CSCI 1800 Cybersecurity and International Relations

Design and Operation of the Internet

John E. Savage

Brown University
Outline

• Network security
• The link layer
• The network layer
• The transport layer
• Denial of service attacks
The Internet

- The Internet is a collection of networks.
  - Networks connect hosts, i.e. individual computers.
  - They may be local, area-wide, enterprise-wide, or national.

- **Protocols** govern data transmission on network
  - Protocol defines acceptable way to package information
    - Specify source, destination, & content and (often) do error checking
  - Ethernet (1973) – local protocol based on collision detection
  - Internet protocol (1974) decomposes data streams into packets and sends them via packet switching.

- Protocols are layered, one communicating to next
Conceptual Internet Layers

- **Physical Layer**
  - At level of wires, cables, radio – physical data transmission

- **Link Layer**
  - Logical level, organizes data into blocks, choose routes.

- **Internet or network Layer**
  - Makes best effort to move packets.

- **Transport Layer**
  - TCP (reliable) and UDP (no guarantees) protocols are here

- **Application Layer**
  - Applications protocols are here. They include HTTP and HTTPs for browsers, DNS for naming, SMTP & IMAP for email, SSL for secure communication, and VoIP for phone service
Internet Packet Encapsulation by Layer

Application Data

TCP header

Applicaton Data

IP header

IP Data

Frame header

IP header

Frame Data

Frame footer

Application Layer

Transport Layer

Internet Layer

Link Layer

UDP also used here
Sending Data via Protocol Layers

Network Topology

Data Flow

Network Security Goals - CIA^4

• **Confidentiality**
  – Keep content private

• **Integrity**
  – Ensure that content is not altered

• **Availability**
  – Ensure content is available

• **Assurance**
  – Enforce data flow policies, e.g. at firewall

• **Authenticity**
  – Authenticate users via signatures

• **Anonymity**
  – Guarantee anonymity when needed
Ethernet – At the Physical Layer

• Data organized into **frames**. Each has
  – **Header** of 175 **bytes** (8 bits/byte)
  – **Payload** of 46 to 1,500 bytes
  – **Footer** contains a 4-byte checksum
    • What is the role of the checksum?

• **If a host wants to send a frame:**
  – **Waits** until no signals heard & transmits one bit of one frame
  – **Listens** for collisions between its bit and bits of others.
    • *If collision detected*, wait a random time and retransmit
    • *If no collisions detected* during packet transit time, success.
  – **Transmits** remaining bits in frame in same manner.
Ethernet Hubs and Switches

• **Ethernet hub** connects multiple hosts
  – All hosts hear messages sent by others

• **Ethernet switch** connects multiple hosts
  – It has multiple hubs. Only hosts on a hub can hear one another.
  – Messages are sent from host on one hub to host on another hub by *switching* packets to that hub.
Media Access Control Addresses

• Each device *network interface* has a MAC address.
  – A *network interface* is the place on a host at which it connects to a network.
  – A MAC address is generally a *unique* 48-bit string assigned by a manufacturer.
  – Although on modern computers, it can be changed under software control.

• MAC addresses are used by Ethernet switches.
Address Resolution Protocol (ARP)

• A link-layer protocol for local area network (LAN)
  – ARP uses host’s hardware address (usually a MAC address) to determine its network layer (IP) address

• A host asks other hosts on its LAN to reply with its MAC address if it has the requested IP address.

• **Spoofing** is possible here. Alice makes request to Eve
  – Eve gives Alice her MAC address for Bob’s IP address

• Bob makes a request to Eve
  – Eve gives Bob her MAC address for Alice’s IP address

• Now communication between Alice & Bob is via Eve
The Internet Protocol (IP)

- IP makes best effort to send packets between source and destination addresses.
- Addresses are 32-bits (IPv4) or 128-bits (IPv6).

\[ 2^{32} = 4 \cdot 2^{30} \text{ or about } 4 \cdot 10^9 \quad \text{or} \quad 2^{128} = 64 \cdot 2^{120} \text{ or about } 64 \cdot 10^{36} \]
The Internet Protocol (IP)

- IP makes best effort to send packets between source and destination addresses.
- Addresses are 32-bits (IPv4) or 128-bits (IPv6).
- An autonomous system has a subset of IP addresses that it assigns to its hosts.
Packet Transmission

• ARP sends packets within local area net (LAN).
• Packets destined for IP address on remote LAN are sent to a LAN Internet gateway, then to remote LAN.
• Gateways and intermediate nodes are routers.
• Routers use routing tables to direct packets.
  – For each IP address, a table specifies a neighbor to receive the packet.
  – To prevent looping, each packet has a time-to-live (TTL) value. It is decreased by one each time it passes through a router. When TTL = 0, packet is discarded.
Internet Structure

• Routers quickly drop, deliver or forward packets.
  – Drop if TTL =0, deliver if dest. is on LAN; forward if not
• Packet forwarding protocol is via one of these:
  – Open Shortest Path First (OSPF) or
  – Border Gateway Protocol (BGP)
• **OSPF** or **BGP** route packets **within** autonomous syst.
• **BGP** also routes packets **between** autonomous systs
• **Note:** A LAN hub/switch is simple but a router must quickly handle complex routing policies.
## Format of IPv4 Packets

\[ 2^{16} = 65,536 \text{ ports} \]

<table>
<thead>
<tr>
<th>Bit Offset</th>
<th>0-3</th>
<th>4-7</th>
<th>8-15</th>
<th>16-18</th>
<th>19-31</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Version</td>
<td>Header Length</td>
<td>Service Type</td>
<td>Total Length</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Identification</td>
<td></td>
<td>Flags</td>
<td>Fragment Offset</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Time to Live</td>
<td>Protocol</td>
<td></td>
<td>Header Checksum</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td></td>
<td>Source Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td></td>
<td>Destination Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>160</td>
<td></td>
<td>(Options)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>160+</td>
<td></td>
<td></td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
</tbody>
</table>

- 4 bits
- 4 bits
- 8 bits
- 3 bits
- 13 bits

Lect06 2/12/2018 © JE Savage
Format of IP Packets

• Header checksum identifies transmission errors
  – Checksum recomputed every time TTL decremented.
• IPv4 addresses are 4 bytes e.g. 128.148.32.5 where each byte (8-bits) is in the range [0-255].
• IPv6 addresses are 8 sets of 4 hexadecimal digits from [0,1,2,...,9,a,b,...,f] each representing 4 bits,
  • \((8 \times 4 \times 4 = 128)\)
  • e.g. 2001:0db8:1234:0000:0000:0000:0000:0000
More on Format of IP Packets

• A domain (prefix) defines a block of IP addresses that is associated with a subnetwork.
• A domain is specified by (IP address)/(integer) and assigned to an autonomous system.
• E.g. 128.148.32.5/24 specifies a set of IPv4 address beginning with first 24 address bits.
  – What are the first 24 bits?
• The domain contains the addresses 128.148.32.0, 128.148.32.1, ..., 128.148.32.255.
• Since there are $2^8 = 256$ choices for the last 8 = 32-24 bits, this prefix defines 256 addresses in the subnetwork.
Internet Control Message Protocol

- **ICMP** is network layer protocol for testing and error notification. Message types shown below
  - Echo request – asks destination to acknowledge
  - Echo response – acknowledges receipt of packet
  - Time exceeded – sends notification that TTL = 0
  - Destination unreachable – packet not delivered
- **Ping** uses ICMP to tell if machine reachable

PING princeton.edu (140.180.223.22): 56 (84) bytes of data
64 bytes from Princeton.EDU (140.180.223.22): icmp_seq=1 ttl=243 time=11.3 ms
64 bytes from Princeton.EDU (140.180.223.22): icmp_seq=2 ttl=243 time=12.2 ms
...

Lect06 2/12/2018 © JE Savage
Traceroute

- **Traceroute** uses ICMP to trace path from source to destination.

```
Packet dropped here, response sent
```

```
<table>
<thead>
<tr>
<th>Time exceeded</th>
<th>Echo request, TTL = 1</th>
</tr>
</thead>
</table>
```

```
<table>
<thead>
<tr>
<th>Time exceeded</th>
<th>Echo request, TTL = 2</th>
</tr>
</thead>
</table>
```

```
<table>
<thead>
<tr>
<th>Time exceeded</th>
<th>Echo request, TTL = 3</th>
</tr>
</thead>
</table>
```

```
<table>
<thead>
<tr>
<th>Time exceeded</th>
<th>Packet dropped here, response sent</th>
</tr>
</thead>
</table>
```
Traceroute Example

- traceroute to princeton.edu (140.180.223.22), 30 hops max, 60 byte packets
- 1 10.116.52.1 (10.116.52.1) 1.414 ms 1.515 ms 1.716 ms
- 2 commodus-int.cs.brown.edu (10.116.1.5) 0.171 ms 0.160 ms 0.150 ms
- 3 138.16.160.253 (138.16.160.253) 1.897 ms 1.898 ms 1.905 ms
- 4 vl2062-ddmz-cit-r.net.brown.edu (10.1.18.1) 0.904 ms 0.923 ms 0.907 ms
- 5 lsb-inet-r-230.net.brown.edu (128.148.230.6) 0.969 ms 0.961 ms 1.198 ms
- 7 bostonlight.oshean.org (198.7.255.1) 3.248 ms 3.566 ms 3.565 ms
- 8 nox300gw1-oshean-re.nox.org (192.5.89.125) 3.541 ms 3.506 ms 3.490 ms
- 9 i2-re-nox300gw1.nox.org (192.5.89.222) 7.809 ms 8.164 ms 8.105 ms
- 10 216.27.100.5 (216.27.100.5) 10.280 ms 10.218 ms 10.197 ms
- 11 remote1.princeton.magpi.net (216.27.98.114) 11.261 ms 11.253 ms 11.226 ms
- 12 core-87-router.Princeton.EDU (128.112.12.130) 11.919 ms 12.503 ms 12.150 ms
- 13 Princeton.EDU (140.180.223.22) 11.505 ms 11.498 ms 11.489 ms
IP Spoofing

• Host/router can change Source Address in a packet.
  – Can be used in denial of service attack.
  – If ICMPs are sent to many destinations with the same spoofed source address, all respond to spoofed source, swamping it.

• Coping with IP spoofing:
  – Routers should drop a packet entering a domain with source address from inside that domain.
  – Should also drop leaving packets whose source is outside.
  – If routers log packets passing through them, which is not always done, can trace spoofed packets back to a source.
Protocol Layers Again

Network Topology

Data Flow

Transport Layer Protocols

• Connect a process at one port of an IP address to a process at a port of a remote IP address. $2^{16}$ ports.
• TCP and UDP are primary protocols at this layer.
• Transmission Control Protocol (TCP) provides reliable packet stream between ports. Packets repeated if lost.
  – What should it be used for? files, web pages, email
• User Datagram Protocol (UDP) provides best-effort communication between ports. Send it and forget it
  – Used for VoIP and apps where lost bytes not important.
Transmission Control Protocol (TCP)

- TCP/IP sets up connection to destination using three-way handshake.
  - Packets are sent with a sequence number so that they can be assembled in order.
  - If a packet is not acknowledged during a congestion window (a reasonable round trip time) it is repeated. Thus, copies of packets can be in network.
  - The sender uses flow control (adjusts window) to avoid overwhelming the receiver.
  - If payload checksum fails, receiver rejects packet.
### TCP Packet Format

<table>
<thead>
<tr>
<th>Bit Offset</th>
<th>0-3</th>
<th>4-7</th>
<th>8-15</th>
<th>16-18</th>
<th>19-31</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td>Source Port</td>
<td>Destination Port</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td>Sequence Number (Seq)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td></td>
<td></td>
<td>Acknowledgement Number (Ack)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>Offset</td>
<td></td>
<td>Reserved Flags</td>
<td>Window Size</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td></td>
<td>Checksum</td>
<td></td>
<td>Urgent Pointer</td>
<td></td>
</tr>
<tr>
<td>160</td>
<td></td>
<td></td>
<td>Options</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| >= 160     |     |       | Data | Data | Data | ...

Port 80 for HTTP, 21 for FTP, 22 for SSH, for example.

$2^{16} = 65,536$ ports
Three-Way TCP Handshake

1. SYN
   Seq = X
2. SYN-ACK
   Seq = Y
   Ack = X+1
3. ACK
   Seq = X+1
   Ack = Y+1
TCP Three-Way Handshake

- Establishes connection between source/dest.

1. **Source S** sends a packet to **destination D** with SYN flag on and random sequence number Seq = X.
2. D sends S a packet with both SYN and ACK flags on adds a random sequence number Seq = Y, and an acknowledgement number Ack = X+1. (S checks X)
3. S sends D a packet with SYN flag off, ACK flag on, Seq = X+1 and Ack = Y+1. (D compares Ack to Y.)

   If successfully completed, TCP connection is made.

- Random values for X and Y help defeat attacks.
User Datagram Protocol (UDP)

- Header includes source and destination ports, length, checksum, and payload
- Designed for speed, not accuracy.
- Used for time-sensitive tasks such as
  - DNS and Voice over IP (VoIP)
Network Address Translator (NAT)

• A **NAT** is hardware that maps one external IP address into multiple internal IP addresses.
• Each internal IP address is assigned a unique port number of the external IP address.
• When packet sent back to the IP address, its port number is used to lookup is internal IP address.
  – The packet IP address is changed to the internal one.
• A NAT hides internal IP addresses – **protects** against random hits
TCP Session Hijacking

• Attacker takes over or spoofs a TCP session.
  – Attacker needs seq numbers for server ACK packets
  – If attacker on same network as client or server, packet sniffing can reveal seq numbers.
  – If not, attacker can try predicting seq numbers.

• Blind injection – attacker sends packet to server, client (not attacker) receives the packet.
  – Can lead to storm of ACK packets between client and server as they try to synchronize one another.

• Spoofing – attacker can become man-in-middle!
Denial of Service (Flooding) Attacks

- Because bandwidth is limited, many packets directed to a client, can overwhelm client.
  - Ping flood attack
  - SYN flood attacks
  - Optimistic TCP attacks
  - Distributed denial of service (DDoS) attacks
    - Denial of service from many sites, such as botnet.
- Can defend against DDoS via IP tracebacks or more sophisticated automatic techniques.
Ping Flood Attack

• Attacker floods victim with pings (ICMP packets)
  – Attacker can be much more powerful than victim.

• SMURF attack – attacker sends ICMP packet with spoofed address to network broadcast site.

• All sites on network respond to spoofed site.
SYN Flood Attacks

• Attacker opens many TCP sessions by sending SYN packets to a victim without replying to SYN/ACK packets from the victim.

• Victim keeps list of SYN seq numbers in memory so that it can synchronize sessions.

• If too many sessions are opened, victim’s memory fills up, blocking other TCP sessions.
  – Routers can be redesigned to avoid this.
Two Defenses Against SYN Flood Attacks

• SYN Cookies
  – Recipient of SYN does not reserve session space.
  – Instead, it sends special seq no. to source identifying it.
  – If SYN/ACK response is with valid seq. no., session space is reserved.
  – Not adopted by Windows – in some Linux versions

• SYN Queue
  – Half-opened TCP connections put on special queue
  – They are dropped if no SYN/ACK reply soon enough
  – Adopted by Windows
IP Traceback

- IP traceback uses one of several techniques to determine the source of packets.

- Examples
  - Mark packets with information about path travelled
  - Node sampling: overwrite an address field with router address with some probability.
    - With high probability all the IP addresses of visited routers can be determined if packet stream long enough.
  - Send info on packet stream going through a router to the destination via an independent stream.
Review

• Network security
• The link layer
• The network layer
• The transport layer
• Denial of service attacks
iClicker Question

TCP was invented by Kahn and Cerf

A. Yes

B. No, it was invented by Thomas C. Paine