Network Working Group
Internet Draft
draft-ietf-ospf-doi-00.txt

R. Atkinson, Editor
@Home Network

15 October 1997

OSPFv2 Domain Of Interpretation (DOI) for ISAKMP

STATUS OF THIS MEMO

1. Abstract

The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges and processing guidelines that occur within a given Domain of Interpretation (DOI). This document details

the OSPFv2 DOI, which is defined to cover the use of ISAKMP to negotiate Security Associations for the OSPFv2 routing protocol.

2. Introduction

Within ISAKMP, a Domain of Interpretation is used to group related protocols using ISAKMP to negotiate security associations. Security protocols sharing a DOI choose security protocol and cryptographic transforms from a common namespace and share key exchange protocol identifiers. They also share a common interpretation of DOI-specific payload data content, including the Security Association and Identification payloads.

Overall, ISAKMP places the following requirements on a DOI definition:

- define the naming scheme for DOI-specific protocol identifiers
- define the interpretation for the Situation field
- define the set of applicable security policies
- define the syntax for DOI-specific SA Attributes (phase II)
- define the syntax for DOI-specific payload contents
- define additional mappings or Key Exchange types, if needed

The remainder of this document details the instantiation of these requirements for using the OSPFv2 cryptographic authentication mechanism to provide data origin authentication for OSPFv2 routing packets sent between cooperating routers.

3. Terms and Definitions

In this document, the words that are used to define the significance of each particular requirement are usually capitalised. These words are defined in RFC-xxxx, which is hereby incorporated into this document by reference. [RFC-xxxx]

Within ISAKMP, all DOI's must be registered with the IANA in the ``Assigned Numbers'' RFC [STD-2]. The IANA Assigned Number for the OSPFv2 DOI is <TO BE ASSIGNED BY IANA>. Within the OSPFv2 DOI, all well-known identifiers MUST be registered with the IANA under the OSPFv2 DOI. Unless otherwise noted, all tables within this document refer to IANA Assigned Numbers for the OSPFv2 DOI.

4.0 Assigned Numbers

The following sections list the Assigned Numbers for the OSPFv2 DOI Security Protocol Identifiers, Transform Identifiers, and

Security Association Attribute Types. Note that all multi-octet binary values are stored in network byte order.

4.1 OSPFv2 Situation Definition

Within ISAKMP, the Situation provides information that can be used by the responder to make a policy determination about how to process the incoming Security Association request. For the OSPFv2 DOI, the Situation field is a four (4) octet bitmask with the following values.

Situation	Value
SIT_AUTHENTICATION	0x01

All other values are reserved to IANA.

The SIT_AUTHENTICATION type specifies that the security association will be identified by source identity information present in an associated Identification Payload. See Section 4.8.2 for a complete description of the various Identification types. All OSPFv2 DOI implementations MUST support SIT_AUTHENTICATION by including an Identification Payload in at least one of the phase I Oakley exchanges ([IO], Section 5) and MUST abort any security association setup that does not include an Identification Payload.

4.2 OSPFv2 Security Protocol Identifiers

The ISAKMP proposal syntax was specifically designed to allow for the simultaneous negotiation of multiple security protocol suites within a single negotiation. As a result, a Protocol ID must be indicated. The size of this field is one octet. The values 3-255 are reserved to IANA.

Protocol ID	Value
RESERVED	0
PROTO_ISAKMP	1
PROTO_OSPFv2	2

4.3 PROTO_ISAKMP

The PROTO_ISAKMP type specifies message protection required during Phase I of the ISAKMP protocol. The specific protection mechanism used for the OSPFv2 DOI is described in [IO]. All implementations within the OSPFv2 DOI MUST support PROTO_ISAKMP.

NB: ISAKMP reserves the value one (1) across all DOI definitions.

4.3.1 PROTO_OSPFv2

The PROTO_OSPFv2 type specifies IP packet data origin authentication. The default OSPFv2 transform includes data origin authentication and replay prevention.

4.4 OSPFv2 ISAKMP Transform Values

As part of an ISAKMP Phase I negotiation, the initiator's choice of Key Exchange offerings is made using some host system policy description. The actual selection of Key Exchange mechanism is made using the standard ISAKMP Proposal Payload. The following table lists the defined ISAKMP Phase I Transform Identifiers for the Proposal Payload for the OSPFv2 DOI.

Transform	Value
RESERVED	0
KEY_OAKLEY	1

The size of this field is one octet. The values 4-255 are reserved to IANA.

The KEY_OAKLEY type specifies the hybrid ISAKMP/Oakley Diffie-Hellman key exchange as defined in the [IO] document. All implementations within the OSPFv2 DOI MUST support KEY_OAKLEY. It is anticipated that in future values will be assigned for Kerberos v5, GKMP, and/or other protocols to handle multicast SA creation more effectively.

4.5 OSPFv2 Cryptographic Authentication Transform Values

The OSPFv2 Cryptographic Authentication mechanism is designed to be algorithm-independent, even though only one algorithm transform was been defined as of the time this document was written. The following table lists the defined OSPFv2 Cryptographic Transform Identifiers for the ISAKMP Proposal Payload for the OSPFv2 DOI.

Transform ID	Value
RESERVED	0
OSPFv2_MD5_KPDK	1

The size of this field is one octet. The values 4-255 are reserved to IANA.

The AH_MD5_KPDK type specifies the AH transform (Key/Pad/Data/Key) described in RFC-2178. Implementations are required to support this mode.

4.6 OSPFv2 Security Association Attributes

The following SA attribute definitions are used in phase II of an ISAKMP/Oakley negotiation. Attribute types can be either Basic (B) or Variable-Length (V). Encoding of these attributes is defined in the base ISAKMP specification.

Attribute Classes

class	value	type
Auth Key Life Type	1	B
Auth Key Life Duration	2	B/V
Enc Key Life Type	3	B
Enc Key Life Duration	4	B/V
SA Life Type	5	B
SA Life Duration	6	B/V
Replay Protection	7	B
Group Description	8	B
CA Distinguished Name	9	B
Encapsulation Mode	10	B

Class Values

Auth Key Life Type
Auth Key Duration
Specifies the time-to-live for the authentication key(s) used in the corresponding AH HMAC transform.

SA Life Type
SA Duration
Specifies the time-to-live for the overall security association. When the SA expires, all keys negotiated under the association (AH or ESP) must be renegotiated regardless of the time-to-live remaining for the keys.

RESERVED	0
seconds	1
kilobytes	2

Values 3-61439 are reserved to IANA. Values 61440-65535 are for experimental use. For a given "Life Type," the value of the "Life Duration" attribute defines the actual length of the component lifetime -- either a number of

seconds, or a number of Kbytes that can be protected.

If unspecified, the default value shall be assumed to be 28800 seconds (8 hours) for Auth, Enc, and SA lifetime.

Replay Protection

RESERVED	0
required	1
disallowed	2

Values 3-61439 are reserved to IANA. Values 61440-65535 are for private use among mutually consenting parties.

There is no default value for Replay Protection, as it must be specified to correctly identify the applicable transform.

Group Description

RESERVED	0
default group	1

Values 2-61439 are reserved to IANA. Values 61440-65535 are for private use among mutually consenting parties.

If unspecified, the default value shall be assumed to be the default Oakley group ([IO], Section 5.5.1).

CA Distinguished Name

RESERVED	0
DNS Security	1

Values 2-61439 are reserved to IANA. Values 61440-65535 are for private use among mutually consenting parties.

If unspecified, the default value shall be assumed to be DNS Security (Section 4.8).

4.7.1 Required Attribute Support

To ensure basic interoperability, all implementations MUST support all of the following attributes:

Auth Key Life Type
Auth Key Duration
SA Life Type
SA Duration
Replay Protection

4.7.2 Attribute List Parsing Requirement

To allow for flexible semantics, the OSPFv2 DOI requires that a conforming ISAKMP implementation MUST correctly parse an attribute list that contains multiple instances of the same attribute class, so long as the different attribute entries do not conflict with one another.

If conflicting attributes are detected, an ATTRIBUTES-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

4.8 OSPFv2 Payload Content

The following sections describe those ISAKMP payloads whose data representations are dependent on the applicable DOI.

4.8.1 Security Association Payload

The following diagram illustrates the content of the Security Association Payload for the OSPFv2 DOI. See above for a description of the Situation bitmap.

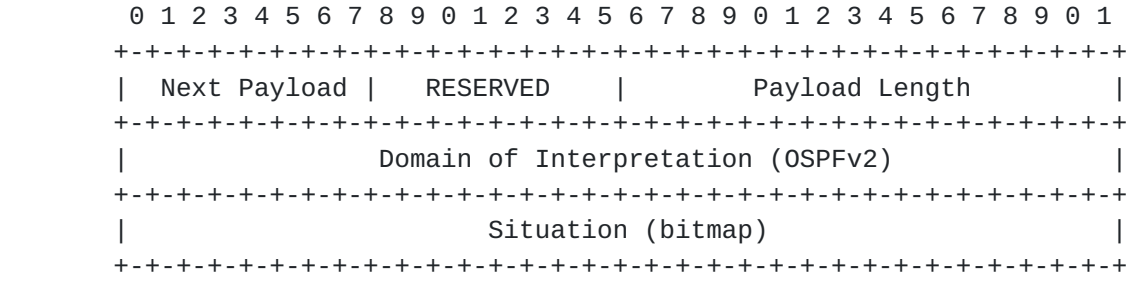

Figure 1: Security Association Payload Format

The Security Association Payload is defined as follows:

- Next Payload (2 octets) - Identifier for the payload type of the next payload in the message. If the current payload is the last in the message, this field will be zero (0).

- RESERVED (1 octet) - Unused, must be zero (0).

- Payload Length (2 octets) - Length, in octets, of the current payload, including the generic header.

- Domain of Interpretation (4 octets) - Specifies the OSPFv2 DOI, which has been assigned the value <To Be Assigned by IANA>.

- Situation (4 octets) - Bitmask used to interpret the remainder of the Security Association Payload. See Section 4.2 for a complete list of values.

4.8.2 Identification Payload Content

The Identification Payload is used to identify the initiator of the Security Association. The identity of the initiator SHOULD be used by the responder to determine the correct host system security policy requirement for the association. Typically, OSPF sessions use an identity that is either an IP Address or a Fully Qualified Domain Name (FQDN).

The Identification Payload provides information that can be used by the responder to make this decision.

The following diagram illustrates the content of the Identification Payload.

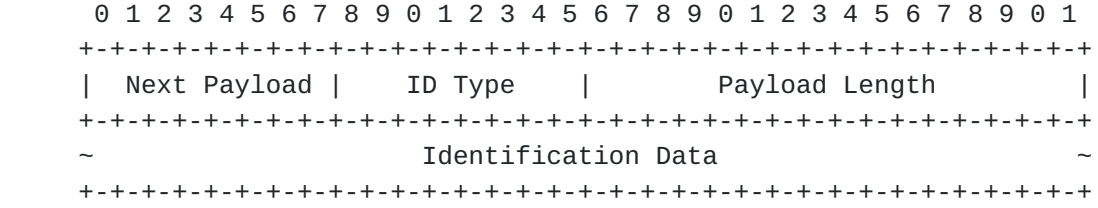

Figure 2: Identification Payload Format

The Identification Payload field is defined as follows:

- Next Payload (2 octets) - Identifier for the payload type of the next payload in the message. If the current payload is the last in the message, this field will be zero (0).

- Identification Type (1 octet) - Value describing the identity information found in the Identification Data field.

- Payload Length (2 octets) - Length, in octets, of the identification data, including the generic header.

4.8.2.1 Identification Type Values

The following table lists the assigned values for the Identification Type field found in the Identification Payload.

ID Type	Value

RESERVED	0
ID_IPV4_ADDR	1
ID_IPV6_ADDR	2
ID_FQDN	3
ID_USER_FQDN	4

The size of this field is one octet. The values 5-255 are reserved to IANA.

The ID_IPV4_ADDR type specifies a single four (4) octet IPv4 address.

The ID_IPV4_ADDR type specifies a single sixteen (16) octet IPv6 address.

The ID_FQDN type specifies a fully-qualified domain name string. An example of a ID_FQDN is, "foo.bar.com".

The ID_USER_FQDN type specifies a fully-qualified username string, An example of a ID_USER_FQDN is, "john-doe@foo.bar.com".

4.9 OSPFv2 Security Parameter Index (SPI) Encoding

ISAKMP defines the SPI field as eight octets in length, however the OSPFv2 Cryptographic Authentication only uses a one octet Key Identifier. All implementations MUST use the following mapping for the ISAKMP SPI field in the OSPFv2 DOI.

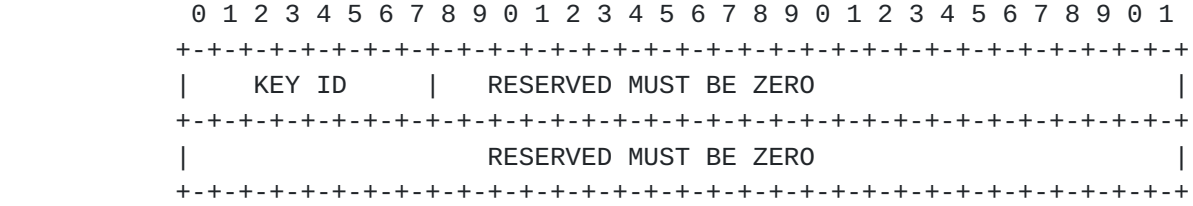

Figure 3: ISAKMP SPI Encoding

The ISAKMP SPI field is defined as follows:

- KEY ID - Key Identifier (1 octet) - contains the KEY ID value which identifies the OSPFv2 Authentication Key.

- RESERVED (7 octets) - Reserved for future use, must be sent as zero (0) and ignored upon receipt.

4.8 OSPFv2 Certificate Authorities

The ISAKMP Certificate Request Payload allows either side of an ISAKMP negotiation to request its peer to provide a certificate chain needed to authenticate itself. The Certificate Request Payload includes a list of acceptable Certificate Types and Certificate Authorities. Appropriate certificate chains are then returned in a Certificate Payload response.

The OSPFv2 DOI defines the following Certificate Authorities for the processing of Certificate Request Payloads. See Section 4.5 for details on the specific data attribute type values for these CAs.

Certificate Authority
DNS Security

4.8.1 DNS Security

This CA type represents the combination of KEY and SIG records, as defined in RFC-2065, that can be used for authentication. The particular encoding required to formulate the Certificate Payload (response) is TBD.

4.9 OSPFv2 Key Exchange Requirements

The OSPFv2 DOI introduces no additional Key Exchange types.

5. Security Considerations

This entire note pertains to a hybrid protocol, combining Oakley ([OAKLEY]) with ISAKMP ([ISAKMP]), to negotiate and derive keying material for security associations in a secure and authenticated manner. Specific discussion of the various security protocols and transforms identified in this document can be found in the associated base documents.

This document describes the additional data needed to apply the ISAKMP protocol for use in managing OSPFv2 Authentication Keys and related data. Implementers should consult the OSPFv2 specification for more information on OSPFv2 Cryptographic Authentication.

ACKNOWLEDGEMENTS:

This document is directly derived from the "IP Security DOI for ISAKMP" by Derrell Piper. That document is in turn derived, in part, from previous works by Douglas Maughan, Mark Schertler, Mark

Schneider, Jeff Turner, Dan Harkins, and Dave Carrel.

REFERENCES:

[RFC-2065] D. Eastlake 3rd & C. Kaufman, "Domain Name System Security Extensions (DNSSEC)", RFC-2065, January 1997.

[RFC-2178] J. Moy, "OSPF Version 2", RFC-2178, July 1997.

[IO] D. Carrel & D. Harkins, "The Resolution of ISAKMP with Oakley," draft-ietf-ipsec-isakmp-oakley-03.txt.

[ISAKMP] D. Maughan, M. Schertler, M. Schneider, & J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," draft-ietf-ipsec-isakmp-07.{ps,txt}.

[OAKLEY] H. K. Orman, "The OAKLEY Key Determination Protocol," draft-ietf-ipsec-oakley-01.txt.

[PFKEY] D.L. McDonald, C.W. Metz, B.G. Phan, "PF_KEY Key Management API, Version 2", draft-mcdonald-pf-key-v2-01.txt, work in progress.

Editor's Address:

Randall Atkinson <rja@home.net>
@Home Network
425 Broadway Street
Redwood City, CA,
USA 94063

+1 (650) 569-5449