NetLabel Introduction

Paul Moore, paul.moore@hp.com

August 2, 2006

Overview

NetLabel is a mechanism which can be used by kernel security modules to attach security attributes to outgoing network packets generated from user space applications and read security attributes from incoming network packets. It is composed of three main components, the protocol engines, the communication layer, and the kernel security module API.

Protocol Engines

The protocol engines are responsible for both applying and retrieving the network packet's security attributes. If any translation between the network security attributes and those on the host are required then the protocol engine will handle those tasks as well. Other kernel subsystems should refrain from calling the protocol engines directly, instead they should use the NetLabel kernel security module API described below.

Detailed information about each NetLabel protocol engine can be found in this directory.

Communication Layer

The communication layer exists to allow NetLabel configuration and monitoring from user space. The NetLabel communication layer uses a message based protocol built on top of the Generic NETLINK transport mechanism. The exact formatting of these NetLabel messages as well as the Generic NETLINK family names can be found in the 'net/netlabel/' directory as comments in the header files as well as in 'include/net/netlabel.h'.

Security Module API

The purpose of the NetLabel security module API is to provide a protocol independent interface to the underlying NetLabel protocol engines. In addition to protocol independence, the security module API is designed to be completely LSM independent which should allow multiple LSMs to leverage the same code base.

Detailed information about the NetLabel security module API can be found in the 'include/net/netlabel.h' header file as well as the 'lsm_interface.txt' file found in this directory.