## NAME

hosts.equiv, rhosts – trusted remote hosts and users

## DESCRIPTION

The **/etc/hosts.equiv** and **.rhosts** files provide the ''remote authentication'' database for **rlogin**(1), **rsh**(1), **rcp**(1), and **rcmd**(3N). The files specify remote hosts and users that are considered *trusted*. Trusted users are allowed to access the local system *without supplying a password.* The library routine **ruserok( )** (see **rcmd**(3N)) performs the authentication procedure for programs by using the **/etc/hosts.equiv** and **.rhosts** files. The **/etc/hosts.equiv** file applies to the entire system, while individual users can maintain their own **.rhosts** files in their home directories.

These files *bypass* the standard password-based user authentication mechanism. To maintain system security, care must be taken in creating and maintaining these files.

The remote authentication procedure determines whether a user from a remote host should be allowed to access the local system with the identity of a local user. This procedure first checks the **/etc/hosts.equiv** file and then checks the **.rhosts** file in the home directory of the local user who is requesting access. Entries in these files can be of two forms. *Positive* entries *allow* access, while *negative* entries *deny* access. The authentication succeeds when a matching positive entry is found. The procedure fails when the first matching negative entry is found, or if no matching entries are found in either file. Thus, the order of entries is important; If the files contain positive and negative entries, the entry that appears first will prevail. The **rsh**(1) and **rcp**(1) programs fail if the remote authentication procedure fails. The **rlogin** program falls back to the standard password-based login procedure if the remote authentication fails.

Both files are formatted as a list of one-line entries. Each entry has the form:

> *hostname* [*username*]

Negative entries are differentiated from positive entries by a '–' character preceding either the *hostname* or *username* field.

### Positive Entries

If the form:

> *hostname*

is used, then users from the named host are trusted. That is, they may access the system with the same user name as they have on the remote system. This form may be used in both the **/etc/hosts.equiv** and **.rhosts** files.

If the line is in the form:

> *hostname username*

then the named user from the named host can access the system. This form may be used in individual **.rhosts** files to allow remote users to access the system *as a different local user*. If this form is used in the **/etc/hosts.equiv** file, the named remote user will be allowed to access the system as *any* local user.

**netgroup**(4) can be used in either the *hostname* or *username* fields to match a number of hosts or users in one entry. The form:

> **+@***netgroup*

allows access from all hosts in the named netgroup. When used in the *username* field, netgroups allow a group of remote users to access the system as a particular local user. The form:

*hostname* **+@***netgroup*

allows all of the users in the named netgroup from the named host to access the system as the local user. The form:

**+@***netgroup1* **+@***netgroup2*

allows the users in *netgroup2* from the hosts in *netgroup1* to access the system as the local user.

The special character '+' can be used in place of either *hostname* or *username* to match any host or user. For example, the entry

**+**

will allow a user from any remote host to access the system with the same username. The entry

**+** *username*

will allow the named user from any remote host to access the system. The entry

*hostname* **+**

will allow any user from the named host to access the system as the local user.

**Negative Entries**

Negative entries are preceded by a '/-' sign. The form:

*–hostname*

will disallow all access from the named host. The form:

*–@netgroup*

means that access is explicitly disallowed from all hosts in the named netgroup. The form:

*hostname –username*

disallows access by the named user only from the named host, while the form:

**+** *–@netgroup*

will disallow access by all of the users in the named netgroup from all hosts.

## FILES

**/etc/hosts.equiv**
**~/.rhosts**

## SEE ALSO

**rcp**(1), **rlogin**(1), **rsh**(1), **rcmd**(3N), **hosts**(4), **netgroup**(4), **passwd**(4)

## NOTES

Hostnames in **/etc/hosts.equiv** and **.rhosts** files must be the official name of the host, not one of its nicknames.

Root access is handled as a special case. Only the **.rhosts** file is checked when access is being attempted for root. To help maintain system security, the **/etc/hosts.equiv** file is not checked.

As a security feature, the **.rhosts** file must be owned by the user who is attempting access.

Positive entries in **/etc/hosts.equiv** that include a *username* field (either an individual named user, a netgroup, or '**+**' sign) should be used with extreme caution. Because **/etc/hosts.equiv** applies system-wide, these entries allow one, or a group of, remote users to access the system *as any local user*. This can be a security hole.