SSH

Damien Miller
djm@openssh.com
https://bsky.app/profile/damienmiller.bsky.social

What is SSH

A suite of cryptographic protocols for performing command-line activities, file transfer operations and for forwarding other protocols over untrusted networks.

What is SSH

The result of reimplementing the Berkeley r*-commands (*rsh, rlogin, rcp*) but with encryption.

What is SSH

A protocol suite:

- An encrypted transport protocol with server->client authentication
- A flexible user (client->server) authentication sub-protocol
- A connection protocol that provides tunneled cleartext client<->server communication channels
- A set of services built over these channels:
    - Command execution, shell sessions, file transfer, TCP port-forwarding, X11 forwarding, authentication agent forwarding
    - … which in turn are used as building blocks for automation and workflows by a vast community of users

What is SSH

A collection of standards:

RFC4251 - The Secure Shell (SSH) Protocol Architecture

RFC4253 - The Secure Shell (SSH) Transport Layer Protocol

RFC4252 - The Secure Shell (SSH) Authentication Protocol

RFC4254 - The Secure Shell (SSH) Connection Protocol

Usage

SSH almost wholly supplanted unencrypted remote access (telnet/rsh) by 2001

SSH is ubiquitous - available by default on just about every general-purpose operating system

SSH is critical internet infrastructure - it is usually the last (and often first) resort for remote management of network and server devices across a network

SSH is a building block upon which other protocols and automation rest:

- NETCONF, scp/sftp/rsync (file transfers), git (transport)

History

1983 - BSD 4.1: rsh, rlogin, rcp

1995 - Tatu Ylönen - ssh v.1, scp

1999-2006: IETF standardisation of SSH v.2 protocol

2006-2017: Minor updates, no active WG

2017-2018: CURDLE WG, many RFCs

2018-2024: No active WG

2024+: SSHM WG

History

1983 - BSD 4.1: rsh, rlogin, rcp

1995 - Tatu Ylönen - ssh v.1, scp

1999-2006: IETF standardisation of SSH v.2 protocol

2006-2017: Minor updates, no active WG

2017-2018: CURDLE WG, many RFCs

2018-2024: No active WG

2024+: SSHM WG

History

2000 - Authentication agent (OpenSSH, after ssh.com), draft-ietf-sshm-ssh-agent

2010 - Certificate keys (OpenSSH)

2013 - X25519 key exchange (LibSSH), became RFC8371 in 2020

2013 - ed25519 signatures (OpenSSH), became RFC8709 in 2020

2013 - chacha20-poly1305 (OpenSSH), draft-ietf-sshm-chacha20-poly1305

2015 - graceful hostkey rotation (OpenSSH)

2019 - Streamlined NTRU Prime key exchange (TinySSH), draft-ietf-sshm-ntruprime-ssh

2023 - Strict key exchange (OpenSSH)

Current work

SSHM now working on standardising community extensions and NIST PQC algorithms (inc. draft-ietf-sshm-mlkem-hybrid-kex)

Currently looking at protocol extensions with wide implementation support

- Crypto improvements: Chacha20/poly1305 AEAD, “strict KEX” (Terrapin attack)
- SSH agent subprotocol
- Post-quantum key agreement: Streamlined NTRUPrime, ML-KEM (both hybrid)

WG has a significant backlog of work

Future work

Standardising the “sftp” file transfer protocol (draft-ietf-secsh-filexfer-02)

Post-quantum signatures.

Fallback / national standard PQ algorithms

Certificate authentication

Thanks