SELinux Project Overview

8th Linux Foundation Japan Symposium
July 2008, Tokyo

James Morris
jmorris@redhat.com
Outline

- SELinux Introduction
- Rationale and Design
- Project Milestones
- Current Work and Challenges
What is SELinux?

Security Framework

- Pluggable security models
- Clean separation of policy and mechanism
- Coherent stacking (composition)
- Fully analyzable
What is SELinux?

Security Model

- Mandatory Access Control (MAC)
- Type Enforcement + RBAC + MLS
  - Least privilege
  - Enforces confidentiality and integrity
  - Strong isolation of applications
  - Information flow control
  - Limits exploitation of vulnerabilities
What is SELinux?

Community Project

- Originated in 1980s security research
- Academic research prototype (Flask) 1990s
- Ported to Linux, released under GPL in 2000
- Distro adoption, upstream merge, certification
- Adoption and innovation by users
Why SELinux?

- Existing MLS solutions:
  - Inflexible
  - Don’t meet general requirements
  - Hindered adoption
  - Niche products: expensive and weird
Why SELinux?

- Better security for general computing:
  - DAC is not enough
  - Need to protect against software flaws
  - Flexibility
  - Meet general requirements
  - Ubiquitous
SELinux Design

- Retrofit into existing OS
- System-wide policy
- Labeling of all security relevant objects
- Policy applied in the kernel (AVC)
Milestones

2000 – 2003

- GPL code release
- Kernel summit presentation
- LSM project
- Port SELinux to LSM
- Kernel 2.6 released Dec 03 with SELinux
- Early community efforts, including Debian Integration
Milestones

• 2004 – 2005
  - Fedora integration
  - Targeted policy
  - RHEL integration (commercially supported)
  - Foundation for viable production model
  - SELinux Symposium, growth of community
Milestones

● 2005 – present
  – Loadable policy modules
  – Reference policy
  – Booleans
  – Libraries
  – Tools
  – Setroubleshoot
  – SLIDE
Modern SELinux
Modern SELinux

Summary
SELinux is preventing the sshd (sshd_t) from binding to port 330.

Detailed Description
SELinux has denied the sshd from binding to a network port 330 which does not have an SELinux type associated with it. If sshd is supposed to be allowed to listen on this port, you can use the semanage command to add this port to a port type that sshd_t can bind to. semanage port -l will list all port types. Please file a bug report against the selinux-policy package. If sshd is not supposed to bind to this port, this could signal a intrusion attempt. If this system is running as an NIS Client, turning on the allow_ypbind boolean, may fix the problem. setsebool -P allow_ypbind=1.

Allowing Access
If you want to allow sshd to bind to this port semanage port -a -t PORT_TYPE -p PROTOCOL 330 Where PORT_TYPE is a type that sshd_t can bind and PROTOCOL is udp or tcp.

Additional Information
Source Context: unconfined_u:system_r:sshd_t:SystemLow-SystemHigh
Target Context: system_u:object_r:reserved_port_t
Target Objects: None [ tcp_socket ]
Source: sshd
Source Path: /usr/sbin/sshd
Port: 330
Host: e
Source RPM Packages: openssh-server-5.0p1-3.fc9

Audit Listener 7/7
Modern SELinux

Domain Access
This will help you create a domain for your module

Module: killerapp
Type: Application

This will help you create a new domain in your module that acts like a user runnable application.

- Label Executable
  - Type: killerapp_exec_t
  - Path: /usr/local/bin/killerapp

- Application has config file
  - Type: killerapp_config_t
  - Path: /etc/killerapp.conf

- Application has PID file
- Application has temporary file
- Application has log file
- Application accesses network
- Helper processes
SELinux Adoption

• Widely adopted in Fedora
  – Smolt statistics show majority have SELinux enabled.

• RHEL adoption by military, govt, finance:
  – Factor in NYSE/Euronext adoption, handling over $140 Billion/day in trades.
  – US Coast Guard Intelligence case study.

• Embedded / consumer electronics:
  – MicroSELinux
  – Many improvements from Japanese developers
Threat Mitigation

“A security framework originally published by the US National Security Agency has begun to rack up an impressive list of protections against security holes.”

– LinuxWorld, Feb 2008

• SELinux has mitigated several serious security threats to everyday users of Fedora & RHEL.

• Tracked @ Tresys Mitigation News
Current Work

• Wider distribution support:
  – Ubuntu, Debian, Gentoo

• Beyond kernel:
  – Virtualization (XSM)
  – Desktop (XACE)
  – Storage (LNFS)
  – Applications (Database etc.)

• Beyond Linux:
  – OpenSolaris FMAC
Cool Stuff

- Flexible design leads to innovative ideas
- Xguest
  - “Kiosk Mode”
  - Anonymous desktop session
  - Protect system from user
  - Utilizes “military” technologies for general use
  - Conferences, training, demos, library, child-proof...
- Russell Coker’s Play Machine
Challenges

- Improved usability, as always!
- Documentation
- Keep community growing
How to Participate

- Install SELinux enabled distribution
- Join mailing lists
- IRC
- Ask questions
- Answer questions!

See Resources page for links.
Resources

- Official Home Page
  - http://nsa.gov/selinux/
- Inevitibility of Failure Paper
- Tresys Mitigation News
- Community Project Server
  - http://selinuxproject.org/