SELinux Symposium and developer summit

An annual exchange of ideas, technology and research involving SELinux.

Managing Red Hat Enterprise Linux 4

Daniel J Walsh

SELinux Lead Engineer

dwalsh@redhat.com

Agenda

1) Introduction to SELinux and the “targeted” policy
2) Modified commands and SELinux utilities
3) Understanding SELinux AVC messages
4) Customizing the policy with booleans
5) Managing file labeling
6) Configuring Auditing
7) Changes in Fedora Core 4/5 and Red Hat Enterprise Linux 5
8) Understanding and Customizing the Apache HTTP SELinux Policy

SELinux Symposium
and developer summit
An annual exchange of ideas, technology and research involving SELinux.

Unit 1

Introduction to SELinux and the “targeted” policy

What is SELinux?

Mandatory Method (MAC)

- Current systems use DAC (Discretionary Access Control)
- User/Programs has limited privilege
- Security policy set by administrator and enforced by the System
- Incorporates program function/trustworthiness into A/C decisions
- Root compromises confined by policy

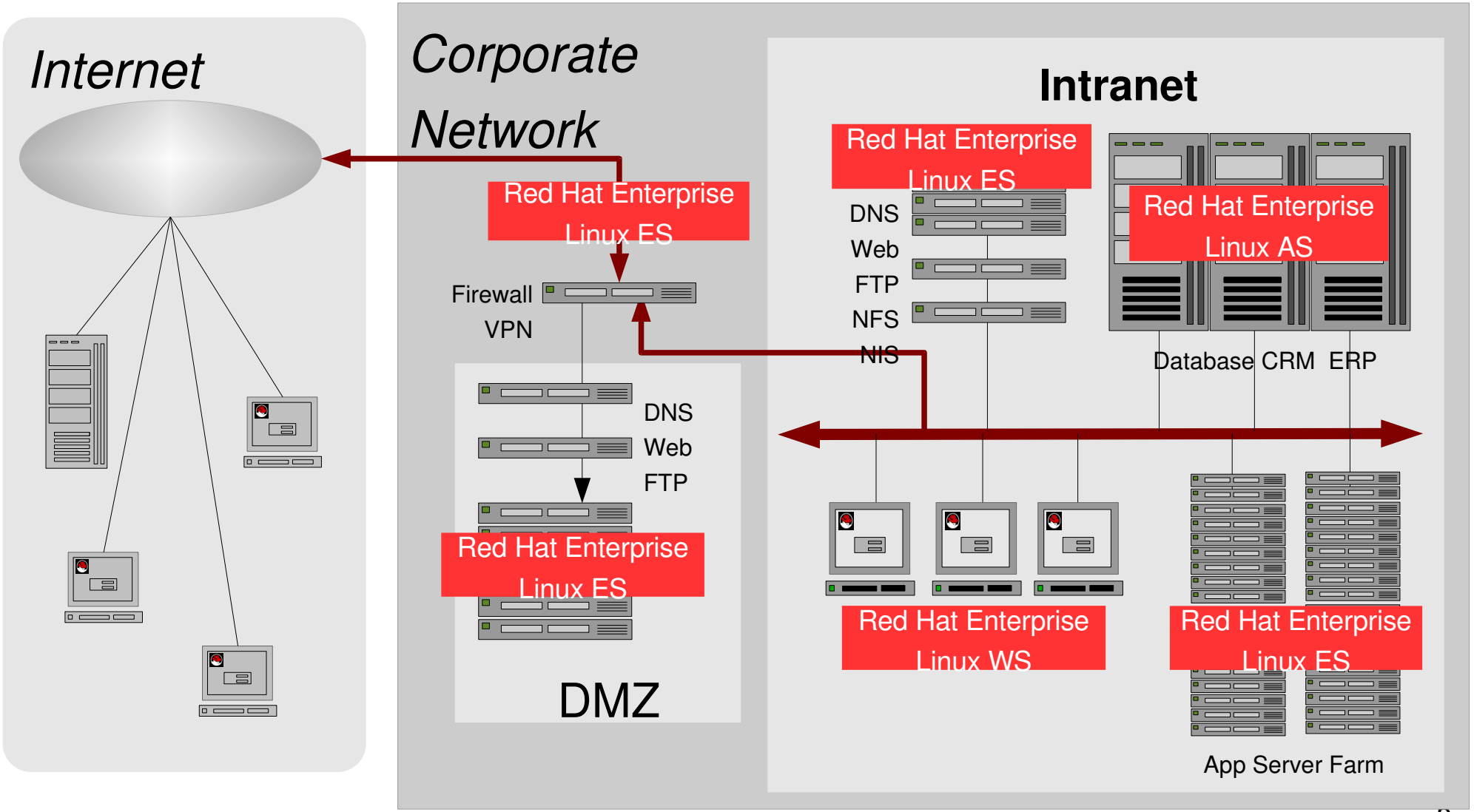
Developed by the NSA

Building many years of NSA's OS security research

Application of NSA's Flask security architecture

- Cleanly separates policy from enforcement using well-defined policy interfaces
- Fine-grained controls over kernel services
- Transparent to applications and users
- Removes power of root, several machines running root as guest account

Where should you run SELinux?



Security Context

- Basic labels used in SELinux
  - system_u:object_r:httpd_exec_t
  - system_u:system_r:httpd_t
- All subjects/objects have an associated security context
- Called a domain when used on a process
- Called a file_context when associated with a file
  - File Context are stored as extended attributes with the inode on the file system
  - On some file systems the kernel that do not support extended attributes the kernel provides the file context.

Security Context

- Made up of 3 or 4 components separated by ":"
  - 4th field is the MLS field which is not supported in RHEL4
  - Type object - "httpd_exec_t
    - Most used section of security context
    - Type enforcement rules revolve around this field
  - Role – Role of the object
    - File objects all labeled "object_r"
    - Process Objects include Role
  - User section "system_u"
    - Denotes SELinux User who created the object

How does SELinux enforce policy?

- Every process and file tagged with a security context
  - Files tagged via extended attributes
- New files context assigned via policy
  - By default new files get assigned container directories security context
  - Policy can override. It might state files created in /var/log by named get named_log_t
- Kernel assigns context to processes via policy
- Certain Applications, such as login, are allowed by policy to set the context of the next executed program

SELinux Key Components

Kernel

- Patch implementing security hooks
- Uses Linux Security Module (LSM)
- Framework for security enhancements to Linux

SELinux Key Components

Applications

- Most user applications and server applications unchanged
- SELinux aware applications
  - Applications used to view or manipulate security contexts
  - Programs required to set user session security context
  - Examples: login/sshd, ls, cp, ps, setfilecon, logrotate, cron ...
  - Covered in Section 2

SELinux Key Components

Policy

Strict – (Not supported in RHEL 4)

- A system where everything is denied by default
  - You must specify allow rules to grant privileges
- SELinux designed to be a strict policy.
  - The policy rules only have allows, no denies
  - Minimal privilege's for every daemon
  - separate user domains for programs like GPG,X, ssh, etc
- Difficult to enforce in general purpose operating system

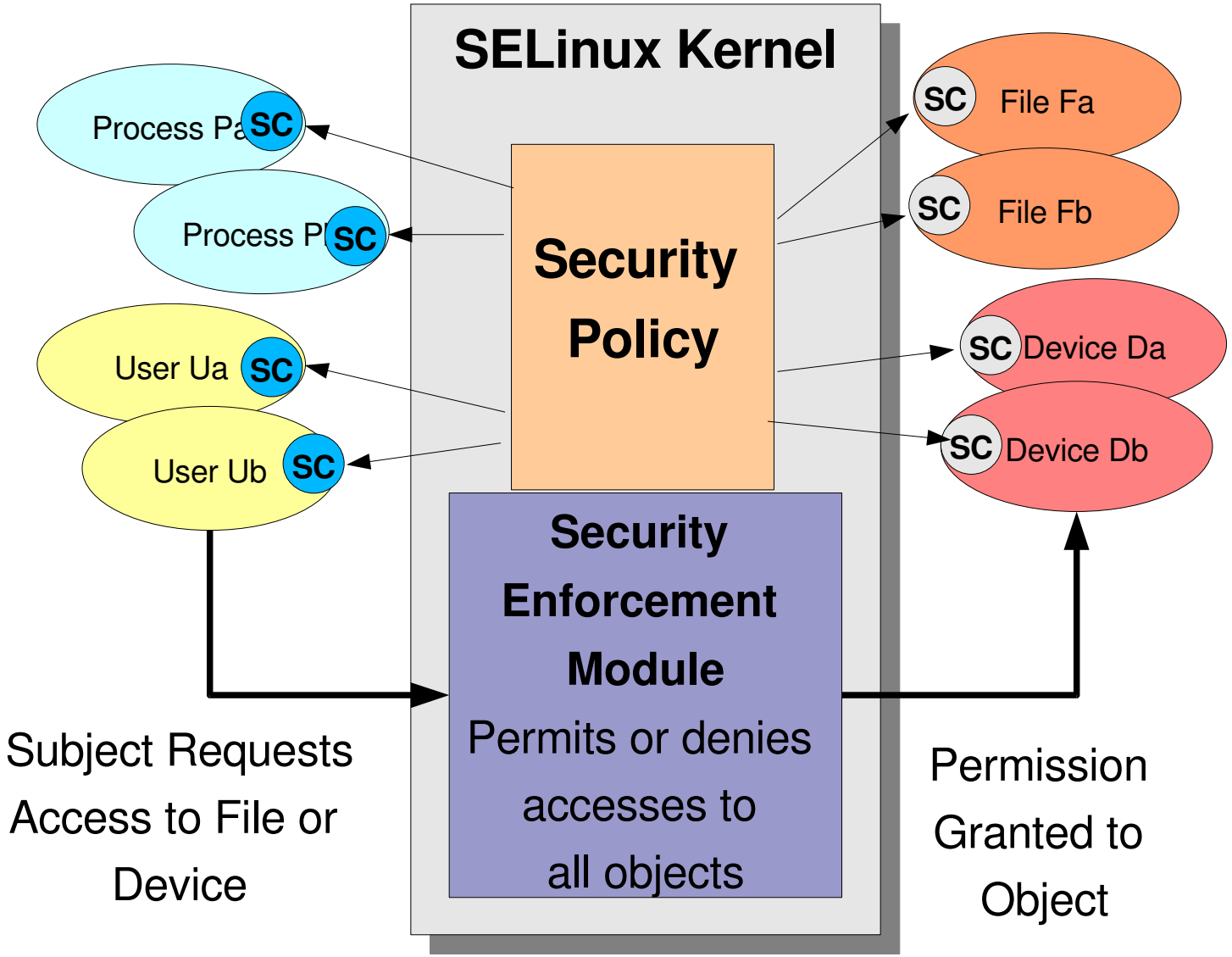
SELinux Key Components

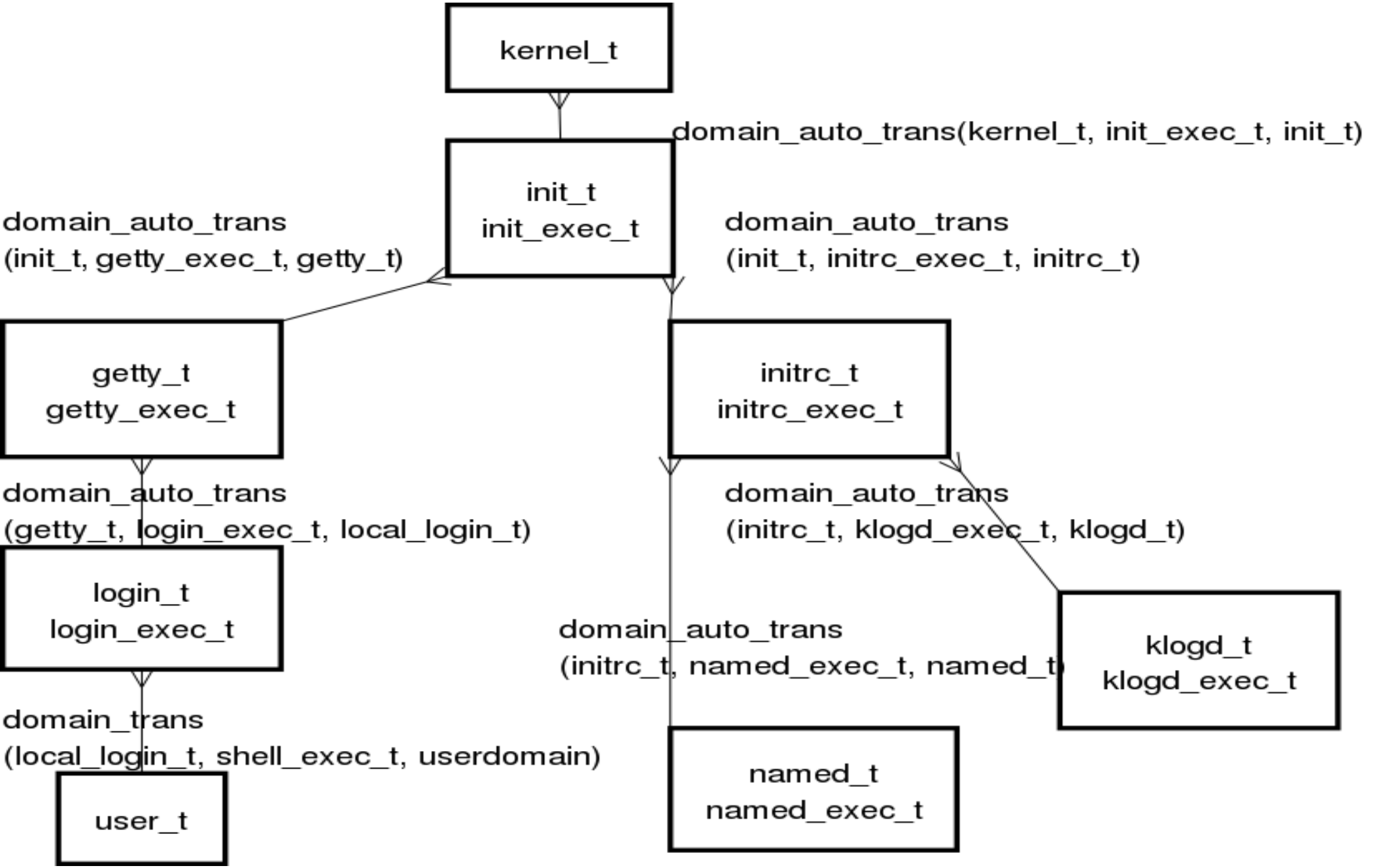
Policy

Targeted

- System where everything is allowed. Use deny rules
- By default processes run in unconfined_t
  - unconfined processes have the same access they would have without SELinux running
- Daemons with defined policy transition to locked down domains
- httpd started from unconfined_t transitions to httpd_t which has limited access.

How SELinux Enforces Security Policy




kernel_t
domain_auto_trans(kernel_t, init_exec_t, init_t)
init_t
init_exec_t
domain_auto_trans
(init_t, getty_exec_t, getty_t)
domain_auto_trans
(init_t, initrc_exec_t, initrc_t)
getty_t
getty_exec_t
initrc_t
initrc_exec_t
domain_auto_trans
(getty_t, login_exec_t, local_login_t)
domain_auto_trans
(initrc_t, klogd_exec_t, klogd_t)
login_t
login_exec_t
domain_auto_trans
(initrc_t, named_exec_t, named_t)
klogd_t
klogd_exec_t
domain_trans
(local_login_t, shell_exec_t, userdomain)
named_t
named_exec_t
user_t

Targeted Domains

- Apache Hypertext Transfer Protocol Server - httpd
- Proxy caching server – Squid
- Open-source implementation of the DMTF CIM and WBEM standards - pegasus
- The GNU Mailing List Manager - Mailman
- Domain Name Server - Named
- Dynamic Host Configuration Protocol Daemon - dhcpd
- The MySQL Server - mysqld
- Name service cache daemon - nscd

Targeted Domains

- Network Time Protocol (NTP) daemon - ntpd
- DARPA port to RPC program number mapper - portmap
- Open Source Database - postgresql
- SNMP Daemon - snmpd
- Linux system logging utilities - syslogd
- Name Service Switch daemon for resolving names from NT Servers – winbindd

Config files

- SELinux stores its config files in /etc/selinux

```
ls -l /etc/selinux
-rw-r--r-- 1 root root  515 Jan 18 11:46 config
drwxr-xr-x 7 root root 4096 Jan 23 14:06 strict
drwxr-xr-x 7 root root 4096 Jan 23 14:06 targeted
```

- /etc/selinux/config identifies policy and enforcing mode

```
more /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted
```

Config files

- /etc/selinux/targeted/contexts/files/
  - file_contexts
  - file_contexts.local
  - file_contexts.homedir
  - homedir_template

Target Policy Man Pages

- Policy targets man pages explain custom features of the policy such as booleans and file context

```
httpd_selinux(8)      httpd SELinux Policy documentation      httpd_selinux(8)

NAME
      httpd_selinux - Security Enhanced Linux Policy for the httpd daemon

DESCRIPTION
      Security-Enhanced Linux secures the httpd server via flexible mandatory
      access control.

FILE_CONTEXTS
      SELinux requires files to have an extended attribute to define the file
      type.   Policy governs the access daemons have to these files.  SELinux
      httpd policy is very flexible allowing users to setup  their  web  ser-
      vices in as secure a method as possible.

      The following file contexts types are defined for httpd:

           httpd_sys_content_t
           - Set files with httpd_sys_content_t for content which is avail-
           able from all httpd scripts and the daemon.

           httpd_sys_script_exec_t
           - Set cgi scripts with httpd_sys_script_exec_t to allow them  to
```

Exercises

- Read through a couple of SELinux Policy man pages
- Which policy is the system currently running?
- Reboot in permissive mode
  - Do you see additional AVC messages?

SELinux Symposium
and developer summit
An annual exchange of ideas, technology and research involving SELinux.

Unit 2

Modified commands and SELinux utilities

Modified Utilities

- "Z" is your friend
- Core Utilities
  - ls -Z
  - cp/mv/install
    - Each handles file_context differently !!!!
  - find / -context=
  - id -Z
  - ps auxZ

Modified Utilities

- Login Programs - PAM
  - ssh, su, login, xdm, sudo
- Password utilities
  - passwd, useradd, groupadd
- rpm

Backup and disc management

- tar, zip
  - You must restorecon after you tar files back in place
  - zip (Extended attribute support is being worked)
- rsync
  - -X, -xattrs
- star
  - star -xattr -H=exustar -c -f output.tar [files]
- amanda

SELinux Utilities

- Policycoreutils
  - newrole
  - run_init
  - audit2allow (See 3.0 Understanding SELinux log messages)
  - audit2why (See 3.0 Understanding SELinux log messages)
  - sestatus
- libselinux
  - getenforce/setenforce
  - selinuxenable

SELinux Utilities

- Managing Booleans
  - setsebool, getsebool, system-config-securitylevel
  - See 4.0 Customizing the policy with booleans
- Managing file context
  - setfiles, restorecon, fixfiles, genhomedircon, chcon
  - See 5.0 Managing file labeling

Exercises: Modified Linux Utilities

- What security context is on /etc/resolv.conf?
- Explore other security context in /etc
- What is the context is the apache process running with?
- What is your security context?
- Create a file in /tmp and mv it to etc
  - What is the security context on the file?
  - Is this a problem?
- Create a new account on your machine
  - What is the security context on /etc/passwd? /etc/shadow?
  - Why do you suppose they are different?

Exersizes: SELinux Utilities

- Is your machine in enforcing mode?
  - Turn on permissive mode
  - What AVC message was generated?
  - Return machine to enforcing mode.
- What is the SELinux status of your machine?
- Use sestatus to check the file context on /etc/shadow
- Create the file /etc/apache
  - Change its context type to httpd_exec_t
  - How would you get this application to run as httpd_t?
- Correct the context of all the files in etc

SELinux Symposium
and developer summit
An annual exchange of ideas, technology and research involving SELinux.

Unit 3
Understanding SELinux AVC Messages

Understanding SELinux log messages

- AVC Access Vector Cache
  - messages in /var/log/messages or /var/log/audit.log

```
type=AVC msg=audit(1140184056.443:78): avc:  denied  { use } for  pid=2185
comm="mingetty" name="ptmx" dev=tmpfs ino=699 scontext=system_u:system_r:getty_t:s0
tcontext=system_u:system_r:kernel_t:s0 tclass=fd

type=AVC msg=audit(1140184056.531:79): avc:  denied  { read write } for  pid=2197
comm="consoletype" name="ptmx" dev=tmpfs ino=699
scontext=system_u:system_r:consoletype_t:s0 tcontext=system_u:object_r:ptmx_t:s0
tclass=chr_file

type=AVC msg=audit(1140184062.111:82): avc:  granted  { execmem } for  pid=2241
comm="Xorg" scontext=system_u:system_r:xdm_t:s0-s0:c0.c255
tcontext=system_u:system_r:xdm_t:s0-s0:c0.c255 tclass=process
```

Understanding SELinux log messages

- audit2allow
  - Tool that generates policy allow rules from logs of denied operations
  - audit2allow -i /var/log/messages
    - allow system_crond_t null_device_t:chr_file { read write };
- audit2why
  - Translates SELinux audit messages into a description of why the access was denied

Analyzing SELinux AVC Messages

- AVC Messages refering to files labeled *:file_t
  - Major Labeling problem, all files probably require labels
  - SELinux kernel labels files with no security context file_t
  - File was created when running with selinux=0 or a new disk.
  - It is safest to relabel the system - touch /.autorelabel; reboot
  - On a new disk you can restorecon -R -v /MOUNTPOINT
- AVC Messages containing default_t
  - Probably a labeling problem
    - If not in / you probably need to relabel
    - If in / and you want confined domains to have access. You need to relabel the file/directory using chcon

Analyzing SELinux AVC Messages

- Many similar messages about the same file
  - This usually indicates a labeling problem
  - For example:
    - Create /home/dwalsh/resolv.conf
    - mv /home/dwalsh/resolv.conf /etc
    - ls -lZ /etc/resolv.conf
    - Confined domains will report errors accessing user_home_t
    - restorecon /etc/resolv.conf

Analyzing SELinux AVC Messages

- AVC Messages indicate that a sharing domain failed to access certain files:
  - Confined sharing domains are httpd, smbd, ftpd, and rsync
  - Files in home directories indicates a boolean problem
    - setsebool -P httpd_enable_homedirs=1
  - Elsewhere you probably need chcon
    - Sharing domains have specific context for reading and writing.
      - Samba needs access to /src; chcon -R -t samba_share_t /src/
    - If multiple domains need access to the same files
      - Use public_context_t or public_context_rw_t
      - setsebool -P allow_DOMAIN_anon_write=1
  - Please refer to the DOMAIN_selinux man page

Missing AVC messages

Sometimes applications fail with no AVC messages

- Setting setenforce 0 and the application works???
- dontaudit rules
  - Expected AVC messages that cause applications to take different code paths.
  - Sometimes cover up Real errors
- Install selinux-policy-targeted-sources
- make -C /etc/selinux/targeted/src/policy enableaudit load

Exercises: SELinux Utilities

- Lets create some avc messages?
  - Turn off enforcing mode
  - Use the runcon command to create a shell running as httpd_t
  - Check the shell to make sure its context is httpd_t
  - Turn on enforcing mode
  - What happens?
  - Check the log files for AVC messages.
- What audit rules could you add to solve these AVC?
- Why did policy refuse this access?

SELinux Symposium
and developer summit
An annual exchange of ideas, technology and research involving SELinux.

Unit 4

Customizing the policy with booleans

SELinux Key Components

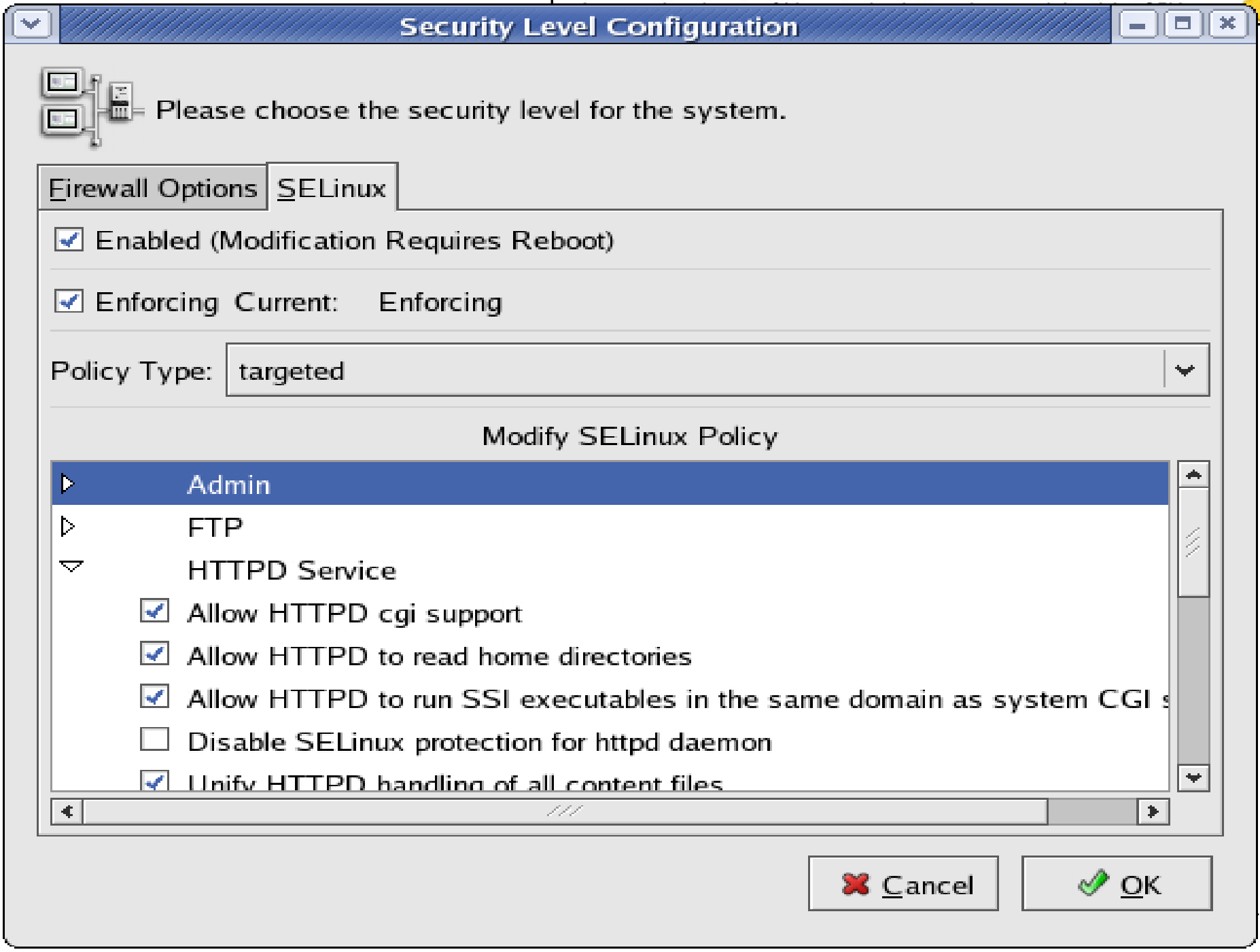
Apache Example

- Apache executable unmodified
- System administrator might have three choices of policy
  - High - Apache only can display html pages in /var/www/html
  - Medium – Apache can run cgi-scripts in /var/www/cgi-bin
  - Low – Apache can display pages in users home directories
- Cracker only has access to files that Apache had access too
  - If Apache had read access to /var/www/html that is all cracker can do.
  - Cracker can cause other pages to display.

Customizing policy with booleans

Booleans are if/then/else statements in policy

- Configure policy without editing policy
- getsebool
  - getsebool -a
- setsebool
  - setsebool -P allow=[1|0]
- system-config-securitylevel
- Turn on/off sections of policy
  - setsebool -P allow_nfs_home_dirs 1
  - /etc/selinux/targeted/booleans


Security Level Configuration
Please choose the security level for the system.
Firewall Options
SELinux
Enabled (Modification Requires Reboot)
Enforcing Current: Enforcing
Policy Type:
targeted
Modify SELinux Policy
Admin
FTP
HTTPD Service
Allow HTTPD cgi support
Allow HTTPD to read home directories
Allow HTTPD to run SSI executables in the same domain as system CGI
Disable SELinux protection for httpd daemon
Cancel
OK

Configuring Policy

Apache Example

- System administrator has multiple choices of policy
  - Booleans
    - httpd_disable_trans, httpd_enable_cgi httpd_enable_homedirs httpd_tty_comm, httpd_unified
- http://fedora.redhat.com/docs/selinux-apache-fc3/
- man httpd_selinux

Exersizes: Managing Booleans

- List all booleans on your machine
- Check the contents of /etc/selinux/targeted/booleans
- Temporarily change a booleans state
- Did the /etc/selinux/targeted/booleans file change?
- If you have time try the previous exercises after you turn on the httpd_tty_comm boolean

5.0 Managing File Labeling

Managing file labeling

- Changing a files context
- chcon
  - Fundamental utility used to change a files context
    - chcon -R -t httpd_sys_script_rw_t /var/www/myapp/data
    - chcon -t httpd_sys_script_t /var/www/cgi-bin/myapp
  - Modeled after chmod command
  - -t type qualifier
  - customizable_types
    - /etc/selinux/targeted/contexts/customizable_types

Managing file labeling

- restorecon
  - Used to set a file back to the system defaults
- setfiles
  - Used to initialize a system. Used at the File system level
  - Requires you to specify file_context file
- fixfiles
  - Script that wraps setfiles/restorecon with several useful features
  - Use rpm to list files within specified packages to restore file contexts
  - restorecon changes between previous file context and new one
- touch /.autorelabel; reboot

Managing file labeling

- Genhomedircon
  - Used to generate file_contexts.homedir
  - Sometimes has problems with homedir locations.
- /etc/selinux/targeted/contexts/files/file_context.local
- system-config-securitylevel

Exercises: Managing file labeling

- Modify /etc/resolv.conf
  - cp /etc/resolv.conf to /tmp
  - Make some changes to the search string
  - mv it back the /etc
  - Fix its security context
- Homedirs
  - Create an a new directory /export/homes
  - Add a user account to that directory
  - Add a user account to the /var directory
  - Run genhomedircon – What happens?
  - Fix the context on these directories

Unit 6

Configuring Auditing

Auditing

- Audit system receives SELinux Events
  - No auditd running
    - AVC in /var/log/messages and dmesg
  - auditd running
    - AVCs in/var/log/audit/audit.log
- audit=1 Command required for full auditing

Auditing CAPP/EAL4+

- CAPP – Controlled Access Protection Profile
  - DAC Profile
  - Security features selection
- eal4+. - E Assurance Level
  - Level of testing and documentation
- cp /usr/share/doc/audit-1.0.12/capp.rules /etc/audit.rules

auditctl

- Utility to control the kernel's audit system
  - -e [0|1] Disable, Enable audit
  - SEE Steve Grubb Audit BOF...

aureport

- Generate summary reports of audit logs
  - -a Report about AVC messages
  - -i interpret numeric fields for human consumption
  - -ts “Time Start” -te “Time End”
    - aureport -a -ts 1:00:00
      - Generate a avc report since 1 AM
  - --success/--failed (Both if you select neither.)
  - --summary (Totals of events)

ausearch

- Search Audit Daemon Logs
  - -m avc
  - -ts
  - -x executable
  - ausearch -m avc -ts 1:00:00 -x named

Exercises: Audit

- Use aureport on audit messages on the system
- Total
- Search for apache avc messages
- Turn off auditing? Where to the AVC message end up?

SELinux Symposium
and developer summit
An annual exchange of ideas, technology and research involving SELinux.

Unit 7
Changes in Fedora Core 4/5 and Red Hat Enterprise Linux 5

SELinux in Fedora Core 4

- **Fedora Core 4**
- **Expand SELinux targeted policy to cover all system services.**
  - Now more than 80 targets
  - All of system space is locked down
- **We keep plugging away at full strict policy**
  - Through the increase of targeted, most policy files are shared
  - Locking down Web Browsers/Mail Clients
  - Lock down Ethereal
- Improved access checks execmem/execmod

SELinux in Fedora Core 4

- Improved protection of network protocols.
  - Finer grained control over network protocols
  - named_connect to prevent spammer attacks on daemons

SELinux in Fedora Core 5

- **Full Multi-Level Security server support**
  - Introduced secadm_r policy to break down sysadm_r
    - Only role allowed to manipulate policy vs administer domains
  - RBAC Support
  - Enable to support for Roles based access control in strict policy
  - Useradd/Usermod...
- Multi Category System
  - Begin investigating use of labeled documents. Users specify document as “Company Confidential” causing print daemons to attach header and footer to document
  - Easier change from Targeted policy to MLS Policy
- Begin process of getting LSPP certification
- Add IBM/TCS technology into mainline OS
  - Polyinstatiated File Systems
  - Labeled Networking with IPSEC
- Trusted Printing

SELinux in Fedora Core 5

- Allow customization of ports and network devices
- Better handling of user customization of apache_domain
- Enable policy creation for third-party applications
  - Tresys loadable modules. Customization by users/third parties without policy sources

SELinux in Red Hat Enterprise Linux 5

- Expand SELinux targeted policy to cover more system services
- Keep plugging away at full strict policy
- Xen Support
- ISV enablement for trusted specific ISVs
- Add better policy administration tools for creating policies

SELinux in Red Hat Enterprise Linux 5

- Enable policy creation for third-party applications
- Distribution and update of custom policies integrated into systems management or configuration management framework
- More work on system auditing system support and tools.

Unit 8

Customizing Apache

Customizing Apache Policy

- httpd - most complex daemon in RHEL 4
- Most complex and configurable of any of the SELinux policies.
  - Confine compromised Apache web server from damaging the rest of the system
  - Finer grained goals
    - Preventing a compromised wiki CGI script from corrupting a blog installation owned by the same person

Exercises: Apache

- Is httpd running under a confined domain?
  - Stop httpd
  - Start apache directly /usr/sbin/httpd
  - Which context is it running under?
  - Why?
- Kill httpd and start it within a confined domain
- Setup an apache web site which supports cgi-scripts where the data is located in /src/www/data directory
- Setup apache to use users home directories and place a html file there
- Advanced: Add a cgi script that needs to write to a particular directory, turn off httpd_unified and make the script work in enforcing mode.

Q/A

- **More Information Red Hat Enterprise Linux Resource**
  - http://www.redhat.com/software/rhel/
- **SELinux Resources**
  - http://www.nsa.gov/selinux
  - http://fedora.redhat.com/projects/selinux/
  - http://fedoraproject.org/wiki/SELinux
- **Mailing Lists**
  - selinux@tycho.nsa.gov - NSA List
  - fedora-selinux-list@redhat.com - Fedora SELinux List