Logging in and Using Passwords [2]

The following chapter describes the login and password procedures used on a UNICOS system with the multilevel security (MLS) feature. The following topics are described:

- Logging in interactively on a UNICOS system
- Logging in interactively on a Cray ML-Safe system configuration
- Your SecurID card
- Choosing passwords
- Login and password protection features available

The following sections also apply to the `ftpd` and `rexecd` daemons (except for the SecurID information), as well as to `login`(1).

2.1 Interactive logins

Note: For information on Cray ML-Safe logins, see Section 2.2, page 24. Some of the information in this section does not apply to Cray ML-Safe logins.

To successfully access the UNICOS system in interactive mode, you must respond with the correct information to the system prompts shown in Example 1, page 23.

You must enter your user name after the `login:` prompt. After your name is entered, the system displays the `Password:` prompt, and you must then enter your correct password. The UNICOS system suppresses the display of your password characters. Your login access can be affected by checks made to the network access list (NAL) and workstation access list (WAL). For more information on the NAL and WAL, see the *TCP/IP Network User's Guide*, Cray Research publication SG–2009.

After successfully entering your name and password, the system displays your active security label, the date and time of day of your last successful login, and where your last valid login originated. If there were any unsuccessful login attempts since the last successful login, the system displays this information also.

If you know that these unsuccessful attempts were not yours, or if you notice any other unusual login problems (such as a successful login that was not performed by you), contact your security administrator immediately.

The final login step is the display of any system messages. A successful login indicates that you have been authenticated for access to the UNICOS system and that `login` has set your clearance. Your security clearance is determined as follows:

- The valid label range for your session is the intersection of your range from the user database (UDB) and the range on the socket connection. Depending on the configuration of your system, the default UDB label can be used as your minimum UDB label.
- If you request a security label, the requested label is the active label for the session. The requested label must be within the range of the session or access is denied.
- If you do not request a security label, your default label is used if it is within the label range of your session. The minimum label of the session is used if the default is not within the range of the session.

To display your current security login environment, use the `spget`(1) command, as shown in Example 1, page 23. The `spget` command, used without options, displays the following information:

- The `permits equal` line displays your security permissions, as defined in the UDB.
- The `security level is` line displays your active security level.
- The `maximum level is` line displays the maximum security level you can activate during your current session.
- The `minimum level is` line displays your minimum security level.

Example 1: Interactive login screen and the `spget` command

```
login:jack
Password:
Active label set to: level2,none

Last successful login was: Wed Oct 7 12:14:29 from training
followed by 2 failed attempts

Welcome to the 8.0 UNICOS system
$
$  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
```

- The `authorized compartments are` line displays the maximum set of security compartments that you can activate during your current session.
- The `active compartments are` line displays your active compartments.
- The `integrity class is` line displays your active class. This value is not used.
- The `maximum class is` line displays your maximum class. This value is not used.

- The `active categories are` line displays your active category. If you use the `spget` command immediately after login (that is, before you use the `setucat` command to change your category), this line is your default category, as defined in the UDB.
- The `authorized categories are` line displays your authorized categories, as defined in the UDB.

You can also use the `-L` *requested_label* option of the `login` command to set your security label at the login prompt, where *requested_label* is the label you want as your active label for the session. The `-L` option of `login` cannot be successfully executed on a Cray ML-Safe configuration.

The following example shows Jack specifying a security label with the `-L` option of the `login` command. The active security label is displayed for all logins.

Example 2: Use of the `login -L` command

```
login:jack -L level1,comp24
Password:
Active label set to: level1,comp24

Last successful login was: Wed Oct 8 16:14:30 from training

Welcome to the 8.0 UNICOS system
$
```

If you specify a security label that is outside of your range (as determined by the UDB and NAL), your login request is denied.

2.2 Interactive Cray ML-Safe logins

Logging into a Cray ML-Safe configuration of the UNICOS operating system follows the same procedures outlined in the previous section for logging into a UNICOS system, but there are restrictions regarding your security label range. You cannot successfully use the `-L` option of the `login` command (explained in the previous section) on a Cray ML-Safe configuration.

On a Cray ML-Safe configuration, the IP security option (IPSO) protocol must, for the most part, be used for network connections to the Cray ML-Safe configuration (see Example 1, page 23). This example shows the IPSO connection between two Cray ML-Safe configurations, and between a

compartmented mode workstation (CMW) and one of the Cray ML-Safe configurations. Also shown, is a non-IPSO connection, which is explained later.

On a Cray ML-Safe configuration, your range is still determined by the combination of your UDB entry and range on the socket connection as explained in the previous section. On an IPSO connection, the socket range is determined when it is established, and the range is based on the label of the process that created the socket connection. If you use the `telnet`(1B) command to connect to a Cray ML-Safe configuration at a label outside of this defined range, you are denied access to the Cray ML-Safe configuration (that is, you never reach the `login` prompt sequence shown in the previous section).

On a Cray ML-Safe configuration, your minimum label, maximum label, and active label are all the same value. This means that whatever label you have when you log in is the only one allowed during that session. You cannot successfully use the `setulvl`(1) and `setucmp`(1) commands to change your label. To change your active label, you must log off completely and establish a socket connection at a different security label.

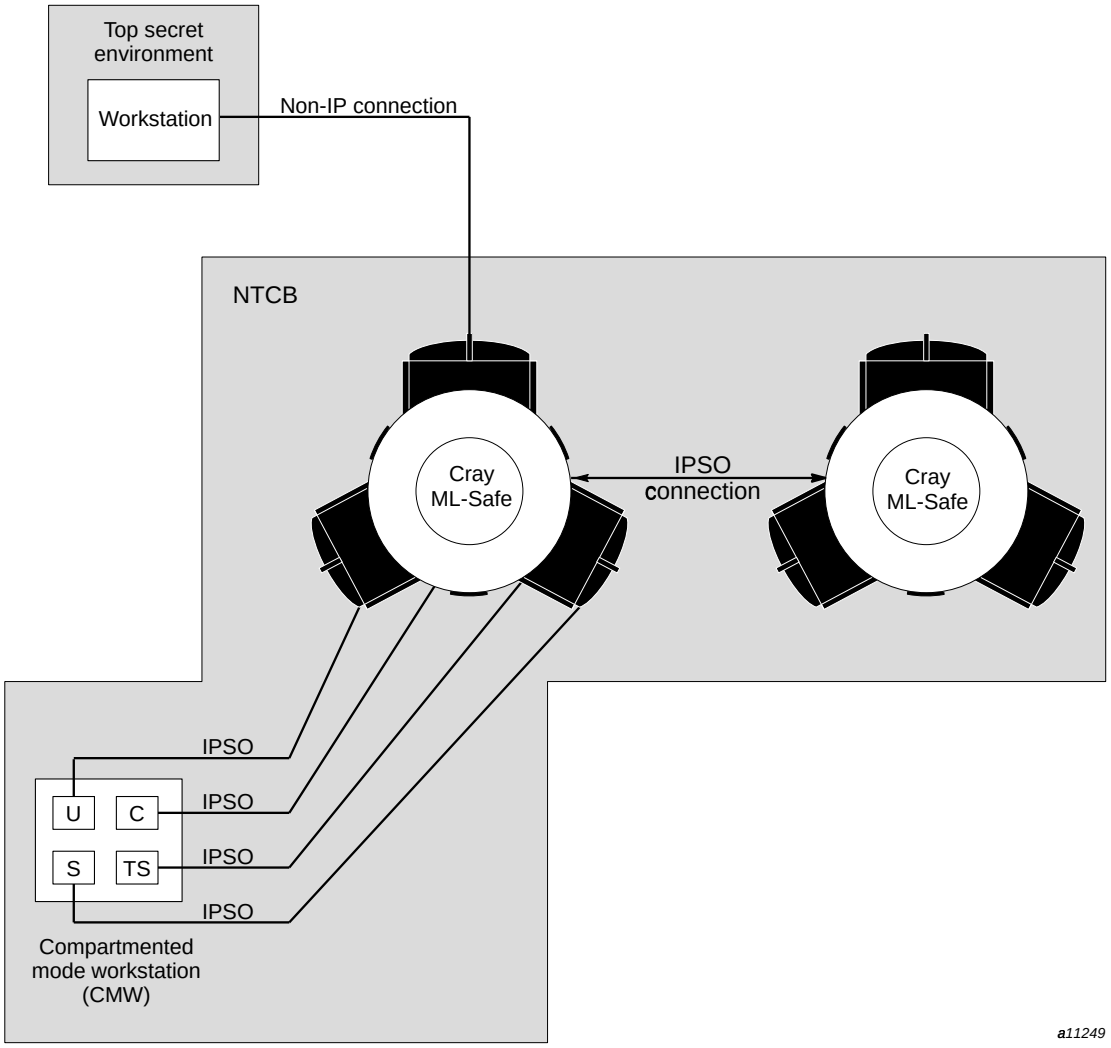

Figure 5. Logging in on a Cray ML-Safe system configuration

In Figure 5, the CMW has four windows, each having a different security label: u (unclassified) c (classified), s (secret), and ts (top secret). Each window has its own IPSO connection into a CrayML-Safe configuration of the UNICOS operating system; each connection can only function at the security label established when the socket was created.

There is limited support for the use of a single-label non-IPSO connection into a CrayML-Safe configuration. Packets on a non-IPSO connection are not labeled and the systems on a non-IPSO network cannot be trusted to label the information they contain.

Because of these limitations, all systems connected to a Cray ML-Safe configuration of the UNICOS system through an non-IPSO network must have the same label, and the network itself must be configured with that label. This allows the use of workstations that do not manage security labels as connections to a Cray ML-Safe configuration without compromising the labeled security of the Cray ML-Safe configuration.

Use of a non-IPSO connection is shown in Figure 5. In this example, a workstation is connected to a top secret, non-IPSO network. All communication on this network occurs at the top secret level, and all workstations on this network are both procedurally and physically secured for the top secret level. If a workstation that was at a secret level were configured into this network, the evaluated rating of the network would be compromised, as this workstation could not differentiate between secret and top secret information, allowing the user of the secret-rated workstation access to top secret information.

2.3 Displaying the operating system's MLS environment

The security level range and valid compartments for the UNICOS operating system are established by your security administrator. Only your security administrator can change these parameters, and all processes are restricted by them. As a user on a UNICOS system, you can work only within the range set for the operating system.

You can display the security environment for your operating system by using the `spget -s` command, as shown in Example 3.

Example 3: Displaying the operating system's security environment (`spget -s`)

```
$ spget -s
system minimum level is 0
               level0
system maximum level is 16
               level16
valid system compartments are 01777
               company
               mktg
               develop
               test
               train
               bnchk
               pubs
               techop
               corp
               cust
```

2.4 Remote logins with SecurID card

The SecurID card, manufactured by Security Dynamics, Inc., can be used on Cray Research systems for interactive logins from remote hosts. This authentication mechanism makes it harder to break into accounts because new passcodes are generated for each authentication and a passcode cannot be used more than one time.

Note: Use of SecurID is optional on a CrayML-Safe configuration of the UNICOS operating system.

Basically, the SecurID card is an electronic device, the size and shape of a credit card (see Figure 6 for an example of a SecurID card).

Figure 6. The SecurID card

For this type of SecurID card, a number appears on the card's LCD display; this number is unique to the card and changes at a predetermined rate. This number, along with your personal identification number (PIN) number, is used in the login sequence or at other times to identify you. It is very important that you do not disclose your PIN by letting others use it or writing it down, as this would allow anyone to use your card to gain access to the system.

The SecurID feature is optional on UNICOS and Cray ML-Safe configurations. Because procedures for using the card can be different for each site, you should contact your security administrator for this information.

2.5 Passwords

The password is the basic tool used by many systems to regulate access to a system. On a secure system, the proper use, protection, and auditing of passwords is the first line of defense in protecting system integrity.

When choosing and using passwords on the UNICOS system, you should observe the guidelines shown in Figure 7, page 31.

There are several system features that can be set by your security administrator that can affect how you use passwords. They are listed in Figure 7, page 31 and explained in the following sections.

2.5.1 Last login notification

At the time of each login, this feature allows the system to display the last login date, the last login time, the number of intervening login failures, and the ID of the terminal at which you last logged in. If you recognize any discrepancy, report it to your security administrator immediately.

2.5.2 Generic login message

This feature allows the system to display a generic `Login incorrect` message when an unsuccessful login attempt is detected. Because it does not explicitly identify the incorrect portion of the login entry, this form of reply makes it harder to guess user names and passwords.

2.5.3 Minimum password size

This feature allows your security administrator to specify a minimum number of characters for a password. To avoid the use of simple passwords, the system default is 6 characters.

Password Guidelines

- Change your passwords often
- Do not let others use your password
- Do not record your password in written form
- Do not choose easy passwords
- Do not use old passwords
- Do not use the same passwords on different systems
- Report any suspicious activity on your login to your security administrator
- Do not use words found in the dictionary
- Use upper/lower case letter and/or alpha/numeric combinations

Password Features

- Last login notification
- Generic login message
- Minimum password size
- Password locking
- Machine-generated passwords
- Login limits/login disable time-out
- Password aging

a11251

Figure 7. Password guidelines and features

2.5.4 Password locking

This feature allows your security administrator to lock your password to prohibit access by your account to the system. This feature is useful if your account is going to be inactive for an extended length of time (for example, while you are on vacation or medical leave) to prevent unauthorized attempts at using your login. If you try to log in after an extended absence and are unable to do so, check with your security administrator to see if your password has been locked.

2.5.5 Machine-generated passwords

If the machine-generated password feature is enabled on your UNICOS system, the `passwd`(1) command executes differently than on other UNICOS systems. This is shown in Example 4.

In this example, you are prompted to enter your old password and then, instead of allowing you to select a new one, the system generates a new password for you. You can select the first password generated or continue to request new passwords by pressing `CR` until a suitable password is generated.

> **Note:** Although the chances are extremely small, the password-generating algorithm can produce a password that may seem offensive to you. The appearance of such a password is random and is not intended to be offensive. You have the choice of rejecting any generated password and picking a subsequent password.

It is important that you do not select a new password in the presence of another person (or, at the very least, shield your screen from the other person's view) when using this feature. Also, when you are done selecting a password, remove or erase the screen, so that no one else can obtain your new password.

Example 4: Machine-generated password example

```
$ passwd
Changing password for jane
Old password:
Your new password is: kudniqui
Re-enter password or (CR) to get another:
Your new password is: keltifok
Re-enter password or (CR) to get another:
Your new password is: onyorja
Re-enter password or (CR) to get another:
Your new password is: rhecirou
Re-enter password or (CR) to get another:
Your new password is: osniyuib
Re-enter password or (CR) to get another:
$
```

2.5.6 Login limit and login disable time-out

Your UNICOS system can use the following site-configurable login features: login limit feature, login disable time-out feature, a delay between failed login attempts feature, and a feature that multiplies the delay between failed login attempts. Your security administrator is responsible for activating and assigning values to these parameters.

The login limit feature defines the number of successive failed login attempts you are allowed before disabling logins from your account.

Use of this feature prevents an unauthorized person from making an unlimited number of attempts at guessing your password. For example, if your security administrator sets the maximum number of failed login attempts feature to 3, you (or a malicious user) are allowed only three consecutive attempts at selecting the correct password. Even if the correct password is selected on the fourth try, the login attempt would not be successful (the generic message, `Login incorrect`, would appear on the screen).

The login disable time-out feature allows your security administrator to define the number of seconds a user is disabled after exceeding the maximum number of failed login attempts. So, if the disable time-out feature is set to 20, and the maximum number of failed login attempts feature is set to 3, after three failed login attempts, you (or a malicious user) would be unable to login until 20-seconds had expired. Then, you are allowed one attempt at logging in. If this attempt fails, the `Login incorrect` message appears for this failed

attempt and any subsequent login attempts that occur prior to the next 20 second interval. This delay continues until a successful login attempt is completed or your security administrator intervenes.

In order to make password guessing more difficult for malicious users, your security administrator can use a feature that defines the number of seconds that must pass between failed login attempts. For example, if the number of seconds is set to 10, then the login prompt would not appear for 10 seconds after each failed login attempt.

Your security administrator can further restrict such attempts by setting a feature that multiplies the number of seconds between failed login attempts by the number of successive failed attempts. This lengthens the delay between each incorrect attempt. For example, using the time set in the previous example, the login prompt would not appear for 20 seconds after the second failed login attempt, 30 seconds after the third failed login attempt, and so on.

The values of these features are site-dependent. It is up to your security administrator to decide how many attempts are allowed and what values are assigned to the features. Regardless of how they are set, it is important for you to watch for and report any suspicious login/password activity to your security administrator as soon as possible.

2.5.7 Password aging

Your security administrator can assign a maximum and minimum number of weeks that your password is valid. The maximum number specifies the maximum number of weeks that you can use your password. When this limit is reached, a message tells you that your password has expired and that you must pick a new one, as shown in Example 5. After picking the new password, the system prompts you to log in again. If your system is using the machine-generated password feature, you are prompted to enter your old password. The system then generates a new password for you.

Your security administrator can also assign a minimum number of weeks that you must use your new password. This feature prevents you from changing to a new password and then immediately changing back to your old one.

Your security administrator can also force you to change your password before the next login attempt.

Example 5: Password aging messages

```
login:jack
Password:
Active label set to: level2,none

Your password has expired.  Choose a new one.
Old password:
New password:
Re-enter new password:
login:
```