

Update From SE Linux Symposium

Cyber Security Lab

Spring 2006

Topics from Symposium

- <http://www.selinux-symposium.org/2006/agenda.php>
- Core Technology
 - SE Linux in Mac OS X
- Policy Language
 - Improved language
 - Policy development
 - Meta Policy for accessing policy
 - Policy Analysis
- Applications
 - Application Firewall (brickwall)
 - Cross Domain Solutions
- New mechanisms
 - MLS, MCS
 - Polyinstantiated directories
 - Labeled printing

SE Linux in other OS's

- Presenter's company created a MAC framework analogous to the Linux Security Module (LSM)
- Port MAC framework to other OS's
 - SE Linux comes over very easily
- Targeting Free BSD and Mac OS X
 - Mac OS X built on Free BSD and Mach
 - Recycling much Trusted Mach work
 - Mach heavily uses IPC

Policy

- Lots of work on improving policy
- Replacing convention and M4 macros with real language
 - Need seen, multiple options proposed
- Eclipse IDE
- Extensions for meta-policy
 - Enable control over who can operate on different parts of policy

Policy Patterns

- Look for patterns in runtime traces
- Identify access enforcement points in application
 - Identify security sensitive operations
 - Run with operation and without operation
 - Calculate the different to get the pattern
- Aid user in creating policy
 - Application writer creates high level specification of application interactions
 - Polgen uses specification and trace to suggest patterns

Application Firewall

- With a regular firewall cannot differentiate between different processes on the same device
 - Cannot say httpd can read port 80 but vulserver cannot read port 80
- SE Linux allows labeling of network elements
 - Interfaces, ports, and addresses
- Can differentiate processes with SE Linux
 - Label port 80 with port80_t
 - allow httpd_t to read and write port80_t
- Tresys prototyped Brickwall
 - Present list of applications and services to configure

Cross Domain Solutions

- High assurance system that sits between a higher security system and a lower security network
 - Series of processes that analyzes and cleanses data to upgrade or downgrade
- Must ensure that data is fed into processes in correct order
 - Can use SE Linux to ensure
 - Must break into enough processes to reveal sufficient granularity to the domain type system.
- Problems with bidirectional communication
 - Data can flow backwards through the pipeline

MLS, MCS

- Dan Walsh was selling MCS as a means to get “normal people” to use the MLS mechanism
 - Broader testing
 - So security feature is not trailing feature
 - The MLS mechanism is enabled by default in FC5
- Targeted policy similarly brought type enforcement into the mainstream OS

Polyinstantiated Directory

- Problem of processes operating and multiple sensitivity levels and accessing common directory like /tmp
 - SystemHigh and SystemLow processes both create “random”
- Use linux kernel to unmap and remap portions of the file system namespace
 - /tmp/random maps to different physical locations for the two processes
- Hooked into PAM

Summary

- Lots of activity
 - Most interest in the government arena
 - RedHat's commitment is encouraging for broader adapting
- Next year
 - Policy language will evolve
 - Products will present SE Linux features for a specialized purpose