SSH Transport Layer Protocol

Tatu Ylönen
SSH Communications Security
e-mail: ylo@ssh.fi

Overview

- Strong encryption, integrity protection, and mutual authentication
- Can interface to almost any public key infrastructure
- All algorithms, public key types, and key exchange methods are negotiated
- Typical one round-trip total (two worst case) for algorithm negotiation, key exchange, mutual authentication, and service request
- Supports key re-negotiation (also for pre-encrypted/pre-authenticated data)
- Can replace Unix `inetd` functionality for secure services

Connection Setup

- Can run over any binary-transparent transport
- Both sides send a protocol version without waiting for the other side
- TCP/IP use: server listens for connections on port 22. After key exchange and authentication, client requests a named service, and server spawns an application server. Concept