CSC 519 Information Security

LECTURE 7: Network Security

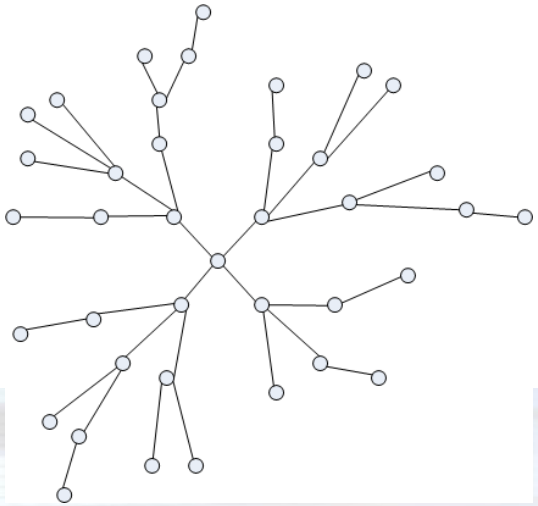
Dr. Esam A. Alwagait
alwagait@ksu.edu.sa

Agenda: Security in networks

- Network concepts
- Network threats
- Network security controls
- Firewalls
- Intrusion Detection/Prevention Systems (IDS/IPS)

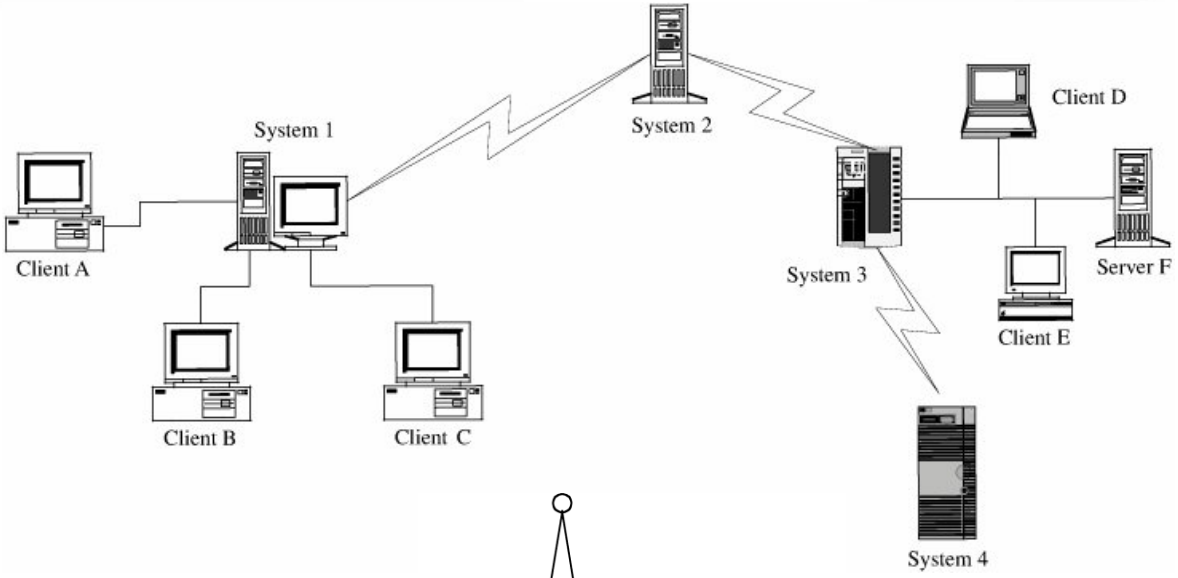
Network concepts

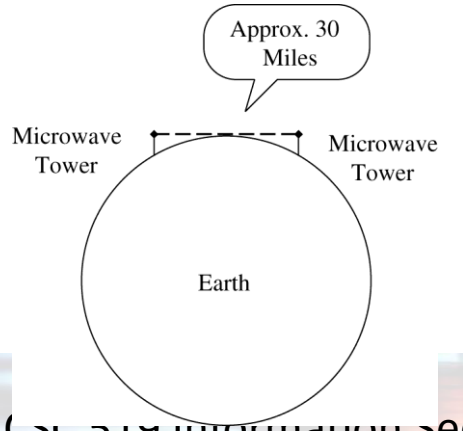
- A **telecommunications network** is a collection of terminal nodes, links and any intermediate nodes which are connected so as to enable telecommunication between the terminals
  - Computer network, telephone network, Internet, etc.
- A **computer network** or data network is a telecommunications network that allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections
- Common topologies
  - Star, ring, bus, mesh, tree
- Organizational scope
  - Intranet, extranet, Internet



Network concepts

- **Single point of failure**: one cut to the network destroys communication functionality
- **Network resilience/fault tolerance:** there is more than one way to get from the source to your neighborhood





Characteristics of the Internet

- No single entity that controls the Internet
- Traffic from a source to a destination likely flows through nodes controlled by different, unrelated entities
- Packets actually could be routed through different paths
- Different types of nodes along the way!
  - Server, laptop, router, switches, UNIX, Windows,
- Different types of communication links
  - Wireless, wired

ISO OSI Model, TCP/IP protocol stack

Layer	Name	Activity
7	Application	User-level data
6	Presentation	Standardized data appearance, blocking, text compression
5	Session	Sessions or logical connections between parts of an application; message sequencing, recovery
4	Transport	Flow control, end-to-end error detection and correction, priority service
3	Network	Routing, message blocking into uniformly sized packets
2	Data Link	Reliable data delivery over physical medium; transmission error recovery, separating packets into uniformly sized frames
1	Physical	Actual communication across physical medium; individual bit transmission

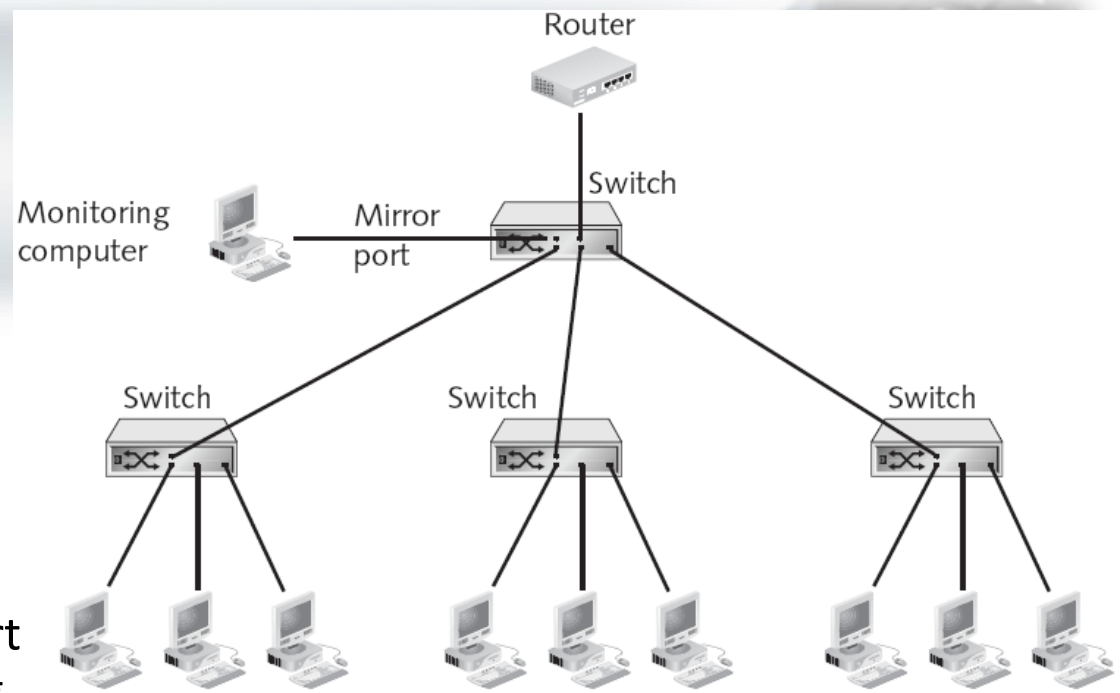
Layer	Action	Responsibilities
Application	Prepare messages form	user interactions, addressing
Transport	Convert messages to packets	Sequencing, reliability (integrity), error correction
Internet	Convert packets to datagrams	Flow control, routing
Physical	Transmit datagrams as individual bits	Data communication

Threats in networks

- Reconnaissance techniques
  - Port scanning
    - To distinguish between multiple applications running on the same server, each application runs on a “port"
    - Port scanning reveals running ports, services, applications, and OS
    - E.g., a web server typically (http) runs on port 80, smtp on 25, pop on 110, etc.
    - Example tools: Nmap, Nessus, etc.
  - Social engineering
    - using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack
  - Intelligence
    - gathering discrete bits of information from various sources and then putting them together like the pieces of a puzzle
    - Google, social networks!
  - Operating System and Application Fingerprinting

Threats in networks

- Threats in transient
  - Eavesdropping
    - overhearing without expending any extra effort
  - Wiretapping
    - intercepting communications through some effort
    - Passive: just listening, active: injecting something in the communication
  - Communication media
    - Cable, optical fiber,
      - Port mirroring, network tap
    - WiFi
      - Easily done
      - Can be done from kilometers away using directed antenna
      - Physical barriers are not helping!



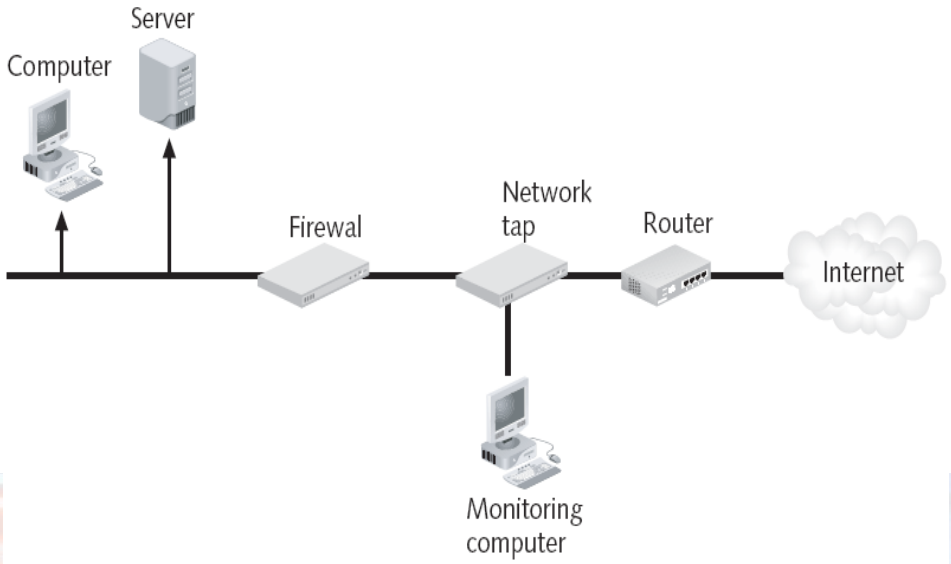
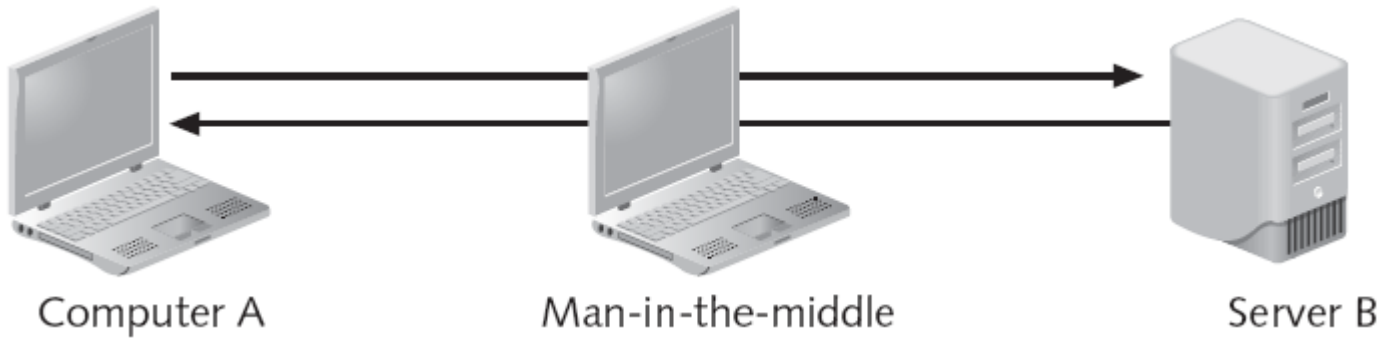


Figure 4-3 Network tap

Threats in networks

- Impersonation
  - Falsely representing a valid entity in a communication
    - Impersonate a person by stealing his/her password
    - Guessing attack
    - Exploit default passwords that have not been changed
- Spoofing
  - An object (node, person, URL, Web page, email, WiFi access point, etc.) masquerades as another one
  - URL spoofing (web page and URL spoofing used in phishing attacks)
    - Exploit typos: www.ksuu.com.sa
    - Exploit similarities: www.paypa1.com

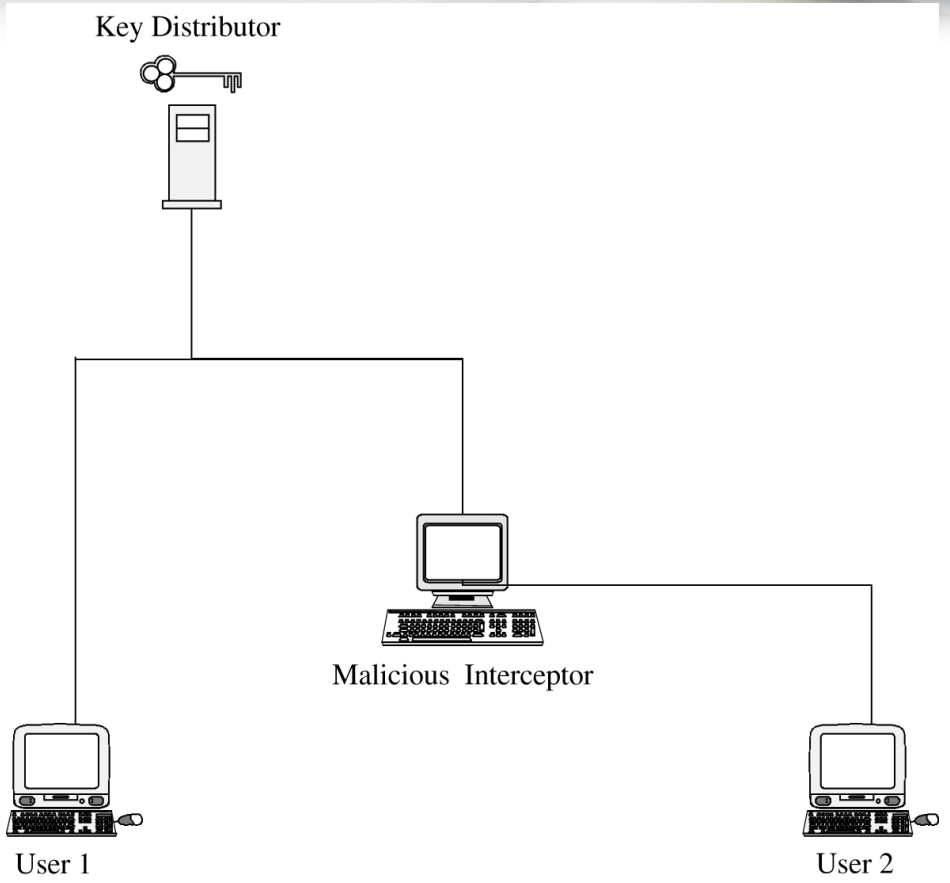
Threats in networks



- Session hijacking
  - TCP sessions
    - TCP protocol sets up state at sender and receiver end nodes and uses this state while exchanging packets (using e.g., sequence numbers for detecting lost packets)
    - Attacker can hijack such a session and masquerade as one of the endpoints
  - Web servers sometimes have client store cookies to re-identify client for future visits
    - Attacker can sniff or steal cookie and masquerade as client
  - Replay attack
    - Attacker captures data and resent it at a later time

Threats in networks

- Session hijacking (Continued)
  - Man-in-the-middle attacks are similar, attacker becomes stealth intermediate node, not end node.
    - usually participates from the start of the session
- Traffic analysis



Key Interception by a Man-in-the-Middle Attack

Threats in networks

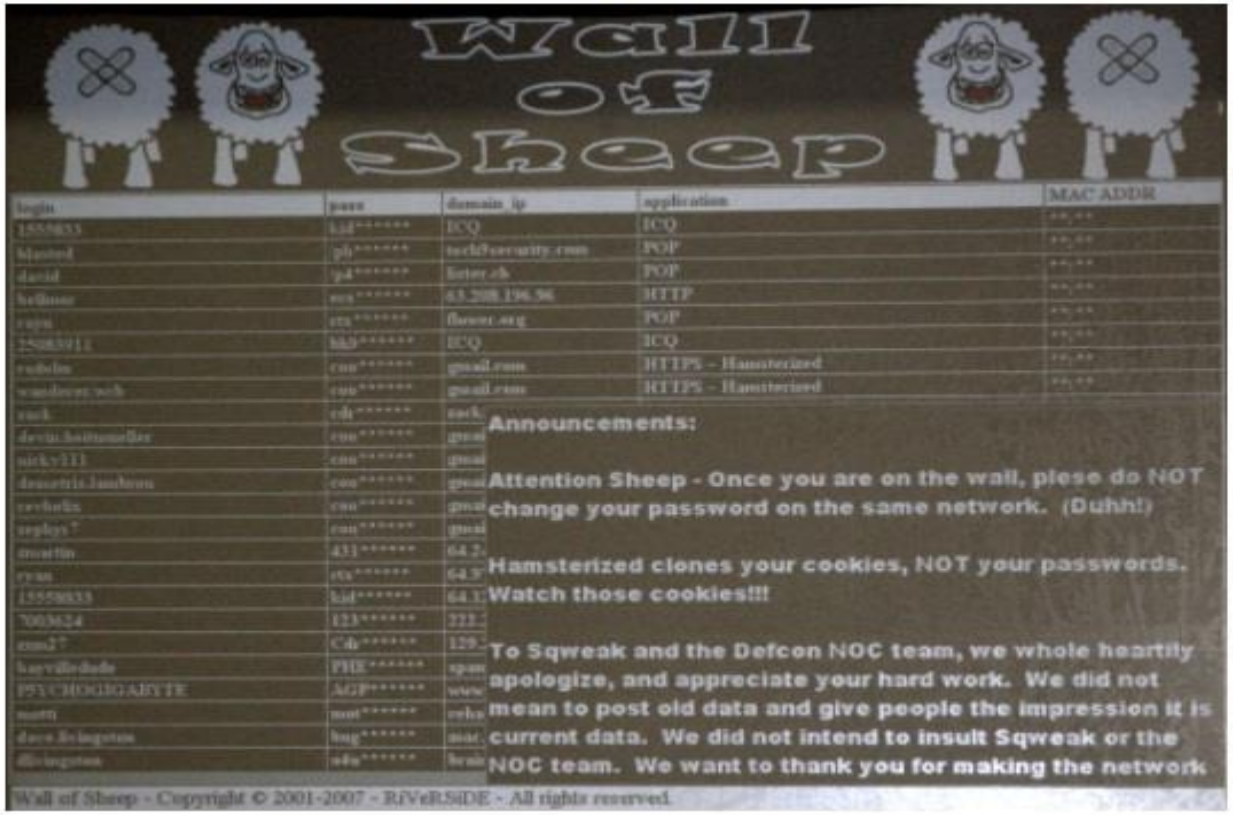
- Wall of Sheep!
- Captured passwords projected on the wall at DEFCON

DEFCON 2007 - Wall of Sheep (shame)

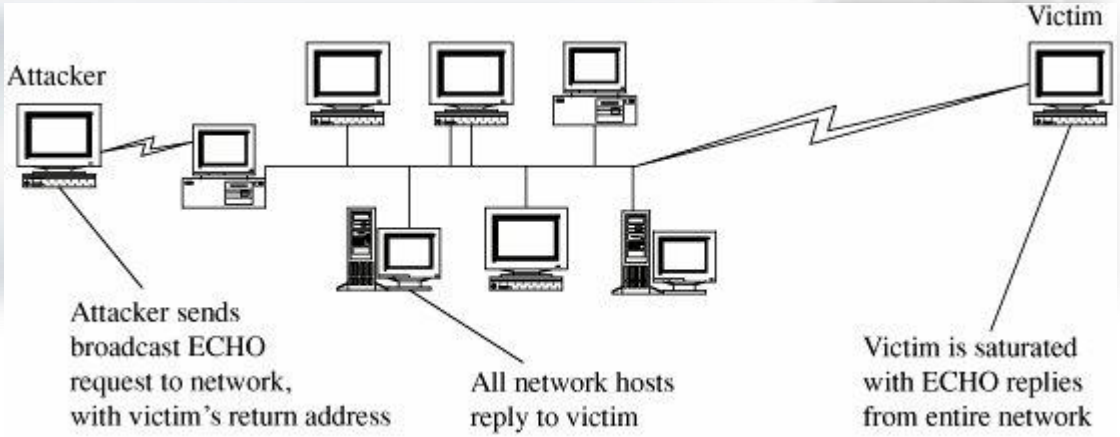
Posted by George Ou @ 11:38 pm

Categories: Infrastructure, Mobile/Wireless, Networking, News, Security
Tags: Google Gmail, Wall, George Ou

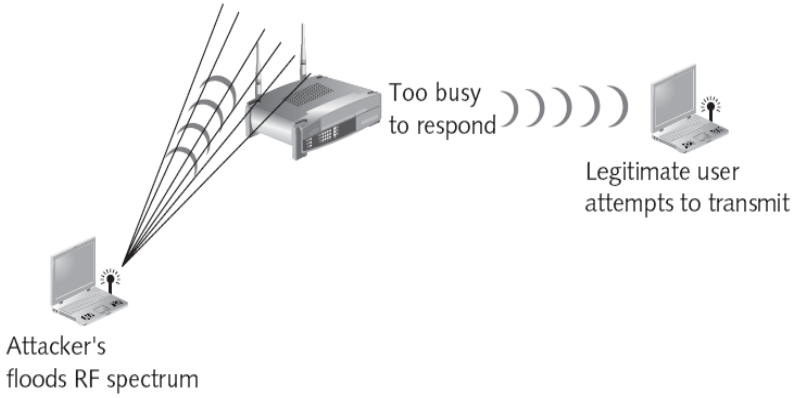
It's time to count sheep again and I don't mean the ones in your sleep. I'm talking about the ones on the Wi-Fi Hotspot that are using insecure protocols and getting their online accounts compromised. What you're looking at below is the DEFCON 15 Wall of Sheep.

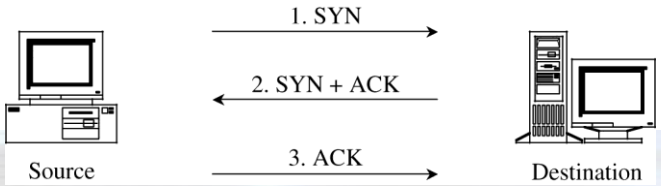


Threats in network



- Denial of Service (DOS)
  - Cutting wire of jamming wireless signal
  - Flooding a node by overloading its network connection or its processing capacity
  - Ping flood
    - Node receiving a ping packet is expected to generate a reply
    - Attacker could overload victim
    - Different from “ping of death", which is a malformatted ping packet that crashes victim's computer
  - Smurf attack (uses ping packet)
    - Spoof address of sender end node in ping packet by setting it to victim's address
    - Broadcast ping packet to all nodes in a LAN
  - Sync flood
    - Uses session-oriented connections of TCP protocol (e.g., Telnet)
  - DNS Attacks
    - poisoning DNS cache so that packets get routed to the wrong host

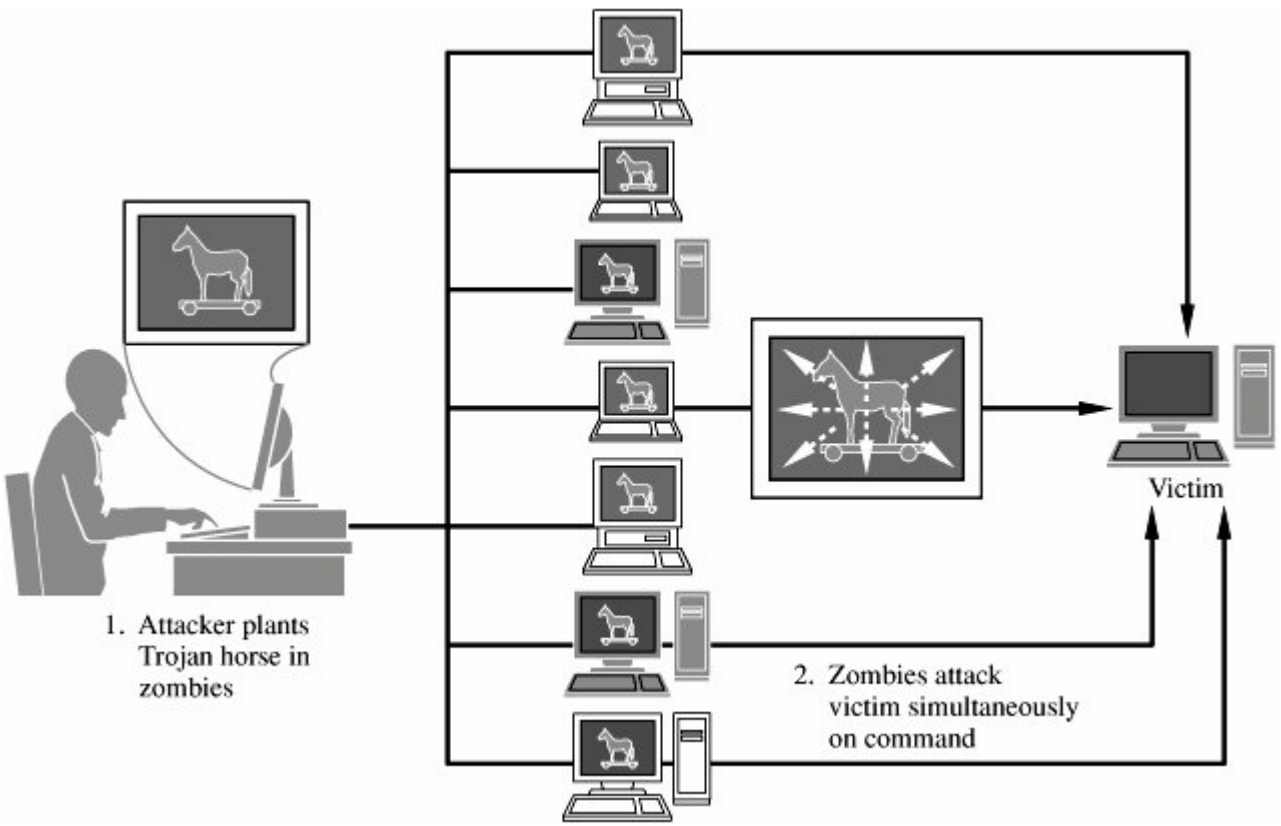




Threats in network

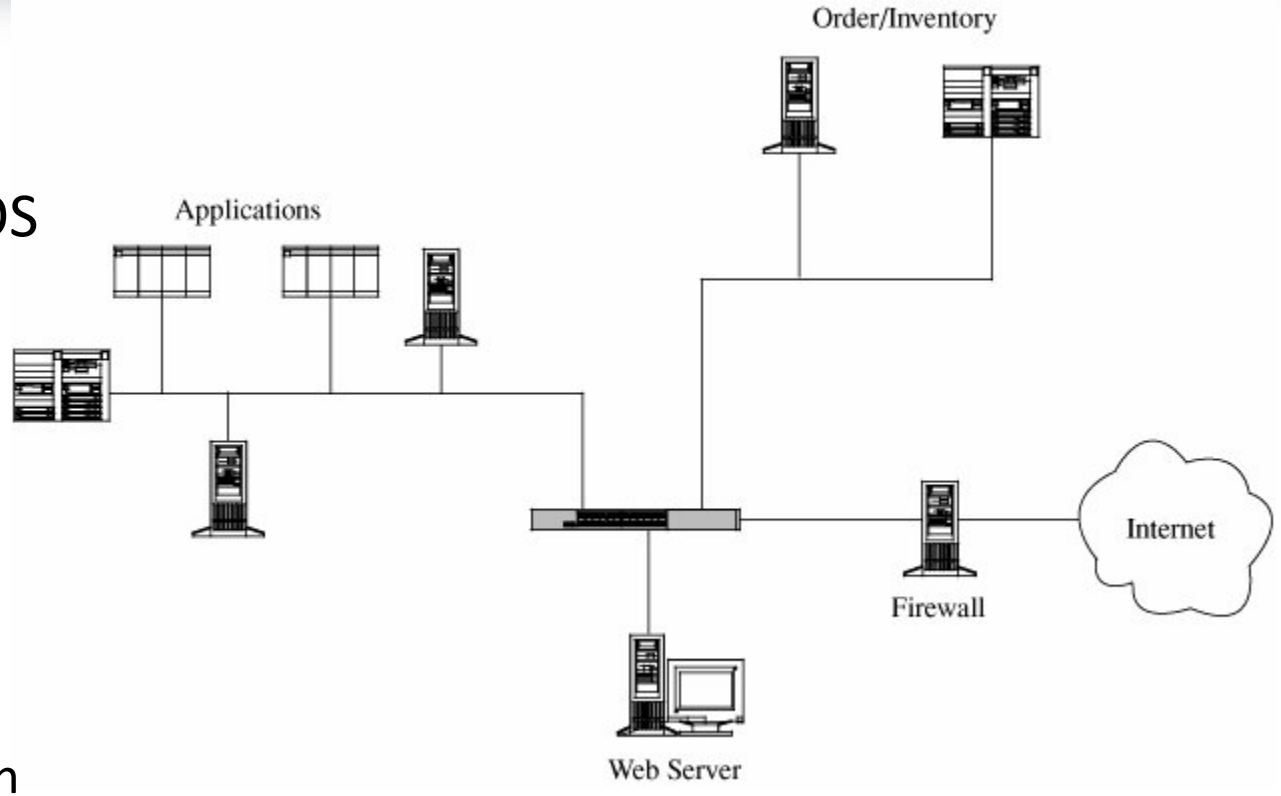
Distributed Denial of Service (DDoS)

- A variant of DOS attack
- May use hundreds or thousands of zombie computers in a botnet to flood a device with requests
- It employs multiplicative effects of attacks
  - Attacker does two things:
    - the attacker uses any convenient attack (such as exploiting a buffer overflow or tricking the victim to open and install unknown code from an e-mail attachment) to plant a Trojan horse on a target machine (creating a **zombie**)
    - sends a signal to all the zombies to launch the attack



Network security controls

- Design and implementation
  - Use controls against security flaws demonstrated earlier (program controls, OS controls, etc.)
- Architecture
  - Segmentation
    - Like OS, it limits the potential of a harm
  - Redundancy
    - Avoid single points of failure!
    - allowing a function to be performed on more than one node, to avoid "putting all the eggs in one basket."



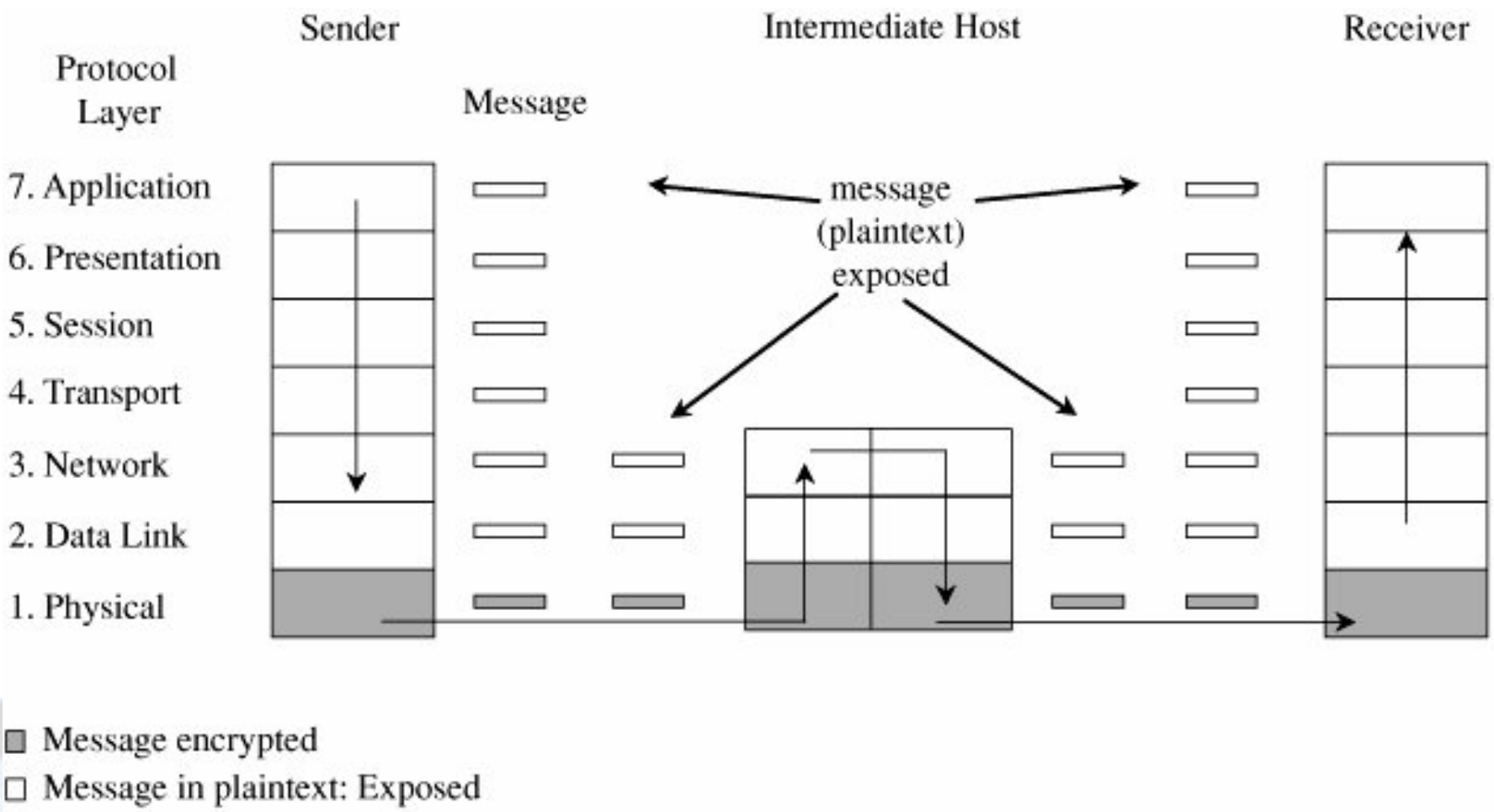
Network security controls

- Access Controls
- ACLs on routers
  - All traffic to an organization typically goes through a single (or a few) routers
  - In case of flooding attack, define router ACL that drops packets with particular source and destination address
  - ACLs can be complicated for high traffic routers
  - Difficult to gather logs for forensics analysis
  - Source addresses of packets in flood are typically spoofed and dynamic
- Honeypots
  - A computer system open to attackers (unprotected computer)!
  - Watch what attackers do, help identify and stop attackers, mislead attackers

Network security controls

Link encryption

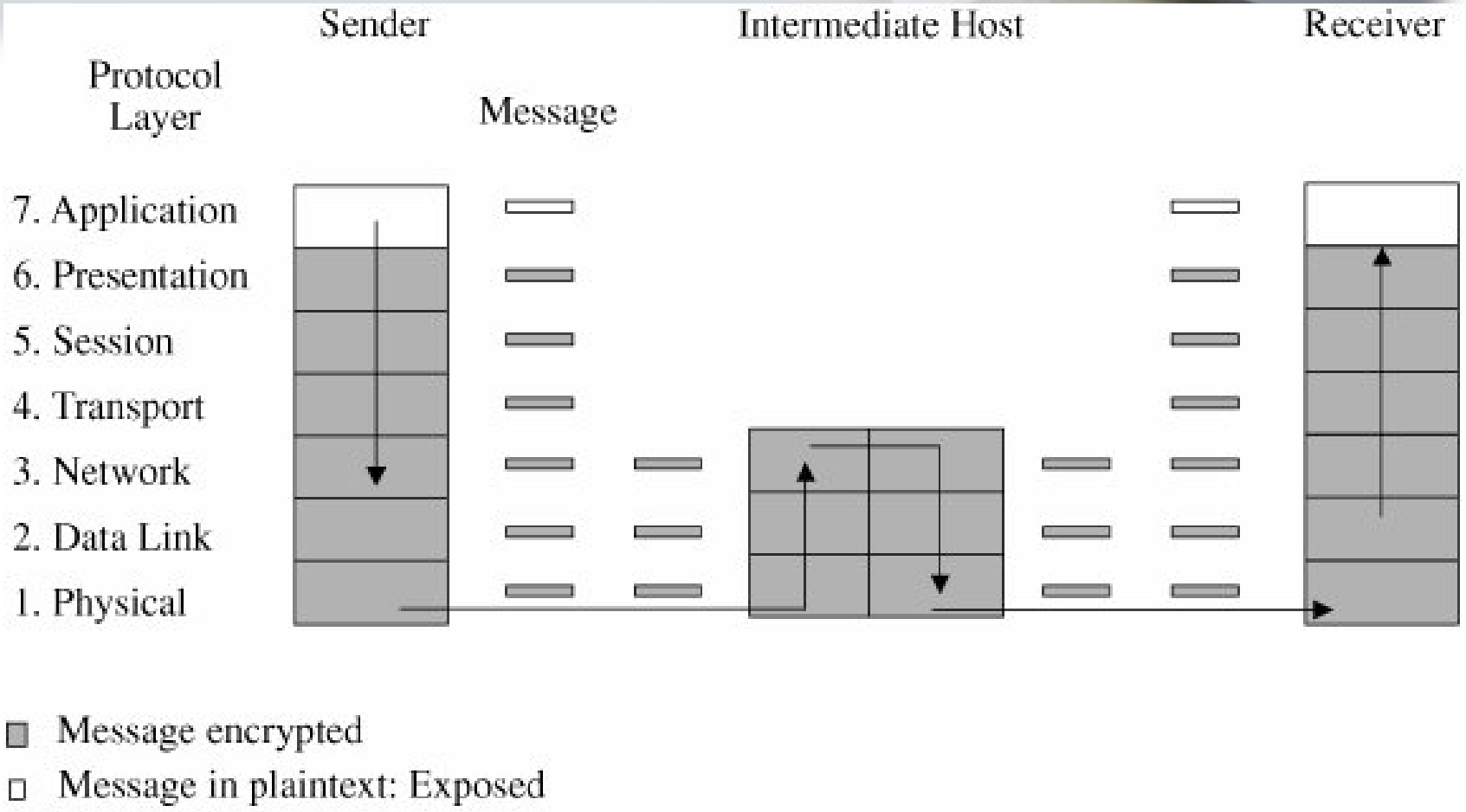
- data are encrypted just before the system places them on the physical communications link
- decryption occurs just as the communication arrives at and enters the receiving computer
- Encryption/decryption occurs at layer 1 or 2 in the OSI model
- More common to use hardware



Network security controls

End-to-End encryption

- the encryption/ decryption is performed at the highest levels (layer 7, application, or perhaps at layer 6, presentation) of the OSI model
- Can be HW or SW
  - SSL for secure browsing
  - S/MIME for secure email



Network security controls

Firewalls

- A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network
- A firewall's primary function is filtering
  - Where a router's primary function is addressing
- Firewalls can also do auditing, can examine an entire packet's contents, including the data portion
  - whereas a router is concerned only with source and destination MAC and IP addresses
- Firewalls cannot protect inside hosts from attacks originating from the inside network

Network security controls

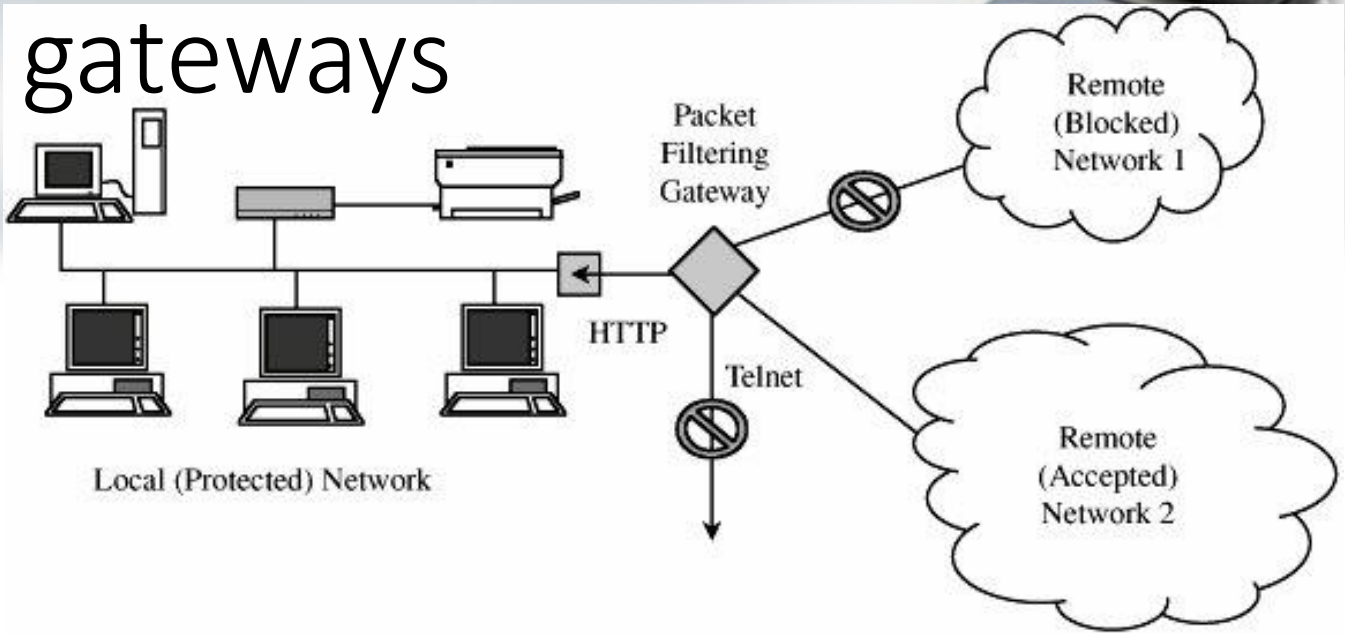
Firewalls have a wide range of capabilities:

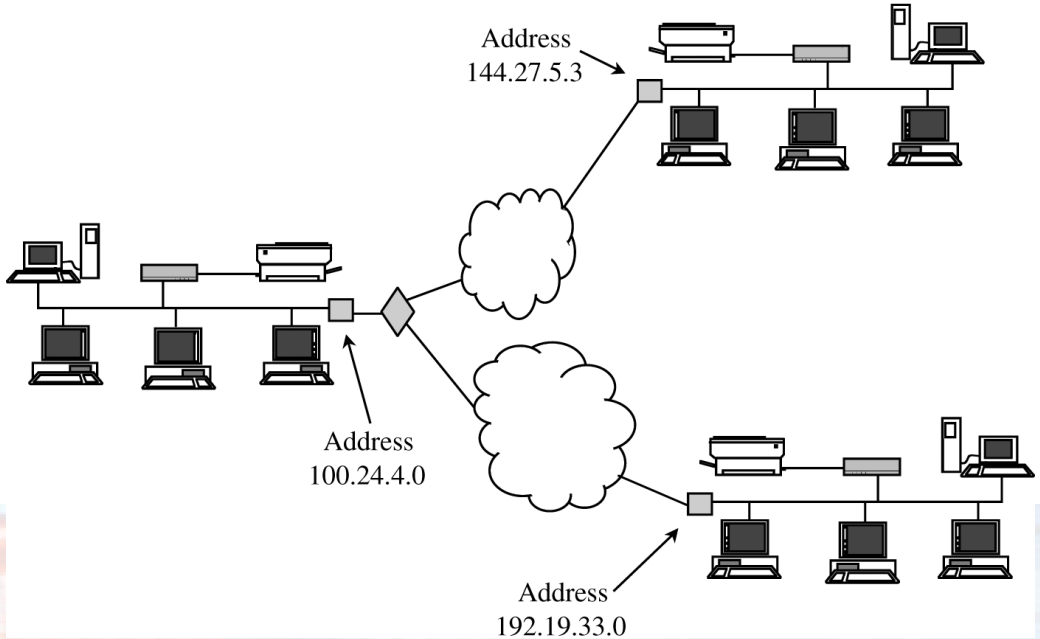
- packet filtering gateways (or screening routers)
- stateful inspection firewalls
- application proxies (or bastion hosts)
- personal firewalls

- Each type performs different functions, no one is completely right and the others are wrong

Firewalls: Packet filtering gateways

- It is the simplest one
- Make decision based on header of a packet
  - source and destination addresses and port numbers
  - port numbers can be used to determine type of packets
  - Examples: 80 for Web, 22 for SSH
- E.g., allow Web, but not SSH
- Packet filters do not "see inside" a packet
  - Ignore packet payload
  - Thus cannot perform sophisticated filtering
- Can drop some spoofed traffic
  - Can drop packets originating from inside KSU with source address from outside (and vice versa)



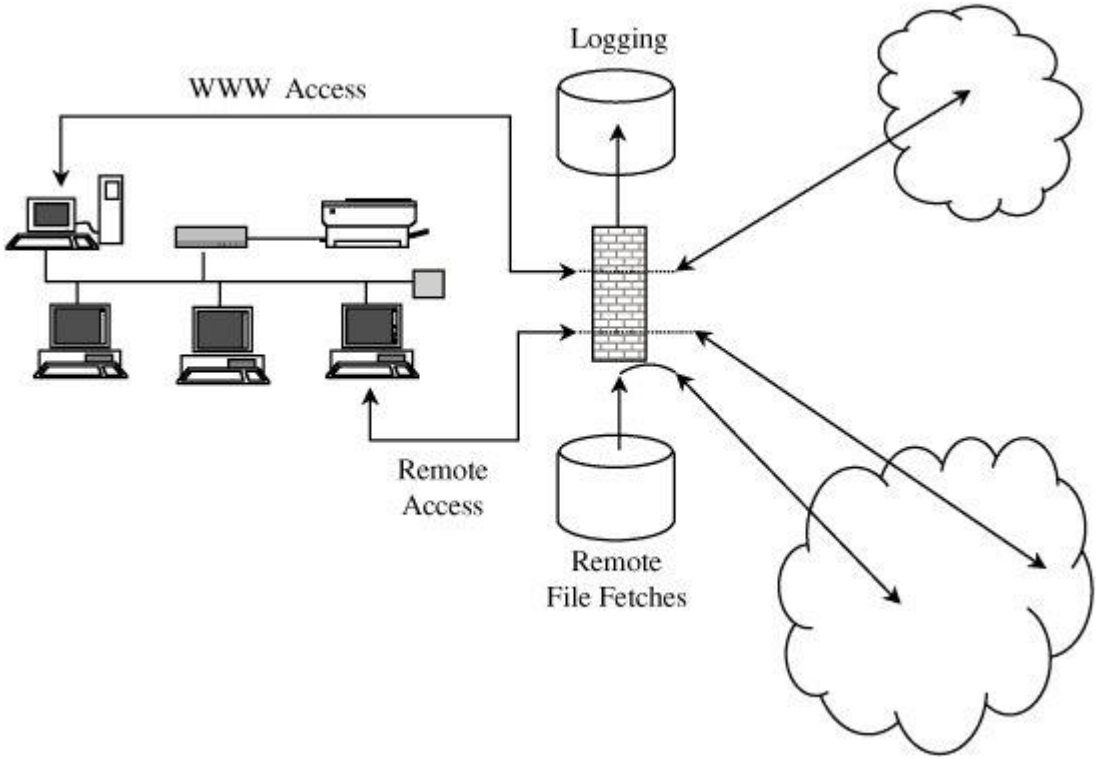


Firewalls: Stateful Inspection Firewall

- More expensive
- Maintains state information from one packet to another in the input stream
  - When a client within the company opens a TCP connection to a server outside the company, firewall must recognize response packets from server and let (only) them through
- One classic attack approach is to break an attack into multiple, very short packets so that a firewall cannot detect the signature of an attack
- So firewall might have to re-assemble packets for stateful inspection

Firewalls: Application Proxy

- specific for applications
- It is a two-headed device: It looks to the inside as if it is the outside (destination) connection, while to the outside it responds just as the insider would
- Has full knowledge about communication and can perform sophisticated processing
- Examples:
  - FTP protocol: might accept get commands, reject put commands, and filter the local response to a request to list files
  - RDMS queries: restricting queries that return the mean of a set of fewer than five values

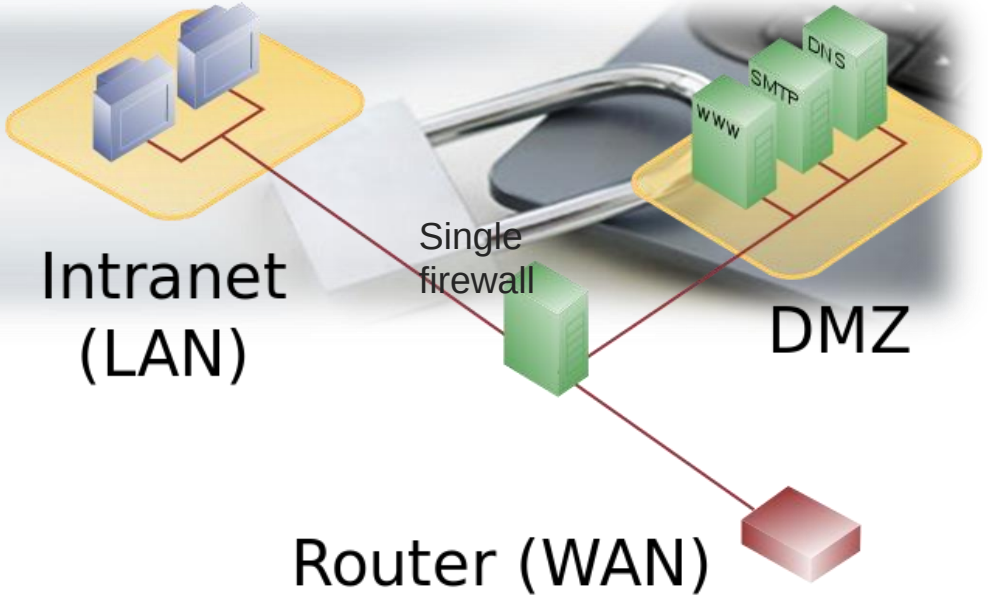


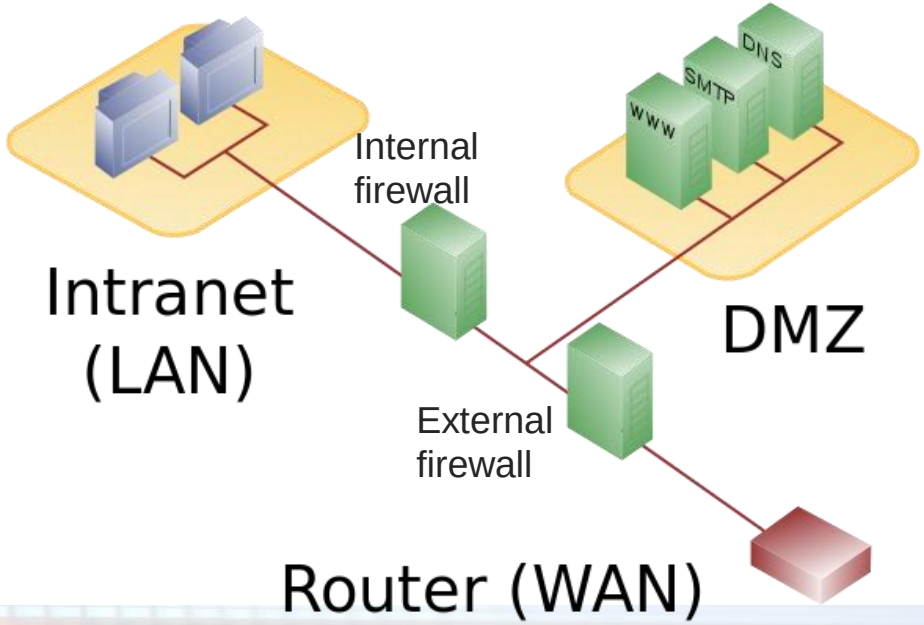
Firewalls: Personal Firewalls

- It is an application program that runs on a workstation to block unwanted traffic, usually from the network
- Normally configured to enforce some policy
  - Example: computers on the company network are highly trustworthy, but outside hosts are not
- Can also generate log files
- Recently, it is more common in software versions in combination with a virus scanner/malware protection tools

Demilitarized Zone (DMZ)

- It is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet
- Main goal is adding additional layer(s) of security to local networks from external sources
  - external attacker only has direct access to equipment in the DMZ, not the internal network resources
- The most common DMZ services:
  - Web servers, mail servers, FTP servers, DNS servers, VoIP servers
- Usually exists in:
  - Single firewall setup
    - At least 3 network interfaces separating internal network, DMZ resources, and external world
  - Dual firewall setup (more secure)
    - External firewall protects DMZ (thus only allows traffic to DMZ)
    - Internal firewall protects internal network from attacks lodged in DMZ (only allows traffic from DMZ)





Source: Wikipedia

Intrusion detection systems (IDSs)

- Primarily a detection mechanism, which complement prevention mechanisms such as firewalls
  - Next line of defense (defense-in-depth concept, which means multiple layers of defense)
- Typically is another separate computer that monitors activity to identify malicious or suspicious events
  - Receives events from sensors
  - Stores and analyzes them
  - Takes actions, if necessary
    - Writing to log files/servers
    - Making phone calls/sms messages/emails, etc.
    - Enable/disable certain ACLs/traffic
- Exists in different types:
  - Host-based and network-based IDSs
  - Signature-based and heuristic/anomaly-based IDSs
  - Passive and reactive detection systems
    - Reactive IDS is also called intrusion prevention system (IPSs)