Cypherbridge® Systems uSSH™ Secure Server

Overview

Portable ANSI C SSH SDK for interactive shell and tunneled TCP/IP security layer.

Implement secure interactive shell and SSH tunneled application functions using the uSSH solution. Secure telnet replacement is just the beginning. uSSH provides a flexible TCP/IP security layer for existing and new applications using the built-in command dispatcher. Easy to integrate with run-time environment using RTOS integration features.

The uSSH SDK can be complied for a range of processors and platforms, and comes equipped with utilities and toolkits to manage user accounts and private keys. Build options include tailored asymmetric and symmetric crypto suite, login banner, account access control and other features. The compact uSSH protocols and fully integrated math and crypto library can be tailored to a very compact memory footprint under 50K on a typical Cortex-M3 flash MCU.

Interactive Shell Application

uSSH supports an interactive secure telnet replacement as shown in the following diagram, where shell communications are encrypted in the SSH secure tunnel:

Figure 1: uSSH Interactive Shell

The shell session is initiated by the system operator using a desktop command line or GUI SSH terminal client such as openSSH, Bitvise, teraterm, or putty. The interactive session connects with uSSH Server on the routed IP address and port over LAN or WAN. Based on the default or explicit session username, the operator is prompted to enter a password. The password is sent over the encrypted channel and verified by the uSSH Server.

uSSH uses an embedded or file loaded passwords file to authenticate the username and password. The authenticated session is handed off to the application's embedded shell that uses simple line oriented message interface to interact with the user.

The uSSH command dispatcher includes flexible support for multiple operator access levels based on login user name. Read-only system monitoring can be enabled for technician level, while configuration changes are restricted to administrator. Changes to factory defaults or service affecting configuration can be restricted at factory access level.

General Purpose Secure Tunnel

uSSH can be used for a general purpose security tunnel using the SSH exec protocol. The exec request is processed by the uSSH command dispatcher and handed off to the application specific task. The task communicates with a desktop or M2M end-point application, as illustrated in the following diagram showing the encrypted SSH tunnel:

Figure 2: End to End SSH Tunnel

The embedded task can be executed in-line with the uSSH dispatcher, asynchronously, or in a dedicated RTOS service task or thread.

uSSH is source code licensed, royalty-free, and available on a range of platforms including CM3, and integrated with leading RTOS and tools including IAR and GCC.

Take advantage of the SSH security protocol and accelerate your time to market with the uSSH SDK.

Features

- ✓ *Standards based SSH 2.0 interoperates with GUI and command line SSH clients*
- ✓ *Flexible command dispatch to implement any secure client server application*
- ✓ *Built-in starter shell extendable to application specific commands. For non-interactive applications no shell is needed*
- ✓ *Authenticates with user name and protected password*
- ✓ *Access control feature supports Technician, Supervisor, Factory levels*
- ✓ *Configurable DSS and RSA asymmetric session support with private key generator utility*
- ✓ *Configurable crypto with 3DES AES and blowfish support*
- ✓ *Portable ANSI-C SDK with small footprint. Portability layer ported to ARM, Cortex-M3, x86*
- ✓ *Memory management layer with dynamic buffer trace*
- ✓ *RTOS integrated using simple task launcher*

Options

- ✓ *SCP secure copy integrated with embedded file system*

For Pricing and Availability Contact:

Cypherbridge Systems, LLC
7040 Avenida Encinas #104211 Carlsbad, CA 92011
www.cypherbridge.com
sales@cypherbridge.com
Tel: (760) 814-1575

About Cypherbridge Systems:

Established in 2005 to offer software, server, security, device and system level products, our portfolio includes software stacks to enable a broad range of connected device applications integrating embedded device, communications networks, and back office servers in a system solution.

CSL-uSSH-0917.1