

comp.security.ssh: I cannot connect with keys to ssh server from openssh client

I cannot connect with keys to ssh server from openssh client

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-01/0266.html>

From: Ray Kinney (*samkinney_at_excite.com*)

Date: 01/29/04

Date: 28 Jan 2004 15:45:31 -0800

I created RSA key on a Sun solaris 8 with OpenSSH3.6.1p1 and OpenSSL 0x0090702f:

```
ssh-keygen -trsa -fmysshkey -N ""
```

I translated to ssh:

```
ssh-keygen -e -fmysshkeypub >mysshkey_ssh2.pub
```

I copied my mysshkey_ssh2.pub to the .ssh2 directory of the server.

I created an authorization file:

```
echo 'Key mysshkey_ssh2.pub' > authorization
```

when I try to connect to the server:

```
ssh -vvv -2 -i mysshkeygen -l xxxxxxxx xxxx.xxxxxxxxxx.xxx
```

in the log i receive:

```
debug1: Found key in /secureftp/.ssh/known_hosts:1
```

```
debug2: bits set: 511/1024
```

```
debug1: ssh_dss_verify: signature correct
```

```
debug2: kex_derive_keys
```

```
debug2: set_newkeys: mode 1
```

```
debug1: SSH2_MSG_NEWKEYS sent
```

```
debug1: expecting SSH2_MSG_NEWKEYS
```

```
debug2: set_newkeys: mode 0
```

```
debug1: SSH2_MSG_NEWKEYS received
```

```
debug1: SSH2_MSG_SERVICE_REQUEST sent
```

```
debug2: buggy server: service_accept w/o service
```

```
debug1: SSH2_MSG_SERVICE_ACCEPT received
```

```
debug1: Authentications that can continue: publickey,password,hostbased
```

```
debug3: start over, passed a different list publickey,password,hostbased
```

```
debug3: preferred publickey,keyboard-interactive,password
```

```
debug3: authmethod_lookup publickey
```

```
debug3: remaining preferred: keyboard-interactive,password
```

```
debug3: authmethod_is_enabled publickey
```

```
debug1: Next authentication method: publickey
```

```
debug1: Offering public key: mysshkey
```

```
debug3: send_pubkey_test
```

```
debug2: we sent a publickey packet, wait for reply
```

```
debug2: input_userauth_pk_ok: SSH_BUG_PKOK
```

```
debug1: Server accepts key: pkalg ssh-rsa blen 149 lastkey 63eb0 hint 0
```

```
debug2: input_userauth_pk_ok: fp 0b:56:48:eb:d4:ac:2b:ea:62:04:33:bf:ef:bb:bc:fb
```

comp.security.ssh: I cannot connect with keys to ssh server from openssh client

debug3: sign_and_send_pubkey

debug1: read PEM private key done: type RSA

debug1: Authentications that can continue: publickey,password,hostbased