# SSH: An Internet Protocol

M4L3

# Content

- Introduction
- The Governing Standards Body
- Specifications of SSH
- Application of SSH
- History
- Advantages and Drawbacks
- Conclusion

# Introduction

- SSH stands for Secure Shell
- SSH is a powerful network protocol that allows the secure exchange of data between computers
- SSH uses strong encryption and authentication to provide confidentiality and authenticity of the data
- SSH was designed as a replacement for Telnet and other insecure remote shells
- SSH is now used by millions worldwide for secure system administration, file transfer, and application connectivity

# The Governing Standards Body

- SSH-2 is a “Proposed Internet Standard”
- SSH-2 is publicized by the Internet Engineering Taskforce (IETF) SECSH working group
- The IETF is an open standards organization that has no formal membership requirements.
- Everyone participating in the development of the protocol is an ad hoc volunteer.

# Specifications of SSH

Secure Shell, as a protocol is a specification of how to achieve secure communication over a network:

- ***Authentication:*** When trying to log into an account on a remote computer, SSH asks for proof of identity. Once the identity is confirmed, it is possible to log onto the system, otherwise SSH rejects the connection.
- ***Encryption:*** To protect data as it passes through a network, SHH encrypts the data that is transmitted to be unintelligible except to the intended recipients.
- ***Integrity:*** SSH guarantees that the data traveling over the network arrives unchanged. Any captures and modifications of data in transit will be detected by SSH which ensures that transmissions are unmodified and unread.

# Application of SSH

- ***Secure System Administration:***
  - Providing secure terminal access to servers.
  - Administrators have adopted SSH as the de-facto standard for administrating remote servers.

- ***Secure File Transfer:***
  - Secure environment for FTP functionality.
  - Used for secure file exchange within networks.

- ***Secure Application Connectivity:***
  - Port-forwarding to protect application protocol connections.
  - Secure environment for terminal-based host access.

# History

- Developed in 1995 by Tatu Ylönen, a researcher at the Helsinki University of Technology in Finland.
- **July 1995:**
  SSH1 was released to the public as free software with access to the source code. By the end of the year, an estimated 20,000 users in 50 countries used SSH1.
- **December 1995:**
  Ylönen founded SSH Communications Security, Ltd to further his product
- **During 1995:**
  The SSH-1 protocol was documented as an IETF Internet Draft that described the SSH1 software.

# History contd.

- **1996:**
  SSH-2, a more secure protocol, was introduced. SSH-2 is incompatible with SSH-1. The IETF formed a working group called SECSH.
- **1998:**
  The SSH2 software which is based on the SSH-2 protocol was released.
- **Late 2000:**
  SSH-2 is slowly becoming more deployed: individual contractors can use the protocol freely > free SSH-2 applications are developed: OpenSSH gains popularity.
- **2005:**
  SSH Communications Security released SSH-G3
- **Early 2006:**
  The IETF standardization process granted SSH "Proposed Standard Status"

# Advantages

- ***Password Exposure:*** SSH eliminates the risk of password exposure because. It doesn't transmit passwords in plaintext format, therefore making it impossible to "sniff" the passwords.
- ***Data Eavesdropping:*** SSH uses strong encryption and authentication when transmitting data. SSH guarantees that only the recipient can read the transmitted data.
- ***Man-in-the-Middle Attack:*** The SSH protocol applies server authentication and cryptographic integrity checks to ensure that the data cannot be modified undetected while sent through a network.

# Drawbacks

- Because no application can address every detail, SSH contains some security issues that it doesn't address.
- ***Password Cracking:*** SSH improves password security through encryption, but it's still a weak form of authentication, because it can be lost, given away, or guesses.
- ***IP and TCP Attacks:*** SSH operates on top of TCP, therefore some of its weaknesses come from TCP/IP problems. of the SSH connection.
- ***Traffic Analysis:*** Traffic patterns can be an important source of information for a hacker. Sudden increase or decrease in traffic can indicate important transactions or unguarded networks.
- ***Covert Channels:*** SSH doesn't attempt to eliminate covert channels, because their analysis is usually performed by other security applications on a system.
- ***Carelessness:*** SSH is an effective tool, but it can't take over every security aspect and its effectiveness depends on the user.

# Conclusion

- Although there are some aspects that the protocol wasn't designed to prevent, overall SSH is a very secure system