

## Re: Trouble with OpenSSH 3.4p1 – Can't connect with an RSA key pair

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-01/0288.html>

---

**From:** Mike ([mike\\_at\\_nomail.com](mailto:mike_at_nomail.com))

**Date:** 01/31/04

Date: Sat, 31 Jan 2004 11:21:07 +0800  
To: LinuxManMikeC <[LinuxManMikeC@netscape.net](mailto:LinuxManMikeC@netscape.net)>

LinuxManMikeC wrote:

> I have a computer functioning as a server using RedHat 8.0 with OpenSSH  
> 3.4p1. I am able to connect using plaintext passwords, but when I  
> disable the plaintext passwords and use only public/private keypairs I  
> can't authenticate a connection. I have the public keys installed on  
> the server in the /home/"username"/.ssh/authorized\_keys file. I have  
> tried using keypairs generated using PuTTY and OpenSSH. I have only  
> used RSA keypairs. This has been a pain to try and figure out, I have  
> already checked the RedHat Network for updated packages, but they don't  
> list any bugs that may be contributing to my problem. I glanced at the  
> OpenSSH changelogs, but I don't have time right now to look through  
> them extensively. If anyone has any ideas I would appreciate the help.  
> I am new to SSH and I'm trying to configure this server so I can access  
> it from school over the Internet. Are keypairs the only secure way to  
> authenticate using SSH? If not, what are my other options? Either way I  
> would still prefer to use keypairs to prevent others from easily  
> compromising my server.  
>  
> P.S.  
> I would appreciate suggestions being emailed to me in addition to being  
> posted on the newsgroup. I'm not sure when I will have a chance to  
> check the newsgroup again.  
>  
> LinuxManMikeC  
> LinuxManMikeC@netscape.net

Most common problem I encounter with pub/priv keys is the permissions on authorized\_keys and ~/.ssh (remote) or even ~/.ssh/identity (local)

Something like should work:

```
[test@remote .ssh]$ ls -la
total 12
drwx----- 2 test test 4096 Dec 21 21:00 .
drwx----- 4 test test 4096 Jan 30 18:20 ..
-r----- 1 test test 1490 Dec 21 21:00 authorized_keys
```

comp.security.ssh: Re: Trouble with OpenSSH 3.4p1 – Can't connect with an RSA key pair

```
[test@remote .ssh]$
```

and

```
[test@local .ssh]$ ls -la
total 28
drwx----- 2 test test 4096 Aug 27 21:31 .
drwx----- 59 test test 4096 Jan 31 10:58 ..
-r----- 1 test test 3311 Aug 10 18:10 identity
-rw----- 1 test test 1572 Dec 10 21:12 known_hosts
[test@local .ssh]$
```

If you run the server in debug mode, you will most likely find your answer.

On another point, passwords are never exchanged in plain text using SSH.

There is nothing particularly unsafe about using password authentication, so long as you stick to good practices like changing your "non trivial" password regularly. You are afforded a little more security using pub/priv keys by the fact that an attacker would need to key log you AND steal your private key file. If you are really worried, you might like to use one time passwords. It is a balance of how much inconvenience you are prepared to put up with versus how likely it is that anybody would expend that much effort to hack your PC.

You should upgrade your OpenSSH to the latest 3.7x something. I was never able to find decent rpms for anything past 3.4, so you may be resigned to downloading the source and compiling.

Mike