

SSH
—
Secure Shell

Interpeak Secure Shell

Secure Shell is the de facto standard for remote secure logins, with an estimated three million users in 80 countries. Typical SSH applications include remote system administration, file transfers, and access to corporate resources over the Internet.

SSH is short for Secure Shell. As the name implies, the protocol creates a secure terminal connection between an SSH client and an SSH server. The connection is encrypted, providing data integrity and replay protection. This effectively eliminates eavesdropping, connection hijacking, IP spoofing and other network-level attacks. Additionally, SSH provides several secure tunnelling capabilities, as well as a variety of authentication methods.

Client Authentication Mechanisms

The SSH protocol supports several authentication mechanisms. The traditional user ID and password based authentication is available. The user ID and password are however transferred after the encrypted channel is established, thus never sent in clear over the network.

Public keys can also be used for authentication. Both the RSA and the DSA algorithms are supported.

Server Authentication

The client always authenticates the server. This provides protection against man-in-the-middle attacks and DNS spoofing.

Remote Login

The basic functionality of SSH is to create a secure channel to a shell on a remote machine. This creates a secure replacement for popular protocols such as *telnet*.

Secure File Transfer

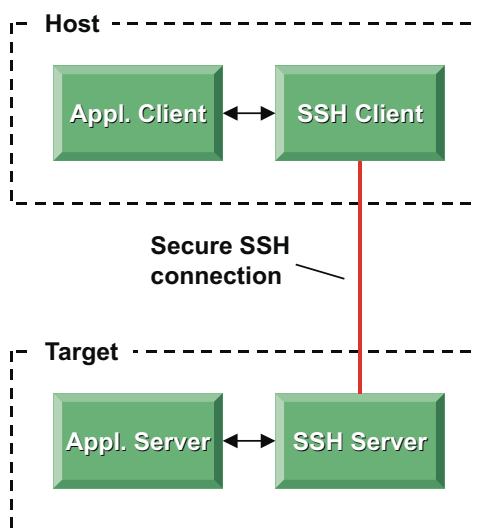
The SSH protocol also provides secure file transfer over the encrypted connection, thus replacing protocols such as FTP. File transfer is supported in both directions, from client to server and from server to client.

Port Forwarding

Existing TCP-based applications can easily be secured with SSH. The application client is reconfigured to connect to the SSH client (running on the same host), instead of connecting directly to

the application server. The SSH client sends a request for port forwarding to the SSH server. The request contains information about what target port the application connection shall be forwarded to. When the application client sends data to the SSH client, data is forwarded to the SSH server over the secure encrypted connection.

The SSH server decrypts the data and forwards it to the application server. Any data sent from the application server is forwarded to the application client in the same manner.



The port forwarding feature of the Interpeak SSH server is a transparent way to secure existing TCP/IP applications.

SSH Server Features

The SSH transport layer protocol contains the basis for the entire SSH protocol suite, and provides an encrypted, integrity and replay protected channel between the client and the server.

Furthermore, it authenticates the server. Once this secure channel is established, the authentication protocol is used to authenticate the client. This means that if the password mechanism is used to authenticate the client, the password and user ID is transferred encrypted over the network.

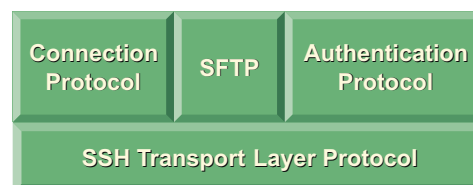
Connection Protocol

The connection protocol uses the secure channel offered by the transport

layer protocol, to provide secure terminal connection and port forwarding services.

Secure FTP

The secure file transfer protocol uses the secure channel offered by the transport layer protocol to provide secure file transfer services.



Interpeak SSH server building blocks.

A versatile source and destination API makes it very simple to read from and write to other sources than a traditional file system. For instance when downloading software upgrades to a system it is often convenient to write the image directly to memory without having to store it on the local file system first.

Authentication Protocol

The authentication protocol is used to authenticate the client. Two different mechanisms are supported, passwords and public keys. The password mechanism uses traditional user ID and password. The public key mechanism uses the RSA and DSA algorithms. The client's public keys must be distributed to the server in a secure off-line manner.

SSH Version 2

The Interpeak SSH server supports version 2 of the SSH protocol. The SSH2 protocol includes both security and performance enhancements over SSH1. Improvements include:

- New algorithms and protocols to increase security.
- Easy to use file transfer by using SFTP (Secure File Transfer Protocol), the secured version of the popular File Transfer Protocol.
- Ability to open several sessions using the same secured channel between two computers.

FEATURES

- SSH Server Mode
- SFTP Client support, both shell command and API
- SSH Version 1.5 and 2
- Terminal Connections
- SFTP Connections
- Port Forwarding
- RADIUS Support (with Interpeak RADIUS)
- Easy to integrate with existing shell/telnet server

IETF DRAFTS

- SSH Protocol Architecture
- SSH Transport Layer Protocol
- SSH Connection Protocol
- SSH File Transfer Protocol
- SSH Authentication Protocol

RTOS INTEGRATION

- Ready-to-run examples
- Complete integration with RTOS shell

AUTHENTICATION METHODS

- Public keys
- Passwords

ENCRYPTION ALGORITHMS

- AES
- DES
- 3DES
- Arcfour
- Blowfish
- Cast

HASH ALGORITHMS

- SHA 1
- SHA 1-96
- MD5
- MD5-96

Interpeak SSH server features.

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company's embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage www.interpeak.com.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 1.23-r5. Copyright © 2005, Interpeak AB. All rights reserved.