ssh - an introduction

Eric McCreath
"ssh (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to replace rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP ports can also be forwarded over the secure channel.

ssh connects and logs into the specified hostname (with optional user name). The user must prove his/her identity to the remote machine using one of several methods depending on the protocol version used"

- from the ssh manual (man page)
ssh uses a client server model. The server on the remote machine you wish to log into listens on port 22 for clients to connect.

When the client connects with the server a secret session key is agreed by both parties. This session key is used for encrypting communication between the client and the server. This session key is never passed between the client and server. Rather, a Diffie-Hellman approach is used.

ssh can use a number of authentication approaches. The main ones are:

- password based authentication (assuming the remote machine permits this),
- public key authentication.
• In symmetric key cryptography the same key is used for encryption and decryption of a message. Common symmetric key approaches are: DES, 3DES, AES, and TwoFish.
The problem with symmetric key cryptography is "How do you share keys over an unsecured channel?" In about 1976 Diffie, Hellman and Merkle came up with what is known as the Diffie-Hellman-Merkle key exchange scheme.
Diffie-Hellman-Merkle key Exchange Scheme

Both Alice and Bob know the number 5 and 7 (we can assume Eve may also know them).

Alice thinks up a random number, say 4. This is not shared.

5^4 \pmod{7} = 2

6^4 \pmod{7} = 1

Bob also thinks up a random number, say 3. This is not shared.

5^3 \pmod{7} = 6

2^3 \pmod{7} = 1

So both Alice and Bob share the same key, namely 1. Even if Eve sees 5, 7, 2, and 6, because "a^x \pmod{b}" is easy to calculate but hard to invert it is difficult for Eve to work out the shared key.
Asymmetric Key Cryptography

- In asymmetric key cryptography two keys are used. One for encryption and a different one for decryption.

- In 1973 Diffie came up with this great idea of using two different keys. In 1977 Rivest, Shamir and Adleman worked out a way of implementing it (RSA).
Strengths:
- simple - you don't need to store or maintain keys so you can log in from different clients,
- generally people will have a password on a unix based system when they obtain an account.

Weaknesses:
- people forget their passwords
- people use the same password for different systems
- passwords can be guessed
Public Key Authentication

ssh_keygen

private key   public key

passphrase

encrypted private key

ssh

private key

passphrase

~/.ssh/authorized_keys

sshd

public key

remote login

client

server
Public Key Authentication provides you with 2 factors. Namely, something you know, the passphrase, and something you have, the encrypted private key. This approach, combined with an authentication agent, such as ssh-agent, provides one with a convenient and secure way of accessing a remote machine.

Weaknesses of this approach include:

• the server can not check that strong passphrases are used (or even if a passphrases is used at all!)
• if someone is able to alter the authorized_keys file then they could include an extra key which may not be detected.
Challenge

• Read the man page for ssh. Focus on:
  - first 2 paragraphs of the DESCRIPTION,
  - the AUTHENTICATION section,
  - the TCP FORWARDING section, and
  - the VERIFYING HOST KEYS section.