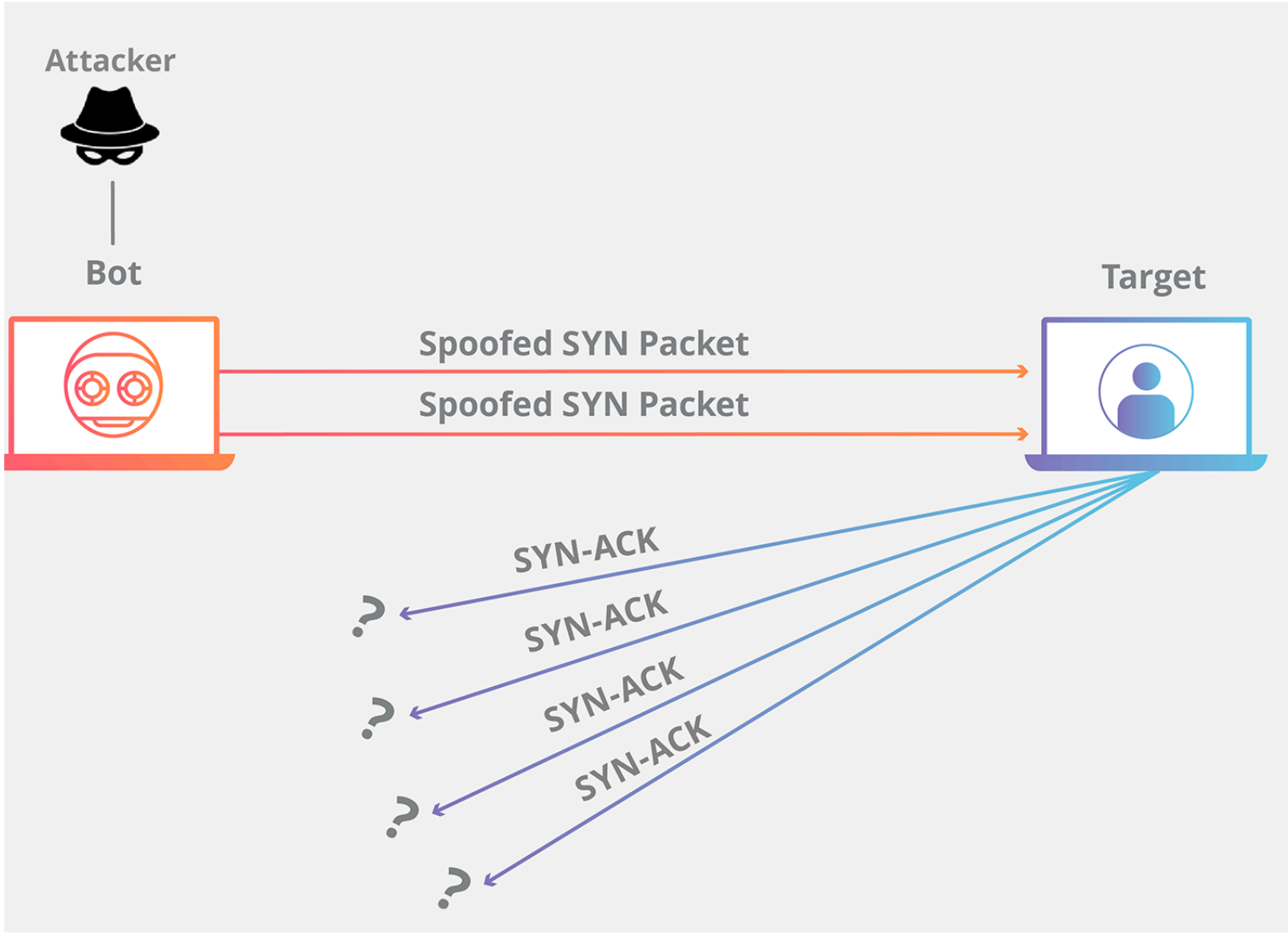
(b) Victim has greater bandwidth

SYN Flood

- 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)
- Server stays open
  - Takes up a lot of server resources
  - Other users will not be able to connect to server
- Eventually the server stops accepting connection requests, thus triggering a denial of service.

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



https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

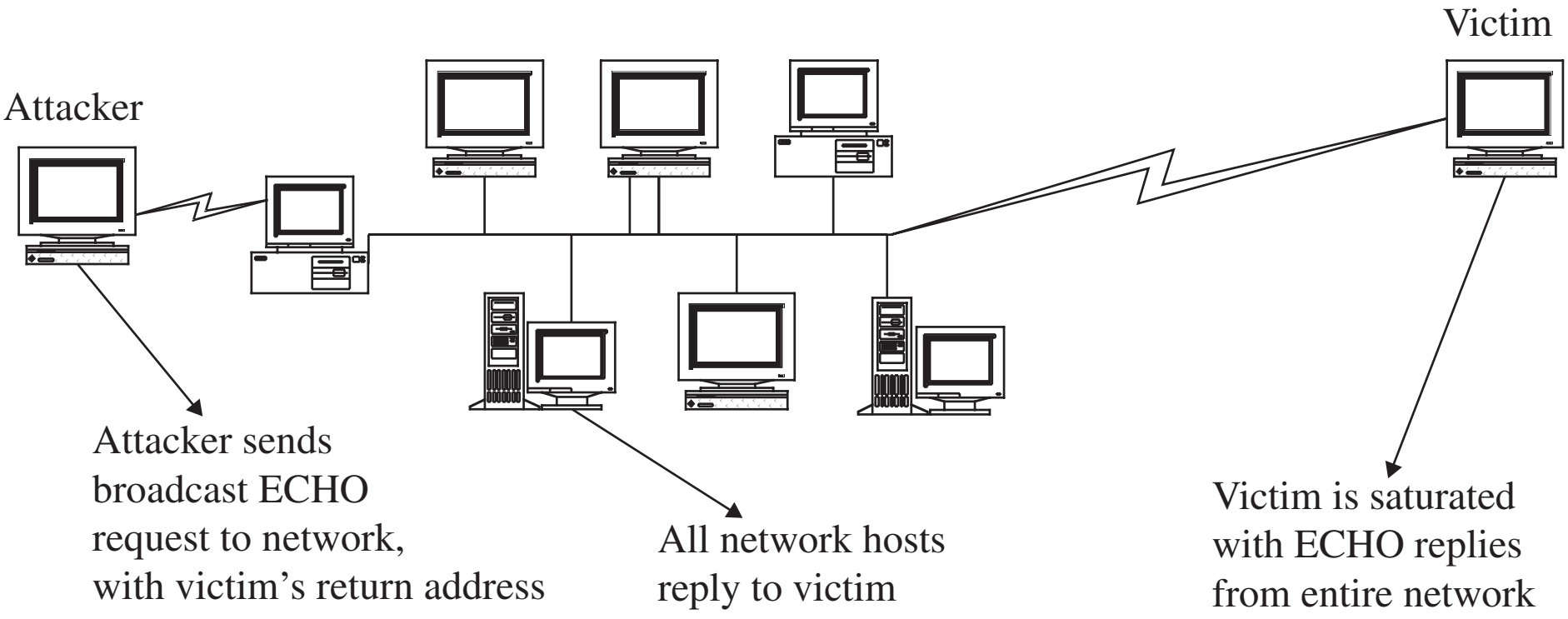
Flood Guard

- Flood guards serve as preventive control against denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Flood guards are available either as standalone devices or as firewall components
- Capable of monitoring network traffic to identify DoS attacks in progress
  - generated through packet flooding.

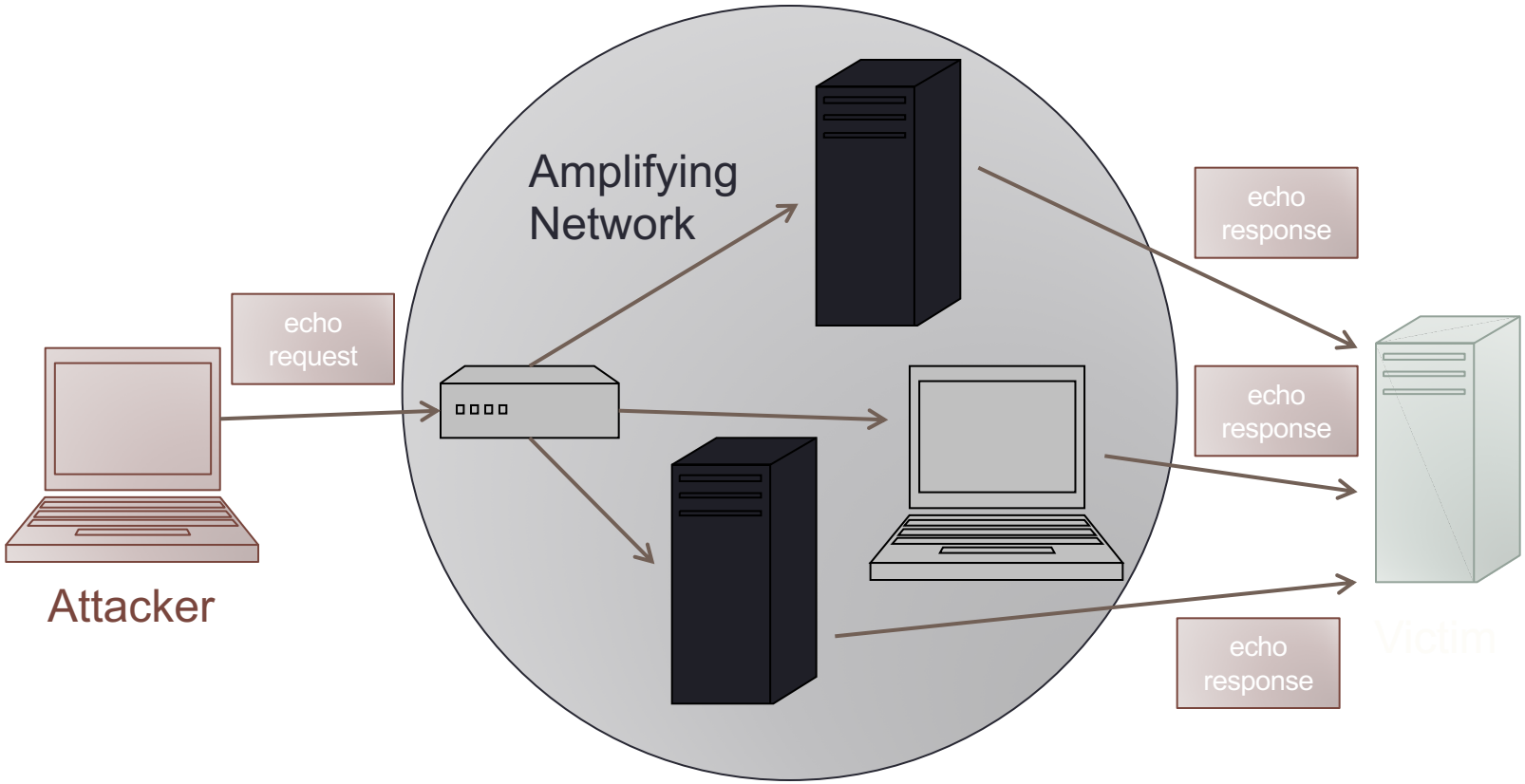
Smurf Attack

- Ping a broadcast address using a spoofed source address
- A distributed denial-of-service attack
  - Multiple systems flood the resources of a targeted system
- Most devices on a network will respond to this by sending a reply to the source IP address
- victim's computer will be flooded with traffic
  - If the number of machines on the network that respond to these packets is very large

DoS Attack: Smurf Attack

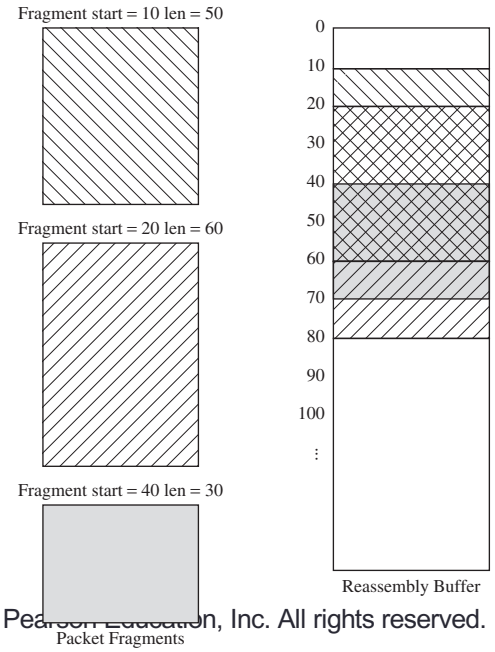


Smurf Attack



DoS Attack: Teardrop Attack

- The attacker sends packets that cannot possibly be reassembled (conflicting reassembly instructions)
- In extreme cases, this can cause the entire OS to lock up.

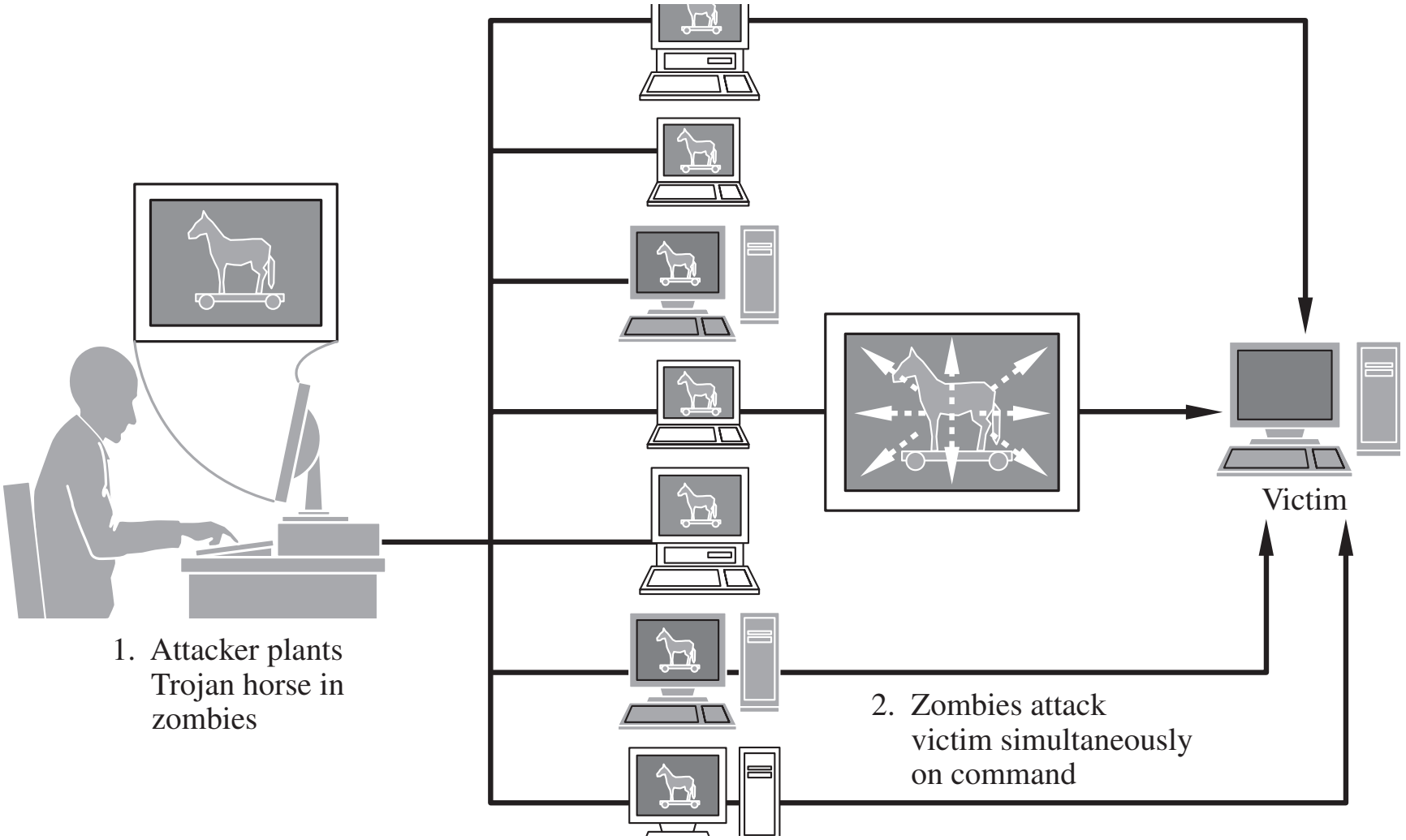


Distributed Denial of Service (DDoS)

- Conscript an army of compromised machines
  - to attack a victim
- Choose a victim
- Have the whole army unleash a DoS attack at once

- DDoS much more effective than traditional DoS attacks
  - employing a multiplied version of the same methods.

Distributed Denial of Service (DDoS)



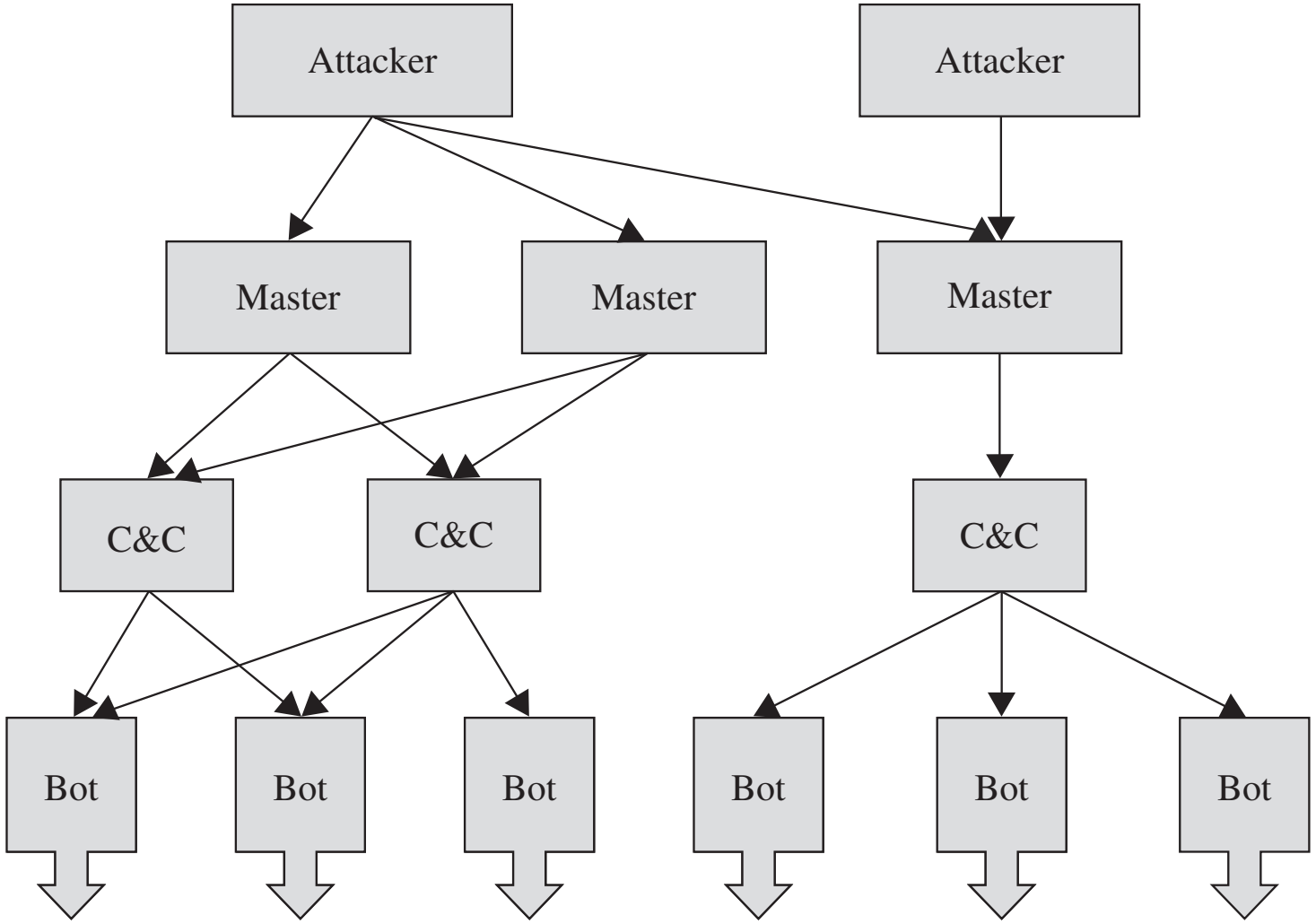
Botnets

- Botnets are networks of machines running malicious code under remote control.
- They often go undetected because they do little harm to the machines they run on.
- Botnets are often used to execute DDoS attacks.

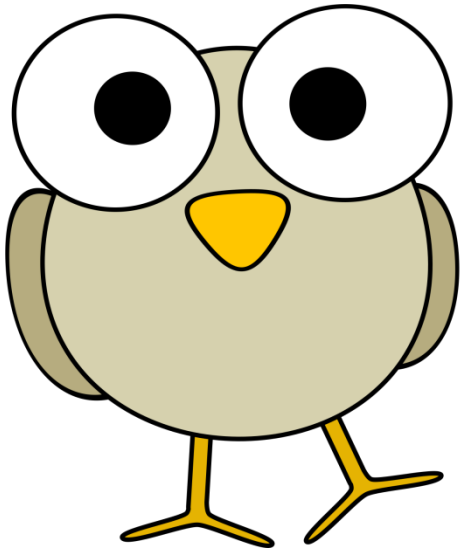
Botnets

- Botnet command and control (C&C):
  - The attacker is separated from the bots by multiple layers
    - making the attacker difficult to trace.
  - Multiple redundant systems are built in
    - if one master or C&C node is taken down, the bots can continue to connect to the botnet.

Botnets



- Questions?



COMPUTER SECURITY QUIZ

Question 1

- Increased Traffic is due to a spike in network traffic from several sources. Assuming this is malicious, what is the MOST likely explanation?
  - A. A smurf attack
  - B. A flood guard attack
  - C. A denial-of-service (DoS) attack
  - D. distributed denial-of-service (DDoS) attack

Question 1

- Increased Traffic is due to a spike in network traffic from several sources. Assuming this is malicious, what is the MOST likely explanation?
  - A. A smurf attack
  - B. A flood guard attack
  - C. A denial-of-service (DoS) attack
  - D. distributed denial-of-service (DDoS) attack

Question 1

- A distributed denial-of-service (DDoS) attack causes spikes in network traffic
  - as multiple systems attempt to connect to a server and deplete the target's resources
- A smurf attack is an attack using directed broadcasts
  - this might be a smurf attack if routers aren't blocking directed broadcasts, but it could also be another type of DDoS attack
- Flood guards protect against SYN flood attacks, and flood guards are not an attack method
- A DoS attack comes from a single system.

Question 2

- A SYN flood is an example of what type of attack?
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - D. Spoofing

Question 2

- A SYN flood is an example of what type of attack?
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - D. Spoofing

Question 3

- An attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as a user ID and password combination. This is known as:
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - D. Sniffing

Question 3

- An attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as a user ID and password combination. This is known as:
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - D. Sniffing

- Questions?