

IKE

Internet Key Exchange

# Internet Key Exchange

*Distribution of IPsec encryption keys is a challenging task which requires careful consideration. The Interpeak IKE application is designed to handle key distribution automatically, using state-of-the-art algorithms to provide maximum flexibility and security.*

**Exchange** of encryption keys is required when two hosts want to communicate securely using the IPsec protocol. Distributing encryption keys is however a difficult task, which requires careful consideration. Before the keys are exchanged, none of the hosts can encrypt any information and if keys are sent in clear text, they can be picked up by someone listening in on the communication.

In order to exchange the keys securely, state-of-the-art key exchange algorithms have to be used, specifically designed to meet the challenge of secure key distribution.

## **IKE—Industry (IETF) Standard**

The Internet Engineering Task Force, IETF, has specified the Internet Key Exchange, IKE, protocol specifically to handle secure encryption key distribution. The protocol is implemented by a large number of well-known vendors in the IT industry, e.g. Microsoft, Sun, HP, IBM, Cisco, etc. This ensures secure interoperability.

## **Simplified IPsec Management**

Interpeak IKE lets the user focus on the network's security policy, and ignore low-level details. The user specifies what security to apply to different connections and does not have to bother about encryption details, such as what keys to use, ensuring that the keys are identically configured on both ends of a secure connection, etc.

## **Flexible Authentication**

The IKE authentication feature is very flexible, using either passwords or X509

certificates. X509 certificates are significantly more secure than using traditional passwords. Passwords, however, are slightly simpler to use. This gives you a very flexible security solution that can be tailored to the security requirements in your system.

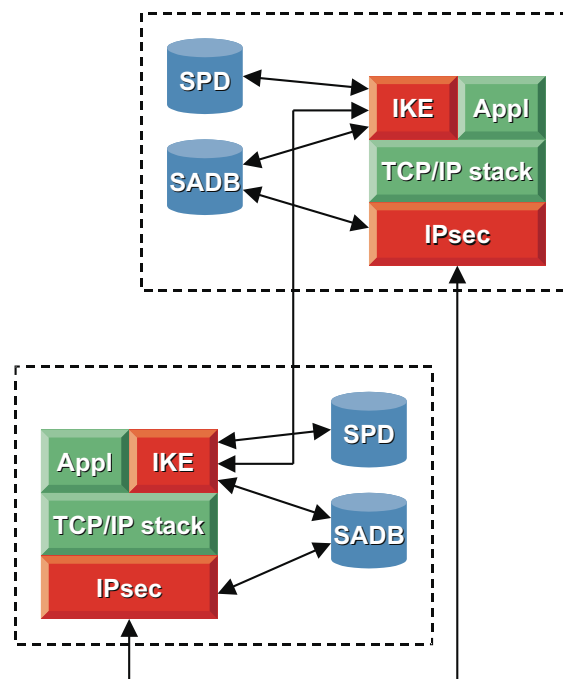
## **Strong Encryption**

Interpeak IKE uses “real” key lengths, 128 bit (or more) symmetric keys and

1024 bit (or more) asymmetric keys. This significantly reduces the risk of security breaches during key distribution.

## **Automatic Re-keying**

Interpeak IKE can be setup to automatically generate new keys for a secure connection after a certain time or after a certain amount of data has been transferred over the connection. This provides an even better security level.



*The picture shows two target systems with IPsec and IKE. The IKE daemons negotiate and setup SAs. The SPD is consulted on the initiating side to determine what SAs to establish. On the receiving side the SPD is consulted to check if the proposed SA shall be accepted. The successfully negotiated SAs are then inserted into the SADB on each side, respectively. When the application start to communicate with the other target system, the application packets are secured by IPsec.*

# Secure Key Distribution

**Interpeak** IKE is an application which generates keys and distributes them securely. The keys are stored in a Security Association Database, SADB. IPsec then fetches the necessary keys from SADB when it needs to apply security to an IP packet.

A security association contains the encryption keys to use, a specification of the IPsec protocols to apply, the lifetime of the SA, etc.

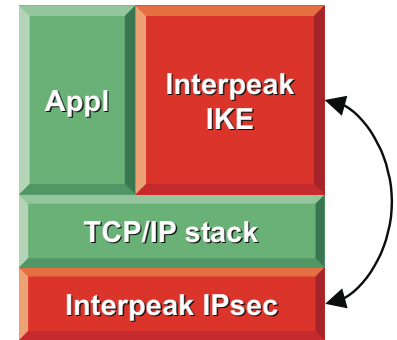
## Security Policy Database

The Security Policy Database (SPD) contains a specification on what outgoing packets that shall be secured. When other IKE daemons request that SAs shall be established, the SPD is

consulted. The SPD contains a specification on what nodes that secure communication is allowed, the required authentication methods, the available encryption algorithms, etc. If the suggested SA is in line with SPD policy, the SA is accepted and inserted into SADB. Otherwise it is rejected.

## SAs in Advance

Interpeak IKE can setup Security Associations at boot time. This is a big advantage in realtime systems. The key exchange is a CPU intensive process, but the encryption of the application packets is a relatively lightweight operation. When SAs are established in advance, e.g. directly following a boot, then the SAs will already be established



*Interpeak IKE used to generate and distribute IPsec keys.*

when the applications start to communicate. This will give minimal latency when application communication is initiated.

- Support for IKE v1 (RFC 2407, 2408, 2409).
- Support for IKE v2 (draft-ietf-ipsec-ikev2).
- Supports NAT traversal (RFC 3947).
- Setup of UDP Encapsulation of IPsec ESP Packets (RFC 3948).
- Diffie Hellman groups: 1 (768 bits), 2 (1024 bits), 5 (1536 bits), 14 (2048 bits), 15 (3072 bits), 16 (4096 bits), 17 (6144 bits), 18 (8192 bits) (RFC 3526).
- Encryption algorithms: AES, DES, 3DES, blowfish, cast
- Hash algorithms: SHA1, MD5, AES-XCBC-MAC-96 (RFC 3566)
- Authentication with pre-shared keys (passwords) or X509 certs (DSA and RSA)
- Perfect forward secrecy
- Per interface enable/disable
- Passive and active establishment of IPsec connections.
- Secure interoperable communication with win2000, Solaris 8, HP-UX, AIX, Linux, BSD-dialects, etc.
- Plug-and-play integration with Interpeak IPsec.
- Flexible and powerful policy-based configuration.
- Establishes both tunnel and transport IPsec connections.
- Delivered in ANSI compliant "C" source code.
- Complete ready-to-run RTOS integration with examples, makefiles etc.

*Interpeak IKE features.*

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