OpenSSH: A Telnet Replacement

Presented by

Aaron Grothe

Heimdall Linux, Inc.

Overview

Questions
Top 5 Rejected Presentation Titles
History of OpenSSH
What OpenSSH offers
How OpenSSH differs from SSH
Why OpenSSH?
Diagram of an OpenSSH connection
Where to get OpenSSH
Installing OpenSSH
Demonstration
Q & A

Questions

How many of you use telnet to connect to remote computers?

How many of you use pop-3 to access a remote mailbox over the internet?

How many of you use non-anonymous ftp to access remote machines?

Top 5 Rejected Presentation Titles

Telnet Must Die
Poor Man's VPN
Welcome to Telnet, You've Been Hacked
OpenSSH Good
OpenSSH Choice of a New Generation

History of OpenSSH

Secure Shell (SSH) was developed by Tatu Ylönen as a replacement for the BSD "r-commands", rsh, rlogin, rcp

SSH can also be used as a replacement for telnet and ftp

SSH can also be used for port forwarding/encrypting regular tcp traffic (E.g. Pop-3, X11, etc)

History of OpenSSH (2)

SSH was originally released with a very liberal license

SSH inc. was formed to take care of the commercialization of SSH

Over time SSH's license became more restrictive

- For almost any commercial use you needed a license

History of OpenSSH (3)

Björn Grönvall took an early version of SSH (v1.2) with the more liberal license and began to release patches/updates to it

Björn called his product OSSH

Added support for SSH protocol v1.5

OSSH available at ftp://ftp.pdc.kth.se/pub/krypto/ossh/

History of OpenSSH (4)

The OpenBSD group needed a replacement for the BSD r-commands, so they decided to create OpenSSH based upon OSSH

The OpenBSD group has put the whole of the OpenSSH source code as used in OpenBSD through a through code review

History of OpenSSH (5)

The OpenBSD group decided to create a version of OpenSSH that would be portable to a variety of operating systems (AIX, SCO UNIX, Linux, Windows, etc.)

OpenBSD uses the SSL libraries created by the OpenSSL group http://www.openssl.org to create the portable version

What OpenSSH offers

OpenSSH is an Open Source replacement for both SSH and everything SSH can replace

OpenSSH implements v2 of the SSH protocol (defined as an RFC-draft)

How OpenSSH differs from SSH

OpenSSH is Open Source
OpenSSH has an active user community for support
OpenSSH is free to use
SSH offers commercial support contracts
SSH has recently revised their license to allow for more free use on Linux and BSD platforms
SSH is a commercial product with all the pros and cons associated with that

Why OpenSSH?

The SSH protocol encrypts all traffic between machines are encrypted. Telnet does not encrypt any information, passwords and account ids are passed in the clear.

OpenSSH is a free program implementing the SSH protocol

OpenSSH has been reviewed by a team of security experts to reduce the number of bugs in it

Diagram of an SSH session

2 machines Home and Work exist connected by a network

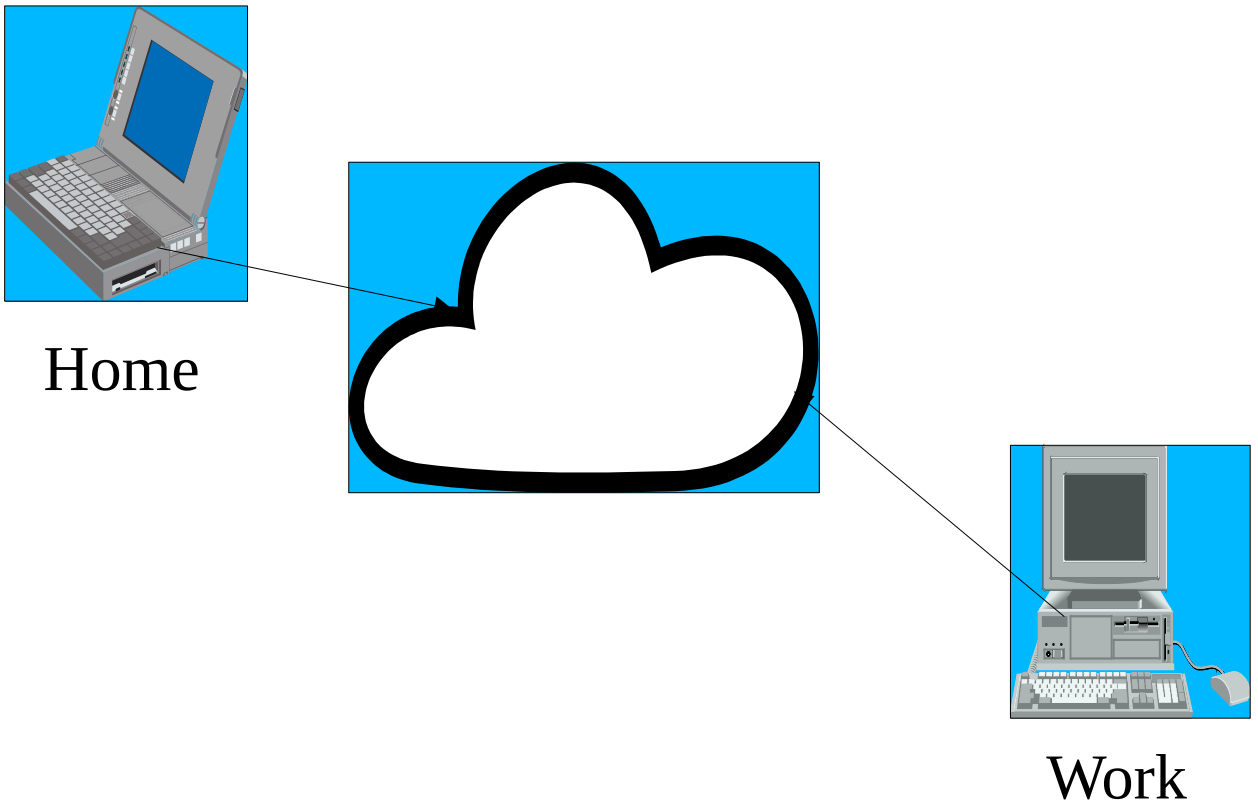

Diagram of an SSH session

A User on home wants to login into Work remotely
On home the user enters the command

```
# ssh work
```

Home connects to Work and compares the key for Work it has in its local database.
If the key doesn't exist it asks the user if they want to accept the key Work is offering
The user accepts the key or the key stored on the system is retrieved

Diagram of an SSH session (2)

A session key is negotiated between the two systems
Home then asks the user for the account password on Work if necessary
The login information is then used an attempt to login is performed

OpenSSH & Patents

RSA The RSA patent has expired, allowing the free use of their algorithms

IDEA still has some restrictions in Europe, the OpenSSH directions detail how to compile OpenSSH to not use that algorithm if needed

Demonstration (telnet & rlogin)

Using OpenSSH as a replacement for telnet and rlogin
Acess remote machine from local machine

```
# ssh work
```

Demonstration (rsh)

Using OpenSSH as a replacement for rsh

Perform a command on the remote command

```
# ssh work ls
```

Demonstration (rcp)

Using OpenSSH as a replacement for rcp

Copy a file from the remote machine to my local machine

```
# scp work:/testfile .
```

Demonstration (ftp)

Using OpenSSH as a replacement for ftp

To replace ftp you need to use xbill http://www.xbill.org/sftp

```
# sftp work

# ls

# get filename

# close
```

Demonstration (X11 forwarding)

Using OpenSSH as a replacement for to automatically encrypt forward an X11 session

Start a session on the remote machine and pop up an application like eyes (note: use -C option for compression)

```
# ssh -C -X work

# xeyes
```

Cool things I'm not showing

Using ssh as a secure transport mechanism pop-3 wrapper

Using the authentication-agent. Authentication-agent is a cool tool that allows you to store keys in memory so you don't have to retype the passwords all the time

Smartcard support

Kerebos authentication

Lessons From OpenSSH

An Open Source product can become an integral part of your security planning

Be careful what license you use for releasing software

Telnet should be replaced by openssh

The BSD r-commands: rcp, rsh, rlogin should be replaced by more secure replacements

Alternatives to OpenSSH (1)

- Alternative implementations of SSH Protocol
  - LSH is a GPL replacement for SSH/OpenSSH
    - http://the.wiretapped.net/security/cryptography/ssh/lsh
      - Designed with the goal of total compatibility with SSH
      - Development should pick up now that the RSA patent has expired
      - Not as well-developed at this time as OpenSSH

Alternatives to OpenSSH (2)

- Alternative protocols
  - SSLwrap http://www.rickk.com/sslwrap/ wraps any protocol in an SSL-protected tunnel
    - Uses original protocol with minimal modifications use telnet/ftp/rcp securely
    - Have to modify each individual protocol separately
    - Author admits it has not been heavily tested

Website References

OpenSSH HOWTO

http://www.heimdall-linux.com/openssh/index.html

OpenSSH Homepage

http://www.openssh.com

SSH Homepage

http://www.ssh.com

This presentation (talks page at Heimdall Linux)

http://www.heimdall-linux.com/

Usenet Groups

comp.security.ssh or http://deja.com/group/comp.security.ssh

General purpose newsgroup talks about ssh, openssh, ossh and the SSH protocol

Books

Unix Secure Shell

Author: Anne Carasik: ISBN: 071349332

Details mostly SSH

SSH, the Secure Shell : The Definitive Guide

Authors: Daniel J. Barrett, Richard Silverman

ISBN: 0596000111

Not currently published

Contacting Me

grothe@heimdall-linux.com

Q & A

Questions