An Overview to SSH : Secure Shell

Deepak Chahal[1], Abhijaat Bhatnagar[2], Jasmeet Singh[3]

Professor[1], Jagan Institute of Management Studies, Sector-5, Rohini
Student Scholar (MCA)[2,3], Jagan Institute of Management Studies, Sector-5, Rohini

ABSTRACT

Secure Shell(SSH) is basically a cryptographic protocol or an interface that can implement network service and communication with the need of remote computer. It authorize users to conduct network communication and other utility on unsecured network.

SSH was firstly planned to toil on a client/server architecture and client securely authenticate and sends encrypted data to be implemented on to the server. SSH mostly uses AES, IDEA and BLOWFISH.

Keywords: Secure Shell, Protocol, Encryption, Communication, Telnet

INTRODUCTION

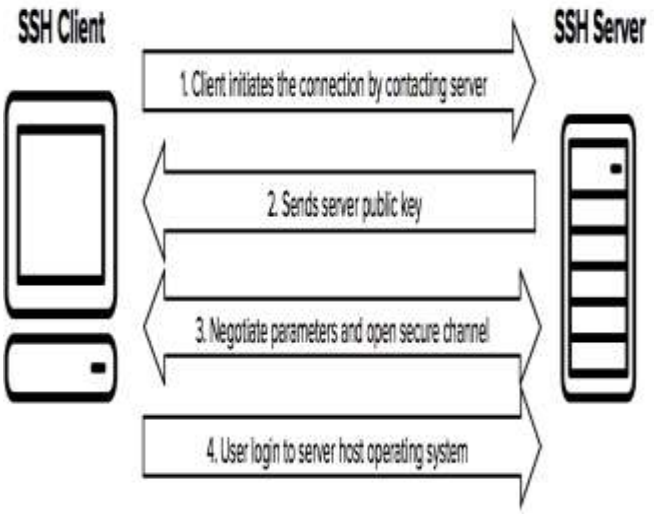

Figure 1: SSH Client and SSH Server

One of the most attractive and efficient feature of this technology is that it basically implements to secure the different types of communication between local machine and remote host that mainly secure remote accessibility to material and remote commands.

This technology also used to build secure tunnels for other application protocols like Window System graphical session. The way an individual communicate with this technology is just like a normal person talk. Users of this technology along with Telnet can interact with themselves, can have meaningful conversations with the machine and SSH may also plan more often on public key pairs to authenticate hosts to one another.

This technology include one session that specifies two public keys such as one public key for the authentication of the remote system to the local system and other key for the authentication of the local system to the remote system.

By default SSH also concentrate on the standard Transmission Control Protocol (TCP) port 22. It also provides well-built authentication and encrypted data communication between two or more connecting devices on an open network like as the Internet.

Secure shell may extensively access by network administrator for managing system and applications remotely, and it also permits them to log into other system over a network and implements commands and moves the files or data from one system to another. SSH also works on delivery of software products, its updates and other administrative or management things**[1].**

There is a SSH port technique that will help in redirecting the network traffic to a particular port/IP address. In this technique the remote host is mainly accessible by the applications of the local host. SSH

tunnels are very useful software for the IT administrator.

ORIGIN

Few years ago, message or data transfer is not possible and said to give unreliable result. But with the advent of time, day by day technology increases with the increase of human demand.

Previously, this message transfer is not possible and is not able to provide correct result. But with the time corrections are made to make it reliable way of communication with the devices.

One of the great researcher Tatu Ylönen of Helsinki University of Finland planned the initial version of protocol which is called as SSH:1 in ayear 1995. The main goal of SSH was to replace the untimely rlogin, TELNET,FTP and rsh protocols, which did not deliver robust validation nor assurance confidentiality. Ylönen released his implementation as Freeware in July 1995.

Ylönen founded the SSH communication Security to market and he developed SSH in December 1995. The main version of the SSH communication uses different parts of software like GNU libgmp, and later varieties released by the SSH progressed into increase software.

There are various categories or the versions used in SSH communications:

- Version 1.x
- Version 2.x
- Version 1.99
- Open SSH
- OSSH

APPLICATION

1. Symmetrical Encryption

It is a structure of encryption where a classified key is used for encryption and decryption of a data communication by the client and the server.
Practically anyone controlling the key can decrypt the massage being transferred. In symmetrical encryption one or more keys are used to pass the data from one system to another and moreover the client and the server expand the keys using agreed method.

2. Asymmetric Encryption

Apart from other encryption this method basically uses two separate key for encryption and decryption and these keys also called as public and private keys.

Public key is the openly distributed and shared in all the devices or systems and more closely connected with the private key with respect to its functionality whereas private key in not shared with the device and its connection is secured and robust in the system.

3 Hashing

Hashing is a part and parcel form of the cryptography which is basically implemented in the secure shell connectivity[2]. There is no need of private and public keysin this part of hashing. There is one way hash functions which is different from other forms of encryption as they are not suitable for the decryption part of the massage from one system to another.
Hashing mainly build a unique value of affixed length in each input that shows the no clear trend that can be destroyed.
Moreover it is not possible to build or generate the input from the hash function as the client holds the correct input and checks whether they are accessing the correct value or not[3].
Secure shell access hash function to check the authentication of the data or the message and it is basically done by the help of HMAC's.

FUNCTIONS

- It mainly secure the remote access towards SSH that enables the network systems and for the users as well as for the automated process.
- It also provide the interactive file or data transfer sessions.
- It mainly focus on issuance of commands on the remote systems.
- It is also secure in management of the network system components.

WORKING

- It is used to replace insecure terminal or login program like FTP (file transfer protocol), Telnet (Telecommunication network), rLogin (remote login), rsh (remote shell) etc.
- It help to enable different functions like session terminal on remote systems.

- It replace file transfer programs like FTP (file transfer protocol), RCP (remote copy) etc.
- Secure Shell is basically used for connecting to a remote host for session of terminal.
- Commonly used command is:- UserName@SSHserver.example.com

- This command will help to connect client and server

- If the connection is building for the first time in between local host and server then the user is provided with the remote host's public key fingerprint and with the help of this key user is capable to make connection otherwise no connection can be made.

- The authenticity of the host can only be maintained with the help of the DSA key fingerprint.
- The DSA key fingerprint will be like:-
- ab:cd:ef:01:23:45:67:89:98:76:54:32:10:fe:dc:ba.

- It will ask the user whether they want to continue (yes/no)?
- If yes then it will retain the created session in between client and server and this DSA key is stored in the user's local system called as host file. It is a hidden file which is by default stored in hidden directory. This hidden directory is called as /.ssh/known hosts in user's home directory.

- Once the key has been stored in the user's host file, the client will automatically connect to the server without any approvals and this key will help to authenticate the connection between client and server.

- Secure shell is an open source protocol which can be implemented in different platforms. And this open source protocol is most commonly found in platforms like Unix, Linux, BSD (Berkeley Software Distribution), Mac Operating System (provided by Apple)[4].

- This protocol is also used in Windows platform. It was firstly run in 2015 on Windows Power Shell. It was also implemented in Windows 10 in the year of 2018. And it is explicitly enabled in the app settings of Windows.

- By default, this protocol is commonly accessible in Operating System like Unix.

- One of the Open Source Implementation of Secure Shell is called as Putty. It was basically developed to run on Windows platform. It was mostly used by Windows for longer period of time. Now-a-Days, it is currently available for Windows, Unix, BSD, Mac OS[5].
- The Secure Shell Protocol is mainly composed of three elements and they are sLogin, SSH and SCP. And earlier for Unix it is composed of 3 elements and they are rLogin, RSH and RCP.
- This protocol authenticate the remote computer by using Public-Key Cryptography and also allow to authenticate the user, if necessary.

- Now there are lots of Secure Shell Protocol available for different platforms provided with open source and proprietary licenses.

- It involve graphical implementation. Their programs are run as CLA (Command Line Argument) or are executed as a script part in the program.

- Execution of the ssh command with no parameter or argument like user ID, destination host will return a list of Secure Shell command parameters and options[6].

- The commonly used SSH command to run the program and the destination host IP address or the destination host name are:-

  - ssh server.example.org
  - ssh remote_host_userID@server.example.org
  - ssh example.org ls
  - sshd
  - ssh-keygen
  - ssh-copy-id
  - ssh-agent
  - ssh
  - scp
  - sftp

ADVANTAGES

The main advantage of this SSH technology is that it could be accessible anywhere anytime.

1. It provides the efficient backup and the migrations and it will help in web server.
2. SSH is very powerful and gives direct access and the customer or client will get the domain in the particular platform.
3. It also provides automation through BASH scripting that will ensure the backend configuration in SSH[8].
4. It also helps in:
   - ✓ IP SOURCE ROUTING
   - ✓ DNS SPOOFING
   - ✓ DATA MANIPULATION
   - ✓ IP ADDRESS SPOOFING

DISADVANTAGES

1. It takes a lot of time in SSH key that work on SSH mode manually.
2. There is no native GUI present in an extra layer that will manage the GUI in the command line.
3. It gets lot of technical requirements for the SSH tools which is not efficient for the average users.

FUTURE SCOPE

With extraordinary beneficial focal points of the innovation, there is a forward advance to the modern idea which look for more it providessecure encrypted communications for an unsecure network and should be access anytime data is transferred which is of a tactful nature. That's why some vendors are initially offer it as a secure alternative for both Telnet and FTP]7].

This upheaval has accomplished a better way to security which could securely transfer the data from client to server which conduct to data level security solutions. This could even lead to valuable intelligence which can be inherited by profiling, fusing and mining traffic patterns or IT task.

REFERENCES

1. https://www.hostinger.in/tutorials/ssh-tutorial-how-does-ssh-work
2. https://www.webopedia.com/TERM/S/SSH.html
3. https://www.ssh.com/ssh/
4. https://searchsecurity.techtarget.com/definition/Secure-Shell
5. https://www.buycpanel.com/ssh-benefits-advantages-know/
6. https://www.inmotionhosting.com/support/website/linux/ssh-advantages
7. https://www.quora.com/What-are-the-weaknesses-of-Secure-Shell
8. https://www.ionos.com/digitalguide/server/tools/ssh-secure-shell/