

Re: Public Key Authentication

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-06/0285.html>

From: jon (jonsnews_at_hotmail.com)

Date: 06/27/03

Date: 27 Jun 2003 03:29:15 -0700

Markus, this is a common enough problem when connecting from SSH Comms or F-Secure boxes TO a nice OpenSSH box...

SSH & F-Secure gen keys in the same way, e.g..for DSA...

```
jon@sshbox $ ssh-keygen -t dsa -b 2048
```

```
<add passphrase>
```

...which produces, by default, a public key file called

id_dsa_2048_a.pub whose contents look like this...

```
----- BEGIN SSH2 PUBLIC KEY -----
```

Subject: jon

Comment: "2048-bit dsa, jon@sshbox, Fri Jun 27 2003 10:01:36"

```
AAAAB3NzaC1kc3MAAAEBAOCdFNWPNw/zc3Tne8wqoJbbe/+lukPwl/ez9ip9kXFaxiVf9+
prwc6baGnwBnwOr6LWsMec7pkVXFawgzKz4ydo1xwPTKfFxChWUAFx5nb0opWt4+1uKG4
WgaWQHsWj6MoKGO+8itgPWiyIh60tTcqPhnRCKvCzcGEhiQONvm52YbauXAYM/IOLRnz3G
Ri7kKC0y6DO+u1bajpkOfmo4qUIKnsFOqmFG1ZV5FwpgOYhZngcpMGuvllGxOenTrVkfHq
Tzg3jhHNQdobaZTQ4E67L+X+VvKNsCsmMC9RCPm7ACD9Uj5JQItAztw7aow2FNzzFOpofk
fK4jhb733oY+kAAAAVAOerYHC8QqHBrfccZ0HIO7zp1SR3AAABAQCh3/g4FbYUWKjssuMO
V0gaPItU6szjnhazKRIdenFH1ORZ3E7ksQI5D3MTd/t3jztqn0LaKZ5brvSzNpJZIUkV+
w+Z/TU+9wVpcF+cd9XGoKqTSXSfs6Ga5zy9fpY35jrdGjU86ueRV9pVWOZpdSNwBR4zBM1
qO1RDck/FPZFLP6mbmc4l5abGL6jwKfovuMQ319EbfXrVvU17Nh65j7S626s/vASxFbS7x
TQP3cs587DTgG9R7kEu1AT/o75XcurCFr2Nv9d3N7nR6sLP4rpICcuTfFWC53tHqYjJe8l
fuSdQMKpHaNsT8w/ccdTRyWJMSHhXv6xkkbQmEGsmw7pAAABAQCQ0nio5fh9YjKBT9i0g9
XcIWMnl0e2GvCTYTxjAXMzUwMvjaN0CkyoMQGpEp8OjrdwuaZ3pHxOuHzrv6mBeCOF9AXn
+uK6m6FybuuVUPxC3Yw4eCRMxcXvXwvIG1Zd7452UN5Yfc5sqZQC2rRkJ9XniiTYvoR7T
SrXho1SORTEB9+St0KbvZdkyvcMRScgz42IU2cWc/XFJOjBO6vU01DboC8SWMJHn16fBPo
7q12DXaJDJTrJpnJLpkBA2xVzkM1dXEbJfyxzuO0ntdsIW7gCp10wqUZTQ6FWX28mIoFNE
PF/FQfO7+toB4aNMGcYfAHQv0jDmpT0IaBEI5t+Tw6
----- END SSH2 PUBLIC KEY -----
```

Now, you've got to copy the public key to the OpenSSH box & convert it. I think this is where you may have gone wrong?!? I'd do something like this...

```
jon@sshbox$ scp id_dsa_2048_a.pub jon@openssh:..ssh/jon.sshbox.pub
<enter password for jon@openssh>
...i.e. call the file something descriptive.
```

comp.security.ssh: Re: Public Key Authentication

Also add an entry "IdKey id_dsa_2048_a" to the identity file, which you have done OK.

Now jump onto the OpenSSH box & convert the key...

```
jon@openssh $ cd ~/.ssh
jon@openssh $ ssh-keygen -i -f jon.sshbox.pub >> authorized_keys
...all it does is remove comments, add 'ssh-dss' at the front and
remove end-of line characters. You can add a comment at the end of
the key for readability...e.g...(read in wide screen)...
ssh-dss
AAAAB3NzaC1kc3MAAAEBAOCdFNWPnW/zc3Tne8wqoJbbE/+lukPwl/ez9ip9kXFaxiVf9+prwc6baGnwBnwOr6
SR3AAABAQCh3/g4FbYUWKlssuMOV0gaPItU6szjnhazKRIdenFh1ORZ3E7kSQI5D3MTd/t3jztqn0LaKZ5brvSzN
MvjaN0CkyoMQGpEp8OjrdwuaZ3pHxOuHzrv6mBeCOF9AXn+uK6m6FybuuVUpxC3Yw4eCRMxcxVcXwvIG1Zd
jon@sshbox
```

Now, you should be ready for action. Go back to the SSH box & try connecting to the OpenSSH box. You should get prompted for your key's passphrase (if you supplied one) and get logged in OK. e.g...

```
jon@sshbox $ ssh jon@openssh
jon@openssh $
```

...if not, post the output from 'ssh -vvv'. Better still, move all your boxes to OpenSSH :-)

NOTE: A word of warning – you cannot use RSA keys between SSH/F–Secure boxes & OpenSSH. ssh-keygen doesn't seem to convert the keys properly. You will only notice why it doesn't work if you run the OpenSSH Server in debug (sshd -d). e.g...you'd see...

```
Found matching RSA key:
fa:92:5c:83:94:79:a6:e7:91:c9:10:ac:b3:a0:9e:b6
debug1: restore_uid: 0/1
bad decrypted len: 34 != 20 + 15
debug1: ssh_rsa_verify: signature incorrect
```