Directions in SELinux Networking

Linux Kernel Networking Summit

Montréal, Canada

July 2005

James Morris <jmorris@redhat.com>

SELinux

- SELinux provides fine-grained, flexible MAC.
- Subjects and objects are labeled with security contexts, policy determines interactions.
- Type Enforcement (TE) model provides an expressive abstraction of security classes and their interactions.

Current Status

- SELinux provides broad coverage across the kernel (140 hooks).
- All socketcalls are mediated, provides high level control over local networking.
- Protocol specific controls for Netlink, Unix, some IP (name_bind, name_connect, rudimentary packet filter).

Networking Directions

- Performance of IP network controls needs to be improved.
- Hit by per-packet lookups for security context of port and IP addresses.
- IBM did some work on an RCU cache, needs further investigation.
- May be replacing IP packet hooks anyway.

Netfilter/iptables

- Possibly replace existing IP packet controls with Netfilter/iptables integration (selipt).
- More flexible & expressive, makes use of conntrack, matches, targets etc.
- Need receiving socket: current code uses ipt_owner patch.
- Better to use socket hook work from Patrick McHardy.

Distributed MAC

- MAC is currently limited to the local machine.
- Historically used with Multi-Level Security (MLS).
- Typically, each packet is labeled via IP options (CIPSO, FIPS-188).
- Selopt implemented, dropped for upstream merge.

Leveraging IPsec

- Trent Jaeger's implicit labeling work (IBM).
- Label SAs instead of packets.
- Draws on previous Flask work.
- Not MLS or even SELinux specific.
- Utilizes IPsec services: confidentiality; authentication; negotiation; automation.

Leveraging IPsec II

- Hooks into xfrm subsystem.
- IPsec policies are labeled: only authorized policies may be used, controlled via SELinux.
- SA labels must match (existing SA or triggered negotiation with IKE).
- Matching packets considered labeled.
- Policy for unlabeled packets (e.g. ISAKMP).

Leveraging IPsec III

- Useful for MLS networking, suitable for LSPP (B1) and beyond.
- Not compatible with IP options schemes.
- More generally useful for extending SELinux across the network.
- Control communication between processes on different systems.

Networked Filesystems

- NSA developed support for NFSv3.
- Future is NFSv4 with named attributes.
- SMB desired by some parties.
- Cluster Filesystems (some OCFS2 work).

Remote Attestation

- Use of TPM and associated hardware to cryptographically verify system from boot.
- IBM Integrity Measurement Architecture (IMA).
- Requires protocol which queries TPM with nonce; TPM signs measurement list and nonce.
- SELinux policy could be used to require that the remote system is attested before some other communication.

Cryptographic Policy

- SELinux policy could be extended to express more general cryptographic policy.
- e.g. foo_t file must be stored with X encryption, and only transmitted by local admin_t to remote admin_t on trusted hosts with Y encryption and Z authentication on the wire.
- May also require use of specific crypto device or software.

Distributed Policy

- Mechanism for distributing and synchronizing policy within a security realm may be useful when using distributed MAC.

Longer Term

- General trend toward increasingly high assurance distributed computing.
- Inter-realm communication. Establishing trust between different “domains of interpretation” is very difficult.
- SE aware firewalling, complicated by Ipsec.

Resources

- SELinux Enhanced IPTables
  http://people.redhat.com/jmorris/selinux/selipt/
- “Architecture of SELinux Network Access Controls”
  http://www.selinux-symposium.org/2005/presentations/session2/2-2-morris.pdf
- “Leveraging IPSec for network access control for SELinux”
  http://www.selinux-symposium.org/2005/presentations/session2/2-3-jaeger.pdf
- Full IBM research report on the above (and more generalized).
  Not yet published
- Ajaya Chitturi's Flask Thesis
  http://www.cs.utah.edu/flux/papers/ajay-thesis-abs.html