



# Trusted Computing with SELinux

Paul Moore, HP

# Agenda

- Linux and Common Criteria at HP
- SELinux Overview
- SELinux and Trusted Solaris
- Additional Information

# Linux and Common Criteria at HP

# Linux and Common Criteria

- HP has successfully completed several Common Criteria evaluations with Red Hat Enterprise Linux
  - RHEL3 Update 3 [CAPP/EAL3+] (September 2004)
  - RHEL4 Update 2 [CAPP/EAL3+] (May 2006)
  - RHEL5 [CAPP, RBACPP, LSPP/EAL4+] (June 2007)
- Certification covers a wide range of hardware platforms
  - ProLiant 32 and 64 bit platforms
    - Blades, rack mounted servers, standalone servers
  - Integrity Itanium servers
  - Carrier Grade systems
  - Workstations, desktops, and notebooks

# RHEL5 CAPP/RBACPP/LSPP Evaluation

- Leveraged and expanded SELinux features to meet LSPP/RBACPP requirements at EAL4+ with RHEL5
  - Development community included HP, IBM, Red Hat, TCS, the NSA and other individuals
    - SELinux MLS policy implements Bell-LaPadula
    - Polyinstantiated/multi-level directories
    - Labeled networking
    - Labeled printing
    - Auditing of security labels
  - HP has contributed key features
    - CIPSO labeled networking for interoperability
    - Labeled printing using CUPS
    - File system auditing

# HP and Red Hat RHEL5 SELinux Support

- HP partnership with Red Hat to provide RHEL5 support on HP platforms
  - Standard RHEL5 configuration with SELinux targeted policy
    - Tier 1 or Tier 2 standard Support Care Packs
  - Certified CAPP/RBACPP/LSPS RHEL5 configuration
    - Builds upon standard RHEL5 support offerings
    - Customized support based on customer needs
      - Custom solution design, implementation, and validation
      - On-site training
      - Specialized MLS support
      - Long term support

# SELinux Overview

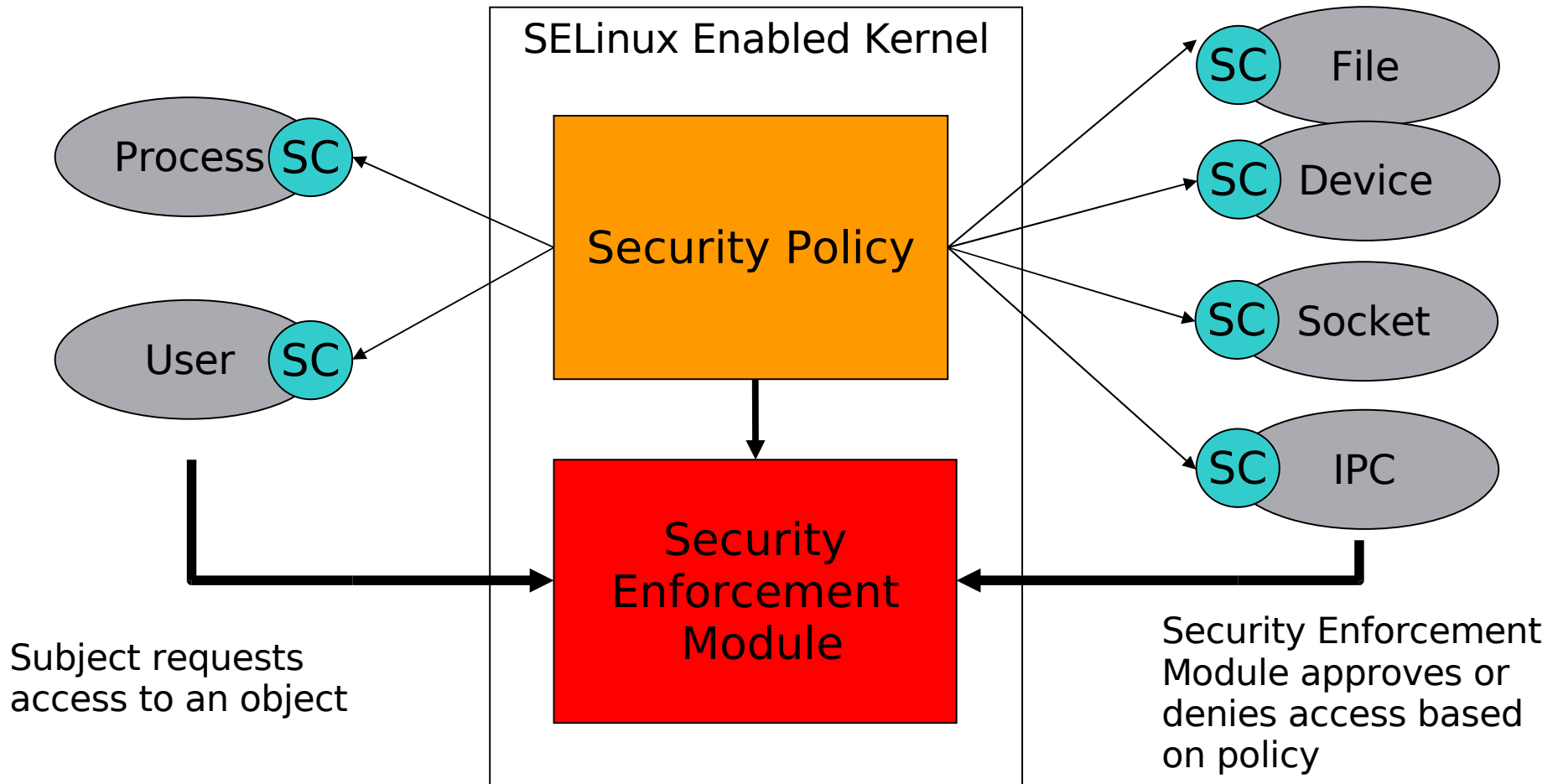
# Introduction to SELinux

- SELinux is a system of flexible mandatory access controls integrated into the Linux kernel
  - Can be used to implement mandatory, role-based access control, and multi-level systems
  - Developed by the NSA based on 10+ years of research
  - Integrated in the mainline 2.6 series Linux kernels
    - Architecture independent
    - Integrated with existing Discretionary Access Controls (DAC)
- Technology based on the Flask security architecture
  - Separates the security policy from security enforcement
  - Policy allows very fine grained control over objects
  - Works with existing applications without modification

# Advantages of SELinux

- Confines users and applications to a predefined set of minimum privileges
  - Reduces or eliminates the impact caused by compromised or improperly configured applications
  - Allows users with high access privileges to run applications without fear of violating the system's integrity
- Separation of security policy from enforcement allows multiple security policies to be developed
  - Modular approach allows customization to fit requirements
  - Several policy variants currently available
    - Targeted policy
    - Strict policy
    - MLS policy

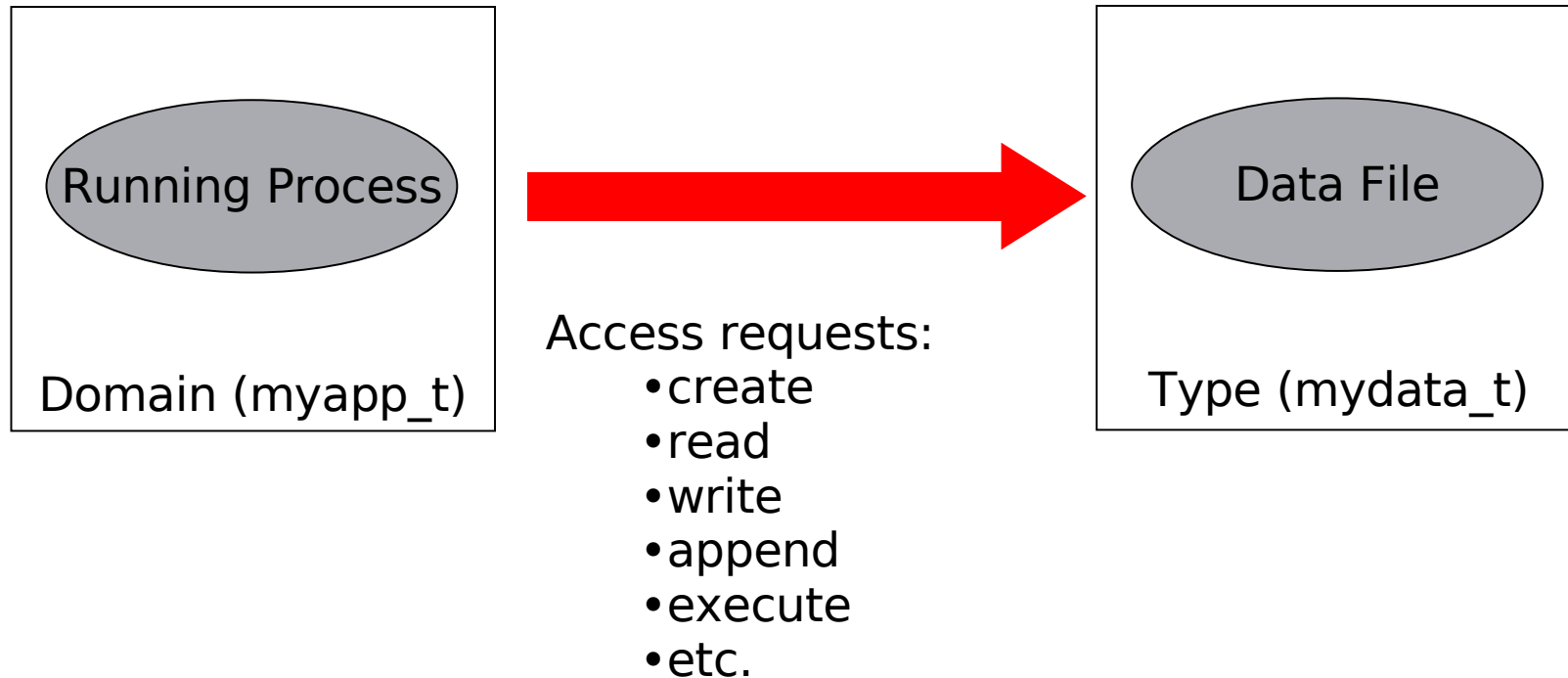
# SELinux Architecture



# SELinux Security Contexts

- A security context consists of a user, role, domain/type, and a MLS sensitivity range
  - Subjects are assigned to a domain
  - Objects are assigned a type
  - MLS sensitivity range consists of a effective and a clearance label
    - MLS sensitivity label translation
  - Example context of a running process (*/bin/ps -Z*)  
`root:secadm_r:netlabel_mgmt_t:SECRET-TOP_SECRET`
- Access decisions are made based on a domain's right to access different types

# SELinux Type Enforcement



# SELinux Multi-Level Security

- SELinux MLS controls work on top of SELinux's type enforcement mechanism
  - First the discretionary access controls are evaluated, then the SELinux type enforcement controls, and finally the SELinux MLS controls
  - The combination of type enforcement and MLS controls allow a much greater level of access control granularity than traditional MLS only systems
- The SELinux MLS security model is controlled by policy
  - Administrators can switch between Bell-LaPadula, Biba, or a custom security model by changing the policy
  - The number of sensitivity levels and compartments are controlled by the policy

# SELinux Role Based Access Control

- SELinux roles are defined by a list of accessible domains
  - The user's current role restricts the user to a predetermined set of domains
  - Users can transition between their assigned roles
    - Transitions can occur automatically via policy or manually through tools and re-authentication
- SELinux users are defined by a list of accessible roles
  - SELinux users are separate from the system users
    - Many system users can share the same SELinux user
  - SELinux user maps a system user to a set of roles
  - Not possible for a system user to transition between SELinux users on the fly

# Active SELinux Work

- **New and improved functionality**
  - Labeled X environment
  - Improved labeled networking access controls
  - Labeled NFS
- **SELinux policy improvements**
  - Merging targeted and strict policies
  - Improved role support
- **Better management and usability**
  - Policy management tools
  - Policy generation tools and wizards
  - Audit log tools

# SELinux and Trusted Solaris

# Trusted Solaris vs RHEL5 SELinux/MLS

## ■ Trusted Solaris

- Sensitivity labels
- Process privileges
- Roles & authorizations
- MaxSix/TSIX & CIPSO
- Labeled X environment

## ■ RHEL5 SELinux/MLS

- Sensitivity labels
- Domain access rights
- Roles
- Labeled IPsec & CIPSO
- Under development

# Labels and Contexts

## ■ Trusted Solaris sensitivity labels

- Contains sensitivity and CMW advisory label information
- Represented in both binary and string formats
- Extensive sensitivity label API

## ■ SELinux security contexts

- Contains both SELinux type enforcement information and the MLS sensitivity range
  - No concept of CMW advisory information label
- Represented in string formats only
- Limited security context API
  - No MLS-only label comparisons
  - No MLS-only label initialization to *Syslo* or *Syshi*

# Privileges and Policy Overrides

- Trusted Solaris has privileges to override security policy
  - Privilege on users, program files, and processes
  - Privilege brackets (API) to activate/disable privileges
    - Requires program source code changes
  - Privilege scope is system wide
  - No need for the root user
- SELinux domains have access rights defined by policy
  - Applications and users operate within SELinux domains
  - Access rights are per-domain, not system wide
  - Security policy determines rights, no bracketing API
  - MLS overrides provided through SELinux security policy
  - Some operations still require root to satisfy DAC

# Roles and Authorizations

- **Trusted Solaris implements roles in userspace**
  - Roles and authorizations are assigned to user accounts
  - Trusted applications check the user's account for specific roles and/or authorizations
    - Allows users to accomplish privileged tasks
    - Trusted applications utilize privileges to bypass policy
- **SELinux implements roles in security policy**
  - Roles are defined in the policy and SELinux users are given access to different roles
  - Roles restrict which domains a user may enter
    - Specific domains have specific access rights
    - Applications do not need to be aware of a user's role
  - Users with multiple roles can transition between roles

# Additional Information

# Additional Information

## HP Linux Security website

- <http://www.hp.com/go/linuxsecurity>

## HP Solaris to Linux migration website

- [http://devresource.hp.com/drc/topics/solaris\\_linux.jsp](http://devresource.hp.com/drc/topics/solaris_linux.jsp)

## NSA SELinux website

- <http://www.nsa.gov/selinux>

## SELinux Wiki

- <http://www.selinuxproject.org>

## My Contact Information

- Paul Moore, [paul.moore@hp.com](mailto:paul.moore@hp.com)