Previous | Contents | Index | Next

Chapter 9: Using Pageant for authentication

Pageant is an SSH authentication agent. It holds your private keys in memory, already decoded, so that you can use them often without needing to type a passphrase.

9.1 Getting started with Pageant

Before you run Pageant, you need to have a private key in `*.PPK` format. See chapter 8 to find out how to generate and use one.

When you run Pageant, it will put an icon of a computer wearing a hat into the System tray. It will then sit and do nothing, until you load a private key into it.

If you click the Pageant icon with the right mouse button, you will see a menu. Select ‘View Keys’ from this menu. The Pageant main window will appear. (You can also bring this window up by double-clicking on the Pageant icon.)

The Pageant window contains a list box. This shows the private keys Pageant is holding. When you start Pageant, it has no keys, so the list box will be empty. After you add one or more keys, they will show up in the list box.

To add a key to Pageant, press the ‘Add Key’ button. Pageant will bring up a file dialog, labelled ‘Select Private Key File’. Find your private key file in this dialog, and press ‘Open’.

Pageant will now load the private key. If the key is protected by a passphrase, Pageant will ask you to type the passphrase. When the key has been loaded, it will appear in the list in the Pageant window.

Now start PuTTY and open an SSH session to a site that accepts your key. PuTTY will notice that Pageant is running, retrieve the key automatically from Pageant, and use it to authenticate. You can now open as many PuTTY sessions as you like without having to type your passphrase again.

(PuTTY can be configured not to try to use Pageant, but it will try by default. See section 4.20.2 and section 3.8.3.9 for more information.)

When you want to shut down Pageant, click the right button on the Pageant icon in the System tray, and select ‘Exit’ from the menu. Closing the Pageant main window does *not* shut down Pageant.

9.2 The Pageant main window

The Pageant main window appears when you left-click on the Pageant system tray icon, or alternatively right-click and select ‘View Keys’ from the menu. You can use it to keep track of what keys are currently loaded into Pageant, and to add new ones or remove the existing keys.

9.2.1 The key list box

The large list box in the Pageant main window lists the private keys that are currently loaded into Pageant. The list might look something like this:

```
ssh1    1024 22:c3:68:3b:09:41:36:c3:39:83:91:ae:71:b2:0f:04 k1
ssh-rsa 1023 74:63:08:82:95:75:e1:7c:33:31:bb:cb:00:c0:89:8b k2
```

For each key, the list box will tell you:

- The type of the key. Currently, this can be `ssh1` (an RSA key for use with the SSH-1 protocol), `ssh-rsa` (an RSA key for use with the SSH-2 protocol), or `ssh-dss` (a DSA key for use with the SSH-2 protocol).
- The size (in bits) of the key.
- The fingerprint for the public key. This should be the same fingerprint given by PuTTYgen, and (hopefully) also the same fingerprint shown by remote utilities such as `ssh-keygen` when applied to your `authorized_keys` file.
- The comment attached to the key.

9.2.2 The ‘Add Key’ button

To add a key to Pageant by reading it out of a local disk file, press the ‘Add Key’ button in the Pageant main window, or alternatively right-click on the Pageant icon in the system tray and select ‘Add Key’ from there.

Pageant will bring up a file dialog, labelled ‘Select Private Key File’. Find your private key file in this dialog, and press ‘Open’. If you want to add more than one key at once, you can select multiple files using Shift-click (to select several adjacent files) or Ctrl-click (to select non-adjacent files).

Pageant will now load the private key(s). If a key is protected by a passphrase, Pageant will ask you to type the passphrase.

(This is not the only way to add a private key to Pageant. You can also add one from a remote system by using agent forwarding; see section 9.4 for details.)

9.2.3 The ‘Remove Key’ button

If you need to remove a key from Pageant, select that key in the list box, and press the ‘Remove Key’ button. Pageant will remove the key from its memory.

You can apply this to keys you added using the ‘Add Key’ button, or to keys you added remotely using agent forwarding (see section 9.4); it makes no difference.

9.3 The Pageant command line

Pageant can be made to do things automatically when it starts up, by specifying instructions on its command line. If you're starting Pageant from the Windows GUI, you can arrange this by editing the properties of the Windows shortcut that it was started from.

If Pageant is already running, invoking it again with the options below causes actions to be performed with the existing instance, not a new one.

9.3.1 Making Pageant automatically load keys on startup

Pageant can automatically load one or more private keys when it starts up, if you provide them on the Pageant command line. Your command line might then look like:

```
C:\PuTTY\pageant.exe d:\main.ppk d:\secondary.ppk
```

If the keys are stored encrypted, Pageant will request the passphrases on startup.

If Pageant is already running, this syntax loads keys into the existing Pageant.

9.3.2 Making Pageant run another program

You can arrange for Pageant to start another program once it has initialised itself and loaded any keys specified on its command line. This program (perhaps a PuTTY, or a WinCVS making use of Plink, or whatever) will then be able to use the keys Pageant has loaded.

You do this by specifying the `-c` option followed by the command, like this:

```
C:\PuTTY\pageant.exe d:\main.ppk -c C:\PuTTY\putty.exe
```

9.4 Using agent forwarding

Agent forwarding is a mechanism that allows applications on your SSH server machine to talk to the agent on your client machine.

Note that at present, agent forwarding in SSH-2 is only available when your SSH server is OpenSSH. The `ssh.com` server uses a different agent protocol, which PuTTY does not yet support.

To enable agent forwarding, first start Pageant. Then set up a PuTTY SSH session in which ‘Allow agent forwarding’ is enabled (see section 4.20.5). Open the session as normal. (Alternatively, you can use the `-A` command line option; see section 3.8.3.10 for details.)

If this has worked, your applications on the server should now have access to a Unix domain socket which the SSH server will forward back to PuTTY, and PuTTY will forward on to the agent. To check that this has actually happened, you can try this command on Unix server machines:

```
unixbox:~$ echo $SSH_AUTH_SOCK
/tmp/ssh-XXNP18Jz/agent.28794
unixbox:~$
```

If the result line comes up blank, agent forwarding has not been enabled at all.

Now if you run `ssh` on the server and use it to connect through to another server that accepts one of the keys in Pageant, you should be able to log in without a password:

```
unixbox:~$ ssh -v otherunixbox
[...]
debug: next auth method to try is publickey
debug: userauth_pubkey_agent: trying agent key my-putty-key
debug: ssh-userauth2 successful: method publickey
[...]
```

If you enable agent forwarding on *that* SSH connection as well (see the manual for your server-side SSH client to find out how to do this), your authentication keys will still be available on the next machine you connect to - two SSH connections away from where they're actually stored.

In addition, if you have a private key on one of the SSH servers, you can send it all the way back to Pageant using the local `ssh-add` command:

```
unixbox:~$ ssh-add ~/.ssh/id_rsa
Need passphrase for /home/fred/.ssh/id_rsa
Enter passphrase for /home/fred/.ssh/id_rsa:
Identity added: /home/fred/.ssh/id_rsa (/home/simon/.ssh/id_rsa)
unixbox:~$
```

and then it's available to every machine that has agent forwarding available (not just the ones downstream of the place you added it).

9.5 Security considerations

Using Pageant for public-key authentication gives you the convenience of being able to open multiple SSH sessions without having to type a passphrase every time, but also gives you the security benefit of never storing a decrypted private key on disk. Many people feel this is a good compromise between security and convenience.

It *is* a compromise, however. Holding your decrypted private keys in Pageant is better than storing them in easy-to-find disk files, but still less secure than not storing them anywhere at all. This is for two reasons:

- Windows unfortunately provides no way to protect pieces of memory from being written to the system swap file. So if Pageant is holding your private keys for a long period of time, it's possible that decrypted private key data may be written to the system swap file, and an attacker who gained access to your hard disk later on might be able to recover that data. (However, if you stored an unencrypted key in a disk file they would *certainly* be able to recover it.)
- Although, like most modern operating systems, Windows prevents programs from accidentally accessing one another's memory space, it does allow programs to access one another's memory space deliberately, for special purposes such as debugging. This means that if you allow a virus, trojan, or other malicious program on to your Windows system while Pageant is running, it could access the memory of the Pageant process, extract your decrypted authentication keys, and send them back to its master.

Similarly, use of agent *forwarding* is a security improvement on other methods of one-touch authentication, but not perfect. Holding your keys in Pageant on your Windows box has a security advantage over holding them on the remote server machine itself (either in an agent or just unencrypted on disk), because if the server machine ever sees your unencrypted private key then the sysadmin or anyone who cracks the machine can steal the keys and pretend to be you for as long as they want.

However, the sysadmin of the server machine can always pretend to be you *on that machine*. So if you forward your agent to a server machine, then the sysadmin of that machine can access the forwarded agent connection and request signatures from your private keys, and can therefore log in to other machines as you. They can only do this to a limited extent - when the agent forwarding disappears they lose the ability - but using Pageant doesn't actually *prevent* the sysadmin (or hackers) on the server from doing this.

Therefore, if you don't trust the sysadmin of a server machine, you should *never* use agent forwarding to that machine. (Of course you also shouldn't store private keys on that machine, type passphrases into it, or log into other machines from it in any way at all; Pageant is hardly unique in this respect.)

If you want to provide feedback on this manual or on the PuTTY tools themselves, see the Feedback page.

[PuTTY release 0.60]