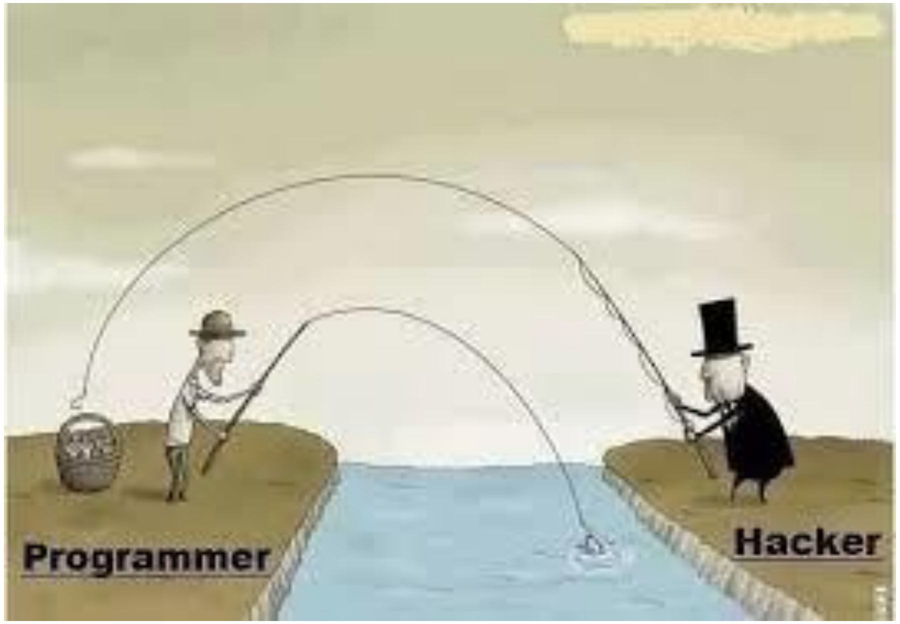
SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks



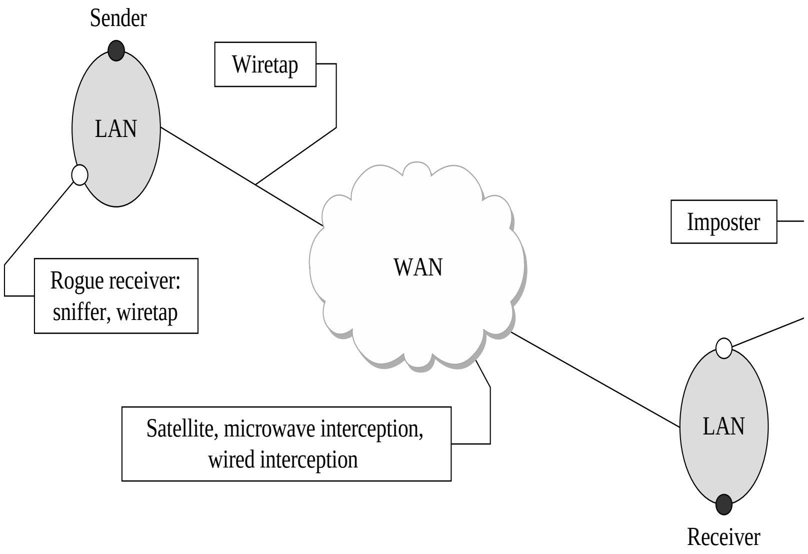
Network Transmission Media

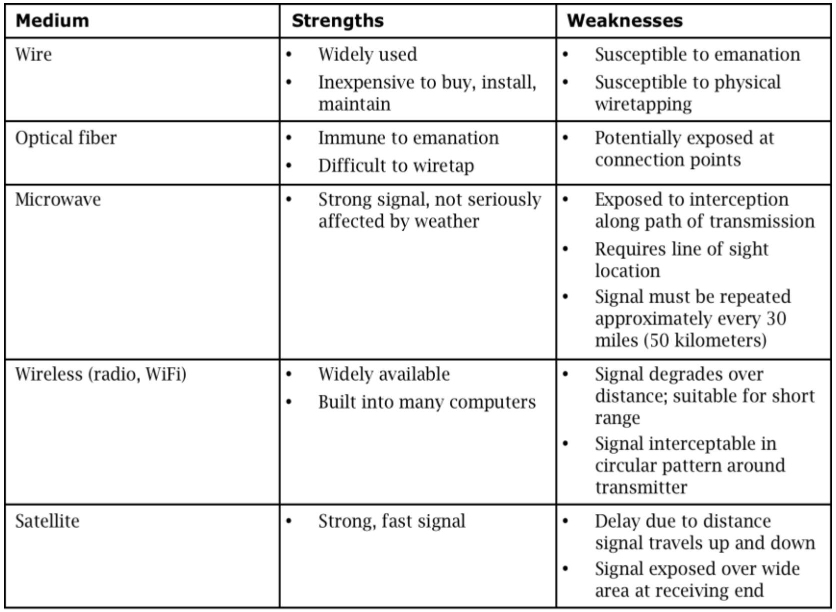
There are vulnerabilities in each of these media.

The purpose of introducing them here is to understand that they all have different physical properties, and those properties will influence their susceptibility to different kinds of attack.

- Cable
- Optical fiber
- Microwave
- WiFi
- Satellite communication

Communication Media Vulnerability

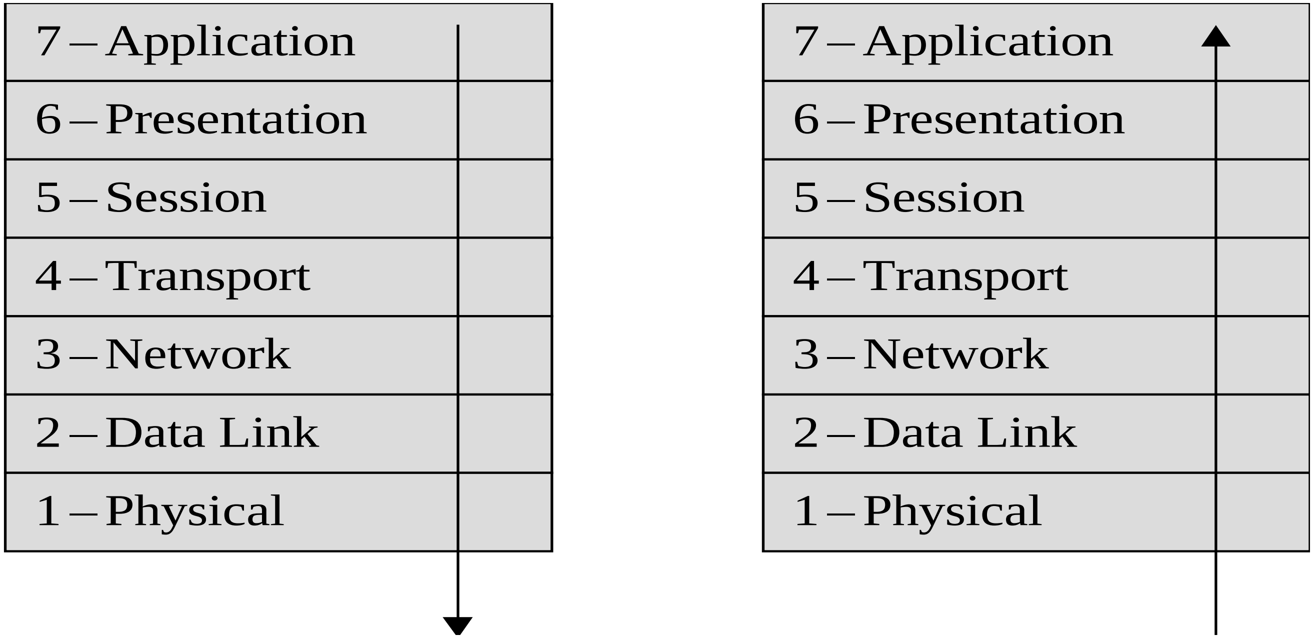

Sender
LAN
Wiretap
Rogue receiver: sniffer, wiretap
WAN
Imposter
Satellite, microwave interception, wired interception
LAN
Receiver



Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping
Optical fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong signal, not seriously affected by weather	• Exposed to interception along path of transmission • Requires line of sight location • Signal must be repeated approximately every 30 miles (50 kilometers)
Wireless (radio, WiFi)	• Widely available • Built into many computers	• Signal degrades over distance; suitable for short range • Signal interceptable in circular pattern around transmitter
Satellite	• Strong, fast signal	• Delay due to distance signal travels up and down • Signal exposed over wide area at receiving end

Different touch points where attackers can take advantage of communication media: wiretaps, sniffers and rogue receivers, interception, and impersonation.

The OSI Model



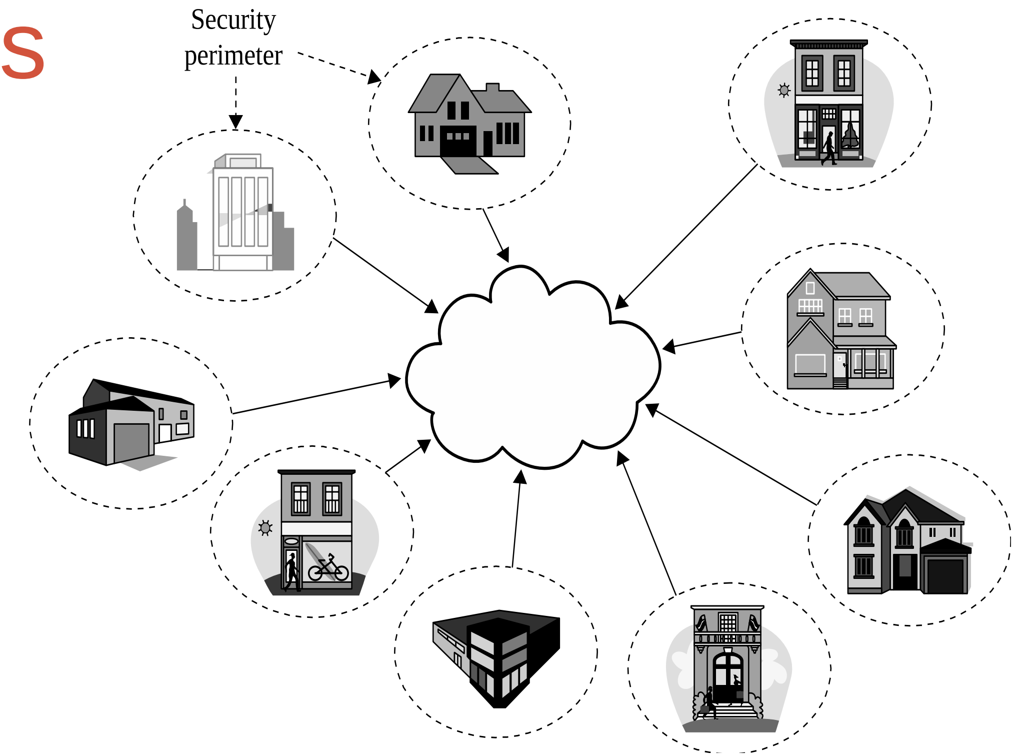
7 – Application
6 – Presentation
5 – Session
4 – Transport
3 – Network
2 – Data Link
1 – Physical

7 – Application
6 – Presentation
5 – Session
4 – Transport
3 – Network
2 – Data Link
1 – Physical

Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

Security Perimeters



- Each of these places is a security perimeter in and of itself. Within each perimeter, you largely have control of your cables, devices, and computers because of physical controls, so you do not need to worry as much about protection.

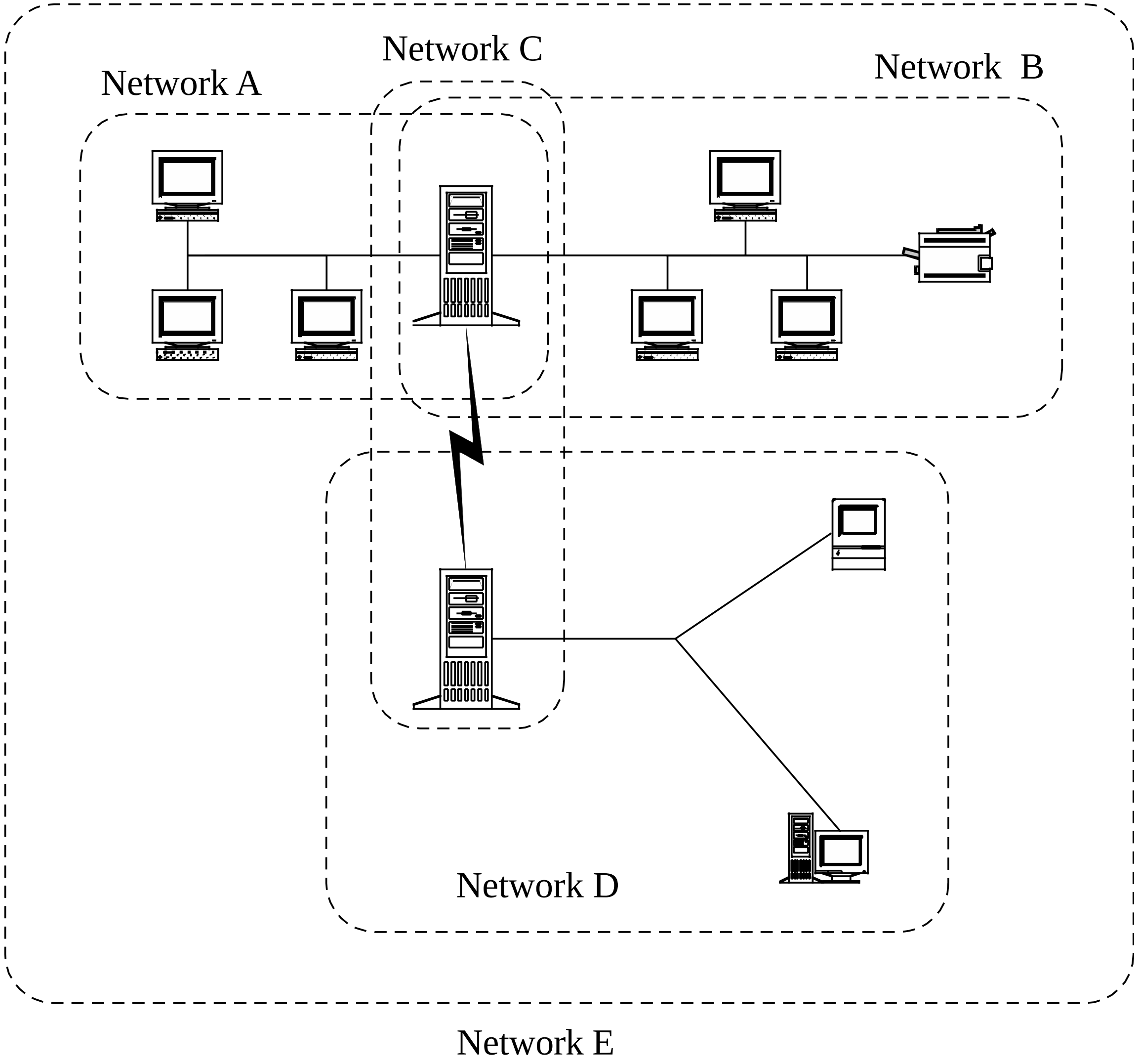
- However, to do anything useful, you have to make connections between security perimeters, which exposes you to all sort of cables, devices, and computers you can't control.

- Encryption is the most common and useful control for addressing this threat.

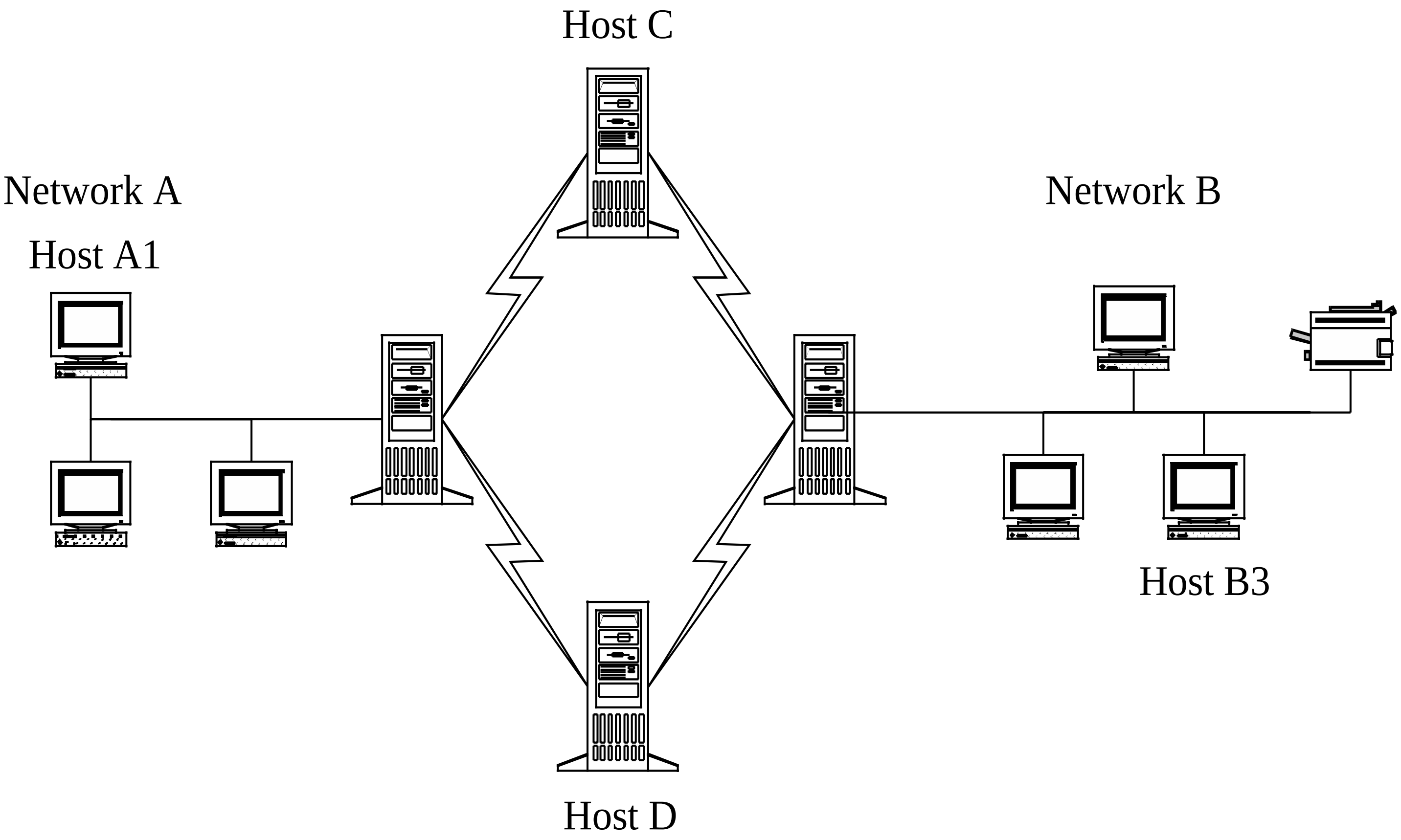
What Makes a Network Vulnerable to Interception?

- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
  - Networked systems open up potential access to more users than do single computers
- System complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter (next slide)
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path (next slide)
  - There may be many paths, including untrustworthy ones, from one host to another

Unknown Perimeter



Unknown Path



Network Perimeter

A network perimeter is the secured boundary between the private & locally managed side of a network. A network perimeter includes:

- **Border Routers:** Routers serve as the traffic signs of networks. They direct traffic into, out of, and throughout networks. The border router is the final router under the control of an organization before traffic appears on an untrusted network, such as the Internet.
- **Firewalls**: A firewall is a device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic.

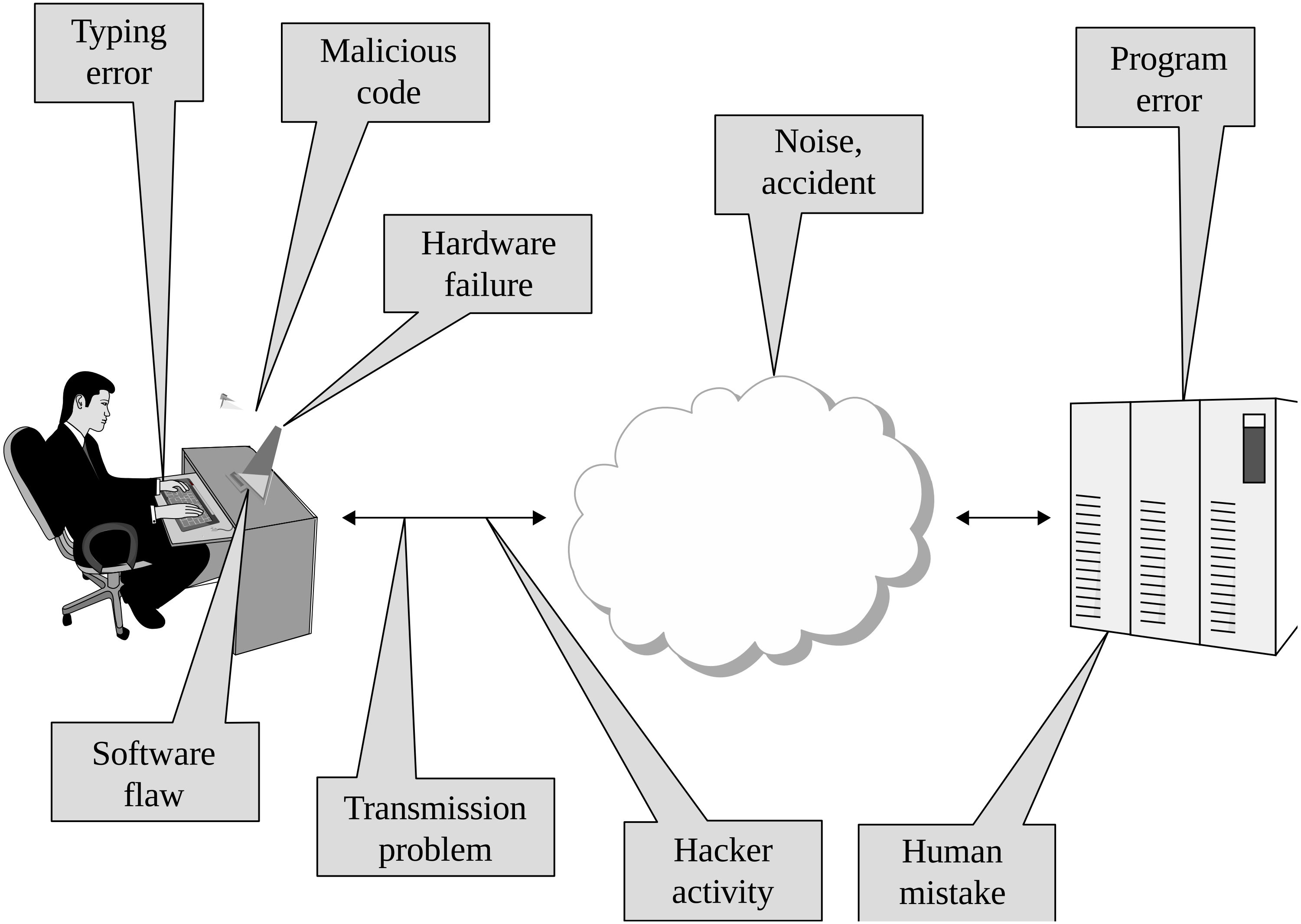
Network Perimeter

- **Intrusion Detection System (IDS):** This functions as an alarm system for your network that is used to detect and alert on suspicious activity. This system can be built from a single device or a collection of sensors placed at strategic points in a network.
- **Intrusion Prevention System (IPS):** Compared to a traditional IDS which simply notifies administrators of possible threats, an IPS can attempt to automatically defend the target without the administrator's direct intervention.

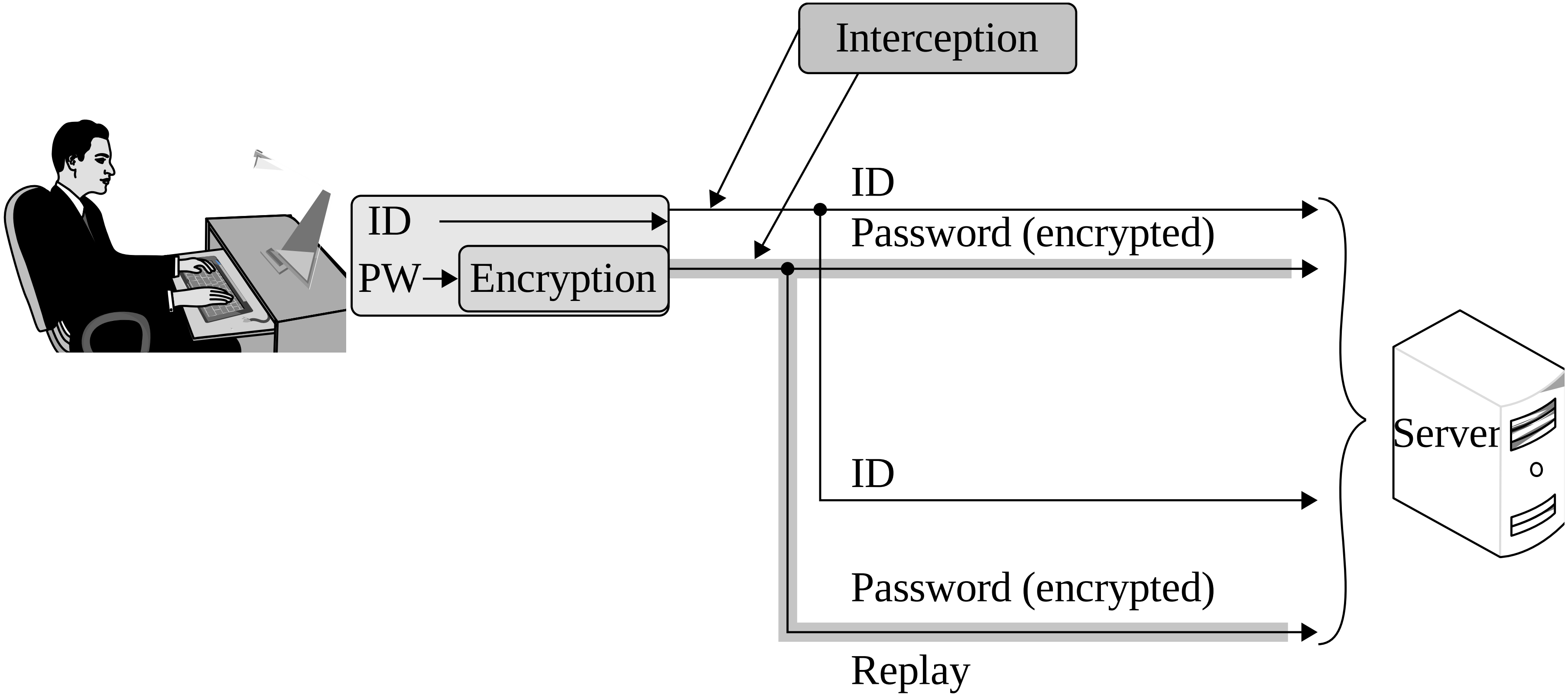
Network Perimeter

- **De-Militarized Zones / Screened Subnets:** DMZ and screened subnet refer to small networks containing public services connected directly to and offered protection by firewall or other filtering device.

Sources of Data Corruption



Simple Replay Attack



Interception

ID

PW→ Encryption

ID

Password (encrypted)

ID

Password (encrypted)

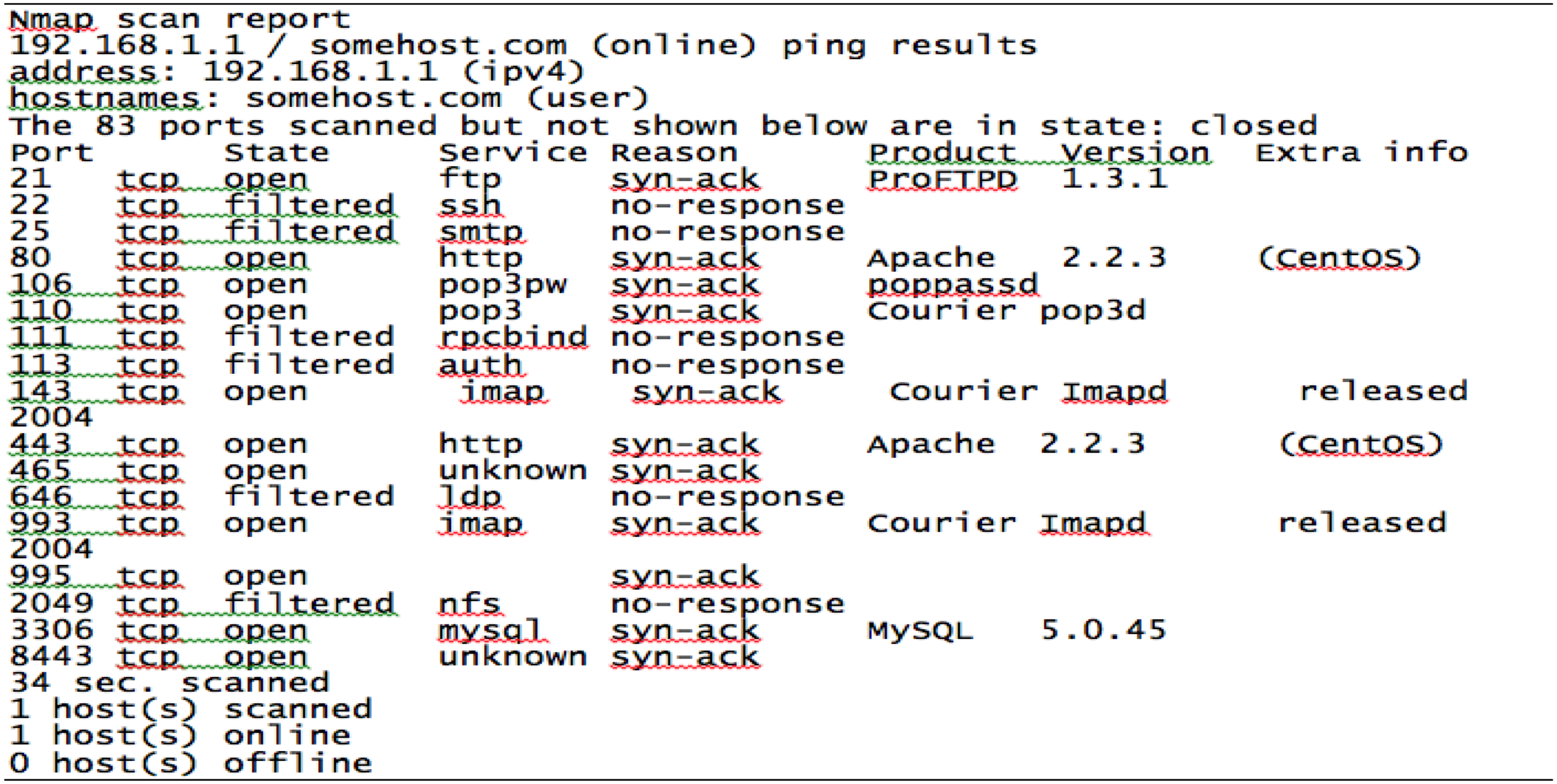
Replay

Server

Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Port Scanning



```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port      State     Service Reason      Product  Version  Extra info
21   tcp  open      ftp     syn-ack     ProFTPD  1.3.1
22   tcp  filtered  ssh     no-response
25   tcp  filtered  smtp    no-response
80   tcp  open      http    syn-ack     Apache   2.2.3    (CentOS)
106  tcp  open      pop3pw  syn-ack     poppassd
110  tcp  open      pop3    syn-ack     Courier pop3d
111  tcp  filtered  rpcbind no-response
113  tcp  filtered  auth    no-response
143  tcp  open       imap    syn-ack     Courier Imapd      released
2004
443  tcp  open      http    syn-ack     Apache  2.2.3      (CentOS)
465  tcp  open      unknown syn-ack
646  tcp  filtered  ldp     no-response
993  tcp  open      imap    syn-ack     Courier Imapd      released
2004
995  tcp  open              syn-ack
2049 tcp  filtered  nfs     no-response
3306 tcp  open      mysql   syn-ack     MySQL   5.0.45
8443 tcp  open      unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Port scanning can best be described as a reconnaissance—and as such doesn't fit cleanly into the category of attack, threat, or vulnerability.

However….note the kind of data that is available: port, protocol, state, service, product, and version.

Vulnerabilities in Wireless Networks

- Confidentiality—Every message in WiFi is a broadcast, unencrypted messages can be read by anyone who’s listening and within range
- Integrity—When WiFi access points receive two streams of communication claiming to be the same computer, they necessarily accept the one with greater signal strength. This allows attackers to take over and forge sessions by spoofing legitimate computers and boosting signal strength.
- Availability—In addition to the obvious availability issues, WiFi creates new availability problems, such as session hijacking, forced disassociation, and jamming.
- Unauthorized WiFi access—Some form of cryptographic control is necessary to address this
- Picking up the beacon—Hidden SSIDs can easily be discovered by monitoring client requests for SSIDs in the absence of SSID beacons from the access point
- SSID in all frames—Similar to picking up the beacon, once a client connects to an access point, the SSID is stored in all communication frames and can be sniffed that way
- Association issues—WiFi clients generally have preferred associations—networks they know and trust to connect to automatically—and these may include very common SSID names, such as AT&Twifi and Apple. Without additional security measures, attackers can spoof these trusted SSIDs and trick devices into connecting to rogue access points.

WEP

- Wired equivalent privacy, or WEP, was designed at the same time as the original 802.11 WiFi standards as the mechanism for securing those communications
- Weaknesses in WEP were first identified in 2001, four years after release
- More weaknesses were discovered over the course of years, until any WEP-encrypted communication could be cracked in a matter of minutes

How it works:

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client, which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it’s the same number to authenticate the client
- Once the client is authenticated, the AP and client communicate using messages encrypted with the key

WEP Weaknesses

- Weak encryption key
  - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV), thus reducing effective key size to 40 or 140 bits
  - Keys were either alphanumeric or hex phrases that users typed in and were therefore vulnerable to dictionary attacks
- Static key
  - Since the key was just a value the user typed in at the client and AP, and since users rarely changed those keys, one key would be used for many months of communications
- Weak encryption process
  - A 40-bit key can be brute forced easily. Flaws that were eventually discovered in the RC4 encryption algorithm WEP uses made the 104-bit keys easy to crack as well
- Weak encryption algorithm
  - WEP used RC4 in a strange way (always a bad sign), which resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication
- IV collisions
  - There were only 16 million possible values of IV, which, in practice, is not that many to cycle through for cracking. Also, they were not as randomly selected as they should have been, with some values being much more common than others
- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors but did not use one that could address malicious modification
- No authentication
  - Any client that knows the AP’s SSID and MAC address is assumed to be legitimate

WPA (WiFi Protected Access)

- WPA was designed in 2003 as a replacement for WEP, followed in 2004 by WPA2, algorithm remains standard today

- Non-static encryption key
  - WPA uses a hierarchy of keys: New keys are generated for confidentiality and integrity of each session, and the encryption key is automatically changed on each packet
  - This way, the keys that are most important are used in very few places and indirect ways, protecting them from disclosure

- Authentication
  - WPA allows authentication by password, token, or certificate

WPA2 is adequately secure if configured well: Choose a strong encryption algorithm (AES without TKIP), and use a long, random passphrase.

- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm

- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check

- Session initiation
  - WPA sessions begin with authentication and a four-way handshake that results in separate keys for encryption and integrity on both ends

While there are some attacks against WPA, they are either of very limited effectiveness or require weak passwords

Denial of Service (DoS)

A denial-of-service, or DoS, attack is an attempt to defeat availability

Denial of service means a user is denied access to authorized services or data.

Confidentiality and integrity are concerned with preventing unauthorized access.

Availability is concerned with preserving authorized access.

DoS attacks are attempts to defeat a system’s availability:

- Volumetric attacks
- Application-based attacks
- Disabled communications
- Hardware or software failure

Denial of Service (DoS)

- One potential weakness is the capacity of the system.
- If demand is higher than the system can handle, some data will not move properly through the network
- These attacks are also known as volume-based or volumetric attacks.
- Similarly to overwhelming basic network capacity, an attack can exhaust the application that services a particular network, in what is called an application based attack.

Denial of Service (DoS)

- Another way to deny service is to cut or disable the communications link between two points.
- Many users will be unable to receive service, especially if that link is a single point through which much traffic must pass.
- A final cause of denied access is a hardware or software failure.
- Although similar to a failure of a communications link, in this case the problem relates to machinery or programs, for which protection can involve concepts like fault tolerance.

Flooding

- An attacker can try for the same overloading effect by presenting commands more quickly than a server can handle them;
- servers often queue unmet commands during moments of overload for service when the peak subsides, but if the commands continue to come too quickly, the server eventually runs out of space to store the demand.
- Such an attack is called an overload or flood. The target of a flooding attack can be an application, such as a database management system; an operating system or one of its components,
- For example, file or print server; or a network appliance like a router. Alternatively, the flooding attack can be directed against a resource, such as a memory allocation table or a web page.
- A flooding attack occurs from demand in excess of capacity, from malicious or natural causes.

Blocked Access

- The attacker may simply prevent a service from functioning. The attacker could exploit a software vulnerability in an application and cause the application to crash.
- Or the attacker could interfere with the network routing mechanisms, preventing access requests from getting to the server.
- Another approach would be for the attacker to manipulate access control data, deleting access permissions for the resource, or
- To disable the access control mechanism so that nobody could be approved for access.

Access Failure

- Either maliciously or not, hardware and software fail from time to time.
- Software stops working due to a flaw, or a hardware device wears out or inexplicably stops.
- The failure can be sporadic, meaning that it goes away or corrects itself spontaneously, or the failure can be permanent, as from a faulty component.
- These are the three root threats to availability:
- • insufficient capacity; overload
- • blocked access
- • unresponsive component

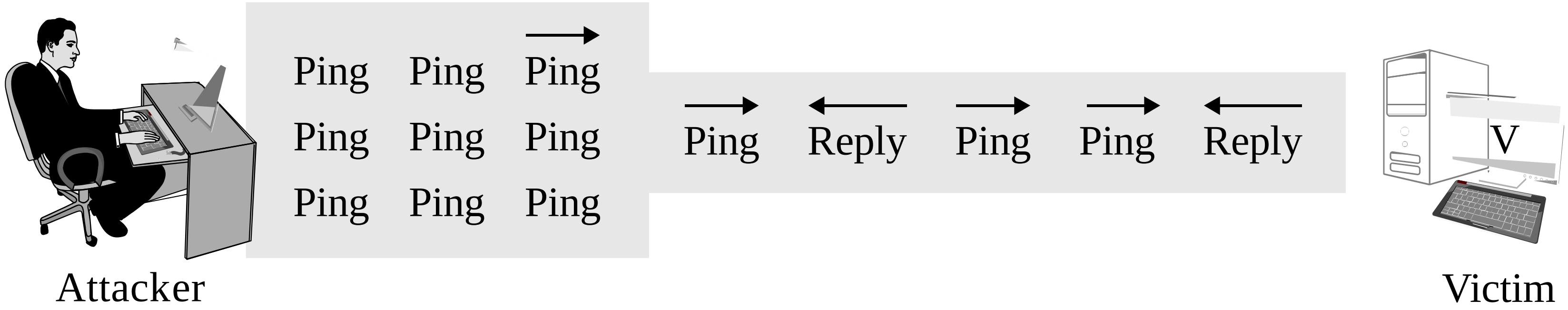
Flooding

- Flooding occurs because the incoming bandwidth is insufficient or resources hardware devices, computing power, software, or table capacity are inadequate.
- More sophisticated attacks use or misuse elements of Internet protocols. In addition to TCP and UDP, there is a third class of protocols, called ICMP or Internet Control Message Protocols.
- ICMP used for system diagnostics/network management

Network Flooding Caused by Malicious Code

- ICMP protocols include
- ping, which requests a destination to return a reply, intended to show that the destination system is reachable and functioning
- echo, which requests a destination to return the data sent to it, intended to show that the connection link is reliable (ping is actually a version of echo)
- destination unreachable, which indicates that a destination address cannot be accessed
- source quench, which means that the destination is becoming saturated and the source should suspend sending packets for a while

DoS Attack: Ping Flood



Ping Ping Ping →

Ping Ping Ping

Ping Ping Ping

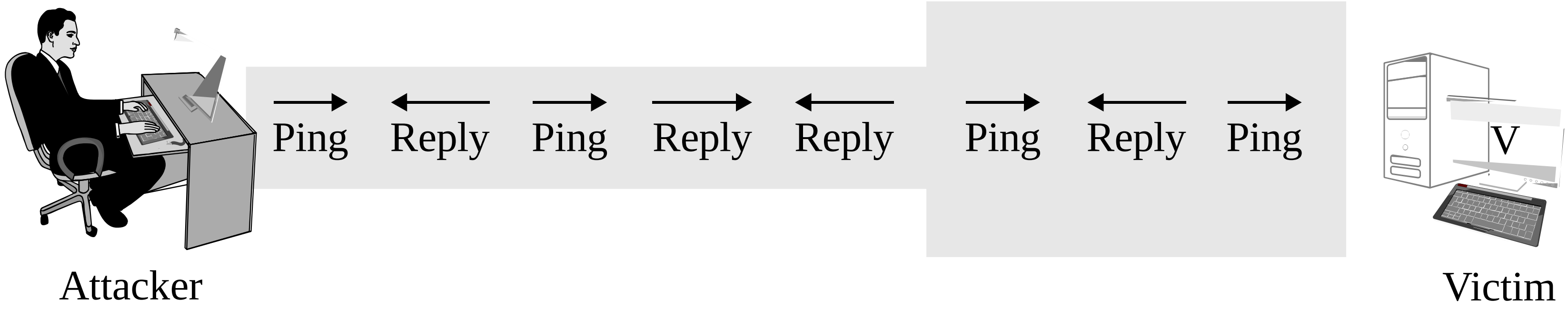
→ Ping ← Reply → Ping → Ping ← Reply

V

Attacker

Victim

(a) Attacker has greater bandwidth



→ Ping ← Reply → Ping → Reply ← Reply → Ping ← Reply → Ping

V

Attacker

Victim

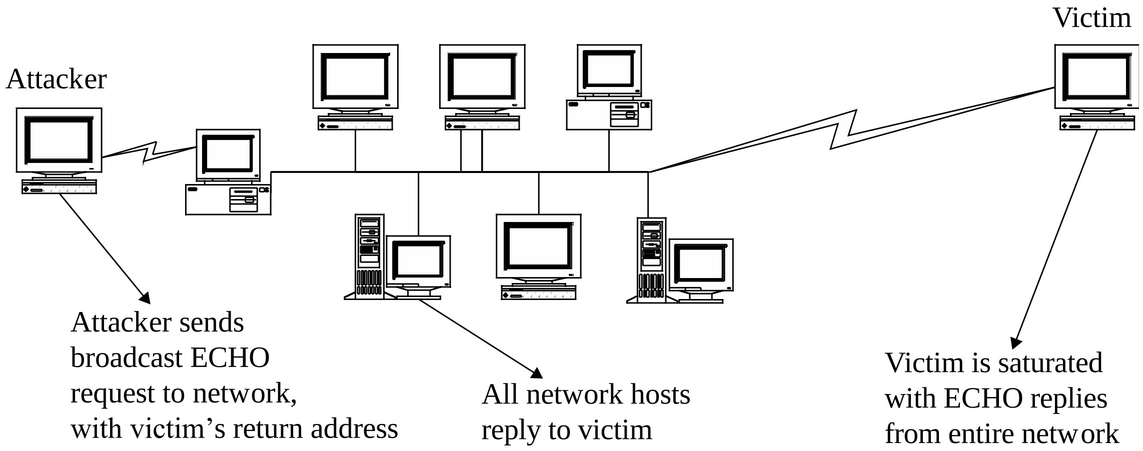
(b) Victim has greater bandwidth

DoS Attack: Smurf Attack

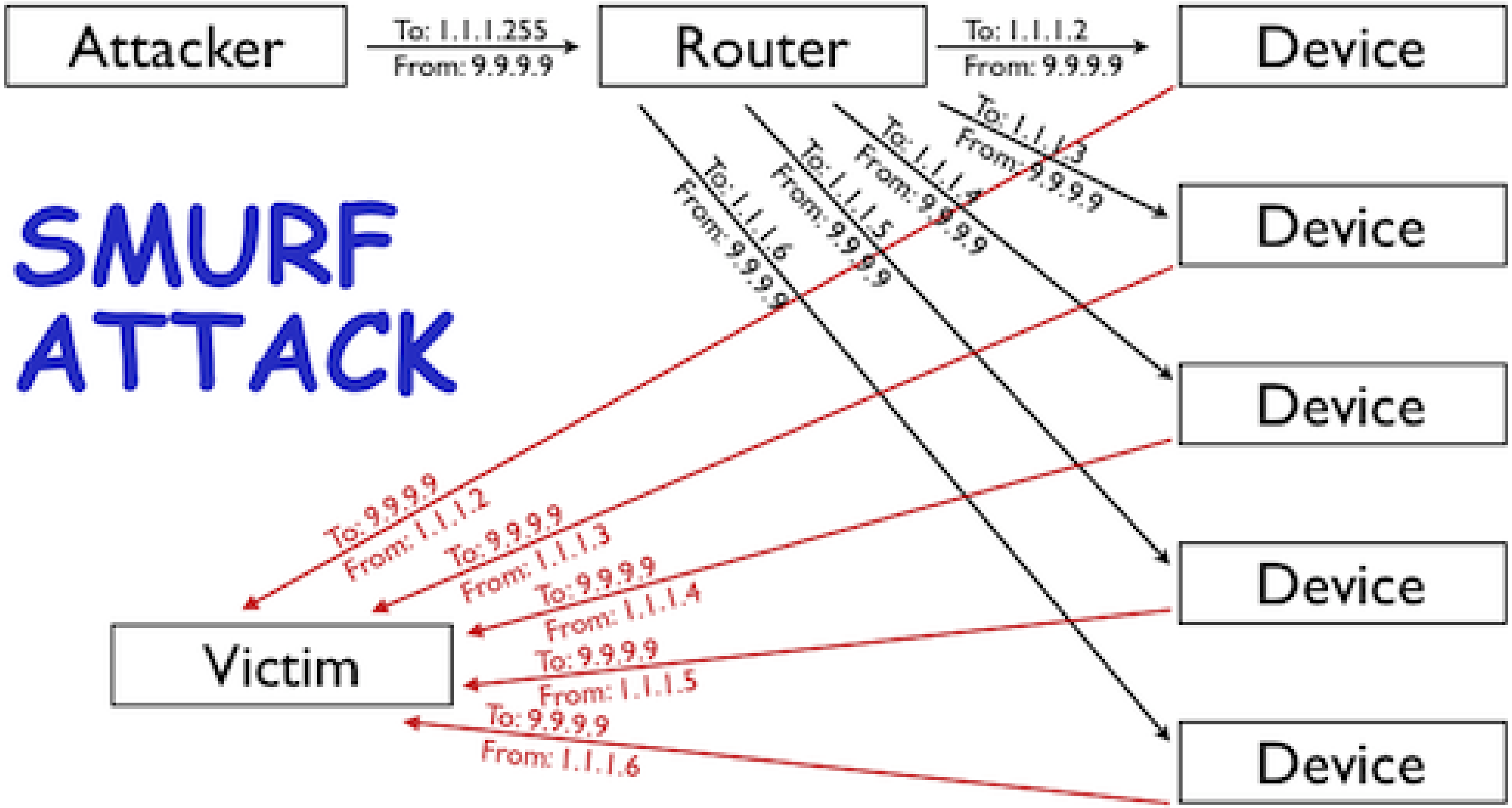
The original amplification attack involves an attacker sending ICMP requests (i.e., ping requests) to the network's broadcast address (i.e., X.X.X.255) of a router configured to relay ICMP to all devices behind the router.

The attacker spoofs the source of the ICMP request to be the IP address of the intended victim. Since ICMP does not include a handshake, the destination has no way of verifying if the source IP is legitimate. The router receives the request and passes it on to all the devices that sit behind it.

All those devices then respond back to the ping. The attacker is able to amplify the attack by a multiple of how ever many devices are behind the router (i.e., if you have 5 devices behind the router then the attacker is able to amplify the attack 5x).

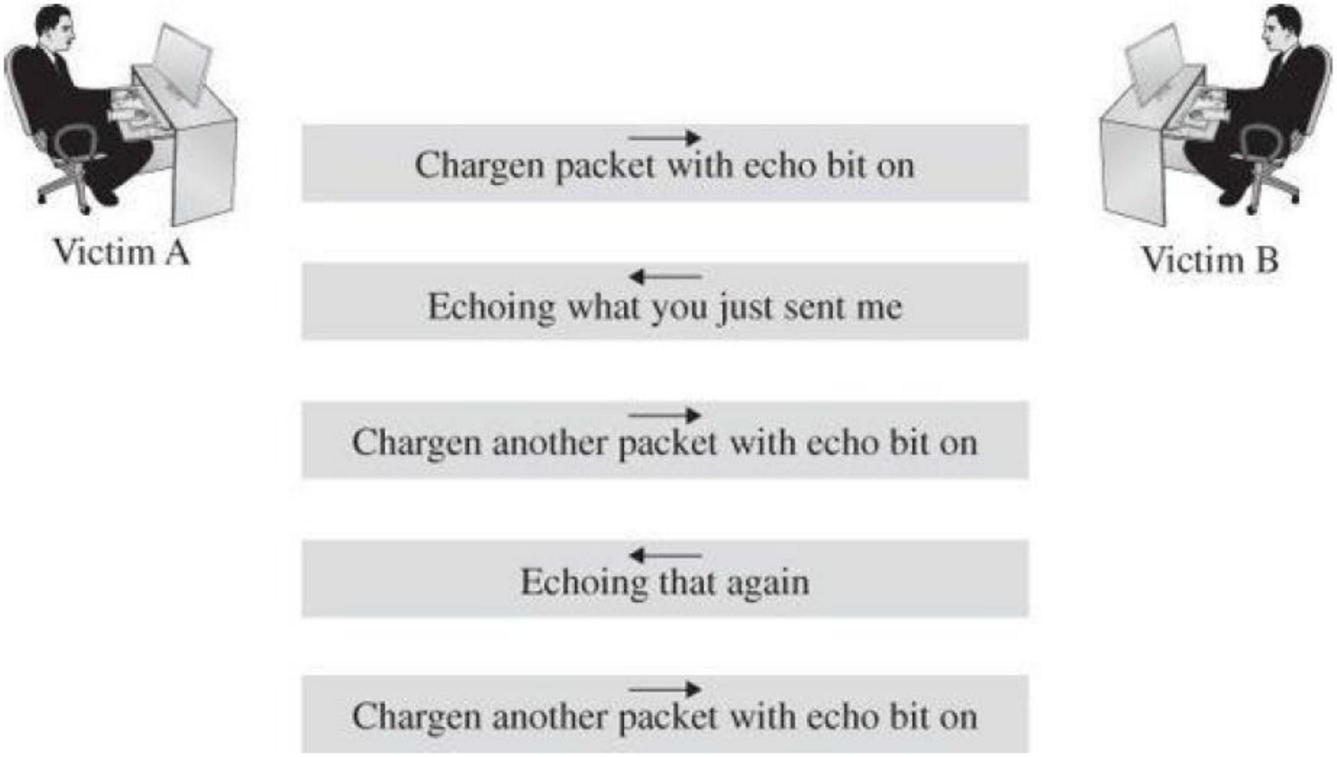

Victim
Attacker
Attacker sends broadcast ECHO request to network, with victim's return address
All network hosts reply to victim
Victim is saturated with ECHO replies from entire network

Smurf Attack



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

Echo–Chargen



→ Chargen packet with echo bit on

← Echoing what you just sent me

→ Chargen another packet with echo bit on

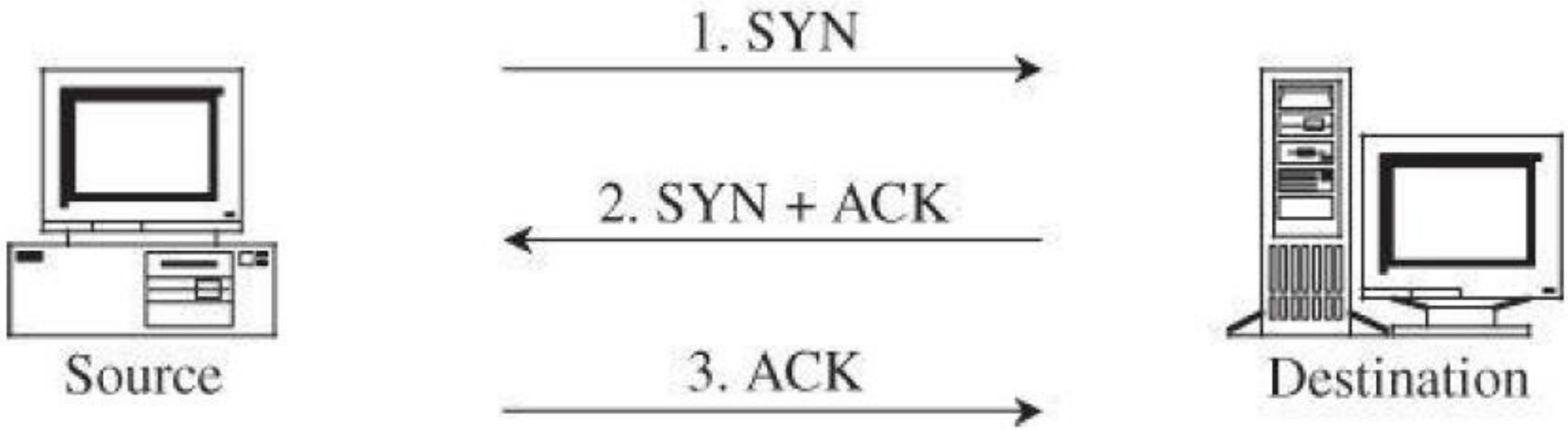
← Echoing that again

→ Chargen another packet with echo bit on

FIGURE 6-20 Echo–Chargen Attack

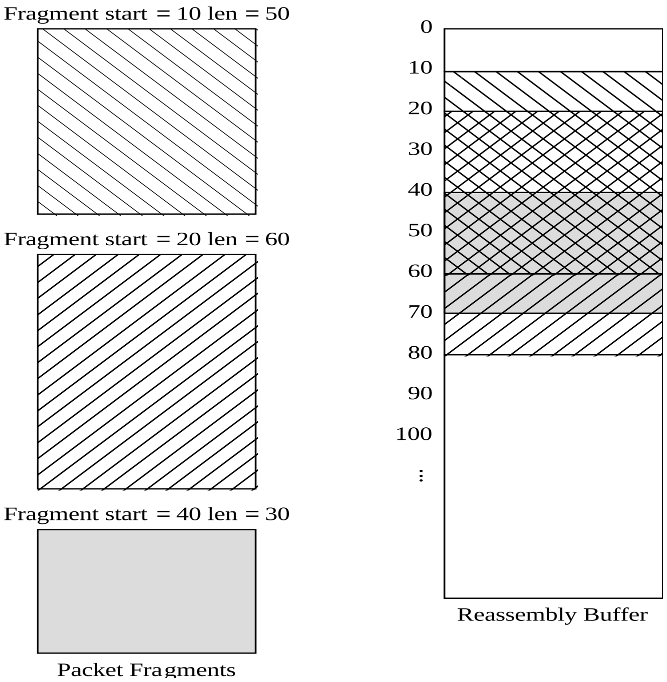
SYN Flood

- The attacker can deny service to the target by sending many SYN requests, to which the target properly responds with SYN-ACK; however, the attacker never replies with ACKs to complete the connections, thereby filling the victim’s SYN_RECV queue.



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

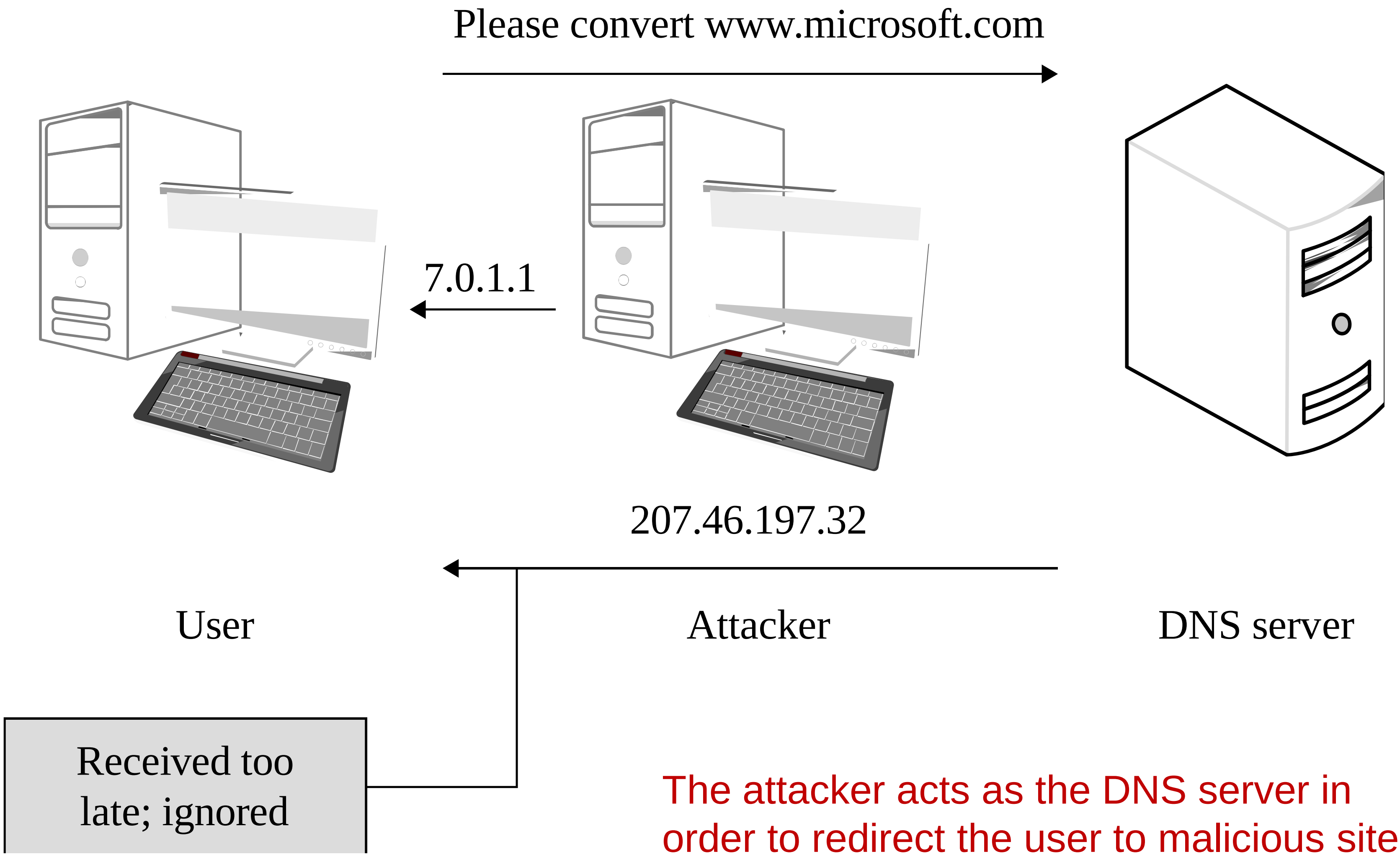
DoS Attack: Teardrop Attack


Fragment start = 10 len = 50
Fragment start = 20 len = 60
Fragment start = 40 len = 30
Packet Fragments
0
10
20
30
40
50
60
70
80
90
100
⋮
Reassembly Buffer

The attacker sends packets that cannot possibly be reassembled (conflicting reassembly instructions).

In extreme cases, this can cause the entire OS to lock up.

DoS Attack: DNS Spoofing



Please convert www.microsoft.com

7.0.1.1

207.46.197.32

User

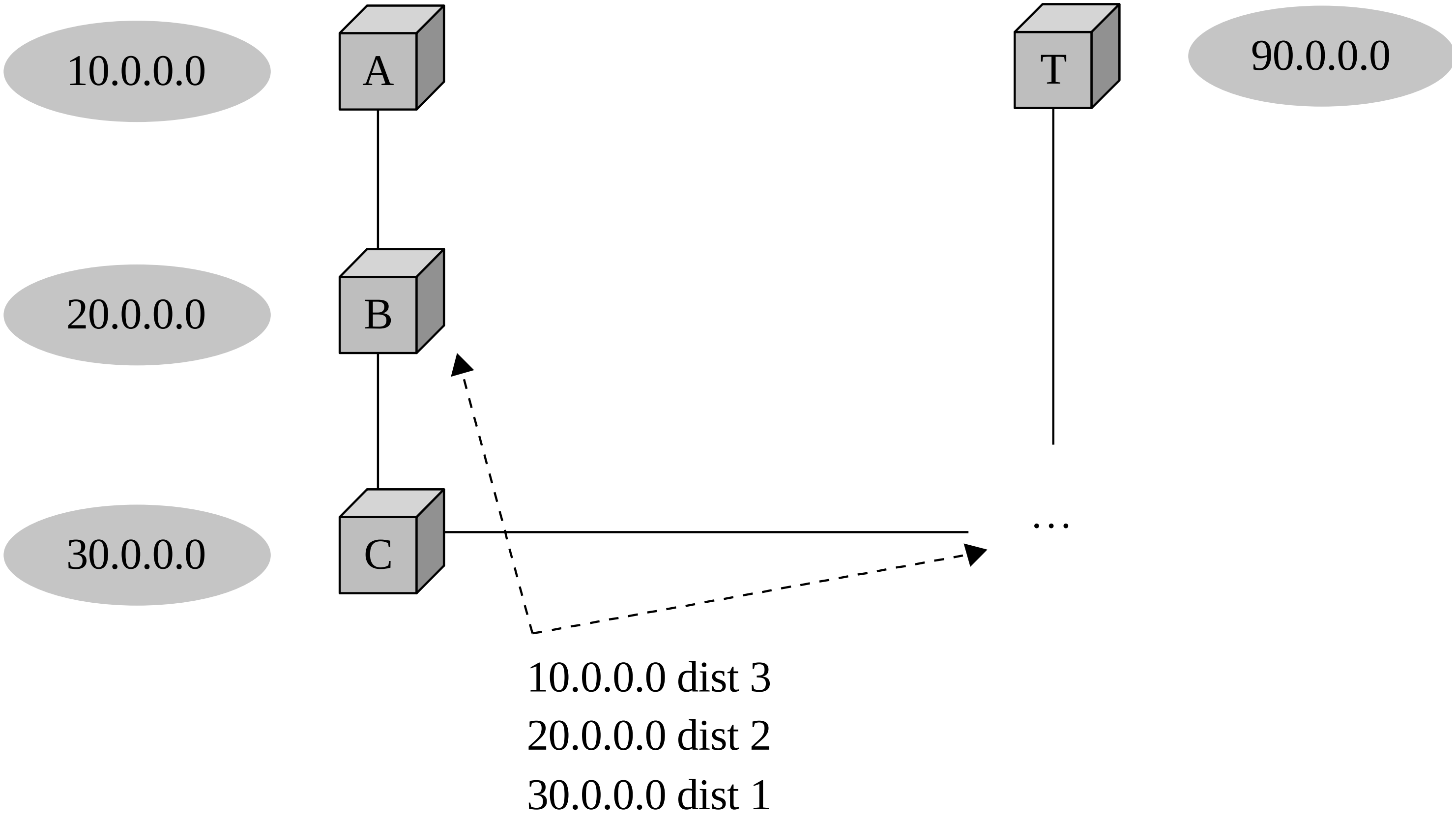
Attacker

DNS server

Received too late; ignored

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

DoS Attack: Rerouting Routing



This picture doesn’t show anything malicious happening. It just shows how one router, C, advertises the routes it knows about to the routers adjacent to it. Routers rely on these advertising messages to be accurate; when they aren’t, DoS can ensue.

Traffic Redirection

- Each router advises its neighbors about how well it can reach other network addresses. This characteristic allows an attacker to disrupt the network.
- Routers trust each other to provide accurate data
- Due to nonmalicious corruption a router will send faulty data
- An intentionally misleading router (or a device maliciously impersonating a router) can persist because of implicit trust.
- A standard countermeasure to exclude impostors is identification and authentication.

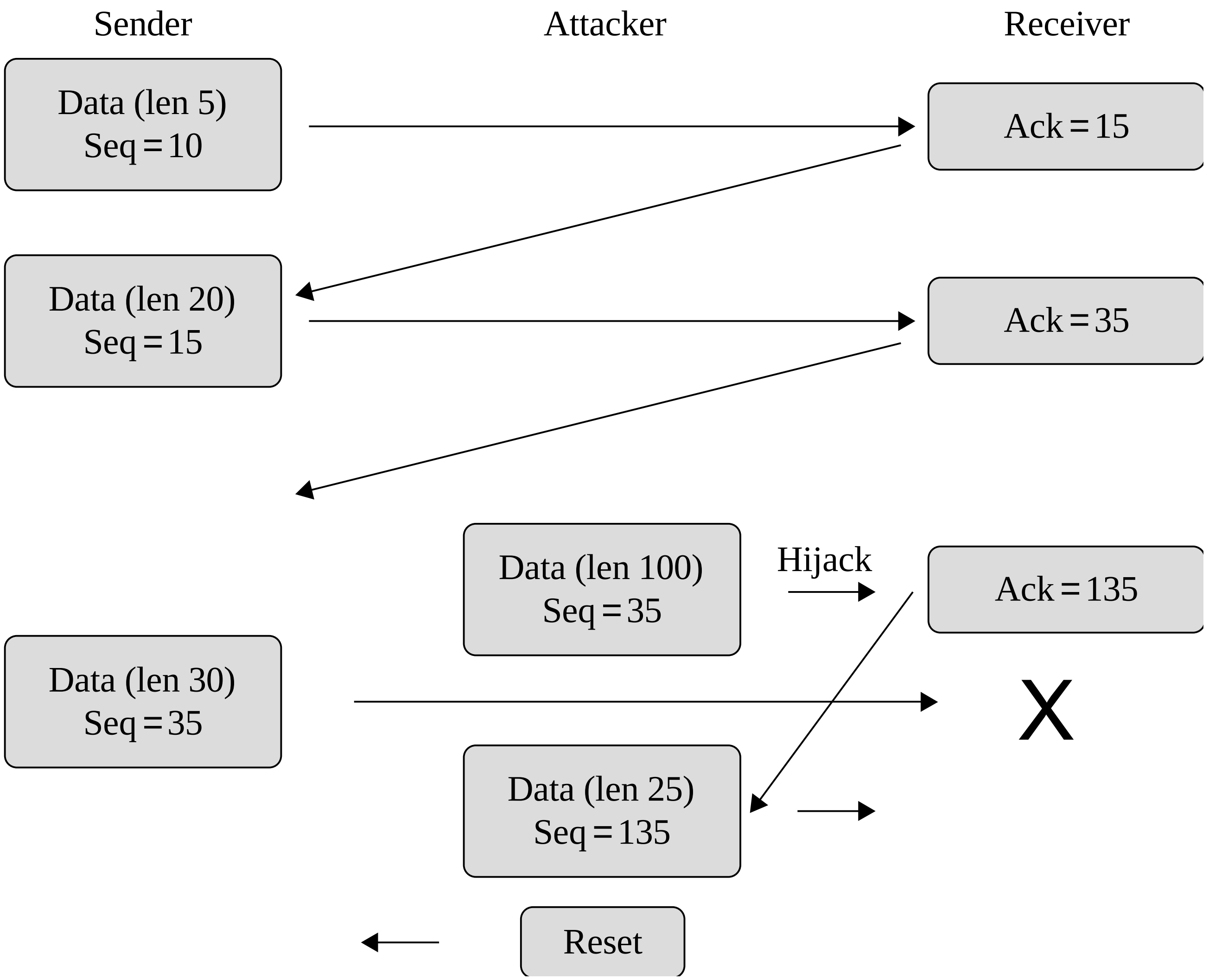
DNS attacks

- A class of attacks based on the concept of domain name server.
- Name Server Application Software Flaws
- Name servers run software called Berkeley Internet Name Domain, or BIND,
- BIND has had numerous flaws, including a now familiar buffer overflow.
- By overtaking a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, with an implication for denial of service.

Top-Level Domain Attacks

- Another way to deny service through address resolution failures involves incapacitating the Internet’s DNS system itself.
- In October 2002, a massive flood of traffic flooded the Internet’s top-level domain DNS servers,
- An attack in March 2005 used a flaw in a Symantec firewall to allow a change in the DNS records used on Windows machines.
- The objective of this attack was not denial of service, however. In this attack, the poisoned DNS cache redirected users to advertising sites that received money from clients each time a user visited the site.

DoS Attack: Session Hijacking



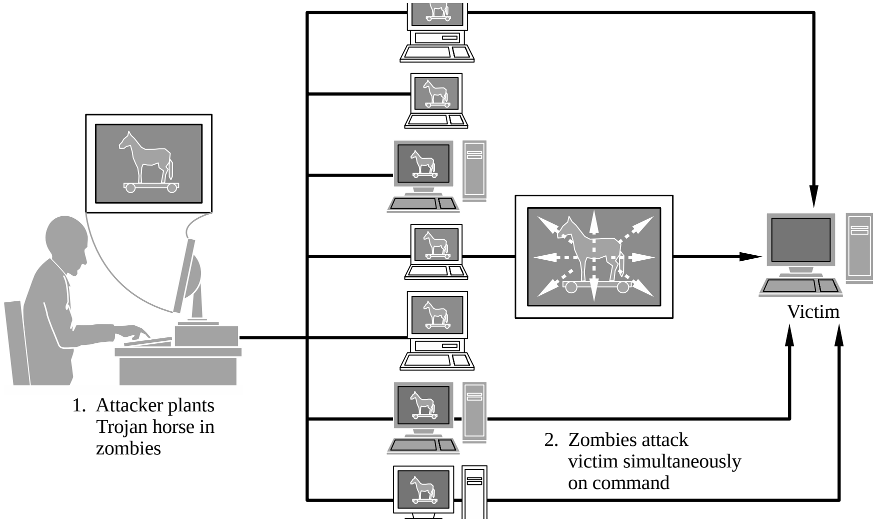
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DDoS

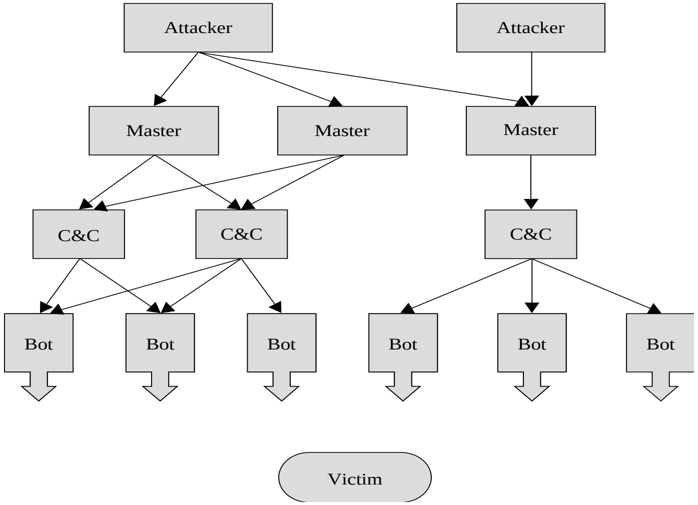
- DDoS attacks most often work by botnets – a large group of distributed computers that act in concert with each other – simultaneously spamming a website or service provider with data requests.
- Attackers use malware or unpatched vulnerabilities to install Command and Control (C2) software on user's systems to create a botnet. DDoS attacks rely on a high number of computers in the botnet to achieve the goal, & the cheapest way to get control of that many machines is by leveraging exploits.
- The DYNDNS attack exploited WIFI cameras with default passwords to create a huge botnet. Once they have the botnet ready, the attackers send the start command to all of their botnet nodes, and the botnets will then send their programmed requests to the target server. If the attack makes it past the outer defenses, it quickly overwhelms most systems, causes service outages, and in some cases, crashes the server.

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

Distributed Denial of Service (DDoS)



1. Attacker plants Trojan horse in zombies
Victim
2. Zombies attack victim simultaneously on command



1) Conscript an army of compromised machines to attack a victim.
2) Choose a victim, and have the whole army unleash a DoS attack at once.

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

- Botnets are machines running malicious code under remote control.

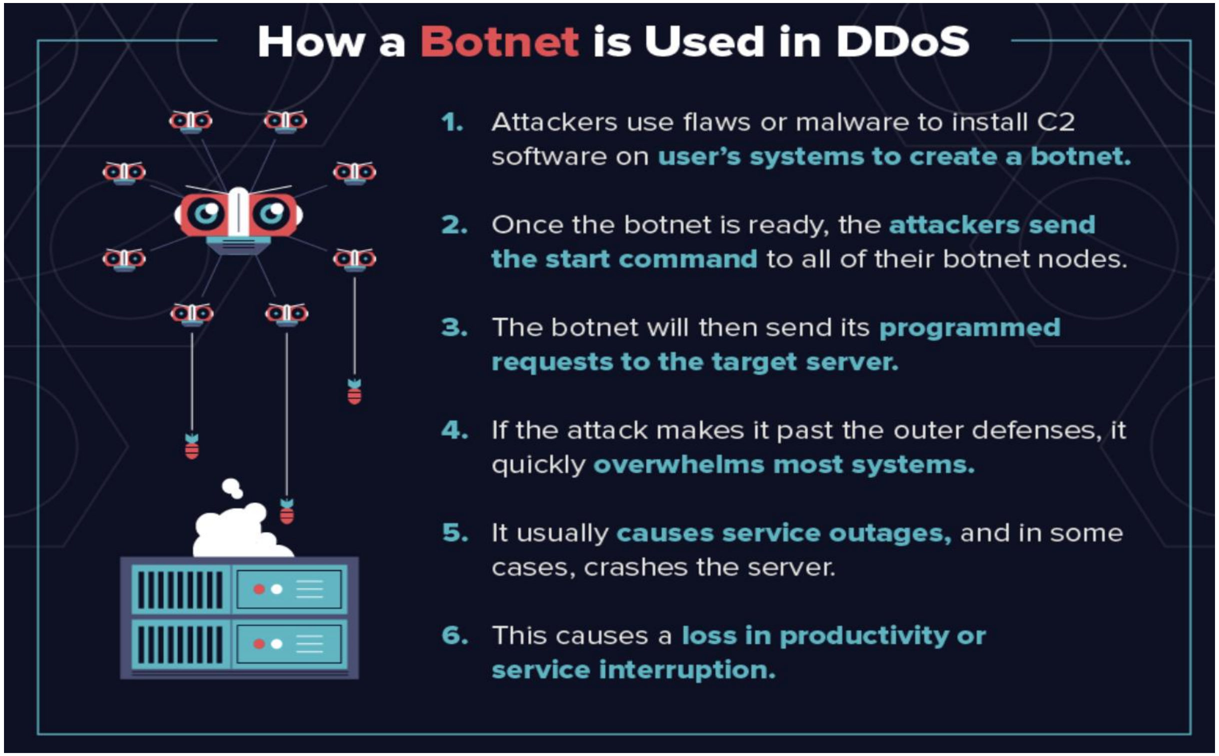
- They often go undetected because they do little harm to the machines they run on.

- Attacker separated from bots by multiple layers, making attacker difficult to trace. Redundancy built in so that if one master or C&C node is down, the bots can continue….

DoS vs DDoS

- A Denial of Service (DoS) attack includes many kinds of attacks all designed to disrupt services. In addition to DDoS, you can have application layer DoS, advanced persistent DoS, and DoS as a service. Companies will use DoS as a service to stress test their networks.

- In short, DDoS is one type of DoS attack – however, DoS can also mean that the attacker used a single node to initiate the attack, instead of using a botnet. Both definitions are correct.



How a Botnet is Used in DDoS

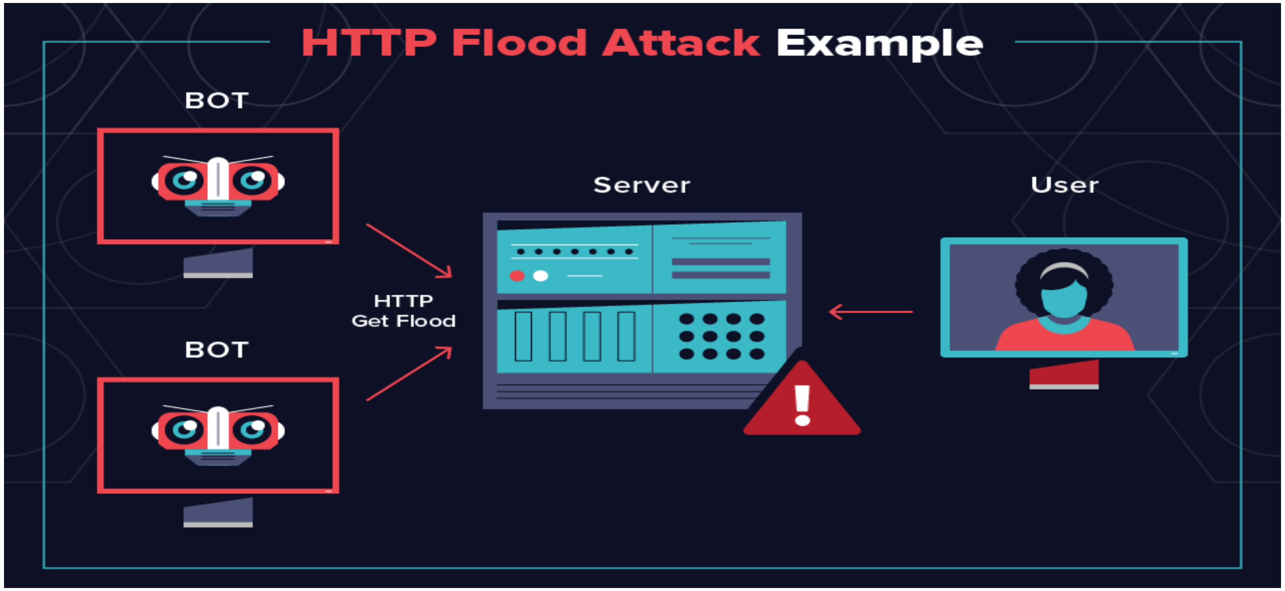
1. Attackers use flaws or malware to install C2 software on **user's systems to create a botnet.**
2. Once the botnet is ready, the **attackers send the start command** to all of their botnet nodes.
3. The botnet will then send its **programmed requests to the target server.**
4. If the attack makes it past the outer defenses, it quickly **overwhelms most systems.**
5. It usually **causes service outages,** and in some cases, crashes the server.
6. This causes a **loss in productivity or service interruption.**

Application Layer Attacks

- Application layer DDoS attacks aim to exhaust the resources of the target and disrupt access to the target's service.

- Attackers load the bots with a complicated request that taxes the target server as it tries to respond. The request might require database access or large downloads. If the target gets several million of those requests in a short time, it can very quickly get overwhelmed and either slowed to a crawl or locked up completely.

- An HTTP Flood attack, for example, is an application layer attack that targets a web server on the target and uses many fast HTTP requests to bring the server down.


HTTP Flood Attack Example
BOT
BOT
HTTP
Get Flood
Server
User