

Name\_\_\_\_\_

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

## SE 4C03 Winter 2006

### Lab Exercise 4

Instructor: William M. Farmer

Revised: 10 March 2006

Assigned: 10 March 2006

Lab report due: 14 March 2006

Do this lab exercise with your partner.

Configure your account on the Little Internet to use public key authentication with the Secure Shell network service (**ssh**).

1. Let  $n$  be your or your partner's account name. Ask one of the teams managing a host directly connected to your host to give you an account named  $n$  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 -t rsa
```

to create an RSA 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\_rsa** and **id\_rsa.x.pub**, respectively. Do the same on host  $y$ .

\_\_\_\_\_/ 3 pts.

3. On both  $x$  and  $y$ , create a file named **authorized\_keys** 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\_rsa.x.pub** and **id\_rsa.y.pub**.

\_\_\_\_\_/ 3 pts.

4. Test the set up by executing

```
ssh -v a_x
```

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 a Secure Shell communication channel from your computer to itself. Verify that the communication channel is established. \_\_\_\_\_/ 4 pts.

5. Test the set up by executing

```
ssh -v a_x
```

on host  $y$ . Authenticate yourself with your passphrase instead of your password. Verify that the communication channel is established. \_\_\_\_\_/ 4 pts.

6. Test the set up by executing

```
ssh -v a_y
```

on host  $x$ . Authenticate yourself with your passphrase instead of your password. Verify that the communication channel is established. \_\_\_\_\_/ 4 pts.

7. Demonstrate your set up of Secure Shell with public key authentication to the TA.

For your team’s lab report, hand in these two sheets. You must also turn in a paper copy of each team member’s log book no later than the beginning of the lecture on March 16, 2006. If your log book is missing or incomplete, 4 points will be deducted from your mark. *You and your partner must hand the lab report in together before the end of the lab session. If you do not attend the lab session or leave the lab before handing in the lab report, you will receive a mark of 0 for the lab exercise.*