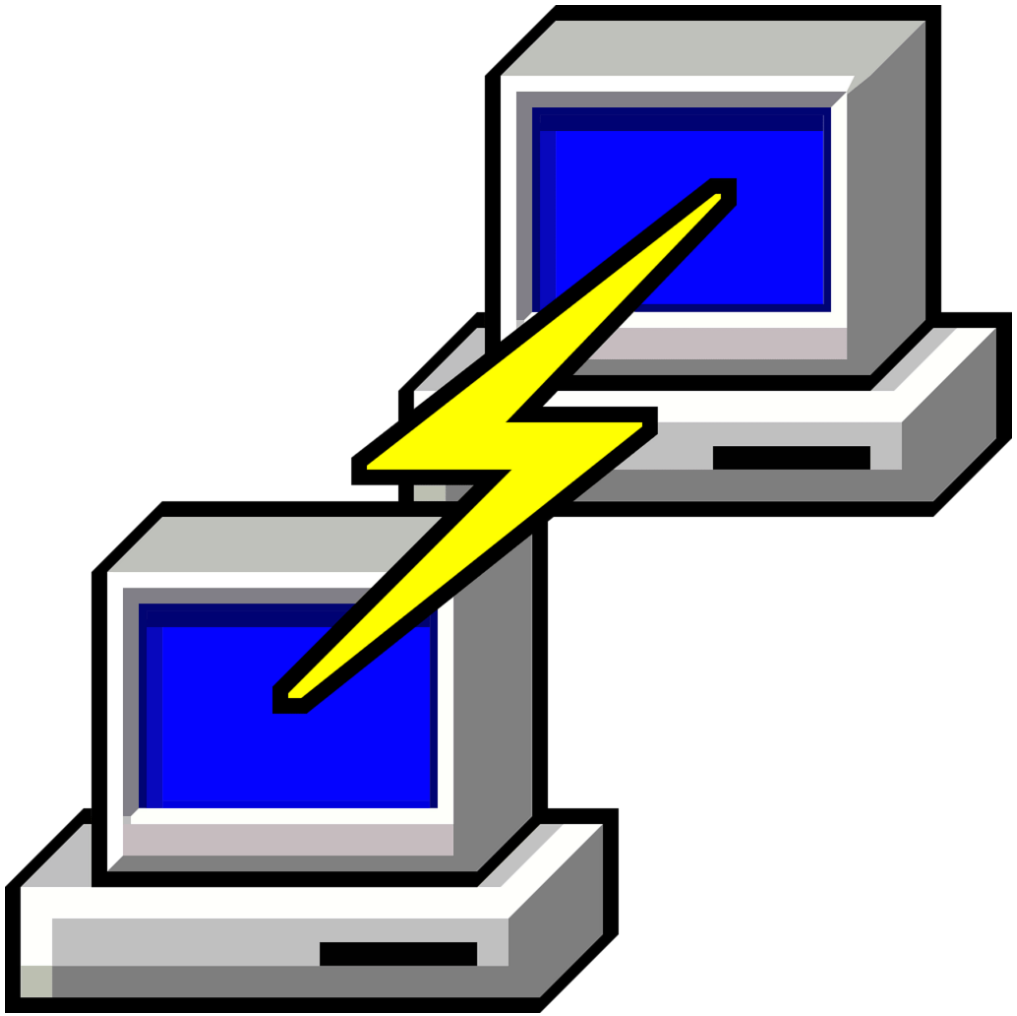
The SSH Protocol

Janika Neuberger (569713)

Projektstudium:
Big Data Management und Analytics in datenzentrischen Wissenschaften

Dr. Patrick Fuhrmann

03-01-2022



[1]

What is SSH ?

- „Secure Shell“
- Protocol that enables a secure transfer of information over an unsecured network
- First version:
  SSH-1 developed by Tatu Ylonen in 1995

Why do we use SSH?

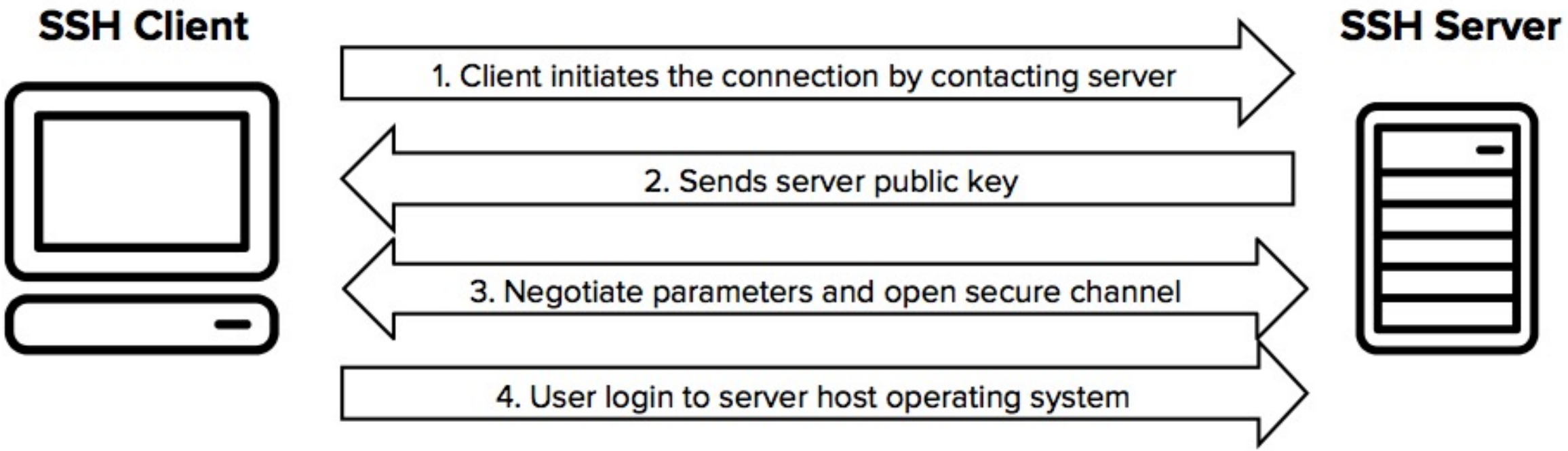
- Late 1960s: Telnet protocol
- Other remote standards: rlogin (remote login), rsh (remote shell), rcp (remote copy)
- Plain text transfers are not secure
- SSH added layer of security over the previous programs and protocols
- **Zero Trust Security**

SSH-2 Protocol

- RFC 4251 - The Secure Shell Protocol Architecture
- RFC 4252 - The Secure Shell Authentication Protocol
- RFC 4253 – The Secure Shell Transport Layer Protocol
- RFC 4254 – The Secure Shell Connection Protocol

How does the SSH Protocol work ?

- Server authentication with public key
- Session key generation with asymmetric key exchange algorithm
- Symmetric encryption of data with session key
- Client authentication



[2]

SSH key management

Information security starts from controlling who is given access to systems and data. If there is no control over access, there is no security, no confidentiality, no integrity, and no guarantees of continued operation.

Sources

- Tatu Ylonen: SSH - Secure Login Connections over the Internet.
  Proceedings of the 6th USENIX Security Symposium, pp. 37-42, USENIX, 1996.

- Jeff Geerling. „A brief history of SSH and remote access“. www.jeffgeerling.com. [Online]. Available:
  https://www.jeffgeerling.com/blog/brief-history-ssh-and-remote-access

- [1]
  www.google.com/search?q=ssh+protocol&tbm=isch&ved=2ahUKEwjbnvyJ46L2AhXs3eAKHdE3AQEQ2cCegQIABAA&oq=ssh+protocol&gs_lcp=CgNpbWcQAzIFCAAQgAQyBAgAEB4yBAgAEB4yBAgAEB4yBAgAEB4yBAgAEB4yBAgAEB4yBAgAEB4yBggAEAgQHjoECAAQQ1CqCljSEGCaEWgAcAB4AIABYogBhQWSAQE4mAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=XvIcYtv3EOy7gwfR74QI&bih=1399&biw=2859&client=firefox-b-d#imgrc=r_SSgw8oDig9dM

- [2]
  www.ssh.com/academy/ssh

Thank you for your attention! Any questions?