

Cyber Security Lab2

Due

Tuesday February 14.

Amended – The MCS scenario (section 2) has been dropped.

Goal

Exercise SELinux type enforcement and MLS policy and make simple extensions to an existing policy.

Scenario

You've been asked to implement a variant of the SELinux strict policy. Instead of just implementing a single domain of unprivileged user (`user_t`), you will need to create another domain (`corporate_t`). Most users will be either members of the `user_t` domain or the `corporate_t` domain. Files created by members of each domain should not be visible to the other.

You have also been asked to investigate the new MCS feature in a targeted SELinux policy. Examine a scenario with three users each working on a subset of three projects. See how you can use MCS to collaborate with users working on the same project but still protect the files from users working on different projects.

Your tasks

You will need to perform the following tasks.

1. First working with type enforcement policy.
 - a. Create a second domain named `corporate_t` analogous to `user_t` along with all the related supporting roles and types.
 - b. Put users Alice, Bob, Carol, and Dave in the `corporate_t` domain, and leave Ellen and Gus in the `user_t` domain.
 - c. Verify that members of `user_t` and `corporate_t` cannot see files created by members of the other domain.
 - d. Verify that otherwise members in each domain can access the same files.
 - e. What is it in the policy that prohibits access between processes labeled `user_t` and `corporate_t`? Can a process labeled `sysadm_t` access files in the `user` and `corporate` home directories?
 - f. Does this solution scale roughly linearly for each new segmented domain you add? That is, for each independent domain can you use the same set of steps or do you have to do something relative to all the existing domains.

