Mandatory Access Control
Networking Update

Netconf 2006
Tokyo

James Morris
jmorris@namei.org
MAC Networking

• Applying Mandatory Access Control (MAC) security to networking:
  1) Local communications
     • Unix Domain
     • Netlink etc.
  2) Local labeling of network packets & objects
     • Packet filtering
  3) Distributed MAC
     • Labeled networking
Status – since last year

- SELinux packet filtering controls have been re-implemented with Secmark:
  - Utilizes IPTables, conntrack etc.
  - Separates labeling and enforcement
  - Much more powerful & flexible
  - Policy is greatly simplified
Status (cont'd)

• Native IPSec/xfrm labeling extended by TCS to provide full support for LSPP (used to be B1) certification.
  - Implements Multilevel Security (MLS), but is generic.
Status (cont'd)

- Support for legacy MLS networking added by HP ("Netlabel"):  
  - CIPSO
    - case 0x86: /* Another "Commercial Security" crap. */
    + case IPOPT_CIPSO:

  - RIPSO and others possible

- Provides interoperability with legacy MLS systems such as Trusted Solaris.

- Argus also porting their CIPSO implementation.
Futures

• Consolidation of labeling schemes (TCS has posted patches), so they all work well together.

• Complete LSPP/EAL4+ certification with RHEL5, which will include SELinux and native labeled networking.

• Look for ways to make labeled networking more generally useful (using Type Enforcement)
  - Example: protected paths between web server and database server processes.
Conclusions

• While immediately most useful to government & military users, the MAC networking frameworks have been implemented generically.

• These features are unprecedented in a general purpose OS.

• Linux now has perhaps the richest network security feature set ever.