Transport-level Security

Secure Shell

Prof.dr. Ferucio Laurenţiu Ţiplea

Fall 2023

Department of Computer Science
“Alexandru Ioan Cuza” University of Iaşi
Iaşi 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Secure Shell (SSH)

Developed by Tatu Ylonen in 1995 as a response to a hacking incident in the Finnish university network.

SSH was designed as a method for secure remote login from one computer to another, providing:

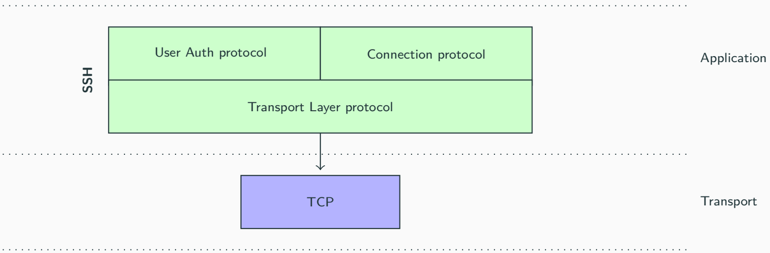
- strong authentication;
- confidentiality;
- integrity;
- forward secrecy.

SSH is a secure alternative to the non-protected login protocols (such as telnet) and insecure file transfer methods (such as FTP).

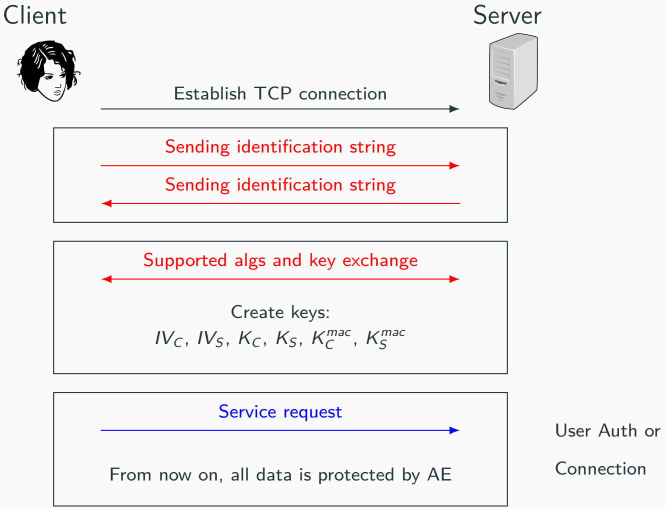
SSH protocol page: `https://www.ssh.com/academy/ssh`

SSH structure

SSH is organized as three protocols that run on top of TCP:



SSH main steps



Client

Server

Establish TCP connection

Sending identification string

Sending identification string

Supported algs and key exchange

Create keys:

IV_C, IV_S, K_C, K_S, K_C^{mac}, K_S^{mac}

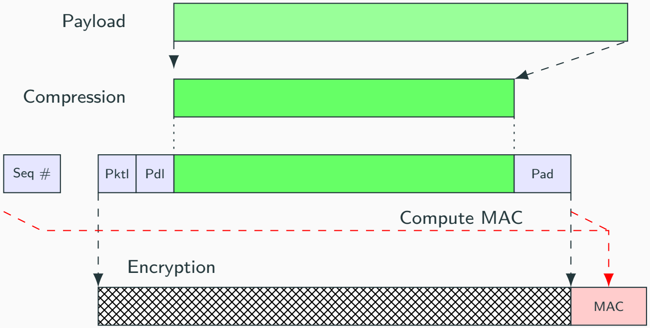
Service request

From now on, all data is protected by AE

User Auth or

Connection

SSH packet transformation



Encryption: AES128-CBC/CTR/GCM, AES192-CBC/CTR/GCM, AES256-CBC/CTR/GCM

Authentication: HMAC-SHA256, HMAC-SHA384, HMAC-SHA512

Applications of SSH

1. Remote control: allow remote machines to access a shell on the host computer. To do this:
   - The host machine must be running an SSH Daemon (sshd), usually on port 22;
   - The remote machine must use an SSH client to connect to the host;
2. File transfer: SFTP (SSH file transfer protocol). This is neither FTPS (FTP over SSL) nor FTP over SSH!
3. SSH tunneling: create an encrypted tunnel from a port on the client machine to a port on the server machine;
4. X11 forwarding: X11 forwarding is a mechanism that allows a user to start up remote applications, and then forward the application display to their local Windows machine.