SELinux Basics

Clint Savage
Fedora Ambassador

Fedora Classroom
November 9, 2008

What is SELinux?

Another layer of security

- *Created by the NSA / Red Hat*
- *Helps add to the multiple layers of defense*
- *Generally used to protect local systems*
- *Affects, processes, ports, users ...*
- *Can't prevent everything*

Discretionary Access Control (DAC)

Standard ***rwx*** permissions for ***user:group***

- -rw------- 1 root root 1404 2008-11-07 09:45 anaconda-ks.cfg

Generally controlled by one user; ***root***

- Has discretion over the system
- Made decisions for the system
- Little control given to users
- Quite a good system to date

Mandatory Access Control (MAC)

Builds on top of DAC

- *Provides another layer of protection*

Policy - A set of rules determining level of protection

- *Defines which components are affected*
- *Processes are either unconfined or restricted*
  - *unconfined processes are allowed within the policy*
- *If an action is undefined, it's denied by default*
- *If allowed DAC still applies*

Security Contexts

A new way to think about access to the system

- *Each file/process has a context*
  - *user:role:type:sensitivity:category*
  - *Provides for multiple layers of protection*
  - *Most systems haven't implemented sensitivity or category*

```
# ls -Z anaconda-ks.cfg buildusb.sh
-rw-------  root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg
-rwxr--r--  root root unconfined_u:object_r:admin_home_t:s0 buildusb.sh

# ps -ef -Z | grep httpd
unconfined_u:system_r:httpd_t:s0 root     6740     1  2 09:30 ?        00:00:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   6742  6740  0 09:30 ?        00:00:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   6743  6740  0 09:30 ?        00:00:00 /usr/sbin/httpd
```

Default Policy: Targeted

Loaded during installation

- *Policy resides in the **/selinux** virtual filesystem*

Primarily uses ***type*** component for enforcement

- *user:role:**type**:sensitivity:category*
- Policy uses the **type** of both process and file

Local processes are generally *unconfined*

- *eg. cp, mv, cat, ls, etc.*

Manipulating Contexts

chcon

- *Useful for changing context of a file or directory*
  - *eg.* ***chcon -t http_t /srv/web/dir***

restorecon (generally safer)

- *Uses the policy's ruleset to determine the context*
- *Regular expressions match the directory or file*
  - *eg.* ***restorecon /export/kickstarts***

Manage / Modify the Policy

SELinux allows tweaks to the policy

- *Three states of the policy*
  - *Enforcing, Permissive, Disabled*
    - *Enforcing/Permissive*
      - *Can be changed without a reboot*
    - *Disabled removes SELinux labels*
      - *Reboot is required*

getenforce

- *Replies with the status of the policy*

setenforce 0 | 1

- *Changes the policy enforcement '**on the fly**'*
  - *Either **Enforcing** or **Permissive***

Making the Policy Persist

system-config-selinux

- *Very nice GUI to tweak the policy, booleans, etc.*

/etc/sysconfig/selinux

- *Defines the policy and status of SELinux on boot*
- *Written to by system-config-selinux*

semanage

- *Lists/Modifies the policy more permanently*

getsebool/setsebool

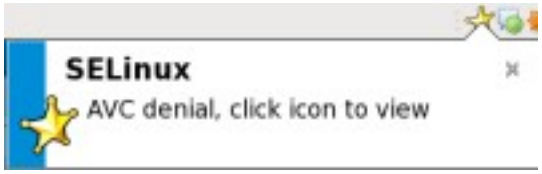
- *Allows modification of predefined sections of the policy*

Troubleshooting

Most people turn SELinux off because they can't understand avc messages

A Tool exists in Fedora to help troubleshoot and give better information about the situation

- ***/usr/sbin/setroubleshootd*** *and* ***/etc/init.d/setroubleshoot***
  - *Provided by the setroubleshoot-server rpm*
  - *Alerts in the notification area*
  - *Logs to the* ***kern*** *facility*
  - *Provides human readable messages*



fedora

Troubleshooting cont'd

setroubleshoot provides useful messages

tail /var/log/messages
Nov 8 10:52:46 machineA setroubleshoot: SELinux is preventing access to files with the label, file_t. For complete SELinux messages. run sealert -l e90521c2-dcd4-43a8-a4ce-3a64a07ee16b

sealert provides how to allow access

sealert -l e90521c2-dcd4-43a8-a4ce-3a64a07ee16b

Summary:
SELinux is preventing the X from using potentially mislabeled files (./fonts.dir).

Detailed Description:
.. snip ..

Allowing Access:
If you want X to access this files, you need to relabel them using restorecon -v './fonts.dir'. You might want to relabel the entire directory using restorecon -R -v '.'.

Resources & Licensing

OpenOffice Impress version of these slides
http://herlo.fedorapeople.org/files/selinux-basics-fc.odp

PDF version of these slides
http://herlo.fedorapeople.org/files/selinux-basics-fc.pdf

NSA's SELinux website
http://www.nsa.gov/selinux/

SELinux in Fedora
http://fedoraproject.org/wiki/SELinux

SELinux in Red Hat Enterprise Linux version 5
http://www.redhatmagazine.com/2007/05/04/whats-new-in-selinux-for-red-hat-enterprise-linux-5/

SELinux Policy Management
http://www.redhat.com/magazine/006apr05/features/selinux/
http://selinux-symposium.org/2005/presentations/session4/4-1-walsh.pdf

fedora