Key Recovery Alliance TMarkham
INTERNET DRAFT Secure Computing Corporation
Catagory: Experimental August 1998

ISAKMP Key Recovery Extensions
<draft-rfced-exp-markham-01.txt>

Status of This Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this document is unlimited.

This contribution has been prepared to assist the Key Recovery Alliance. This proposal is made by the authors as a basis of discussion. This contribution should not be construed as a binding proposal on the authors or their companies. Specifically, the authors and their companies reserve the right to amend or modify the statements contained herein.

Comments on this document should be sent to key-recovery@raleigh.ibm.com.

Table of Contents

1. INTRODUCTION

ABSTRACT

This document describes the proposed approach for negotiating and exchanging key recovery information within the Internet Security Association Key Management Protocol (ISAKMP).

This document describes the method for transmitting the Common Key Recovery Block (CKRB) when two entities establish a security association using ISAKMP [DM97]. ISAKMP is used to negotiate the mechanism to carry key recovery information carried within the CKRB as specified in [SG98].

Section 2, Requirements, Goals And Issues, provides background information on the technical approach and rational.

Section 3, Typical Use provides information on the Key Recovery Mechanism (KRM) negotiation and use of the ISAKMP notify to carry the CKRB.

Section 4, Acknowledgments

Section 5, References

Section 6, Author information

2. REQUIREMENTS, GOALS AND ISSUES

This section explains the proposed approach and rational for inserting key recovery into ISAKMP.

2.1 Requirements and Goals

The following have been identified as requirements or goals for key recovery within the context of ISAKMP.

o Interoperability: The key recovery mechanisms must allow interoperability to the greatest extent allowed by the applicable security policies. Key recovery aware implementations MUST be able to interoperate with other key recovery aware implementations. Non-key recovery aware implementations SHOULD be able to interoperate with key recovery aware implementations.

o Business requirements: The key recovery mechanism must allow organizations to comply with government regulations with respect to the use of encryption. The mechanism must also allow an organization to defend its business practices by monitoring intra- and inter-organization communications within legal limits. This requires

that the organization must be able to intercept the CKRB at the time of key establishment or periodically while the security association remains active. This requires that the key recovery enabled entity transmit the CKRB during the key establishment protocol and every N hours during the security association.

o Government Requirements: Governments must be able to intercept the CKRB at the time of key establishment or periodically while the security association remains active. This requires that the key recovery enabled entity transmit the CKRB during the key establishment protocol and every N hours during the security association.

o ISAKMP compatibility: The key recovery approach must maintain compatibility with ISAKMP.

o Security: The key recovery mechanisms must negligibly reduce the strength of the cryptographic system.

2.2 Issues

o Subvertability: The key recovery information SHOULD be bound to the ISAKMP negotiation in a way which makes it difficult to subvert the key recovery function. However, the binding mechanism used SHOULD be no stronger than necessary to meet the reasonable business and Government evaluation criteria. Mechanisms which increase complexity and cost beyond what is required to meet these requirements SHOULD be avoided.

o Changing IETF ISAKMP: The IETF ISAKMP is not an RFC yet.
The key recovery mechanism must be reviewed as ISAKMP evolves.

2.3 Requirements Terminology

In this document, the words that are used to define the significance of each particular requirement are usually capitalized. 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. KEY RECOVERY WITHIN ISAKMP

3.1 Overview

The CKRB [SG98] may be passed across the network using two methods in the ISAKMP/IPSEC environment. When key recovery is required and ISAKMP is used, the CKRB MAY be transmitted in the ISAKMP notify message. When key recovery is required and ISAKMP is not used, the CKRB MUST be transmitted in the IPSEC Key Recovery Header (KRH).

ISAKMP will be used to negotiate the use of the KRM in much the same way that the use of AH and ESP are negotiated. Two entities will negotiate and pick a proposal which may include AH, ESP and the KRM. The peer ISAKMP MUST always be notified when key recovery will be applied to the IPSEC security association. Key recovery is not applied to the ISAKMP Phase I security association. Some policies may allow ISAKMP to negotiate the use of weaker cryptography (e.g., 40 bit) if the peer device rejects the proposal(s) to do key recovery.

The values for the KRMs are defined in the IPSEC key recovery DOI. (A draft version of the proposed DOI values are included as an appendix to this document.) The KR negotiation addresses the following parameters independently for initiator and responder;

- Key Recovery Mechanism: This is a security association attribute. Example KRMs include IBM, Cylink, TIS, Any (key recovery is required but any mechanism recognized by policy is accepted), or none (no key recovery).

- KRH Interval: The KRH protocol is a header similar in concept to AH. The KRH protocol is described in [CW98]. The negotiation includes the interval, in seconds, at which the KRH will be sent. A value of zero indicates that the KRH will never be sent.

This negotiation and transmission of the CKRB only occurs within the context of an ISAKMP phase 2 exchange. Key recovery is not applied to ISAKMP phase 1 exchanges.

3.2 Exchange of CKRBs in ISAKMP

The ISAKMP proposal negotiation process allows the initiator to create an ordered set of proposals. The responder is required to pick from one of these proposals or send a message indicating that all proposals were rejected. There are many permutations of sender and receiver

policies/implementations which affect interoperability. The key recovery negotiation is actually a pair of negotiations due to the asymmetric nature of key recovery. The initiator sends the responder two sets of proposals. One proposal addresses what key recovery, if any, the initiator will do. The other addresses what key recovery, if any, the responder will do.

This subsection outlines multiple cases of exchanging the byte oriented CKRB within the ISAKMP phase 2 exchange. Please see the ISAKMP specification [DM99] for complete information on the negotiation process. The integrity mechanisms to protect the CKRB are negotiated as part of the negotiation to determine the KRM to be used.

The exchanges of interest are:

- Initiator does key recovery but responder does not
- Initiator does not do key recovery but responder does
- Initiator and responder do key recovery

Two entities which MUST perform key recovery could fail to negotiate a security exchange if the KRM negotiation fails. A device which is key recovery unaware cannot prevent the peer device from sending a CKRB. The examples below provide an overview of the exchange process. Detailed protocol information is contained in subsection **3.2.4 - Security Association and Attributes 3.2.5 - Security Protocol.**

3.2.1 Initiator does key recovery but responder does not

In this example assume the initiator MUST do key recovery and the responder will not issue a CKRB but will communicate with initiators which issue CKRBs.

1. The initiator creates two ordered sets of proposals. The initiator must do key recovery so all of the proposals which apply to the initiator contain the KRM(s) as part of the proposed suite(s). The set of proposals which apply to the responder contain key recovery and non-key recovery options. These proposals are sent to the responder.

2. The responder picks one proposal to be applied to the initiator and one proposal to be applied to the responder. If none of the initiator proposals are accepted or none of the responder proposals are accepted, the responder sends the initiator an error message indicating the reason for the rejection.

The responder may not understand the proposals because of the KRM. If this occurs, the initiator MAY omit the KRM from the proposals and simply exchange the CKRB within the ISAKMP notify message. The initiator is responsible for ensuring the lifetime of the security association conforms to local policy.

NOTE: This could lead to situations in which key recovery is

supported without the explicit consent of the responder. Implementations which MUST NOT support key recovery MUST terminate the security association when a CKRB is received.

3. The initiator completes the ISAKMP exchange and sets the commit bit within the ISAKMP header. This informs the responder that it must not use the newly created security association until the initiator sends an informational exchange carrying the notify payload indicating the security association may be used.

4. The responder completes the ISAKMP exchange and waits for the notify from the initiator.

5. The initiator prepares the notify payload containing the CKRBs. One CKRB contains the initiator to responder key and the other CKRB contains the responder to initiator key. The notify message value indicates that the security association may now be used. The initiator sets the encryption bit/flag to 0, indicating that the payload is not encrypted, and sends this notify payload to the responder. The message will be protected by the ISAKMP authentication mechanism but it will not be encrypted. The authentication prevents undetected tampering with the contents of the CKRBs yet allows the CKRBs to be intercepted. This notify message SHOULD NOT contain payloads which require confidentiality protection.

6. Both initiator and responder may use the security association when the responder receives and processes the notify message. If the notify message has been corrupted, the responder performs the standard ISAKMP processing.

The setting and resetting of the commit bit by multiple protocols within a single device is the local responsibility of that device. For example, if both key recovery and ESP within the initiating device set the commit bit, the logic within the initiating device determines when the notify message may be sent to clear the commit bit.

3.2.2 Initiator does not do key recovery but responder does

In this example assume the initiator is not key recovery aware but the responder must issue a CKRB. The responder is allowed to communicate with initiators which do not issue CKRBs.

1. The initiator creates an ordered set of proposals. The initiator is not key recovery aware so none of the proposals contain the KRM as part of the proposed suite. These proposals are sent to the responder.

2. The responder picks one of the proposals and informs the initiator which proposal was accepted. If none of the proposals are accepted, the responder sends the initiator an error message indicating the reason for the rejection.

The responder sets the commit bit within the ISAKMP header sent to the initiator. This prevents use of the security association until after the responder has transmitted the CKRB. The responder is responsible for ensuring the lifetime of the security association conforms to local policy.

3. The initiator completes the ISAKMP exchange and waits for the notify payload from the responder.

4. The responder completes the ISAKMP exchange and sends the notify payload containing the CKRBs. One CKRB contains the initiator to responder key and the other CKRB contains the responder to initiator key. The notify message value indicates that the security association may now be used. The responder sets the encryption bit/flag to 0, indicating that the payload is not encrypted, and sends this notify payload to the initiator. The message will be protected by the ISAKMP authentication mechanism but it will not be encrypted. The authentication prevents undetected tampering with the contents of the CKRBs yet allows the CKRBs to be intercepted. This notify message SHOULD NOT contain payloads which require confidentiality protection.

> NOTE: This could lead to situations in which key recovery is supported without the explicit consent of the initiator. Implementations which MUST NOT support key recovery MUST terminate the security association when a CKRB is received.

5. Both initiator and responder may use the security association when the initiator receives and processes the notify message.

3.2.3 Initiator and responder do key recovery

In this example assume both the initiator and responder do key recovery.

1. The initiator creates two ordered sets of proposals. The initiator must do key recovery so all of the proposals which apply to the initiator contain the KRM as part of the proposed suite. The proposals which apply to the responder allow the responder the option of doing key recovery or not. These proposals are sent to the responder.

2. The responder picks one of the initiator proposals and one of the responder proposals and informs the initiator which proposals were accepted. If none of the initiator proposals or none of the responder proposals are accepted, the responder sends the initiator an error message indicating the reason for the rejection.

3. The initiator completes the ISAKMP exchange and sets the commit bit within the ISAKMP header. This informs the responder that it must not use the newly created security association until the initiator sends an informational exchange carrying the notify payload indicating the

security association may be used.

4. The responder completes the ISAKMP exchange and also sets the commit bit within the ISAKMP header sent to the initiator. This prevents use of the security association until after the responder has transmitted the CKRB.

5. The initiator prepares the notify payload containing the CKRBs. One CKRB contains the initiator to responder key and the other CKRB contains the responder to initiator key. The initiator sends both CKRBs even if the responder is also performing key recovery. The notify message value indicates that the initiator is ready to use the security association.

The initiator sets the encryption bit/flag to 0, indicating that the payload is not encrypted, and sends this notify payload to the responder. The message will be protected by the ISAKMP authentication mechanism but it will not be encrypted.

6. The responder sends the notify payload containing the CKRBs. One CKRB contains the initiator to responder key and the other CKRB contains the responder to initiator key. The responder sets the encryption bit/flag to 0, indicating that the payload is not encrypted, and sends this notify payload to the initiator. The message will be protected by the ISAKMP authentication mechanism but it will not be encrypted.

The notify message value indicates that the security association is cleared for use by the responder. Both initiator and responder are able to use the security association when the initiator receives and processes the notify message.

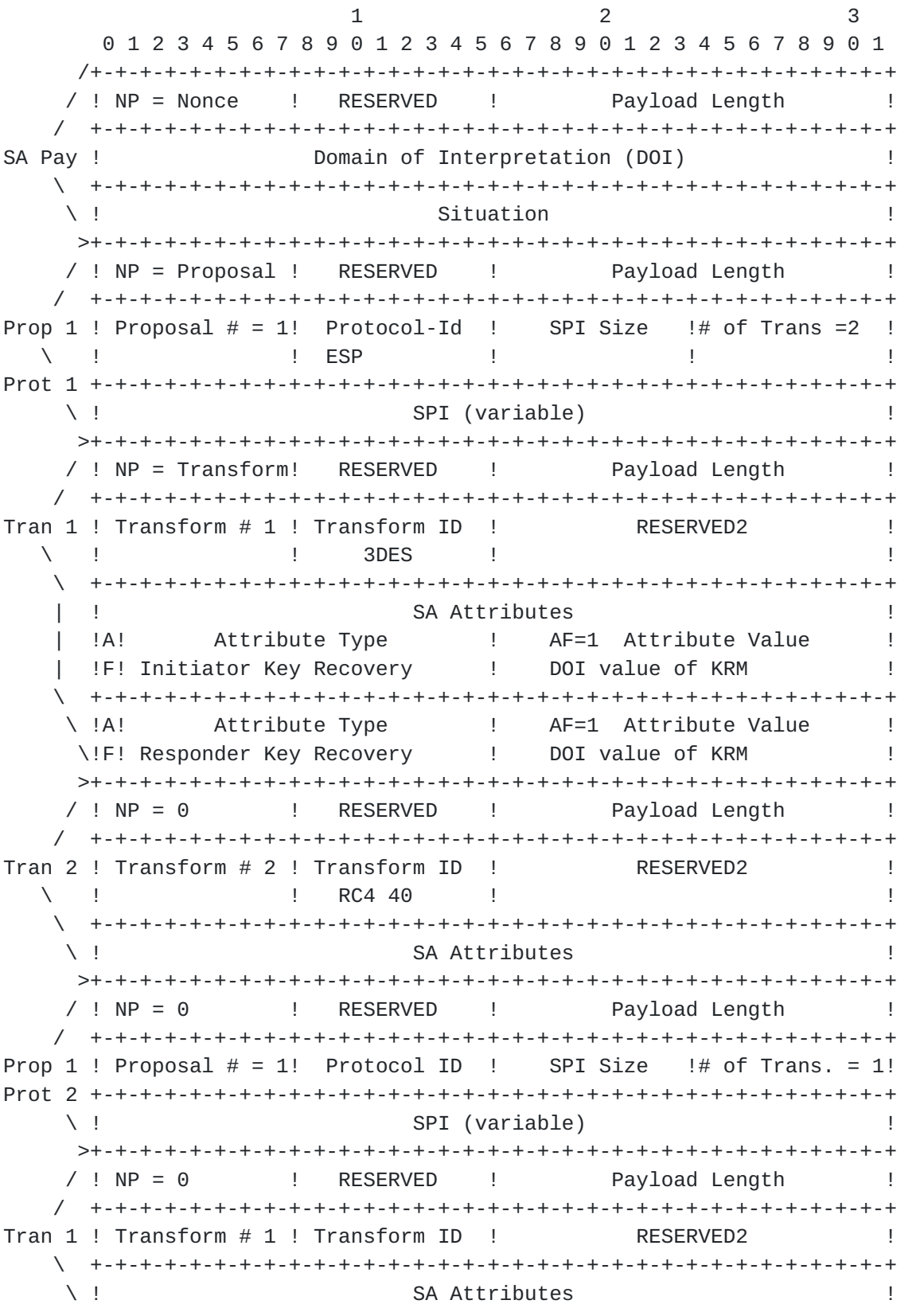
3.2.4 - Security Association Attributes

The key recovery mechanism to be used by each party is negotiated using the Security Association payload, Proposal payload, Transform payload, Security Association attribute field. The example in Figure 1 below shows a proposal for a combined protection suite with two different protocols. The first protocol is presented with two transforms supported by the proposer. The second protocol is presented with a single transform. An example for this proposal might be: Protocol 1 is ESP with Transform 1 as 3DES using key recovery as defined in the SA Attributes and Transform 2 as **40 bit RC4 with no key recovery AND Protocol 2 is AH with Transform 1 as** SHA.

Figure 1 shows the example values for the transform ID and key recovery related fields. The attribute flag and attribute type consume 16 bits. The DOI value for the KRM uses basic encoding so it fits in 16 bits. In this example, there is no key recovery attribute associated with the 40 bit RC4 transform.

The responder MUST select from the two transforms proposed for ESP. The

resulting protection suite will be either (1) 3DES (with key recovery) AND SHA OR (2) 40 bit RC4 (no key recovery) AND SHA, depending on which ESP transform was selected by the responder. Note this example is shown using the Base Exchange.



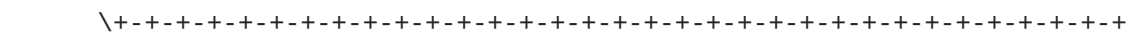


Figure 1. Example payload containing key recovery attributes.

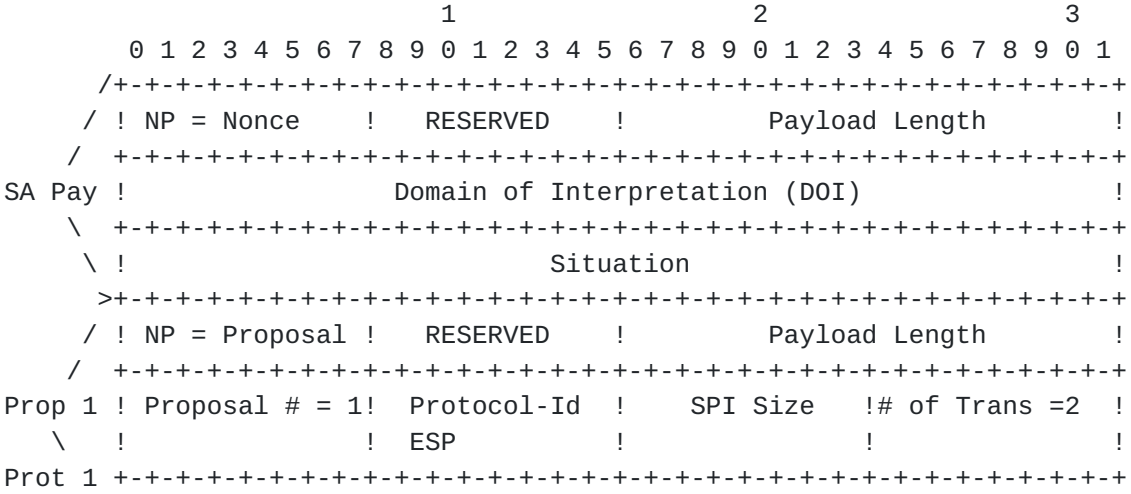
The protocol allows key recovery attributes to be associated with AH (proposal 1, protocol 2 in the example above). This could be used to allow an intermediate device such as a firewall to authenticate packets without decrypting them. If an organization uses this feature, the CKRB intended for the firewall SHOULD be protected using a mechanism which prevents unwanted access by entities outside the organization.

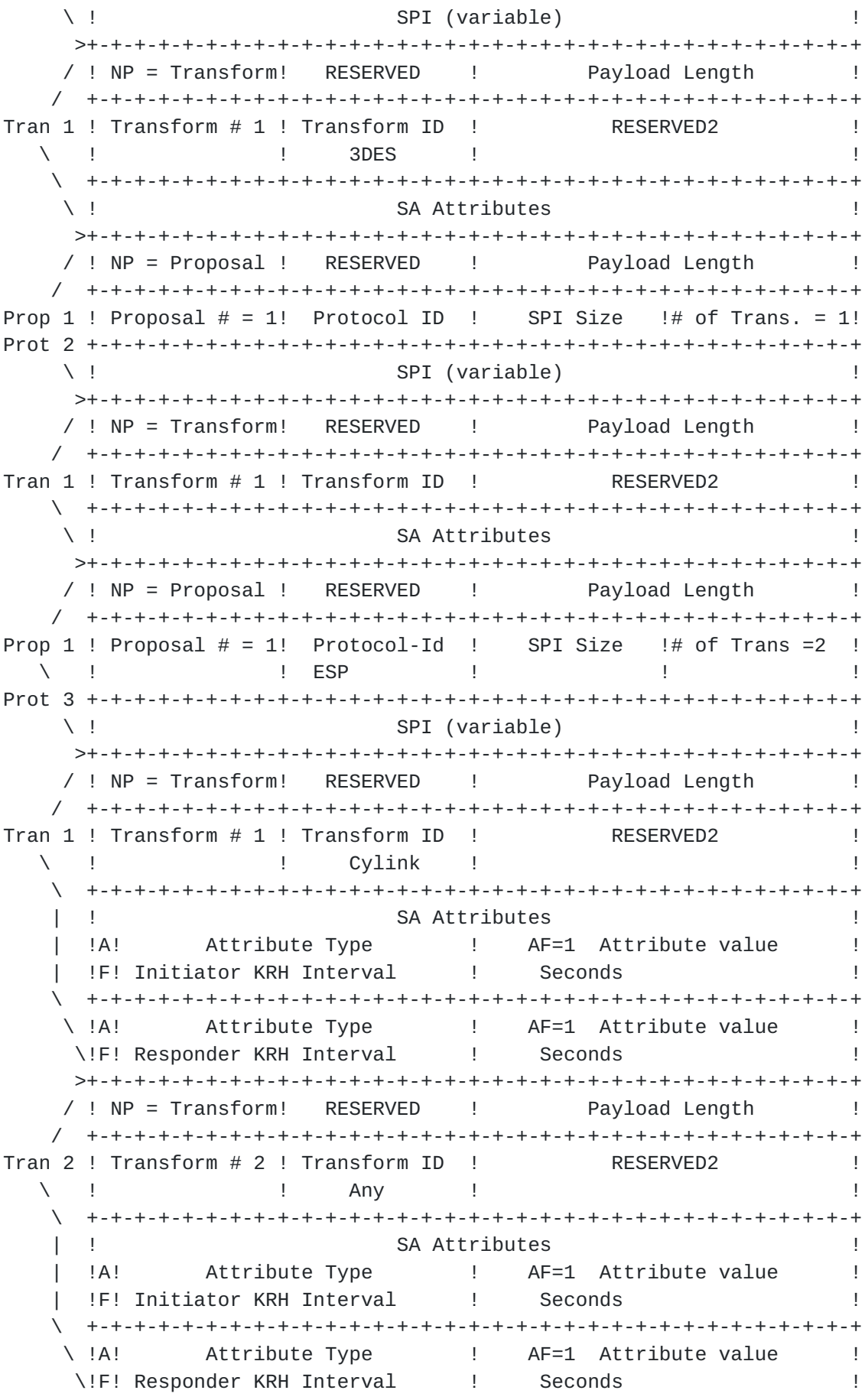
3.2.5 - Security Protocol.

The use of the Key Recovery Header (KRH) protocol is negotiated in the same manner as other protocols (e.g., AH and ESP). Figure 2 below shows a proposal for a combined protection suite with 3 different protocols. The third protocol, KRH, uses a transform ID which reflects the key recovery mechanism as defined in the DOI. The KRH attributes (e.g., the interval between KRH transmissions) are contained within the SA attributes for the KRH protocol. It is not necessary (or desirable) to send the KRH on each IPSEC packet. The intervals at which the initiator and responder send KRH headers is established independently. A value of 0 indicates the associated entity will never send the KRH. Thus, an initiator could send the KRH every hour while the responder never sends the KRH.

An example for this proposal might be: Protocol 1 is ESP with Transform 1 as 3DES, AND Protocol 2 is AH with Transform 1 as SHA AND Protocol 3 is KRH with Transform 1 as Cylink and Transform 2 as Any.

In this example, the responder MUST accept KRH and select from the two transforms proposed for KRH. The resulting protection suite will be either 3DES (with key recovery) AND AH SHA AND KRH with (1) the Cylink mechanism OR (2) Any CKRB mechanism authorized by the policy, depending on which KRH transform was selected by the responder.




SPI (variable)
NP = Transform
RESERVED
Payload Length
Tran 1
Transform # 1
Transform ID
RESERVED2
3DES
SA Attributes
NP = Proposal
Proposal # = 1
Protocol ID
SPI Size
# of Trans. = 1
Prot 2
SPI (variable)
NP = Transform
RESERVED
Payload Length
Tran 1
Transform # 1
Transform ID
RESERVED2
SA Attributes
NP = Proposal
Proposal # = 1
Protocol-Id
SPI Size
# of Trans =2
Prot 3
ESP
SPI (variable)
NP = Transform
RESERVED
Payload Length
Tran 1
Transform # 1
Transform ID
RESERVED2
Cylink
SA Attributes
A
F
Attribute Type
AF=1
Attribute value
Initiator KRH Interval
Seconds
Responder KRH Interval
NP = Transform
RESERVED
Payload Length
Tran 2
Transform # 2
Transform ID
RESERVED2
Any
SA Attributes
Attribute Type
AF=1
Attribute value
Initiator KRH Interval
Seconds
Responder KRH Interval

```
>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2. Example payload containing a key recovery header proposal.

3.2.6 Transmission of the CKRBs

The CKRBs are transmitted in the notify payload. Each CKRB contains 1 key so 2 CKRBs are transmitted. The first contains the initiator to responder key and the second contains the responder to initiator key.

The key recovery mechanism uses the Commit Bit to prevent encrypted IPSEC traffic until the CKRB pair has been transmitted. The Commit Bit is set by either party intending to send a CKRB pair via the notify message within an Informational Exchange. If the Commit Bit is set(1), the entity which did not set MUST wait for an Informational Exchange containing a Notify payload (with the CONNECTED Notify Message) from the entity which set the Commit Bit. This indicates that the SA establishment was successful and the receiving entity can now proceed with encrypted traffic communication.

The CKRBs MUST be sent within the Informational Exchange and not as part of a payload which is encrypted. The information exchange is normally encrypted using the ISAKMP SA. The Authentication Only Bit is used to send the informational exchange using authentication but not encryption. This protects the CKRBs from unauthorized modification while allowing the CKRBs to be observed.

Figure 3 shows the format of the Notification Payload containing CKRBs.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
! Next Payload  !   RESERVED    !         Payload Length        !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!              Domain of Interpretation  (DOI)                 !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!  Protocol-ID  !   SPI Size    !      Notify Message Type      !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                                                               !
~               Security Parameter Index (SPI)                  ~
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                      Notification Data                        !
!      Connected                !                               !
!  Type = CKRB                  !   length of CKRB              !
!                              CKRB                             ~
!  Type = CKRB                  !   length of CKRB              !
!                              CKRB                             ~
!                                                               !
```

Figure 15: Notification Payload Format with CKRBs

3.3 Discussion

When one of the communicating ISAKMP entities does not accept any proposals containing the KRM, the entity performing key recovery is responsible for ensuring that the CKRBs are transmitted at intervals required by the situation.

Manually keyed IPSEC security associations MUST use the Key Recovery Header to pass the CKRBs.

Some situations may require the CKRB to be retransmitted periodically. This MAY be done via the KRH or via the ISAKMP notify message. A second ISAKMP phase 2 exchange MUST be performed when a notify message is used to retransmit the CKRB.

ISAKMP is defined to be key recovery tolerant. If an ISAKMP implementation receives a well formed notify containing an unknown CKRB, then the receiver gracefully discards the CKRB and continues the security association. This allows key recovery enabled devices to interoperate with legacy devices which are key recovery unaware.

4. ACKNOWLEDGMENTS

This document was produced based on the combined efforts of the protocol subcommittee of the Key Recovery Alliance. Comments on this document should be sent to key-recovery@raleigh.ibm.com.

5. REFERENCES

[Atk95a] Atkinson, R., "IP Authentication Header", RFC 1826, NRL, August 1995.

[Atk95b] Atkinson, R., "IP Encapsulating Security Payload", RFC 1827, NRL, August 1995.

[CW98] Charles Williams, Tom Markham, Key Recovery Header for IPSEC, DRAFT Key Recovery Alliance Recommendation 2, April 1998

[DoD85] US National Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, US Department of Defense, Ft. Meade, MD., December 1985.

[DM97] Internet Security Association and Key Management Protocol (ISAKMP), Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, INTERNET-DRAFT draft-ietf-ipsec-isakmp-08.txt, .ps, July 26, 1997

[DP98] The Internet IP Security Domain of Interpretation for ISAKMP [DP98], Derrell Piper, Network Alchemy, May 12, 1998

[RA95] Security Architecture for the Internet Protocol, **R. Atkinson, Naval Research Laboratory, Request for Comments: 1825,** Category: Standards Track, August 1995

[SG98] A Common Key Recovery Block Format: promoting Interoperability between dissimilar key recovery schemes, Sarbari Gupta, Key Recovery Alliance Recommendation 1, April 1998

6. SECURITY CONSIDERATIONS

This entire document discusses a means to disclose cryptographic keys in a controlled manner. The session keying material is contained in a common key recovery block [SG98] which itself is cryptographically protected.

Implementors must apply good coding practices to prevent the introduction of vulnerabilities into the common key recovery block processing.

A second security concern is the potential for unauthorized access to the session key after the common key recovery block has been decrypted. This protection is provided by the key recovery agent which is outside the scope of this protocol.

The security issues associated with key recovery may be explored using this experimental protocol in the context of a larger key recovery system.

7. AUTHOR INFORMATION

Tom Markham
Secure Computing Corp
2675 Long Lake Road
Roseville, MN 55113 USA

Phone: 651.628.2754, Fax: 651.628.2701
EMail: tom_markham@securecomputing.com

8. APPENDIX A: Proposed DOI Values

This appendix is temporary. It will be removed and placed in a separate DOI document if/when the key recovery documents progress through the standards process.

The addition of key recovery to ISAKMP requires the extension of the existing Internet IP Security Domain of Interpretation for ISAKMP [DP98]. The following types of extensions are required.

- Protocol ID
- SA Attributes
- Transforms

An identifiers for the Type = CKRB used within the Notify must also be defined.

A1. Protocol ID - IPSEC Security Protocol Identifier

The following table lists the values for the Security Protocol Identifiers referenced in an ISAKMP Proposal Payload for the IPSEC DOI.

Protocol ID	Value
RESERVED	0
PROTO_ISAKMP	1
PROTO_IPSEC_AH	2
PROTO_IPSEC_ESP	3
PROTO_IPCOMP	4
PROTO_KRH	5

PROTO_IPSEC_KRH

The PROTO_IPSEC_KRH type specifies IP Key Recovery Header containing a pair of CKRBs.

A2. SA Attributes

The SA Attributes will be extended to include the following.

Attribute Types

class	value	type
SA Initiator Key Recovery	TBD	B
SA Responder Key Recovery	TBD	B
SA Initiator KRH Interval	TBD	B
SA Responder KRH Interval	TBD	B

Initiator Key Recovery indicates that the initiator will perform key recovery. The value associated with this attribute specifies the CKRB Transform Identifier which applies to the CKRB to be transmitted by the initiator.

Responder Key Recovery indicates that the responder will perform key recovery. The value associated with this attribute specifies the CKRB Transform Identifier which applies to the CKRB to be transmitted by the responder.

Initiator KRH Interval indicates the maximum interval between KRHs sent by the initiator.

Responder KRH Interval indicates the maximum interval between KRHs sent by the responder.

A3. Transforms - IPSEC CKRB Transform Identifier

The CKRB specification specifies a common wrapper for multiple key recovery technologies each using unique transforms.

Transform ID	Value
None	0
Any	1
Bull-P	2
Bull-G	3
Cylink	4
IBM	5
NETA	6
Novell	7

None: No key recovery is to be performed.

Any: Any key recovery mechanism recognized by the applicable policy is acceptable.

Bull-P: The Bull transform using the ISAKMP protocol integrity mechanism.

Bull-G: The Bull transform using the split key generation mechanism.

Cylink: The Cylink CyKey mechanism together with the ISAKMP protocol integrity mechanism.

IBM: The IBM mechanism together with the ISAKMP protocol integrity mechanism.

NETA: The Network Associates (formerly TIS) mechanism together with the ISAKMP protocol

integrity mechanism.

Novell: The Novell mechanism together with the ISAKMP protocol integrity mechanism.

9. FULL COPYRIGHT STATEMENT