.

a

IT221 T PROJECT 2022 – second-semester

Group Members

Name	ID
مجد محمد العمري	443007585
[redacted]	
[redacted]	

PNU

The project is about SSH protocol Application protocol

.

- *Introduction*:

SSH Protocol is a network communication protocol made to help two devices to communicate. An inherent feature of SSH is that the communication between the two computers is encrypted meaning that it is suitable to use on insecure networks.

SSH stands for secure shell, and it is a method for secure remote login between two devices. SSH's main objective is to protect the communication's security and integrity by utilizing strong encryption.

The protocol can be used to:

1. provide secure access for users and automated processes.
2. interact and automate file transfer.
3. issue remote commands.
4. manage the network infrastructure and other mission-critical system components.

SSH clients will support SCP (Secure Copy) or SFTP (SSH File Transfer Protocol) for transferring data, some people recommend using SFTP but all of them can work perfectly.

.

· *Protocol operation*:[1]

SSH Secure Shell (SSH) is a straightforward and reasonably priced network protocol that may be used for network operations including email and file transfer. Three protocols that run on top of TCP make up the SSH architecture:

· Provides server authentication, data confidentiality, and data integrity with forward secrecy via the Transport Layer Protocol. Additionally, it can offer compression.

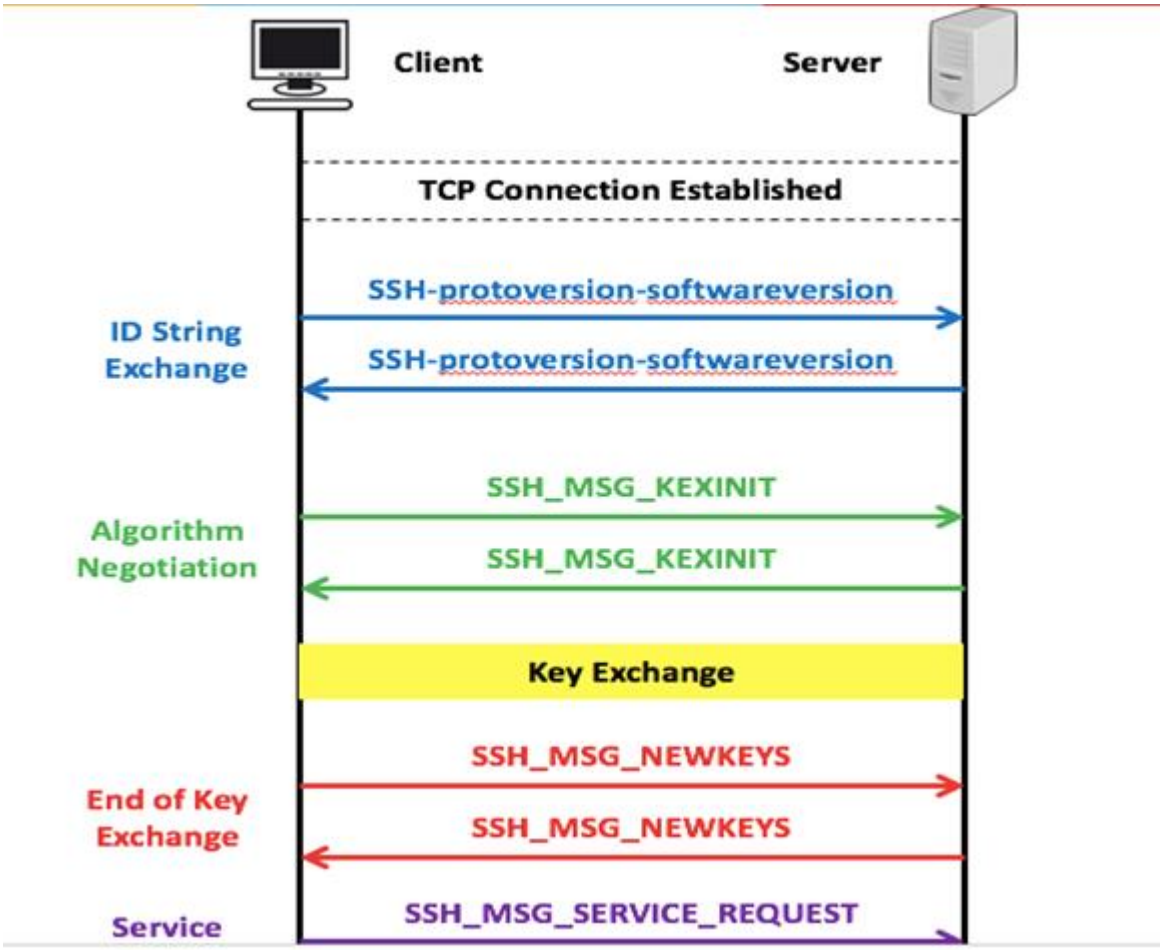
· Authenticates the user to the server using the user authentication protocol.

· Combining numerous logical communication channels over a single, underlying SSH connection is the Connection Protocol.

Today, SSH is used in almost every significant network environment, including those in governments, large corporations, and financial institutions, to secure data in transit and enable remote system administration.

[1] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," Internet Engineering Task Force (IETF) Network Working Group, RFC 4251, January 2006.

.



SSH Authentication in detail:

1-TCP connection: Following the establishment of the TCP connection, the client and server exchange an ID string.

2-Algorithm Negotiation: In this step, a list of key messages is sent along with a list of algorithms, keys, and compression algorithms.

3-key exchange: during this stage, the server and client are both authorized, and the key is also generated for server message authentication.

4-The key exchange has concluded, and both parties can now begin transferring messages using an encryption and compression technique.

Protocol for SSH User Authentication:

.

Depending on the level of security required, SSH User Authentication Protocol enables the server to authenticate the client at one or more levels.

There are various kinds of authentication techniques, including the following:

1-Password: The client sends a message that is encrypted by the Transport Layer Protocol and contains a plaintext password.

2-Public Key: The client transmits a message including its public key, which is then signed by its private key and sent to the server. Upon receiving this message, the server determines whether the supplied key is appropriate for authentication and, if so, determines whether the signature is accurate.

3-Host-based: Rather than the client itself, the host of the client is used for authentication. As a result, a host that accommodates several clients would offer authentication for each of them. The client sends a signature that was generated using the client host's private key to carry out this operation. As a result, the SSH server checks the identification of the client host rather than the user's identity directly.

Different Channel Types in the ssh protocol :

Multiple channels can be opened with the server using the SSH Connection Protocol through negotiation.

1-session: A remote program execution. The application could be a shell, a file transfer or email application, a system command, or a built-in subsystem. The remote program is launched via successive requests when a session channel has been opened.

2-x11: This stands for the X Window System, a network protocol and computer software system that offers a graphical user interface (GUI) for connected computers. Applications can run on a network server using X, but they must be viewed on a desktop computer.

3-Forwarded-tcpip: This is an example of a remote port forward.

4-direct-tcpip: Local port forwarding is what this is

.

The use of encryption is SSH's key advantage over competing protocols. SSH encrypts all communication in transit between a client and a server.

Symmetric, asymmetric, and hash encryption are the three encryption techniques used by SSH.

Vulnerabilities: [2]

- **Key Tracking Troubles :**

End users can copy or create new SSH keys (credentials) without restriction. Once a company accumulates a significant number of SSH keys over time, it could easily lose track of these credentials.

- **Embedded SSH Keys :**

  Applications and scripts typically include SSH keys as embedded data. Administrators are frequently reluctant to rotate them because of the level of collaboration needed to prevent system disruptions or because they do not comprehend the coding the keys are encoded in. Static SSH keys inserted in programs, code, and scripts can thereby give attackers access to permanent backdoors.

- **Static SSH Keys :**

[2] A. Hassen, "An Overview of SSH Protocol Vulnerabilities and Attacks," Journal of Network and Computer Applications, vol. 34, no. 6, pp. 1071-1082, November 2011.

.

For fear of forgetting a vital component or employee, many IT administrators and security specialists rarely change and re-distribute keys. This leaves attackers open to compromising an unchanged key, using it to move laterally through the organization and gaining permanent, unauthorized access to sensitive data.

Alternatives: [3]

Each of the protocols mentioned as alternatives to Secure Shell (SSH) serves a specific purpose and may be better suited to certain tasks or situations than SSH. Here is a summary of the main differences between these protocols and the problems they are designed to solve:

1. Remote Desktop Protocol (RDP): RDP is a protocol developed by Microsoft that allows users to remotely access and control a computer or virtual machine. It is commonly used for remote administration and support, and is available on most modern operating systems. SSH, on the other hand, is a text-based protocol that allows users to remotely access and control a computer using a command-line interface.

2. Virtual Private Network (VPN): A VPN is a network technology that creates a secure, encrypted connection between a client and a server. VPNs are commonly used to enable remote access to corporate networks, and can also be used to protect internet traffic from eavesdropping and other forms of interception. SSH is primarily used for secure remote access and command execution, and does not provide the same level of protection for internet traffic.

3. Telnet: Telnet is a protocol that allows users to remotely access and control a computer or device using a command-line interface. It is an older protocol than SSH, and is generally less secure due to its lack of encryption. Telnet is a protocol that allows users to remotely access and control a computer or device using a command-line interface. SSH, on the other hand, uses strong encryption to secure the connection between the client and the server, making it more secure than Telnet.

4. Secure Copy Protocol (SCP): SCP is a file transfer protocol that is similar to FTP, but uses SSH for secure transfer of files between computers. It is commonly used to transfer

[3] J. Smith and M. Jones, "Exploring Alternatives to the SSH Protocol for Remote Access," Proceedings of the Annual Conference on Computer Communications, pp. 123-137, April 2016.

files between servers, and is often used in conjunction with SSH for secure remote access. SSH itself is not specifically designed for file transfer, but it does include the SCP command which can be used to securely transfer files between computers using the same secure connection as the SSH protocol.

Ultimately, the best protocol for a given situation will depend on the specific needs and requirements of the users and the systems being accessed. SSH is generally considered a secure and reliable protocol, but other protocols may be more suitable in certain situations.

5. *References*: Use IEEE reference style.

[1] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," Internet Engineering Task Force (IETF) Network Working Group, RFC 4251, January 2006.

[2] A. Hassen, "An Overview of SSH Protocol Vulnerabilities and Attacks," Journal of Network and Computer Applications, vol. 34, no. 6, pp. 1071-1082, November 2011.

[3] J. Smith and M. Jones, "Exploring Alternatives to the SSH Protocol for Remote Access," Proceedings of the Annual Conference on Computer Communications, pp. 123-137, April 2016.