Architecture of SELinux Network Access Controls

SELinux Symposium 2005

James Morris
Red Hat, Inc.
jmorris@redhat.com

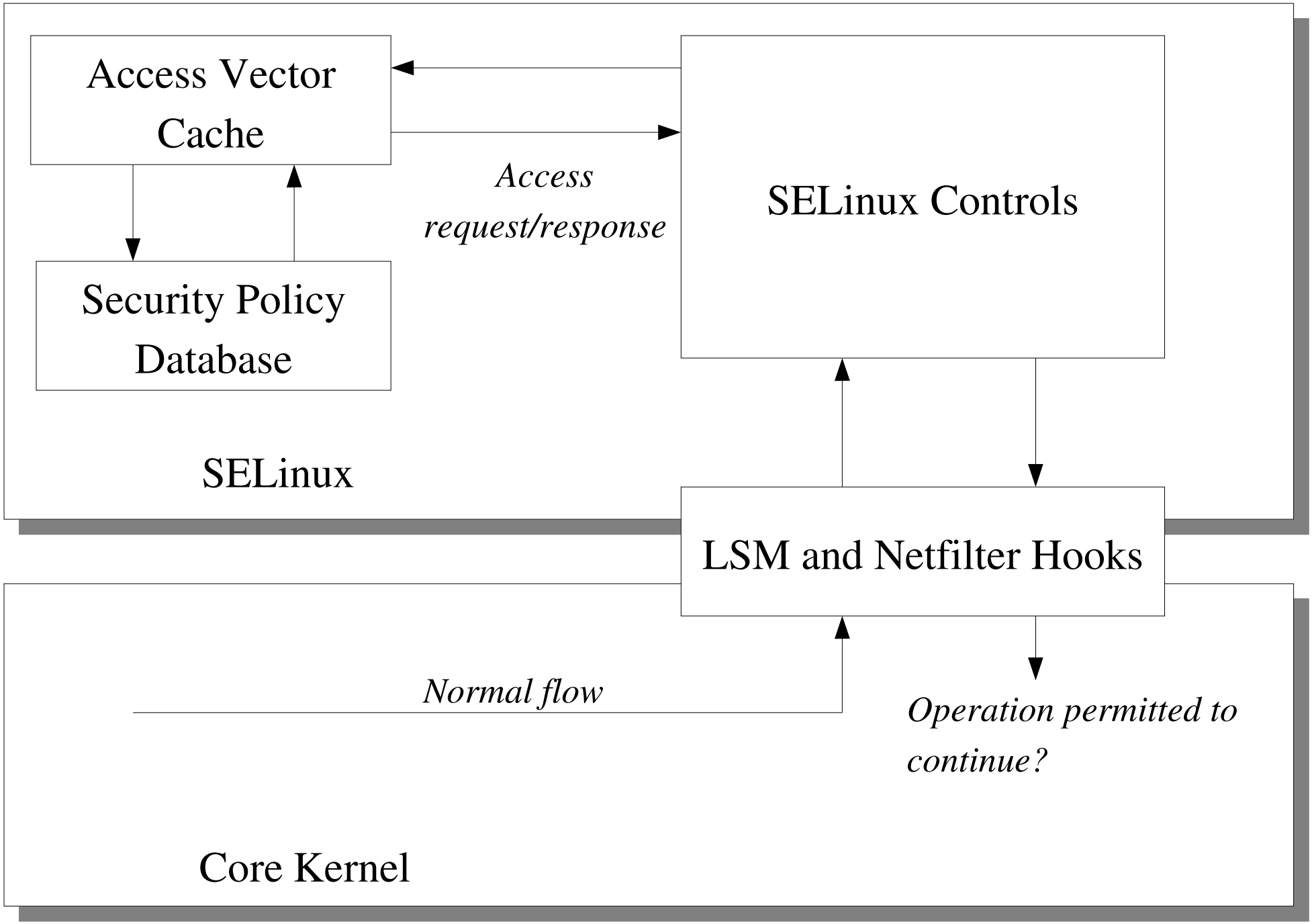
Introduction

- Network access controls under SELinux follow the same general model as other SELinux controls:
  - Security labeling of objects and subjects at the kernel level.
  - Mediating access to objects according to security policy.

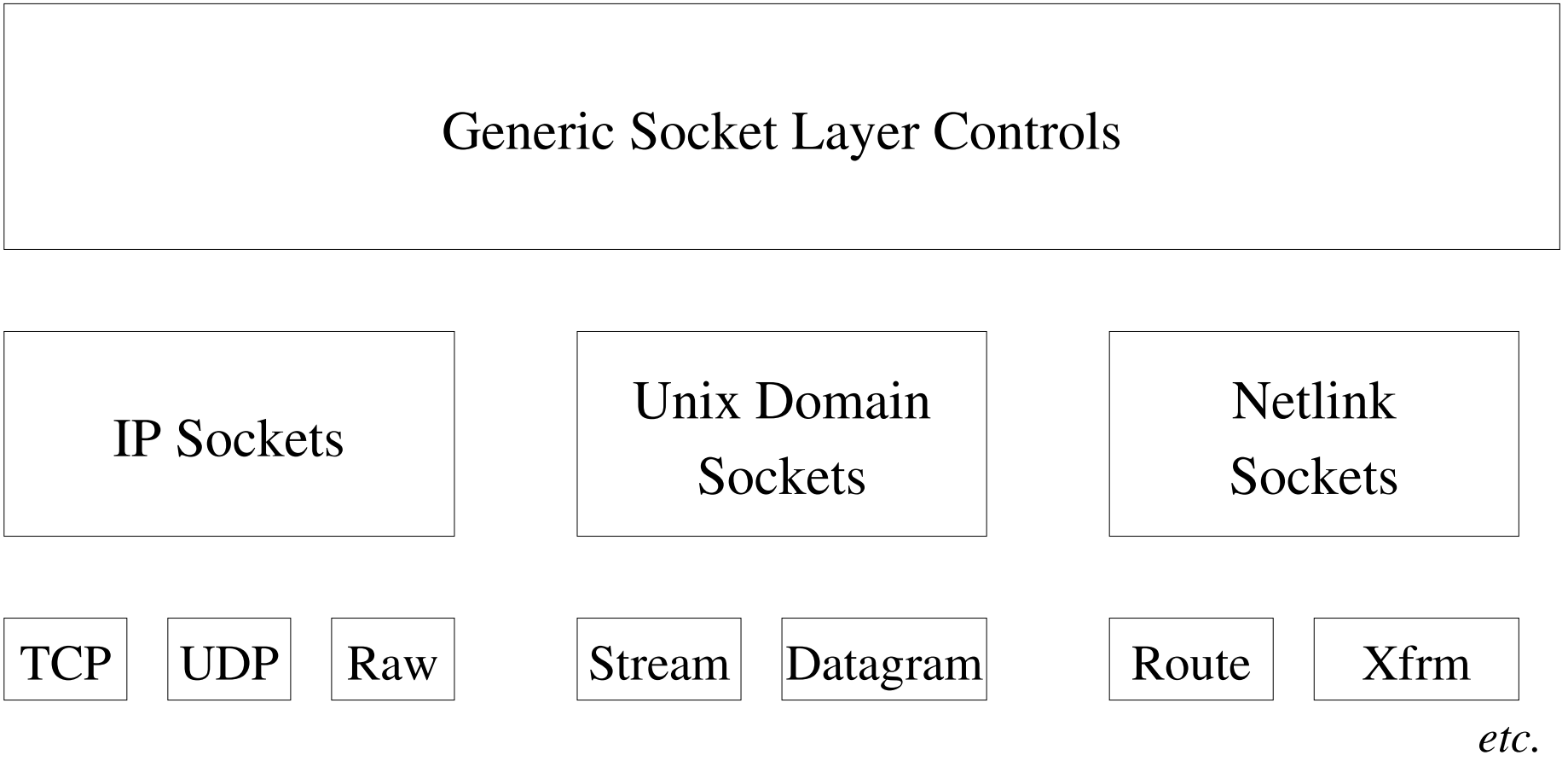
Network Objects

- Network objects labeled by SELinux
  - Sockets.
  - Ports.
  - “Nodes”, i.e. IP address/mask.
  - Network interfaces (netifs).

Kernel Architecture



Network Control Hierarchy



- SELinux socket objects are subclassed.
- Permissions selectively applied to classes.
- Class specific controls.

IPv4 and IPv6 Controls (1)

- Extending the generic bind(2) control:
  - *node_bind* permission extends a generic *bind* permission for sockets binding to types of nodes.
  - *name_bind* controls whether a socket can bind to a type of port, if the port number falls outside the ephemeral port range.

IPv4 and IPv6 Controls (2)

- Mediation of IP traffic flow based on IP packet attributes:
  - Network interface
  - Node
  - Port

Unix Domain Networking

- Interesting for SELinux as it is used for local IPC.
- Mediation between sockets in the Linux abstract namespace.
- Mediate directionality of Unix communication.
- SO_PEERSEC socket option, analogous to SO_PEERCRED authentication.

Netlink Sockets

- Netlink sockets are a userspace-kernel communication system.
- Logically divided into “families”, such as NETLINK_ROUTE and NETLINK_XFRM.
- SELinux subclasses socket types for each of these, to allow differentiation between families.
- Also able to differentiate between read and write operations. e.g. Routing table view vs. update.

Labeled Networking

- Network packets are sent over the network with labels attached.
- Typical use is MLS networking using CIPSO (IP option) labels.
- Current status: not supported. Selopt code dropped during upstream LSM merge.
- Alternative is implicit labeling via IPSec. (See Trent Jaeger's talk).

Issues & Future Directions

- Network performance tuning.
- Possibly integrate with iptables.
- MLS networking (also see Chad Hanson's talk).
- Clustering.
- NFS.

Questions?

Resources

- Linux Journal SELinux Networking Article
  - http://www.intercode.com.au/jmorris/selinux-networking-lj.html
- Selopt
  - http://www.intercode.com.au/jmorris/selopt/
- Implementing Mandatory Network Security in a Policy-flexible System, Ajaya Chitturi, 1998.
  - http://www.cs.utah.edu/flux/papers/ajay-thesis-abs.html