

Name \_\_\_\_\_ /20 pts.

## SE 4C03 Winter 2003

### Lab Exercise 4

Instructor: William M. Farmer

Revised: 06 March 2003

Assigned: 07 March 2003  
Lab report due: 21 March 2003

Do this lab exercise by yourself.

Configure your account to use public key authentication with the Secure Shell network service.

1. Suppose your account name is *a*. Ask one of the other groups in the class to give you an account named *a* on their host. (Do not use the **intruder** account for this purpose.) Let *x* denote your host and *y* denote the other host. \_\_\_\_\_ / 2 pts.
2. Use the command

`ssh-keygen -d`

to create a DSA public key pair for your account on *x* (and an `.ssh` directory). You will have to enter a passphrase which will be used to encrypt/decrypt your private key. Name the private and public key files `id_dsa` and `id_dsa_x.pub`, respectively. Do the same on host *y*. \_\_\_\_\_ / 3 pts.

3. On both *x* and *y*, create a file named `authorized_key2` in the `.ssh` directory. Make these two files readable and writeable by the owner only, and then put in both of them the contents of `id_dsa_x.pub` and `id_dsa_y.pub`. \_\_\_\_\_ / 3 pts.
4. Test the set up by executing

`ssh -v ax`

on host  $x$  where  $a_x$  is one of the two IP addresses of  $x$ . Authenticate yourself with your passphrase instead of your password. The `-v` option for “verbose” will show each step of the process of creating an Secure Shell communication channel from your computer to itself. After the communication channel is established, try starting an X Windows client like `xterm` or `netscape`. \_\_\_\_\_/ 4 pts.

5. Test the set up by executing

```
ssh -v ax
```

on host  $y$ . Authenticate yourself with your passphrase instead of your password. After the communication channel is established, try starting an X Windows client like `xterm` or `netscape`. \_\_\_\_\_/ 4 pts.

6. Test the set up by executing

```
ssh -v ay
```

on host  $x$ . Authenticate yourself with your passphrase instead of your password. After the communication channel is established, try starting an X Windows client like `xterm` or `netscape`. \_\_\_\_\_/ 4 pts.

7. **Demonstrate your set up of Secure Shell with public key authentication to one of the TAs. After you are done with the demonstration, give the TA your lab report consisting of the two sheets of this exercise and a copy of your log book.**