

# Using Putty on Windows to login Linux securely via OpenSSH

- Submitted by: Man-wai CHANG
- Update by: Man-wai CHANG
- Date Submitted: 31 May 2006
- Document Version: 1.0
- Last Updated: 02/02/2008 17:46:43

This is a guide about using Putty on Windows with OpenSSH on Linux. You would learn about how to:

- configure OpenSSH on linux side to accept version 2 public-key authentication.
- create public and private keys with OpenSSH on the linux side,
- convert OpenSSH keys to Putty format using puttygen.exe at the Window side,
- use putty.exe to talk to OpenSSH using the converted private key.

I would assume that you have OpenSSH installed. As per 31-May-2006, the latest version of OpenSSH was 4.3p1. Your Linux distribution may likely use an older version, however.

# **Configuring OpenSSH to accept public-key authentication**

To enable your OpenSSH to accept version 2 public key, you would need to modify /etc/ssh/sshd\_config. You could use vi editor (or whatever editor you are familiar with) to uncomment/add/modify the following lines to /etc/ssh/sshd\_config:

```
# the default SSH port is 22, you could alter it if necessary
Port 22
# accept version 2 keys only
Protocol 2
# NEVER allow root to login directly over the net
PermitRootLogin no
StrictModes yes
MaxAuthTries 3
# enable public-key authentication
RSAAuthentication no
PubkeyAuthentication yes
# securing your OpenSSH
# do not use host-based authentication for security reason
RhostsRSAAuthentication no
HostbasedAuthentication no
IgnoreUserKnownHosts yes
PermitEmptyPassword no
# do not allow telnet-type login for security reason
```

```
ChallengeResponseAuthentication no PasswordAuthentication no
```

X11Forwarding yes X11DisplayOffset 10

After you have made changes to /etc/ssh/sshd\_config, you would need to restart the OpenSSH daemon by executing `/etc/init.d/ssh restart` (on Ubuntu).

### Generating OpenSSH private and public key pair

To use public key authentication, the first step is to generate a pair of private and public keys on the Linux side. I would assume that you login as a user called "toylet".

```
1. Login Linux as user "toylet". You could do it at the Linux console
  or via telnet.
2. Execute `ssh-keygen -t rsa` to generate a version 2 public
  and private key pair into directory /home/user/.ssh.
  The passphrase is optional (but preferred).
toylet@server:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/toylet/.ssh/id rsa):
/home/toylet/.ssh/id rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/toylet/.ssh/id rsa.
Your public key has been saved in /home/toylet/.ssh/id rsa.pub.
The key fingerprint is:
ec:f4:3f:b5:fe:2f:de:22:6c:42:8c:38:ad:6c:5e:96 toylet@server
3. Execute `cd /home/toylet/.ssh`
4. You should see 2 files: id rsa and id rsa.pub.
  Now execute the following command:
```

#### 5. Copy /home/toylet/.ssh/id\_rsa from Linux to Windows.

cp id rsa.pub authorized keys

#### Converting the OpenSSH private key to Putty format

Next, we head to the Windows side. In step 4, you created two key files (id\_rsa and id\_rsa.pub). Putty cannot directly open OpenSSH keys. We need to convert id\_rsa to id\_rsa.ppk using a program called puttygen.exe.

```
6. At the Windows side, download puttygen.exe from <u>Putty website</u>.7. Execute puttygen.exe
```

PuTTY Key Generator		
e Key Conversions Help Load private key Save public key Save private key		
Exit		
Actions		Generate
Generate a public/private key pair		Generate
		Load
Generate a public/private key pair	Save pyblic ke	Load
Generate a public/private key pair Load an existing private key file	Save pyblic ke	Load
Generate a public/private key pair Load an existing private key file Save the generated key		Load

 Click File->Load Private Key, load the file "id\_rsa" from Step 5. Enter the passphrase if you used it in step 2.

PuTTY Key Genera	tor		
ile <u>K</u> ey Con <u>v</u> ersion	s Help		
-Key Dublic key (or pactice	a into OpenSSH authorized k	unum film:	
ssh-rsa AAAAB3NzaC1yc2E wLeaYZP1tP0pUXtN MEIzgAzNIINs4sz3fN	AAAABIwAAAQEAs8CWVG WARUX7SeRDP4VEhTEc/ //mwr8GmjfLbS7EIP190vX28n /WOVsAki+JAjtcD9LgIWhJJi	ql+v5q+ojQebFcVoTiDj cenYZ3K9giAzfwOkOhn xAB9dKrNlzjNJPY8oIM8	4vmxVeq6k48z8RE
Key fingerprint	ssh-rsa 2048 76:f0:95:76:	1c:78:5e:77:52:34:72:68:t	9:86:55:48
Key <u>c</u> omment	imported-openssh-key		
Key p <u>a</u> ssphrase:			
Confirm passphrase:	Ananana		
Actions			
Generate a public/pri	ivate key pair		Generate
Load an existing priv	ate key file		Load
Save the generated I	key	Save p <u>u</u> blic key	Save private key
Parameters			
Type of key to gener	ate:	⊂ ss⊦	12 <u>D</u> SA
	and the second		1024

9. Now the key has been loaded as in the figure above. Hit the button "Save private key". The converted key would be saved as "id\_rsa.ppk".

## Logging in Openssh using id\_rsa.ppk

Download putty.exe from <u>Putty website</u>. It's time to really login OpenSSH using putty.exe on Windows side. The steps here would be a little bit more complicated.

10. Invoke putty.exe
10.1. Click "Session" in the sidebar.

Putty Configuration		×
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation	192.168.1.2     2       Protocol:     C       Baw     C       Load, save or delete a stored session	
- Selection - Colours - Data - Proxy - Telnet - Rlogin - SSH - Kex	Saved Sessions Default Settings	Load Sa⊻e Delete
– Auth – X11 – Tunnels – Bugs	Close <u>w</u> indow on exit. C Always C Never C Only on clean	exit
About	Open	Cancel

10.1.1. Enter ip address of your server (e.g., 192.168.1.2)
10.1.2. Click "SSH" in the Protocol option
10.2. Choose "SSH" under "Connection" in the sidebar

Category:	
B Session	Options controlling SSH connections
– Logging ⊟- Terminal – Keyboard – Bell	Data to send to the server Bemote command:
- Features - Window - Appearance - Behaviour - Translation - Colours - Connection - Dete	Protocol options ☐ Don't allocate a gseudo-terminal ☐ Don't start a shell or command at all ☐ Enable compression Preferred SSH protocol version: ☐ 1 only ☐ ☐ ☐ 2 ⓒ 2 only
- Data - Proxy - Telnet - Rlogin ■ SSH - Kex - Auth - X11 - Tunnels - Bugs	Encryption options Encryption cipher <u>s</u> election policy: AES (SSH-2 only) Blowfish 3DES - warn below here - DES C Enable legacy use of single-DES in SSH-2

# 10.2.1. In "Preferred SSH protocol version", select "2 only" 10.2.2. click "Auth" under "SSH"

Category:	-
<ul> <li>Session         <ul> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> </ul> </li> <li>Window         <ul> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> <li>Selection</li> <li>Colours</li> </ul> </li> <li>Connection         <ul> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Kex</li> <li>Auth</li> <li>X11</li> <li>Tunnels</li> <li>Bugs</li> </ul> </li> </ul>	Options controlling SSH authentication         Authentication methods         □ Attempt TIS or CryptoCard auth (SSH-1)         □ Attempt "keyboard-interactive" auth (SSH-2)         Authentication parameters         □ Allow agent forwarding         □ Allow attempted changes of username in SSH-2         Private key file for authentication:         D:\man.wai.chang\ssh\id_rsa.ppk

10.2.2.1. Hit the Browse button, select the file "id\_rsa.ppk" from Step 9. 10.3. hit "Session" again in step 10.1

Category:		
<ul> <li>Session         <ul> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> </ul> </li> </ul>	Basic options for your PuTTY's Specify your connection by host name or II Host Name (or IP address) [192.168.1.2 Protocol: C Baw C Telnet C Rlogin Load, save or delete a stored session	
- Selection - Colours - Data - Proxy - Telnet - Rlogin - SSH - Kex	Saved Sessions toylet.session Default Settings	Load Sa⊻e Delete
– Auth − X11 − Tunnels – Bugs	Close <u>w</u> indow on exit. C Always C Never C Only on	clean exit

10.3.1. Enter a name (e.g. "toylet.session") in the textbox directly under "Saved Sessions".

10.3.2. Hit the "Save" button. The name "toylet.session" would appear in the listbox of "Saved Sessions".



10.4. Double-click "toylet.session". Now you would be presented with a login screen for OpenSSH.10.4.1. Enter the linux user name "toylet"10.4.2. Enter the passphrase if you specified it in step 2.

```
Login as: toylet
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Last login: Wed May 31 12:35:00 2006 from 192.168.1.10
toylet@server:~$
```

11. You have successfully logged into your Linux server via OpenSSH.

# Epilogue

- You should change both your private and public keys periodically by repeating the steps above.
- You may disable the telnet daemon foreever since telnet doesn't encrypt the connection, allowing eavedropping easily.