Using Security Labels [4]

This chapter describes the mandatory access controls used by a UNICOS system. Mandatory access controls are rules that control access based directly on a comparison of the subject's clearance and the object's classification. On a UNICOS system with the multilevel security (MLS) feature, these rules are incorporated into the UNICOS security policy. This chapter describes the following:

- The UNICOS security policy
- The commands needed to display and change security labels

4.1 UNICOS security policy

The UNICOS security policy is defined as the set of rules and practices by which a system regulates the disclosure of information. The UNICOS security policy uses security labels to enforce the following rules (see Figure 10 for a summary of this policy):

- A subject may read or execute an object only if the subject's current security label dominates the security label of the object.
- A subject may write or append to an object only if the subject's security label is equal to the security label of the object.

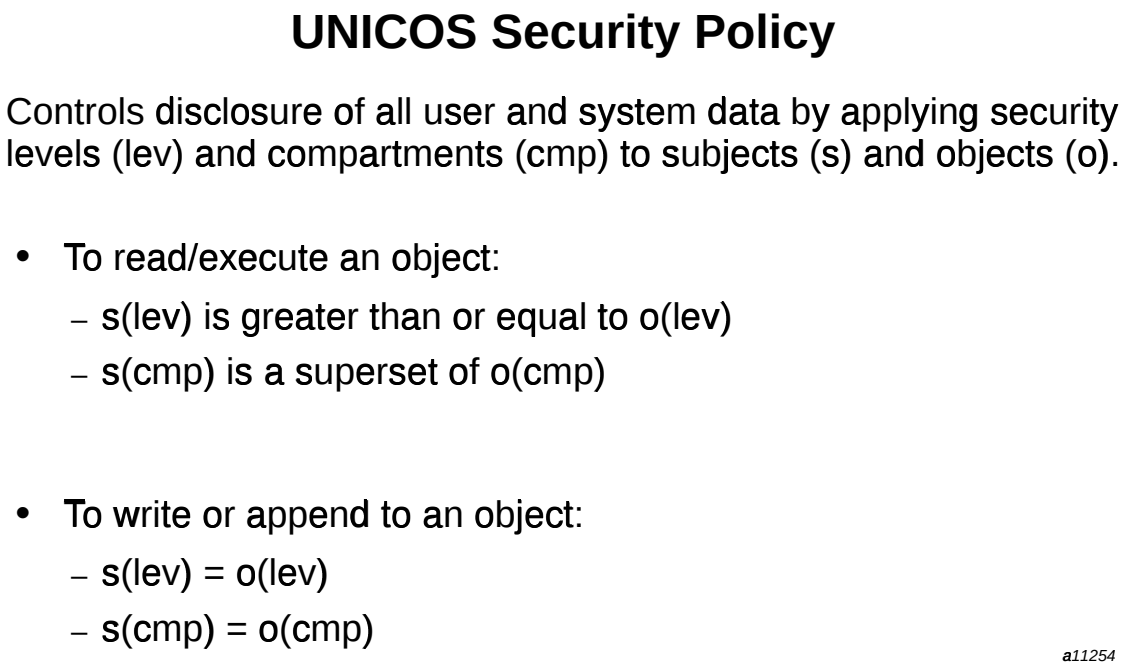

Figure 10. Mandatory access controls; UNICOS security policy

4.1.1 Changing security labels (`setulvl` and `setucmp`)

When you log into a UNICOS system, you are assigned a label consisting of a security level and a set of compartments. You can choose to operate at the assigned label throughout the entire session or you can execute the `setulvl`(1) and/or `setucmp`(1) commands to upgrade your label.

If you upgrade your label using either or both of these commands, the resulting label must dominate your current label and be dominated by your maximum security label (your maximum label is defined by your maximum security level and authorized compartments assigned to you in the UDB).

You cannot upgrade your label on a Cray ML-Safe configuration of the UNICOS system, because your active security label and your maximum security label are always equal on a Cray ML-Safe configuration.

The `setulvl`(1) command can set the security level component of a security label to a specified number. The number can range form 0 to 16, where 0 is the lowest clearance and 16 is the highest clearance. Optionally, your security

administrator may assign names to these values; if this has been done at your site, you can specify a named value instead of a number.

Note: You cannot successfully use the `setulvl` command on a Cray ML-Safe configuration or a network connection configured with the IP security option on a UNICOS system. You are allowed to operate only at the security label established when the network login socket connection was created.

Example 21 shows the `setulvl`(1) command used with the number 2 as an argument. This example also shows how to use the `spget`(1) command without options to display your security parameters, including your maximum, minimum, and default security levels.

Example 22 shows the `setulvl`(1) command used with the `level2` as an argument. In both cases, the message returned by `setulvl`(1) confirms that the level has changed to 2.

Example 21: Example of `setulvl` command

```
$ setulvl 2
setulvl:  New security label is
Level[2:level2] Compartments [none]
$  spget
permits equal 00000
               none
security level is 2
               level2
maximum level is 16
               level16
minimum level is 0
               level0
authorized compartments are 010
               test
active compartments are 00
               none
integrity class is 0
               class0
maximum class is 0
               class0
active categories are 00
               none
authorized categories are 00000000000
               none
```

Example 22: Example of `setulvl level2` command

```
$ setulvl level2
setulvl:  New security label is
Level[2:level2] Compartments [none]
```

The `setucmp`(1) command is similar in operation to the `setulvl`(1) command, except that it adds compartments to your current compartment set rather than setting an absolute value. Compartments can be set in one of the following ways:

- By using an octal mask; the mask is a bit value corresponding to one or more compartments to be activated. This argument must be expressed in octal.
- By specifying `ALL`, which activates all authorized compartments
- By specifying a comma-separated list of names

Example 23 shows how the `setucmp` command is used to change your security compartments. This example also shows how to use the `spget`(1) command without options to display your security parameters, including your active and authorized compartments.

Note: You cannot successfully use the `setucmp` command on a Cray ML-Safe configuration or a network connection configured with the IP security option on a UNICOS system to add to your security compartments. You are allowed to operate only at the security label established when the network login socket connection was created.

Example 23: Example of `setucmp` command

```
$ setucmp test
setucmp:  New security label is
Level [2:level2] Compartments [test]
$ spget
permits equal 00000
               none
security level is 2
               level2
maximum level is 16
               level16
minimum level is 0
               level0
authorized compartments are 010
               test
active compartments are 010
               test
integrity class is 0
               class0
maximum class is 0
               class0
active categories are 00
               none
authorized categories are 00000000000
               none
```

The `setulvl`(1) and `setucmp`(1) commands can be issued successfully only when the shell is the only process in your session. For example, if you log in to the C shell (`csh`(1)) and execute the Korn shell (`ksh`(1)) as a sub-shell, or execute a command in the background, you are not allowed to change your label from the sub-shell or while the background process is still running. If you replace your C shell with a Korn shell by using the `exec`(1) shell built-in command, you are allowed to change your label from the Korn shell, provided no other process was currently in your session.

Changing your label can fail for the following reasons:

- You tried to change to a label that does not dominate your current label.
- You tried to change to a label that is not dominated by your maximum label.
- You have open files other than the controlling `tty` within your process.

- The shell from which you issued the request is not the only process in the session.
- You have an open socket connection.
- The label you requested is not within the range of labels allowed on your system.
- Your system is configured to enforce strict B1 compliance and the security label is not equal to the current label.

4.1.2 MLS permissions

On UNICOS systems, you can be assigned MLS permissions (shown in Figure 11) at login time. These permissions are specified with your other login account attributes in the user database (UDB).

MLS permissions grant a user special capabilities on a UNICOS system. The MLS permissions are useful only on a UNICOS system using the super-user mechanism; they have no affect on UNICOS systems that use only the PAL-based privilege mechanism.

You can use the `spget`(1) command to display your MLS permissions. You may see the `suidgid` permission assigned to your account.

MLS Permissions

Set setuid/setgid (`suidgid`): Gives the user explicit permission to set the set-user-ID (setuid) and/or set-group-ID (setgid) bits for a file. Restricted management of setuid and setgid files is enforced only on UNICOS systems configured to do so. This permission is used only on UNICOS systems using the super-user mechanism.

MLS Permissions

- Set setuid/setgid (`suidgid`): Gives the user explicit permission to set the set-user-ID (setuid) and/or set-group-ID (setgid) bits for a file. Restricted management of setuid and setgid files is enforced only on UNICOS systems configured to do so. This permission is used only on UNICOS systems using the super-user mechanism.

***a**11303*

Figure 11. Permissions