

SSHell :)

christian.heinrich@cmlh.id.au
SAGE-AU - Sydney - 15 November 2011

Disclaimer

These slides are my own and not representative of any specific implementation.

Consider these lessons learned so that you don't repeat the same mistakes.

whoami

👁 <http://www.linkedin.com/in/ChristianHeinrich>

1. Windows (MCSE)
2. Slackware (August 1998)
 - 👁 Linux 1.x Monolithic Kernel
3. OpenBSD and Gentoo
4. Ubuntu (LiveCD) and OS X

Secure File Transfer

National Privacy Principals (NPP)

At Rest

• PGP/GPG, X.509, etc

In Transit

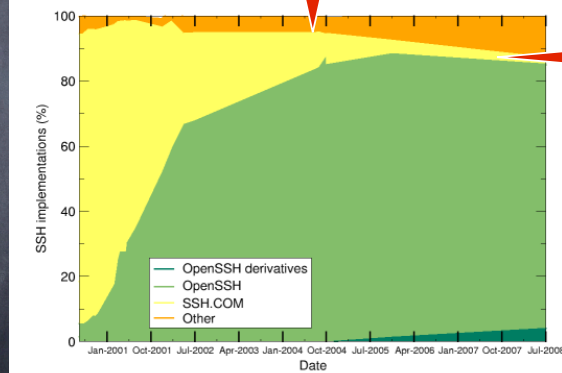
• SCP/SFTP (SSH), HTTPS (SSL/TLS), etc

OpenSSH - History

1. Free SSH v1.2.12 by Tatu Ylönen of ssh.com
2. OpenSSH v1.2.12 in OpenBSD 2.6
 - <ftp://ftp.pdc.kth.se/pub/krypto/ossh/>
 - Support Protocol SSH v1.3
3. OpenSSH (SSH v2) in OpenBSD 2.7
4. ssh.com attempts "chilling effect"

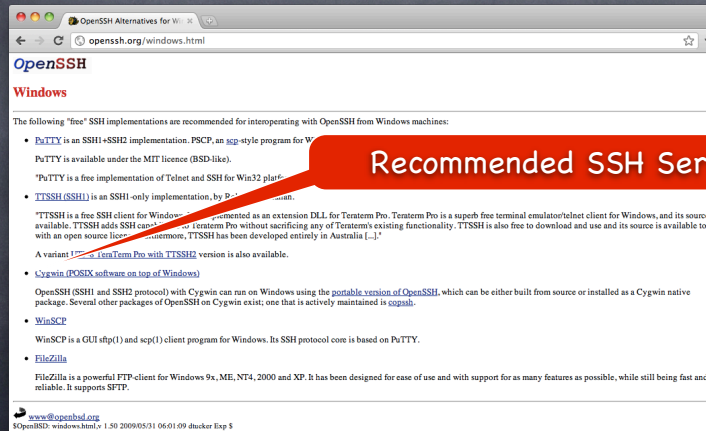
Usage - sshscan

Convert OpenSSH Key Format



OpenVMS

Windows



The screenshot shows a web browser window with the address bar displaying "openssh.org/windows.html". The page title is "OpenSSH Alternatives for Windows". The main heading is "OpenSSH Windows". Below this, a paragraph states: "The following 'free' SSH implementations are recommended for interoperating with OpenSSH from Windows machines:". A list of alternatives follows, including PuTTY, TeraTerm Pro, and Cygwin. A red callout box with the text "Recommended SSH Server" points to the "TTSSH (SSH)" link in the list.

OpenSSH

Windows


The following "free" SSH implementations are recommended for interoperating with OpenSSH from Windows machines:

- [PuTTY](#) is an SSH1+SSH2 implementation. PSCP, an scp-style program for Windows, is also available. PuTTY is available under the MIT licence (BSD-like).
"PuTTY is a free implementation of Telnet and SSH for Win32 platforms."
- [TTSSH \(SSH\)](#) is an SSH1-only implementation, by [Teraterm Pro](#).
"TTSSH is a free SSH client for Windows... implemented as an extension DLL for Teraterm Pro. Teraterm Pro is a superb free terminal emulator/telnet client for Windows, and its source is available. TTSSH adds SSH capabilities to Teraterm Pro without sacrificing any of Teraterm's existing functionality. TTSSH is also free to download and use and its source is available too, with an open source licence. Furthermore, TTSSH has been developed entirely in Australia [...]"
A variant [TeraTerm Pro with TTSSH2](#) version is also available.
- [Cygwin \(POSIX software on top of Windows\)](#)
OpenSSH (SSH1 and SSH2 protocol) with Cygwin can run on Windows using the [portable version of OpenSSH](#), which can be either built from source or installed as a Cygwin native package. Several other packages of OpenSSH on Cygwin exist; one that is actively maintained is [cypnsh](#).
- [WinSCP](#)
WinSCP is a GUI ftp(1) and scp(1) client program for Windows. Its SSH protocol core is based on PuTTY.
- [FileZilla](#)
FileZilla is a powerful FTP-client for Windows 9x, ME, NT4, 2000 and XP. It has been designed for ease of use and with support for as many features as possible, while still being fast and reliable. It supports SFTP.

[www.openssh.org](#)
40openssh/windows.html - 1.50 2008/05/31 06:01:09 ducker Exp 5

Recommended SSH Server

Transiting from FTP

1. scp  Don't use HTTPS/SSL

- sftp HERE Document

2. Public Key Auth or ssh-pass

- no passphrase

- ssh-agent or keychain

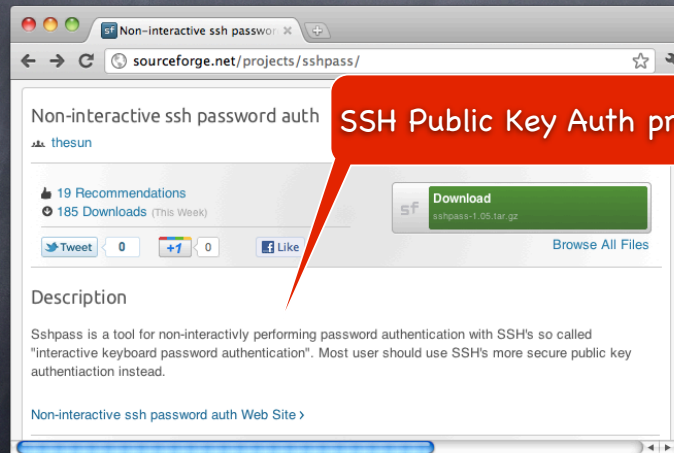
 cron

passphrase vs password

```
Terminal — bash — 80x24
osx:~ cmlh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/cmlh/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/cmlh/.ssh/id_rsa.
Your public key has been saved in /Users/cmlh/.ssh/id_rsa.pub.
The key fingerprint is:
ae:fa:0b:0d:34:59:63:76:56:e7:07:7b:41:f8:a6:b2 cmlh@osx.local
The key's randomart image is:
+--[ RSA 2048 ]-----+
|      = + 0.. 000 |
|      +   0.. 0   |
|      .+   00    |
|      .S   0     |
|      0 . . .    |
|      . . 0     |
|      . . E     |
|      .0+      |
+-----+
osx:~ cmlh$
```

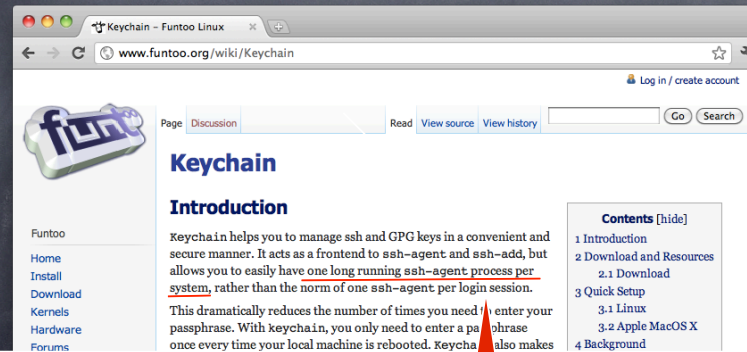
Decrypts SSH Key

ssh-pass



SSH Public Key Auth preferred

keychain



The screenshot shows a web browser window displaying the Funtoo Linux Wiki page for Keychain. The browser's address bar shows the URL `www.funtoo.org/wiki/Keychain`. The page features the Funtoo logo on the left, a navigation menu with links to Home, Install, Download, Kernels, Hardware, and Forums, and a search bar at the top right. The main content area is titled "Keychain" and includes an "Introduction" section. The introduction text states: "Keychain helps you to manage ssh and GPG keys in a convenient and secure manner. It acts as a frontend to `ssh-agent` and `ssh-add`, but allows you to easily have one long running `ssh-agent` process per system, rather than the norm of one `ssh-agent` per login session. This dramatically reduces the number of times you need to enter your passphrase. With keychain, you only need to enter a passphrase once every time your local machine is rebooted. Keychain also makes". To the right of the introduction is a "Contents" table of contents with links to Introduction, Download and Resources (including Download), Quick Setup (including Linux and Apple MacOS X), and Background.

Keychain helps you to manage ssh and GPG keys in a convenient and secure manner. It acts as a frontend to `ssh-agent` and `ssh-add`, but allows you to easily have one long running `ssh-agent` process per system, rather than the norm of one `ssh-agent` per login session. This dramatically reduces the number of times you need to enter your passphrase. With keychain, you only need to enter a passphrase once every time your local machine is rebooted. Keychain also makes

```
SSH_AGENT_PID=/tmp/ssh-XXXXXXX/agent.pid
```

SFTP

scp is preferred
i.e. wildcards are static

```
1.sftp user@host << SFTP  
2.put *  
3.bye  
4.SFTP
```

HERE Documents

Questions

Latest Slides available from:

- <http://www.slideshare.net/cmlh>
- <https://github.com/cmlh/ssh>

Contact Information: <http://cmlh.id.au/contact>