What's New with SELinux

Stephen D. Smalley

sds@tycho.nsa.gov

National Information Assurance Research Laboratory

National Security Agency

Advances in SELinux

- Deploying new technologies.
- Enabling evaluation and accreditation.
- Spanning the network.
- Securing the desktop.
- Reaching the user.
- Transferring the concepts.

Deploying New Technology

- Successful deployment of several new technologies:
  - Reference policy
  - Loadable modules
  - Policy management infrastructure

Reference Policy

- Improved base policy for SELinux.
- Strong modularity with explicit interfaces.
- In-line documentation.
- Single source base.

Loadable Policy Modules

- Build and package policy modules separately.
- Local customizations without base policy sources.
- Enables third party policy.
- Enables decomposition of distribution policy.

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 local policy store.
  - Work in progress for remote policy.
- Used by policy management tools.
  - semodule, semanage, setsebool

Deploying New Technology

- New technologies Integrated into several distributions:
  - Fedora Core 5 and 6
  - Red Hat Enterprise Linux 5
  - Hardened Gentoo
  - Debian etch
- A new generation of SELinux technology is available to users.

Enabling Evaluation and Accreditation

- Meeting requirements for evaluation.
  - Enhanced audit and MLS support.
  - RHEL 4 - Validated for CAPP EAL4+
  - RHEL 5 - In evaluation for CAPP, LSPP, RBACPP EAL4+
- Meeting requirements for accreditation.
  - Providing a mechanism for data separation.
  - NetTop, NetTop 2
  - Certifiable Linux Integration Platform (CLIP)
  - Cross Domain Solutions (CDS)

Enhanced Audit Support

- 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.

Enhanced MLS support

- Mainstreaming of MLS support.
  - Runtime option.
  - Constraint-based configuration.
  - Engine and labeling enabled by default.
- New functionality for MLS.
  - Multi-level directories via Linux namespaces.
  - Labeled networking (labeled IPSEC, NetLabel).
  - Application integration.

Spanning the Network

- End-to-end data labeling and control of network traffic.
  - Labeled IPSEC (improved)
  - NetLabel (new)
- Flexible policy-based packet filtering.
  - SECMARK (new)

Labeled IPSEC

- Implicit packet labeling via IPSEC/xfrm.
- Security contexts exchanged by IKE daemons.
- Several extensions and improvements in 2006:
  - Granular security associations based on socket context.
  - Support for obtaining peer security context.
  - Flow and sock labeling.
  - MLS labeling of child sockets.
- Enables integration of network protection with data labeling.

NetLabel

- Explicit packet labeling framework.
  - Supports use of CIPSO with IPv4 for MLS labels.
  - Planned extensions for IPv6, full contexts.
- Enables compatibility with legacy trusted OSes.
- Enables packet filtering based on explicit labels.

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.
- Userland and policy integration incomplete.
- Compatibility mode for legacy controls (compat_net).

Securing the Desktop

- X Access Control Extension (XACE) framework
  - General framework for access control in X server.
  - Similar to LSM framework for the Linux kernel.
  - Merged into Xorg server 1.2
- XSELinux module
  - Flask policy engine for flexible MAC.
  - Planned to be merged into Xorg server 1.4

Reaching the User

- Reporting and diagnosing problems
  - Setroubleshoot (new)
- Generating policy
  - Polgen (updated)
    - Generate based on pattern recognition on trace data.
  - Razor (new)
    - Generate from application-specific configuration.
  - Madison / SEPolgen (new)
    - Generate from SELinux (avc) audit data.

Reaching the User

- Authoring policy
  - SLIDE (new)
    - Eclipse-based Integrated Development Environment (IDE)
    - Integrated support for testing policy on remote system.
  - CDS Framework (new)
    - High level language and IDE for expressing CDS architecture and goals
    - Generate policy from high level description.
- Understanding policy
  - SETools (updated)

Reaching the User

- Managing policy
  - semodule, semanage, setsebool (updated)
    - Command line tools, use libsemanage.
    - Manage modules, contexts, booleans.
  - system-config-selinux (new)
    - GUI front-end.
  - Brickwall (new)
    - Product for managing SELinux on RHEL.
    - Ease of configuration, network policy.

Transferring the Concepts

- Securing the platform
  - Xen Security Modules (XSM) and Flask
- Applying to applications
  - GConf, PostgresQL
  - RADaC
- Influencing other operating systems
  - SEBSD and SEDarwin
- Porting to other environments
  - Embedded

Next Steps

- Securing the desktop
  - Labeled windows, trusted input and display
  - Desktop applications
- Policy management
  - Fine-grained access control over policy
  - Distributed policy management
  - Managing the platform policy
  - Improved front-end tools

Next Steps

- Distributed policy enforcement
- Easier policy development
- Policy language and toolchain improvements
- Further userland integration
  - SELinux awareness
  - Leveraging SELinux
  - Application level access control

Credits

- Deploying New Technology - Red Hat, Tresys
- Evaluation and Accreditation - HP, IBM, Red Hat, TCS, Tresys
- Spanning the Network - HP, IBM, Red Hat, TCS, Tresys
- Securing the Desktop - NSA, TCS
- Reaching the User - Tresys, Red Hat, MITRE
- Transferring the Concepts - NSA, SPARTA, NEC, Hitachi Software
- 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
- Book: SELinux by Example (Frank Mayer et al, Prentice Hall, 2006)

Questions?

- Mailing list: Send 'subscribe selinux' to majordomo@tycho.nsa.gov
- Contact our team at: selinux-team@tycho.nsa.gov
- Contact me at: sds@tycho.nsa.gov

End of Presentation