“We don’t need no data protection.
We don’t need no access control.”

Wanli Liu
CSC457:Computer Networks
Nov. 20th, 2001
Why Firewall?

- Curious hackers
- Vandals
- Industrial spies
- Accidental data disclosure

Solution? Firewall
What is Firewall?

A computer or computer software that prevents unauthorized access to private data (as on a company’s local area network or intranet) by outside computer users (as of the Internet)

By definition, firewall is a combination of hardware and software.

• Architecture
• Functions
Firewall Architecture(I)

• Single Layer
  functions concentrated on one host, small number of networks inter-connected
  
  cost-effective, easy to maintain

  susceptibility to implementation flaws or configuration errors
Firewall Architecture(II)

• Multi-Layer
  firewall functions distributed on a number of hosts

✓ Greater security, can use different tech in different hosts to reduce implementation flaws and configuration errors

✗ Costly, difficult to design, configure and operate
Firewall Functions

• packet filtering : *simple, fast*
• application proxies : *complex, slow*
• combination of above two (stateful inspection packet filters)
Function I: **Packet filtering**

- Executed by routers (or host acting as router)
- Checking packet headers (e.g. source IP, destination IP, protocol, port)
- High level performance coming from low layer configuration
Packet filtering: Checking header

- IP address filtering
- TCP/UDP port filtering
- Client TCP/UDP port filtering
Packet filtering: Checking payload

- Stateful inspection packet filters
- Filtering decision based on inspection of both header and payload
- Provide more complex access control
<table>
<thead>
<tr>
<th>Router vs. Computer</th>
<th>Special purpose router</th>
<th>General purpose computer</th>
<th>Minimal functional extensibility May require more memory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Highest performance</td>
<td>Unlimited functional extensibility</td>
<td>Small number of interfaces</td>
</tr>
<tr>
<td></td>
<td>Large number of interfaces</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Function II: **Application Proxy**

- Proxy forward traffic in two/one direction
- Proxy running on proxy machines or general purpose computers
Introduction to TIS firewall

- TIS – Trusted Information System
- A set of programs and configuration practices
- Designed to run on UNIX systems using TCP/IP with Berkeley-style socket interface
Configuration I: Dual-homed Gateway

- The host connected to Internet and private network
- Routing between Internet and private network disabled
- Private network invisible to Internet except host, which provides proxies to services
Configuration II: Screened Host Gateway

- Packet screening capability of router
- Traffic permitted only to bastion host
Screened Host Gateway

• Most common, most flexible
• Screening router can be configured to permit nodes on private network to directly access Internet via TELNET or FTP
Configuration III: Screened Subnets

- A “sandbox” network between Internet and private network
- Nodes on Internet and private network can only communicate with “sandbox” network
Proxies / Application Gateway

- Application gateways handle store and forward traffic and some types of interactive traffic
- Log/audit traffic
TIS Toolkit Proxies

- Tn-gw : TELNET protocol proxy
- Rlogin-gw : Rlogin
- Ftp-gw : FTP protocol proxy
- Plug-gw : Generic TCP “plug-board” proxy
Example: Netacl, Telnet-Gw

- Netacl manages network access control
- Permit access based on client’s network address and service requested
- No support for UDP security, disabled
- System call *chroot* before invoking service so that service is performed in an empty directory and no executables are available for attackers
Netacl, Telnet-Gw (continued)

- Rely on IP address and/or host names
- Susceptible to IP spoofing via source-routing
- Router capable of screening source routed packets is necessary