CSCI 7000-001 — Network-level Security: IPSec Key and Association Management Framework

October 25, 2001

References:

- RFC 2409 (`http://www.ietf.org/rfc/rfc2409.txt`)

1 Security association

A security association is identified by

- *security parameter index (SPI)*: a key that identifies a set of parameters for this association, stored in the Security Association Database
- *destination address* (currently only unicast addresses)
- *security protocol identifier*: AH or ESP

2 Security associations and security services

A security association (SA) is a set of policy and key(s) used to protect information. The ISAKMP SA is the shared policy and key(s) used by the negotiating peers in this protocol to protect their communication.
The general IPSec architecture specifies two classes of SA and key management:

- *manual*: ad-hoc, network administrators directly configure the security databases and the policy databases.
- *automated*: IKE: using Oakley, an authenticated key-exchange protocol
- IPSec protocols (AH and ESP) are mostly independent of the way SAs are set up and maintained

- however, the ultimate level of security of an IPSec association is almost completely dependent on the process by which the SA is setup and managed.
- also, some specific features (for example, the anti-replay counter feature) require a specific

3 Manual vs Automated SA and key management

Obvious advantages and disadvantages of manual management

+ ad hoc: easier to implement, at least initially

− not scalable

− unable to support some IPSec features (e.g., anti-replay in both AH and ESP)

and of automated management:

+ scalable to large networks, and across administrative boundaries

− requires PKI for complete authentication

4 Automated SA and key management

The default automated key management protocol for IPSec is called ISAKMP/Oakley.

ISAKMP Internet Security Association and Key Management Protocol provides a framework for authentication and key exchange. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchange protocols.

Oakley is a specific key-exchange protocol defined as the default key-exchange protocol in ISAKMP.

5 Overview of ISAKMP

Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (not to be confused with the SAs that the protocol is trying to establish).

Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation

6 Overview of Oakley

Oakley is a refinement of Diffie-Hellman. Diffie-Hellman has the following problems that Oakley solves:

- no authentication
- vulnerable to man-in-the-middle attack
- computationally intensive, therefore vulnerable to DOS attack

Oakley uses the following features to counter these weaknesses:

- *cookies* to counter clogging attacks
- *groups* global parameters of the Diffie-Hellman key exchange (q and α). Oakley allows parties to negotiate groups.
- *nonces* to protect against replay attacks
- *authenticated Diffie-Hellman* to protect against man-in-the-middle attack. Authentication is based on either:
  - digital signature (with public/private keys)
  - public-key encryption
  - symmetric-key encryption

7 ISAKMP

ISAKMP defines procedures and packet format (i.e., a protocol) to establish, negotiate, modify, and delete security associations.
In essence, ISAKMP defines a header that introduces the following types of payloads:

proposal payload used for SA negotiation

- SA protocol (AH or ESP)
- sender's SPI
- a list of *transform payloads*

transform payload identifies a cryptographic function for a specific protocol function (e.g., 3DES for ESP), and its parameters.

key exchange payload Oakley, or Diffie-Hellman, or RSA-based key exchange, etc.

identification payload identifies the two ISAKMP peers

certificate payload passes a public-key certificate

hash payload verification (authentication) hash computed over some state information of this running ISAKMP

nonce payload random data used during the exchange

notification payload either error or status information associated with the current SA or with the SA negotiation

delete payload identifies one or more SAs that the sender has deleted from its database