The State of Security Enhanced Linux

James Morris
jmorris@namei.org

FOSS.IN/2007 – Bengaluru, India

Outline

- Brief SELinux overview
- Project update
- Challenges
- Ongoing and Future work

What is SELinux?

Security Framework

- Pluggable security models
- Clean separation of policy
- Coherent stacking (composition)
- Fully analyzable

What is SELinux?

Security Mechanism

- Type Enforcement + RBAC + MLS
- Mandatory Access Control (MAC)
- Least privilege
- Enforces confidentiality and integrity
- Limits exploitation of vulnerabilities

What is SELinux?

Community Project

- Originated in security research community c. 1980s
- Prototyped as academic research 1990s (Flask)
- Ported to Linux and released as GPL in 2000
- Adopted by distributions, merged upstream and certified

Current Status

- Primarily adopted in Fedora and RHEL
- Supported by Debian, Ubuntu, Gentoo, others
- Market adoption: military, government embedded, finance.
- Unprecedented: MAC security available freely in an off the shelf OS. With source code!

Project Update

Since last here (2005, Fedora Core 4 era)

Reference Policy

- Interfaces & encapsulation
- Designed
- Policy management infrastructure & tools
- Flexibility
- Documentation
- Full MLS support

Project Update

Loadable Policy Modules

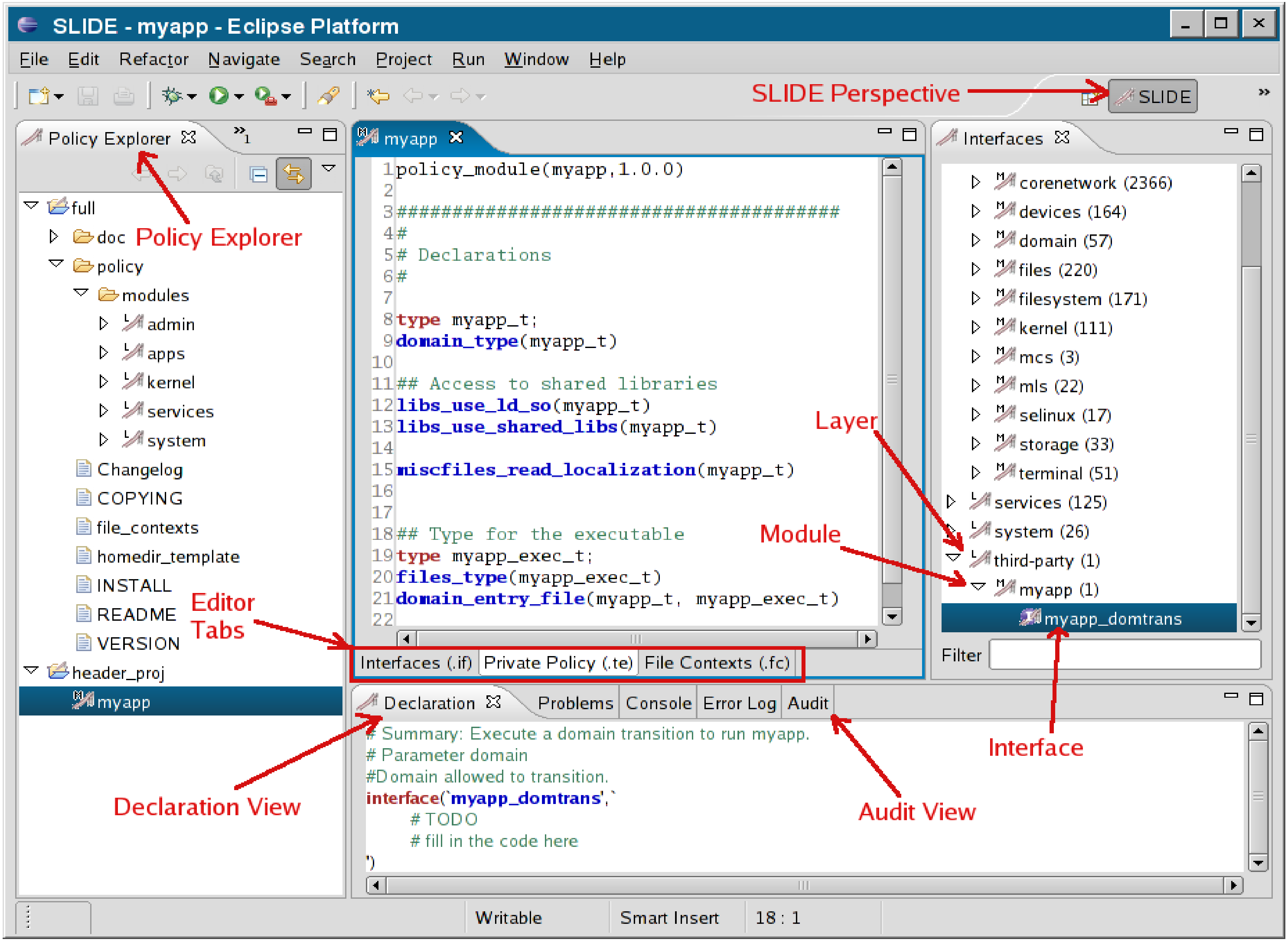
- Dynamic loading and unload of policy
- Easier customization
- Third party policy
- Manage & ship policy with applications

Project Update

Policy Tools

SELinux Policy IDE (SLIDE)

- GUI policy development
- Eclipse-based
- Remote policy deployment & monitoring



```
policy_module(myapp,1.0.0)

########################################
#
# Declarations
#

type myapp_t;
domain_type(myapp_t)

## Access to shared libraries
libs_use_ld_so(myapp_t)
libs_use_shared_libs(myapp_t)

miscfiles_read_localization(myapp_t)


## Type for the executable
type myapp_exec_t;
files_type(myapp_exec_t)
domain_entry_file(myapp_t, myapp_exec_t)

```

```
# Summary: Execute a domain transition to run myapp.
# Parameter domain
#Domain allowed to transition.
interface(`myapp_domtrans',`
      # TODO
      # fill in the code here
')
```

Project Update

Toolkit

libsemanage

- Standard library for managing policy
- Used by higher level tools, from command line to GUI
- Extensible, e.g. Remote policy management

Project Update

Toolkit

semanage

- Simplifies several tasks which previously required editing different config files and recompiling policy.
- Examples: mapping users to roles, labeling network ports.

Project Update

Toolkit

restorecond

- Automatic relabeling of files which tend to get mislabeled, via inotify
- Reduces administrative overhead

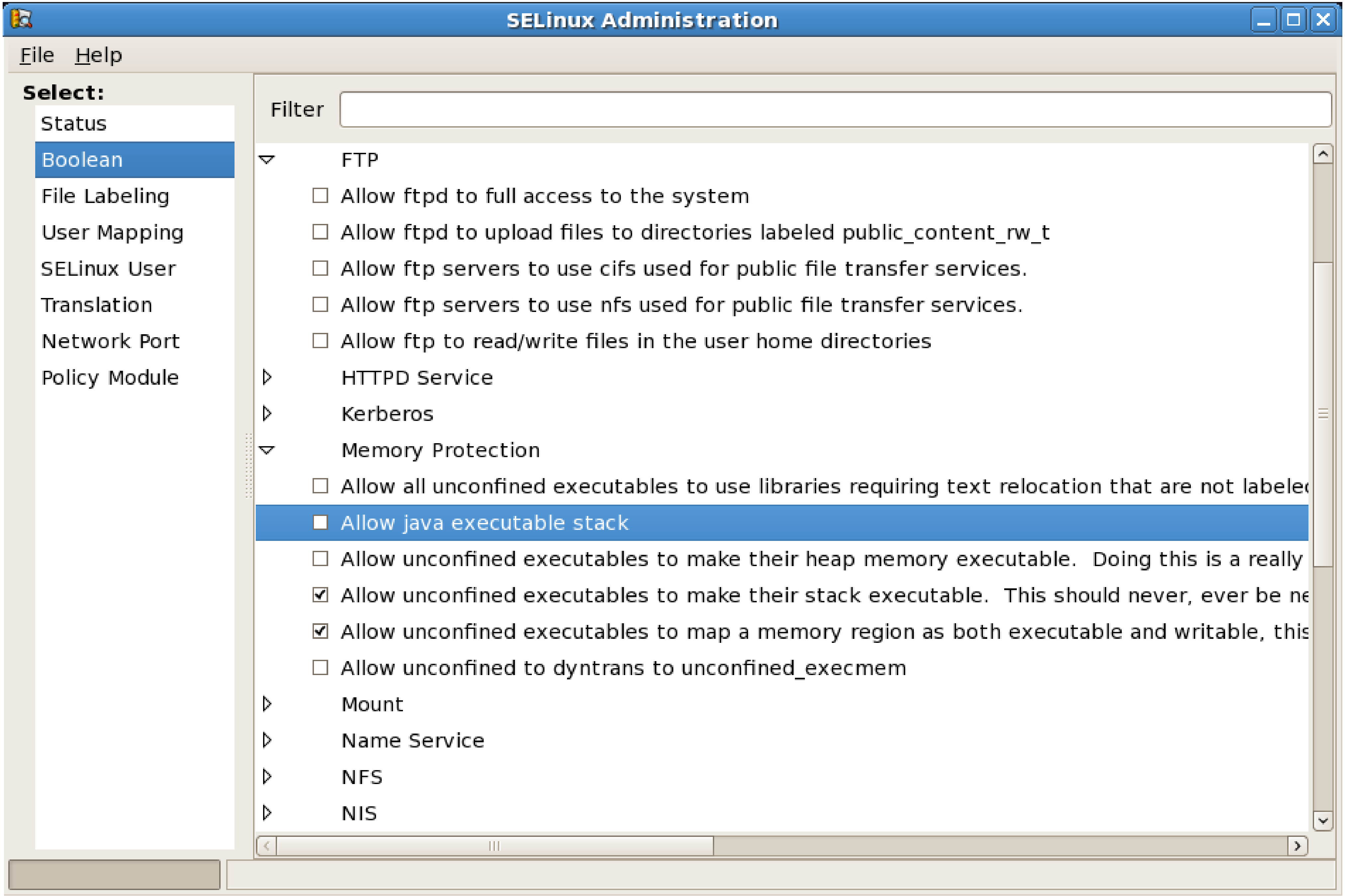
Project Update

Toolkit

policycoreuitls-gui

- Python toolkit for GUI configuration of SELinux
- Integrated into *system-config-selinux*

system-config-selinux



FTP

☐ Allow ftpd to full access to the system

☐ Allow ftpd to upload files to directories labeled public_content_rw_t

☐ Allow ftp servers to use cifs used for public file transfer services.

☐ Allow ftp servers to use nfs used for public file transfer services.

☐ Allow ftp to read/write files in the user home directories

HTTPD Service

Kerberos

Memory Protection

☐ Allow all unconfined executables to use libraries requiring text relocation that are not labele

☐ Allow java executable stack

☐ Allow unconfined executables to make their heap memory executable. Doing this is a really

☑ Allow unconfined executables to make their stack executable. This should never, ever be ne

☑ Allow unconfined executables to map a memory region as both executable and writable, this

☐ Allow unconfined to dyntrans to unconfined_execmem

Mount

Name Service

NFS

NIS

Project Update

Toolkit

audit2why

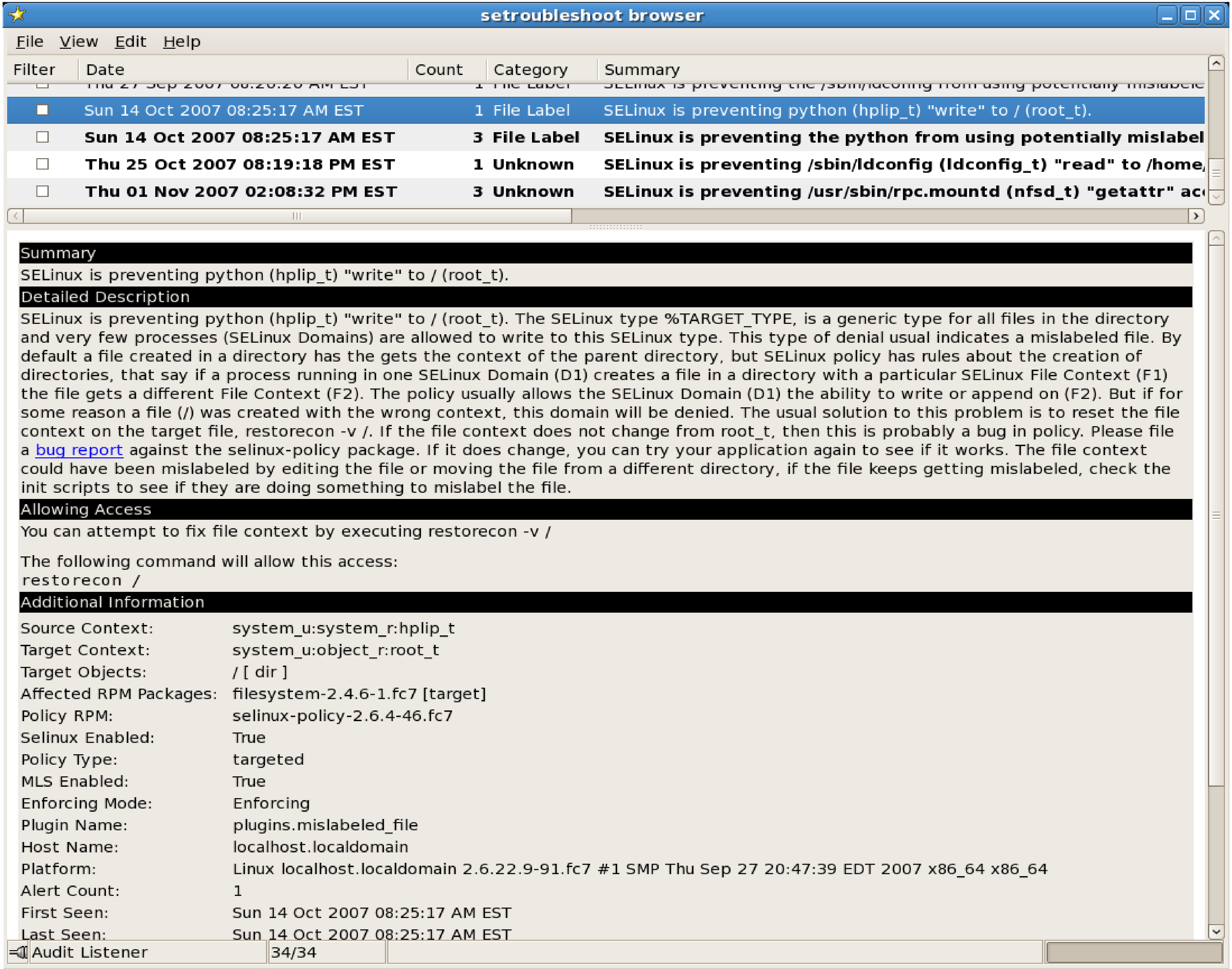
- Tries to explain entries in the audit log
- Offers helpful suggestions

Project Update

Toolkit

setroubleshoot

- Diagnostic alerts
- Gnome applet
- GUI browser
- Extensible plugin architecture
- Email alerts



Filter	Date	Count	Category	Summary
□	Thu 27 Sep 2007 08:20:20 AM EST	1	File Label	SELinux is preventing the /sbin/ldconfig from using potentially mislabele
□	Sun 14 Oct 2007 08:25:17 AM EST	1	File Label	SELinux is preventing python (hplip_t) "write" to / (root_t).
□	**Sun 14 Oct 2007 08:25:17 AM EST**	**3**	**File Label**	**SELinux is preventing the python from using potentially mislabel**
□	**Thu 25 Oct 2007 08:19:18 PM EST**	**1**	**Unknown**	**SELinux is preventing /sbin/ldconfig (ldconfig_t) "read" to /home,**
□	**Thu 01 Nov 2007 02:08:32 PM EST**	**3**	**Unknown**	**SELinux is preventing /usr/sbin/rpc.mountd (nfsd_t) "getattr" ac**

Summary

SELinux is preventing python (hplip_t) "write" to / (root_t).

Detailed Description

SELinux is preventing python (hplip_t) "write" to / (root_t). The SELinux type %TARGET_TYPE, is a generic type for all files in the directory and very few processes (SELinux Domains) are allowed to write to this SELinux type. This type of denial usual indicates a mislabeled file. By default a file created in a directory has the gets the context of the parent directory, but SELinux policy has rules about the creation of directories, that say if a process running in one SELinux Domain (D1) creates a file in a directory with a particular SELinux File Context (F1) the file gets a different File Context (F2). The policy usually allows the SELinux Domain (D1) the ability to write or append on (F2). But if for some reason a file (/) was created with the wrong context, this domain will be denied. The usual solution to this problem is to reset the file context on the target file, restorecon -v /. If the file context does not change from root_t, then this is probably a bug in policy. Please file a bug report against the selinux-policy package. If it does change, you can try your application again to see if it works. The file context could have been mislabeled by editing the file or moving the file from a different directory, if the file keeps getting mislabeled, check the init scripts to see if they are doing something to mislabel the file.

Allowing Access

You can attempt to fix file context by executing restorecon -v /

The following command will allow this access:

```
restorecon /
```

Additional Information

Source Context:	system_u:system_r:hplip_t
Target Context:	system_u:object_r:root_t
Target Objects:	/ [dir]
Affected RPM Packages:	filesystem-2.4.6-1.fc7 [target]
Policy RPM:	selinux-policy-2.6.4-46.fc7
Selinux Enabled:	True
Policy Type:	targeted
MLS Enabled:	True
Enforcing Mode:	Enforcing
Plugin Name:	plugins.mislabeled_file
Host Name:	localhost.localdomain
Platform:	Linux localhost.localdomain 2.6.22.9-91.fc7 #1 SMP Thu Sep 27 20:47:39 EDT 2007 x86_64 x86_64
Alert Count:	1
First Seen:	Sun 14 Oct 2007 08:25:17 AM EST
Last Seen:	Sun 14 Oct 2007 08:25:17 AM EST

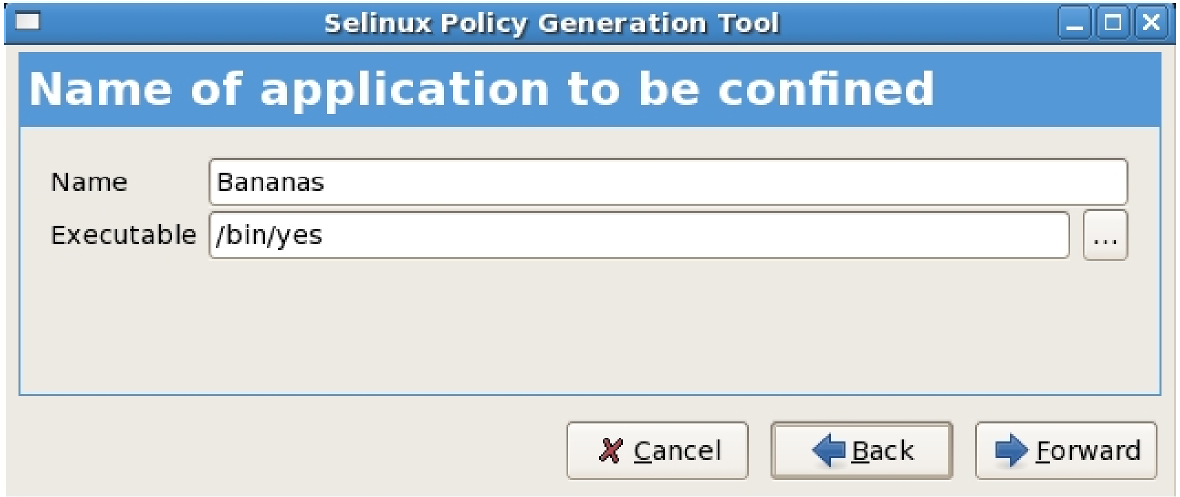
Audit Listener 34/34

Project Update

Toolkit

Policy Wizard GUI

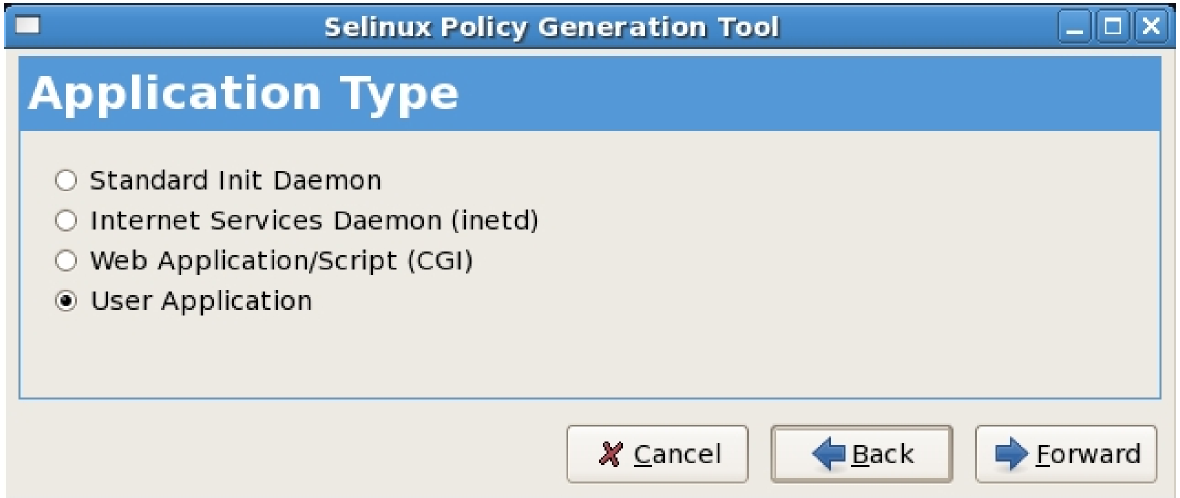
- Simple guided policy generation tool
- Uses common application traits to create a loadable policy module for an application



Name of application to be confined

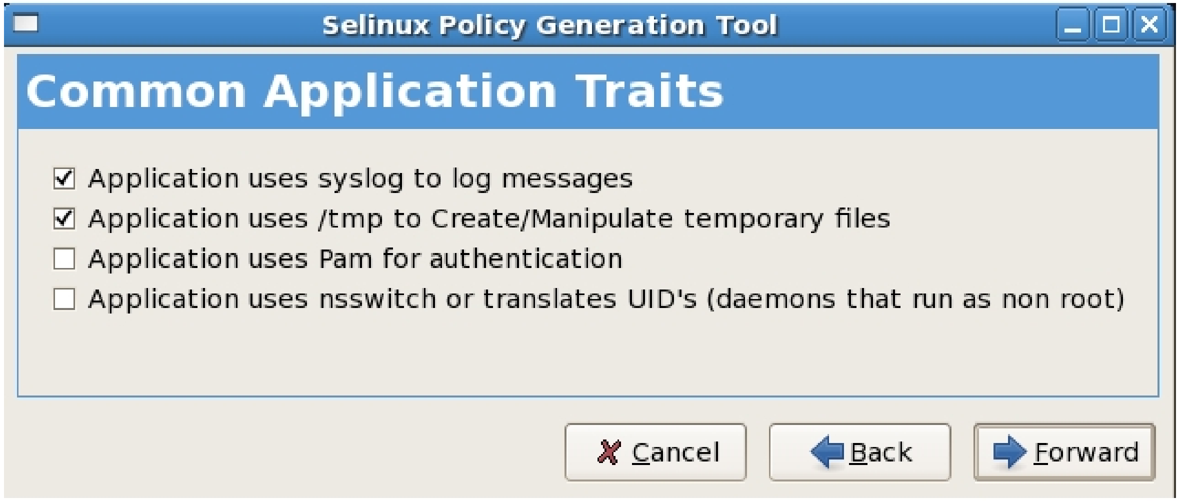
Name: Bananas

Executable: /bin/yes



Application Type

○ Standard Init Daemon
○ Internet Services Daemon (inetd)
○ Web Application/Script (CGI)
● User Application



Common Application Traits

☑ Application uses syslog to log messages
☑ Application uses /tmp to Create/Manipulate temporary files
□ Application uses Pam for authentication
□ Application uses nsswitch or translates UID's (daemons that run as non root)

Project Update

Protection

- Memory access checks
- Targeted policy now covers ~240 confined domains.

Project Update

Certification

RHEL5 Common Criteria certified to EAL4+ against the protection profiles:

- LSPP – Labeled Security (“MAC”)
- CAPP – Controlled Access (“audit”)
- RBACPP – Role Based Access Control

Performed on IBM and HP hardware.

Project Update

Certification

- Significantly enhanced audit capabilities
- pam_namespace utilizes kernel namespaces to provide private views of the fileystem
- Improved labeled networking, including IPsec-based and legacy CIPSO labels for talking to existing Trusted OSs

Project Update

Secmark

- Uses iptables to categorize & label packets
- Leverages iptables tools, modules, connection tracking, connection assurance etc.
- More secure and also vastly simplifies policy

Project Update

X Access Control Extension (XACE)

- Security framework extension for X server
- Merged into X.org
- Important step in securing the desktop

Project Update

Continued extension beyond Linux kernel

- Gconf – desktop environments
- SE-PostgreSQL – databases
- XSM – virtualization
- SEDarwin – other operating systems

Project Update

Testing

Linux Test Project (LTP) support for Reference Policy

IBM and HP released certification testsuites to LTP

Project Update

General

SELinux By Example published, very comprehensive book

xguest: constrained guest user for kiosk use

Many contributions from Japanese community:

- Performance and memory use improvements
- Busybox integration
- Segatex (QT-based management suite)
- SEedit (simplified policy editor)

Challenges

Usability

- Security and usability are inherently at odds
- No magic bullet
- Progress being made; need to continue building higher level tools and abstractions

Ongoing Work

- Better support for developers and administrators
- High level tools for end users
- Continued work on desktop support
- Full NFS support
- Higher level policy language
- Architectural refinements

How to Help

- Join the mailing list
  - http://www.nsa.gov/selinux/info/subscribe.cfm
- Submit bug reports
- Documentation
- Developer and admin tools
- Usability for end users
- Your distribution probably has an SELinux team

Resources

Main page

http://www.nsa.gov/selinux/

News & planet

http://selinuxnews.org/

Conference papers

http://selinux-symposium.org/

Tresys open source projects

http://oss.tresys.com/