Have You Driven an SELinux Lately?

An update on the Security Enhanced Linux Project

James Morris
Red Hat Asia Pacific Pte Ltd

Ottawa Linux Symposium 2008
Project Timeline

• 1980s – 1990s
  – Academic R&D

• 2000 – 2003
  – GPL release, upstream merge

• 2003 – 2005
  – Distribution integration

• 2005 – present
  – Infrastructure and usability improvements
Infrastructure Work

- Loadable Policy Modules
- Reference Policy
- Policy Booleans
- Libraries
- Toolchain
User Experience

• Targeted Policy
  – Initially confined only critical applications
  – Now re-merged with hundreds of modules
    • Targeted behavior selected via the unconfined module

• Setroubleshoot
  – Inspired by GNOME bug buddy
setroubleshoot

Summary
SELinux is preventing the sshd (sshd_t) from binding to port 330.

Detailed Description
SELinux has denied the sshd from binding to a network port 330 which does not have an SELinux type associated with it. If sshd is supposed to be allowed to listen on this port, you can use the semanage command to add this port to a port type that sshd_t can bind to. semanage port -l will list all port types. Please file a [bug report](https://bugs.example.com) against the selinux-policy package. If sshd is not supposed to bind to this port, this could signal a intrusion attempt. If this system is running as an NIS Client, turning on the allow ypbind boolean, may fix the problem. setsebool -P allow_ypbind=1.

Allowing Access
If you want to allow sshd to bind to this port semanage port -a -t PORT_TYPE -p PROTOCOL 330 Where PORT_TYPE is a type that sshd_t can bind and PROTOCOL is udp or tcp.

Additional Information
Source Context: unconfined_u:system_r:sshd_t:systemLow:systemHigh
Target Context: system_u:object_r:reserved_port_t
Target Objects: None [ tcp_socket ]
Source: sshd
Source Path: /usr/sbin/sshd
Port: 330
Host: e
Source RPM Packages: openssh-server-5.0p1-3.fc9

Audit Listener 7/7
System Administration

- audit2why
- semanage
- restorecond
- system-config-selinux
### SELinux Administration

#### Boolean Configuration

<table>
<thead>
<tr>
<th>Active</th>
<th>Module</th>
<th>Description</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cvs</td>
<td>Allow cvs daemon to read shadow</td>
<td>allow_cvs_read_shadow</td>
</tr>
<tr>
<td>✔️</td>
<td>domain</td>
<td>Allow all domains to use other domains file descriptors</td>
<td>allow_domain_fd_use</td>
</tr>
<tr>
<td></td>
<td>exim</td>
<td>Allow exim to connect to databases (postgres, mysql)</td>
<td>exim_can_connect_db</td>
</tr>
<tr>
<td></td>
<td>exim</td>
<td>Allow exim to create, read, write, and delete unprivileged user files.</td>
<td>exim_manage_user_files</td>
</tr>
<tr>
<td></td>
<td>exim</td>
<td>Allow exim to read unprivileged user files.</td>
<td>exim_read_user_files</td>
</tr>
<tr>
<td>✔️</td>
<td>ftp</td>
<td>Allow ftp to read and write files in the user home directories</td>
<td>ftp_home_dir</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
<td>Allow ftp servers to login to local users and read/write all files on the system.</td>
<td>allow_ftpd_full_access</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
<td>Allow ftp servers to use nfs used for public file transfer services.</td>
<td>allow_ftpd_use_nfs</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
<td>Allow ftp servers to upload files, used for public file transfer services.</td>
<td>allow_ftpd_anon_write</td>
</tr>
<tr>
<td></td>
<td>ftp</td>
<td>Allow ftp servers to use cifs used for public file transfer services.</td>
<td>allow_ftpd_use_cifs</td>
</tr>
<tr>
<td></td>
<td>global</td>
<td>Allow unconfined executables to make their heap memory executable. Doing</td>
<td>allow_execheap</td>
</tr>
<tr>
<td>✔️</td>
<td>global</td>
<td>Support NFS home directories</td>
<td>use_nfs_home_dirs</td>
</tr>
<tr>
<td>✔️</td>
<td>global</td>
<td>Allow all unconfined executables to use libraries requiring text relocation that</td>
<td>allow_execmod</td>
</tr>
<tr>
<td></td>
<td>global</td>
<td>Enabling secure mode disallows programs, such as newrole, from transitioning to secure mode</td>
<td>secure_mode</td>
</tr>
<tr>
<td></td>
<td>global</td>
<td>Support SAMBA home directories</td>
<td>use_samba_home_dirs</td>
</tr>
</tbody>
</table>
Policy Development

- Command line tools for quick fixes
- SLIDE
- SEEdit
**Domain Access**

This will help you create a domain for your module.

<table>
<thead>
<tr>
<th>Module: <code>killerapp</code></th>
<th>Type: <code>Application</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>This will help you create a new domain in your module that acts like a user runnable application.</td>
<td></td>
</tr>
</tbody>
</table>

- **Domain of Running Process**
  - `killerapp_t`

- **Label Executable**
  - **Type**: `killerapp_exec_t`
  - **Path**: `/usr/local/bin/killerapp`

- **Application has config file**
  - **Type**: `killerapp_config_t`
  - **Path**: `/etc/killerapp.conf`

- **Application has PID file**

- **Application has temporary file**

- **Application has log file**

- **Application accesses network**

- **Helper processes**
Core Enhancements

- Performance and scalability improvements
- Integrated with kernel memory protection
- Netfilter-based network controls
- Labeled Networking
- Better MLS
Security Evaluation

- RHEL5 Common Criteria certifications
  - LSPP, RBACPP, CAPP at EAL4+
  - IBM, HP and SGI hardware
  - Community effort
  - Led to improved audit and other features

- Other Accreditation
  - US Coast Guard Intelligence case study
Threat Mitigation

“A security framework originally published by the US National Security Agency has begun to rack up an impressive list of protections against security holes.”
– *LinuxWorld, Feb 2008*

• SELinux has mitigated several serious security threats to everyday users of Fedora & RHEL.

• Tracked @ Tresys Mitigation News
SELinux Adoption

- Widely adopted in Fedora
  - Smolt statistics show majority have SELinux enabled.
- RHEL adoption by military, govt, finance:
  - Factor in NYSE/Euronext adoption, handling over $140 Billion/day in trades.
- Embedded / consumer electronics:
  - Reduce risks and costs of vulnerabilities
  - Simpler systems can have tighter policy
Kiosk Mode (xguest)

- Anonymous desktop sessions

- Innovative application of several security technologies

- Useful for conferences, training, trade shows, libraries, child-proofing...
Current Work

- Wider distribution support:
  - Ubuntu, Debian, Gentoo
- Beyond kernel:
  - Virtualization (XSM)
  - Desktop (XACE)
  - Storage (LNFS)
  - Applications (Database etc.)
- Beyond Linux:
  - OpenSolaris FMAC
Challenges

● Improved usability, as always!
● Documentation
● Keep community growing
How to Participate

- Install SELinux enabled distribution
- Join mailing lists
- IRC
- Ask questions, report bugs!