RED HAT SUMMIT

10 YEARS *and counting*

SAN FRANCISCO | APRIL 14-17, 2014

Secure Foundations:

An SELinux Primer

Shawn Wells

Director, Innovation Programs &
Lead Developer, SCAP

redhat.

20 MINUTES, 2 QUESTIONS

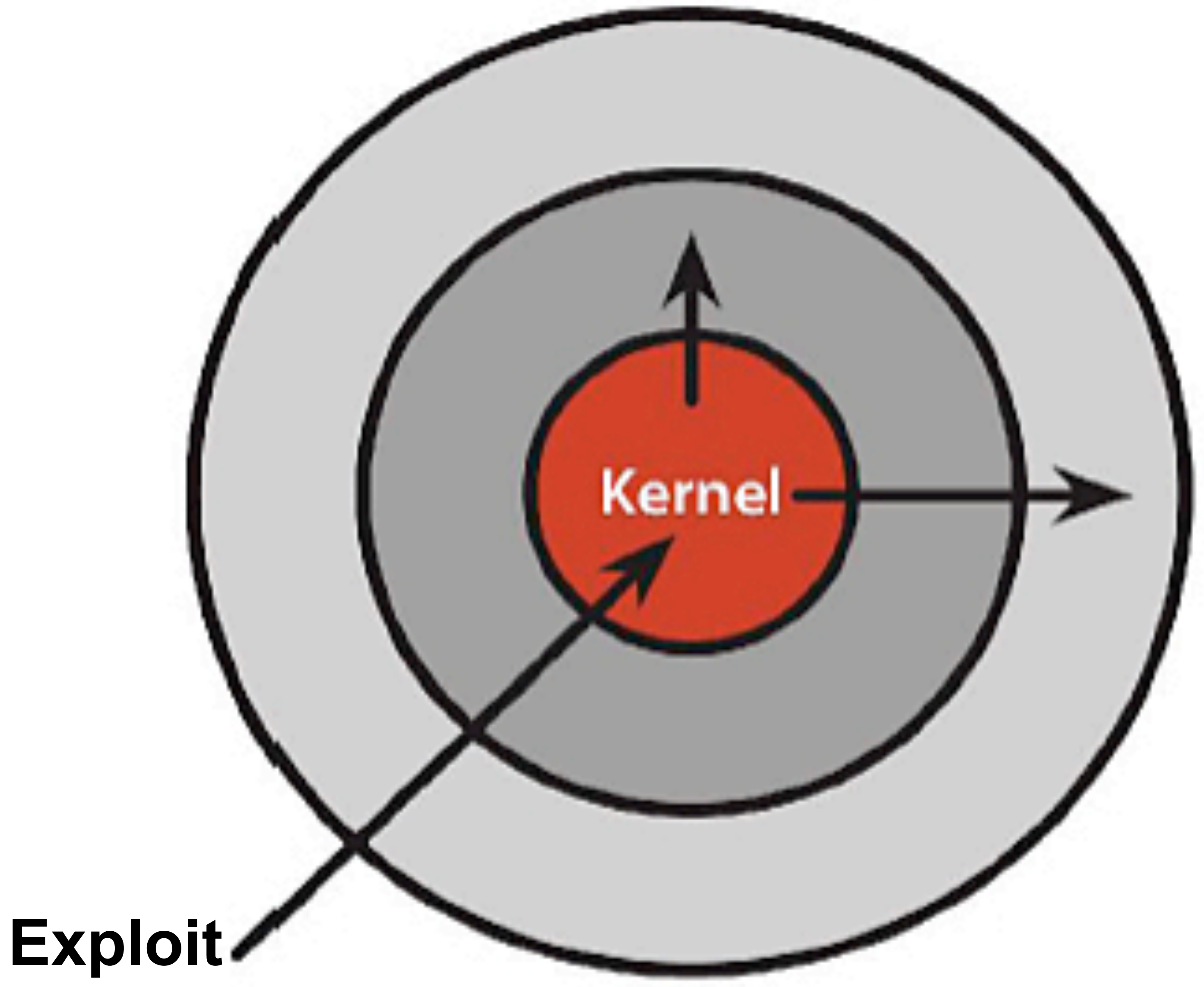
1. How do we label data?

2. How do we verify security compliance?

FIRST: An SELinux History Lesson

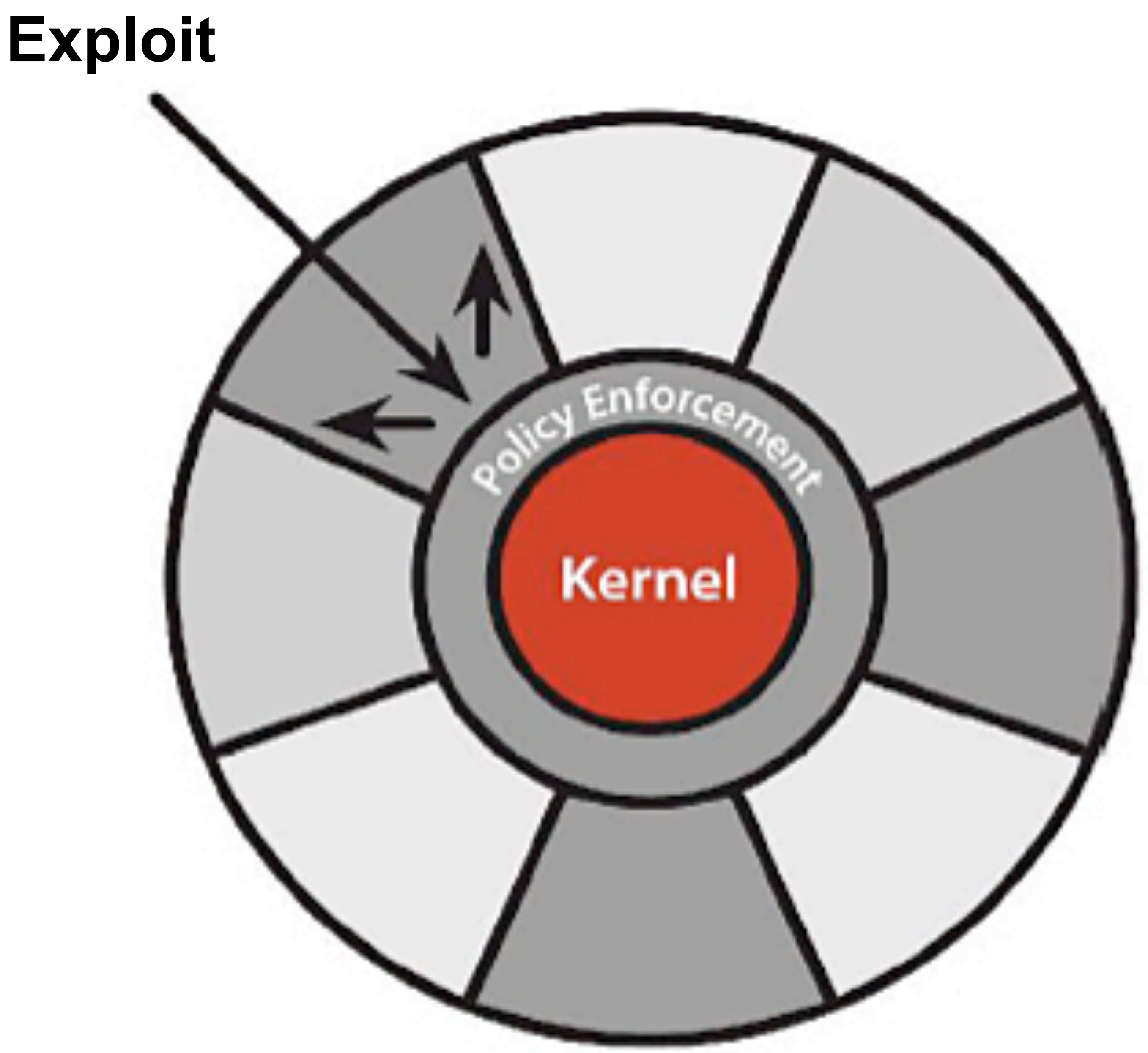
- Originated from NSA R&D
- First release in December 2010
- Integrated into mainline Linux in 2003

FIRST: An SELinux History Lesson



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.



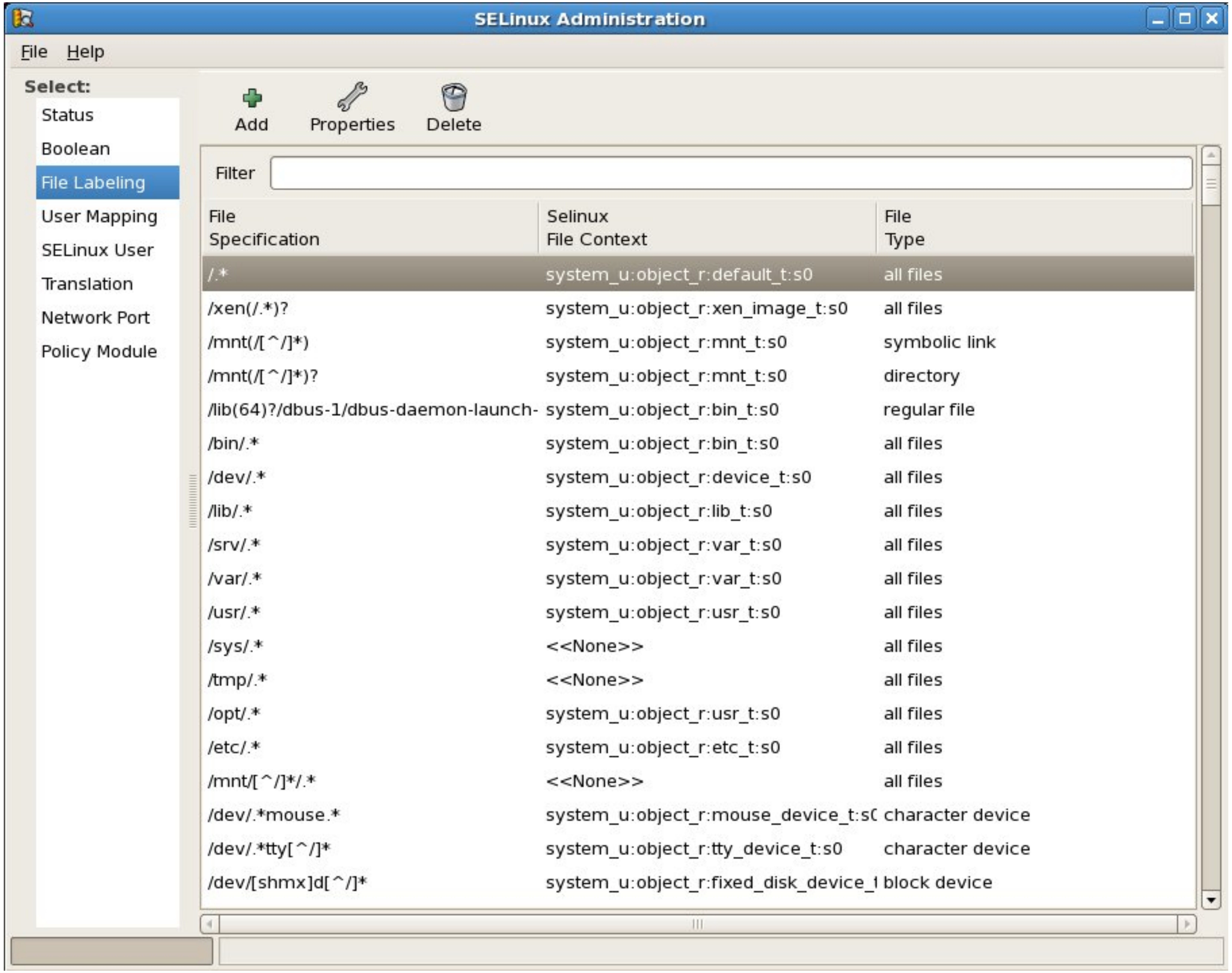
Mandatory Access Control

Kernel policy defines application rights, firewalling applications from compromising the entire system.

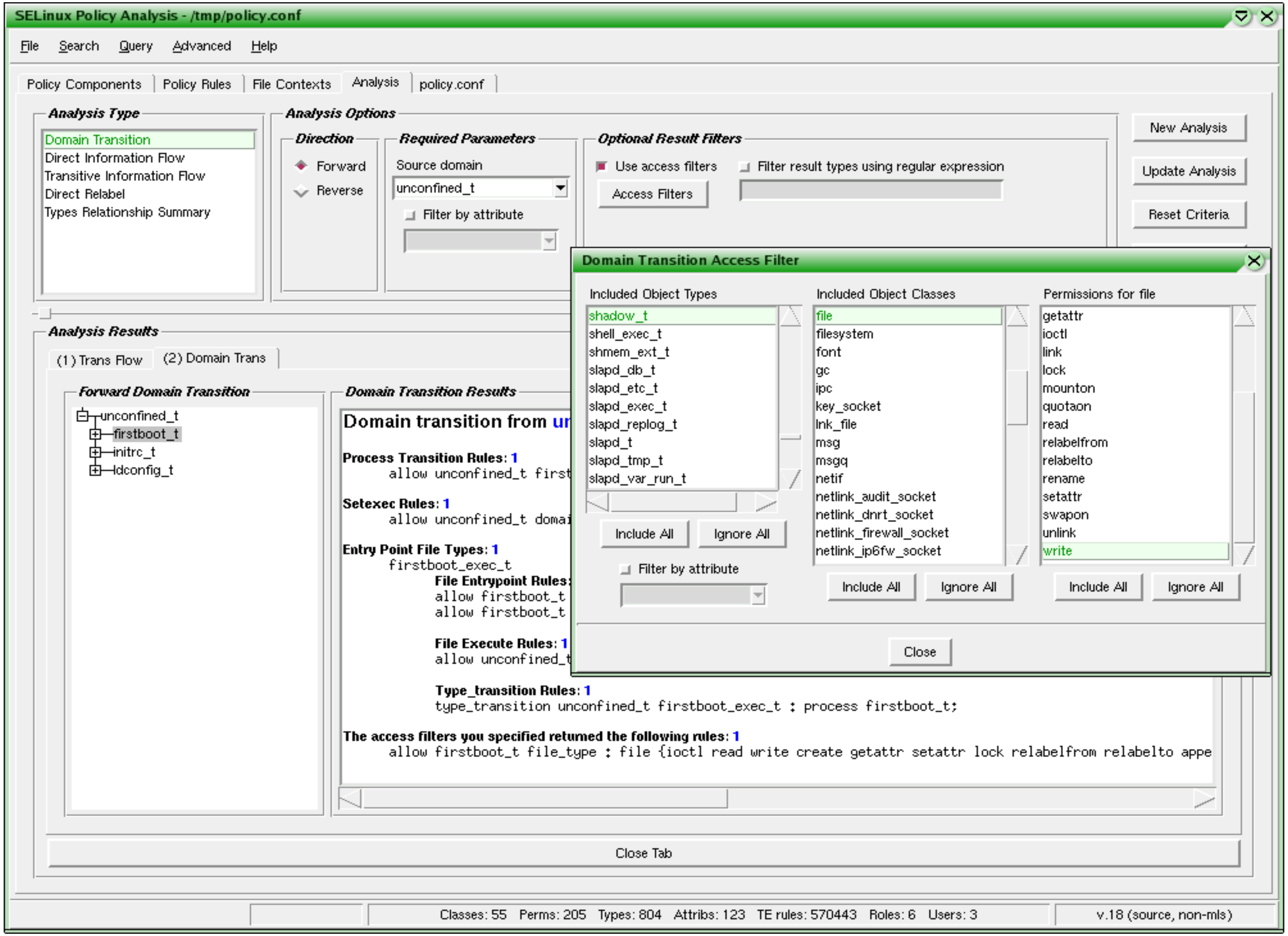
What An Attacker Can’t Do

- Read/manipulate user data
- Read/manipulate system files
- Attack data/processes owned by other compartments (via polyinstantiation)
- Attack other machines on the network, unless authorized to pass traffic on specific port
- Evade audit subsystem

Role Based Access Control



File Specification	Selinux File Context	File Type
/.*	system_u:object_r:default_t:s0	all files
/xen(/.*)?	system_u:object_r:xen_image_t:s0	all files
/mnt(/[^/]*)	system_u:object_r:mnt_t:s0	symbolic link
/mnt(/[^/]*)?	system_u:object_r:mnt_t:s0	directory
/lib(64)?/dbus-1/dbus-daemon-launch-	system_u:object_r:bin_t:s0	regular file
/bin/.*	system_u:object_r:bin_t:s0	all files
/dev/.*	system_u:object_r:device_t:s0	all files
/lib/.*	system_u:object_r:lib_t:s0	all files
/srv/.*	system_u:object_r:var_t:s0	all files
/var/.*	system_u:object_r:var_t:s0	all files
/usr/.*	system_u:object_r:usr_t:s0	all files
/sys/.*	<<None>>	all files
/tmp/.*	<<None>>	all files
/opt/.*	system_u:object_r:usr_t:s0	all files
/etc/.*	system_u:object_r:etc_t:s0	all files
/mnt/[^/]*/.*	<<None>>	all files
/dev/.*mouse.*	system_u:object_r:mouse_device_t:s(	character device
/dev/.*tty[^/]*	system_u:object_r:tty_device_t:s0	character device
/dev/[shmx]d[^/]*	system_u:object_r:fixed_disk_device_	block device



Analysis Type

- Domain Transition
- Direct Information Flow
- Transitive Information Flow
- Direct Relabel
- Types Relationship Summary

Analysis Options

Direction

● Forward
○ Reverse

Required Parameters

Source domain: unconfined_t

□ Filter by attribute

Optional Result Filters

☒ Use access filters
□ Filter result types using regular expression

Domain Transition Access Filter

Included Object Types	Included Object Classes	Permissions for file
shadow_t	file	getattr
shell_exec_t	filesystem	ioctl
shmem_ext_t	font	link
slapd_db_t	gc	lock
slapd_etc_t	ipc	mounton
slapd_exec_t	key_socket	quotaon
slapd_replog_t	lnk_file	read
slapd_t	msg	relabelfrom
slapd_tmp_t	msgq	relabelto
slapd_var_run_t	netif	rename
	netlink_audit_socket	setattr
	netlink_dnrt_socket	swapon
	netlink_firewall_socket	unlink
	netlink_ip6fw_socket	write

□ Filter by attribute

Analysis Results

(1) Trans Flow (2) Domain Trans

Forward Domain Transition

```
unconfined_t
  firstboot_t
  initrc_t
  ldconfig_t
```

Domain Transition Results

```
Domain transition from ur
Process Transition Rules: 1
      allow unconfined_t first
Setexec Rules: 1
      allow unconfined_t domai
Entry Point File Types: 1
      firstboot_exec_t
            File Entrypoint Rules:
            allow firstboot_t
            allow firstboot_t

            File Execute Rules: 1
            allow unconfined_t

            Type_transition Rules: 1
            type_transition unconfined_t firstboot_exec_t : process firstboot_t;

The access filters you specified returned the following rules: 1
      allow firstboot_t file_type : file {ioctl read write create getattr setattr lock relabelfrom relabelto appe
```

Classes: 55 Perms: 205 Types: 804 Attribs: 123 TE rules: 570443 Roles: 6 Users: 3 v.18 (source, non-mls)

SCAP
Security Guide

DEFENSE INFORMATION SYSTEMS AGENCY

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

redhat

SCAP HTML

OpenSCAP Firefox

	Red Hat Enterprise Linux 6 with KVM	Red Hat Enterprise Linux 5.6 with KVM	IBM z/VM Version 5 Release 3 (for IBM System z Mainframes)	VMWare vSphere 5.0	VMWare ESXi 4.1	Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050
Certification Date	2012-10-08	2012-04-20	2008-08-06	2012-05-18	2010-12-15	2009-07-24
EAL Level	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+
CAPP	YES	YES	YES	NO	NO	NO
RBAC	YES	YES	NO	NO	NO	NO
LSPP	YES	YES	YES	NO	NO	NO