SELinux Year in Review

Stephen D. Smalley

sds@tycho.nsa.gov

National Information Assurance Research Laboratory

National Security Agency

Outline

- SELinux Background
- The Year in Review
- What Lies Ahead

The Problem: Inadequate OS Security

- OS protection mechanisms are foundational.
- General purpose OSes lack adequate security mechanisms.
  - No protection against flawed or malicious applications.
  - Key missing feature: Mandatory Access Control (MAC)
- "Trusted" OSes had a form of MAC but:
  - were not mainstream
  - used a fixed, limited MAC model (BLP/Biba)

The Solution: Flexible MAC

- Generalize MAC and make it flexible and configurable
- Developed several research prototypes
- Selected Linux for optimal technology transfer
- Released reference implementation in December 2000
- Reworked approach for Linux Security Module framework
- Integrated into mainline Linux 2.6 in August 2003

What SELinux Provides

- Flexible MAC integrated into 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.

Uses of SELinux

- Enforce legal restrictions on data.
- Prevent disclosure of sensitive data.
- Prevent tampering with software and data.
- Enforce critical processing on data.

Uses of SELinux

- Restrict system services to authorized data.
- Sandbox applications.
- Prevent privilege escalation.
  - Contain damage from 0-day exploits.
  - Reduce need for immediate security patching of applications.

A Year Ago

- SELinux included and enabled in Fedora Core 3 and Red Hat Enterprise Linux 4.
  - With several daemons locked down including Apache...
- SELinux included as an option in Hardened Gentoo.
  - With strict policy, servers only.
- SELinux available for other distributions.
  - Separate packages available for Debian unstable, SuSE.

Now

- SELinux coverage significantly expanded in Fedora Core 4 (June 2005) and 5 (soon).
  - Targeted policy has grown to ~120 confined domains.
- SELinux updates in Hardened Gentoo.
- SELinux support being mainstreamed into Debian.
  - Patches upstreamed into Debian unstable.
  - Separate back-port packages available for Debian stable.

A Year Ago

- SELinux Multi-Level Security support was experimental and unused.
- Auditing support was limited and not well integrated with SELinux.
- No distribution with SELinux included had been evaluated.

Now

- Multi-Level Security support enhanced and mainstreamed.
- Audit system enhanced and increasingly integrated.
- RHEL4 evaluated against CAPP (excludes SELinux).
- RHEL5 entered into evaluation against CAPP, LSPP, and RBAC with SELinux coverage.

A Year Ago

- Monolithic policy.
  - Source modules only, little encapsulation.
- Limited, ad-hoc forms of policy customization.
  - Difficult to customize and still track vendor policy updates.
- No programmatic interface for policy management.
  - Manipulation of text files, execution of policy build process.
- Limited support for policy generation and development.

Now

- Loadable policy modules
  - Build and package policy modules separately.
- Reference policy
  - Explicit interfaces, strong encapsulation.
- Policy management API (libsemanage)
  - Supports module operations and variety of local policy customizations.
- Improved support for policy development.
  - Polgen, SEEdit, SLIDE, CDS Framework.

A Year Ago

- No upstream solution for labeled networking.
- Newly created files not labeled atomically.
- File security labels only visible for some filesystems.
- SMP scalability increasingly a problem.
- Kernel memory use by policy increasingly a problem.

Now

- IPSEC-based packet labeling upstream, scheduled for Linux 2.6.16.
- Atomic labeling of new files.
- File security labels visible for all filesystems exactly as seen by SELinux.
- Major improvements in SMP scalability.
- Significant reduction in kernel memory use by policy.

What Lies Ahead

- Fine-grained access control over policy
- Distributed policy management
- Policy IDE and generation tools
- Flexible networking controls
- Network protected paths
- Security-aware applications
- Securing the desktop
- Completion of the LSPP/RBAC functionality

Credits

- HP (audit, MLS)
- IBM (audit, polyinstantiation, IPSEC, MLS)
- MITRE (slat, polgen)
- NEC (SMP scalability)
- Red Hat (targeted policy, MCS, audit, semanage)
- Tresys Technology (setools, modules, refpolicy, semanage, SLIDE, CDS Framework)
- Trusted Computer Solutions (MLS, audit)
- And the entire SELinux community...

Questions?

- Download code and documents from http://www.nsa.gov/selinux
- 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