Securing Data in a RHEL SELinux Multi-Level Secure Environment

201504

MLS Overview

- Red Hat Enterprise Linux (RHEL) forms the foundation of the Multi-Level Security (MLS) system
- Security Enhanced Linux (SELinux) provides the inner core of RHEL providing the addition security
  - NSA develop SELinux & released open source December 2000
  - SELinux was merged with main Linux kernel August 2003
    - Fully commercially support since
  - Introduces Mandatory Access Controls (MAC)
  - Securely enforces separation of data and accesses
  - Introduces Role Based Access Controls (RBAC)
  - Introduces secure auditing
  - All users, data, processes, and networks receive security context which is checked by kernel before interactions are allowed

Overview

- Red Hat Enterprise Linux with Multi-Level Secure policy enforcing Mandatory Access Control (MAC) labeling provides the only solid OS configuration framework currently available that supports protections including:
  - Role Based Access Controls (RBAC)
    - Mitigates insider threats
  - Mandatory Access Controls (MAC)
    - Allows out-of-the-box data fusion configuration
    - Allows out-of-the-box multi-tenancy
  - Automated Auditing
    - RBAC restricts audit file access to those with Audit Admin
  - General enterprise level configurations built from Government owned or commercially available parts

Overview

- Baseline configuration is highly modular and allows additional security as needed
  - Add in encryption
    - Point-to-point data in flight
    - Data at rest
  - Trusted system interchanges
    - As enterprise computing expands, trusted system exchanges available
  - Network file systems available
    - Seagate Lustre allows MAC labeled and audited data exchanges between MLS and non-MLS systems while maintaining security labels

MLS In-Depth

- Operating System
  - RHEL 6.5 w/ SELinux enforcement mode & MLS policy applied
  - MLS Policy
    - All processes, users, data, networks are restricted by MLS policy
    - Adjudicates interactions based MAC first
    - If MAC approves, then DAC governance is validated
- Networking
  - Trusted systems
    - Defined as MLS enabled system with same data labeling scheme
    - Accepts label applied to incoming traffic from trusted systems
  - Un-Trusted systems
    - Defined as any system not in the Trusted system list
    - Apply level to incoming network traffic

MLS In-Depth

- Network Labeling
  - Data labels from each trusted IP address are not overwritten
  - Data from each untrusted system is labeled at the network interface (e.g. Sx:Cy)
- File Labeling
  - For new file, uses MLS context of creator for initial label
  - For existing files, compares MLS context to adjudicate interactions
  - When an object of “higher” security context modifies an object, the system (MAC) applies the higher security context to the modified object

Role Based Access Controls

- RBAC used in SELinux
- Roles are based on least privilege
- Basic roles (modified from RH roles) at CSCF
  - User
  - Backup Admin
  - Unix Admin
  - Security Admin
  - Audit Admin
- Provides additional security

ICD 503 Accreditation

- NIST 800-53 and associated documents define certification process for all federal systems
  - Congress mandated
- ICD 503 derived from NIST 800-53
  - Controls tailored to IC community
  - LM certifications based on ICD 503 with Cross Domain System (CDS) Overlay and several others
  - CDS defined as a system with connections to different security level networks

Controls Application and Support

- Currently uses configuration managed scripts
- Certification Test Plan (CTP) is combination scripting and hand testing
- Security Content Automation Protocol (SCAP)
  - Provides both installation automation and CTP automation
  - Currently being used for testing documentation only
    - Xml files are output

MLS Ecosystem

- MLS OS configuration is certified
  - HW layer is handled through a different procurement layer
  - Technical risk in different hardware
    - May not support RHEL configuration
    - Security body of evidence has to be recreated on the specific system
  - Configuration owned by Government
  - Configurations
    - Single system image – current and certified
    - Cluster/Blade configuration – current and in certification process

MLS Ecosystem

- Storage
  - Direct attached
    - Ext, xfs, zfs – current and certified
    - GPFS in certification process
  - Parallel Network File System – Lustre
    - Seagate Secure Data Appliance
    - Scales horizontally – max single rack is 1.5 PB @ 42 GBs
- Resource Management
  - Altair PBS Professional – current and certified
- Audit Reduction
  - Splunk – current and certified
- IB HPC Interconnect
  - Mellanox working to include security context in native IB

MLS Ecosystem

- System Monitoring and Metrics
  - Altair PBS Analytics – current and certified
  - Splunk – current and certified
- MLS Databases
  - NSA funded and open source
    - Postgres SQL through Crunchy Data Systems
      - Integration to LM RHEL configuration kick off this week
    - Accumulo through MIT-LL
      - Seagate leading LM RHEL integration
- Enterprise Data Sharing
  - Long Haul IB – Bay Microsystems
  - Campus IB – Bay Microsystems and Mellanox