

SSL

Secure Socket Layer



# Secure Socket Layer

*The standard Internet communication protocol is completely unprotected, allowing hosts to inspect or modify data in transit. Adding Interpeak SSL to your system will resolve this limitation by providing authentication, integrity, privacy and non-repudiation.*

**Due** to the design of the Internet core protocols, communication on the Internet today is vulnerable to security breaches. This means that extra measures must be taken to increase security to an acceptable level. There are basically four major aspects to secure communication.

The first is *authentication*, where both ends of a communication must identify each other. Second is message *integrity*, where the recipient of a message can verify that the contents have not been altered since it was generated by a legitimate source. Third, *privacy* makes it possible to prevent other people from intercepting and reading the contents of a message. The fourth aspect, *non-repudiation*, signifies that a message's characteristics, such as the content, sender and time of delivery, can be verified at a later date in order to substantiate a claim or an argument.

## Designed by Netscape

The Secure Sockets Layer protocol (SSL) was invented by Netscape Communications to include security in its browser products in order to make communication safe. SSL was originally intended for use with the HTTP protocol used by Web servers and browsers but is now an important component in all kinds of secure Internet communication.

## Industry Standard Protocols

SSL has become the de-facto standard for secure Internet communication on the application level. There is a multitude of application protocols being run on top of SSL. The most well known is the HTTP protocol, commonly known as HTTPS when run over SSL, but many other protocols are commonly being run over SSL in order to provide security.

**HTTP, SMTP,  
LDAP, IMAP,  
POP3, TELNET**

*Application protocols  
commonly run over SSL.*

## Secures Any TCP Application

SSL may be used with any application that runs on top of TCP, or in fact any connection-oriented transport. Many applications use TCP so the potential number of applications that are possible to secure with SSL is enormous.

OpenSSL is an independent and free implementation of the SSL protocols and related cryptography standards. Choosing Interpeak SSL gives you secure interoperability with a vast range of vendors and products.

## RTOS Port by Interpeak

Interpeak has ported OpenSSL to a number of Realtime Operating Systems (RTOS), in order to support embedded realtime systems that require secure Internet communication, as well as an advanced high-performance RTOS.

Interpeak SSL can be used to implement strong *authentication*, *privacy*, *non-repudiation* and *integrity* for customer-specific client or server applications, as well as an interface to standard Internet applications. SSL is easy to use because it is already included in all browsers and it allows systems to be securely managed using a standard browser.

- Based on OpenSSL (former SSLeay).
- SSL protocol: SSL v2, SSL v3 and TLS v1 [RFC2246].
- Extensive cryptographic library (hash/MAC algorithms, asymmetric and symmetric encryption, ASN1, X509 etc.).
- Over 30 shell-based target and host-based utility programs, e.g. certificate handling, CA scripts, CRL, encryption/decryption etc.
- Full scale RTOS integration including ready-to-run examples.
- Guaranteed quality, an extensive target test-suite included for verification.
- Delivered in ANSI compliant "C" source code.
- Complete ready-to-run RTOS integration with examples, makefiles etc.

*Interpeak SSL features.*

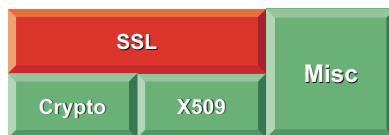
# Your Security Partner

**Many** qualities are required to successfully design and implement network security in an application based on an embedded realtime operating system. The engineers must not only be skilled in RTOS design and development, but also experts on TCP/IP and network security.

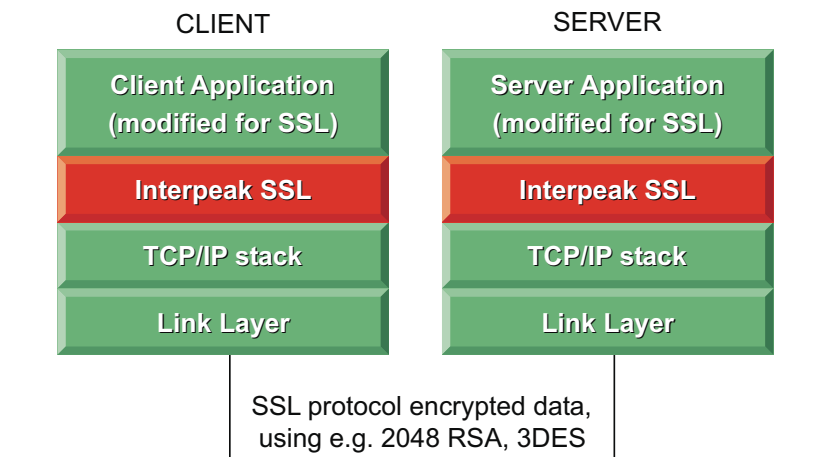
However, with such demanding requirements, it is difficult to find a company or engineer who can understand all the necessary aspects of a project. Interpeak's years of experience in designing and developing embedded realtime TCP/IP and security products makes Interpeak the ideal partner for adding network security to your projects.

## Support

Purchasing your project components from multiple product vendors or consultants can cause anxiety and logistical difficulties for any project. It is often hard to figure out which one of the products that is responsible for a certain problem, resulting in poor support quality and long response times. By purchasing Interpeak SSL, as opposed to downloading and porting OpenSSL yourself, you are not only guaranteed



Interpeak SSL Modules



*Example of a Client/Server application using Interpeak SSL for secure Internet communication. The application is modified on both ends to use the OpenSSL API for SSL protocol communication, instead of BSD TCP sockets.*

excellent SSL, TCP/IP and RTOS support, but also continuity. Regular updates of the latest SSL version ported to the latest RTOS releases minimize the costs of using Interpeak SSL. There is no danger of your own SSL port becoming outdated and non-compliant with the latest RTOS and SSL products.

## Standards-Based Solutions

Interpeak is committed to providing standards-based security and TCP/IP solutions. We perform extensive testing to verify that Interpeak SSL is fully compliant with other important standard SSL applications from companies such as Microsoft and Netscape.

The SSL protocol implementation and its underlying cryptographic components and utilities comply with all the relevant security standards and specifications. In fact, as OpenSSL is used in both the Apache Web Server and the Opera Browser, it is literally tested millions of times each day. It is thereby guaranteed to be fully compliant with the standards and products that adhere to it, e.g. browsers such as Netscape and Microsoft Internet Explorer.

Interpeak SSL also strictly adheres to all the standards involved for the numerous algorithms, ciphers, certificates, etc., which are included in the Interpeak SSL release.

# Product Description

**While** SSL is normally used to transport HTTP messages for web browsing, it can be used to transport any application layer protocol using TCP sockets. In fact, it is so flexible that it can be used over any reliable transport protocol. By layering proprietary or standard applications on top of the SSL protocol, the following security for application-to-application communication is achieved:

- Integrity—MAC ensures no one tampers with the contents.
- Privacy—Encrypted messages warrant no eavesdropping.
- Authentication—Verifying the remote side's identity.
- Non-Repudiation—Achieved by using SSL digital signatures.

There are numerous advantages to using Interpeak SSL to secure your applications. The SSL protocol is layered between the application and the underlying reliable communication layer (e.g. BSD sockets), which has the benefit of requiring no modifications at the lower layers. Consequently, security can be achieved on top of unprotected or non-trusted networks, regardless of the underlying topology.

## Web-Based System Management

Furthermore, if SSL is built into the application to support the HTTP protocol, standard Web browsers can be used to securely manage the system over the Internet. The obvious advantage is an easy-to-use product that does not in-

roduce any additional proprietary tools or require painstaking modifications to lower layers, such as the kernel or TCP/IP stack.

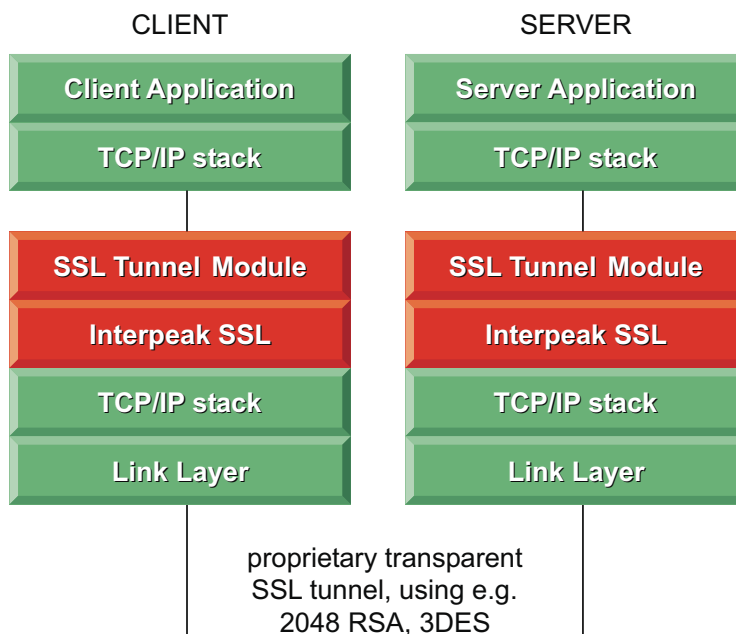
Security can be added to standard applications by simply introducing a new TCP port number and tunnelling the data using SSL. Alternatively, an existing port can be changed to use the SSL protocol.

## Secure Socket Layer Protocol

SSL provides secure communication between client and server by allowing mutual authentication, the use of digital signatures for integrity, and encryption for privacy. The protocol is designed to support a range of choices for specific algorithms used for cryptography, digests and signatures. This allows algorithm selection for specific servers to be made based on legal export or other concerns, and also enables the protocol to take advantage of new algorithms. Choices are negotiated between client and server at the start of establishing a protocol session.

## Extensive Cryptographic Library

Interpeak SSL is much more than an implementation of the SSL protocols. It contains implementations of widely used services and cryptographic algorithms that can run on your embedded target system. The numerous algorithms and functions are assembled into a single, powerful crypto library, that provides a solid foundation for any security-based development. All of the Interpeak SSL functions and algorithms comply with the relevant standards and specifications, and fully inter-operate with other products.



*Example of a Client/Server application using Interpeak SSL for secure Internet communication through a proprietary transparent SSL tunnel. By implementing a SSL tunnel module, the application does not have to be modified.*

# Powerful High-Quality Tools

**Interpeak** SSL also includes a powerful I/O module called BIO, which includes routines that handle filtering, buffering, encryption or decryption on basic input and output over sockets, file descriptors, memory, etc. Multiple BIO modules can be stacked to perform advanced cryptographic routines with minimum programming effort. The library contains functions for random number generation, as well as an advanced big number math library that is used for the cryptographic functions.

Furthermore, the library includes plentiful PKCS, PEM, X.509 and ASN.1 routines that deal with the storing and handling of certificates and dig-

ital objects. There are also additional utility modules, including hash tables, lists, memory allocation, error handling and configuration file parsing.

## Numerous Powerful Tools

Interpeak SSL provides a port of the OpenSSL command line tool *openssl*, a tool for using the various cryptography functions of the Interpeak SSL crypto library from a shell. The program consists of a collection of over 30 utility programs and can be run directly from a target system shell. The *openssl* tool can perform tasks such as:

- Creation of RSA, DH and DSA key parameters.
- Creation and verification of X.509 certificates, CSRs and CRLs.

- Calculation of message digests.
- Encryption and decryption with ciphers.
- SSL/TLS client and server tests.
- PEM, PKCS#12 format conversions.

The Interpeak SSL tool library can be used to run a multitude of cryptographic routines and handle the necessary tasks of a Certificate Authority (CA).

## Quality Assurance

Superior product quality is often promised with little or no proof to back up the claim. The Interpeak SSL product however, provides an extensive test system that thoroughly tests the robustness and functionality of the entire product. The test system consists of the *openssl* command line tool, over 20 additional command line test programs, as well as multiple shell scripts that are used to execute the programs with different arguments. The test system encrypts and decrypts files, generates various kinds of certificates, and converts back and forth between various standards and formats.

## Target System Test Suite

Interpeak SSL provides a target port of the extensive OpenSSL test system, making it possible to run the test system on the embedded target system. The entire target test system is included in the release in order for the customer to verify the quality of the RTOS integration, as well as the functionality and robustness of the Interpeak SSL port. By running the automated target test system, users can feel confident of the quality of the Interpeak SSL product.

### SYMMETRIC CIPHERS

DES and triple DES  
RC2, RC4 and RC5  
Blowfish  
CAST

### SYMMETRIC MODES

ECB  
CBC  
OFB  
CFB

### ASSYMMETRIC CIPHERS

RSA  
Diffie-Hellman  
DSA

### CERTIFICATE & UTILITIES

X.509 and X.509v3  
PKCS#12  
PEM  
ASN.1

### HASH ALGORITHMS

MD2 and MD5  
MDC2  
SHA and SHA1  
RIPEMD

### MAC ALGORITHMS

HMAC-MD5  
HMAC-SHA  
HMAC-RIPEMD

*Summary of the functions and algorithms included in the Interpeak SSL crypto library.*

*The Interpeak SSL product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit, [www.openssl.org](http://www.openssl.org). The product also includes cryptographic software written by Eric Young, [ey@cryptsoft.com](mailto:ey@cryptsoft.com), and software written by Tim Hudson, [thj@cryptsoft.com](mailto:thj@cryptsoft.com).*



### **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](http://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 1.21-r5. Copyright © 2005, Interpeak AB. All rights reserved.*