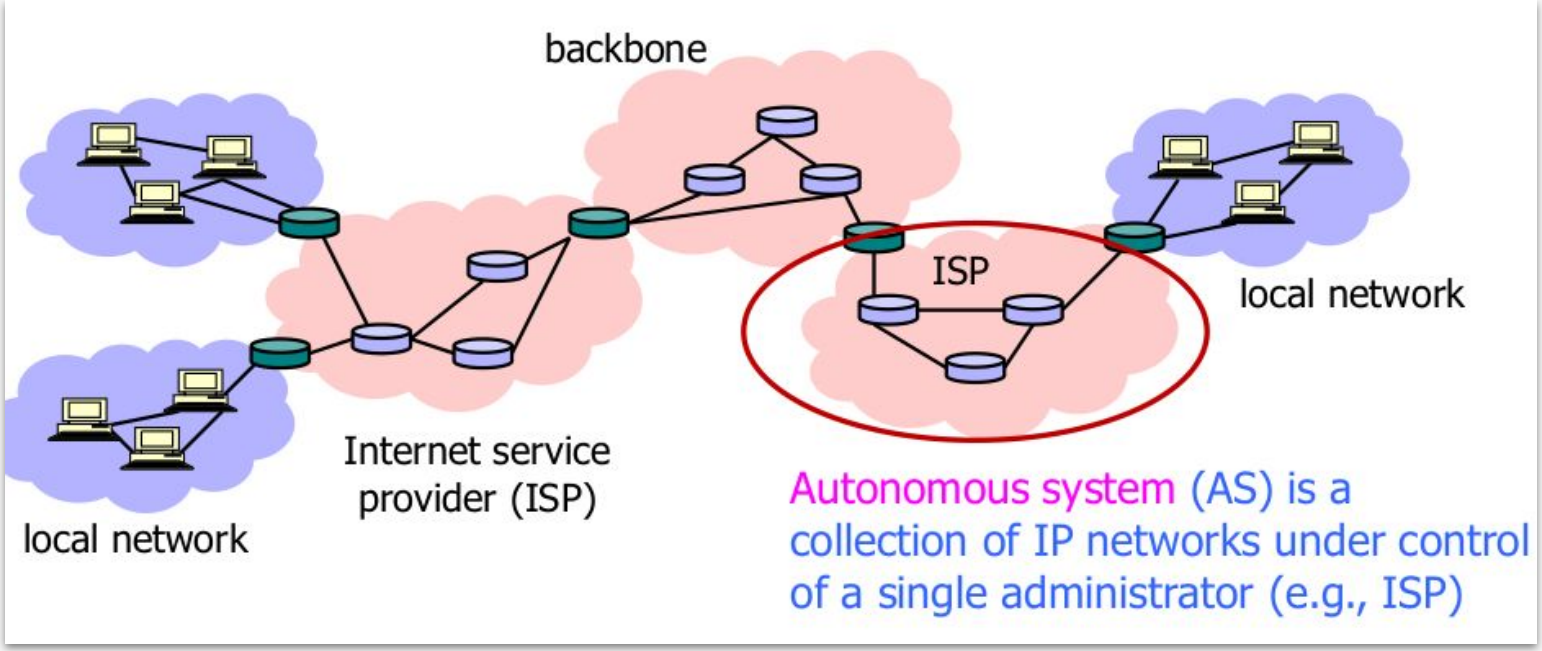
Network Security

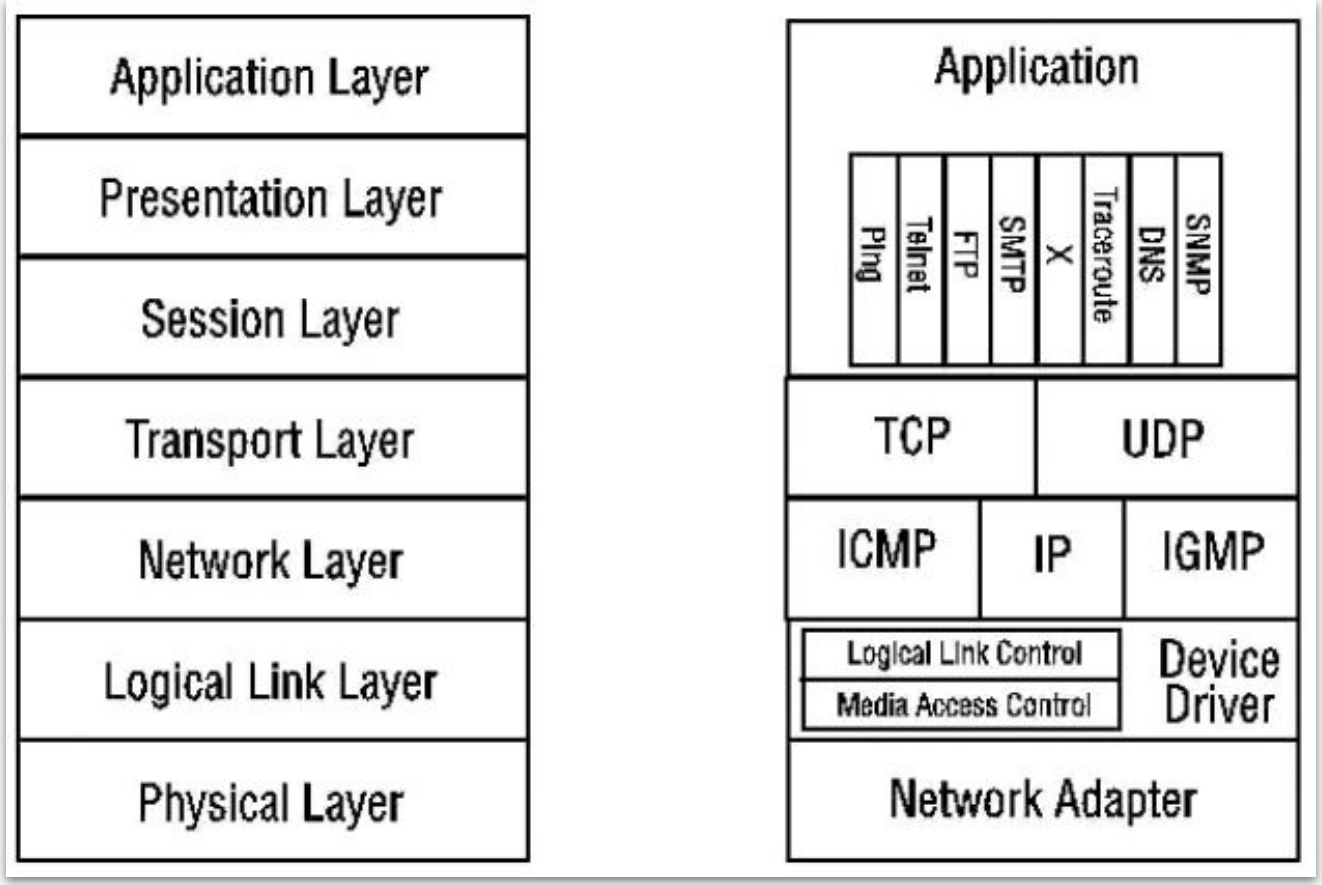
Mustakimur R. Khandaker

Internet Is a Network of Networks

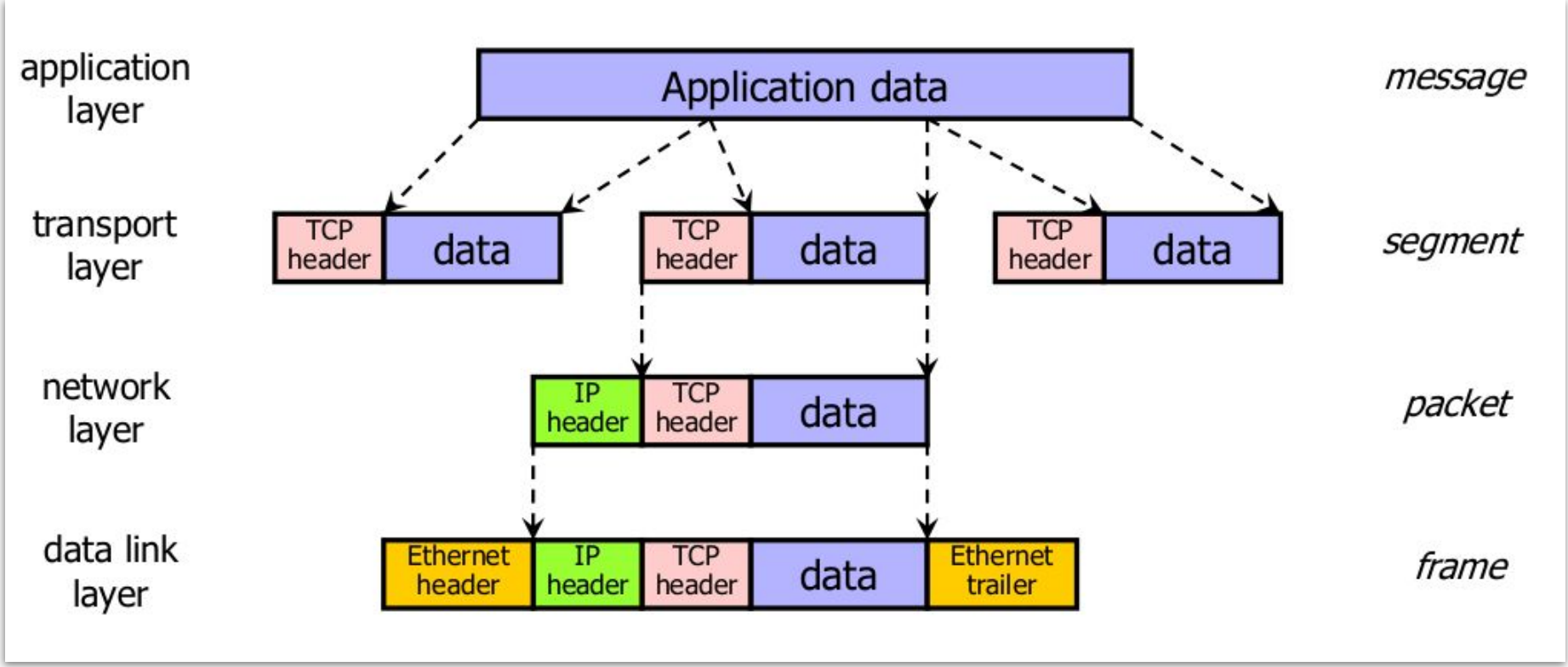


- TCP/IP for packet routing and connections.
- Border Gateway Protocol (BGP) for route discovery.
- Domain Name System (DNS) for IP address discovery.

OSI Reference Model



Data Formats



Expectation & Attacks

Desired properties (Assets):

- Confidentiality.
  - Packet sniffing.
- Integrity.
  - Session hijacking.
- Availability.
  - Denial of service attacks.
- Common.
  - Address translation poisoning attacks.
  - Routing attacks.

Types of attack (Adversaries):

- Passive attack.
  - Eavesdrop but do not modify.
- Active attack.
  - Transmit, replay, modify, delete messages from network, covert channels.
- Local vs remote attacks.

Threats

Network protocols have no integrity or confidentiality.

Vulnerabilities in network services enable remote exploits.

End-to-end argument - dumb network:

- If you want security (or anything else) then get it.
- But what if the ends are incompetent? Or what if only “one end” supports it?

Physical Layer Attacks

Wire taps:

- 1970: U.S. learned of USSR undersea cable.
  - Connected Soviet naval base to fleet headquarters.
- Joint US Navy, NSA, CIA operation to tap cable in 1971.
  - Saturation divers installed a 3-ft long tapping device.
  - Coil-based design, wrapped around cable to register signals by induction.
  - Communication on cable was unencrypted.

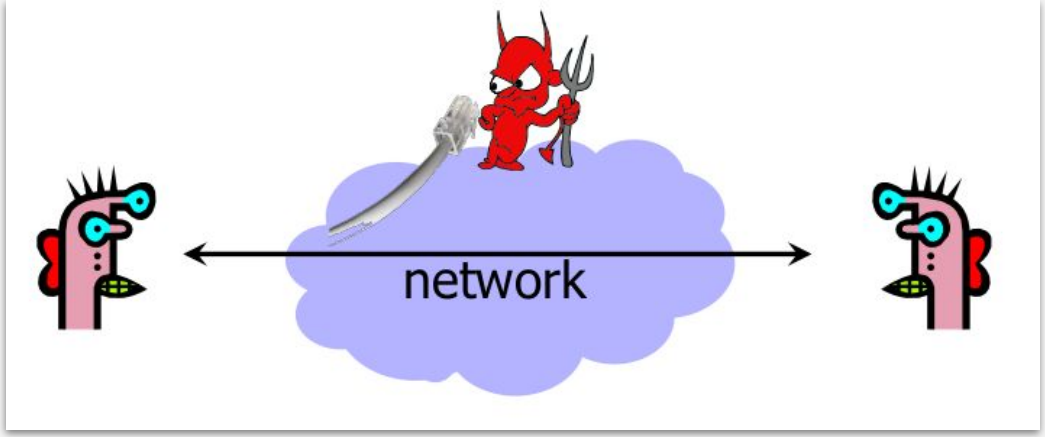
Wireless Sensor Network (WSN):

- Health care monitoring.
- Smart home.
- Industrial IoTs.

Packet Sniffing

Many applications send data unencrypted.
- ftp, telnet send passwords in the clear.

Network interface card (NIC) in *"promiscuous mode"* reads all passing data.



Solution: encryption (e.g., IPsec, HTTPS), improved routing.

Other Attacks

Ping of Death:
If an old Windows machine received an ICMP packet with a payload longer than 64K, machine would crash or reboot.

- Programming error in older versions of Windows.
- Packets of this length are illegal, so programmers of Windows code did not account for them.

Teardrop:
TCP fragments contain Offset field.

- Attacker sets Offset field to overlapping values.
  - Bad implementation of TCP/IP will crash when attempting to re-assemble the fragments.

Smurf Attacks

Broadcast IP addresses allow you to send messages to a whole subnet at once.

- Send ICMP echo requests (ping) to broadcast address but spoof the return address as victim.
- The subnet will now flood the victim with pings.
- Fix - don’t answer pings to a broadcast address and shun those who do.

Link Layer (LANs)

Address Resolution Protocol (ARP) is a protocol for finding the link layer (MAC) address from IP address on local network.

- ARP Request. Computer A asks the network, "Who has this IP address?"
- ARP Reply. Computer B tells Computer A, "I have that IP. My MAC address is [whatever it is]."
- Reverse ARP Request (RARP). Same concept as ARP Request, but Computer A asks, "Who has this MAC address?"
- RARP Reply. Computer B tells Computer A, "I have that MAC. My IP address is [whatever it is]"

Replies can be sent without requests, results are cached …
Any problems with this?

ARP Spoofing (ARP Poisoning)

Send fake or 'spoofed', ARP messages to an Ethernet LAN.

- claiming to be another computer on the LAN, bad result cached.
- Traffic gets sent to attacker instead.

Defenses:

- static ARP table.
- DHCP snooping (use access control to ensure that hosts only use the IP addresses assigned to them, and that only authorized DHCP servers are accessible).
- detection: Arpwatch (sending email when updates occur).

Legitimate use:

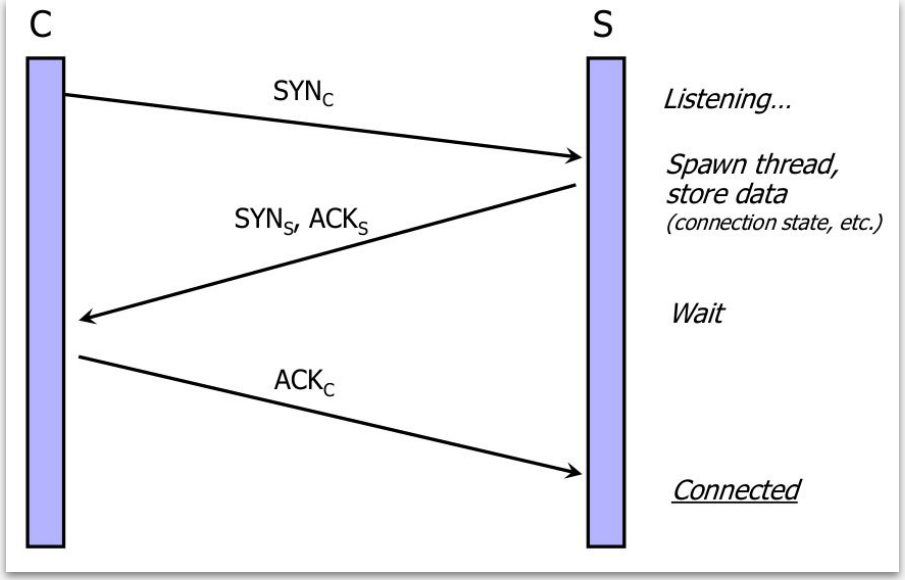
- redirect a user to a registration page before allow usage of the network.

Transmission Control Protocol

Connection-oriented, preserves order.

- Sender
  - Break data into packets.
  - Attach sequence numbers.
- Receiver
  - Acknowledge receipt; lost packets are resent.
  - Reassemble packets in correct order.

TCP Handshake



Sequence number has a dual role:

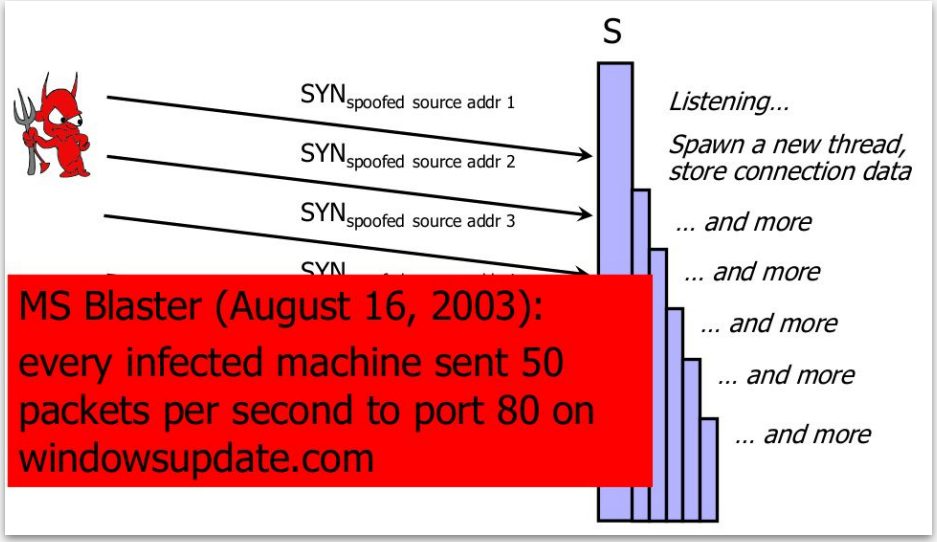
- If the SYN flag is set, then this is the initial sequence number. The sequence number of the actual first data byte is this sequence number plus 1.
- If the SYN flag is clear, then this is the accumulated sequence number of the first data byte of this packet for the current session.

Acknowledgment number

- If the ACK flag is set then this the next sequence number that the receiver is expecting.
- This acknowledges receipt of all prior bytes (if any).

SYN Flood Attack

- Attacker sends many connection requests with spoofed source addresses.
- Victim allocates resources for each request.
  - New thread, connection state maintained until timeout.
- Once resources exhausted, requests from legitimate clients are denied.
- This is a classic denial of service pattern.



MS Blaster (August 16, 2003): every infected machine sent 50 packets per second to port 80 on windowsupdate.com

Preventing Denial of Service

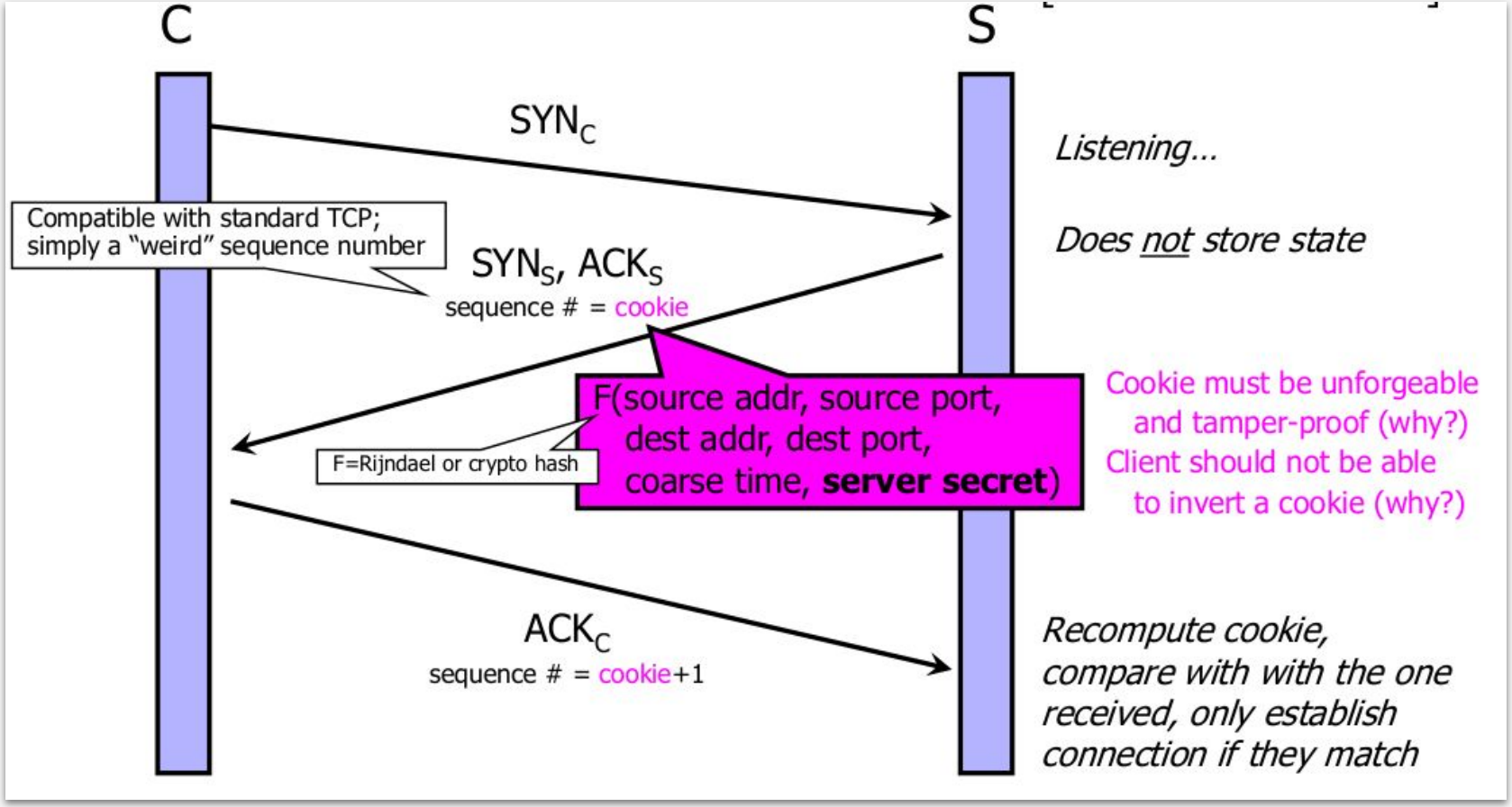
DoS is caused by asymmetric state allocation.

- If responder opens new state for each connection attempt, attacker can initiate thousands of connections from bogus or forged IP addresses.

Cookies ensure that the responder is stateless until initiator produced at least two messages.

- Responder's state (IP addresses and ports of the connection) is stored in a cookie and sent to initiator.
- After initiator responds, cookie is regenerated and compared with the cookie returned by the initiator.

SYN Cookies

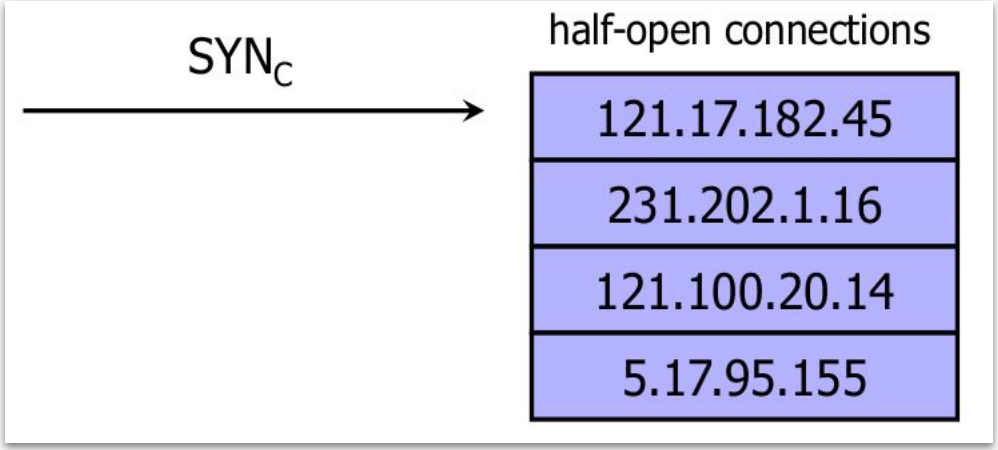

C
S
SYN$_C$
Listening…
Compatible with standard TCP; simply a "weird" sequence number
Does not store state
SYN$_S$, ACK$_S$
sequence # = cookie
F(source addr, source port, dest addr, dest port, coarse time, **server secret**)
F=Rijndael or crypto hash
Cookie must be unforgeable and tamper-proof (why?)
Client should not be able to invert a cookie (why?)
ACK$_C$
sequence # = cookie+1
Recompute cookie, compare with with the one received, only establish connection if they match

Random Deletion

If SYN queue is full, delete random entry.

- Legitimate connections have a chance to complete.
- Fake addresses will be eventually deleted.

Easy to implement.



TCP Connection Spoofing

Each TCP connection has associated state.

- Sequence number, port number.

TCP state is easy to guess.

- Port numbers standard, seq numbers predictable.

Can inject packets into existing connections.

- If attacker knows initial sequence number and amount of traffic, can guess likely current number.
- Guessing a 32-bit seq number is not practical, BUT …
- Most systems accept large windows of sequence numbers (to handle packet losses), so send a flood of packets with likely sequence numbers.

DoS by Connection Reset

If attacker can guess the current sequence number for an existing connection, can send Reset packet to close it.

Especially effective against long-lived connections.

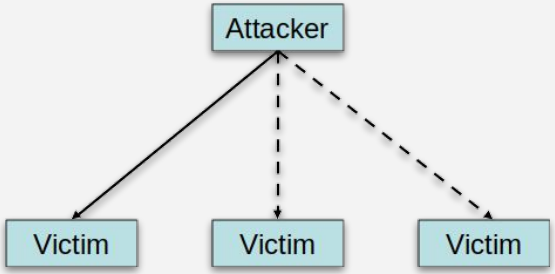
- For example, BGP route updates.

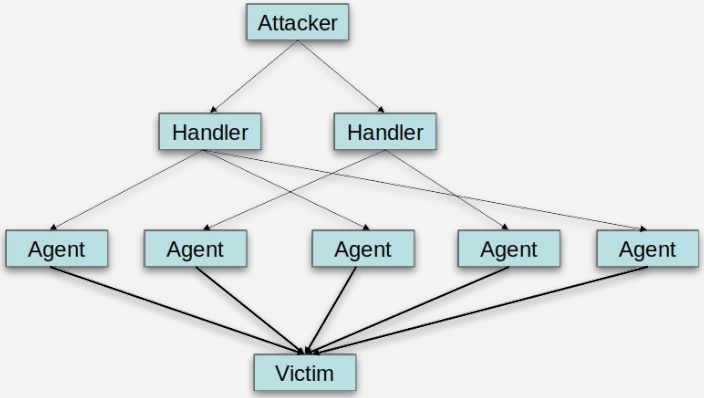
Distributed DoS

Simple DoS
- The Attacker usually spoofed source address to hide origin.
- Easy to block.

DDoS
- Gather a botnet of machines.
- Have them all send traffic to target.
- More traffic, harder to track down or block.

Types of DDoS
- Bandwidth exhaustion - flood network with more traffic than they can consume.
- Resource exhaustion - use up client resources.
- Application exploitation - weaknesses in the actual application.





Countermeasures

Above transport layer: Kerberos.

- Provides authentication, protects against application-layer spoofing.
- Does not protect against connection hijacking.

Above network layer: SSL/TLS and SSH.

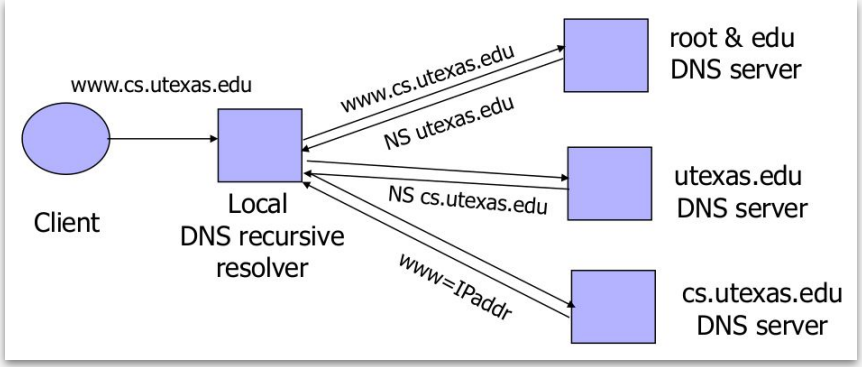
- Protects against connection hijacking and injected data.
- Does not protect against DoS by spoofed packets.

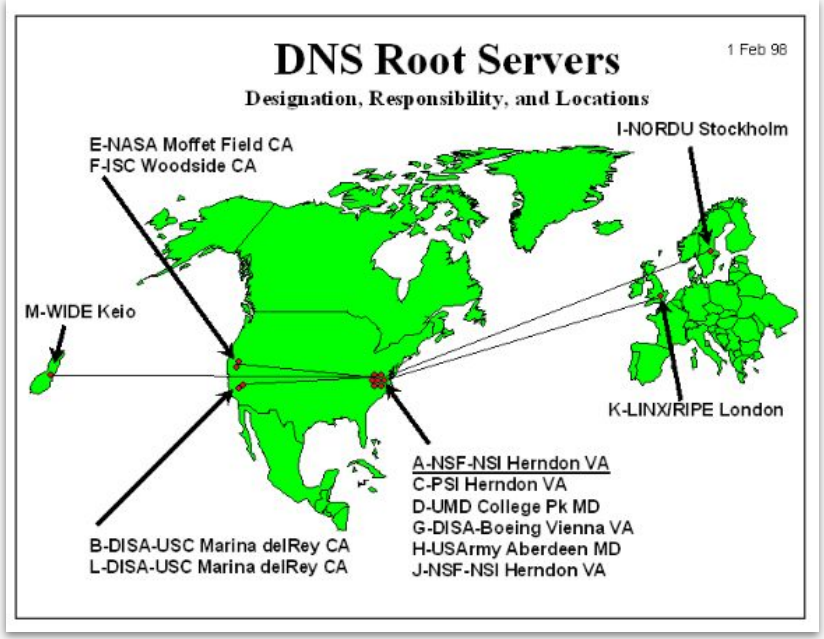
Network (IP) layer: IPsec.

- Protects against hijacking, injection, DoS using connection resets, IP address spoofing.

DNS: Domain Name Service

DNS maps symbolic names to numeric IP addresses.
(for example, www.cs.utexas.edu → 128.83.120.155)

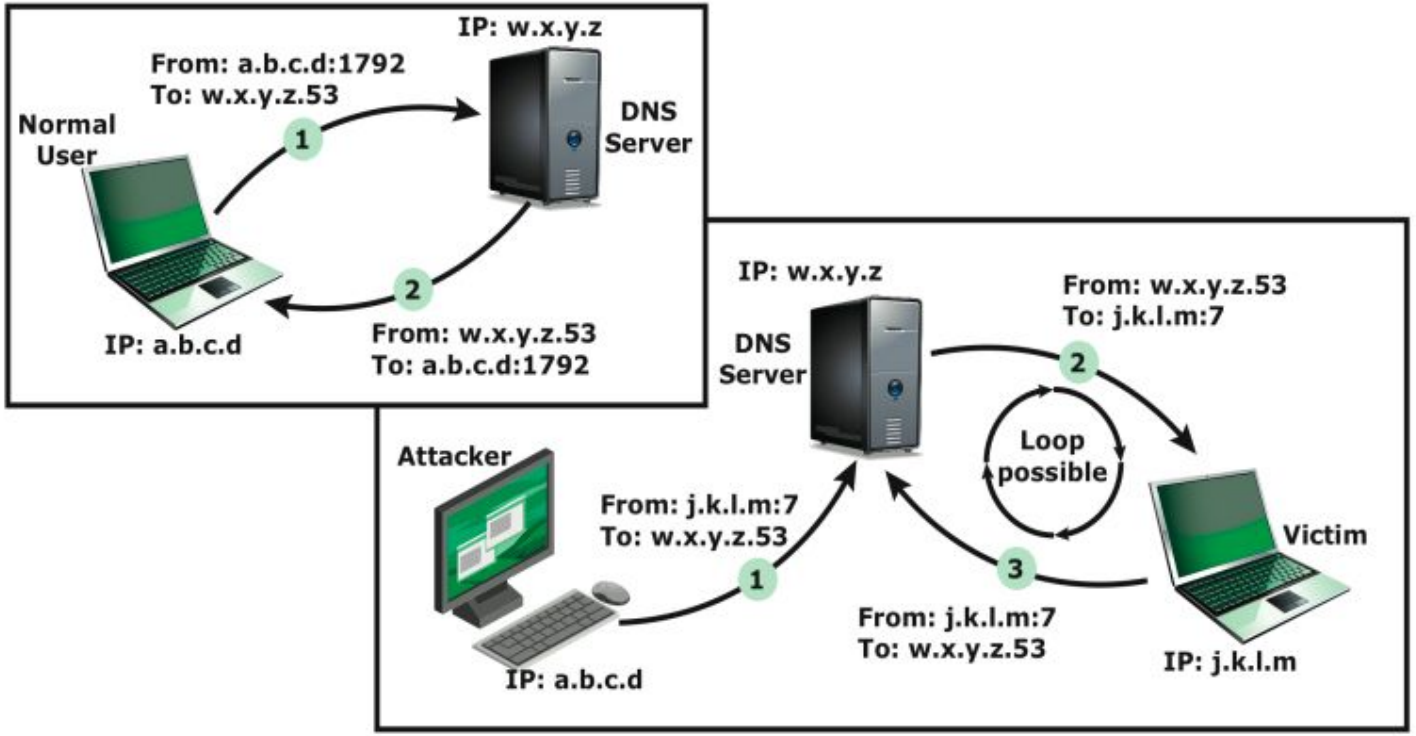




DNS Root Name Servers

- Root name servers for top-level domains.
- Authoritative name servers for subdomains.
- Local name resolvers contact authoritative servers when they do not know a name.

DNS Reflection Attack



DNS Amplification Attacks

- Use packets directed at a legitimate DNS server as the intermediary system.
- Attacker creates a series of DNS requests containing the spoofed source address of the target system.
- Exploit DNS behavior to convert a small request to a much larger response (amplification).
- target is flooded with responses.
- basic defense against this attack is to prevent the use of spoofed source addresses.

Border Gateway Protocol

BGP is a path-vector protocol between ASes.

Just like distance-vector, but routing updates contain an actual path to destination node.

- List of traversed ASes and a set of network prefixes belonging to the first AS on the list.

Each BGP router receives update messages from neighbors, selects one “best” path for each prefix, and advertises this path to its neighbors.

- Can be the shortest path, but doesn’t have to be.
- Always route to most specific prefix for a destination.

BGP Misconfiguration

Domain advertises good routes to addresses it does not know how to reach.

- Result: packets go into a network “black hole”.

April 25, 1997: “The day the Internet died”.

- AS7007 (Florida Internet Exchange) de-aggregated the BGP route table and re-advertised all prefixes as if it originated paths to them.
- Huge network instability as incorrect routing data propagated and routers crashed under traffic.

BGP (In)Security

BGP update messages contain no authentication or integrity protection.

Attacker may falsify the advertised routes.

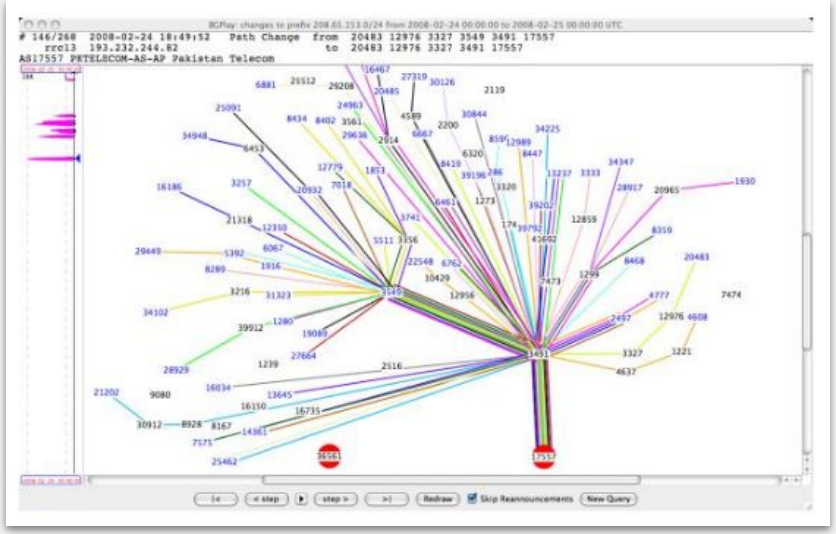
- Modify the IP prefixes associated with a route.
  - Can blackhole traffic to certain IP prefixes.
- Change the AS path.
  - Either attract traffic to attacker's AS, or divert traffic away.
  - Interesting economic incentive: an ISP wants to dump its traffic on other ISPs without routing their traffic in exchange.
- Re-advertise/propagate AS path without permission.
  - For example, a multi-homed customer may end up advertising transit capability between two large ISPs.

YouTube (February 24, 2008)

Pakistan government wants to block YouTube.

- AS17557 (Pakistan Telecom) advertises 208.65.153.0/24.
- All YouTube traffic worldwide directed to AS17557.

Result: two-hour YouTube outage.



Secure Network Configurations

Best way to secure a network, secure machines in the network.

Keep them patched, don’t run insecure services, teach users about security.

This is expensive and difficult.

Firewalls

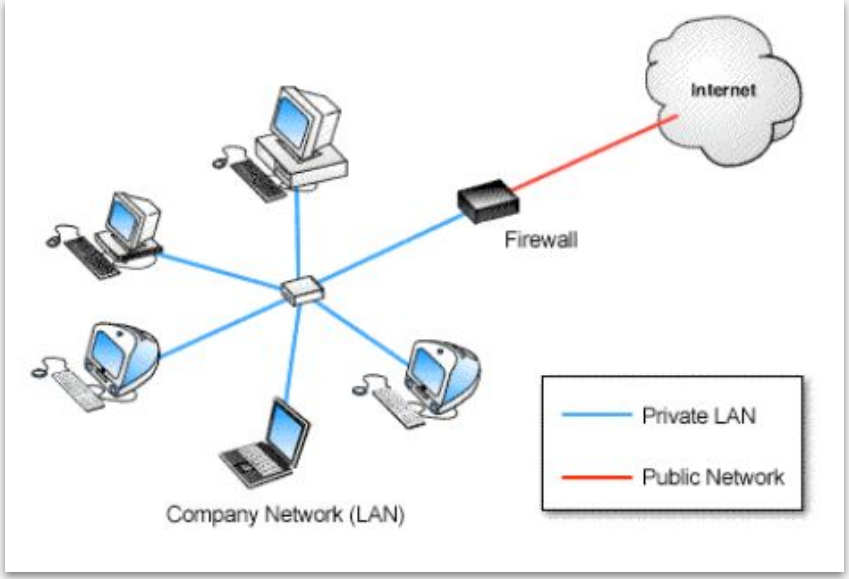
Most commercially successful network security product.

- Limit access to the network.
- Put firewalls across the perimeter of the network.

Firewall inspects traffic through it.

Allows traffic specified in the policy.

Drops everything else.



Two Types:

- Packet Filters.
- Proxies.

Packet Filters

Packet filter selectively passes packets from one network interface to another.

Usually done within a router between external and internal networks.
- screening router.

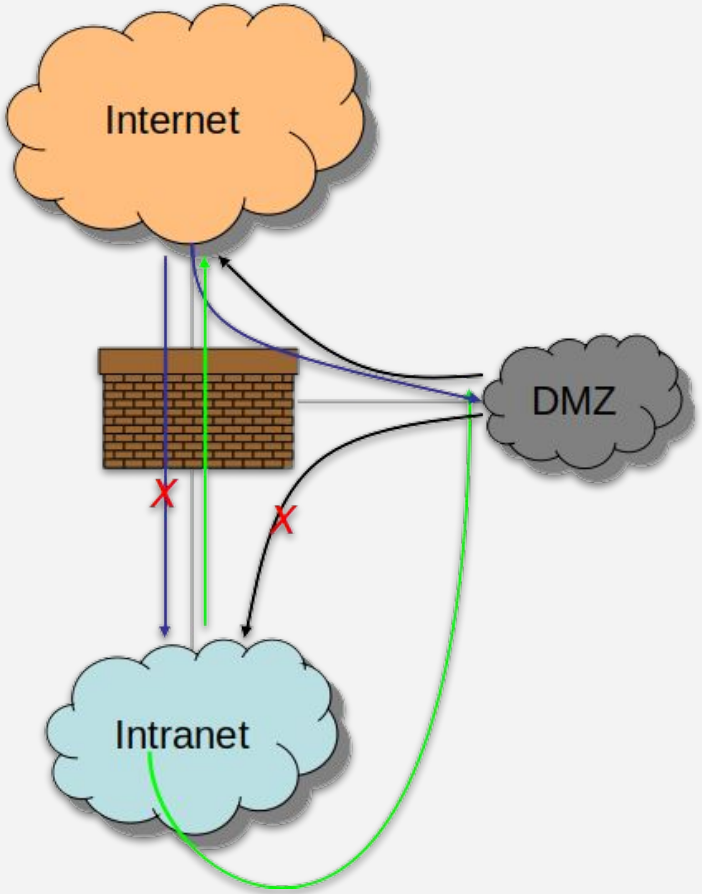
Can be done by a dedicated network element.
- packet filtering bridge.
- harder to detect and attack than screening routers.

Example filters:
- Block all packets from outside except for SMTP servers.
- Block all traffic to a list of domains.
- Block all connections from a specified domain.

Typical Firewall Configuration

- Internal hosts can access DMZ and Internet.
- External hosts can access DMZ only, not Intranet.
- DMZ hosts can access Internet only.
- Advantages:
  - if a service gets compromised in DMZ it cannot affect internal hosts.

** DMZ = demilitarized zone.*



Continue ...

Advantages:

- Transparent to application/user.
- Simple packet filters can be efficient.

Disadvantages:

- complex to configure.
- cannot prevent application-layer attacks.
- susceptible to certain types of TCP/IP protocol attacks.
- do not support user authentication of connections.
- limited logging capabilities.

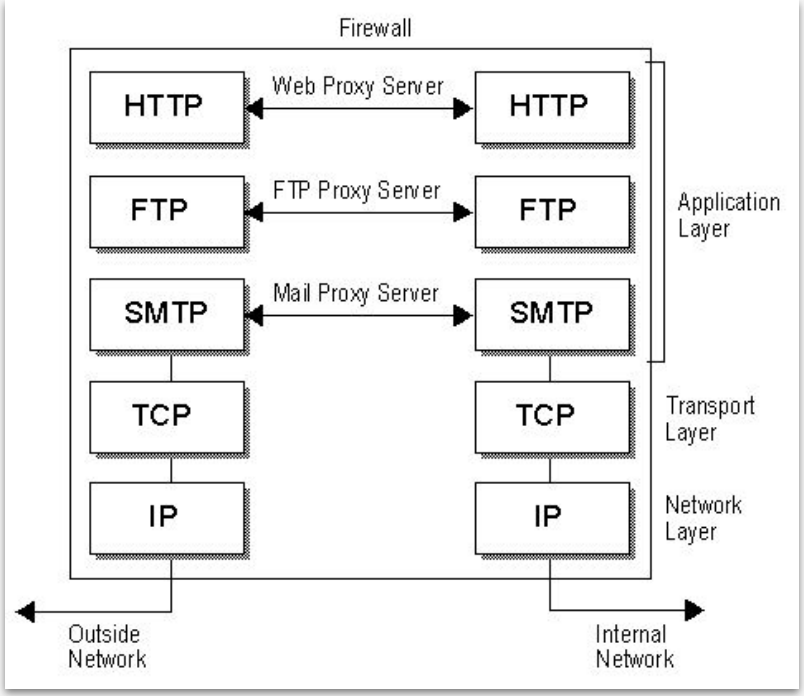
Proxy Firewalls

Two connections instead of one.
- Either at transport level
  - SOCKS proxy.
- Or at application level
  - HTTP proxy.

Requires applications to be modified to use the proxy.

Advantage:
- Better policy enforcement, Better logging, Fail closed.

Disadvantage:
- Doesn't perform as well, One proxy for each application, Client modification.



Intrusion Detection Systems

Firewalls allow traffic only to legitimate hosts and services.

Traffic to the legitimate hosts/services can have attacks.

- CodeReds on IIS.

Solution:

- Intrusion Detection Systems.
- Monitor data and behavior.
- Report when identify attacks.

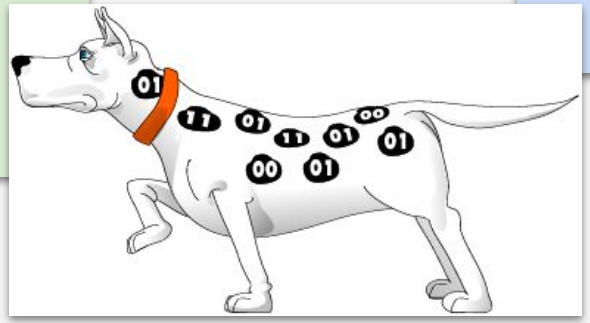
Signature-based IDS

Characteristics:

- Uses known pattern matching to signify attack.

Advantages:

- Widely available.
- Fairly fast.
- Easy to implement.
- Easy to update.



Disadvantages:

- Cannot detect attacks for which it has no signature.

Anomaly-based IDS

Characteristics:

- Uses statistical model or machine learning engine to characterize normal usage behaviors.
- Recognizes departures from normal as potential intrusions.

Advantages:

- Can detect attempts to exploit new and unforeseen vulnerabilities.
- Can recognize unauthorized usage that falls outside the normal pattern.

Disadvantages:

- Generally slower, more resource intensive compared to signature-based IDS.
- Greater complexity, difficult to configure.
- Higher percentages of false alerts.

Summary

TCP/IP security vulnerabilities:
- Spoofing.
- Flooding attacks.
- TCP session poisoning.

DOS and DDOS.

Firewalls.
- Packet Filters.
- Proxy.

IDS.
- Signature and Anomaly IDS.

< Network Security />