Review of TCP/IP Networks

Mahalingam Ramkumar
CSE 4383/6383
Network Layers

- Physical
- Datalink / MAC (PPP, Ethernet, Wireless Ethernet)
- Network: IP
- Transport: TCP / UDP
- Application: WWW, Email, DNS, FTP
Functions of Layers

- Physical layer: Convert bits to electrical signals
- MAC / DL: Send frames from one machine to another using a physical medium
- Network Layer: Send an IP packet from one computer to another (usually over several hops). IP packets are carried over each hop in different DL/MAC frames: each hop may employ different MAC/DL layers depending on the underlying physical layer
IP

- Every computer has a unique IP address
- IP packets indicate source and destination address
- IP packet routed from source to destination by routers
- IP layer component (in every machine: end points and routers) looks at the destination IP address to determine the next hop
  - determined by routing tables / protocols
- Routers are aware of mappings between autonomous systems (AS), and IP address prefixes, and the best path to reach a router serving some AS
Transport Layer

- Establish a reliable connection from between two processes (usually in different machines)
  - Port numbers used to identify specific processes / connections
  - TCP/UDP packets are payloads of IP packets
  - UDP: adds very little functionality over IP (UDP header specifies port number)
TCP

- Provides reliable connection
  - Three way handshake for connection establishment
  - Four (or three) way handshake for termination
  - Acknowledgements
- Two independent connections
- Sequence numbers / ACK numbers used to keep track of application bytes sent over the connection (in either direction)
- Sequence numbers chosen randomly by both parties.
Network vs Application Layer

- Routers look at the Internet as an interconnection of ASes
- Application viewpoint: The Internet is organized into ones of the domain name system (DNS) hierarchy
- DNS helps clients locate services run by servers, connect to them, send queries, and get responses
- Different client-server protocols used for different types of applications (HTTP, FTP, SMTP)
Security Issues

- In an ideal world we implicitly expect every layer to do what it is supposed to do.
- Unfortunately, even in a non-ideal world, end-users have some implicit expectations.
- Security unaware users assume:
  - that an email from Joe is indeed a mail from Joe.
  - the website they are visiting is indeed citibank.com because the browser says so.
- If they trust CNN as a news source they can trust cnn.com.
Attackers

- We have to deal with attackers who try to exploit this implicit trust
  - How can attackers mess up things?
  - How can we address attacks?
  - What is the cost?
    - Cost vs benefit?
  - What is the attacker capability?
    - Obviously depends on the type of attacker: State backed, systems administrator, internal attacker, man-in-the-middle, external attacker
Attacker Types

- Forget about the first two categories for now (very little can be done?)
- Man-in-the-middle:
  - Can intercept and modify packets
- Internal attacker:
  - Can (passively) observe packets
- External: not internal, not a man-in-the-middle (cannot observe traffic between the end points)