NetLabel

Netconf 2006
Tokyo

Paul Moore
paul.moore@hp.com

Agenda

- Introduction
- Design goals
- Architectural overview
- Initial implementation
- SELinux support
- Future ideas

Introduction

- Growing number of Trusted OS users want to shift from legacy Trusted OSes to Linux
  - Requires labeling of all user generated traffic
  - Requires interoperability with legacy labeling protocols
  - Wants labels that are understandable on the wire
- Unfortunately the IPsec SA labeling mechanism does not satisfy all of these requirements

Design Goals

- Protocols must be supported by existing Trusted OSes
  - CIPSO, RIPSO, TSIX/MAXSIX
- Implementation must be well contained
  - Use existing LSM hooks and data structures
- Performance impact must be minimal
  - Zero impact when not enabled at compilation
  - Minimal impact when enabled but not configured

Architectural Overview

- Utilize existing SKB receive and socket syscall LSM hooks
  - Outbound packets are labeled by adding an IP option to the socket
  - Inbound packet IP options are parsed/validated as part of normal option processing
  - Access control handled in the LSM
- Management is handled through the Generic Netlink interface
- Implementation is LSM agnostic

Initial Implementation

- Provides minimal CIPSO support
  - Limited to labeling packets with the MLS label
  - Configuration parameters not explicitly supported
  - Implementation is limited to MUST support
- Supports multiple CIPSO DOIs and unlabeled traffic
  - Type of outbound labeling can be defined on a per-LSM-domain basis
  - No requirements are placed on the CIPSO DOIs used for incoming traffic

SELinux Support

- Sockets are assigned IP options/labels based on their context
  - If unable to set the IP option then socket creation is denied or writes are not allowed
- Sockets created by incoming connections are labeled according to the connection
  - New context is a combination of the parent socket’s SELinux context and the connection’s MLS label
- Context of incoming traffic is generated similar to incoming TCP connections

Future Ideas

- Provide better CIPSO support
  - The remaining tag types
  - CIPSO/IPv6 as used by Trusted Solaris
- Investigate support for other labeling protocols such as RIPSO, TSIX/MAXSIX
- Implement support for sending full SELinux contexts
- General improvements, etc

More Information

- Kernel patches in net-2.6.19
- SourceForge project started to hold userspace utilities
  - http://netlabel.sf.net