CSE 484 (Winter 2008)

Network Security

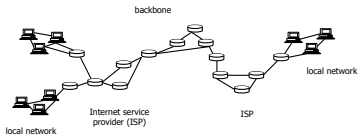
Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

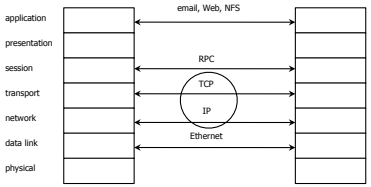
- Network Security Attacks
  - Routing
  - IP
  - TCP
  - DNS
- Key points:
  - Failures at interaction between layers
  - Asymmetry between attacker and defender
  - Some attacks designers never considered
  - All motivations for existing security decisions (SSL/TLS, filter certain types of packets, check inputs, etc).

Internet Infrastructure

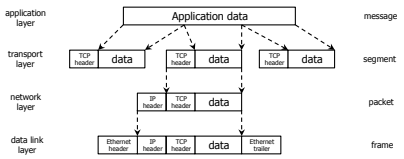


- TCP/IP for packet routing and connections
- Border Gateway Protocol (BGP) for route discovery
- Domain Name System (DNS) for IP address discovery

OSI Protocol Stack

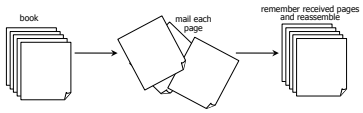


Data Formats



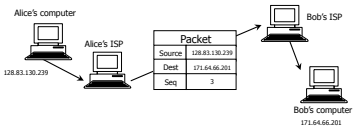
TCP (Transmission Control Protocol)

- Sender: break data into packets
  - Sequence number is attached to every packet
- Receiver: reassemble packets in correct order
  - Acknowledge receipt; lost packets are re-sent
- Connection state maintained on both sides



IP (Internet Protocol)

- Connectionless
  - Unreliable, "best-effort" protocol
- Uses numeric addresses for routing
  - Typically several hops in the route



IP Routing

- Routing of IP packets is based on IP addresses
- Routers use a forwarding table
  - Entry = destination, next hop, network interface, metric
  - For each packet, a table look-up is performed to determine how to route it
- Routing information exchange allows update of old routes and creation of new ones
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First Protocol)
  - BGP (Border Gateway Protocol)

Routing Attacks

- Source routing
  - Source of the packet specifies a particular route
    - For example, because the automatic route is dead
  - Attacker can spoof source IP address and use source routing to direct response through a compromised host
  - Solution: reject packets with source routing!
    - More heavy-duty: allow source route only via trusted gateways
- Routing Information Protocol (RIP)
  - Use bogus routing updates to intercept traffic
    - RIP implicitly assumes that routers are trusted
  - "Black hole" attacks and many others

BGP Misconfiguration

- Domain advertises good routes to addresses it does not known 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
  - In effect, AS7007 was advertising that it has the best route to every host on the Internet
  - Huge network instability as incorrect routing data propagated and routers crashed under traffic

ICMP (Control Message Protocol)

- Provides feedback about network operation
  - "Out-of-band" messages carried in IP packets
  - Error reporting, congestion control, reachability, etc.
- Example messages:
  - Destination unreachable
  - Time exceeded
  - Parameter problem
  - Redirect to better gateway
  - Reachability test (echo / echo reply)
  - Message transit delay (timestamp request / reply)

Security Issues in TCP/IP

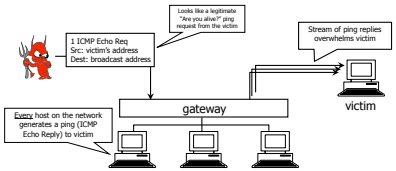
- Network packets pass by untrusted hosts
  - Eavesdropping (packet sniffing)
- IP addresses are public
  - Smurf attacks
- TCP connection requires state
  - SYN flooding
- TCP state is easy to guess
  - TCP spoofing and connection hijacking

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), improved routing

Smurf Attack



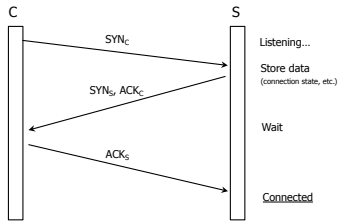
Solution: reject external packets to broadcast addresses

"Ping of Death"

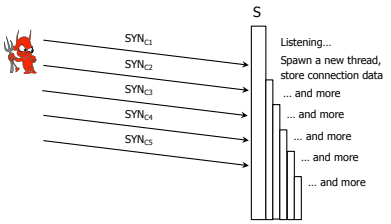
- If an old Windows machine received an ICMP packet with a payload longer than 64K, machine would crash or reboot
  - Programming error in older versions of Windows
  - Packets of this length are illegal, so programmers of Windows code did not account for them
- Recall "security theme" of this course - every line of code might be the target of an adversary

Solution: patch OS, filter out ICMP packets

TCP Handshake



SYN Flooding Attack



SYN Flooding Explained

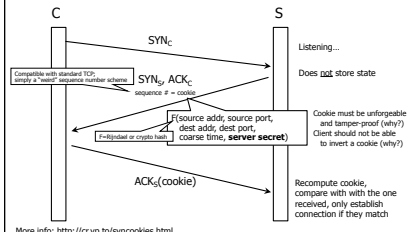
- Attacker sends many connection requests with spoofed source addresses
- Victim allocates resources for each request
  - Connection state maintained until timeout
  - Fixed bound on half-open connections
- Once resources exhausted, requests from legitimate clients are denied
- This is a classic denial of service (DoS) attack
  - Common pattern: it costs nothing to TCP initiator to send a connection request, but TCP responder must allocate state for each request (asymmetry!)

Preventing Denial of Service

- DoS is caused by asymmetric state allocation
  - If responder opens a 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 2 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

[Bernstein and Schenk]

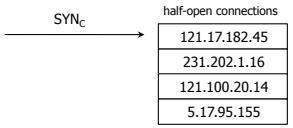


More info: http://cr.yp.to/syncookies.html

Anti-Spoofing Cookies: Basic Pattern

- Client sends request (message #1) to server
- Typical protocol:
  - Server sets up connection, responds with message #2
  - Client may complete session or not (potential DoS)
- Cookie version:
  - Server responds with hashed connection data instead of message #2
  - Client confirms by returning hashed data
    - If source IP address is bogus, attacker can't confirm
  - Need an extra step to send postponed message #2, except in TCP (SYN-ACK already there)

Another Defense: Random Deletion

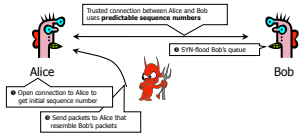


- If SYN queue is full, delete random entry
  - Legitimate connections have a chance to complete
  - Fake addresses will be eventually deleted
- Easy to implement

TCP Connection Spoofing

- Each TCP connection has an associated state
  - Sequence number, port number
- TCP state is easy to guess
  - Port numbers are standard, sequence numbers are often predictable
  - Can inject packets into existing connections
- If attacker knows initial sequence number and amount of traffic, can guess likely current number
  - Send a flood of packets with likely sequence numbers

"Blind" IP Spoofing Attack



- Can't receive packets sent to Bob, but maybe can penetrate Alice's computer if Alice uses IP address-based authentication
  - For example, rlogin and many other remote access programs uses address-based authentication

DoS by Connection Reset

- If attacker can guess current sequence number for an existing connection, can send Reset packet to close it
  - With 32-bit sequence numbers, probability of guessing correctly is $1/2^{32}$ (not practical)
  - Most systems accept large windows of sequence numbers ⇒ much higher probability of success
    - Need large windows to handle massive packet losses