

New Zealand Linux Users Group

Security Enhanced Linux

Kerry Thompson,
Open Systems Specialists Ltd (OSS)



Introduction

- Kerry Thompson, CISSP
 - Open Systems Specialists Ltd
 - Open Systems & Networking Consultant
 - Specialist in IT Security
 - Contributor to SELinux project 2 years
 - Author of the (unofficial) SELinux FAQ

Presentation Overview

- History
 - What can it do for you?
 - Access Control Models : DAC and MAC
 - SELinux Access Controls in detail : TE, RBAC, MLS
 - File contexts and labelling
 - TE Rules
 - User identity
 - Installation
 - SELinux-aware applications and tools
 - Building policies for new applications
 - Future Directions
 - Demonstration (Hardened Gentoo)
-
-

SELinux History

- Released by NSA September, 2001
 - Based on previous research projects (FLASK and Flux OS)
 - Development from many .gov and .mil organisations
 - Integrated with Linux Security Module (LSM)
 - Adopted into 2.6 kernel series
 - To be released in Fedora Core2 as standard
-
-

The Importance of a Secure OS

- Stronger access controls required
 - The requirement for process separation
 - Vulnerability in one should not lead to compromise of all
 - Protection from malware
 - 3 core objectives for security:
 - Confidentiality
 - Integrity
 - Availability
-
-

Access Control Models 101

- Discretionary Access Control (DAC)
 - Classical Unix controls
 - Users can change security attributes at request
 - Allowing programs running on behalf of user to affect the results of access controls
 - Violates the least-privilege model
 - Mandatory Access Control (MAC)
 - Like firewall rules
 - Users cannot change security attributes at request
 - User programs must work within the constraints of access rules
 - MAC access rules are controlled by the security administrator
-
-

SELinux Access Controls

- Type Enforcement (TE) rules – which subjects can access which objects
 - Role-Based Access Control (RBAC) – which roles users can adopt and what they can do
 - Multi-Level Security (MLS) – confidential, secret, top-secret
 - Policy loaded into kernel
 - Fully compatible with existing software
 - Insignificant security overhead
-
-

File Contexts and Labelling

- All files (objects) are assigned security contexts
 - eg. (/etc/shadow)
system_u:sysadm_r:shadow_t
 - Rulebase to define types for all files in Linux system (regular expressions)
 - Labelling process to read labelling rules and apply to whole system
 - Fine-grained commands to change individual labels
 - chcon, getfilecon, setfilecon
 - Be careful with backup and recovery
-
-

Processes and Domains

- A process running with a specific security context is said to be running within a domain
 - eg. `system_u:system_r:named_t`
- Rules are configured to:
 - Specify which objects a domain can access, and how
 - Specify which roles a domain can transition to



Type Enforcement (TE) Rules

- Clearly define which subjects can access which objects, and how
 - eg. allow user_t bin_t : file { read execute };
 - Define domain transitions
 - Very flexible and detailed
 - Can be very large and complex : tens of thousands of rules is not uncommon
 - Current default rulebase : 1,000 types, 18,000 allow rules, 1,000 type transitions
 - Complexity can be difficult to audit
 - Written in plain text, processed by the m4 macro processor, loaded by checkpolicy
-
-

TE Rules (continued)

Example : named.te

```
allow named_t etc_t:file { getattr read };
allow named_t etc_runtime_t:{ file lnk_file } { getattr read };
allow named_t resolv_conf_t:file { getattr read };

#Named can use network
can_network(named_t)
# allow UDP transfer to/from any program
can_udp_send(domain, named_t)
can_udp_send(named_t, domain)
can_tcp_connect(domain, named_t)

# Bind to the named port.
allow named_t named_port_t:udp_socket name_bind;
allow named_t { named_port_t rndc_port_t }:tcp_socket name_bind;

#read configuration files
r_dir_file(named_t, named_conf_t)

#read zone files - change this to rw_dir_create_file() to
# enable domain auto updates.
r_dir_file(named_t, named_zone_t)
```

User identity

- User processes (such as the login shell) are placed into a domain by the login, sshd programs when the user logs in
 - The user identity does not change, even when the uid changes
 - Users can switch to other roles using the newrole command
 - RBAC conforms to least privilege principle
-
-

SELinux Installation 1

- Easy way : Fedora Core 2 (yet to come)
- Hard way : start with a recent distribution
 - Fedora Core 1
 - Debian
- Update to 2.6 kernel, with Extended Attributes & test
- Build SELinux-enabled kernel
 - Enable NSA SELinux extensions
 - With DEVELOPMENT flag set

SELinux Installation 2

- Load SELinux base tools
 - Load SELinux policy
 - Load SELinux user packages (not mandatory, but strongly advised)
 - Load policy into kernel
 - Run full filesystem relabel
 - Reboot! (into permissive mode)
 - Check messages and start
 - Switch to enforcing mode
-
-

SELinux-aware Applications

- Many basic Linux commands have been modified to be SELinux-aware
 - login, ls, ps, id, cron
 - Other applications patched for SELinux
 - OpenSSH
 - Additional commands added to perform SELinux functions
 - chcon, run_init, etc.
 - Tresys GUI tools for managing policies
-
-

Building new policies for Applications

- Assign types and file labels
- Run in permissive mode, collect log output
- Use audit2allow utility to generate rules from avc messages
- Add rules to rulebase
- Refer to Faye Coker's HOWTO develop security policies



Getting Help

- FAQs, HOWTOs, White papers
- Mailing List (on NSA site)
- NSA site : <http://www.nsa.gov/selinux>
- Kerry's resources :
<http://www.crypt.gen.nz/selinux>

Caveats

- Lack of documentation
- An additional level of complexity
- Backup and recovery can be difficult
- Potential for unbootable/unrecoverable filesystems
- Need to write policies for new Apps

... but on the other hand

- Less need to continually update security fixes
- More security in depth, less dependance on perimeter & firewalls



Future Directions

- Conditional policy extensions
- Security Enhanced X-Windows (SE-X)
- Auditing extensions
- Policy Management Tools



SELinux - Questions?

Demonstration : Hardened Gentoo LiveCD

