

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
- Settroubleshoot
 - Inspired by GNOME bug buddy

setroubleshoot

The screenshot shows the 'setroubleshoot browser' window. The title bar includes a star icon, the text 'setroubleshoot browser', and standard window controls. The menu bar contains 'File', 'Edit', 'View', and 'Help'. Below the menu is a table with columns: 'Quiet', 'Date', 'Host', 'Count', 'Category', and 'Summary'. A single row is visible with a checked 'Quiet' box, the date 'Thu 12 Jun 2008 08:42:29 PM EST', host 'e', count '2', category 'Network Ports', and summary 'SELinux is preventing the sshd (sshd_t) from...'. Below the table is a scrollable area with sections: '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 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_yppbind boolean, may fix the problem. setsebool -P allow_yppbind=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.), and '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). At the bottom left is an 'Audit Listener' icon and the text '7/7'.

Quiet	Date	Host	Count	Category	Summary
<input checked="" type="checkbox"/>	Thu 12 Jun 2008 08:42:29 PM EST	e	2	Network Ports	SELinux is preventing the sshd (sshd_t) from...

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](#) 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_yppbind boolean, may fix the problem. `setsebool -P allow_yppbind=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`

system-config-selinux

The screenshot shows the SELinux Administration window. The title bar reads "SELinux Administration". The menu bar includes "File" and "Help". On the left, a "Select:" sidebar lists various configuration options, with "Boolean" selected. The main area shows a "Revert" button and a "Customized" status. A "Filter" input field is present above a table of SELinux modules. The table has columns for "Active", "Module", "Description", and "Name". The "ftp" module is highlighted in blue, and its "ftp_home_dir" boolean is checked. Other modules like "domain", "global", and "exim" also have some booleans checked.

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

Policy Development

- Command line tools for quick fixes
- SLIDE
- SEEdit

SLIDE

New Policy Module

Domain Access

This will help you create a domain for your module

Module: killerapp Type: Application

This will help you create a new domain in your module that acts like a user runnable application.

Domain of Running Process: killerapp_t

- Label Executable
 - Type: killerapp_exec_t
 - Path: /usr/local/bin/killera
- 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

Help < Back Next > Finish Cancel

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!

