State of SELinux Labeled Networking

Paul Moore

paul.moore@hp.com

SELinux Labeled Networking

- The past year
  - Peer label consolidation
  - Fallback peer labeling
  - Traffic ingress/egress controls
  - Dynamic network access controls
- The next year (hopefully)
  - NetLabel address selectors
  - Loopback labeling that works

The Past Year (aka 2.6.25)

Peer Label Consolidation

- Consolidated NetLabel and Labeled IPsec access controls
  - Reconciliation of labels from both subsystems
    - Traffic is dropped when labels are not equivalent
  - Introduction of the *peer* object class
    - SELinux policy no longer needs to be subsystem specific
  - Subsystems share a single access check
    - Less maintenance costs and per-packet overhead
- Backwards compatible with older SELinux policy
  - Utilizes *network_peer_controls* policy capability to conditionally enable access controls

Fallback Peer Labeling

- Peer labels without labeling protocol support
  - Labels assigned based on IP source address
    - Support for both networks and individual nodes
  - Assigns peer labels to conventional systems
    - Windows, Mac OS, ordinary Linux systems, etc.
- Utilizes the NetLabel framework
  - Fallback labels only assigned when peer label information is not present
    - CIPSO and Labeled IPsec override the fallback label
  - Support provided in *netlabel_tools* version 0.18
    - RH/Fedora bugzilla #439833

Traffic Ingress/Egress Controls

- SELinux access controls for all network traffic
  - Access controls for local and forwarded traffic
    - Access controls for the network interface and address
  - Separate permissions for local and forwarded traffic
- Interface controls provide increased assurance
  - Peer labels on network traffic can be compared with the label of the physical interface
- Backwards compatible with older SELinux policy
  - Utilizes *network_peer_controls* policy capability to conditionally enable access controls

Dynamic Network Access Controls

- Enables access controls based on configuration
  - Access controls are only executed when labeled networking has been configured to label traffic
  - Reduces performance impact of network access controls on common configurations
- Requires current policy and configuration
  - *compat_net* disabled
    - Migrate to iptables/secmark based labeling
  - *network_peer_controls* policy capability
    - Currently disabled in SELinux Reference Policy

The Coming Year

(aka 2.6.28?)

NetLabel Address Selectors

- Allow labeling based on the traffic destination
  - Apply NetLabel labeling based on domain and traffic's destination address
    - Supports both local and forwarded traffic
  - Works with existing domain based labeling
    - Different configuration type can be used for each domain
- Work in progress
  - Initial kernel development is almost complete
    - Kernel boots but new features are untested
  - Changes to *netlabel_tools* required
    - Not started
  - Targeting kernel 2.6.28

Loopback Labeling That Works

- Current solutions are problematic
  - NetLabel/CIPSO limited to MLS attributes
  - Labeled IPsec is difficult to get working and slow
- Extend CIPSO to support full SELinux contexts
  - Transfer the SELinux kernel SID in a CIPSO tag
    - Non-standard but okay for loopback
- Work in progress
  - Depends on NetLabel address selector effort
    - Requires the ability to target specific localhost addresses
  - Significant policy concerns when enabled
    - Can client_t talk to server_t?

More Information

- NetLabel Website

  http://netlabel.sourceforge.net

- SELinux Wiki

  http://selinuxproject.org

- My Email

  paul.moore@hp.com

- My Blog

  http://paulmoore.livejournal.com

invent