Assurance: SELinux Executive Overview

Chris Runge
Agenda

- System security in an insecure world
- Red Hat Enterprise Linux security features
- An overview of Discretionary Access Control and Mandatory Access Control
- What is Security-Enhanced Linux?
- Security-Enhanced Linux in Red Hat Enterprise Linux 4
- Security-Enhanced Linux in Red Hat Enterprise Linux 5
- Additional resources
System security in an insecure world

- What are crackers after?
  - Resources for sending bulk email
  - Personal information—credit card numbers and identity theft
  - Classified secrets and trade secrets
  - Any other information or resources of value
- Authorized users can be just as dangerous
- 0 Day Exploits
- New challenges forced by regulatory compliance
  - Sarbanes-Oxley
  - HIPAA
Red Hat Enterprise Linux Security Features (non-SELinux)

- Modular OS architecture
- Built-in firewall
- Kickstart %post
- Support for No eXecute (NX) and eXecute Disable (XD) technologies
- Exec-Shield
- Position Independent Executables (PIE)
- GCC and GLIBC enhancements
- New audit subsystem
Discretionary Access Control

- Model used by most operating systems
- Users have control (discretion) over their files and programs
- Programs run as a user have that user's privileges
- Root/superuser has complete control
- Attacker's goal is to exploit program running with root privileges
Mandatory Access Control

- Secure applications require a secure OS
- Security policy is the final arbiter of all access decisions; users cannot override the policy
- Supplements DAC
- Multiple models: Type Enforcement, RBAC, Multi-Level Security
- Benefits: integrity and/or confidentiality
What is Security-Enhanced Linux?

- Security-Enhanced Linux – Strong, flexible MAC architecture
  - Flask architecture allows for alternative security policies and models
- Initially a research prototype out of NSA; now part of the upstream Linux 2.6 kernel
- Growing community of use and development
  - SELinux Symposium
- Available in a number of Linux distributions
  - Added to Fedora in FC2; Red Hat Enterprise Linux in RHEL 4
- Initial focus on Type Enforcement (TE)
  - Principle of least privilege
SELinux Web Server Example

• Basic example SELinux httpd policy
  - Listen on port 80 on eth1
  - Read /etc/httpd/httpd.conf
  - Read/append /var/log/httpd/*
  - Read /var/www/html/*

• Successful attacker is limited to these actions
SELinux in Red Hat Enterprise Linux 4

• Fully integrated into Red Hat Enterprise Linux 4
  - Benefits of MAC in a modern, mainstream operating system
  - Not a separate set of extensions or a completely separate OS
• Provides Type Enforcement (TE)
  - Flexible policy model
    • Map security policy to operational and functionality requirements
  - Example applications
    • Lock down web servers, DNS servers, and other network-listening services
    • Cross Domain Solutions (guards)
SELinux in Red Hat Enterprise Linux 4

- Default targeted policy – isolate commonly attacked, network-listening services
  - e.g., Apache, BIND, portmap, NTP, etc.
  - By default, enabled in enforcing mode
  - Useful compromise between enhanced security while not overly impacting functionality
- Optional strict policy – locks down additional applications and user privileges
Multi-Level Security (MLS)

- Some critical scenarios in the military and intelligence community require Multi-Level Security (MLS)
- Formerly the exclusive province of expensive, niche “trusted” operating systems
- Bell-LaPadula (BLP) model
  - Focus is on confidentiality
  - Ensures users and programs on a system can only access resources for which they have been appropriately cleared
  - Maintains the separation between different sensitivity (Top Secret, Secret, Confidential, Unclassified) and categorization levels
  - “No read up; no write down”
Multi-Category Security (MCS)

- MCS = MLS with a single sensitivity level
- Goal: prevent accidental leakage by the user of confidential documents, etc.
- User-focused, discretionary scheme
- Analogous to the targeted policy; extend the benefits of preserving confidentiality to a wider audience
- Uses many of the same code paths as MLS
- Available today in Fedora Core 5
SELinux in Red Hat Enterprise Linux 5

- Red Hat Enterprise Linux 5 will include support for MLS and MCS
  - SELinux will be used as the foundation
  - Capabilities preview in Fedora Core 5, available today
- Retain flexibility and choice
  - One OS, rather than multiple, can be used for a variety of roles
  - Available policy models
    - Targeted with MCS (selinux-policy-targeted)
    - Strict with MCS (selinux-policy-strict)
    - Strict with MLS (selinux-policy-mls)
      - No separate “trusted” version
      - Common Criteria EAL4+/CAPP/LSPP/RBACPP
Additional Resources

• Red Hat Global Learning Services
  - https://www.redhat.com/training/
  - RHS427 Introduction to SELinux and Red Hat Targeted Policy
  - RHS429 Red Hat Enterprise SELinux Policy Administration

• Whitepapers
  - Red Hat Enterprise Linux 4 Security Features
  - The Path to Multi-Level Security in Red Hat Enterprise Linux

• Mailing List
  - https://www.redhat.com/mailman/listinfo/redhat-lspp