SSH Basics

What is ssh?

To quote the README file:

SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels. It is intended as a replacement for rlogin, rsh, and rcp.

Additionally, ssh provides secure X connections and secure forwarding of arbitrary TCP connections.

Why should I use it?

The traditional BSD 'r' - commmands (rsh, rlogin, rcp) are vulnerable to different kinds of attacks. Somebody who has root access to machines on the network, or physical access to the wire, can gain unauthorized access to systems in a variety of ways. It is also possible for such a person to log all the traffic to and from your system, including passwords (which ssh never sends in the clear).

The X Window System also has a number of severe vulnerabilities. With ssh, you can create secure remote X sessions which are transparent to the user. As a side effect, using remote X clients with ssh is more convenient for users.

Users can continue to use old .rhosts and /etc/hosts.equiv files; changing over to ssh is mostly transparent for them. If a remote site does not support SSH, a fallback mechanism to rsh is included.

What kinds of attacks does ssh protect against?

SSH protects against:

IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host. SSH even protects against a spoofer on the local network, who can pretend he is your router to the outside. IP source routing, where a host can pretend that an IP packet comes from another, trusted host. DNS spoofing, where an attacker forges name server records Interception of cleartext passwords and other data by intermediate hosts. Manipulation of data by people in control of intermediate hosts Attacks based on listening to X authentication data and spoofed connection to the X11 server. In other words, SSH never trusts the net; somebody hostile who has taken over the network can only force ssh to disconnect, but cannot decrypted or play back the traffic, or hijack the connection.

The above only holds if you actually use encryption. SSH does have an option to use encryption of type "none" this is only for debugging purposes, and should not be used.

What kind of attacks does ssh not protect against?

SSH will not help you with anything that compromises your host's security in some other way. Once an attacker has gained root access to a machine, he can then subvert SSH, too.

If somebody malevolent has access to your home directory, then security is nonexistent. This is very much the case if your home directory is exported via NFS.

All communications are encrypted using IDEA or one of several other ciphers (three-key triple-DES, DES, RC4-128, TSS, Blowfish). Encryption keys are exchanged using RSA, and data used in the key exchange is destroyed every hour (keys are not saved anywhere). Every host has an RSA key which is used to authenticate the host when RSA host authentication is used. Encryption is used to protect against IP-spoofing; public key authentication is used to protect against DNS and routing spoofing.

RSA keys are also used to authenticate hosts.