Why Firewalls?

- Need for the exchange of information; education, business, recreation, social and political
- Need to do something useful with your computer
- Drawbacks; unsolicited attention and bugs

Why Firewalls?

- There are a lot of people on the Internet
- Millions of people together -> bad things happen
- True for cities; it is true for the Internet
- With the Internet...
  - Everyone is in your backyard!
  - You can be scoped out at any time from anywhere
  - The community discourages neighborhood watch like activities (a hot potato!)

Bugs, Bugs, Bugs

- All programs contain bugs
- Larger programs contain more bugs!
- Network protocols contain;
  - Design weaknesses (SSH CRC)
  - Implementation flaws (SSL, NTP, FTP, SMTP...)
- Careful (defensive) programming & protocol design is **hard**
What is a Firewall?

- Literally?
  - Prevents fire from spreading!
- The Castle & Moat Analogy
  - Restricts access from the outside
  - Prevents attackers from getting too close
  - Restricts people from leaving  <- Important!!

What is a Firewall?

- Logically
  - A separator, a restrictor and an analyzer
- Rarely a single physical object!
- Practically any place where internal and external data can meet

Where do you put a Firewall?

- Between insecure systems & the Internet
- To separate test or lab networks
- For networks with more sensitive data;
  - Financial records
  - Student grades
  - Secret projects
- Partner or joint venture networks

Firewall Design & Architecture Issues

- Least privilege
- Defense in depth (very important)
- Choke point
- Weakest links
- Fail-safe stance
- Universal participation
- Diversity of defense
- Simplicity
Firewall Architectures

Packet Filtering: IPv4 Packet Header

http://www.faqs.org/rfcs/rfc760.html

Packet Filtering: UDP Packets

http://www.faqs.org/rfcs/rfc768.html

Packet Filtering: TCP packet structure

http://www.faqs.org/rfcs/rfc761.html
Packet Filtering: Ipv6 Packet Header

+---------+----------+-----------------+
| Version | Prio.    | Flow Label      |
+---------+----------+-----------------+
| Payload Length | Next Header | Hop Limit |
+---------+----------+-----------------+
| Source Address |
+---------+----------+-----------------+
| Destination Address |


Packet Filtering: Summary

- IP Source Address
- IP Destination Address
- Protocol/Next Header (TCP, UDP, ICMP, etc)
- TCP or UDP source & destination ports
- TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
- ICMP message type
- Packet size
- Fragmentation

Router Knowledge

- Interface packet arrives on
- Interface a packet will go out
- Is the packet in response to another one?
- How many packets have been seen recently?
- Is the packet a duplicate?
- Is the packet an IP fragment?

Filtering Example: Inbound SMTP
Filtering Example: Outbound SMTP

Stateful or Dynamic Packet Filtering

Network Address Translation (NAT)
Port & Address Translation (PAT)

Normal Fragmentation
Abnormal Fragmentation

<table>
<thead>
<tr>
<th>Normal</th>
<th>Overlapping data</th>
<th>Overlapping headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
<td>TCP Header</td>
<td>DATA...</td>
</tr>
<tr>
<td>IP Header</td>
<td>TCP Header</td>
<td>DATA...</td>
</tr>
<tr>
<td>IP Header</td>
<td>TCP Header</td>
<td>DATA...</td>
</tr>
<tr>
<td>IP Header</td>
<td>TCP Header</td>
<td>DATA...</td>
</tr>
</tbody>
</table>

Firewall Architectures

**Screened Host Architecture**

- Bastion Host
  - A secured system (it will interact/accepts data from the Internet)
  - Disable all non-required services; keep it simple
  - Install/modify services you want
  - Run security audit to establish baseline
  - Connect system to network ← important
  - Be prepared for the system to be compromised

**Screened Subnet Architecture Using Two Routers**
Firewall Architectures

Proxies

- Application level; dedicated proxy (HTTP)
- Circuit level; generic proxy
  - SOCKS
  - WinSock – almost generic proxy for Microsoft
- Some protocols are “natural” to proxy
  - SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)
Firewall Architectures

A web server using a database on a perimeter network

Problems with Firewalls

- They interfere with the Internet
- They don’t solve the real problems;
  - Buggy software
  - Bad protocols
- Generally cannot prevent Denial of Service
- Are becoming more complicated
- Many commercial firewalls permit very, very complex configurations

Elizabeth D. Zwicky, Simon Cooper
D. Brent Chapman

Questions?

Simon Cooper <sc@sgi.com>