IPSEC Working Group
INTERNET-DRAFT
draft-ietf-ipsec-revised-enc-mode-01.txt
Expire in six months

R. Canetti, P. Cheng, H. Krawczyk
IBM Research and the Technion

July 1997

A revised encryption mode for ISAKMP/Oakley
<draft-ietf-ipsec-revised-enc-mode-01.txt>

Status of this Memo

1. Abstract

The ISAKMP/Oakley document [HC97] describes a proposed standard for using the Oakley Key Exchange Protocol in conjunction with ISAKMP to obtain authenticated and secret keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

The public-key encryption method of carrying out Phase 1 of the key exchange in the ISAKMP/Oakley document provides significant security advantages over the other alternatives and should be the method of choice in many implementations. Unfortunately, as currently described in [HC97] the method requires two public key encryption and decryption operations from both the Initiator and the Responder. The present document describes a small modification to this method. The resulting scheme requires only one public key encryption and decryption operation from each party, while maintaining (and even improving on) the strong security properties of the ISAKMP/Oakley public-key encryption mode.

Remark: This document is NOT self-contained, it is intended as an addendum to the authentication methods defined in [HC97].

In particular, it uses notation and definitions of [HC97].
Thus, it is best read in conjunction with [HC97].

2. Introduction

The ISAKMP/Oakley protocol [HC97] defines three alternative methods of carrying out Phase 1 of the key exchange. Two of these methods are usable by parties that do not already share a secret key. These are the Signature Method (Section 5.1 in [HC97]) and the Encryption Method (Section 5.2 in [HC97]).

The Encryption Method enjoys several significant advantages over the Signature Method. These advantages are sketched in Section 5. However, in the ISAKMP/Oakley draft the Encryption Method requires TWO public key encryption and decryption operations for each party. This is unnecessarily expensive. (In overloaded or weak processors the extra exponentiation may have a significantly adverse effect in performance.)

This document describes a simple modification of the ISAKMP/Oakley Encryption Method. The resulting method enjoys the same security advantages, and requires only ONE public key encryption and decryption operation for each party. This method, called the Revised Encryption Method, is presented as an alternative method to the ISAKMP/Oakley Encryption Method. In fact, the revised method enjoys even additional security advantages on top of the ISAKMP/Oakley Encryption Method, as elaborated below. The required changes are minimal.

The change from the ISAKMP/Oakley Encryption Method is basically as follows. There, each party's identity and nonce are encrypted via TWO separate applications of the public-key encryption algorithm. (In fact, if the party's identity is long then this may require additional applications of the public-key encryption algorithm.)

In the Revised Encryption Method the nonce is still encrypted using the public-key encryption algorithm. However, the sending party's identity (and also the certificate, if it is sent) is encrypted via symmetric encryption (e.g. DES), with a key derived from the nonce. This solution adds no significant complexity to the implementation and saves a costly long (RSA or other) exponentiation. In addition, the Key Exchange payload (ie. the DH challenges) is also encrypted using the same derived key. This provides additional protection against cryptanalysis of the DH exchange.

The Revised Encryption mode has another advantage. The (optional) Certificate payload is also encrypted using the same derived key. Consequently anonymity is preserved even if the certificate is sent as part of the exchange.

The rest of this document is organized as follows. In Section 3 the Revised Encryption Method is described. The description is written in a way so that Section 3 can be read as a replacement to

Section 5.2 in [HC97]. Section 4 specifies default algorithms.

Section 5 discusses some security advantages of the Encryption Method relative to the Signature method. (These advantages are shared by the Revised Encryption Method.) Appendix A holds the authentication method value of the new method (see ISAKMP [MSST96] and Appendix A of [CH97]).

3. The new method: Revised Encryption Method of Oakley Phase 1

Using public key encryption to authenticate the exchange, the ancillary information exchanged is encrypted nonces. Each party's ability to reconstruct a hash (proving that the other party decrypted the nonce) authenticates the exchange.

In order to perform the public key encryption, the initiator must already have the responder's public key. In the case where a party has multiple public keys, a hash of the certificate of the initiator used to encrypt the ancillary information is passed as part of the third message. In this way the responder can determine which corresponding private key to use to decrypt the encrypted payloads and identity protection is retained.

The nonces are encrypted with the other party's public key. The Key Exchange payloads (KE) and the identities of the parties (IDii and IDir) are encrypted with the negotiated symmetric encryption algorithm (e.g DES), using a key derived from the nonce. If the Initiator's certificate is passed from Initiator to Responder then, for anonymity, the certificate is also encrypted under the same key. In all these cases only the body of the payload is encrypted, the payload header is left in the clear; and the length field in the payload header is the length of the ciphertext (including any pre-pended information and padding) plus the size of the payload header.

That is, Phase 1 (Main Mode) is defined as follows.

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

HASH(1) is a hash (using the negotiated hash function) of the responder's certificate which the initiator is using to encrypt the nonce.

The values of HASH_I and HASH_R are as defined in [HC97], namely,

```
HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAp | IDii)
HASH_R = prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAp | IDir)
```

with SKEYID (also defined in [HC97]) being:

```
SKEYID = prf(Ni | Nr, CKY-I | CKY-R)
```

The notation <...>PubKey refers to public key encryption (e.g. using the RSA algorithm) while the notation <...>Ke refers to encryption under the negotiated symmetric cipher. The keys for the symmetric cipher are derived as follows. First, compute the values Ne_i and Ne_r:

```
Ne_i = prf(Ni, CKY-I)
Ne_r = prf(Nr, CKY-R)
```

Next, the keys Ke_i and Ke_r are derived from Ne_i and Ne_r, respectively, in the way described in Appendix B of [HC97]. That is, to derive Ke_i run the procedure described in Appendix B of [HC97] for deriving encryption keys used to protect the ISAKMP SA, but replacing SKEYID_e with Ne_i. To derive Ke_r run the procedure described in Appendix B of [HC97], where SKEYID_e is replaced by Ne_r.

For completeness, we detail the procedure for deriving Ke_i. Ke_r is derived analogously. If the desired length of Ke_i is at most the length of Ne_i then Ke_i is the sufficient number of most significant bits of Ne_i. If the desired length of Ke_i exceeds the length of Ne_i then more bits are generated by applying the prf with Ne_i as the key and a byte of 0 as the input. The output of the prf is fed back into itself until sufficient number of bits are generated. For example, if the output of prf is 128-bit long and Ne_i needs to be 320-bit long, then Ne_i is the most significant 320 bits of K, where K = K1 | K2 | K3 and

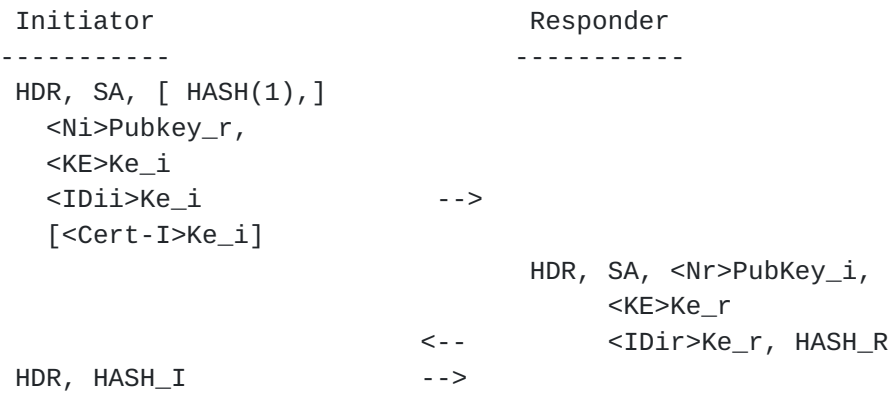
```
K1 = prf(Ne_i, 0)
K2 = prf(Ne_i, K1)
K3 = prf(Ne_i, K2)
```

Note that the values of Ke_i and Ke_r are ephemeral and discarded after this use.

If CBC mode is used for the symmetric encryption then the initialization vectors (IV) are set as follows. The IV for encrypting KE is set to 0. The IV for encrypting IDii (resp., IDir) is the last ciphertext block of <KE>Ke_i (resp., <KE>Ke_r). The IV for encrypting the certificate is the last ciphertext block of <IDii>Ke_i (resp., <IDir>Ke_r). Encrypted payloads are padded up to the nearest block size. All padding bytes, except for the last one, contain 0x00. The last byte of the padding contains the number of the padding bytes used, excluding the last one. Note that this means that there will always be padding. Note also that the IV chaining method used here implies that KE, the ID and the certificate have to be encrypted in that order. (We stress that this encryption order does not require that these payloads appear in that same order in the ISAKMP message; indeed [MSST96] does allow for arbitrary ordering of these payloads).

When a Certificate payload is sent in the context of the Revised Encryption Method, it MUST be encrypted in the manner described above.

Oakley Aggressive Mode in conjunction with the Revised Encryption Method is described as follows (using the same notation as above):



RSA encryption MUST be encoded in PKCS #1 format. The PKCS #1 encoding allows for determination of the actual length of the cleartext payload upon decryption.

4. Algorithms

The above mode can use any public key encryption algorithm. Implementations SHOULD support RSA encryption (see Appendix A for the corresponding authentication method value), and MUST support DES-CBC as specified in [HC97] for payload encryption.

5. Security Considerations

In this section we sketch the advantages of authentication by public-key encryption, as opposed to authentication by signature. First, in the Encryption mode an attacker has to break BOTH the the public key encryption in use (e.g. RSA) and DH exchange in order to learn the agreed key. In the Signature Mode breaking the DH exchange is sufficient. This is a substantial security advantage in a scenario where the same prime is used to secure a large number of exchanges: such a prime will become an attractive target for cryptanalysis, thus it may provide only weak security. It also adds protection against a party that chooses weak parameters in the DH exchange, such as a weak prime or short exponents. This aspect of security is further enhanced by the encryption of the KE payload.

Next, using encryption for authentication provides for a plausibly deniable exchange. There is no proof (in contrast to the use of digital signatures) that the conversation ever took place since each party could have generated both sides of the exchange.

Furthermore, unlike other authentication methods, authentication with public key encryption allows for identity protection even in Aggressive Mode (even certificates are protected in this case).

We remark that both the ISAKMP/Oakley Encryption Method and the Revised Encryption method described here are based on a similar mode in [Kra96] where a more extensive discussion on the above issues and analysis of security can be found.

6. Acknowledgments

We thank Dan Harkins for helpful discussions and suggestions.

7. References

[HC97] Harkins, D. and D. Carrel, "The resolution of ISAKMP with Oakley", draft-ietf-ipsec-isakmp-oakley-04.txt, July 1997.

[Kra96] Krawczyk, H., "SKEME: A Versatile Secure Key Exchange Mechanism for Internet", from IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security.

[MSST96] 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}.

[Pip96] Piper, D., "The Internet IP Security Domain Of Interpretation

for ISAKMP", version 3, draft-ietf-ipsec-ipsec-doi-03.txt.

Appendix A: XCHG attribute assigned number

This Appendix defines a new authentication method value for the Revised Encryption Method. This value is to be negotiated in Phase 1 (see [MSST96] and Appendix A in [HC97]). The value is:

authentication method value	
Revised RSA Encryption	5

Authors' Addresses:

Ran Canetti
IBM TJ Watson Research Center
POB. 704, Yorktown Heights,
NY 10598
Tel. 1-914-784-7076
canetti@watson.ibm.com

Pau-Chen Cheng
IBM TJ Watson Research Center
POB. 704, Yorktown Heights,
NY 10598
Tel. 1-914-784-7446
pau@watson.ibm.com

Hugo Krawczyk
IBM TJ Watson Research Center
POB. 704, Yorktown Heights,
NY 10598
hugo@ee.technion.ac.il