

Open Source Software Development Series

SELinux

by Example

Using Security Enhanced Linux

FRANK MAYER
KARL MACMILLAN
DAVID CAPLAN

SELinux by Example

SELinux by Example: Using Security Enhanced Linux

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents

Part I: SELinux Overview

Chapter 1 Background

1.1 The Inevitability of Software Failure

1.2 The Evolution of Access Control Security in Operating Systems

1.3 Summary

Exercises

Chapter 2 Concepts

2.1 Security Contexts for Type Enforcement

2.2 Type Enforcement Access Control

2.3 The Role of Roles

2.4 Multilevel Security in SELinux

2.5 SELinux Features Familiarization

2.6 Summary

Exercises

Chapter 3 Architecture

3.1 The Kernel Architecture

3.2 Userspace Object Managers

Table of Contents

3.3 SELinux Policy Language

3.4 Summary

Exercises

Part II: SELinux Policy Language

Chapter 4 Object Classes and Permissions

4.1 Purpose of Object Classes in SELinux

4.2 Defining Object Classes in SELinux Policy

4.3 Available Object Classes

4.4 Object Class Permission Examples

4.5 Exploring Object Classes with Apol

4.6 Summary

Exercises

Chapter 5 Type Enforcement

5.1 Type Enforcement

5.2 Types, Attributes, and Aliases

5.3 Access Vector Rules

5.4 Type Rules

5.5 Exploring Type Enforcement Rules with Apol

5.6 Summary

Exercises

Chapter 6 Roles and Users

6.1 Role-Based Access Control in SELinux

6.2 Roles and Role Statements

6.3 Users and User Statements

6.4 Exploring Roles and Users with Apol

6.5 Summary

Exercises

Chapter 7 Constraints

Table of Contents

7.1 A Closer Look at the Access Decision Algorithm

7.2 Constrain Statement

7.3 Label Transition Constraints

7.4 Summary

Exercises

Chapter 8 Multilevel Security

8.1 Multilevel Security Constraints

8.2 Security Contexts with MLS

8.3 MLS Constraints

8.4 Other Impacts of MLS

8.5 Summary

Exercises

Chapter 9 Conditional Policies

9.1 Overview of Conditional Policies

9.2 Boolean Variables

9.3 Conditional Statements

9.4 Examining Booleans and Conditional Policies with Apol

9.5 Summary

Exercises

Chapter 10 Object Labeling

10.1 Introduction to Object Labeling

10.2 File-Related Object Labeling

10.3 Network and Socket Object Labeling

10.4 System V IPC

10.5 Miscellaneous Object Labeling

10.6 Initial Security Identifiers

10.7 Exploring Object Labeling with Apol

10.8 Summary

Exercises

Table of Contents

Part III: Creating and Writing SELinux Security Policies

Chapter 11 Original Example Policy

11.1 Methods for Managing the Build Process

11.2 Strict Example Policy

11.3 Targeted Example Policy

11.4 Summary

Exercises

Chapter 12 Reference Policy

12.1 Goals of the Reference Policy

12.2 Overview of Policy Source File Structure

12.3 Design Principles

12.4 Examining a Reference Policy Module

12.5 Build Options for Reference Policy

12.6 Summary

Exercises

Chapter 13 Managing an SELinux System

13.1 SELinux Configuration and Policy Management Files

13.2 Impact of SELinux on System Administration

13.3 Summary

Exercises

Chapter 14 Writing Policy Modules

14.1 Overview of Writing a Policy Module

14.2 Preparation and Planning

14.3 Creating an Initial Policy Module

14.4 Testing and Analyzing the Policy

14.5 Emerging Policy Development Tools

14.6 Complete IRC Daemon Module Listings

14.7 Summary

Table of Contents

Appendix A: Obtaining SELinux Sample Policies

A.1 Example Policy

A.1.1 Example Policy from Upstream SELinux Sites

A.1.2 Strict and Targeted Policies for Fedora Core 4

A.1.3 Red Hat Enterprise Linux 4 (RHEL4)

A.1.4 Fedora Core Experimental and Test Policies

A.2 Reference Policy

A.2.1 Primary Reference Policy

A.2.2 Red Hats Fedora Core 5 Reference Policy

Appendix B: Participation and Further Information

B.1 The SELinux Mail List

B.2 The Annual SELinux Symposium

B.3 The NSA

B.4 Tresys Technology

B.5 Open Source Projects

B.6 The SELinux IRC Channel

B.7 The Fedora Core Site

B.8 Hardened Gentoo

B.9 Other Related Security Information

Appendix C: Object Classes and Permissions

C.1 Common Permission Sets

C.2 Object Classes and Defined Permission Sets

C.2.1 File-Related Object Classes

C.2.2 Network and Socket Object Classes

C.2.3 System V IPC-Related Object Classes

C.2.4 Miscellaneous Object Classes

Appendix D: SELinux Commands and Utilities

Table of Contents

D.1 System Utilities

D.1.1 Policy Tools

D.1.2 SELinux Status Information

D.1.3 Security Context Labeling

D.1.4 Security Context Changing Utilities

D.1.5 SELinux Modified Commands

D.1.6 Policy Module Manual Pages

D.2 SETools Suite

D.3 Other SELinux Tools

Index