RED ISAKMP e Oakley Information

Sommario

Introduzione

In questo documento vengono fornite informazioni sul protocollo ISAKMP (Internet Security Association and Key Management Protocol) e sul protocollo Oakley Key Determination Protocol. Questi protocolli sono i principali contendenti per la gestione delle chiavi Internet al vaglio del gruppo di lavoro IPSec della Internet Engineering Task Force (IETF).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Informazioni tecniche

Informazioni su ISAKMP

ISAKMP fornisce una struttura per la gestione delle chiavi Internet e un supporto di protocollo specifico per la negoziazione degli attributi di sicurezza. Da solo, non stabilisce le chiavi di sessione. Tuttavia, può essere utilizzato con vari protocolli di definizione delle chiavi di sessione, come Oakley, per fornire una soluzione completa alla gestione delle chiavi Internet. La specifica ISAKMP è disponibile anche in postscript.

Oakley

Il protocollo Oakley utilizza una tecnica ibrida Diffie-Hellman per stabilire le chiavi di sessione sugli host e sui router Internet. Oakley fornisce l'importante proprietà di sicurezza di Perfect Forward Secrecy (PFS) ed è basato su tecniche crittografiche che sono sopravvissute a sostanziali controlli pubblici. Oakley può essere utilizzato da solo, se non è necessaria alcuna negoziazione degli attributi, oppure Oakley può essere utilizzato insieme a ISAKMP. Se con Oakley si utilizza il protocollo ISAKMP, il deposito a garanzia delle chiavi non è realizzabile.

I protocolli ISAKMP e Oakley sono stati combinati in un protocollo ibrido. La risoluzione di ISAKMP con Oakley utilizza la struttura di ISAKMP per supportare un sottoinsieme di modalità di scambio chiave di Oakley. Questo nuovo protocollo di scambio delle chiavi offre funzionalità PFS facoltative, negoziazione di attributi di associazione di protezione completa e metodi di autenticazione che consentono sia il ripudio che il non ripudio. Le implementazioni di questo protocollo possono essere utilizzate per stabilire VPN e consentire agli utenti di siti remoti (che possono avere un indirizzo IP allocato in modo dinamico) di accedere a una rete protetta.

Informazioni su IPSec

Il gruppo di lavoro IPSec dell'IETF sviluppa standard per i meccanismi di protezione a livello IP sia per IPv4 che per IPv6. Il gruppo sta inoltre sviluppando protocolli generici di gestione delle chiavi da utilizzare su Internet. Per ulteriori informazioni, consultare il documento sulla panoramica della protezione e della crittografia IP.

Software ISAKMP

Implementazione sistemi Cisco

Il software daemon ISAKMP di Cisco Systems è disponibile gratuitamente per tutti gli usi commerciali e non commerciali, al fine di promuovere ISAKMP come soluzione standard per la gestione delle chiavi Internet.

Il software Cisco ISAKMP è disponibile negli Stati Uniti e in Canada tramite un modulo di download Web del Massachusetts Institute of Technology (MIT). A causa delle normative di controllo sull'esportazione vigenti negli Stati Uniti, Cisco non è in grado di distribuire il software al di fuori degli Stati Uniti e del Canada.

Il daemon Cisco ISAKMP utilizza l'API (Application Program Interface) PF_KEY per registrarsi con un kernel del sistema operativo (che ha implementato questa API) e con l'infrastruttura di gestione delle chiavi circostante. Le associazioni di sicurezza negoziate dal daemon ISAKMP vengono inserite nel motore delle chiavi del kernel. Sono quindi disponibili per l'utilizzo da parte dei meccanismi di protezione IPSec standard del sistema (Authentication header [AH] e

Encapsulating Security Payload [ESP]).

La distribuzione del software IPv6+IPSec del NRL (U.S. Naval Research Laboratory) liberamente distribuibile per sistemi derivati da 4.4 BSD (incluso Berkeley Software Design, Inc. [BSDI] e NetBSD) include l'implementazione di IPv6, IPSec per IPv6, IPSec per IPv4 e l'interfaccia PF_KEY. Il software NRL è disponibile negli Stati Uniti e in Canada tramite un modulo di download dal MIT. Al di fuori degli Stati Uniti e del Canada, il software NRL è disponibile tramite FTP da ftp://ftp.ripe.net/ipv6/nrl .

Il daemon Cisco si basa sulla versione 5 di ISAKMP e usa le funzionalità del protocollo Oakley Key Determination Protocol versione 1.

Una lista di distribuzione per problemi, correzioni di bug, modifiche ai porting e discussioni generali su ISAKMP e Oakley è stata stabilita sul sito isakmp-oakley@cisco.com. Per partecipare all'elenco, invia una richiesta tramite e-mail con il corpo del messaggio **subscribe isakmp-oakley** a: majordomo@cisco.com.

Implementazione del Dipartimento della Difesa degli Stati Uniti

L'ufficio statunitense per la ricerca sulla sicurezza delle informazioni (DoD Office of Information Security Research) ha reso liberamente disponibile per la distribuzione negli Stati Uniti la sua implementazione del prototipo ISAKMP . È disponibile un'interfaccia basata sul Web per il download del software. Questa implementazione non include alcuna funzionalità di scambio di chiavi di sessione, ma include funzionalità ISAKMP complete.

Informazioni correlate

- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems