CMPE 151: Network Administration

Lecture 6

Spring 2004
Project 6: Network Gateway

- Firewall.
- NAT.
Firewalls

- What is a firewall?
  - Security at the network level.
- Wide-area network access makes vital information/resources available (corporations, educational and research institutions).
- But, security threats from (mainly) the “outside world”.
- Secure each machine and/or protect the whole network.
Firewalls

- “Outer security wall”.
- Protect organization’s network from attacks originating outside network.
  - Also, single “choke point” for security and auditing purposes.
- Firewall can be a single machine or a group of machines performing the firewall functions collaboratively.
Firewalls (cont’d)

- Convenient location for other “Internet-related” functions, e.g., NAT’ing, auditing Internet usage, etc.
Firewall operation

- All incoming/outgoing traffic must pass through firewall.
- Only authorized traffic (as defined by local security policy) allowed to pass.
- Firewall itself immune to penetration (trusted system + secure OS).
Types of access control

- Service control: types of service that can be accessed (inside and outside).
  - Filtering based on IP address and TCP port #.
  - Proxy services that receives and interprets traffic.
  - May host service, e.g., Web server.
- Direction control: determines directions in which certain traffic allowed to flow.
Types of access control (cont’d)

- User control: determines which user allowed to access which service.
- Behavior control: controls access to particular services (e.g., filtering out e-mail spam, enabling external access to only portion of Web server information, etc.).
Types of firewalls

- Packet-filtering.
- Application-level.
- Stateful inspection.
- Circuit-level.
Packet-filtering firewalls

- Restricts type of traffic that go through.
- Applies set of rules to each IP packet.
  - Decides to forward or discard it.
- Filters packets in both directions.
- Filtering based on packet header (IP and transport) information (e.g., destination/source address, port number, IP protocol field).

Spring 2004
Rules

- Consist of `<expression>` and `<action>`.
- `<expression>`: IP/TCP/UDP fields and values.
- `<action>`: discard or forward.

Default policies:
- Discard: whatever is not expressly permitted is discarded.
- Forward: ...

Rules are added as new threats become known.

Spring 2004
## Example rules

<table>
<thead>
<tr>
<th>action</th>
<th>ourhost</th>
<th>port</th>
<th>theirhost</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>OUR-GW</td>
<td>25</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>block</td>
<td>*</td>
<td>*</td>
<td>SPIGOT</td>
<td>*</td>
</tr>
</tbody>
</table>
Observations

- Service-specific filtering based on client using non-privileged port to contact privileged server port.
- FTP uses 2 TCP connections: one for control and another for data.
  - Client initiates control connection and server initiates data connection.
  - If FTP is allowed, need to allow inbound access to all non-privileged (> 1024) TCP ports.

Spring 2004
Two-stage filtering

- One machine gateways to the Internet; the other lies between the outer gateway and the rest of the local net.
  - Outer gateway relatively open.
  - Inner gateway very conservative.
  - FTP and other “less secure” network services available from outer gateway.
Limitations

- Cannot protect against attacks bypassing the firewall (e.g., local users with dial-up connections to ISP).
- Cannot protect against internal threats (e.g., malicious local user).
- Cannot protect against transfer of virus-infected files.
Application-level firewalls

- Also called service proxy firewalls.
- Acts as relay for application-level traffic.
- Intercepts connections to/from outside world and establish connections to service outside/inside local network.
- User contacts firewall using specific application (e.g., telnet, http, etc.); firewall contacts remote host and relays application traffic between two endpoints.
- Firewall must support specific applications.

Spring 2004
Observations

- Application-level firewalls tend to be more secure: they only need to secure a few applications.
  - Easier to log and audit application-level traffic.

- Drawbacks:
  - Non-transparent.
  - Slower.
  - Less flexible.

Spring 2004
Stateful inspection firewalls

- Inspect traffic that flows through to detect “abnormal” activity.

- Example:
  - Examine FTP control exchange for data port; firewall should expect data connection to that port.

- Problem: keep state for all active connections using different protocols.
  - Current stateful inspection firewalls inspect limited number of connections/protocols.
  - Or, search for known attack patterns.

Spring 2004
Circuit-level firewalls

- Acts as intermediate to all TCP connections.
  - Always sets up 2 connections: between local user and itself and itself and remote host.
  - Usually relays data without inspection.
  - Security relies on determining which connections to allow.

Spring 2004
Circuit-level gateway example

- SOCKS package.
  - SOCKS version 5 specified in RFC 1928.
- Client opens connection to appropriate SOCKs port on SOCKs server (port 1080).
- Authentication exchange and then relay request.
- Server evaluates request and establishes TCP connection or denies it.
Firewall configurations

- More complex configurations.
- Combine multiple firewalls.
How safe are firewalls?

- Should not be the single defense.
- Supplemental security measure.
  - Negative effect if it causes other defenses to be weakened/not employed.
- Individual hosts should be protected.
  - Tools like crack, COPS, tripwire, etc.
Security policies

- Local users should be able to connect to any Internet service.
- But, outside users should only be allowed to connect to limited set of local services (e.g., FTP access to local archive, SMTP connections to mail server).
Sources of security-related information

- CERT
  - Computer Emergency Response Team.
  - DARPA sponsored organization at CMU.
  - Basically, informational: CERT advisories.
    - Vendor security patches.
    - Security tool announcements.
    - Known security attacks.
More sources of security info...

- SecurityFocus.com
  - Security information repository: news, relevant papers, tools.
  - BugTraq mailing list.
    - Discussion of security vulnerabilities and fixes.
    - Mail to listserv@securityfocus.com.

- SANS
  - System Administrator, Networking and Security Institute.
  - Sponsors conferences, training, etc.
  - www.sans.org.

Spring 2004
NAT

Spring 2004
NAT

- Network address translation.
- Quick fix to address depletion problem.
  - Organization assigned one or a few IP addresses.
  - NAT box replaces “internal” addresses with real IP address on the way out.
NAT Illustration

Operation: Sp wants to talk to Dg:
• Create Sg-Sp mapping
• Replace Sp with Sg for outgoing packets
• Replace Sg with Sp for incoming packets

Q: What happens if we reverse the question and Dg wants to talk to Sp?

Spring 2004
NAT disadvantages

- Need to keep track of who originated the connection to be able to route back to that host/port.
- TCP source port field replaced with index into NAT box translation table which holds internal IP address and port number.
NAT disadvantages (cont’d)

- Violates “IP address uniqueness”.
- Violates “stateless” design principle.
- Violates layering principle or Internet’s “end2end”ness.
- What if TCP and UDP are not used?
  - Application-specific gateways.
More details

- Also, look at references on both books.