

INTEGRITY



WEBS

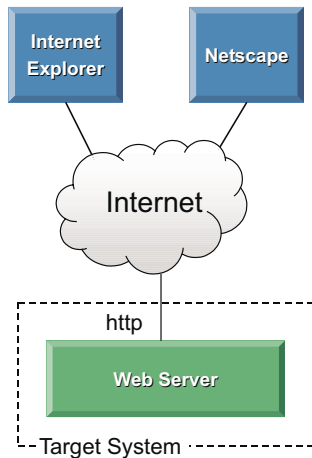
Secure Embedded Web Server

Secure Embedded Web Server

The Secure Embedded Web Server is specifically designed for embedded systems, and features full IPv6 support. This enables development and service personnel to use a standard Web browser to securely configure, monitor and manage an embedded system over the Internet.

Since the World Wide Web emerged globally in the mid 1990s, the underlying protocol has become probably the most used communication standard on the Internet. Millions of people around the world surf the Internet every day, in most cases without thinking about what actually takes place on the network. The protocol that makes user agents or Web browsers able to talk to a Web server is called Hypertext Transfer Protocol or HTTP.

Integrating a Web server in an embedded product presents special requirements on the server in terms of memory consumption, performance, security and functional requirements. Embedded HTTP servers are more often used to display dynamic information about



The standard protocol between Web browsers and servers is HTTP. It completely lacks security features, and therefore enables a minimum Web Server footprint.

the product than to provide large number of informational HTML pages. Another purpose can be to provide a means to configure the product or display its status through a Web interface.

The Interpeak Web Server is a versatile, configurable, high performance HTTP server that has low ROM and RAM footprint. It is specifically designed for operating in an embedded environment.

IPv4 and IPv6 Operation

The Web Server supports the traditional IPv4 protocol as well as the new IPv6 version. It can be configured to use IPv4, IPv6 or both.

HTTP/1.0 and HTTP/1.1

The Web Server includes support for HTTP versions 1.0 and 1.1 as well as pre 1.0 clients.

Persistent Connections

Web browsers running older versions of the HTTP protocol generated a new TCP connection for each URI, which could possibly increase the load on the HTTP server and cause network congestion. The HTTP/1.1 specification defines how persistent connections should be implemented. The Interpeak Web Server supports persistent connections for HTTP/1.1 requests.

Concurrent Server

The default operation of the Web Server is to run as a concurrent server, which means that it can handle simultaneous requests from different clients. It can also be configured to run as a single process, thus supporting only one request at a time. This configuration is

useful when minimum footprint is desired.

Pipelined Requests

A client may pipeline requests, i.e. send multiple requests without waiting for a response. The Interpeak Web Server supports such requests, which may improve performance radically for certain combinations of request/response scenarios.

HTTP Methods

In addition to the mandatory GET and HEAD methods, the Web Server also supports the POST method. This enables the Web browser to transmit entities to the Web Server.

Filesystem Mode

The Filesystem Mode is maybe the most obvious mode for a HTTP server in which the server matches incoming request-URIs with paths and filenames on the target's embedded file system.

Precompiled HTML

When the target system lacks a file system, it is possible to have HTML pages and other files embedded in the target system image. The conversion of the HTML files are done with a HTML to C compiler called *iphtmlc*, which is included in the Web Server product.

Function Hooks

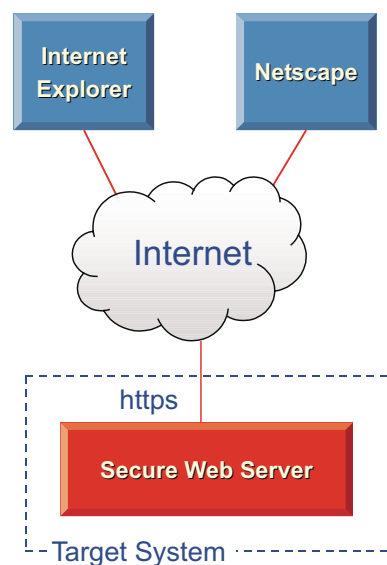
Function hooks provide a way to execute C code functions based on the request-URI. This mode is very similar to CGI scripts used in common Web servers. Several public API functions are available as well as custom methods for sending HTTP headers and entities.

Web Server Features

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.

To overcome this security limitation, the HTTPS protocol was invented, and has now become the de facto standard for secure web communication. It introduces Secure Socket Layer (SSL) functionality in the communication between the Web Server and the browser. This almost eliminates the risk of security breaches.

The Interpeak Secure Web Server supports the SSL protocol through the optional Interpeak SSL module. Interpeak SSL contains an extensive implementation of the SSL protocol version 1.0 and 2.0, as well as its successor TLS 1.0. The SSL support is configurable, and can be tailored to get minimum footprint.



The Web Server can improve security by using SSL functionality for the communication with the browser.

- **Dual Internet protocol versions supported (IPv4 and IPv6)**
- **Supports early versions of the HTTP protocol <1.0**
- **Supports HTTP/1.0 (RFC1945) and HTTP/1.1 (RFC2616).**
- **Supports HTTP methods GET, HEAD and POST.**
- **Supports incoming entities.**
- **Implements persistent connections (HTTP/1.1).**
- **Supports pipelined requests (HTTP/1.1).**
- **Supports chunked mode transfer encoding.**
- **Implements access authentication (RFC2617).**
- **Supports SSL v2, SSL v3 and TLS 1.0 (RFC2246)***
- **Sends target system files upon client requests.**
- **List directory contents on the target file system.**
- **Supports precompiled HTML files (HTML compiler included).**
- **Supports custom function hooks in a CGI-like fashion.**
- **Implements public API for sending HTML responses.**

*Interpeak WEBS features. *SSL is supported in the optional Interpeak SSL module.*

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.

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.

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!

Strong Encryption

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

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 the Interpeak Secure Web Server.



Worldwide Headquarters

30 West Sola Street • Santa Barbara, California 93101
Tel: 805.965.6044 • Fax: 805.965.6343 • Email: sales@ghs.com • www.ghs.com

International Offices

France: +33 (0)1 46 96 07 00 • Germany: +49 (0)721 98 62 580
The Netherlands: +31 (0)33 4613363 • Sweden: +46 (0)46 211 33 70
United Kingdom: +44 (0) 1844 267950 • Japan (ADaC): +81.3.3576.5351

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