Lab 13.1: Using RSA Keys With PuTTY
IN618 Security

May 28, 2015

Introduction

We regulary use PuTTY to connect to remote servers using SSH. SSH in an encrypted network protocol so we don't have to worry about a third party intercepting our packets and capturing data. There is still a weakness, however, in the way we have used it. We send our password to the remote server for authentication. Why is this an issue? Think about this so we can discuss it later.

In this lab we will see how to create and use RSA keys to authenticate so that we do not have to use passwords.

1 Generate your keys

We will generate our RSA keys using the PuTTYgen utility. If it is not on the lab machines, you can download it from `;http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`. Carry out the following steps:

1. Start the PuTTYgen utility;
2. For Type of key to generate, select SSH-2 RSA;
3. In the Number of bits in a generated key field, specify 2048 or 4096 (You can use more bits. A longer key is harder to break.);
4. Click the Generate button;
5. Move your mouse pointer around in the blank area of the Key section, below the progress bar to generate some entropy until the progress bar is full;
6. A private/public key pair has now been generated;
7. In the Key comment field, enter any comment you'd like, to help you identify this key pair, later (e.g. your e-mail address.)
8. You can enter a passphrase that will be required when you use the keys, but for this lab leave the passphrase blank.
9. Click the Save public key button and name your file `id_rsa.pub`).
10. Click the Save private key button and name it `id_rsa` (You can save it in the same location as the public key, but it should be a location that only you can access and that you will not lose.);
11. Right-click in the text field labeled "Public key for pasting into OpenSSH authorized_keys file" and choose Select All; Right-click again in the same text field and choose Copy.

2 Copy your public key on the server

To place your public key on the server, excute the following steps:

1. Log onto the lab server as directed by the lecturer;
2. Create your `.ssh` directory in your home directory:

   ```
   mkdir ~/.ssh
   chmod 0700 ~/.ssh
   touch ~/.ssh/authorized_keys
   chmod 0644 ~/.ssh/authorized_keys
   ```

3. You will copy your key into the `authorized_keys` file;
4. Enter the command `vi ~/.ssh/authorized_keys`;
5. Tap the i key on your keyboard and right-click your mouse to paste;
6. Press escape, then enter `ZZ`.

3 Set up a profile in PuTTY

You can save session information in PuTTY so that it will use you keys and so that you don't have to reenter the same information all the time.

1. Start PuTTY;
2. In the Host Name field, enter the IP address of our server;
3. Enter 22 in the Port field;
4. Select SSH under Protocol;
5. Along the left-hand side of the window, select the Data sub-category, under Connection;
6. Specify your username in the Auto-login username field;
7. Expand the SSH sub-category, under Connection;
8. Highlight the Auth sub-category and click the Browse button, on the right-hand side of the PuTTY window;
9. Browse your file system and select your previously-created private key;
10. Return to the Session Category and enter a name for this profile in the Saved Sessions field;
11. Click the Save button for the Load, Save or Delete a stored session area.

Now you can log in without entering a password.

4 Conclusions

If every user on a system is using RSA keys, then it's possible to disable password based logins entirely. What are some advantages to this?