ATOL: SELinux

Marek Grác
xgrac@fi.muni.cz

Red Hat Czech s.r.o. / Faculty of Informatics, Masaryk University

Advanced Topics of Linux Administration

Basic Terms

- Policy – Rules for access decision making
- Security attributes – Metadata assigned to individual processes and resources
- Decision maker – Kernel, DB server, X, Apache, . . .

Discretionary Access Controls (DAC)

- Basic access control policies to objects
- Set of discretion of the owner of the objects (eg. file permissions rwx)
- Users (root and non-root), groups
- Processes can change security attributes
- Gross granularity based on UID, GID

SELinux I

- Implemented using Linux Security Model (LSM)
- Transparent for most of the applications
- Fine granularity
- MAC-based policy – normal processes cannot change security attributes

SELinux II

- Base form of access control
  - Type Enforcement (TE) – primary
  - Role-Based Access Control (RBAC)
  - Multi-Level Security (MLS) – Bell-LaPadula
- Configuration using language to describe policy
  - Configuration files for system stored in one place
  - Three basic policies (targeted, strict, mls)
  - Access is denied by default
  - Rights can be only added to existing policy

SELinux III

- Processes (subjects) and resources (objects) have security context
- *ls -Z, ps axZ, id -Z*

Type Enforcement I

- Based on security attribute *type*
- Type is given to both subjects and objects
- Attributes for access control
  - Subject Type, Object Type, Class of Subject, Operation
  - Example: *http_t, httpd_sys_content_t, file, read*

Type Enforcement II - Initial type

- Inherited to files from directories
- Privileged subjects can explicitly set context (eg. chcon)
- Inherited to child from parent processes
- Transition rules: init (init_t) - httpd init script (initrc_t) - httpd (httpd_t)

Lab: Installation

- Goals:
    - Create a file with permission 0777 that cannot be read by normal user
    - Use SELinux to block access to 'ping' for normal users

Lab: Prepare a paper

- Themes:
  - Describe AppArmour and compare it to SELinux
- Format:
  - Short presentation (15–20 minutes; 5-7 slides)
  - Paper containing comparision (500 words)