NetLabel CIPSO/IPv4 Protocol Engine

Paul Moore, paul.moore@hp.com

May 17, 2006

* Overview

The NetLabel CIPSO/IPv4 protocol engine is based on the IETF Commercial IP Security Option (CIPSO) draft from July 16, 1992. A copy of this draft can be found in this directory, consult '00-INDEX' for the filename. While the IETF draft never made it to an RFC standard it has become a de-facto standard for labeled networking and is used in many trusted operating systems.

* Outbound Packet Processing

The CIPSO/IPv4 protocol engine applies the CIPSO IP option to packets by adding the CIPSO label to the socket. This causes all packets leaving the system through the socket to have the CIPSO IP option applied. The socket's CIPSO label can be changed at any point in time, however, it is recommended that it is set upon the socket's creation. The LSM can set the socket's CIPSO label by using the NetLabel security module API; if the NetLabel "domain" is configured to use CIPSO for packet labeling then a CIPSO IP option will be generated and attached to the socket.

* Inbound Packet Processing

The CIPSO/IPv4 protocol engine validates every CIPSO IP option it finds at the IP layer without any special handling required by the LSM. However, in order to decode and translate the CIPSO label on the packet the LSM must use the NetLabel security module API to extract the security attributes of the packet. This is typically done at the socket layer using the 'socket_sock_rcv_skb()' LSM hook.

* Label Translation

The CIPSO/IPv4 protocol engine contains a mechanism to translate CIPSO security attributes such as sensitivity level and category to values which are appropriate for the host. These mappings are defined as part of a CIPSO Domain Of Interpretation (DOI) definition and are configured through the NetLabel user space communication layer. Each DOI definition can have a different security attribute mapping table.

* Label Translation Cache

The NetLabel system provides a framework for caching security attribute mappings from the network labels to the corresponding LSM identifiers. The CIPSO/IPv4 protocol engine supports this caching mechanism.