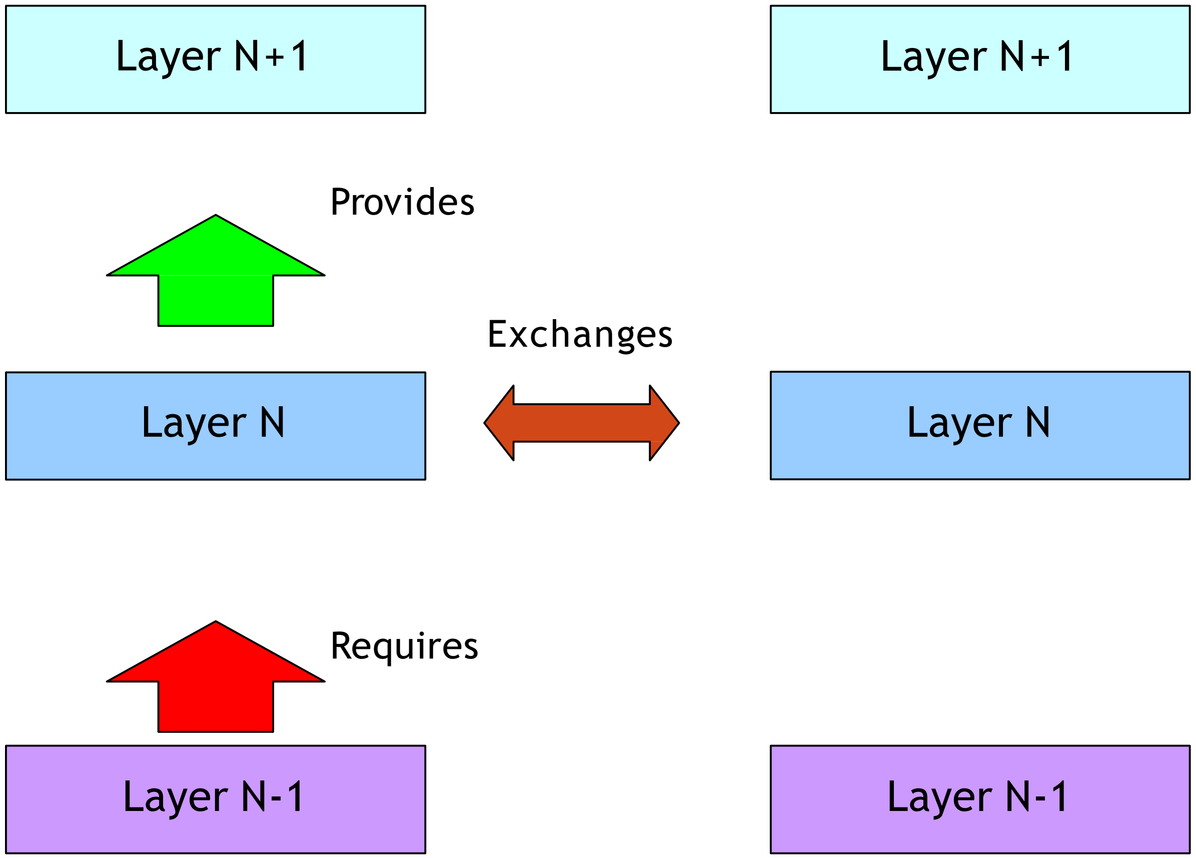
NETWORK SECURITY

NETWORK MODELS

- Network models use layers to describe networks
- Each layer describes the services provided to the layer above it and those required from the layer below it
- It also describes the format of exchanges between peer layers on different network hosts
- Because the layers "stack" on top of one another, we often refer to network protocol "stacks" when we talk about the implementation



NETWORK MODELS

- The most well-known network model is the OSI (Open Systems Interconnect) Reference Model defined and maintained by the Organization for International Standardization (ISO)
- It consists of seven layers, numbered from the bottom (closest the network) to the top (closest the user)

Layer 7 – Application

Layer 6 – Presentation

Layer 5 – Session

Layer 4 – Transport

Layer 3 – Network

Layer 2 – Data Link

Layer 1 – Physical

OSI REFERENCE MODEL

- Layer 1 –The Physical Layer
  - Defines the type of media to be used
  - Defines representation of data on the medium
    - Is a 'o'"high" or "low", "on" or "off"?
    - What order are bits transmitted (if serial)?

Layer 1 –Physical

OSI REFERENCE MODEL

- Layer 2 –The Data Link Layer
  - Defines "right to transmit" rules
  - Provides directly-connected host-to-host data transfer
  - Defines higher-level structure of data (frames)
  - Defines "physical" address structure for hosts

Layer 2 –Data Link

Layer 1 –Physical

OSI REFERENCE MODEL

- Layer 3 –The Network Layer: logical communication between hosts
  - Provides end-host-to-end-host data transfer across (potentially) multiple data links
  - Defines higher-level structure of data (packets)
  - Defines “abstract” address structure for hosts

Layer 3 –Network

Layer 2 –Data Link

Layer 1 –Physical

OSI REFERENCE MODEL

- Layer 3 –The Transport Layer: logical communication between processes
  - Provides delivery of a message from one process to another.
  - Defines guarantees in packet delivery
  - Defines “abstract” port structure for hosts

Layer 4 –Transport

Layer 3 –Network

Layer 2 –Data Link

Layer 1 –Physical

OSI REFERENCE MODEL

- Layer 5 –The Session Layer
  - Provides a logically persistent connection between processes
  - May involve user or host authentication (login), transaction encapsulation (for database access), etc.

Layer 5 –Session

Layer 4 –Transport

Layer 3 –Network

Layer 2 –Data Link

Layer 1 –Physical

OSI REFERENCE MODEL

- Layer 6 –The Presentation Layer
  - Defines the network representation of data
  - Converts between the network and host representations of data (ASCII/EBCDIC, byte order, encryption, compression, etc.)

Layer 6 –Presentation

Layer 5 –Session

Layer 4 –Transport

Layer 3 –Network

Layer 2 –Data Link

Layer 1 –Physical

OSI REFERENCE MODEL

- Layer 7 – The Application Layer
  - Provides a portal for the application to access the network
  - Describes the dialog between two applications communicating across the network.

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

TCP/IP NETWORK

- When TCP/IP was defined in the early days of the Internet, the OSI Reference Model had not been defined, so a different layering model was used
- It consists of 4 or 5 layers, and maps closely to the OSI Reference Model

Layer 5 –Application

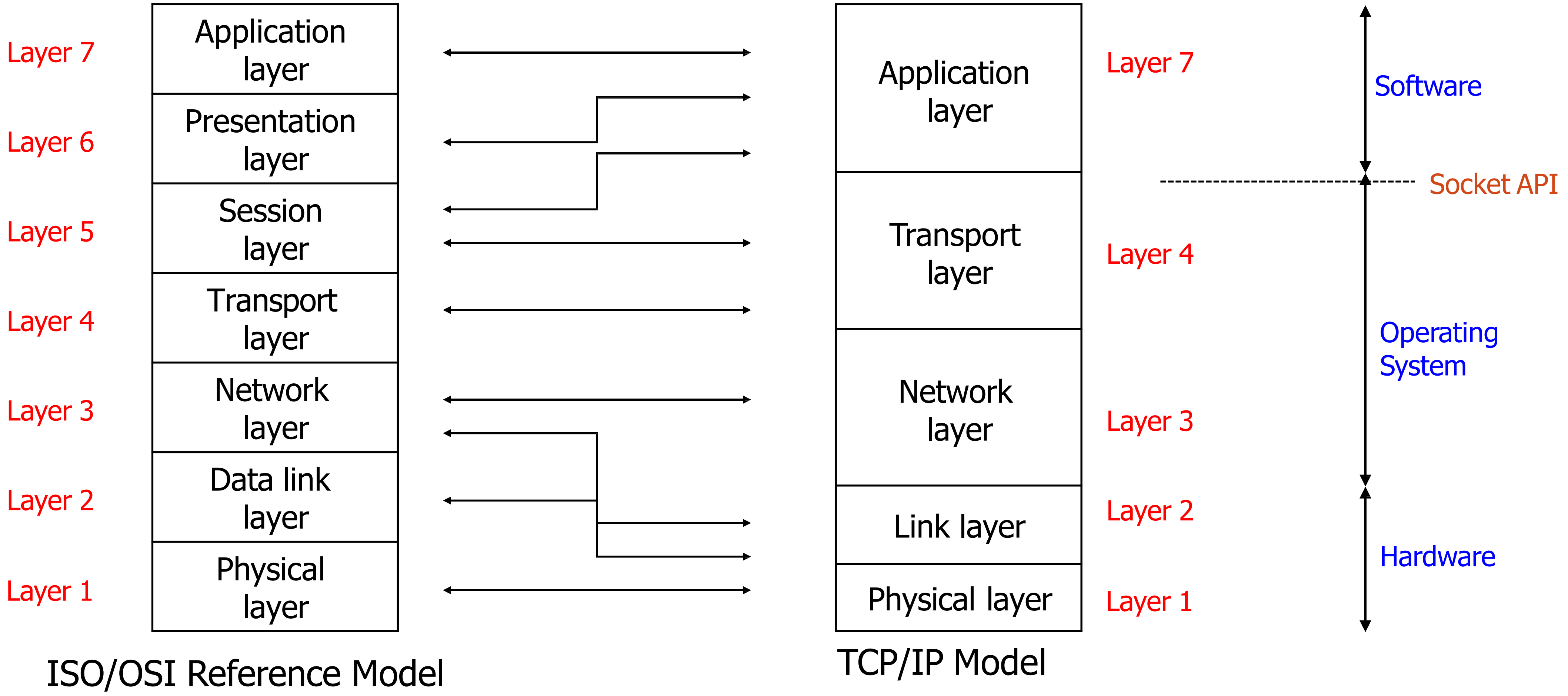
Layer 4 –Transport

Layer 3 –Internetwork

Layer 2 –Link

Layer 1 –Physical

LAYERED PROTOCOL ARCHITECTURE



NETWORK SECURITY GOALS

Confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message
- Privacy: hide `who is doing what with whom`

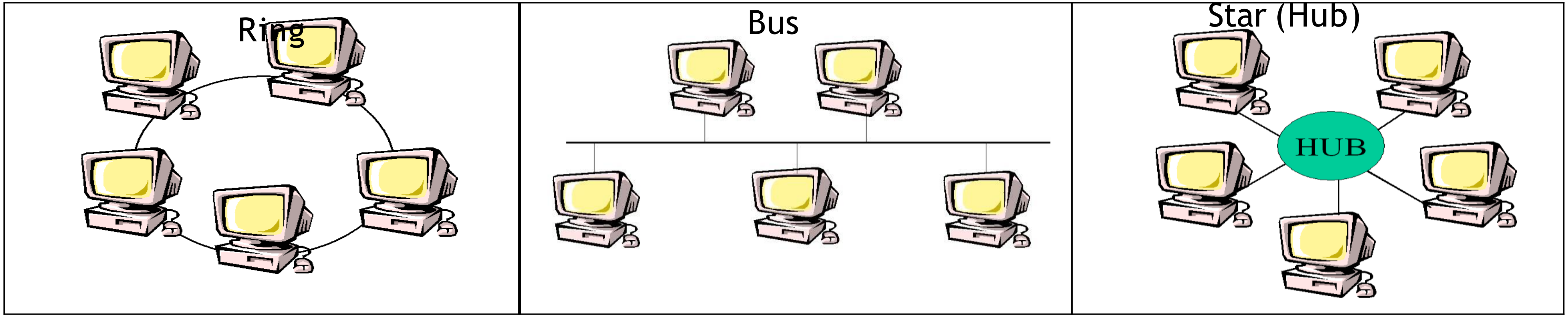
Authentication: sender, receiver want to confirm identity of each other

Integrity: sender, receiver want to ensure messages are not altered (in transit, or afterwards) without detection

Access and Availability: services must be accessible and available to users

SHARED MEDIA (BROADCAST) NETWORKS

- Shared media net: all traffic passes thru all computers
  - Mostly Local Area Networks (LAN)
  - E.g. Ethernet, token-ring, Wireless LANs, Cellular…
  - Usually: promiscuous mode listends to all messages on Net
- Shared Media Attack Model:
  - Easy: eavesdropping (sniffing) –passive attack
    - Unless cryptographically protected: encryption
  - Harder (but possible): spoofing –active attack



INTERNET ATTACK MODEL

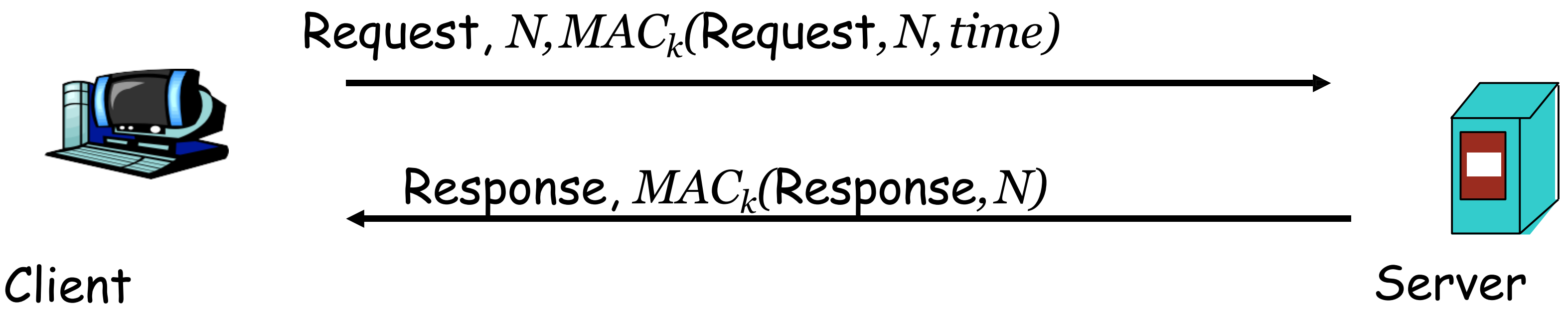
- Easy: inject messages, spoof (misrepresent)
  - Source address spoofing (IP, e-mail)
  - Spoofing by deceitful content, address (web, e-mail)
- Harder: intercept (eavesdrop/modify) message
  - Except if in same LAN as attacker or broken router
  - Hijacking attacks: intercept message by…
    - Route hijack: force routing via LAN / router
    - Address hijack: source sends to attacker's IP addr
    - Exercise: show such attacks with protocols we learned!
- Compare to shared-media attack model:
  - Easy: passive (eavesdropping)
  - Harder: active (modify, inject messages)
- Motivates: request-response protocols

REQUEST/RESPONSE PROTOCOLS

- Client sends *request*, server sends *response*
- Reliable pairing of response to request
  - Random ID (nonce) in request
- Weak authentication of response
  - Since it is hard to intercept request
- Server is often *stateless*
  - Do not keep state (e.g. connection) for each request
  - Efficiency and resiliency to DOS (Denial Of Service)
- Preferable design for security services
  - Due to simplicity, efficiency, resiliency to DOS
- Secure (strong) authentication of response …

SECURE REQUEST-RESPONSE MATCHING

- Attach random nonce N to request
- Attach $MAC_k(response,N)$ to response to validate
- Attach $MAC_k(request,N)$ to validate nonce, request
  - Does not prevent request re-play / reordering
  - To prevent replay: add time, $MAC_k(request,N,time)$
    - Server remembers nonces during `acceptable time window`
  - But this requires (some) state in server, and clocks

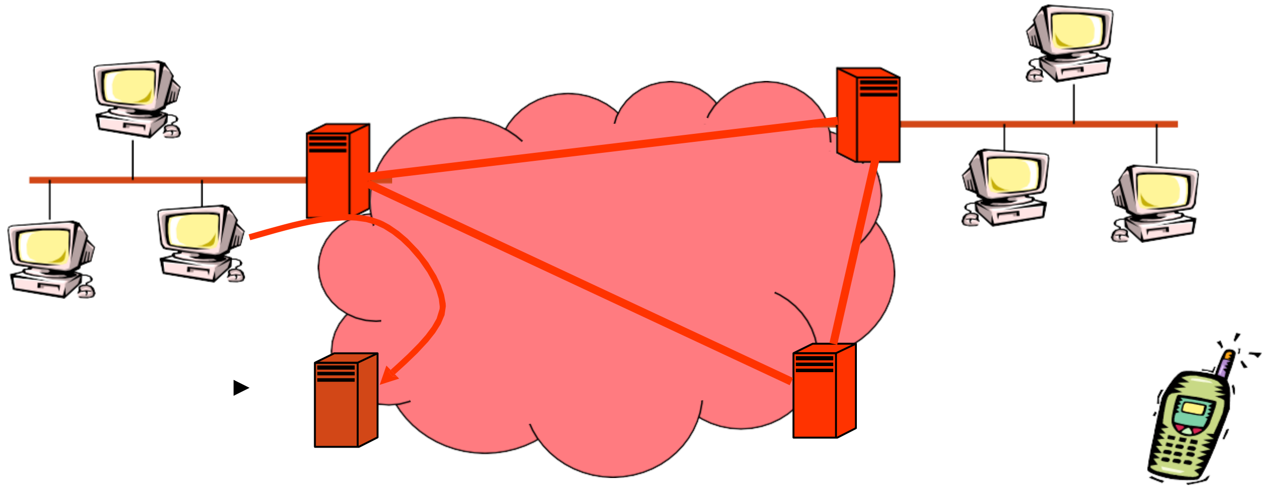


Or: request-response over *reliable, secure connection*

SECURE CONNECTION (TUNNEL): END-TO-END VS. HOP-BY-HOP

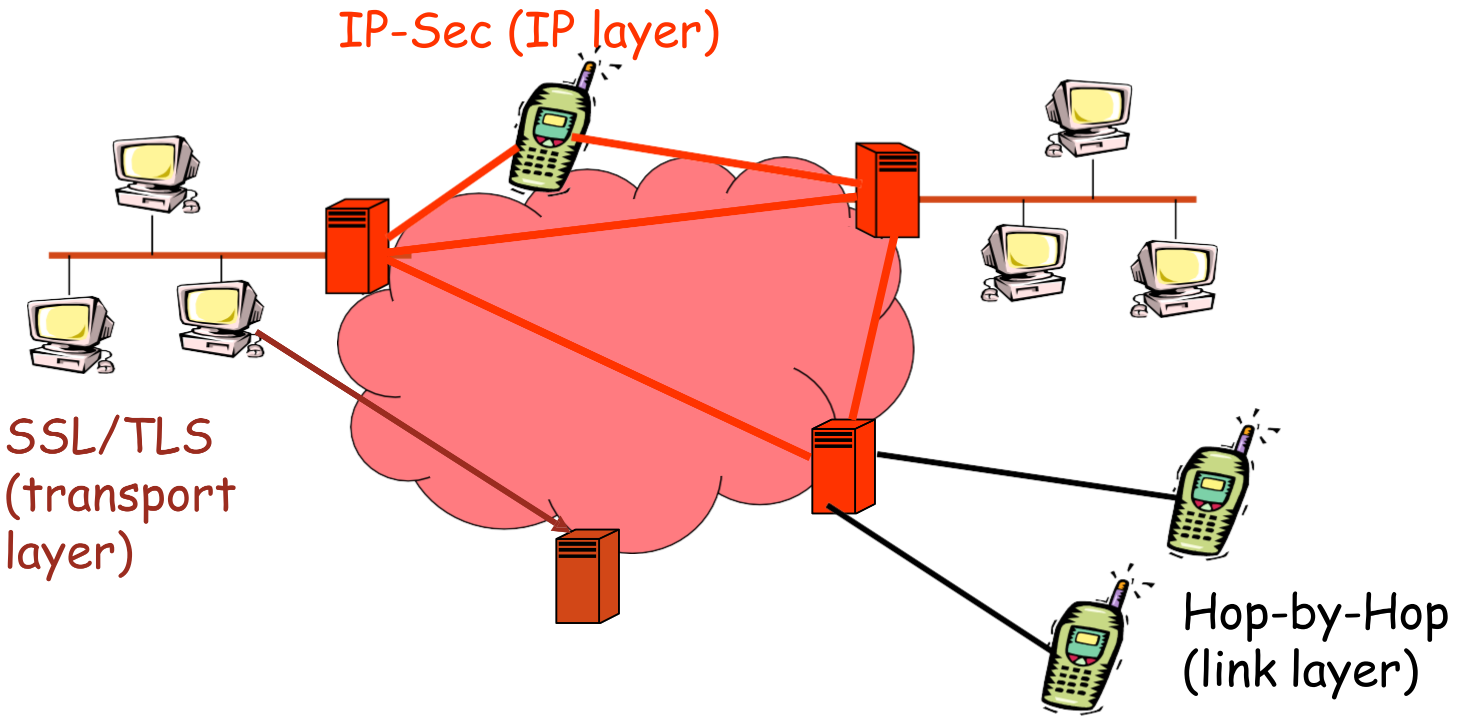
Can protect connection

- Crypto protects traffic over insecure link/Net
- Link layer: one `hop` (e.g. wireless link)
- IP Layer (IP-Sec): transparent to application
- Transport Layer (SSL/TLS): easy, widely used
- Application Layer (PGP, S/MIME)



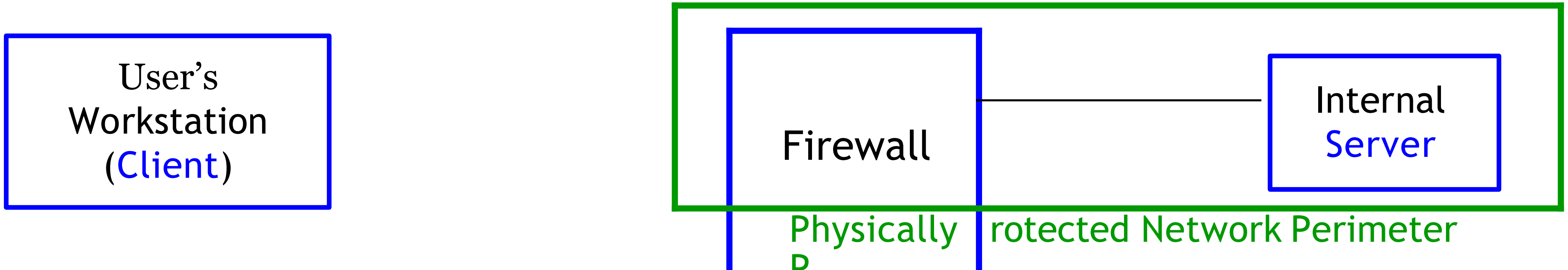
SECURE TUNNELS:

- Crypto protects traffic over insecure link/Net
- Hop-by-Hop (link layer) or End-to-End (higher layers)
- IP-Sec: also Gateway to Gateway or End-to-Gateway



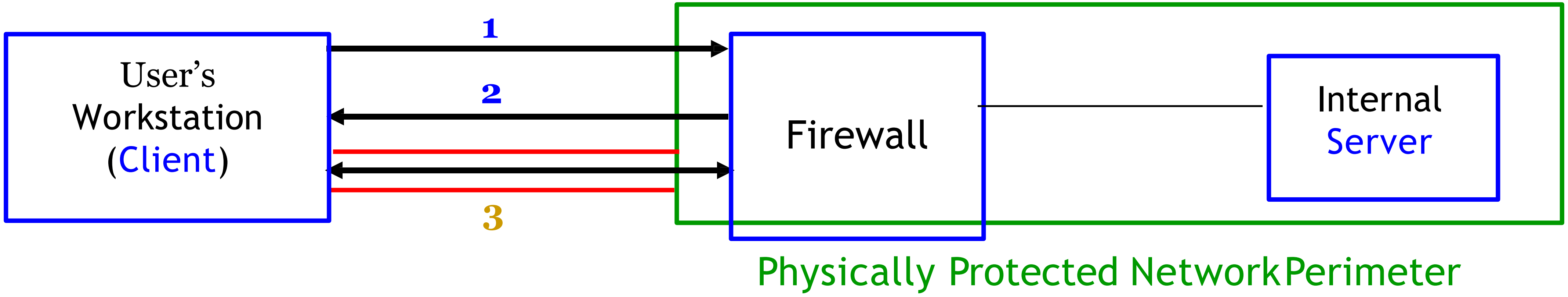
VIRTUAL PRIVATE NETWORK (VPN)

- Virtual private network (VPN) = connection over public network giving its user impression of being on private network
  - It could be viewed as „logical link" encryption
  - Could be viewed as end to end encryption between client & server
  - Protecting remote user's connection with her network
- Greatest risk for remote connection via public network:
  - Between user's workstation (client) and perimeter of „home" network (with server)



- Firewall protects network against external traffic (more later)

VIRTUAL PRIVATE NETWORK (VPN)



- Example VPN connection scenario 1

–C authenticates to firewall

(firewall passes user's authentication data to authentication server [not shown], which decides whether authentication is OK)

2 –Firewall replies with encryption key

(after negotiating with C a session encryption key)

3 –C and S communicate via encrypted *tunnel*

COMMON SECURITY ATTACKS AND THEIR COUNTERMEASURES

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

WHAT IS A FIREWALL?

- A **choke point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
  - only authorized traffic is allowed
- Auditing and controlling access
  - can implement alarms for abnormal behavior
- Itself immune to penetration
- Provides **perimeter defence**

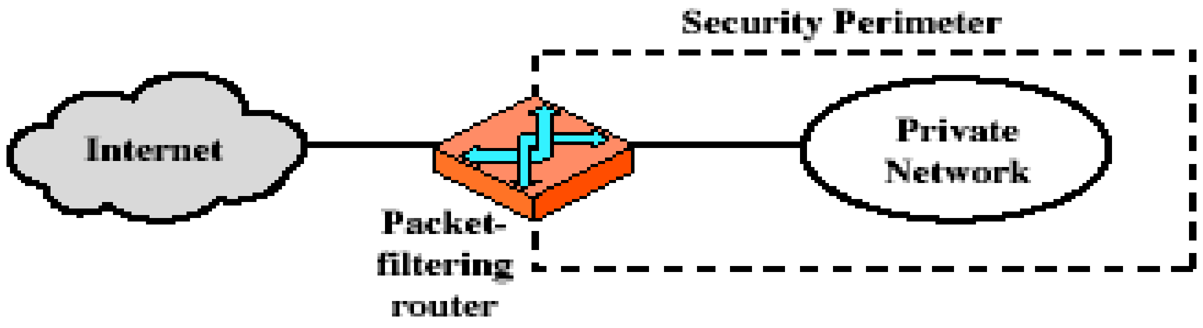
CLASSIFICATION OF FIREWALL

Characterized by protocol level it controls in

- Packet filtering
- Circuit gateways
- Application gateways

- Combination of above is dynamic packet filter

FIREWALLS – PACKET FILTERS



(a) Packet-filtering router

FIREWALLS – PACKET FILTERS

- Simplest of components
- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers

USAGE OF PACKET FILTERS

- Filtering with incoming or outgoing interfaces
  - E.g., Ingress filtering of spoofed IP addresses
  - Egress filtering
- Permits or denies certain services
  - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems

INTRUSION DETECTION

- Used to monitor for “suspicious activity” on a network
  - Can protect against known software exploits, like buffer overflows
- Open Source IDS: Snort, www.snort.org

INTRUSION DETECTION

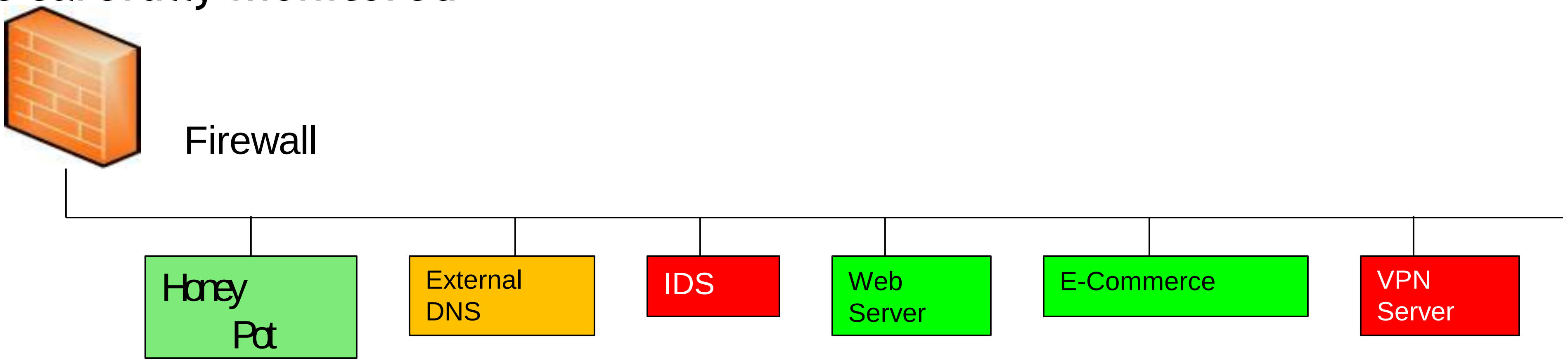
- Uses "intrusion signatures"
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.
- Example
  - IRIX vulnerability in `webdist.cgi`
  - Can make a rule to drop packets containing the line
    - `"/cgi-bin/webdist.cgi?distloc=?;cat%20/etc/passwd"`
- However, IDS is only useful if contingency plans are in place to curb attacks as they are occurring

HONEYPOT & HONEYNET

Honeypot: A system with a special software application which appears easy to break into

Honeynet: A network which appears easy to break into

- Purpose: Catch attackers
- All traffic going to honeypot/net is suspicious
- If successfully penetrated, can launch further attacks
- Must be carefully monitored



4.2: Denial of Service (DoS) Attacks

- What is a DoS attack?
  - An attempt to make a server or network unavailable to legitimate users by flooding it with attack packets
- What is NOT a DoS attack?
  - Faulty coding that causes a system to fail
  - Referrals from large websites that overwhelm smaller websites

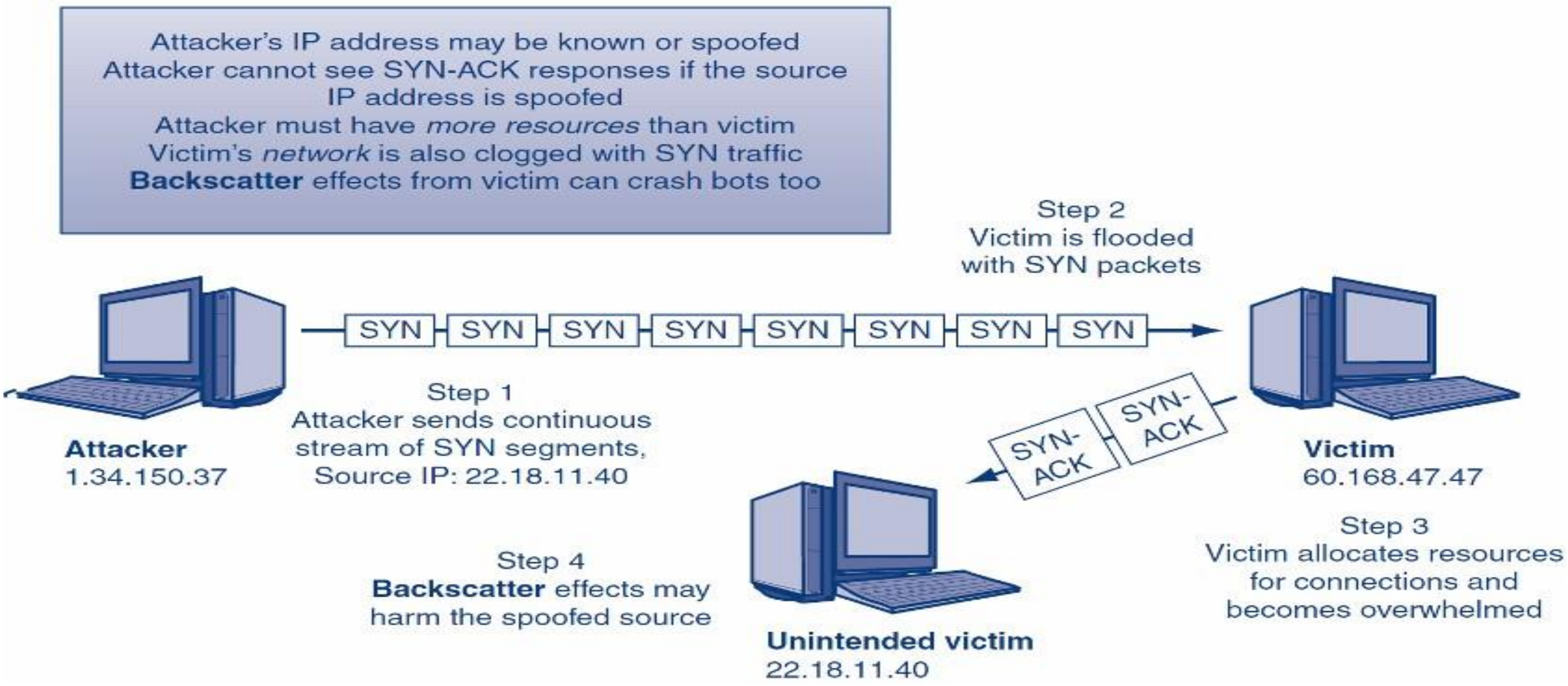
4.2: Goals of DoS Attacks

- Ultimate goal of DoS attacks is to cause harm
  - Harm includes: losses related to online sales, industry reputation, employee productivity, customer loyalty, etc.
- The two primary means of causing harm via DoS attacks include:
  1. Stopping critical services
  2. Slowly degrading services

4.2: Methods of DoS Attacks

- Direct DoS Attack
  - An attacker tries to flood a victim with a stream of packets directly from the attacker's computer
- Indirect DoS Attack
  - The attacker's IP address is **spoofed** (i.e., faked) and the attack appears to come from another computer

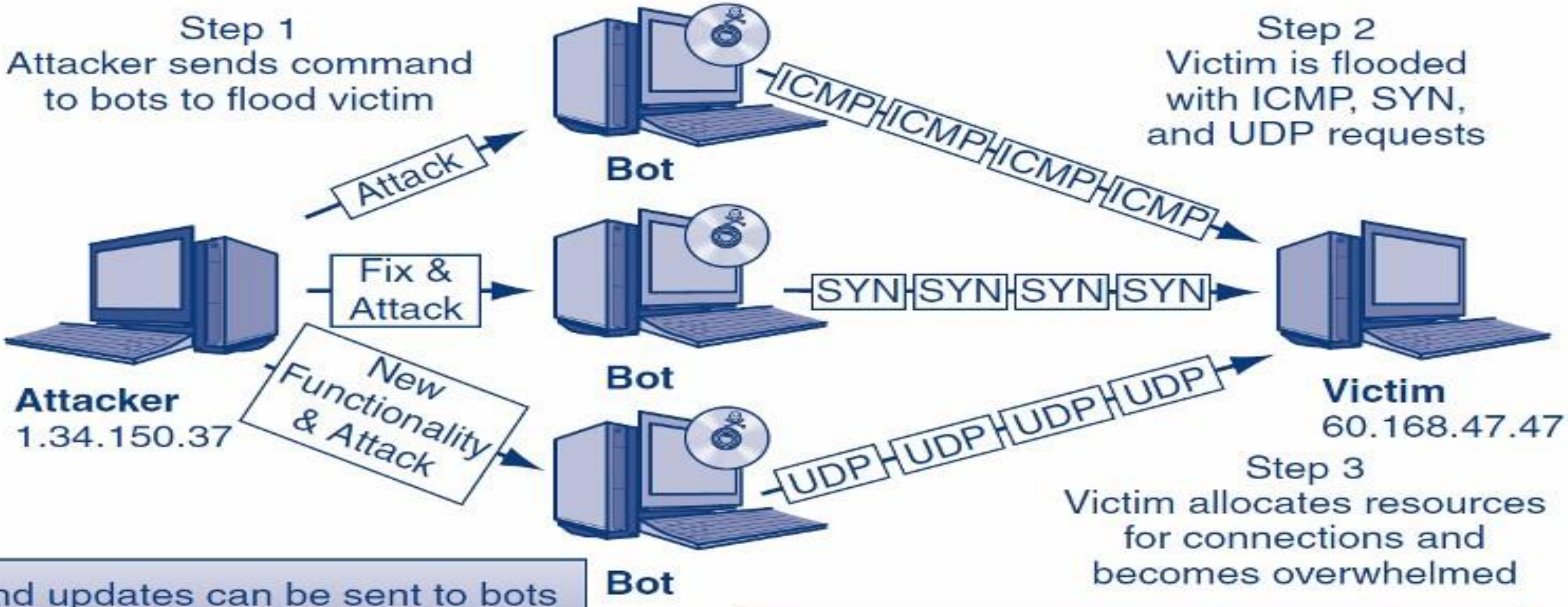
4.2: SYN Flood DoS Attack (Figure 4-1)



4.2: Intermediaries (Bots)

- **Bots**
  - Updatable attack programs
  - Botmaster can update the software to change the type of attack the bot can do
    - May sell or lease the botnet to other criminals
  - Botmaster can update the bot to fix bugs
- Botmaster can control bots via a handler
  - Handlers are an additional layer of compromised hosts that are used to manage large groups of bots

4.2: Fixing and Updating Bots (Figure 4-5)



Fixes and updates can be sent to bots
New **functionality** can be implemented

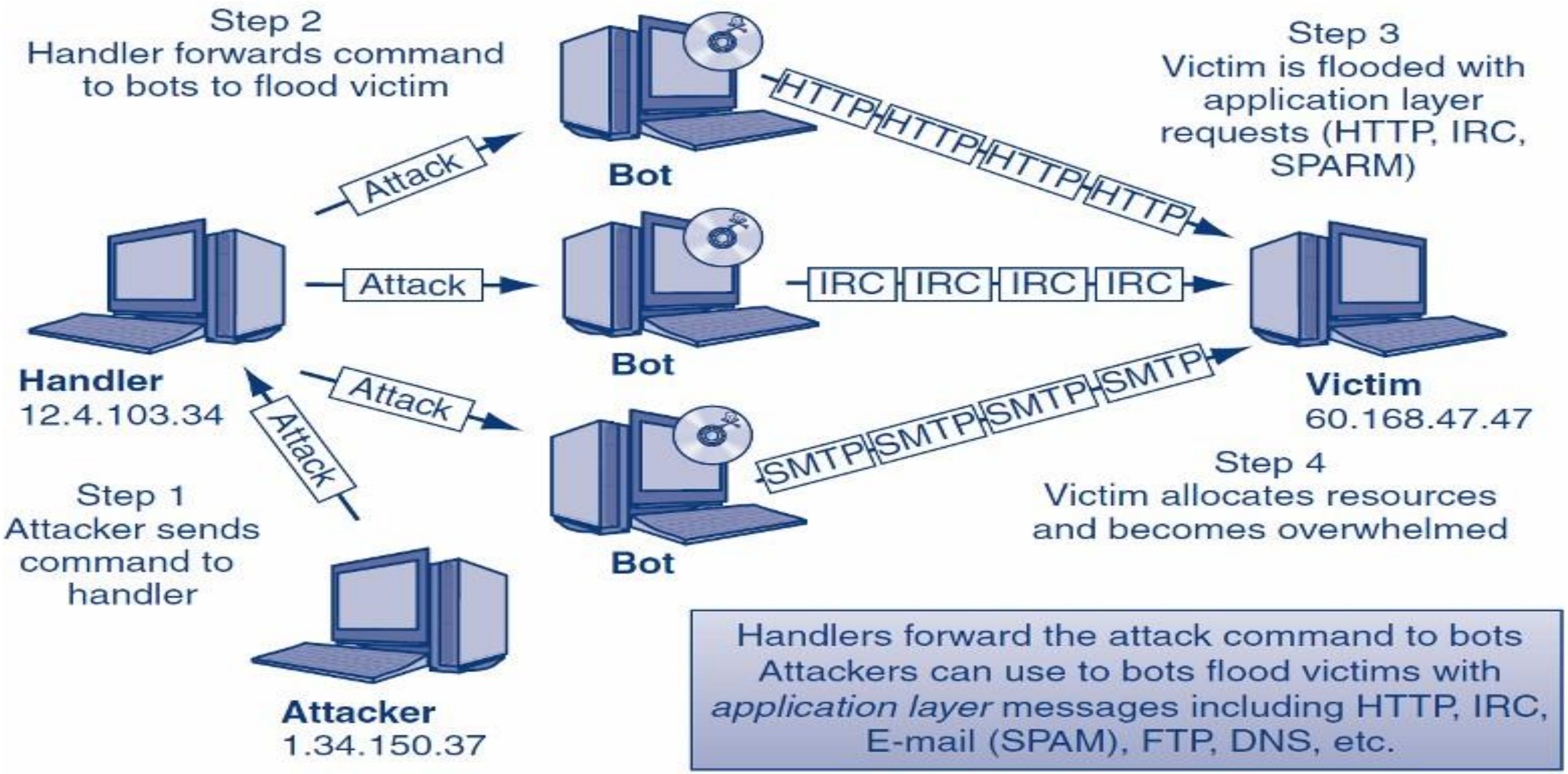
Attacker doesn't directly attack the victim
Attackers can use many bots to flood
victims with different requests including
ICMP (echo), SYN, UDP, etc.

4.2: Types of DoS Packets Sent (Figure 4-4)

- Types of packetssent:

	Name	Description
TCP	Transmission Control Protocol	Guarantees delivery of packets over the Internet
SYN	Synchronize	First part of a three-way TCP handshake to make a network connection
SYN-ACK	Synchronize-Acknowledge	Second part of a three-way TCP handshake sent in response to a SYN
ICMP	Internet Control Message Protocol	Supervisory protocol used to send error messages between computers
HTTP	Hypertext Transfer Protocol	Protocol for sending data over the Web

4.2: DDoS Attack (Figure 4-6)

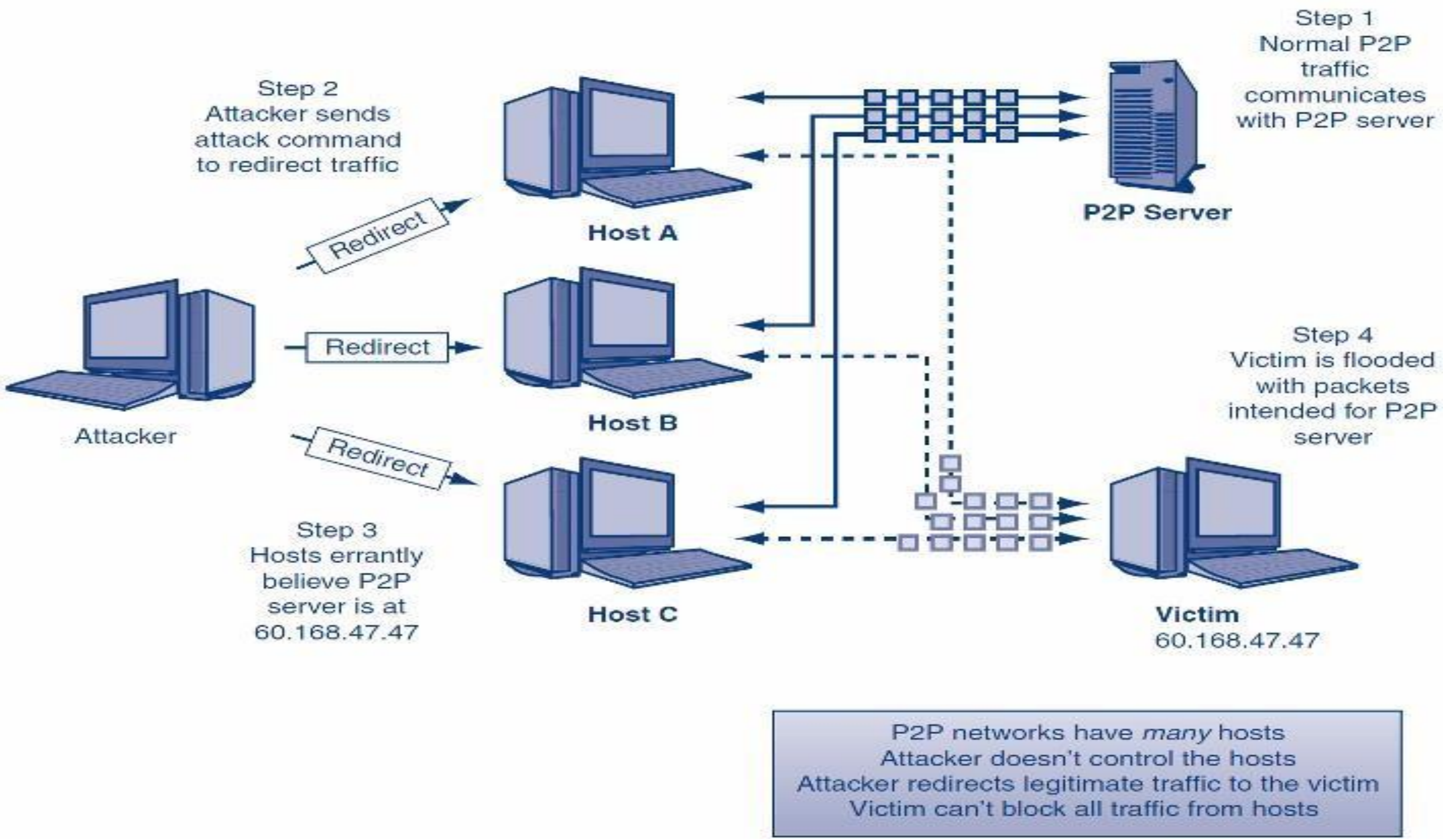


Handlers forward the attack command to bots
Attackers can use to bots flood victims with
application layer messages including HTTP, IRC,
E-mail (SPAM), FTP, DNS, etc.

4.2: P2P DoS Attacks

- **Peer-to-peer (P2P) redirect DoS attack**
  - Uses many hosts to overwhelm a victim using normal P2P traffic
  - Attacker doesn't have to control the hosts, just redirect their *legitimate* P2P traffic

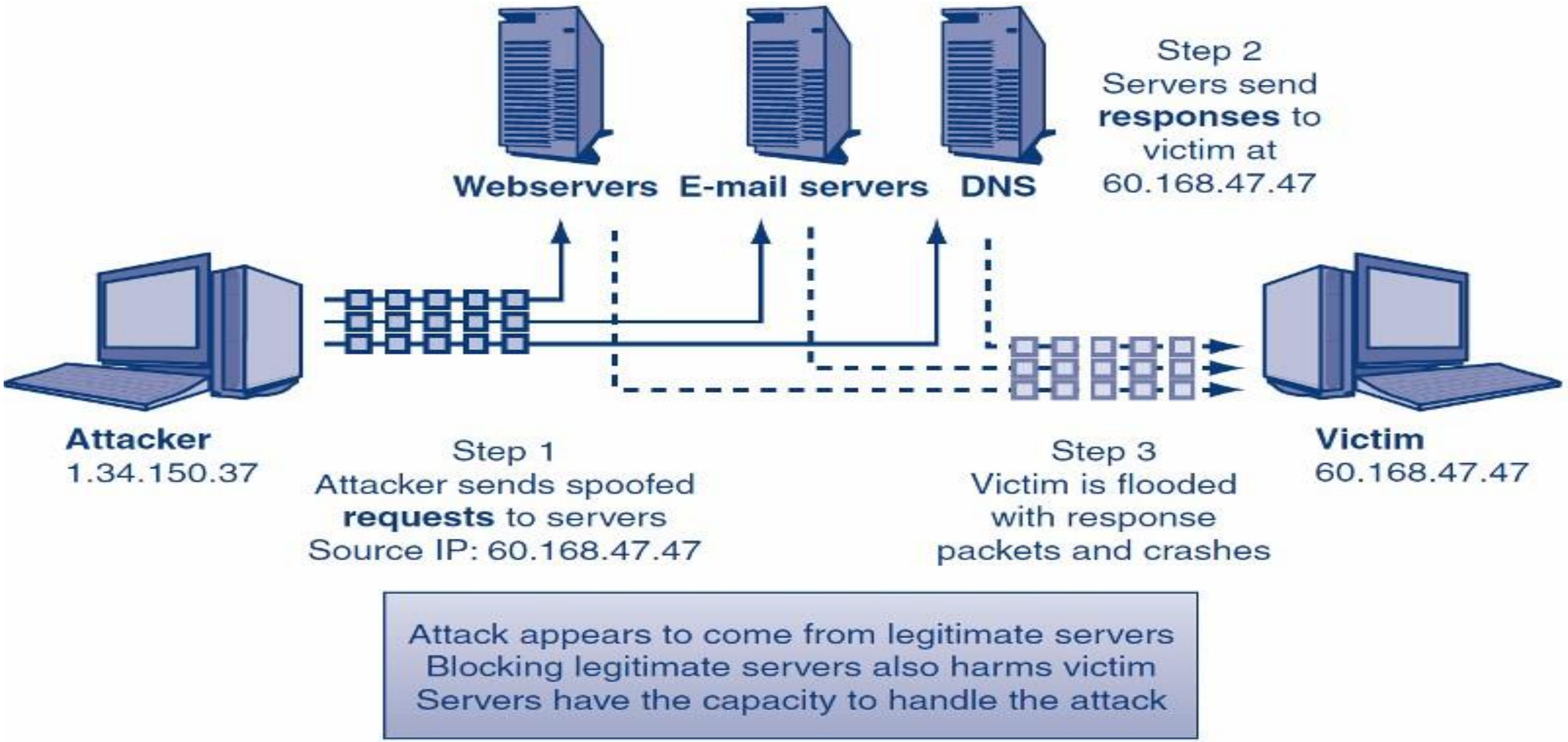
4.2: Peer-to-Peer Redirect Attack (Figure 4-7)



4.2: REFLECTED DOS ATTACKS

- **Reflected DoS attack**
  - Responses from legitimate services flood a victim
  - The attacker sends *spoofed* requests to existing legitimate servers (Step 1)
  - Servers then send all responses to the victim (Step 2)
  - There is no redirection of traffic

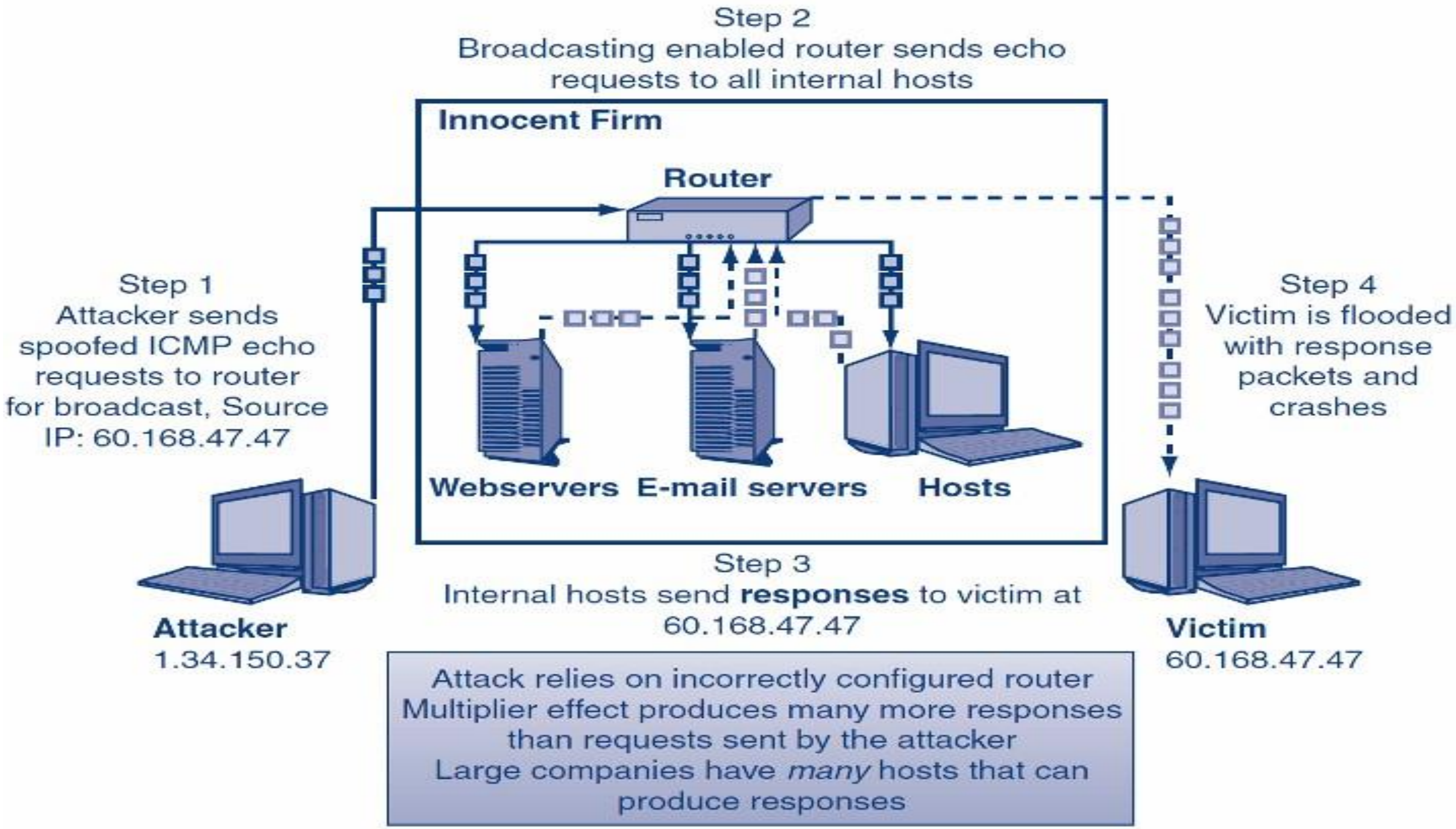
4.2: Reflected DRDoS Attack (Figure 4-8)



4.2: REFLECTED DOS ATTACKS

- Smurf Flood
  - The attacker sends a *spoofed* ICMP echo request to an *incorrectly* configured network device (router)
  - Broadcasting enabled to all internal hosts
  - The network device forwards the echo request to *all* internal hosts (multiplier effect)

4.2: Smurf Flood (Figure 4-9)



4.2: DEFENDING AGAINST DOS ATTACKS

- Black holing
  - Drop all IP packets from an attacker
  - Not a good long-term strategy because attackers can quickly change source IP addresses
  - An attacker may knowingly try to get a trusted corporate partner black holed

4.2: DEFENDING AGAINST DOS ATTACKS

- Validating the handshake
  - Whenever a SYN segment arrives, the firewall itself sends back a SYN/ACK segment, without passing the SYN segment on to the target server (false opening)
  - When the firewall gets back a legitimate ACK the firewall send the original SYN segment on to the intended server
- Rate limiting
  - Used to reduce a certain type of traffic to a reasonable amount
  - Can frustrate attackers, and legitimate users

Security threat analysis

- Threat analysis steps :
  1) Analyze system components and their interactions
  2) Analyze possible damage to C-I-A
  3) Hypothesize possible kinds of attacks

- Network elements to be considered:
  - Local elements
    - Nodes / comm links / data storage / processes / devices / LANs
  - Non-local elements
    - Gateways / comm links / control resources / routers / network resources (e.g., databases)

SECURITY THREAT ANALYSIS

- Network threats:
  - Accessing programs or data at remote host
  - Modifying programs or data at remote host
  - Running a program at a remote host
  - Interception of data in transit
  - Modifying data in transit
  - Insertion of data into communication traffic
    - Incl. replaying previous communication
  - Blocking selected/all traffic
  - Impersonation of entities

- Attack enablers:
  - Size / anonymity / ignorance / misunderstanding
  - Complexity / motivation / programming skills

IMPACT OF NETWORK ARCHITECTURE/ DESIGN & IMPLEMENT. ON SECURITY

- Security principles for good analysis, design, implementation, and maintenance (as discussed in sections on program Security and OS Security) apply to networks

- Architecture can improve security by:

1) Segmentation
2) Redundancy
3) Single points of failure
4) Other means

IMPACT OF NETWORK ARCHITECTURE/ DESIGN & IMPLEMENT. ON SECURITY

1) Segmentation

- Architecture should use segmentation to limit scope of damage caused by network penetration by:
  - Reducing number of threats
  - Limiting amount of damage caused by single exploit
  - Enforces least privilege and encapsulation

- Example 1: component segmentation
  - Placing different components of e-commerce system on different hosts
    - Esp. put on separate host most vulnerable system components
      - E.g., separate host for web server (w/ public access)
  - Exploit of one host does not disable entire system

IMPACT OF NETWORK ARCHITECTURE/ DESIGN & IMPLEMENT. ON SECURITY

- Example 2: access separation
  - Separating from each other:
    - Production system
    - Testing system
    - Development system
  - E.g., no developer has access to production system and no customer has access to development system

IMPACT OF NETWORK ARCHITECTURE/ DESIGN & IMPLEMENT. ON SECURITY

2) Redundancy

- Architecture should use redundancy to prevent losing availability due to exploit/failure of a single network entity
- Example: having a redundant web server (WS) in a company

- Types of redundancy include:
  - *Cold spare* –e.g., when WS fails, replace it manually with spare WS
  - *Warm spare* – e.g., *failover mode* = redundant WSs periodically check each other
  - *Hot spare* – e.g., 3 WSs configured to perform majority voting

IMPACT OF NETWORK ARCHITECTURE/ DESIGN & IMPLEMENT. ON SECURITY

3) Single points of failure (SPF)

- Architecture should eliminate SPFs to prevent losing availability due to exploit/failure of a single network entity
- Using redundancy is a special case of avoiding SPFs
- Network designers must analyze network to eliminate all SPFs
  - Example of avoiding SPF (*without* using redundancy)
    - Distribute 20 pieces of database on 20 different hosts (so called *partitioned database*)
    - Even if one host fails, 95% of database contents (19/20=95%) still available
- Elimination of SPFs (whether using redundancy or not) adds cost

IMPACT OF NETWORK ARCHITECTURE/ DESIGN & IMPLEMENT. ON SECURITY

4) Other architectural means for improving security

- Will be mentioned below as we discuss more network security controls