Network Protocols and Vulnerabilities

John Mitchell

Outline

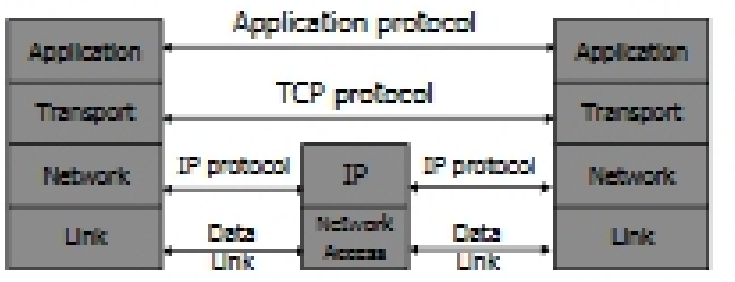
- Basic Networking (FMU)
- Network attacks
  - Attack host networking protocols
    - SYN flooding, TCP Spoofing, …
  - Attack network infrastructure
    - Routing
    - Domain Name System

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

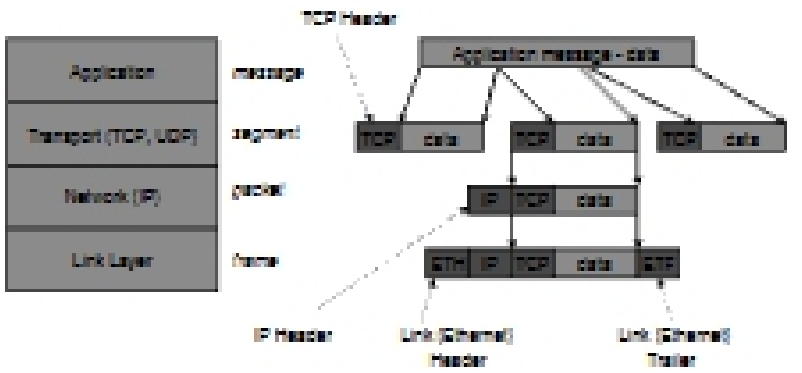
Internet Infrastructure

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

TCP Protocol Stack



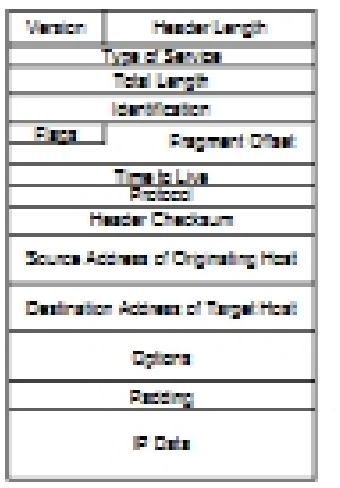
Data Formats



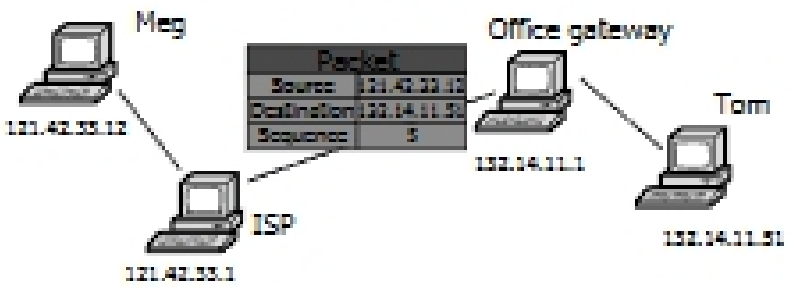
IP

Internet Protocol

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



IP Routing



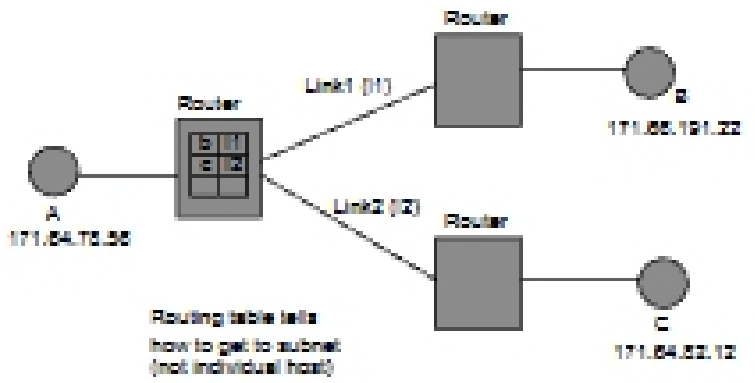
- Internet routing uses numeric IP address
- Typical route uses several hops

Two-level Address Hierarchy

- Addresses divided into two parts
  - First: the domain (network) of the host
  - Second: address of host within domain

Three different address formats: Class A, Class B, Class C
(not important for this course)

Simple Routing Example



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