NAME

d_passwd – dial-up password file

SYNOPSIS

/etc/d_passwd

DESCRIPTION

A dial-up password is an additional password required of users who access the computer through a modem or dial-up port. The correct password must be entered before the user is granted access to the computer.

d_passwd is an ASCII file which contains a list of executable programs (typically shells) that require a dial-up password and the associated encrypted passwords. When a user attempts to log in on any of the ports listed in the **dialups** file (see **dialups**(4)), the login program looks at the user's login entry stored in the **passwd** file (see **passwd**(4)), and compares the login shell field to the entries in **d_passwd**. These entries determine whether the user will be required to supply a dial-up password.

Each entry in **d_passwd** is a single line of the form:

*login-shell***:***password***:**

where

login-shell The name of the login program that will require an additional dial-up password.

password A 13-character encrypted password. Users accessing the computer through a dial-up port or modem using *login-shell* will be required to enter this password before gaining access to the computer.

d_passwd should be owned by the **root** user and the **root** group. The file should have read and write permissions for the owner (**root**) only.

If the user's login program in the **passwd** file is not found in **d_passwd** or if the login shell field in **passwd** is empty, the user must supply the default password. The default password is the entry for **/usr/bin/sh**. If **d_passwd** has no entry for **/usr/bin/sh**, then those users whose login shell field in **passwd** is empty or does not match any entry in **d_passwd** will not be prompted for a dial-up password.

Dial-up logins are disabled if **d_passwd** has only the following entry:

/usr/bin/sh:*:

EXAMPLES

Here is a sample **d_passwd** file:

```
/usr/lib/uucp/uucico:q.mJzTnu8icF0:
/usr/bin/csh:6k/7KCFRPNVXg:
/usr/bin/ksh:9df/FDf.4jkRt:
/usr/bin/sh:41FuGVzGcDJlw:
```

Generating An Encrypted Password

The **passwd** (see **passwd**(1)) utility can be used to generate the encrypted password for each login program. **passwd** generates encrypted passwords for users and places the password in the **shadow** (see **shadow**(4)) file. Passwords for the **d_passwd** file will need to be generated by first adding a temporary user id using **useradd** (see **useradd**(1M)), and then using **passwd**(1) to generate the desired password in the **shadow** file. Once the encrypted version of the password has been created, it can be copied to the **d_passwd** file.

For example:

1. Type **useradd tempuser** and press Return. This creates a user named **tempuser**.
2. Type **passwd tempuser** and press Return. This creates an encrypted password for **tempuser** and places it in the **shadow** file.
3. Find the entry for **tempuser** in the **shadow** file and copy the encrypted password to the desired entry in the **d_passwd** file.
4. Type **userdel tempuser** and press Return to delete **tempuser**.

These steps must be executed as the **root** user.

FILES

/etc/d_passwd	dial-up password file
/etc/dialups	list of dial-up ports requiring dial-up passwords
/etc/passwd	password file
/etc/shadow	shadow password file

SEE ALSO

passwd(1), **dialups**(4), **passwd**(4), **shadow**(4)

WARNINGS

When creating a new dial-up password, be sure to remain logged in on at least one terminal while testing the new password. This ensures that there is an available terminal from which you can correct any mistakes that were made when the new password was added.