Dynamic Management of the IPsec Parameters: The IKE Protocol

Ghislaine.Labouret@hsc.fr

Hervé Schauer Consultants

HSC

www.hsc.fr

ABSTRACT

Although it is possible to manually enter all the parameters needed for IPsec operation on the various devices, this approach is limited both in security and scalability. As a consequence, the IPsec working group has developed a protocol to dynamically manage the IPsec parameters. The resulting protocol, formerly known as ISAKMP/Oakley, has been renamed IKE (Internet Key Exchange) and focuses on two things: authenticated key exchange and management of the security associations in general. This protocol is rather complex and has many options and modes of operation which provide different features.

This talk will introduce the basic concepts of key management and give an overview of IKE.

Introduction

- The first version of the IPsec RFCs in 1995 didn't include any dynamic key management: the security parameters were configured manually.
- Manual IPsec is limited both in security and scalability.
- Work on key management really started in 1995/1996.
- The second version of the IPsec RFCs, which was published in November 1998, includes the definition of the IKE (Internet Key Exchange) protocol.
- This protocol is still maturing and being completed (various Internet Drafts are available).

Agenda

- 1. Key Management Concepts
  - Keys lifetimes and PKIs
  - Key Exchange Protocols Properties
  - Diffie-Hellman
- 2. Key Management for IPsec
  - Historical Reminder and Various Available Protocols
  - IKE Overview
  - Interactions Between IKE and the IPsec Mechanisms
- 3. IKE Internals
  - Course of the protocol
  - Phases and modes
  - Phase 1 details
  - Phase 2 details

1. Key Management Concepts

- Some reminders of useful concepts

Keys lifetimes and PKIs

- Keys lifetimes and roles
  - Keys with a long lifetime (long-term keys) are generally used for peer authentication only.
  - The keys used for data protection (encryption and authentication) generally have a short lifetime and are called session keys because their lifetime is roughly the same as the session's lifetime.
- Public Key Infrastructures (PKI)
  - IKE can use public keys for peers authentication.
  - Some PKIs which can theoretically be used with IPsec:
    - PKIX (Public Key Infrastructure X.509)
    - SPKI (Simple Public Key Infrastructure)
    - DNSSEC
    - PGP signed keys

When considering the "keys" used in IPsec and IKE, you need to keep in mind that we are dealing with two types of keys: long-term keys, which are be used by IKE for peer authentication only, and short term keys, which are generated by IKE and used by IPsec to protect data.

IKE does not provide any management of certificates or long term keys in general. Shared secrets should be exchanged offline; public keys can be exchanged offline, by using another protocol, or during the IKE negotiation.

Key Exchange Protocols Properties

- Links between key exchange and mutual authentication
  - Key exchanges must be authenticated to prevent attacks.
  - A session key makes it possible to extend an initial authentication to the whole communication.
  - "Authentication and key exchange protocols" provide direct authentication and authenticated key exchange all-in-one.
- Perfect Forward Secrecy (PFS)
  - Even if an attacker discovers long-term secret(s), he will not be able to recover the session keys (past and future).
  - Provided when long-term secrets are only used for authentication and do not take part in session keys generation.
- Identity Protection
  - No identity is transmitted in the clear, so a spy can't know who the communicating peers are.

Diffie-Hellman

- What is the DH protocol?
  - Cryptographic protocol which enables two peers to generate a shared secret without any previous information on one another.
- Principle
  - Private values: a and b
  - Public values: $A = g^a \bmod n$ and $B = g^b \bmod n$
  - Shared secret: $K_{AB} = B^a \bmod n = g^{ab} \bmod n = A^b \bmod n = K_{BA}$
- Susceptible to a man-in-the-middle attack
  - The attacker, Eve, sends her public value in place of Alice's and Bob's and shares a secret with both peers.
  - Solution: authenticate the public values; the resulting protocol is called authenticated Diffie-Hellman.
- Provides perfect forward secrecy
  - Authenticated DH provides PFS if the long-term values are only used for authentication.

2. Key Management for IPsec

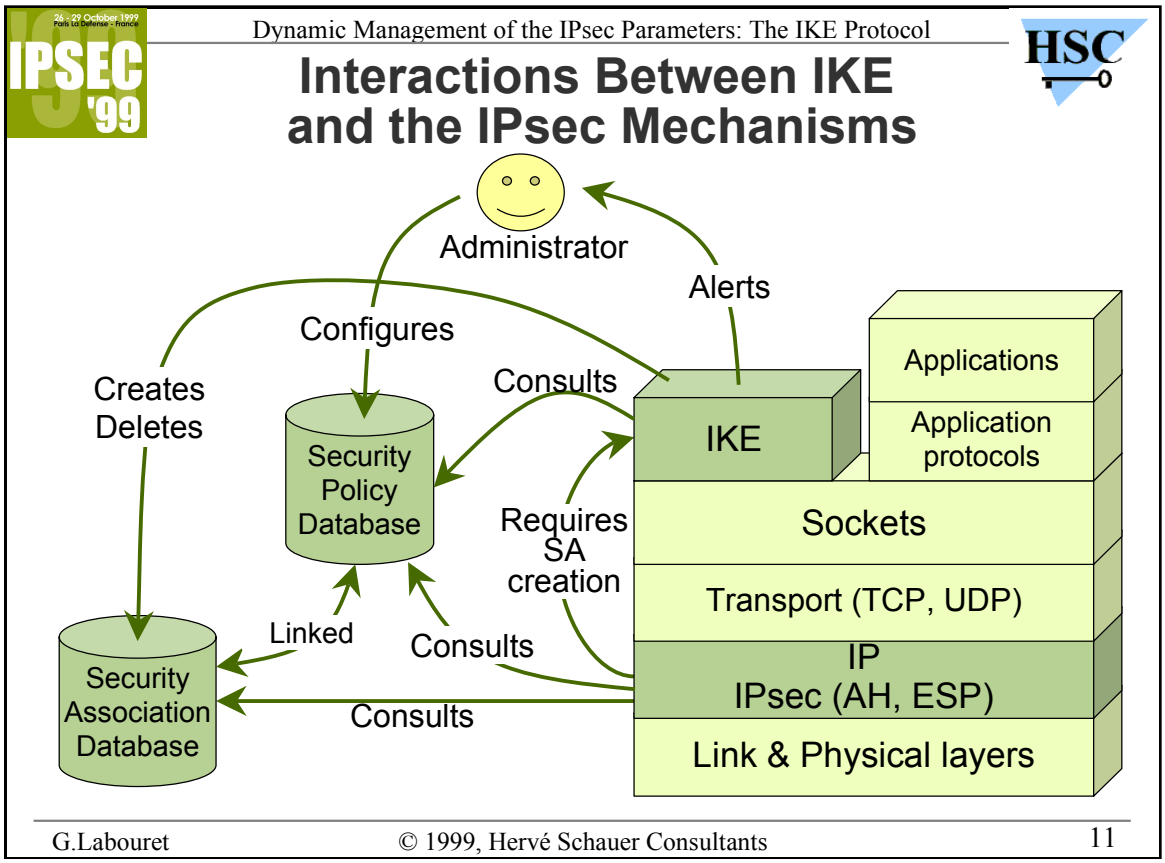
- More than just key management, it's about managing the security associations (SA)
  - Management of all the parameters related to securing a comunication (keys are just one parameter).
  - Concerns only the short-term parameters; no management of the long-term secrets or certificates.

Historical Reminder and Various Available Protocols

- **SKIP**
  - Created in 1994 by Sun Microsystems; ISAKMP/Oakley was preferred as the mandatory protocol for IPsec in September 1996; SKIP is still used in SunScreen SKIP product.
  - Connectionless protocol based on DH with long-term values; does not require any exchange before sending IPsec data.
  - Manages only keys, not the whole SAs.
- **Photuris**
  - Being developed since 1995; RFCs published in 1999; meant for IPsec but not mandatory so not included in many implementations.
  - Introduced the idea of anti-clogging tokens ("cookies").
- **ISAKMP/Oakley, renamed IKE (Internet Key Exchange)**
  - Hybrid of the Oakley and SKEME protocols that operates inside a framework defined by ISAKMP; default automated key management protocol selected for use with IPsec.
  - Generic and extensible protocol, but as a consequence very complex (lots of possible options).

IKE Overview

- Principle
  - Key management is separate from the security mechanisms; it is only linked to them through the SAs.
  - SAs are used by IPsec to define the processing done on a specific IP datagram; IKE manages the SAs (dynamic configuration, lifetime expiry enforcement…).
  - Connection oriented (uses UDP port 500).
- Provides:
  - Negotiation and management of IKE and IPsec parameters.
  - Authenticated secure key exchange with perfect forward secrecy (based on the Diffie-Hellman protocol).
  - Mutual peer authentication using public keys or a shared secret (beware: there is no protection against dictionary attacks, so the shared secret must be a real random key, not a password).
  - Identity protection when main mode is used (or aggressive mode authenticated with public key encryption).



We can consider that IPsec is located right under IP. Indeed, it processes outgoing IP packets before sending them across the network, and it receives incoming IPsec packets, which it verifies and decrypts before passing them to IP.

The administrator configures IKE and IPsec through the SPD; the SPD contains:
• ordered rules which indicate which traffic should be protected and how;
• the parameters IKE should use for its negotiations.

When the SPD indicates that outgoing traffic should be protected, IPsec consults the SAD to see if an appropriate SA is up. If not, it requests one from IKE.

IKE then consults the SPD to get all the parameters it needs and launches the negotiation.

If IKE negotiation is a success, a new SA bundle is created and stored in the SAD for use by IPsec.

One thing needs to be mentioned: IPsec must of course be configured to allow unprotected IKE traffic in (UDP 500).

3. IKE Internals

- How the IKE negotiations work (simplified)
- IKE is defined in RFC 2409, but I recommend reading the new draft from May 1999 if you want more info because it is easier to understand.

Course of the protocol

- Phase 1: Negotiate an ISAKMP SA
  - This SA will be used to protect the following IKE exchanges (confidentiality and authenticity).
  - The same ISAKMP SA can be used to protect several phase 2 negotiations; it has a longer lifetime than phase 2 SAs.
  - Two possible modes:
    - Main Mode (6 messages, provides identity protection)
    - Aggressive Mode (quicker, only 3 messages)
- Phase 2: Negotiate IPsec SAs (AH, ESP, IPCOMP)
  - Those SAs are used to protect data exchanges.
  - Two options: Quick Mode with or without PFS.
- Informational messages: used to report errors or notify SA deletion.

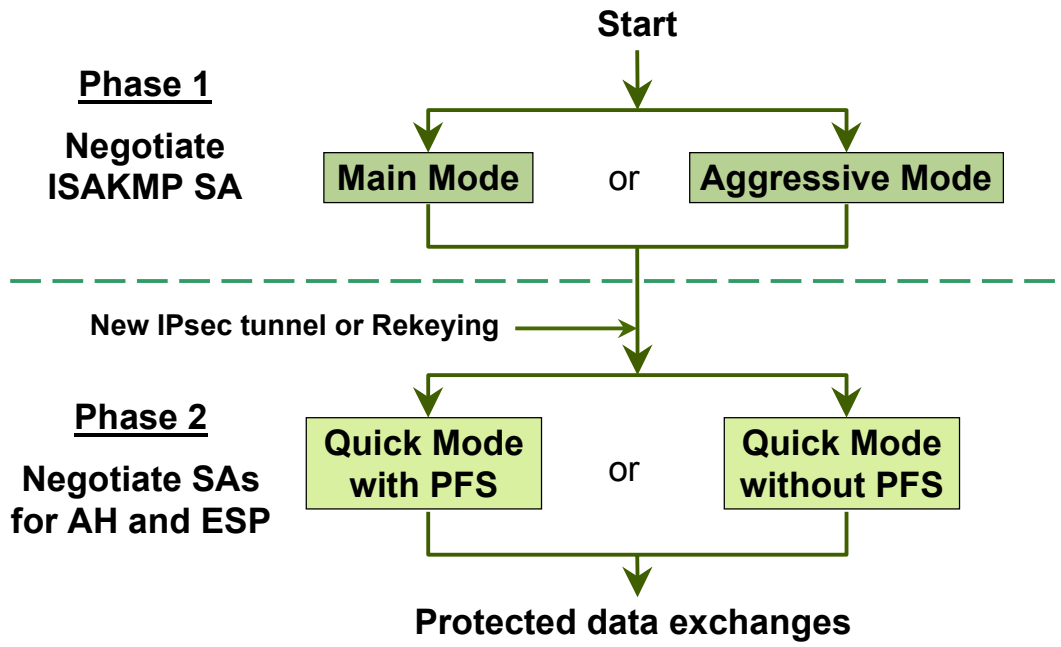
IKE has two phases, phase 1 and phase 2

The aim of phase 1 is to authenticate peers and establish a secure tunnel which will protect further IKE negotiations.

Phase 2 really establishes the IPsec SAs.

Phase 1 results in what is called an ISAKMP SA, because it is similar in concept to IPsec SAs. The main difference is that ISAKMP SAs are bi-directional, while IPsec SAs are unidirectional (you need two to protect a communication). But, in fact, phase 2 results in the creation of two symmetric SAs or SA bundles.

Phases and modes

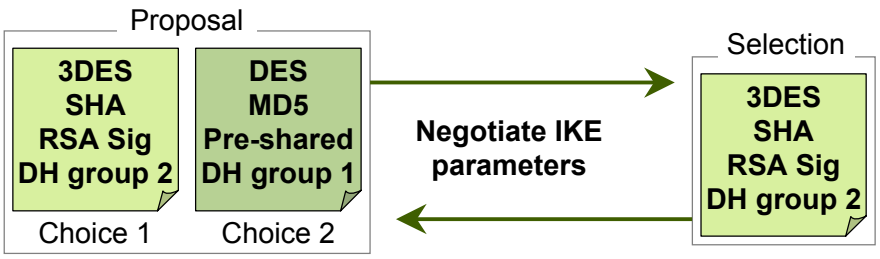


There are two possible modes during phase 1: main mode and aggressive mode, which have different properties.

Phase 2 has only one mode, but it can be used with or without additional PFS.

Other modes are defined in various drafts.

Phase 1 - Main Mode (1)
(simplified)



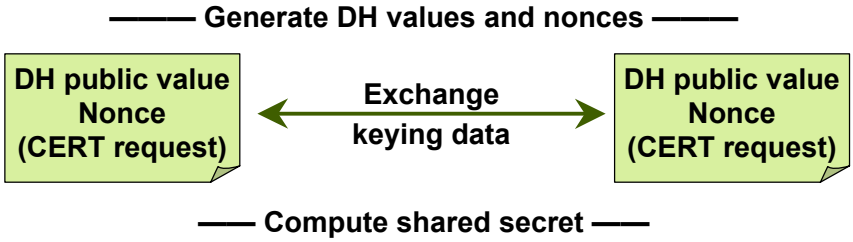
- First message pair's aim: Negotiate IKE parameters
  - Encryption algorithm (3DES, CAST, Blowfish, DES...)
  - Hash function (MD5, SHA or Tiger)
  - Authentication method:
    - pre-shared key
    - two forms of public key encryption (RSA or El-Gamal)
    - signature (RSA or DSA)
  - Group for Diffie-Hellman (numbered MODP and EC2N groups)

Main mode has 3 message pairs, which aims are, respectively, negotiate IKE parameters, exchange keying data and authenticate.

In this first message pair, the initiator sends a proposal, which can contain several choices, and the responder selects one of these. This is a really bare-bones negotiation!

The default authentication methods are used in a symmetric way, which is not well adapted to the client/gateway situation. As a consequence, extensions have been proposed which provide other authentication methods, in particular legacy authentication methods such as RADIUS and SecurID tokens.

Phase 1 - Main Mode (2)
(simplified)

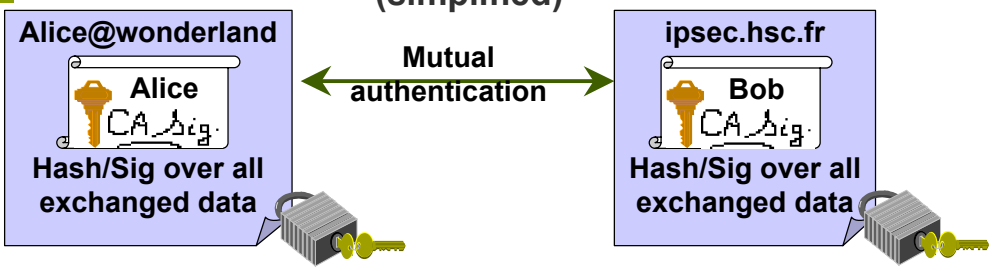


- Second message pair's aim: Establish a shared secret and derive IKE session keys
  - Uses Diffie-Hellman with the group agreed upon with the first message pair.
  - Two of the derived keys will be used, with the negotiated encryption algorithm and hash function, to protect the following IKE messages.
  - The nonces protect against replay by taking part in the shared secret computation.

If authentication with public key encryption was selected, the nonce are encrypted with the peer's public key.

Phase 1 - Main Mode (3)

(simplified)



- Third message pair's aim: Exchange and prove identities, retroactively authenticate the previous messages
  - ID types include IP address, email, X.500 distinguished name...
  - Uses the authentication method agreed upon with the first message pair (pre-shared secret, public key encryption or signature).
    - The shared secret has to be exchanged offline.
    - The public keys can be exchanged offline, by using another protocol, or online using certificate payloads.

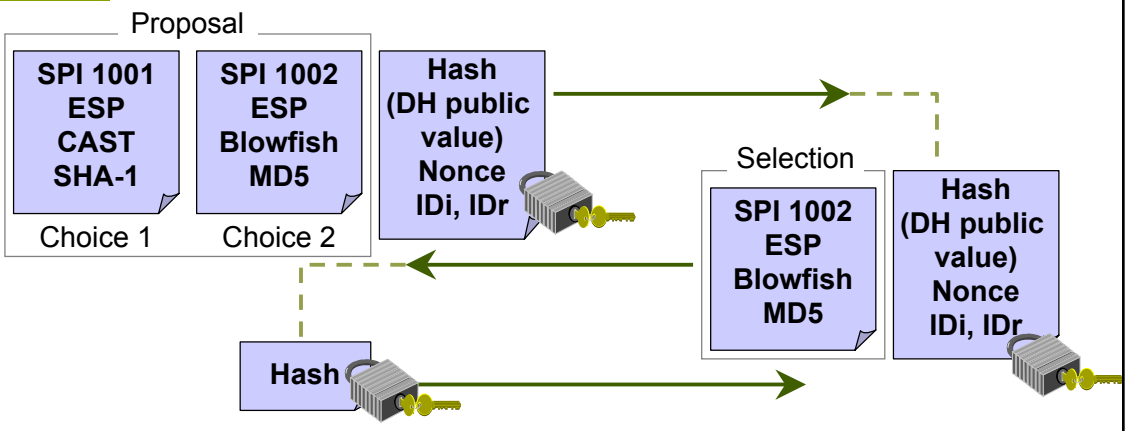
Those messages are encrypted, which provides identity protection.

They can optionally include the peers' certificates if certificates where requested in the previous exchange and if authentication with signature is used.

Phase 1 - Aggressive Mode

- Aggressive Mode combines data so as to reduce the number of total messages to three.
- Drawbacks of Aggressive Mode:
  - Parameters negotiation is limited.
  - No identity protection, except when using the public key encryption authentication methods.
  - More vulnerable do denial of service attacks.
- Drawback of Main Mode not present in Aggressive Mode:
  - When using the pre-shared key method for authentication, it is possible to use other IDs than the packets' IP addresses.

Phase 2 - Quick Mode



- Aim: Establish symmetric IPsec SAs
  - Negotiate IPsec parameters (SA bundles).
  - Exchange nonces to derive session keys from the IKE shared secret; optionally exchange DH values to generate a new key.
  - Optionally identify which traffic this SA bundle will protect using selectors (IDi and IDr payloads).

For Further Info

- How to contact me:
  Ghislaine.Labouret@hsc.fr
- Those slides are available online:
  http://www.hsc.fr/presentations/ike/
- Documents related to IPsec on HSC's web site:
  http://www.hsc.fr/veille/ipsec/