IP Security working group
Internet Draft

Baiju V. Patel,
Michael Jeronimo,
Intel Corp.

Document: draft-ietf-ipsec-isakmp-SA-revised-00.txt
November, 1997

Revised SA negotiation mode for ISAKMP/Oakley

Status of this Memo

1. Abstract

ISAKMP/OAKLEY [2][3] is the key management protocol defined by IPSEC working to be a framework for authentication, security association negotiation and key management. The protocol defines two phases whereby, in the phase 1, the peers are authenticates, the security association (SA) for ISAKMP/Oakley, and keying material is agreed upon by the peers to secure ISAKMP messages. The phase 2 is used to negotiate security association for security applications (e.g., IPSEC AH and ESP). When perfect forward secrecy is required, phase 2 is also used to exchange keying material for the application. However, when perfect forward secrecy is not a requirement, the keying material from the phase 1 is used to generate session keys for the secure communication applications.

The proposal in this document is based on the observation that when perfect forward secrecy is not a requirement, if application

specific SA was negotiated during phase 1, the application can start immediately after phase 1. The phase 2 can be used subsequently for key refresh on per need bases in the future. Therefore, this proposal reduces startup time for communication and improves the efficiency of the protocol.

Remark: This document is NOT self-contained, it is intended as an addendum to [2][3]. Thus, it is best read in conjunction with [2][3].

2. Revised modes of ISAKMP/Oakley

2.1. Notation

SA_App: is an SA negotiation payload with one or more proposals

specific to the application (e.g., IPSEC AH or ESP),

SA_App_p: is the entire body of the SA_App payload (minus the ISAKMP

generic header) -- i.e., the DOI, situation, all proposals, and all

transforms included in SA_App.

HASH_I =

prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | Sap | SA_App_p | IDii)

HASH_R =

prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAp | SA_App_p | IDir)

Observe that the HASH-I and HASH-R functions in this revised mode

include application specific SA's. This a change from the

specification in [3].

Unless otherwise specified, all the notations used in this document

are same as those in [3].

2.2. Phase 1 authenticated with Signatures

Main Mode with signature authentication is described as follows:

```
Initiator                          Responder

----------                         -----------

HDR, SA                    -->

                           <--     HDR, SA

HDR, KE, Ni                -->

                           <--     HDR, KE, Nr

HDR*, IDii, SA_App [ CERT, ] SIG_I -->

                           <--     HDR*, IDir, [ CERT, ] SIG_R
```

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

```
    Initiator                          Responder

  -----------                        -----------

HDR, SA, SA_App, KE, Ni, IDii       -->
```



```
                           <--     HDR, SA, SA_App, KE, Nr,

                                     IDir, [ CERT, ] SIG_R

HDR, [ CERT, ] SIG_I       -->
```

2.3.

Phase 1 Authenticated With Public Key Encryption

When using encryption for authentication, Main Mode is defined as follows.

```
Initiator                          Responder
-----------                        -----------
HDR, SA                    -->
                           <--     HDR, SA
HDR, KE, [ HASH(1), ]
     <IDii>PubKey_r,
     <Ni>PubKey_r           -->
                                    HDR, KE, <IDir>PubKey_i,
                           <--             <Nr>PubKey_i
HDR*, SA_App, HASH_I                -->
                           <--     HDR*, SA_App, HASH_R
```

Aggressive Mode authenticated with encryption is described as follows:

```
 Initiator                          Responder
 -----------                        -----------
 HDR, SA, SA_App, [ HASH(1),] KE,
    <IDii>Pubkey_r,
    <Ni>Pubkey_r            -->
                                    HDR, SA, SA_App, KE,
                                         <IDir>PubKey_i,
                            <--          <Nr>PubKey_r, HASH_R
 HDR, HASH_I                -->
```

Where HASH(1) is a hash (using the negotiated hash function) of the certificate which the initiator is using to encrypt the nonce and identity.

2.4. Phase 1 Authenticated With a Pre-Shared Key

When doing a pre-shared key authentication, Main Mode is defined as follows:

```
Initiator                          Responder
----------                         -----------
HDR, SA                 -->
                        <--     HDR, SA
HDR, KE, Ni             -->
                        <--     HDR, KE, Nr
HDR*, SA_App IDii, HASH_I  -->
                        <--     HDR*, SA_App, IDir, HASH_R
```

Aggressive mode with a pre-shared key is described as follows:

```
Initiator                       Responder
-----------                     -----------
HDR, SA, SA_App, KE, Ni, IDii -->
                      <--    HDR, SA, SA_App, KE, Nr, IDir, HASH_R
HDR, HASH_I           -->
```

3. Security Considerations

This draft defines a security protocol.

4. References

[1]. Bradner, S, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, Harvard University, March 1997.

[2]. Maughhan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", version 8, draft-ietf-ipsec-isakmp-08.{ps,txt}.

[3]. D. Harkins, D. Carrel, "The resolution of ISAKMP with Oakley", Internet Draft, <draft-ietf-ipsec-isakmp-oakley-04.txt>, July 1997

[4]. Krawczyk, H., Bellare, M., Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[5]. Schneier, B., "Applied Cryptography, Protocols, Algorithms, and Source Code in C", 2nd edition.

5. Acknowledgments

This draft is largely based on the Dan Harkin's IETF draft on ISAKMP/OAKLEY resolution.

6. Author's Addresses

Baiju V. Patel
Intel Corp
2511 NE 25th Ave
Hillsboro, OR 97124
Phone: 503 264 2422
Email: baiju@mailbox.jf.intel.com

Michael Jeronimo
Intel Corp
2511 NE 25th Ave
Hillsboro, OR 97124
Phone: 503 264 5970
Email: jeronim@ccm.jf.intel.com