RED ISAKMP und Oakley Information

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Internet Security Association und zum Key Management Protocol (ISAKMP) sowie zum Oakley Key Determination Protocol. Diese Protokolle sind führende Bewerber für das Internet Key Management, die von der IPSec-Arbeitsgruppe der Internet Engineering Task Force (IETF) geprüft werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Technische Informationen

Info über ISAKMP

ISAKMP bietet ein Framework für die Verwaltung von Internet-Schlüsseln und stellt die spezifische Protokoll-Unterstützung für die Aushandlung von Sicherheitsattributen bereit. Es werden allein keine Sitzungsschlüssel erstellt. Sie kann jedoch mit verschiedenen Sitzungs-Key-Establishment-Protokollen wie Oakley verwendet werden, um eine Komplettlösung für das Internet-Schlüsselmanagement bereitzustellen. Die ISAKMP-Spezifikation ist auch als Postscript verfügbar.

Über Oakley

Das Oakley-Protokoll verwendet eine Hybrid-Diffie-Hellman-Technik, um Sitzungsschlüssel auf Internet-Hosts und -Routern einzurichten. Oakley stellt die wichtige Sicherheitseigenschaft von Perfect Forward Secrecy (PFS) bereit und basiert auf kryptografischen Techniken, die eine beträchtliche öffentliche Kontrolle überstanden haben. Oakley kann selbst verwendet werden, wenn keine Attributverhandlung erforderlich ist, oder Oakley kann zusammen mit ISAKMP verwendet werden. Wenn ISAKMP zusammen mit Oakley angewendet wird, ist ein Key-escrow nicht machbar.

Die Protokolle ISAKMP und Oakley wurden zu einem Hybridprotokoll kombiniert. Die Auflösung von ISAKMP mit Oakley verwendet das Framework von ISAKMP, um eine Teilmenge von Oakley Key Exchange Modi zu unterstützen. Dieses neue Schlüsselaustauschprotokoll bietet optionales PFS, vollständige Assemblyattribut-Aushandlung und Authentifizierungsmethoden, die sowohl Ablehnung als auch Nichtabstreitbarkeit bieten. Implementierungen dieses Protokolls können verwendet werden, um VPNs einzurichten und Benutzern von Remote-Standorten (die möglicherweise über eine dynamisch zugewiesene IP-Adresse verfügen) den Zugriff auf ein sicheres Netzwerk zu ermöglichen.

Info zu IPSec

Die IPSec-Arbeitsgruppe der IETF entwickelt Standards für IP-Sicherheitsmechanismen für IPv4 und IPv6. Die Gruppe entwickelt auch generische Schlüsselverwaltungsprotokolle für die Verwendung im Internet. Weitere Informationen finden Sie unter Übersicht über IP-Sicherheit und -Verschlüsselung.

ISAKMP-Software

Cisco Systems-Implementierung

Die ISAKMP-Daemon-Software von Cisco Systems ist für kommerzielle oder nicht-kommerzielle Zwecke kostenlos verfügbar, um ISAKMP als Standardlösung für das Internet-Schlüsselmanagement weiterzuentwickeln.

Die Cisco ISAKMP-Software ist in den USA und Kanada über ein Web-Download-Formular vom Massachusetts Institute of Technology (MIT) erhältlich. Aufgrund der Exportkontrollgesetze der USA ist Cisco nicht in der Lage, diese Software außerhalb der USA und Kanada zu vertreiben.

Der Cisco ISAKMP-Daemon verwendet die API PF_KEY Key Management Application Program Interface (API), um sich bei einem Betriebssystem-Kernel (der diese API implementiert hat) und der umliegenden Infrastruktur für das Management zu registrieren. Sicherheitszuordnungen, die

vom ISAKMP-Daemon ausgehandelt wurden, werden in die Schlüsselengine des Kernels eingefügt. Sie sind dann für die Verwendung durch die standardmäßigen IPSec-Sicherheitsmechanismen des Systems verfügbar (Authentication Header [AH] und Encapsulating Security Payload [ESP]).

Die frei verteilbare U.S. Naval Research Laboratory (NRL) IPv6+IPSec-Softwareverteilung für abgeleitete 4.4-BSD-Systeme (einschließlich Berkeley Software Design, Inc. [BSDI] und NetBSD) umfasst die Implementierung von IPv6, IPSec für IPv6, IPSec für IPv4 und der PF_KEY-Schnittstelle. Die NRL-Software ist in den USA und Kanada über ein Web-Download-Formular vom MIT erhältlich. Außerhalb der USA und Kanada ist die NRL-Software über FTP unter ftp://ftp.ripe.net/ipv6/nrl erhältlich.

Der Cisco Daemon basiert auf ISAKMP Version 5 und verwendet Funktionen des Oakley Key Determination Protocol Version 1.

Eine Mailingliste für Probleme, Bugfixes, Portierungsänderungen und allgemeine Diskussionen über ISAKMP und Oakley wurde unter isakmp-oakley@cisco.com erstellt. Um dieser Liste beizutreten, senden Sie eine E-Mail-Anfrage mit einem Nachrichtenhauptteil "**subscribe isakmp-oakley"** an: majordomo@cisco.com.

Implementierung des US-Verteidigungsministeriums

Das US-amerikanische DoD Office of Information Security Research hat seine ISAKMP Prototype Implementation kostenlos für den Vertrieb in den USA zur Verfügung gestellt. Zum Herunterladen der Software steht eine webbasierte Benutzeroberfläche zur Verfügung. Diese Implementierung umfasst keine Funktionen für den Austausch von Sitzungsschlüsseln, aber vollständige ISAKMP-Funktionen.

Zugehörige Informationen

- IPSec-Support-Seite
- Technischer Support - Cisco Systems