An Overview of Network Security

Coverage

• Lower Layers
• Upper Layers
• The Web

• From Security Point of View
Network taxonomy

Telecommunication networks

- Circuit-switched networks
  - FDM
  - TDM

- Packet-switched networks
  - Networks with VCs
  - Datagram Networks

What’s the Internet: “nuts and bolts” view

- millions of connected computing devices: *hosts, end-systems*
  - PCs workstations, servers
  - PDAs phones, toasters
    running *network apps*
- *communication links*
  - fiber, copper, radio, satellite
    transmission rate = *bandwidth*
- *routers*: forward packets (chunks of data)
What’s the Internet: “nuts and bolts” view

- **protocols** control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, FTP, PPP
- **Internet:** “network of networks”
  - loosely hierarchical
  - public Internet versus private intranet
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force

What’s the Internet: a service view

- **communication infrastructure** enables distributed applications:
  - Web, email, games, e-commerce, database, voting, file (MP3) sharing
- **communication services provided to apps:**
  - connectionless
  - connection-oriented

- **cyberspace** [Gibson]:
  “a consensual hallucination experienced daily by billions of operators, in every nation, ...."
A closer look at network structure:

- **network edge:** applications and hosts
- **network core:**
  - routers
  - network of networks
- **access networks, physical media:** communication links

The network edge:

- **end systems (hosts):**
  - run application programs
  - e.g. Web, email
  - at “edge of network”
- **client/server model**
  - client host requests, receives service from always-on server
  - e.g. Web browser/server; email client/server
- **peer-peer model:**
  - minimal (or no) use of dedicated servers
  - e.g. Gnutella, KaZaA

Copyright © 2003 Jun Li.
All rights reserved.
The network core

- mesh of interconnected routers
- *the* fundamental question: how is data transferred through net?
  - circuit switching: dedicated circuit per call: telephone net
  - packet-switching: data sent thru net in discrete “chunks”

Lower Layers

- IP
- ARP
- ICMP
- TCP
- UDP
- SCTP
- Routing Protocols
  - RIP, OSPF, BGP
- DNS
- BOOTP & DHCP
- IPv6
- NAT
- Wireless Security
IP
A network layer protocol:

transport layer: TCP, UDP

Routing protocols
- path selection
- OSPF, BGP

forwarding table

IP datagram format

header length
(type) of data
max number
remaining hops
(decremented at
each router)
upper layer protocol
to deliver payload to

IP protocol version
number

32 bit destination IP address
32 bit source IP address

32 bit destination IP address

length

E.g. timestamp,
record route
taken, specify
list of routers
to visit.

Options (if any)

head

flags

frag

offset

Internet checksum

time to live

upper layer

IP protocol
- addressing conventions
- datagram format
- packet handling conventions

ICMP protocol
- error reporting
- router "signaling"

Transport layer: TCP, UDP

Routing protocols
- path selection
- OSPF, BGP

forwarding table

Link layer

physical layer
IP Packet Forwarding

- no call setup at network layer
- routers: no state about end-to-end connections
  - no network-level concept of “connection”
- packets forwarded using destination host address
  - packets between same source-dest pair may take different paths

IP Security Issues

- IP Spoofing
  - Forged source address
    - Any host can transmit a packet with any source address
- Packet inception
  - Man-in-the-middle attack
- What else?
ARP: Address Resolution Protocol

Question: how to determine MAC address of B knowing B's IP address?

- Each IP node (Host, Router) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes
  - < IP address; MAC address; TTL>
  - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

ARP Security Issues

- Problematic if an untrusted node has write access to the local net
- ARP spoofing
  - Use phony queries or replies
  - Such that all/some traffic misdirected
- What else?
ICMP: Internet Control Message Protocol

• used by hosts, routers, gateways to communication network-level information
  – error reporting: unreachable host, network, port, protocol
  – echo request/reply (used by ping)
• network-layer “above” IP:
  – ICMP msgs carried in IP datagrams
• ICMP message: type, code plus first 8 bytes of IP datagram causing error

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>echo reply (ping)</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>dest. network unreachable</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>dest host unreachable</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>dest protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>dest port unreachable</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>dest network unknown</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>dest host unknown</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>source quench (congestion control - not used)</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>echo request (ping)</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>route advertisement</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>router discovery</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>TTL expired</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>bad IP header</td>
</tr>
</tbody>
</table>

ICMP Security Issues

• ICMP can be abused to tear down connections
• Can also be abused to create new paths to a destination
  – Using the REDIRECT ICMP message
• Block ICMP messages at firewalls?
TCP

- point-to-point:
  - one sender, one receiver
- reliable, in-order byte stream:
  - no “message boundaries”
- pipelined:
  - TCP congestion and flow control set window size
- send & receive buffers

- full duplex data:
  - bi-directional data flow in same connection
  - MSS: maximum segment size
- connection-oriented:
  - handshaking (exchange of control msgs) init’s sender, receiver state before data exchange
- flow controlled:
  - sender will not overwhelm receiver

TCP Segment

- source port #
- dest port #
- sequence number
- acknowledgement number
- head len
- URG, ACK, PSH:
  - URG: urgent data (generally not used)
  - ACK: ACK # valid
  - PSH: push data now (generally not used)
- RST, SYN, FIN:
  - RST, SYN, FIN: connection estab (setup, teardown commands)
- Internet checksum (as in UDP)
- receive window
- checksum
- Urg data pointer
- Options (variable length)

- application data (variable length)
- # bytes rcvr willing to accept
- counting by bytes of data (not segments!)
TCP Security Issues

• TCP open
• TCP privileged ports
• TCP stream vs. firewall

TCP Security Issues
- TCP Open

• SYN Attacks
  – Flood a TCP server with SYN packets
  – Make the server in half-opened status with many connections
  – Can cause DDoS
• Detect what services a server provides
• Sequence number attack
  – If an attacker can predict the sequence number expected by an victim
TCP Security Issues
- Privileged ports

- What are privileged ports
  - A unix convention that only can be created by the root
  - Less than 1024
  - Goal: remote systems can trust the authenticity of into written to such ports

- This goal really is just a hope
  - Not required by TCP specification
  - Meaningless on non-Unix systems
  - One may not necessarily trust the sanctity of a privileged port

TCP Security Issues
- TCP Stream vs. Firewall

- With TCP, data flows like a stream
  - There is no boundary
  - Thus hard for a firewall to filter individual packets
TCP Security Issues

• What else?

UDP

• Extends to applications the same level of service used by IP
  – Best-effort delivery
• Security Issues
  – UDP has no flow control, etc.
    • Large UDP transmissions may swamp the network
  – Certainly still has the IP spoofing problem
  – What else?
SCTP

• A new transport protocol (stream control transmission protocol)
• Read the brief description from course reserve materials

Routing Protocols

• Routing is the process of discovering, selecting, and employing paths from sources to destinations
• Often asymmetric
• RIP, OSPF, IS-IS, BGP, etc.
Security Issues

• Some routing options can be abused
  – Source routing
• A routing protocol itself can be subverted
  – Inject bogus routing updates, for example
    • A good router may be cheated to spread deceptive
      routing updates
  – A router could be compromised

BGP Security Issues

• BGP is a routing protocol for the core of the
  Internet at AS level
  – Routing announcements are exchanged via TCP
• Corrupt announcements can be used to perform a
  variety of attacks
  – An attacker can play BGP games
    • Can eavesdrop on, hijack or suppress BGP sessions
  – And other attacks
DNS

• A distributed database that maps hostnames to IP addresses, or vice versa
• Two logically distinct tree-structured namespaces
  – One for name to IP address (forward mapping), the other for IP address to name (backward mapping)
• Transport protocols for DNS
  – DNS query is UDP-based
  – But zone transfer is TCP-based
    • For backup servers to get a full copy of their portion in the name space

DNS Security Issues

• An attacker in control of the inverse mapping tree
  – A non-trusted IP address may thus map to a trusted name
  – Well, easy to deal if the forward mapping tree is authentic (cross-checking)
  – The attacker can further try to poison the victim’s DNS cache
• Omission of a trailing period
  – “foo.com” will be tried as “foo.com.cs.uoregon.edu” then “foo.com.uoregon.edu” then “foo.com.edu” then “foo.com”
  – What if an attacker builds a name server for “com.edu” domain?
BOOTP & DHCP

- DHCP is an extension of the simpler BOOTP
- Through a DHCP server, a client can obtain a lot of info
  - IP address
  - DNS server
  - Default route address
  - Default domain name, or even
  - NTS server
  - etc.

DHCP Security Issues

- DHCP runs on a LAN
  - Thus less security concerns
- But still subject to man-in-the-middle and DOS attacks
  - Essentially same security issues as ARP
- A rogue DHCP server?
- Applying for DHCP service endlessly?
  - To deplete available IP addresses for a local domain
- What else?
IPv6

- Same philosophy as IPv4 as an unreliable best-effort delivery protocol
- Allows interesting address types
  - Anycast addresses
    - Multiple machines map to the same address
  - Site-local addresses
    - Some addresses are purely local to a “site”
  - Link-local addresses
    - Limited to a single link
- New protocols
  - Neighbor Discovery protocol (similar to ARP)
  - DHCPv6

IPv6 Security Issues

- Renumbering
  - How to enforce a secure incremental v4->v6 transition?
- Hosts can generate its own temporary IP address
  - Making the traceback harder
- Anycast addresses
  - How to decide exactly which machine is the attacker
- Site-local and link-local addresses
  - Uncertain whether this is a good access control mechanism
- IPv6-capable firewall?
- What else?
NAT Security Issues

- Does not get along well with encryption
  - The port number is often encrypted as part of IP payload
  - IPsec is not compatible with NAT
    - IPsec protects checksum, which includes the IP address
Wireless Security

• Limited energy
  – Battery attack

• Easier eavesdropping
  – Cannot just lock your office door

• Harder border control
  – Can a wireless firewall be set up?

• Fragile routing infrastructure
  – Normal wireless nodes used as forwarding nodes

• Harder to trace back an attacker
  – Nodes are often mobile

• Security service is often not available
  – Hardly any on authentication, key management, etc.