# Meeting Government Security Goals With SELinux

Karl MacMillan <kmacmillan@tresys.com>

© 2008 Tresys Technology

# Introduction to CLIP

- Linux with SELinux is a compelling platform
  - Offers appropriate security mechanisms
  - Reasonable assurance level w/ CC evaluation
  - Rich and approachable development platform
- Meeting government requirements is challenging
  - Technically – default configuration not suitable
  - Historically – open source, no “Trusted” variant, unfamiliar
  - Documentation – certification requires complex evidence
- Certifiable Linux Integration Platform (CLIP)
  - Linux platform to build government solutions
  - Eases certification of Linux systems

# CLIP Overview

- Configurations of Enterprise Linux Distributions
  - Designed to meet various security standards
    - DCID 6/3 PL4, DoD 8500.2, DISA Stigs, etc.
  - Includes certification evidence and other documentation
  - Open source: http://oss.tresys.com/projects/clip
  - Current versions available for RHEL 4 and 5
  - Distributed as RPMs, kickstart files, scripts
  - Configuration spans all security functions
    - SELinux, DAC, audit, integrity measurement, PAM, iptables, network configuration, etc.
- Maps requirements to security functions
  - Documents how Linux meets requirements
  - Includes optional configurations (e.g., MLS vs. MCS)

# Lessons Learned from CLIP

- MLS is often unnecessary
  - Very few true multi-level systems exist
  - Result of network based separation
  - CDS often only have a few “levels”
  - TE usually a better alternative
- Large overlap among security requirements
  - Possible to meet many requirements w/ single config
- Many requirements open to interpretation
  - Imperative to understand “typical” interpretation
  - STIG and SNAC guidance helps
- Documentation often most difficult aspect
  - Particularly since SELinux is not traditional MAC
  - Requirements traceability especially time consuming

# Future Goals

- Improved configuration mechanism
  - Based on existing, open source tool (e.g., Puppet)
  - Abstract, desired state description
    - Rather than current “bit-flipping” approach
  - Repeatable application to systems
- Integrate with configuration auditing tools
  - Verify that system in valid configuration
  - Emerging NIST standards compelling (XCCDF)
- Extend to other platforms
  - OpenSolaris w/ FMAC
  - UBUNTU
- Continue to expand community involvement

# Questions / Discussion

Karl MacMillan <kmacmillan@tresys.com>