Computer Security Pt. 2 & FreeBSD Security

Dr. Sean Peisert
Guest Lecture for UCD ECS 150 (Operating Systems)
June 4, 2008

peisert@cs.ucdavis.edu
http://www.sdsc.edu/~peisert
Goals

• Confidentiality

• Integrity

• Availability
Security Methods

- Detection
- Prevention
- Recovery
- Analysis
- (repeat)
Issues

• Physical security

• Operational security
  • Technical solutions
  • Procedural solutions
Technical Mechanisms

- The Players
  - Subjects (and Domains)
  - Objects
  - Actions

- Access control (and access control lists)

- Protection domains in practice, and capability-based systems
Protection Rings (as in MULTICS)
Protection Rings (as in MULTICS)
Saltzer and Schroeder’s Design Principles

- *Economy of Mechanism*
- *Fail-Safe Defaults*
- *Complete Mediation*
- *Open Design*
- *Separation of Privilege*
- *Least Privilege*
- *Least Common Mechanism*
- *Psychological Acceptability*
Several FreeBSD Mechanisms

• Explicit:
  • Access Controls
  • Encryption (e.g., crypt, ssh, IPsec)
  • “BSM”
  • Verified Exec (in NetBSD)
  • Jail/chroot

• Implicit
  • Good code!
  • Simple code!
  • Documented code!
  • Open code!
## Basic Access Control Example

<table>
<thead>
<tr>
<th>File /tmp/x</th>
<th>Owner</th>
<th>Group</th>
<th>World</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Write</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Permissions Example

Listing permissions:
% ls -l x
   -rwxr-xr--  1 sean  staff  0 May 27 16:53 x

(first char is ‘l’ for symlinks, ‘d’ for directories, etc...)

Changing permissions:
% chmod u+rwx x
% chmod g+rx
% chmod o+r

or

% chmod 754 x
Access Control Lists in FreeBSD

- `getfacl` and `setfacl` commands
- Specific lists of users (not just groups)
- Read, Write, Execute
- Rename, Delete, Append, Inherit, etc...
FreeBSD Kernel Security Level

- Immutability
- Append only
- “No delete”
Examples of Kernel Security Levels in FreeBSD

<table>
<thead>
<tr>
<th>System Property</th>
<th>Securelevel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-1</td>
</tr>
<tr>
<td>System immutable and append-only flags can be changed</td>
<td>√</td>
</tr>
<tr>
<td>Raw disk devices for mounted file systems can be written</td>
<td>√</td>
</tr>
<tr>
<td>/dev/mem and /dev/kmem can be written</td>
<td>√</td>
</tr>
<tr>
<td>Kernel modules can be loaded and unloaded</td>
<td>√</td>
</tr>
<tr>
<td>Non-mounted raw disk devices can be written</td>
<td>√</td>
</tr>
<tr>
<td>Filesystems can be mounted</td>
<td>√</td>
</tr>
<tr>
<td>Time can be adjusted more than one second forward or back</td>
<td>√</td>
</tr>
<tr>
<td>IP filtering and firewall rules can be changed</td>
<td>√</td>
</tr>
</tbody>
</table>
Setting Kernel Security Level in FreeBSD

• In `/etc/rc.conf`

  • `kern_securelevel_enable="YES"`

  • `kern_securelevel="2"`
Mandatory Access Control

- Policy is set in the kernel, not by the user

- Multi-Level Security (MLS)
  - Biba model
    - “No writes up, no reads down”
  - Bell-LaPadula model
    - “No reads up, no writes down”
Logging

- syslog
- TCPWrappers
- BSM
Questions?

• Email: peisert@cs.ucdavis.edu

• Web: http://www.sdsc.edu/~peisert