NSA Security-Enhanced Linux (SELinux)

http://www.nsa.gov/selinux

Stephen D. Smalley

sds@tycho.nsa.gov

National Information Assurance Research Laboratory

National Security Agency

What is SELinux?

- Flexible Mandatory Access Control (MAC) for Linux.
- Configurable policy engine supporting:
  - Type Enforcement (TE), Role-Based Access Control (RBAC)
  - Optionally Multi-Level Security (MLS)
- Ability to enforce confidentiality and integrity guarantees.
- Ability to confine flawed and malicious applications.
- Ability to enforce assured pipelines.

SELinux: Key Properties

- Complete mediation
  - Control over all processes, objects, operations.
- Control based on all security-relevant information.
  - Properties of the actual process and object, not just its name.
- Configurable support for meeting application security requirements transparently.
  - Assured pipelines.
- Infrastructure for security-aware applications.
  - A secure system requires more than just a secure OS.

SELinux: Background

- Originated from NSA R&D.
- First public release by NSA in Dec 2000.
- Large and growing user and developer community.
- First packaged externally for Debian.
- Integrated into Hardened Gentoo.
- Integrated into mainline Linux 2.6 in Aug 2003.
- Included and enabled in Red Hat distributions.
  - Fedora Core 3, 4, and 5; Red Hat Enterprise Linux 4

Recent Advances in SELinux

- Improved integration with audit subsystem.
- Enhanced network packet labeling and control.
- Enhanced filesystem labeling support.
- Key management controls.
- Improved base policy.
- Loadable policy modules.
- Policy management infrastructure and tools.
- Improved and new policy development tools.

Improved Audit Integration

- Extended syscall audit records with security contexts.
- Enabled filtering based on security contexts.
- Added auditing of SELinux specific events.
- Enabled audit of netlink capability checks.
- Some parts included in Linux 2.6.17, further support added for 2.6.18.

Network Labeling: IPSEC/xfrm

- Implicit packet labeling via IPSEC/xfrm.
- Security context stored in xfrm policy rules and states.
- Authorize socket's use of policy based on context.
- Build SAs with context of policy.
- Included in Linux 2.6.16.
- TCP SO_PEERSEC support, UDP SCM_SECURITY support added in Linux 2.6.17.

Network Control: SECMARK

- Motivation: Existing SELinux network controls very limited in expressiveness and coverage.
- Solution: Separate labeling from enforcement.
  - Use iptables to select and label packets.
  - Use SELinux to enforce policy based on those labels.
- SECMARK and CONNSECMARK targets added.
- http://james-morris.livejournal.com/11010.html
- For 2.6.18.

Network Labeling: MLS enhancements

- Granular IPSEC associations
  - Allow a single xfrm poilcy rule to cover a MLS range.
  - Instantiate individual SAs for individual levels within the range.
- Flow labeling outside of socket context
  - Label based on origin when no socket involved (e.g. forward)
- Label socket IPSEC policy from socket.
- Label TCP child sockets from peer.
- In progress, see redhat-lspp and netdev lists.

Network Labeling: NetLabel

- Explicit packet labeling via IP option.
- Motivation: Compatibility with other trusted OSes.
  - Also avoids requiring use of iPSEC for labeling.
  - Also enables packet filtering based on the explicit labels.
- Presently limited to CIPSO, MLS labels.
- Code and info at http://free.linux.hp.com/~pmoore/projects/linux_cipso/

Filesystem Labeling

- Jffs2 xattr support (for 2.6.18)
- Improvements to mount context options (for 2.6.18)
- Atomic labeling of new files (2.6.14)
- VFS fallback for security xattrs (2.6.14)
- Canonicalization of getxattr results (2.6.15)

Key Management Controls

- Added security labeling of keys upon creation.
- Added basic permission checks on key operations.
- Added keycreate support to specify key labels.
- Randomized key serial number generation.
- Filtered /proc/keys output.
- For 2.6.18.

Reference Policy

- Improved base policy for SELinux, replaces old example policy.
- Strong modularity with explicit interfaces.
- Inline documentation.
- Ability to build policy variants from single source base.
- Deployed as the base policy in Fedora Core 5.
- http://oss.tresys.com

Loadable Policy Modules

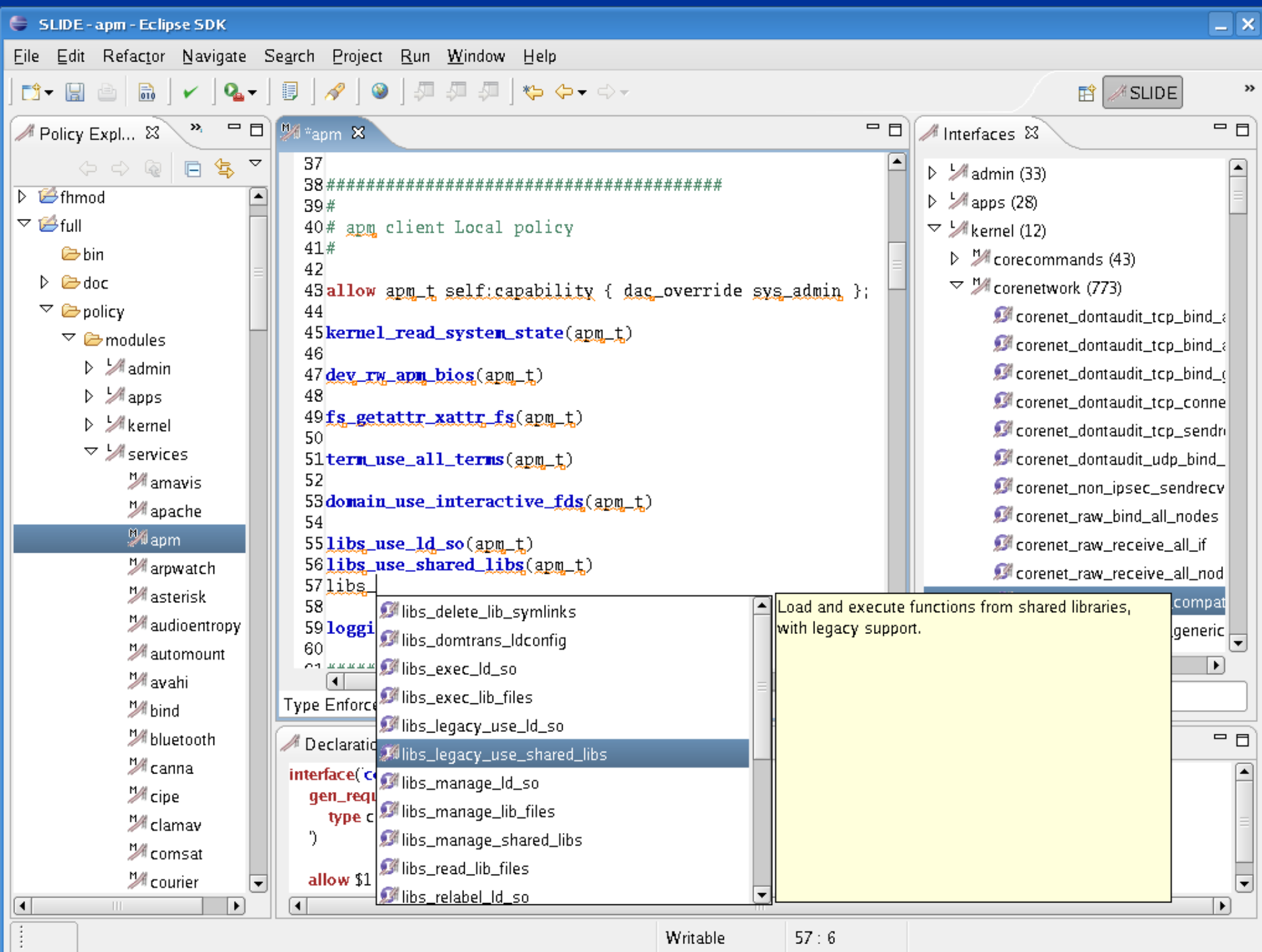
- Ability to build and package policy modules separately.
- Avoids need for policy sources for local customizations.
- Enables third party policy and decomposition of distro policy.
- Initially deployed in Fedora Core 5.
- Ongoing work to migrate policy into individual packages for Fedora Core 6.

Policy Management

- Standard library for applications to use to manipulate policy (libsemanage).
- Designed to support multiple back-ends transparently.
  - Initial support for direct manipulation of policy store.
  - Work in progress for policy management server daemon.
- Used by policy management tools.
  - Semodule, semanage, setsebool

Policy Development Tools

- SLIDE, http://oss.tresys.com
  - Integrated Development Environment for policy
  - Eclipse plugin, integrates with reference policy
- SEEdit, http://seedit.sourceforge.net
  - Policy editor with simplified policy language, GUI
- Polgen, http://www.mitre.org/tech/selinux
  - Policy generation tool based on pattern recognition
- SETools, http://www.tresys.com/selinux
  - Policy analysis tools


SLIDE - apm - Eclipse SDK
File Edit Refactor Navigate Search Project Run Window Help
SLIDE
Policy Expl...
fhmod
full
bin
doc
policy
modules
admin
apps
kernel
services
amavis
apache
apm
arpwatch
asterisk
audioentropy
automount
avahi
bind
bluetooth
canna
cipe
clamav
comsat
courier
*apm
37
38 ##
39 #
40 # apm client Local policy
41 #
42
43 allow apm_t self:capability { dac_override sys_admin };
44
45 kernel_read_system_state(apm_t)
46
47 dev_rw_apm_bios(apm_t)
48
49 fs_getattr_xattr_fs(apm_t)
50
51 term_use_all_terms(apm_t)
52
53 domain_use_interactive_fds(apm_t)
54
55 libs_use_ld_so(apm_t)
56 libs_use_shared_libs(apm_t)
57 libs_
58
59 loggi
60
Type Enforce
libs_delete_lib_symlinks
libs_domtrans_ldconfig
libs_exec_ld_so
libs_exec_lib_files
libs_legacy_use_ld_so
libs_legacy_use_shared_libs
libs_manage_ld_so
libs_manage_lib_files
libs_manage_shared_libs
libs_read_lib_files
libs_relabel_ld_so
Load and execute functions from shared libraries, with legacy support.
Declaratio
interface(`c
gen_requ
type c
')
allow $1
Interfaces
admin (33)
apps (28)
kernel (12)
corecommands (43)
corenetwork (773)
corenet_dontaudit_tcp_bind_
corenet_dontaudit_tcp_bind_
corenet_dontaudit_tcp_bind_
corenet_dontaudit_tcp_conne
corenet_dontaudit_tcp_sendr
corenet_dontaudit_udp_bind_
corenet_non_ipsec_sendrecv
corenet_raw_bind_all_nodes
corenet_raw_receive_all_if
corenet_raw_receive_all_nod
compat
generic
Writable
57 : 6

Next Steps

- Securing the desktop
  - Reviving the XACE/XSELinux implementation, upstreaming it.
  - Labeled windowing.
  - Addressing other desktop infrastructure components.
  - Ensuring that user applications function properly in a secured environment.
- Improved useability
  - New troubleshooting tool
  - Continued improvements to policy tools

Next Steps (Cont)

- Policy Management
  - Completing the policy management server daemon and the libsemanage backend support.
  - Extending management to collections of SELinux hosts, including support for local variations and policy splitting.
  - Reconciling differences in policies between SELinux systems.
- Improvements to policy modules
  - Language support for interfaces
  - Integration with package management

Next Steps (Cont)

- Integration with SE-Xen
  - Flask architecture in Xen hypervisor.
  - Support for Xen object managers, like XenStore.
  - Policy management for Xen policy (shared toolchain).
  - Coordination with guest policies.
- NFS integration
  - Extending NFSv4 to support process and file security attributes.
  - Ensuring correct enforcement on client and server.

Credits

- HP (audit, MLS, NetLabel)
- IBM (audit, MLS, IPSEC labeling)
- MITRE (Polgen)
- NEC (SMP scalability, jffs2 xattr, embedded)
- Red Hat (audit, fs labeling, SECMARK, semanage)
- Tresys Technology (refpolicy, modules, semanage, policy server, SLIDE, SETools)
- Trusted Computer Solutions (audit, MLS, IPSEC labeling)
- And the entire SELinux community...

Resources

- SELinux News http://selinuxnews.org
- Sourceforge project http://selinux.sourceforge.net
- SELinux Symposium http://selinux-symposium.org
- NSA SELinux site http://www.nsa.gov/selinux
- Tresys Technology site http://oss.tresys.com

End of Presentation