

## PAM authentication on solaris (with openssh-3.7.1p2) is not quite right

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-12/0178.html>

---

*From:* Neil W Rickert ([rickert+nn\\_at\\_cs.niu.edu](mailto:rickert+nn_at_cs.niu.edu))

*Date:* 12/21/03

Date: Sun, 21 Dec 2003 03:55:41 +0000 (UTC)

Background:

I am using nis+ on our solaris 8 systems. Home directories are NFS mounted with secure nfs (requires the nisplus credentials).

If I use ssh to login to a client machine, all is fine.

If I use ssh to login to one of our servers, there are problems. Specifically, the credentials have not been properly registered with keysevr, and as a result NFS mounted home directories are not accessible. I can use the "keylogin" command to correct the problem.

On the client machine, the shadow data is not accessible without the credentials. Presumably because of this, the PAM routines properly establish credentials so that they can get the shadow data to validate the password.

On the server machines, the root user can access the shadow data without credentials first being established. Apparently this shortcut route is used, causing the problem.

sshd\_config contains

UsePAM yes

It makes no difference whether I set "PasswordAuthentication no". Either way, challenge response authentication is used.

By way of comparison, "rlogin" does work properly on either client or server. Here "server" means a nis+ server that is in the admin nisplus group.

The relevant auth entries from pam.conf

rlogin auth sufficient pam\_rhosts\_auth.so.1

comp.security.ssh: PAM authentication on solaris (with openssh-3.7.1p2) is not quite right

```
rlogin auth requisite pam_authok_get.so.1
rlogin auth required pam_dhkeys.so.1
rlogin auth required pam_unix_auth.so.1
```

```
other auth requisite pam_authok_get.so.1
other auth required pam_dhkeys.so.1
other auth required pam_unix_auth.so.1
```

Since there was nothing relevant in ".rhosts" in my tests with rlogin, I would have thought both should behave the same.

-----

Test procedure:

First login to the server, and use: keylogout  
(this de-registers credentials)

Next try to login with ssh  
try to login with rlogin

After each login, check whether credentials are registered with keysevr . The simplest check is to try accessing a secure-nfs mounted file system.