Zaytoon Ahmed

I 012-1117

Question: How does Secure Shell (SSH) work?

Answer:

Secure shell (SSH) is a cryptographic network protocol that allows secure communication between two computers over an insecure network, such as the internet. It is widely used for secure connecting to servers, transferring files and managing Git repositories on platforms like github. In my case I will explain managing and setting ssh on github.

STEPS

1 CREATING SSH KEYGEN

- Generating ssh pairs on computer which are private and public, the private pairs stays on computer and are secretly stored while the public ~~pairs~~ keys are uploaded to github which tells the computer is allowed access.

CODE `ssh-keygen -t ed25519 -C "mystudent_email address.com"`

After running the above command, my SSH is then stored in {~/.ssh/}

2 ADDING THE PUBLIC KEY TO GITHUB

- Github uses the public key to recognize my computer, to do this on github I paste the copied public key into my github's settings under SSH and GPG keys, through this github knows if a computer can prove it has the matching private key or not. So doing so github recognizes my computer whenever I want to connect without needing a username and password each time.

3 ESTABLISHING A CONNECTION

When I try to interact with github (e.g git push or git pull), github sends a challenge message to my computer trying to confirm that my computer owns the private key

4 AUTHENTICATION USING PRIVATE KEY

My computer uses the private key to encrypt the challenge message, then the encrypted challenge message is now sent back to github.

5 GITHUB VERIFICATION

Github then make use of the stored private key to decrypt the message

If the decrypt message matches the challenge it sent, it will now confi

the legitimacy of my Computer.

6 SECURE COMMUNICATION ESTABLISHED

Once authenticated, a secure, encrypted channel is established between my computer and github. All data transmitted during this session like Commits and Pushes are now encrypted, ensuring Privacy and Protection against eavesdropping.

7 PASSWORD-FREE INTERACTION

After all this have been set and completed, we can securely Push, Pull, or clone-repositories from github without entering our github username and password-everytime. The ssh pair handles authentication automatically

8 ENCRYPTION STRENGTH

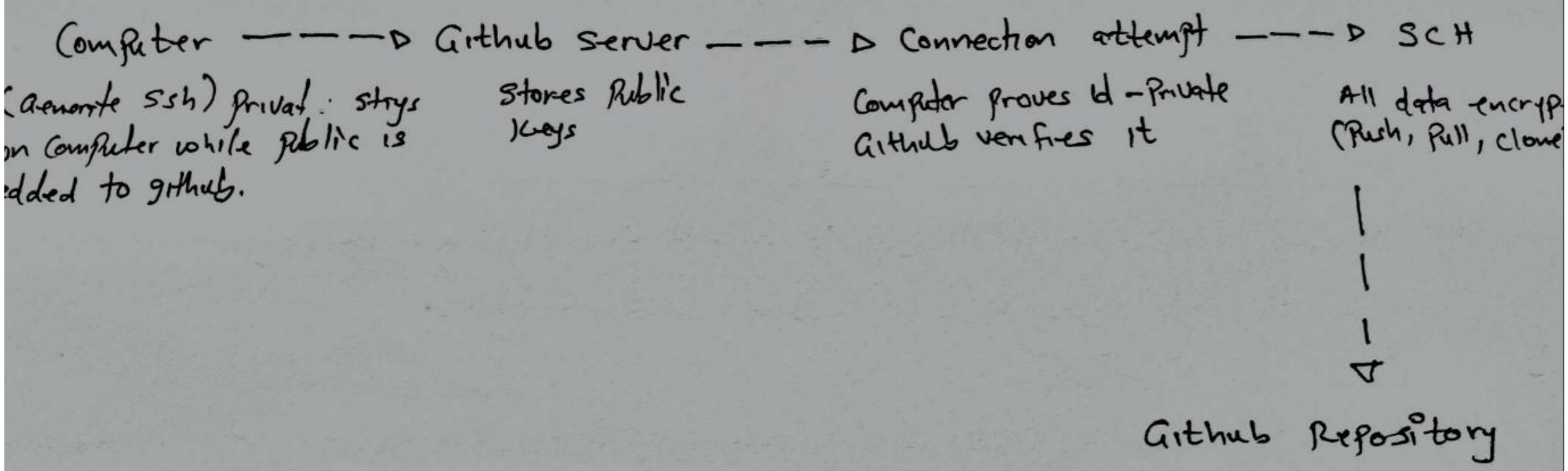
Ssh uses strong encryption algorithms like RSA/Ed25519 to ensure that even if some one intercepts the communication they cannot read or modify the data. This makes connection on github highly secure.

9 KEY MANAGEMENT

With github we can generate ssh keys for different devices. A key for my laptop, one for my android or desktop. It stored all keys and recognize any device used.

10 PRIVATE KEY SAFETY

These keys should always be kept private and away from any other person, that is why is recommended to use a passphrase to add an extra layer Protection.



SSH — GITHUB (WORKFLOW)