Internet Engineering Task Force
IP Security Working Group
Internet Draft
Expires in six months

R. Pereira, TimeStep Corp.
P. Bhattacharya, IBM Corp.

February 19, 1998

IPSec Policy Data Model
<draft-ietf-ipsec-policy-model-00.txt>

Status of this Memo

This document is a submission to the IETF Internet Protocol Security (IPSECond) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@tis.com) or to the editor.

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 draft documents are 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 learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Abstract

This document presents a data model for IPSec policy based on ISAKMP.

Table of Contents

1. Introduction

The original intent of this document was to present a flexible, extensible and interoperable IPSec policy model that would be used by all IPSec compliant devices. This version of this document represents a scaled down effort of that original goal. This is due to many reasons, most notably the size of such an undertaking and the number of equally correct policy paradigms that IPSec can be molded into.

The authors hope that this base IPSec data model will provide implementers sufficient information on the base IPSec negotiation mechanism that they can create an Enterprise policy architecture with the correct IPSec model.

It is assumed that the reader is familiar with the terms and concepts described in the "Security Architecture for the Internet Protocol" [Atkinso95] and "IP Security Document Roadmap" [Thayer97] documents as well as all other referenced IPSec documents.

1.1. Specification of Requirements

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", and "MAY" that appear in this document are to be interpreted as described in [Bradner97].

2. Data Model

To understand IPSec, the reader must realize that there really exists two different policy areas; one for the ISAKMP security association and one for the actual IPSec (ESP/AH) security association. While the ISAKMP SA relies on the two negotiating peers, the IPSec SA will rely on the hosts actually being protected, which in many cases are the same as the negotiating peers (client to client).

The current version of this document does not try to represent objects on the network (gateways, firewalls, routers, workstations, ...) and their relationship to these data models. This work might be in future versions of this document, but it is foreseeable that most organizations will require different network security policy architectures.

The following data models are represented in ASN.1 notation merely for clarity and is not intended to imply any preference for ASN.1 based policy mechanisms however, a LDAP schema will be added to future versions of this document.

2.1. ISAKMP Model

The ISAKMP SA protects the two negotiating peers while they are communicating with ISAKMP.

The specification below allows for such examples as;
 '(DES MD5) or (DES SHA)'

```
IsakmpDescriptor ::=
  SEQUENCE {
    exchange ENUMERATED {
      MainMode,
      AggressiveMode } OPTIONAL,
    proposal SEQUENCE OF IsakmpProposal
  }
```

o The main ISAKMP object mainly includes proposals, but also includes which exchange to utilize. AggressiveMode does not hide the identity of the negotiating peers, while MainMode does. Please refer to [Harkins98] for a more complete reference to both of these two exchange modes.

The exchange mode MAY not be included in this object since it MAY instead depend on the peers.

o The proposals are all taken as logical ORs when presented together.

```
IsakmpProposal ::=
  SEQUENCE {
    cipher IsakmpCipherAlg,
    keylength INTEGER OPTIONAL,
    hash HashAlg,
    group INTEGER OPTIONAL,
    expiry Expiry
  }
```

o The keylength attribute is only valid when the cipher algorithm is CAST, RC5 or Blowfish.

o The default for the group attribute is 1.

```
HashAlg ::=
  ENUMERATED {
    md5,
    sha1,
    tiger
  }
```

o The hash algorithm values are specified in [Harkins98].

```
IsakmpCipherAlg ::=
  ENUMERATED {
    des,
    idea,
    blowfish,
    rc5,
    des3,
    cast
  }
```

o The cipher algorithm values are specified in [Harkins98].

```
Expiry ::=
  SEQUENCE {
    seconds INTEGER OPTIONAL,
    kilobytes INTEGER OPTIONAL
  }
```

2.2. IPSec Model

The IPSec SA(s) protects the actual IP traffic between two systems. IPSec allows for security gateways (firewalls, routers or edge devices, ...) to proxy on behalf of systems behind them so that the

negotiating system may not be the end-system. Thus rules based on IpsecDescriptor SHOULD be referenced by the actual end-systems being protected. Additionally, rules MAY also be referenced by either edge devices proxing on their behalf.

The specification below allows for such examples as;

```
 '(ESP (DES HMAC MD5) OR (DES HMAC SHA)) OR
  ((ESP DES) AND
    (AH (HMAC MD5) OR (HMAC SHA)))'
```

```
IpsecDescriptor ::=
  SEQUENCE {
    pfs BOOLEAN,
    proposal SEQUENCE OF IpsecProposal
  }
```

o The Perfect Forward Secrecy (pfs) attribute is situated in the IPSec object and not in the ISAKMP object since this attribute is used in QuickMode (phase 2) for the initial IPSec SA and for subsequent rekeyed SAs.

o The proposals are all taken as logical ORs when presented together.

```
IpsecProposal ::=
  SEQUENCE OF {
    protectionSuite IpsecSuite
  }
```

o The protectionSuite attributes are all taken as logical ANDs when presented together thus allowing for multiple protocols to be negotiated together.

```
IpsecSuite ::=
  CHOICE {
    espProtocol SEQUENCE OF EspProposal,
    ahProtocol SEQUENCE OF AhProposal,
    compProtocol SEQUENCE OF IpcompProposal
  }
```

o The IpsecSuite represents one of three possible protocol types. ESP allows for confidentiality and integrity/authentication, AH only allows for integrity/authentication and IPComp allows for compression.

```
EspProposal ::=
  SEQUENCE {
    cipher IpsecCipherAlg,
    keylength INTEGER OPTIONAL,
    keyrounds INTEGER OPTIONAL,
    integrity IntegrityAlg OPTIONAL,
    group INTEGER OPTIONAL,
    expiry Expiry OPTIONAL
  }
```

- o The keylength attribute MUST only be present when the cipher algorithm is either CAST, RC5, or blowfish.

- o Key rounds is currently not defined for any cipher algorithm, but if a cipher algorithm is specified in the future that utilizes key rounds, then this attribute MAY be present.

- o The group attribute defaults to 1 and SHOULD only be present if the PFS attribute is TRUE.

```
AhProposal ::=
  SEQUENCE {
    integrity IntegrityAlg,
    group INTEGER OPTIONAL,
    expiry Expiry OPTIONAL
  }
```

- o The group attribute defaults to 1 and SHOULD only be present if the PFS attribute is TRUE.

```
IpcompProposal ::=
  SEQUENCE {
    compression CompressionAlg,
    expiry Expiry OPTIONAL
  }

CompressionAlg ::=
  ENUMERATED {
    oui,
    deflate,
    lzs,
    v42bis
  }
```

- o The compression algorithm values are specified in [Piper98].

```
   IntegrityAlg ::=
     ENUMERATED {
       hmacMd5,
       hmacSha1,
       hmacDes,
       keyedMd5,
       hmacRipem
   }
```

o The integrity algorithm values are specified in [Piper98].

```
   IpsecCipherAlg ::=
     ENUMERATED {
       none,
       rfc1829-iv64,
       des,
       des3,
       rc5,
       idea,
       cast,
       blowfish,
       3idea,
       rfc1829-iv32,
       rc4
     }
```

o The cipher algorithm values are specified in [Piper98].

3. Security Considerations

This draft merely presents a data model of the IPSec documents. All security considerations within those actual specification MUST be considered previously to implementing a policy architecture.

4. References

[Atkinso95] R. Atkinson, "Security Architecture for the Internet Protocol", draft-ietf-ipsec-arch-sec-01

[Bradner97] S. Bradner, "Key words for use in RFCs to indicate Requirement Levels", RFC2119

[ISAKMP] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management

Protocol", draft-ietf-ipsec-isakmp-08

[Harkins98] D. Harkins, "The Resolution of ISAKMP and Oakley", draft-ietf-ipsec-isakmp-oakley-06

[Droms97] R. Droms, "Dynamic Host Configuration Protocol", RFC2131

[Radius97] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC2138

[Ldap97] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)", RFC2251

[Keromy98] A. Keromytis, N. Provos, "The Use of HMAC-RIPEMD-160-96 within ESP and AH", draft-ietf-ipsec-auth-hmac-ripemd-160-96-01.txt

[Piper98] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", draft-ietf-ipsec-ipsec-doi-07.txt

5. Editors' Addresses

Roy Pereira
rpereira@timestep.com
TimeStep Corporation
+1 (613) 599-3610 x 4808

Partha Bhattacharya
IBM Corporation
partha@watson.ibm.com
+1 (919) 863-7981

The IPSec working group can be contacted via the IPSec working group's mailing list (ipsec@tis.com) or through its chairs:

Robert Moskowitz
rgm@icsa.net
International Computer Security Association

Theodore Y. Ts'o
tytso@MIT.EDU
Massachusetts Institute of Technology