Computer Network basics

CS 594 Special Topics/Kent Law School:

Computer and Network Privacy and Security: Ethical, Legal, and Technical Consideration

Networks: Two or more computers communicating

- Networks are formed when distinct computers communicate via some mechanism.
- **Networks have several layers to them**
  - **At the bottom level is the physical substrate.**
    - What are the signals being passed on?
  - **Levels higher determine how data is encoded.**
    - Do we use sound frequencies to represent 0's and 1's, or radio waves?
    - Do we send a bit at a time? A byte at a time? Or in *packets* larger than that?
  - **Levels even higher determine the protocol of communication.**
    - How do I *address* a particular computer I want to talk to? Or many computers?
    - How do I tell a computer that I want to talk to it? That I'm starting to send it

Circuit switching

- **Circuit switching network** = dedicated **circuit/channel** established between end points before two principals can communicate.
- E.g., early telephone exchanges, with operator with the plug board.
- This is ***not*** *how the Internet operates!*

Packet switching

- Traffic is split into chunks, called **packets** that are routed over a shared network.
- Each packet is individually addressed and may take a distinct path among the networks' nodes.

Internet: A collection of networks

- The Internet is a network of networks.
- The Internet is built on a set of agreements about:
  - **How computers will be addressed**
    - A set of four numbers (each one byte now, soon to grow) separated by periods, e.g., 10.1.0.5.
    - A way of associating *domain names* with these numbers, like www.cnn.com (which really is a name that resolves to a set of four numbers), using *domain name servers*.
  - **How computers will communicate**
    - That data will be put into packets with various pieces in them.
    - That computers will format their data and talk to one another using *TCP/IP* suite of protocols, including especially TCP and IP
  - **How packets are routed around the network to find their destination.**

The Internet is not new

- The Internet agreements date back 40 years.
- It was originally set up for military applications.
- **One of the features of the Internet is that packets find their destination even if part of the Internet is destroyed, damaged, or subject to censorship.**
- The Internet originally had only a handful of computers (*nodes*) on it, but it has grown

Internet ≠ Web!

- 1st node of what was to become the Internet went live Oct. 1969; I started using it regularly in 1985.

- World wide web became publicly available in August 1991; I started using it in late 1994.

  - Today, Web and email perhaps the two most popular of many Internet services

Security: Networked systems are different

- Network traffic is not subject to physical security like servers, workstations
  - Attackers can see, modify, remove your traffic
- Multiple organizations
  - And issues of organizational trust
- Many of the network protocols (layers)

DNS

- Domain Name System (DNS) is "phonebook:" converts either way between globally unique **host name** (e.g., en.wikipedia.org) and globally unique **IP address** (e.g., 66.230.200.100).
- Distributed system: hierarchical set of DNS servers. I ask somebody near by and if they don't know they have a bigger guy to ask.

DNS & Security

- DNS dates to early 1983, before today's security issues
- Was massive source of security problems in late 1990s and early 200s; BIND through version 8 had huge security holes
- Current version 9 of BIND was total rewrite; still some issues but vastly better.

Local color

- 2nd most popular DNS software is djbdns
- DJB offers $500 prize for first security hole found in it; still unclaimed

Two ways to analyze Internet

- One, "horizontally" as system of end-user computers, web-site hosts, etc., at edges, and all the network in the middle.
- Second, "vertically" as series of layered abstractions, starting with high & low voltages on wires, going through packets, and eventually up to, e.g., HTTP

Internet structure (horizontal view)

- **Network** is vast collection of **nodes** (computers) connected by bidirectional **links** (think wires)

- Your computer/your home network is one node, connected to a single link to your ISP
- Crudely end-user nodes (you, cnn.com) are at edge with 1 connection; **router** (small electronic box with *very* dumb computer)

Data flow over

- Packets (of data) start from one end-user node, forwarded by many routers, arrive at destination end-user node.

- Routers store packets (“buffering”) when they’re busy with lots; throw away packets when they’re really busy.

  - Networks protocols know about this and do proper resents.

Network topology larger structure

- Middle of network is metaphorically first tiny trickles, then little creeks and rivulets, then huge rivers
- Equivalent of Missisippi River Basin is **Autonomous System (AS)** owned by some **Internet Service Provider (ISP)**
- One AS sends messages to another fast and

Intelligence at edges vs. in middle

- Internet unusual among networks: smart devices are computers at edge; routers dumb
- Good thing because:
  - Edge computers more likely to know users' desires
  - Innovation usually easier at edge
  - More edge computers than routers; use

Vertical Layered View of Networks

- Conceptually, networks designed in layers; 7-layer Open Systems Interconnection (OSI) model, 4_5 layer Internet Reference models all popular. From bottom to top:
- Physical link/layer: physical connection between 2 points, includes specification of connectors, wires, electrical parameters, etc.
- Network Access/Data Link: Logical connection: error correction, flow control, unique low-level physical address (MAC) of each device; network

Network layer

- Network/Internet/Internetworking layer: Determines the data links that will be taken to get from a source address to destination address
  - Internet Protocol (IP) most important thing at this level; also ICMP (More on IP soon)
  - Generally lowest level with any security

Top layers

- Host-to-host or Transport layer: where flow-control and connection protocols exist, especially TCP (also UDP)
    - Concerned with opening and maintaining connections
- At top: Application (process) layer: email, web, file transfer, etc. Single biggest source of security vulnerabilities. (OSI model splits

Internet Protocol (IP)

- Packet-based protocol used at the network (technically the packets here called *datagrams*).
  - Each datagram individually addressed; *there is no such thing as a connection in the network.*
- Each packet has source and destination *IP address*, e.g., `64.236.91.21 (www.cnn.com)`

IP: Routing, etc.

- At IP level, protocol finds best next link to travel to get to final destination.
  - I.e., network self configures to find "best" route; and routes are constantly changing
- Also allowed to split datagrams at any point if smaller size seems more convenient
- Not intended to be stand-alone; has TCP at

Network-layer security issues

- Datagrams include source address, but source address is not checked
- With administrative control you can create *any* source address
  - ⇒You don't know where IP datagrams really came from.

TCP

- Transmission Control Protocol (TCP): Most popular transport protocol used at transport (and related session) layer. (#2 is UDP)
- Used to implement mail, web, file transfer
- Sits on top of IP
- For process-to-process communication at 2 endpoints; semantics 100% at end points.

Connections; ports

- TCP adds, among other things, source and destination **ports** to packet (now *packet* not datagram) header: Number like phone extension to IP address phone number.
- TCP is connection oriented; connection is defined by source IP + port and destination IP + port

What does TCP add?

- TCP is where both reliability and error checking comes in
- Checksum error checking and acknowledgment of receipt and thus TCP designed to recover form lost, corrupted, duplicate packets
- Also congestion control

Transport Layer Security Issues

- Transport layer was designed in 1970s without any security
  - Any host could request connection to any other host
  - OS interfaces provided no screening
- In 1970s networking was between servers in locked machine rooms over dedicated

Top layer(s): Application

- Application layer (in 7 layer model, split into 3).
- Where the protocol for the application lives
  - E.g., DNS, FTP, HTTP, IMAP and POP, SMTP, SSH, SSL
- Also, in 4 and 5 layer models where

Summary of Network Overview WRT

- Packet-switched network traffic can be seen, modified, or removed by attackers
- Connections can originate from anywhere in the world.
- IP source and destination addresses are world readable
- Many protocols at all levels are not security