RED ISAKMP and Oakley Information

Document ID: 14139

Contents

Introduction

This document provides information on the Internet Security Association and Key Management Protocol (ISAKMP) and the Oakley Key Determination Protocol. These protocols are leading contenders for Internet key management being considered by the IPSec Working Group of the Internet Engineering Task Force (IETF).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Technical Information

About ISAKMP

The ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management. The ISAKMP specification also is available in postscript.

About Oakley

The Oakley protocol uses a hybrid Diffie−Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible.

The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non−repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec

The IETF's IPSec Working Group develops standards for IP−layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview.

ISAKMP Software

Cisco Systems Implementation

Cisco Systems's ISAKMP daemon software is available free of charge for any commercial or non−commercial use to help advance ISAKMP as a standard solution to Internet key management.

The Cisco ISAKMP software is available within the United States and Canada through a web download form from the Massachusetts Institute of Technology (MIT). Due to United States export control laws, Cisco is unable to distribute this software outside the United States and Canada.

The Cisco ISAKMP daemon uses the PF_KEY Key Management Application Program Interface (API) to register with an operating system kernel (which has implemented this API) and the surrounding key management infrastructure. Security associations that have been negotiated by the ISAKMP daemon are inserted into the kernel's key engine. They are then available for use by the system's standard IPSec security mechanisms (Authentication header [AH] and Encapsulating Security Payload [ESP]).

The freely−distributable U.S. Naval Research Laboratory (NRL) IPv6+IPSec software distribution for 4.4−BSD derived systems (including Berkeley Software Design, Inc. [BSDI] and NetBSD) includes implementation of IPv6, IPSec for IPv6, IPSec for IPv4, and the PF_KEY interface. The NRL software is available within the United States and Canada through a web download form from MIT. Outside the United States and Canada, the NRL software is available through FTP from ftp://ftp.ripe.net/ipv6/nrl .

The Cisco daemon is based on ISAKMP version 5 and uses features from the Oakley Key Determination Protocol version 1.

A mailing list for problems, bug fixes, porting changes, and general discussion of ISAKMP and Oakley has been established at isakmp−oakley@cisco.com. To join this list, send an email request with a message body of **subscribe isakmp−oakley** to: majordomo@cisco.com.

United States Department of Defense (DoD) Implementation

The U.S. DoD Office of Information Security Research has made its ISAKMP Prototype Implementation freely available for distribution within the United States. A web−based interface is available for downloading the software. This implementation does not include any session key exchange capabilities, but does include full ISAKMP features.

Related Information

- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 14, 2008 Document ID: 14139