Secure Shell(SSH)

Kiran Vasudev[1]

[1]Hochschule Bonn-Rhein-Sieg

March 19, 2018

Outline

What is it? I

- A powerful software based approach to network security.
- Based on a client/server architecture.
- The SSH server program accepts/rejects connections to its host computer.
- The SSH client program runs on other computers and are used to make requests to the server.
- All communication between server and client are encrypted and hence are protected from any modifications.
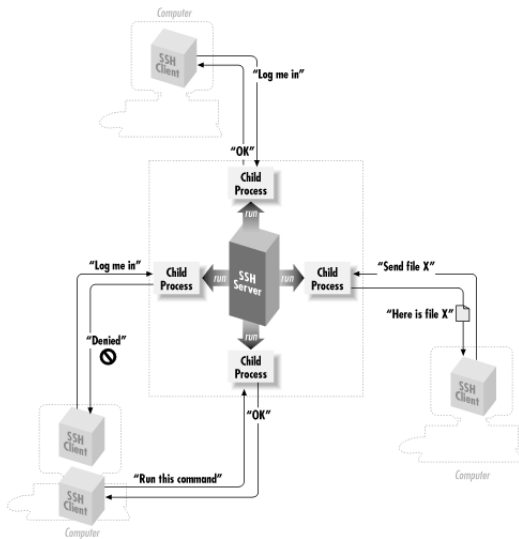- Better than non secure traditional architectures such as FTP and TELNET.

What is it? II

Figure: SSH Architecture[1]

What it is not

- It is not a true shell and hence does not provide a command history or command interpreter. A channel is created using SSH to run a shell on a remote computer.
- It is not a complete security solution. It still can be hacked.

Why use SSH?

- Prevents interception of data between two systems.
- Tackles the problem where a nefarious computer impersonates a particular host.

SSH in MAS

- Use SSH to run processes on robots. Example: ROSMASTER.
- Can also use SSH to access and clone repositories from GitHub.

Hands-on

- Installation using `sudo apt-get install openssh-client`.
- Check if you have any keys stored in `.ssh` folder.
- The `id_rsa` and `id_rsa.pub` are basically the private and public key.
- Generate your keys using `ssh-keygen -t rsa`

References

SSH Architecture