Internet Security Association and Key Management Protocol

Internet Security Association and Key Management Protocol (**ISAKMP**) is a protocol defined by RFC 2408 for establishing Security association (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK) provide authenticated keying material for use with ISAKMP. For example: IKE describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.[1]

Contents

- Overview
- Implementation
- Vulnerabilities
- See also
- References
- External links

Overview

ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques and threat mitigation (e.g. denial of service and replay attacks). As a framework,[1] ISAKMP typically utilizes IKE for key exchange, although other methods have been implemented such as Kerberized Internet Negotiation of Keys. A Preliminary SA is formed using this protocol; later a fresh keying is done.

ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations. SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes and for negotiating, modifying and deleting SAs. ISAKMP serves as this common framework.

ISAKMP can be implemented over any transport protocol. All implementations must include send and receive capability for ISAKMP using UDP on port 500.

Implementation

OpenBSD first implemented ISAKMP in 1998 via its isakmpd(8) (https://man.openbsd.org/isakmpd.8) software.

The IPsec Services Service in Microsoft Windows handles this functionality.

The KAME project implements ISAKMP for Linux and most other open source BSDs.

Modern Cisco routers implement ISAKMP for VPN negotiation.

Vulnerabilities

Leaked NSA presentations released by *Der Spiegel'* indicate that ISAKMP is being exploited in an unknown manner to decrypt IPSec traffic, as is IKE.[2] The researchers who discovered the Logjam attack state that breaking a 1024-bit Diffie–Hellman group would break 66% of VPN servers, 18% of the top million HTTPS domains, and 26% of SSH servers, which is consistent with the leaks according to the researchers.[3]

See also

- Oakley protocol
- IPsec
- IKE
- GDOI

References

1. The Internet Key Exchange (IKE), RFC 2409, §1 Abstract
2. *Fielded Capability: End-to-end VPN SPIN9 Design Review* (http://www.spiegel.de/media/media-35529.pdf) (PDF), NSA via 'Der Spiegel', p. 5
3. Adrian, David; Bhargavan, Karthikeyan; Durumeric, Zakir; Gaudry, Pierrick; Green, Matthew; Halderman, J. Alex; Heninger, Nadia; Springall, Drew; Thomé, Emmanuel; Valenta, Luke; VanderSloot, Benjamin; Wustrow, Eric; Zanella-Béguelin, Santiago; Zimmermann, Paul (October 2015). *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice* (https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf) (PDF). 22nd ACM Conference on Computer and Communications Security (CCS '15). Denver. Retrieved 15 June 2016.

External links

- RFC 2408 — *Internet Security Association and Key Management Protocol*
- RFC 2407 — *The Internet IP Security Domain of Interpretation for ISAKMP*