NSA Security-Enhanced Linux (SELinux)

http://www.nsa.gov/selinux

NSA SELinux team
selinux-team@tycho.nsa.gov

Information Assurance Research Group
National Security Agency
What is SELinux?

- Flexible mandatory access controls integrated into Linux.
  - Can confine malicious or flawed applications and services.
  - Can enforce strong separation based on confidentiality, integrity, or purpose.
  - Can support fine-grained least privilege.
  - Architecture supports wide range of security policies.
  - API supports security-aware applications and application policy enforcers.
  - Transparency provided for unmodified applications.
SELinux Status

- Initial public release in Dec 2000, regular updates
- Active public mailing list, >900 members
  - External developer and user community
- Motivated development of Linux Security Module (LSM) framework
  - SELinux drove requirements for the LSM framework
  - LSM adopted into Linux 2.5/2.6 kernel
  - Provides infrastructure for supporting SELinux
- SELinux in Linux 2.6 kernel
SELinux Integration

• RedHat
  – Integrated in Fedora Core (FC) 2, but off by default
  – Enabled by default in FC 3 with targeted policy

• Gentoo
  – Integrated in Hardened Gentoo

• Debian
  – Available as separate packages from Russell Coker

• SuSE
  – Partially integrated in SuSE Linux 9.1
  – Available as separate packages from Thomas Bleher
SELinux and Auditing

- SELinux originally used existing kernel logging infrastructure for its audit messages.
- RedHat developed a new kernel audit framework and converted SELinux to use it.
- Advantages:
  - Audit can be directed to a separate daemon
  - Audit flooding can be more effectively addressed
  - Audit framework captures information not available to SELinux
  - Audit framework provides calls that can be safely called from any context
SELinux and NFS

- **NFSv3 SE Linux support**
  - Provides fine-grained labeling and access controls on NFS files
  - Not targeted for mainstream inclusion

- **NFSv4 SE Linux support**
  - Started dialogue with NFSv4 developers
  - Seeking to leverage named attribute and RPCSEC_GSS support
  - Goal is for mainline support for NFSv4 and SE Linux
Security-Enhanced X

- Available as a branch in xorg CVS tree.
- Provides labeling and access controls for X objects.
- Implemented using a security hook framework.
- Drove development of general infrastructure for userspace policy enforcers.
- Limited to X server, does not address window manager issues.
- Policy still needs to be developed.
Security-Enhanced DBUS

- D-BUS is a message bus system for inter-application communication.
  http://www.freedesktop.org/Software/dbus
- SE-DBUS adds labeling and access controls for D-BUS to control the ability to register services and to communicate via D-BUS.
- Patch has been submitted and revised, undergoing assessment for integration into mainstream D-BUS.
- Policy still needs to be developed.
Policy Tools

- **Setools** from Tresys Technology, 
  http://www.tresys.com/selinux
  - Included in upstream NSA SELinux releases
  - Packaged for Fedora Core 2 and 3
  - Policy analysis, audit analysis, user management

- **Slat** from MITRE, http://simp.mitre.org/selinux
  - Included in upstream NSA SELinux releases
  - Policy analysis
Policy Infrastructure

• Policy modules
  – Under development by Tresys
  – Allow well-defined modules to be added and removed to policy at runtime
  – Provide proper dependency checking, stronger encapsulation

• Policy daemon
  – Under development by Tresys
  – Allow fine-grained access for making changes to policy
  – Allow delegation of userspace policies
MLS/Trusted System Support

• Being extended and enhanced by TCS.
• May require adding a level of indirection between security contexts and human-readable labels.
• May require adding limited support for non-tranquility of processes.
• May require ability to authorize capabilities based solely on SELinux policy.
Future Directions

• Integrate with IPSEC for labeling and protection.
• Identify and add controls to other userspace object managers beyond X and D-BUS.
• Assess effectiveness of SELinux primitives for application security requirements.
• Identify and replace hardcoded userspace policy logic (e.g. uid 0 assumptions) with calls to SELinux API.
Questions?

• NSA SELinux site: http://www.nsa.gov/selinux
• Public mailing list: Send 'subscribe selinux' to majordomo@tycho.nsa.gov
• Contact us at: selinux-team@tycho.nsa.gov
• Sourceforge project: http://sf.net/projects/selinux
• SELinux for Distributions:
  – Fedora Core: fedora.redhat.com
  – Gentoo: www.gentoo.org/proj/en/hardened
  – SuSE: www.cip.ifi.lmu.edu/~bleher/selinux/suse
Possible topics

• Using SELinux user identity and roles as intended
  – Keeping policy user database in sync with real users
  – Dealing with pseudo user identities and su
  – Reducing need to trust su, sudo, etc.

• Increasing acceptability/transparency of strict policy
  – without loss in protection

• Increasing protection provided by targeted policy
  – without loss in acceptability/transparency

• Hindrances to SELinux acceptability/useability
End of Presentation