

VPN

Virtual Private Network

Interpeak VPN

Embedded systems connected to the Internet are exposed to a number of serious security threats. A powerful way to address this problem is to create a Virtual Private Network (VPN), that prevents unauthorized access to your system.

Most embedded systems perform critical tasks, and must therefore never be accessed by unauthorized parts. This often presents problems when connecting such systems to the Internet. The original Internet protocols have no security features, and consequently cannot stop intruders from accessing the embedded system.

One powerful way of addressing this problem is to use a Virtual Private Network, which is a way of creating secure connections over an insecure network. This means that a third party never is able to compromise the state of the embedded system by means of the network.

A robust VPN solution will protect private communication by adding *strong encryption, integrity, authentication and replay protection*.

Encryption—No one can read your information

Strong encryption will ensure that data can not be accessed by unauthorized hosts, making a brute force attack virtually impossible.

Authentication—The peer identity is certified

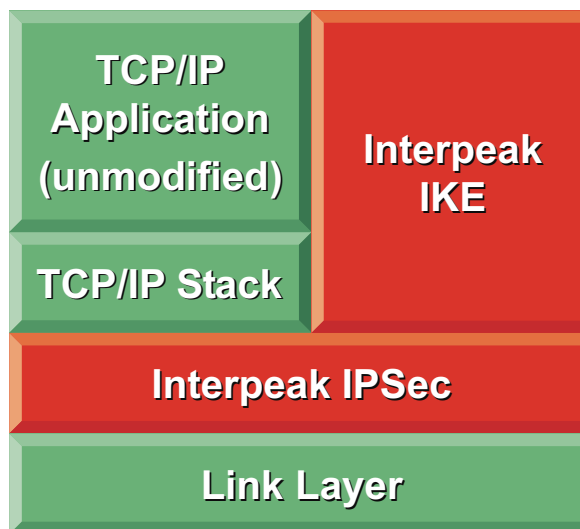
Authentication can be used to sign your data so that others can verify that it is really you that sent it.

Integrity—Modified packets are discarded

By calculating advanced cryptographic checksums on the data, all modified packets can be detected and thrown away.

Replay Protection—Duplicates are ignored

By using sequence numbers protected by cryptographic measures, duplicate packets can be detected and ignored.



Interpeak VPN consists of Interpeak IPsec and Interpeak IKE. IPsec provides strong encryption, integrity, authentication and replay protection while IKE is used for secure key distribution.

Interpeak VPN Features

IPSec is a versatile security solution because it can perform different security mechanisms. Authentication is used to certify that a packet originates from the correct sender, encryption to ensure data content confidentiality, integrity to make sure that the packets have not been modified in transit and replay protection to stop duplication of old transactions.

IPSec uses a database called Security Policy Database (SPD) which contains information on what security to apply to different IP packets. The policy database utilizes selectors such as source and destination IP address, source and destination port, and IP protocol numbers. Additionally, address ranges and wildcard selectors can be used for added flexibility.

For each IP packet, the database is searched for a best match entry, containing information on what encryption and authentication algorithms to use, what algorithm key lengths are needed, and whether to tunnel the packet or not. Because of this design, IPSec can be configured to send some traffic unprotected, some partially protected, and some strongly protected. Furthermore, security can be changed or added later simply by updating the security policy.

Since IPSec is applied on the IP level, all IP based protocols are protected, e.g. TCP and UDP. IPSec resides in the TCP/IP stack and is transparent to applications. This makes it possible to add security to an existing system, without having to change a single line of application code.

IKE is a key distribution protocol that is designed to cooperate with IPSec. IKE manages negotiation of the security characteristics on the different types of communication. With IKE one can specify that users with a certain password or a certain certificate are allowed to connect using IPSec. For example, this can be used to specify that users with a certain

certificate are allowed to connect (using IPSec) only to the FTP server, and no other services.

Especially large systems will benefit from using Interpeak IKE. When the number of nodes increases, manual configuration becomes unfeasible. In such large systems, IKE is typically deployed to automatically handle the key configuration and exchange.

- **IPSec IPv4 Gateway and Host [RFC-2401].**
- **Tunnel/transport mode in any SA combination [RFC-2401].**
- **AH - IP Authentication Header [RFC-1826], [RFC-2402].**
- **ESP - IP Encapsulating Payload [RFC-1827], [RFC-2406].**
- **IPIP - IP in IP tunneling [RFC-1853].**
- **Bypass/apply/discard IP packet filtering with I/O selectors.**
- **SNMP/MIB support, "IPSec Monitoring MIB" [draft-ietf-ipsec-monitor-mib-03.txt]**
- **Key and SA management: "PF_KEY Key Management API", Version 2 [RFC-2367] + OpenBSD IKE extensions.**
- **Authentication transforms: HMAC-MD5-96 [RFC-2403], KDPK-MD5 [RFC-1828], HMAC-SHA-1-96 [RFC-2404], HMAC-RIPE-MD-160-96 [draft-ietf-ipsec-auth-hmac-ripemd-160-96-02], KDPK-SHA [RFC-1852].**
- **Encryption algorithms: ESP_NULL [RFC-2410], DES-CBC with explicit IV [RFC-2405], DES_IV64 [RFC-1829 using a 64-bit IV], 3DES [RFC-2451], CAST-128 [RFC-2144] & [RFC-2451], BLOWFISH [RFC-2451].**
- **Delivered in ANSI compliant "C" source code.**
- **Complete ready-to-run RTOS integration with examples, makefiles.**

Interpeak VPN features.

The industry has already introduced IPSec in full scale and its use is increasing fast. Microsoft Windows 2000, Sun Solaris and the BSD operating system family all have IPSec built-in. Most network companies that deliver routers, switches, gateways etc. also have IPSec built-in. Cisco, Nortel, etc. all advocate use of IPSec. It is clearly the emerging standard for IP Security.

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