Securing the networking system using Linux Security Modules

Index terms: security
Keywords: Linux Security Modules, networking system
Team size: 2

1. Project theme

Linux Security Modules is a lightweight access control framework developed for the Linux kernel that is used to create loadable kernel modules that implement various access control mechanisms. LSM provides a set of network hooks in the socket layer and additional fine-grained hooks for IPv4, Unix domain and Netlink protocols.

The project implements a security application that uses Linux Security Modules API to enforce Mandatory Access Control to the networking system applications. The security application consists in a loadable kernel module that is able to restrict any operation with sockets and packets.

2. Objectives

This project aims to implement a software application that will meet the following requirements:

- The security application for the networking system should be implemented in a loadable kernel module
- The kernel module should use Linux Security Modules API to access networking hooks
- The security module should use the socket-related hooks in order to manage socket operations
- The security field introduced by LSM in packets should be used to manage security across the network and per-packet
- Netfilter hooks should be used to filter packets, decode options, and manage fragments and encapsulation.
- A configuration file should be used as the method to configure the security application

3. Bibliography

[1] C. Wright, C. Cowan, J. Morris, S. Smalley, and G. Kroah-Hartman, "Linux security modules: general security support for the linux kernel", *Foundations of Intrusion Tolerant Systems, 2003 [Organically Assured and Survivable Information Systems]*, 2003, pp. 213-226.

[2] C. Wright, C. Cowan, J. Morris, S. Smalley, and G. Kroah, "Linux security module framework", *Ottawa Linux Symposium*, vol. 8032, 2002.

4. Prerequisites

Networking, security, kernel programming.