IPSEC Working Group
INTERNET-DRAFT
draft-ietf-ipsec-isakmp-oakley-00.txt
Expire in six months

D. Harkins, D. Carrel, Editors
cisco Systems

June 1996

The resolution of ISAKMP with Oakley
<draft-ietf-ipsec-isakmp-oakley-00.txt>

Status of this Memo

1. Abstract

[MSST96] (ISAKMP) provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independant; that is, it is designed to support many different key exchanges.

[Orm96] (Oakley) describes a series of key exchanges-- called "modes"-- and details the services provided by each (e.g. perfect forward secrecy for keys, identity protetion, and authentication).

This document describes a proposal for using the Oakley Key Exchange Protocol 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 ISAKMP Internet DOI.

2. Discussion

This draft combines ISAKMP and Oakley. The purpose is to negotiate, and provide authenticated keying material for, security associations

in a protected manner.

Processes which implement this draft can be used for negotiating virtual private networks (VPNs) and also for providing a remote user from a remote site (whose IP address need not be known beforehand) access to a secure network.

Proxy negotiation-- in which the negotiating parties are not the endpoints for which security association negotiation is taking place-- is supported. When used in proxy mode, identities of the end parties, remain hidden.

This proposal does not implement the entire Oakley protocol, but only the smallest subset necessary to satisfy its goals. It does not claim conformance or compliance with the entire Oakley protocol. For greater understanding of the Oakley protocol and the mathematics behind it, please refer to [Orm96].

3. Terms and Definitions

3.1 Requirements Terminology

In this document, the words that are used to define the significance of each particular requirement are usually capitalised. These words are:

- MUST

  This word or the adjective "REQUIRED" means that the item is an absolute requirement of the specification.

- SHOULD

  This word or the adjective "RECOMMENDED" means that there might exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before taking a different course.

- MAY

  This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor might choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

3.2 Notation

The following notation is used throughout this draft.

HDR is an ISAKMP header whose exchange type is the mode

SA is an SA negotiation payload with one or more proposals. An initiator MAY provide multiple proposals for negotiation; a responder MUST reply with only one.

KE is the key exchange payload.

NONCE is the nonce payload

IDx is the identity payload for "x". x can be: "ii" or "ir" for the ISAKMP initiator and responder respectively during phase one negotiation; or "ui" or "ur" for the user initiator and responder respectively during phase two. The ID payload format for the Internet DOI is defined in Appendix A of [MSST96].

SIG is the signature payload. The data to sign is exchange-specific.

CERT is the certificate payload.

HASH is the hash payload.

ENV{} is the envelope payload. The braces are not part of the protocol but are included to illustrate the payloads which are enveloped. These follow the envelope payload.

prf() is the keyed hash function negotiated as part of the ISAKMP SA.

SKEYID = prf(Ni | Nr, g^xy | cookie-I | Cookie-R).

--> signifies "initiator to responder" communication (requests).

<-- signifies "responder to initiator" communication (replies).

[x] indicates that x is optional.

Payload encryption (when noted by a '*' after the ISAKMP header) MUST begin immediately after the ISAKMP header. When communication is protected, all payloads following the ISAKMP header MUST be encrypted.

4. Introductuction

Since Oakley defines a method to establish an authenticated key exchange-- how payloads are constructed, the order in which they are processed and how they are used-- its modes MUST be valid ISAKMP exchange types.

The following attributes are required by Oakley and MUST be negotiated as part of the ISAKMP Security Association:

- encryption algorithm (e.g. DES, IDEA, Blowfish).

- hash algorithm (e.g. MD5, SHA)

- authentication algorithm (e.g. DSS, RSA)

- information about a group over which to do Diffie-Hellman.

The selected hash algorithm MUST support both keyed and unkeyed modes.

Oakley implementations MUST support the following default attributes:

- DES-CBC with a weak, and semi-weak, key check (weak and semi-weak keys are defined in [Sch94]). The first 8 non-weak bytes of keying material are used for the DES key.

- MD5 and SHA in native and HMAC mode.

- Digital Signature Standard. RSA SHOULD be supported.

- MODP over the default Oakley group (see below). ECP and EC2N groups MAY be supported.

In the Internet DOI, Oakley MUST be supported as a key exchange protocol. All other DOIs MAY use Oakley provided they implement the mandatory modes described below.

5. Exchanges

There are two basic methods used to establish an authenticated key exchange: Oakley Main Mode and Oakley Agressive Mode. Oakley in Main Mode MUST be implemented; Oakley Aggressive Mode SHOULD be implemented. In addition, Oakley Quick Mode MUST be implemented as a mechanism to generate fresh keying material. Oakley Quick Mode will provide keying material for all security associations negotiated with ISAKMP except the ISAKMP SA itself. In additon, Oakley New Group Mode SHOULD be implemented as a mechanism to define private groups for

Diffie-Hellman exchanges.

Exchanges are standard ISAKMP-- e.g. timeout and retransmit; notify response is given when a proposal is unacceptable, or a signature verification or decryption was unsuccessful, etc.

5.1 Oakley Main Mode

Oakley Main Mode in conjunction with ISAKMP is described as follows:

```
     Initiator                          Responder
    ----------                         -----------
     HDR, SA                    -->
                                <--     HDR, SA
     HDR, KE, NONCE(Ni)         -->
                                <--     HDR, KE, NONCE(Nr)
     HDR*, IDii, SIG [, CERT]   -->
                                <--     HDR*, IDir, SIG [, CERT]
```

where the signature in SIG is a hash of the concatenation of the cookies, g^xy, nonces, and IDs using the negotiated hash function. One or more certificate payloads MAY be optionally passed.

5.2 Oakley Aggressive Mode

Oakley Aggressive mode in conjunction with ISAKMP is described as follows:

```
     Initiator                          Responder
    -----------                        -----------
     HDR, SA, KE, NONCE, IDii   -->
                                <--     HDR, SA, KE, NONCE, IDir,
                                             SIG [, CERT]
     HDR, SIG [, CERT]          -->
```

where the signature in SIG is a hash of the concatenation of the cookies, g^xy, nonces, and IDs using the negotiated hash function. One or more certificate payloads MAY be optionally passed.

5.3 Oakley Quick Mode

Oakley Quick Mode is not a complete exchange itself, but is used as part of the ISAKMP SA negotiation process (phase 2) to derive keying material for the SA being negotiated. When used with SA negotiation, the information exchanged along with Oakley Quick Mode MUST be protected by the ISAKMP SA-- i.e. all payloads except the ISAKMP header are encrypted.

Quick Mode is essentially an exchange of nonces that provides replay protection. The nonces are used to generate fresh key material.

The envelope payload is used to group related payloads-- the negotiation proposal(s), nonce, and hash result-- into entities which MUST be treated as a whole.

In ISAKMP for the Internet DOI, Quick Mode appears as follows

```
     Initiator                        Responder
    -----------                      -----------
     HDR*, ENV{SA, Ni, HASH(1)}
           [, IDui, IDur ]     -->
                               <--    HDR*, ENV{SA,  Nr, HASH(2)}
                                            [, IDui, IDur ]
     HDR*, ENV{HASH(3)}        -->
```

Where:

```
   HASH(1) = prf( SKEYID, Ni )
   HASH(2) = prf( SKEYID, 1 | Nr | Ni )
   HASH(3) = prf( SKEYID, 0 | Ni | Nr )
```

The new keying material is defined as KEYMAT = prf(SKEYID, Ni | Nr) and MAY be used in the negotiated SA. If ISAKMP is acting as a proxy negotiator on behalf of another party the identities of the parties MUST be passed as IDui and IDur. Local policy will dictate whether the proposals are acceptible for the identities specified. If IDs are not exchanged, the negotiation is assumed to be done on behalf of each ISAKMP peer. If an ID range (see Appendix A of [MSST96]) is not acceptable (for example, the specified subnet is too large) an BAD_ID_RANGE notify message followed by an acceptible ID range, in an ID payload, MUST be sent.

Multiple SA's and keys can be negotiated with one exchange as follows:

```
     Initiator                        Responder
    -----------                      -----------
     HDR*, ENV1{SA1, Ni1, HASH1(1)},
           ENV2{SA2, Ni2, HASH2(1)}
           [, IDui, IDur ]     -->
                               <--    HDR*, ENV1{SA1, Nr1, HASH1(2)},
                                            ENV2{SA2, Nr2, HASH2(2)}
                                            [, IDui, IDur ]
     HDR*, ENV1{HASH1(3)},     -->
           ENV2{HASH2(3)}
```

Each enveloped entity is evaluated alone, components of entities MUST NOT be swapped. The initiator of the protocol can impose a selection criterion on the responder by using the Collate bit in the ISAKMP header. When this bit is set the responder MUST select the same ordinal proposal for all entities-- e.g. proposal three for ENV1 and proposal three for ENV2.

5.4 Oakley New Group Mode

Oakley New Group Mode MUST NOT be used prior to establishment of an ISAKMP SA. The description of a new group MUST only follow phase 1 negotiation. (It is not a phase 2 exchange, though).

```
     Initiator                          Responder
    -----------                        -----------
     HDR*, SA                 -->
                              <--       HDR*, SA
```

The proposal will be an Oakley proposal which specifies the characteristics of the group (see A.6 in [MSST96], "Oakley Attribute Classes"). Group descriptions for private Oakley Groups MUST be greater than or equal to 2^31. If the group is not acceptable, the responder MUST reply with a Notify payload with the message type set to GROUP_NOT_ACCEPTABLE (13).

ISAKMP implementations MAY require private groups to expire with the SA under which they were established.

Groups may be directly negotiated in the SA proposal with Oakley Main Mode. To do this the Prime, Generator, and Group Type are passed as SA attributes (see Appendix A in [MSST96]). Alternately, the nature of the group can be hidden using Oakley New Group Mode and only the group identifier is passed in the clear during Main Mode.

5.5 Oakley Groups

[Orm96] defines several groups. The value 0 indicates no group. The value 1 indicates the default group described below. Other values are also defined in [Orm96]. All values 2^31 and higher are used for private group identifiers.

5.5.1 Oakley Default Group

Oakley implementations MUST support a MODP group with the following prime and generator. This group is assigned id 1 (one).

The prime is: 2^768 - 2 ^704 - 1 + 2^64 * { [2^638 pi] + 149686 }
Its hexadecimal value is

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A63A3620 FFFFFFFF FFFFFFFF

The generator is: 2.

other groups can be defined using Oakley New Group Mode. This default group was generated by Richard Schroeppel at the University of Arizona. Properties of this prime are described by the following exerpt from [Orm96]:

> The prime for this group was selected to have certain properties. The high order 64 bits are forced to 1. This helps the classical remainder algorithm, because the trial quotient digit can always be taken as the high order word of the dividend, possibly +1. The low order 64 bits are forced to 1. This helps the Montgomery-style remainder algorithms, because the multiplier digit can always be taken to be the low order word of the dividend. The middle bits are taken from the binary expansion of pi. This guarantees that they are effectively random, while avoiding any suspicion that the primes have secretly been selected to be weak.
>
> The prime is chosen to be a Sophie-Germain prime (i.e., (P-1)/2 is also prime), to have the maximum strength against the square-root attack. The starting trial numbers were repeatedly incremented by 2^64 until suitable primes were located.
>
> Because this prime is congruent to 7 (mod 8), 2 is a quadratic residue. All powers of 2 will also be quadratic residues. This prevents an opponent from learning the low order bit of the Diffie-Hellman exponent. Using 2 as a generator is efficient for some modular exponentiation algorithms. [Note that 2 is technically not a generator in the number theory sense, because it omits half of the possible residues mod P. From a cryptographic viewpoint, this is a virtue.]

A further discussion of the properties of this group, the motivation behind its creation, as well as the definition of several more groups can be found in [Orm96].

5.6 Payload Explosion for Complete ISAKMP-Oakley Exchange

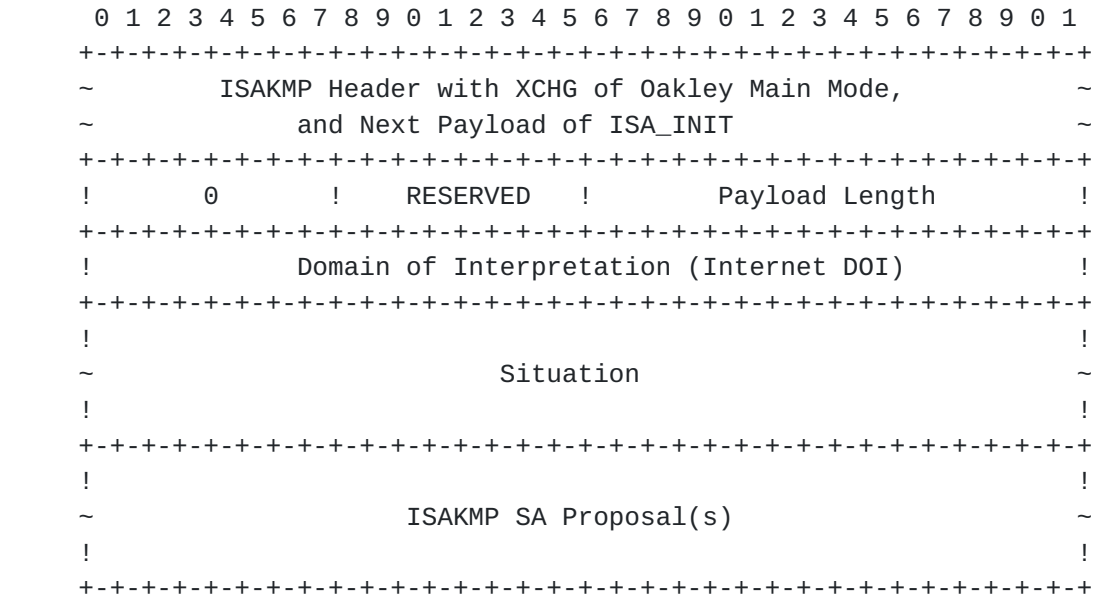
This section illustrates how ISAKMP payloads are used with Oakley to:

- establish a secure and authenticated channel between ISAKMP processes (phase 1); and

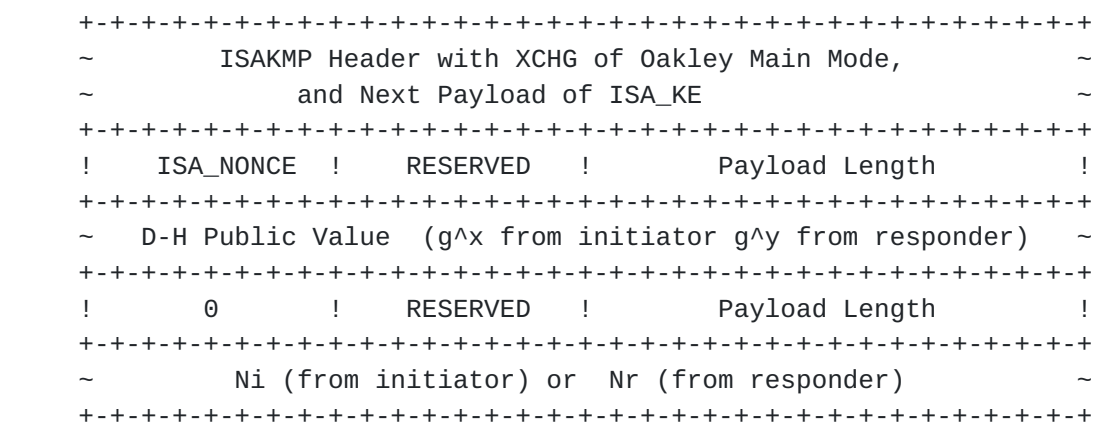
- generate key material for, and negotiate, an IPsec SA (phase 2).

5.6.1 Phase 1 using Oakley Main Mode

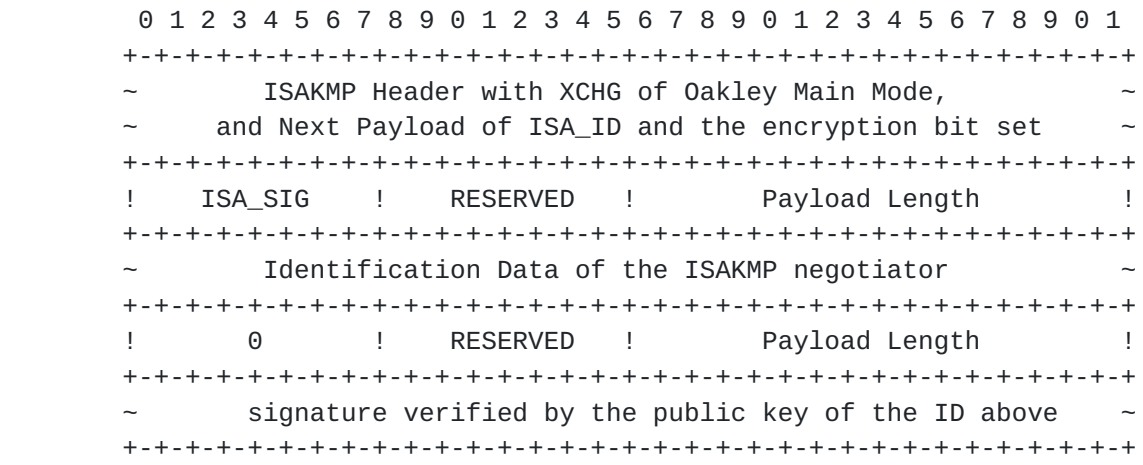
The following diagram illustrates the payloads exchanged between the two parties in the first round trip exchange. The initiator MAY propose several proposals; the responder MUST reply with one.



The second exchange consists of the following payloads:



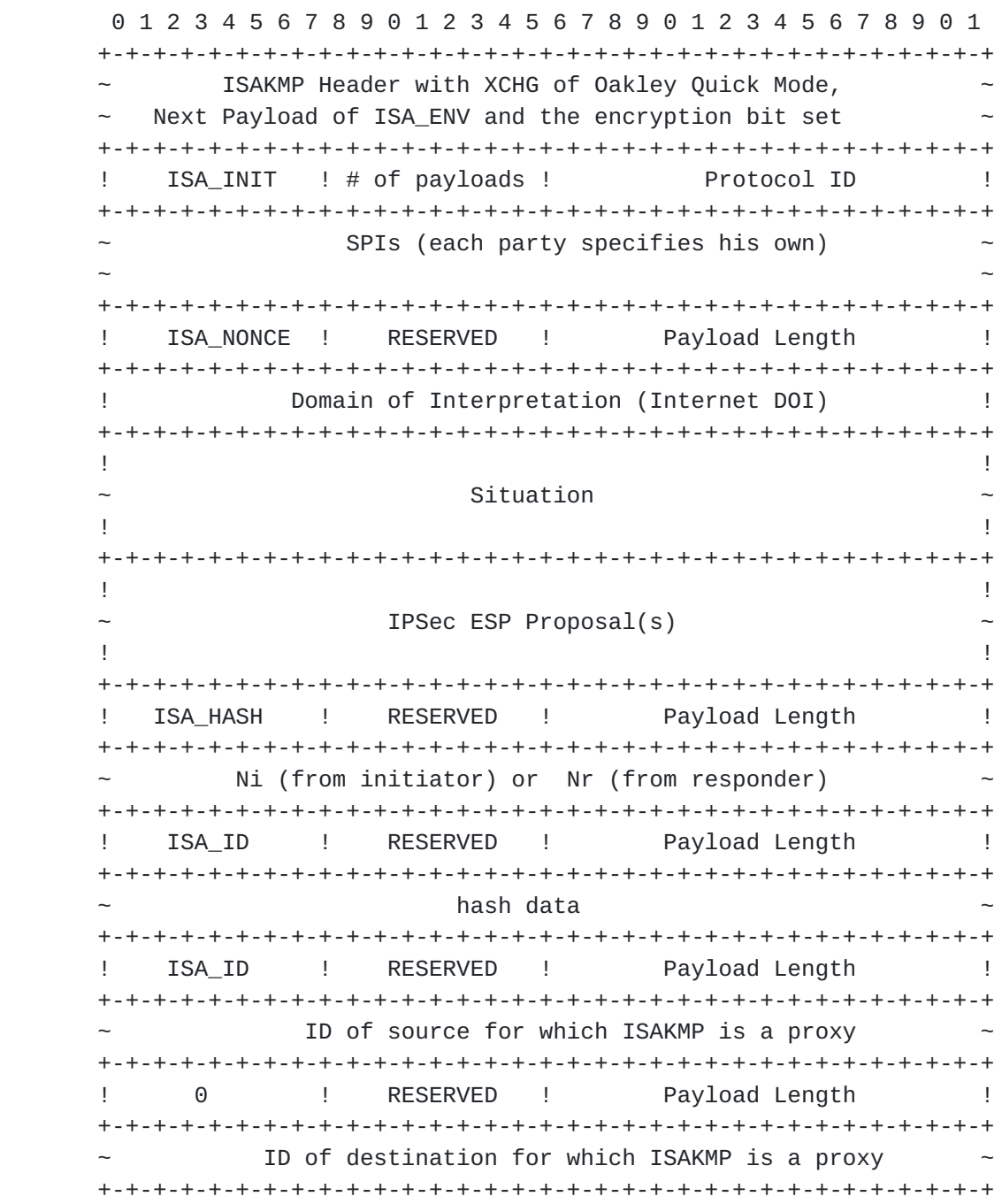
A shared key, SKEYID = prf(Ni | Nr, g^xy | Cookie-I | Cookie-R) where "prf" is the keyed hash function negotiated as part of the ISAKMP SA, is now used to protect all further communication. Note that SKEYID is unauthenticated.



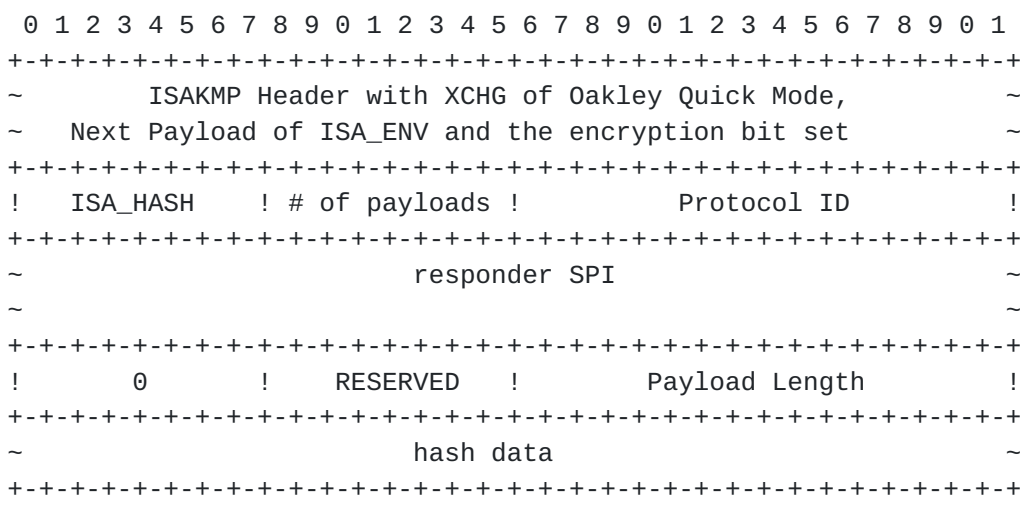
The key exchange is authenticated over a signed hash of the cookies, the nonces, the identities, and g^xy. Once the signature has been verified using the authentication algorithm negotiated as part of the ISAKMP SA, the shared key, SKEYID can be marked as authenticated. (For brevity, certificate payloads were not exchanged).

5.6.2 Phase 2 using Oakley Quick Mode

The following payloads are exchanged in the first round of Oakley Quick Mode with ISAKMP SA negotiation. In this hypothetical exchange, the ISAKMP negotiators are proxies for other parties which have requested security.



where the contents of the hash are described in 5.3 above. The # of Payloads field of the envelope payload is used to encapsulate the SA, nonce, and hash, and tie all three to the specified SPI. Upon receipt, and validation, of this payload, the initiator can provide the negotiation server (or key engine) with the negotiated security association and the keying material derived from Quick Mode. To prevent replay attacks from creating bogus security associations, the responder does not provide the security association and keying material until receipt and validation of the next payload.



where the contents of the hash are described in 5.3 above. The # of Payloads field of the envelope payload is used to associate the hash payload with the responder's SPI. At this point the responder has verified that the request was not the result of a replay attack and can provide the SA and key material to the negotiation server (or key engine).

To provide for secure duplex communication, the ISAKMP negotiators MUST construct two security associations for each accepted proposal. The first, identified by the SPI is from the source to the destination (in the event that there is no proxy negotiation it will be from initiator to responder); the second identified by the AUX-SPI is from the destination to the source (or responder to initiator).

6. Security Considerations

This entire draft discusses a hybrid protocol, combining Oakley with ISAKMP, to negotiate, and derive keying material for, security associations in a secure and authenticated manner.

Confidentiality is assured by the use of a negotiated encryption algorithm. Authentication is assured by the use of a negotiated digital signature algorithm. The confidentiality and authentication of this exchange is only as good as the attributes negotiated as part of the ISAKMP security association.

Repeated re-keying using Quick Mode can consume the entropy of the Diffie- Hellman shared secret. Implementors should take note of this fact and set a limit on Quick Mode Exchanges between exponentiations. This draft does not proscribe such a limit.

7. Acknowledgements

This document is the result of close consultation with Hilarie Orman, Douglas Maughan, Mark Schertler, Mark Schneider, and Jeff Turner. It relies completely on protocols which were written by them. Without their interest and dedication, this would not have been written.

We would also like to thank Cherly Madson and Harry Varnis for technical input.

8. References

[MSST96] Maughhan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", version 5, draft-ietf-ipsec-isakmp-05.{ps,txt}.

[Orm96] Orman, H., "The Oakley Key Determination Protocol", version 2, draft-ietf-ipsec-oakley-02.txt.

[Sch94] Schneier, B., "Applied Cryptography, Protocols, Algorithms, and Source Code in C", 1st edition.

Editors' Addresses:

Dan Harkins <dharkins@cisco.com>
Dave Carrel <carrel@cisco.com>
cisco Systems
170 W. Tasman Dr.
San Jose, California, 95134-1706
United States of America
+1 408 526 4000

Editors' Note:

The editors encourage independent implementation, and interoperability testing, of this hybrid exchange.