SECURE SHELL (SSH) PROTOCOL

Presented by :
Mark Lopes(9913)
Vivian Ludrick(9914)
Rohit Patra(9928)

INTRODUCTION

What is SSH?

Secure Shell (SSH) is a cryptographic network protocol that allows secure communication between a client and a server. It operates at the Application Layer of the OSI model.

WHY SSH IS IMPORTANT

1

Security in Network Communication

In today's digital world, securing remote access is crucial to protect sensitive data on servers, enable secure IT maintenance, and prevent unauthorized access.

2

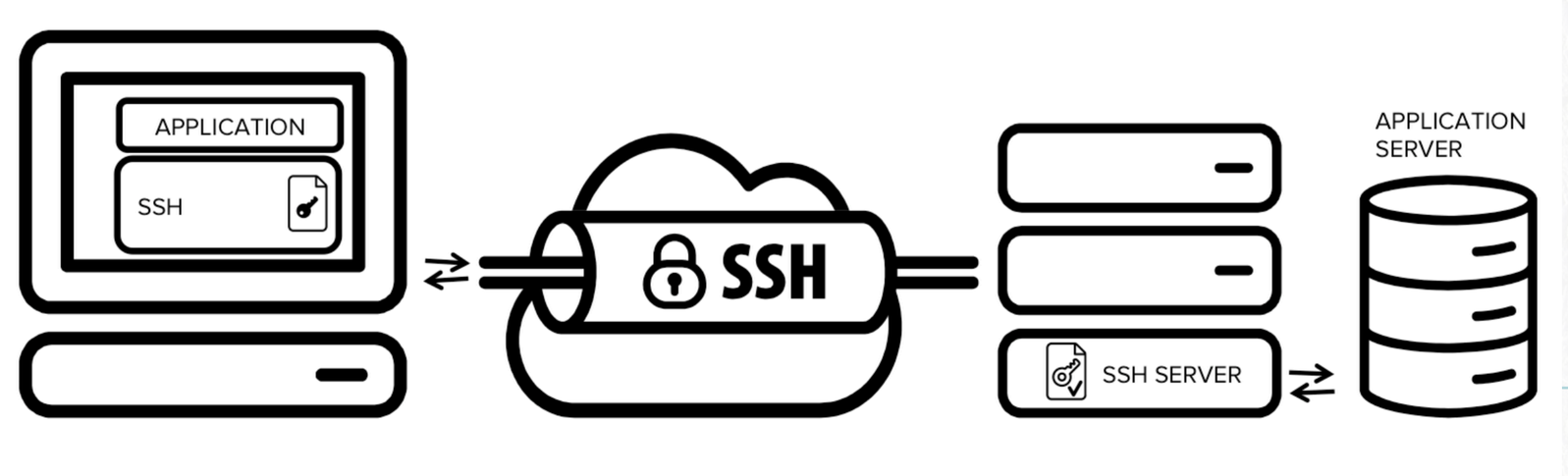
Historical Context

SSH was developed as an improved,secure alternative to the older and less secure Telnet protocol, which transmitted data in plain text.

SSH VS TELNET

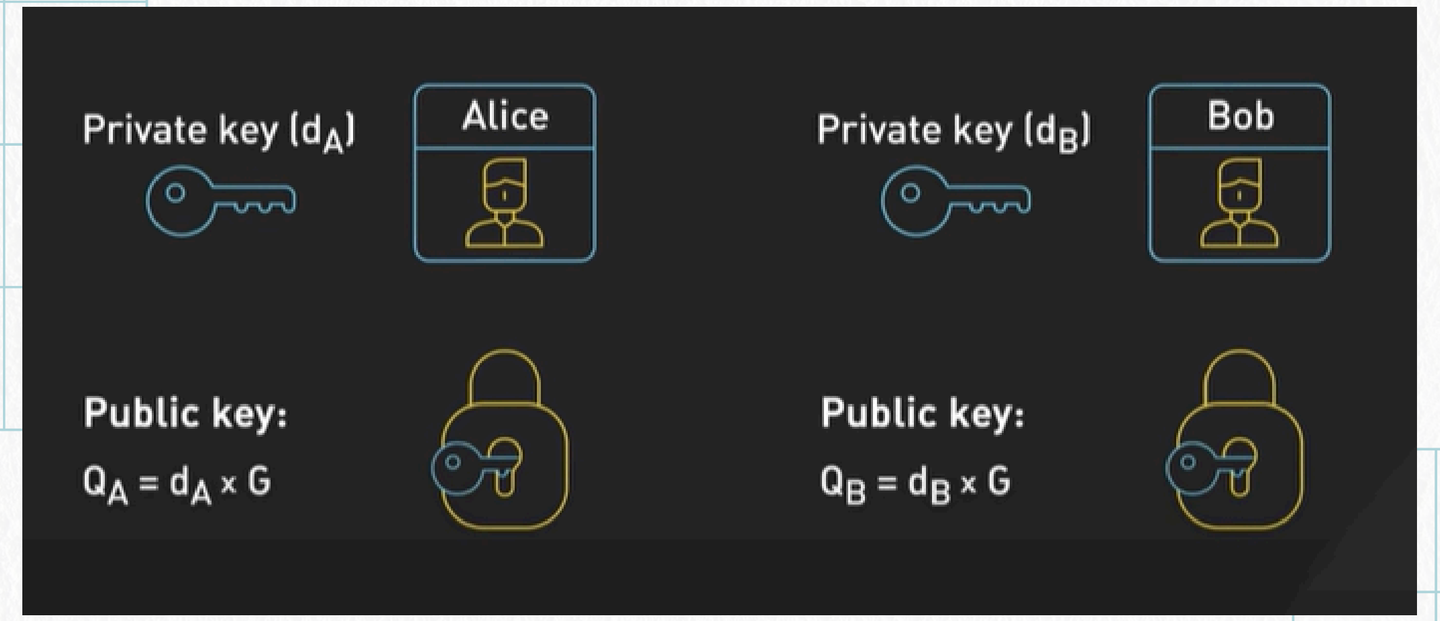
SSH (Secure Shell)	Telnet
Runs on port 22	Runs on port 23
Very Secure Protocol	Not Secure Protocol
Difficult to decrypt	No data encryption
Provides data integrity checks	No data integrity checks

HOW SSH WORKS



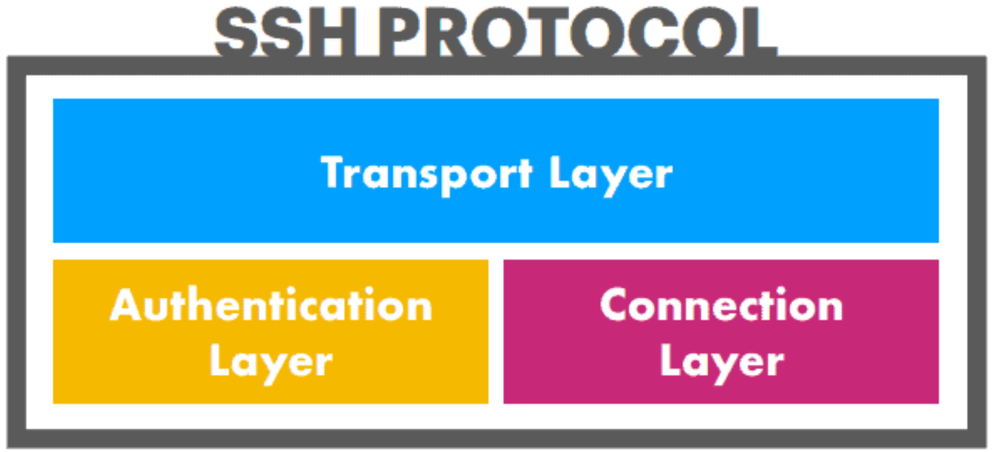
This diagram illustrates the SSH handshake process, showing how a client initiates a secure connection request, the server's identity verification, and the final establishment of an encrypted session

PUBLIC AND PRIVATE KEYS



This diagram shows how Alice and Bob each have a private key and a derived public key, allowing secure communication. Public keys are shared openly, while private keys remain confidential, ensuring encryption and secure data exchange.

SSH PROTOCOL LAYERS



Transport Layer Protocol

- Establishes secure connection
- Manages encryption

Authentication Protocol

- Verifies user identity
- Supports multiple methods (password, public key)

Connection Protocol

- Handles multiple channels in one session
- Enables command execution and file transfer

SSH PRACTICAL USES

Remote Server Management

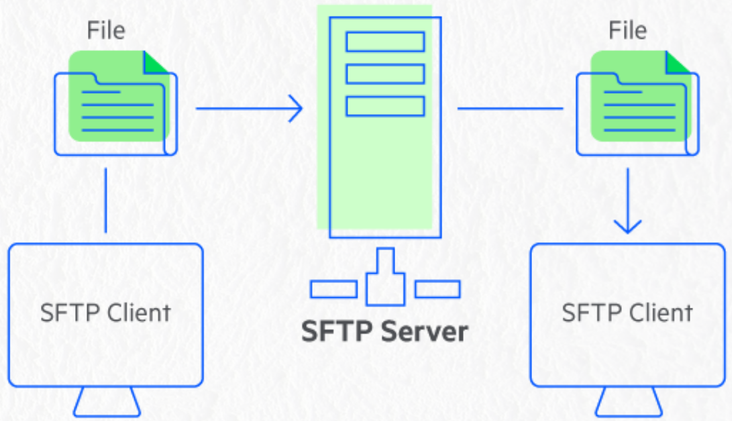
- Securely access and manage servers from anywhere
- Commonly used by system administrators

Secure File Transfers (SFTP)

- Transfer files securely over SSH
- Useful for uploading/downloading data to/from servers

Port Forwarding/Tunneling

- Creates secure tunnels to redirect network traffic
- Used to access services behind firewalls securely



CONCLUSION

Summary

- SSH is essential for secure network communication.
- Enables remote access, secure file transfers, and tunneling.
- Uses encryption and authentication to protect data.

Final Thoughts

- SSH's importance in network security continues to grow.
- A critical tool for safeguarding modern IT infrastructure.
- Understanding SSH is key to secure digital communication.

REFERENCES

slide 4- https://ccnp300-115.blogspot.com/2016/09/difference-between-telnet-ssh.html

slide-6 https://www.youtube.com/watch?v=rlMfRa7vfO8

slide7-https://phoenixnap.com/kb/how-does-ssh-work