Network Protocols and Vulnerabilities

John Mitchell

Outline

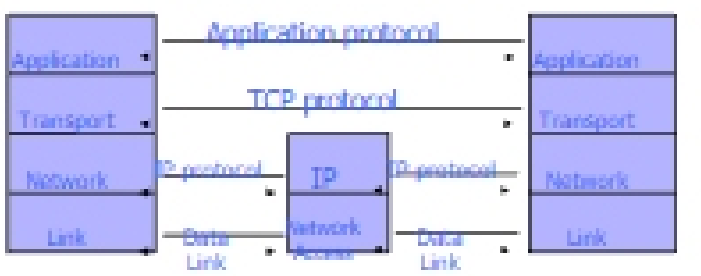
- Basic Networking (FMU)
- Network attacks
  - Attack host networking protocols
    - SYN flooding, TCP Spoofing, …
  - Attack network infrastructure
    - Routing
    - Domain Name System

This lecture is about the way things work now and how they are not perfect. Next lecture – some security improvements (still not perfect).

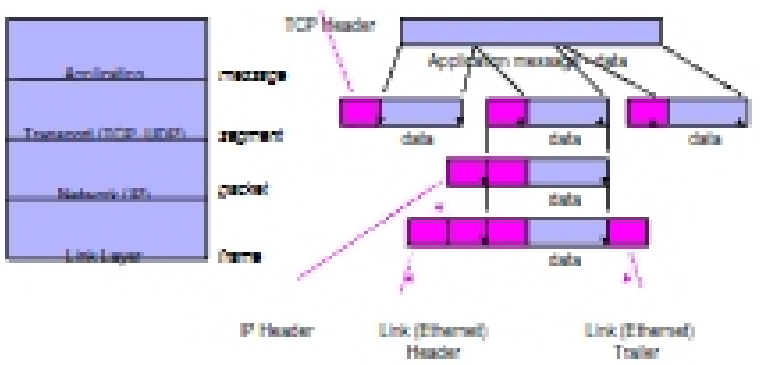
Internet Infrastructure

- Local and interdomain routing
  - TCP/IP for routing, connections
  - BGP for routing announcements
- Domain Name System
  - Find IP address

TCP Protocol Stack



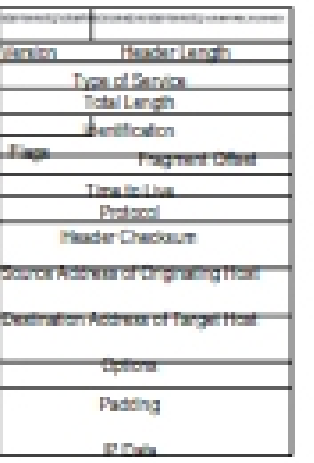
Data Formats



IP

Internet Protocol

- Connectionless
  - Unreliable
  - Best effort
- Transfer datagram
  - Header
  - Data



IP Routing

- Internet routing uses numeric IP address
- Typical route uses several hops

IP Protocol Functions (Summary)

- Routing
  - IP host knows location of router (gateway)
  - IP gateway must know route to other networks
- Error reporting
  - IP reports discards to source
- Fragmentation and reassembly
  - If packets smaller than the user data

UDP

User Datagram Protocol

- IP provides routing
  - IP address gets datagram to a specific machine
- UDP separates traffic by port
  - Destination port number gets UDP datagram to particular application process, e.g., 128.3.23.3, 53
  - Source port number provides return address
- Minimal guarantees (... mice and elephants)
  - No acknowledgment
  - No flow control
  - No message continuation

TCP

Transmission Control Protocol

- Connection-oriented, preserves order
  - Sender
    - Break data into packets
    - Attach packet numbers
  - Receiver
    - Acknowledge receipt; lost packets are resent
    - Reassemble packets in correct order

ICMP

Internet Control Message Protocol

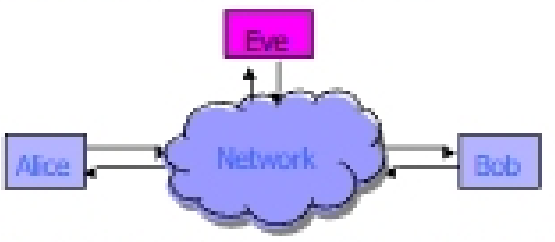
- Provides feedback about network operation
  - Error reporting
  - Reachability testing
  - Congestion Control
- Example message types
  - Destination unreachable
  - Time exceeded
  - Parameter problem
  - Redirect to better gateway
  - Echo/echo reply - reachability test
  - Timestamp request/reply - measure transit delay

Basic Security Problems

- Network packets pass by untrusted hosts
  - Eavesdropping, packet sniffing
- IP addresses are public
  - Smurf
- TCP connection requires state
  - SYN flooding attack
- TCP state easy to guess
  - TCP spoofing attack

Packet Sniffing

- Promiscuous NIC reads all packets
  - Read all unencrypted data
  - ftp, telnet send passwords in clear!



Sweet Hall attack installed sniffer on local machine

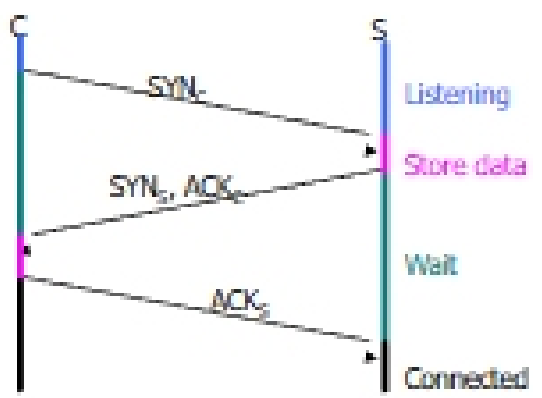
Prevention: Encryption, improved routing (Next lecture: IPSEC)

Smurf Attack

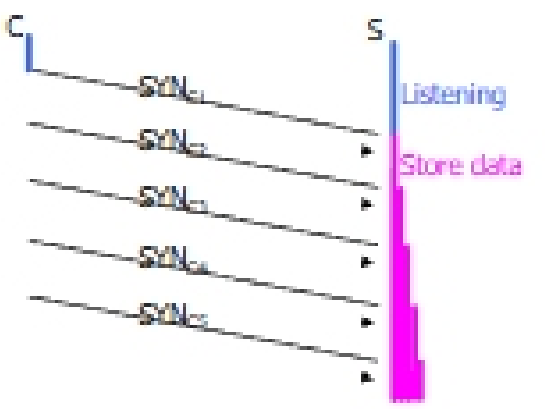
- Choose victim
  - Idea: Flood victim with packets from many sources
- Generate ping stream (ICMP Echo Req)
  - Network broadcast address with spoofed source IP set to victim
- Wait for responses
  - Every host on target network will generate a ping reply (ICMP Echo Reply) to victim
  - Ping reply stream can overload victim

Prevention: Turn off ping? Authenticated IP addresses?

TCP Handshake



SYN Flooding



SYN Flooding

- Attacker sends many connection requests
  - Spoofed source addresses
- Victim allocates resources for each request
  - Connection requests exist until timeout
  - Fixed bound on half-open connections
- Resources exhausted ⇒ requests rejected

Protection against SYN Attacks

[Bernstein, Schenk]

- Client sends SYN
- Server responds to Client with SYN-ACK cookie
  - sqn = f(src addr, src port, dest addr, dest port, rand)
  - Server does not save state
- Honest client responds with ACK(sqn)
- Server checks response
  - If matches SYN-ACK, establishes connection

See http://cr.yp.to/syncookies.html