

# WEBSEC

## Web Server Security Package

# Web Server Security Package

*The HTTP protocol has no built-in security. This means that the communication between a Web Server and a browser is vulnerable to security breaches. The Interpeak Web Server Security Package will resolve this by adding SSL security to your Web Server.*

**The** HTTP protocol contains no security features. This means that the information exchanged between the server and the browser is sent in clear. Confidential information can be inspected and even modified in transit, which is unacceptable in many embedded applications.

A good example of this lack of security is that the HTTP protocol transforms passwords using the base-64 algorithm. It is a simple task to reverse transform this algorithm and obtain the password in clear.

## Add SSL to Your Web Server

The Interpeak Web Server Security Package (Websec) will introduce Secure Socket Layer (SSL) functionality in the communication with your Web Server. This almost eliminates the risk of security breaches.

## Confidentiality

When SSL is used, the communication between the Web Server and the browser is encrypted, which makes it virtually impossible for a third party to access confidential information.

## Integrity

SSL will ensure that no one can modify the contents of messages in transit between the Web Server and the browser.

## Replay Protection

SSL contains protection against replay attacks, where old messages are used which previously have been sent between the Web Server and the browser.

## Authentication

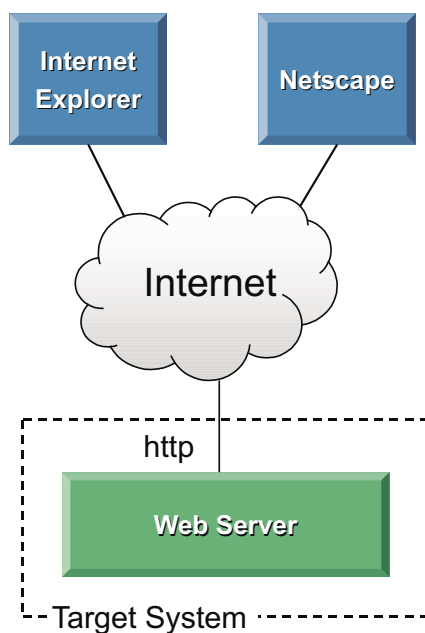
Client authentication using X509 certificates is much more secure than the traditional password authentication. When the client authentication of SSL is used, smart cards can be used with the browsers. This provides the strongest login security available today!

## Secure Transfer

With SSL you can securely access more services and transfer more information over the Internet. The security level of the web interface is significantly improved with SSL. This makes it possible to make more critical services and sensitive information available to web browsers. This means new business opportunities and lowered costs.

## No Additional Client Software Required

All major web browsers, e.g. Netscape, Internet Explorer, Opera, etc. already support SSL. This means that no additional client software is required when using Interpeak Websec.



*The standard protocol between Web Servers and browsers is HTTP. This protocol has no built-in security features, and is therefore not suitable for most embedded applications.*

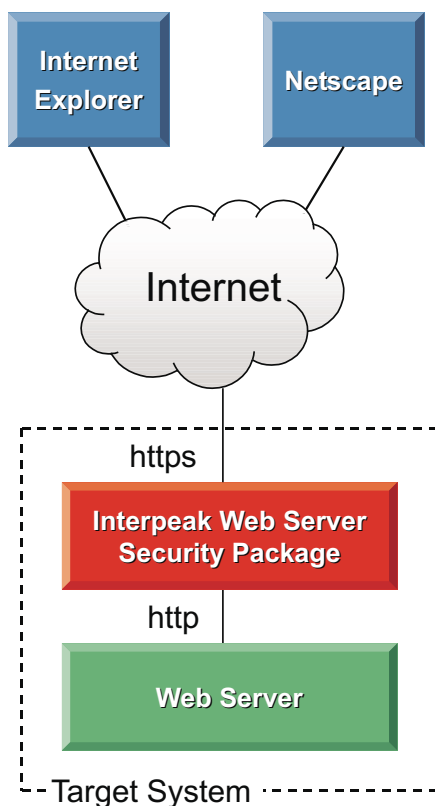
# Interpeak Websec Features

The functionality of the Web Security Package is contained in an SSL Proxy, which listens on incoming SSL connections. For each browser that connects, the SSL proxy connects to the Web Server, decrypting data from the browser before it is sent to the server, and encrypting data from the server before it is sent to the browser.

For maximum security, the Web Server should also be protected from direct HTTP access by enabling filters in the TCP/IP stack.

- **Configuration options:**
  - **Port and address to listen on and connect to, respectively**
  - **Turn client authentication in SSL on/off**
  - **Propagate client certificate to Web Server**
- **No modifications on Web Server or CGI function hooks**
- **Supports SSL v2, SSL v3 and TLS 1.0 [RFC2246]**
- **Supports Persistent Connections**
- **Function hooks:**
  - **Enhanced key protection**
  - **Certificate validation**

*Interpeak Websec features.*



*The Web Server Security Package will improve security by using SSL functionality for the communication between the Web Server and the browser.*

## Strong Encryption

Interpeak Websec supports both strong symmetric keys (128 bits or more) and strong asymmetric keys for certificates (1024 bits or more).

## Highly Configurable

Many parameters of the security package can be configured, e.g. the port the Proxy listens on, the IP address and port number. This can be used to run the SSL Proxy on one host and the Web Server on another. The accepted cipher types are also configurable, giving you control over whether old browsers with so called export ciphers should be able to connect.

The client authentication feature of SSL can be turned on and off. When client authentication is requested in SSL, the clients must have a valid X509 certificate in order to connect. This provides significantly better security than traditional passwords.

## Key Generation and Certificate Requests

The Websec product also contains a number of shell commands for key generation and creation of certificate requests according to the PKCS#10 standard. PKCS#10 requests are supported by all Certificate Authorities.

### **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.*