Internet Draft
draft-ietf-ipsec-isakmp-di-mon-mib-05.txt
April 15, 2003
Expires in six months

Editor: Paul Hoffman
VPN Consortium

ISAKMP DOI-Independent Monitoring MIB

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Table of Contents

[[Needs to be generated in the RFC publication step]]

Introduction

This document defines a DOI (domain of interpretation) independent monitoring MIB for ISAKMP.

The purpose of this MIB is to be used as the basis for protocol specific MIBs that use ISAKMP as the basis for key exchanges or security association negotiation.

As such, it has no DOI-dependent objects.

1. The SNMP Management Framework

The SNMP Management Framework presently consists of five major components:

- An overall architecture, described in RFC 2571 [RFC2571].
- Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of

Management Information (SMI) is called SMIv1 and described in STD 16, RFC 1155 [RFC1155], STD 16, RFC 1212 [RFC1212] and RFC 1215 [RFC1215]. The second version, called SMIv2, is described in STD 58, RFC 2578 [RFC2578], RFC 2579 [RFC2579] and RFC 2580 [RFC2580].

- Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, RFC 1157 [RFC1157]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [RFC1901] and RFC 1906 [RFC1906]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [RFC1906], RFC 2572 [RFC2572] and RFC 2574 [RFC2574].

- Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15, RFC 1157 [RFC1157]. A second set of protocol operations and associated PDU formats is described in RFC 1905 [RFC1905].

- A set of fundamental applications described in RFC 2573 [RFC2573] and the view-based access control mechanism described in RFC 2575 [RFC2575].

A more detailed introduction to the current SNMP Management Framework can be found in RFC 2570 [RFC2570].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

This memo specifies a MIB module that is compliant to the SMIv2. A MIB conforming to the SMIv1 can be produced through the appropriate translations. The resulting translated MIB must be semantically equivalent, except where objects or events are omitted because no translation is possible (use of Counter64). Some machine readable information in SMIv2 will be converted into textual descriptions in SMIv1 during the translation process. However, this loss of machine readable information is not considered to change the semantics of the MIB.

1.1 Object Definitions

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the subset of Abstract Syntax Notation One (ASN.1) defined in the SMI. In particular, each object type is named by an OBJECT IDENTIFIER, an administratively assigned name. The object type together with an object instance serves to uniquely identify a

specific instantiation of the object. For human convenience, we often use a textual string, termed the descriptor, to refer to the object type.

2. ISAKMP DOI-independent MIB Objects Architecture

The ISAKMP DOI-independent MIB consists of a table of security associations (SAs), providing the DOI-independent portion of all SAs that use ISAKMP as the basis of their negotiations.

There are also provided entity statistics related to generic ISAKMP SA usage. The traffic statistics collected include re-transmissions and both encrypted and unencrypted traffic to allow network administrators determine how much of their total traffic is related to ISAKMP, and thus management of security associations in general.

There is a single trap defined. The reason for this is that the DOI-independent portion of ISAKMP makes no assumptions about the use of ISAKMP, aside from the aggregate statistics assumption stated above. The single trap defined is the invalid cookie trap; it is provided since repeated detection of this error can indicate systems that have become badly out of sync or are subject to denial-of-service attacks.

There is no count of notifications sent or received. The reason for this is that the usage of notifications is associated with specific DOIs (even though there are ISAKMP defined notification types), and this is a DOI-independent MIB. Protocols that use the notifications must be designed to allow counting of the notification types from DOI of 0 if they use the ISAKMP notification types in addition to their own.

2.1 Phase 1 Security Associations Table

This table includes the uniqueness identifiers for those SAs, some version information, some communications information and some basic status information. Also included are aggregate statistics based on the assumption that DOI-specific usage of ISAKMP is for the purpose of negotiating SAs.

Additional tables could be generated that are specific to the ISAKMP DOI, however, there is no attempt to define these tables as part of this MIB. These tables are intended to be part of a separate MIB.

3. MIB Definitions

```
 ISAKMP-DOI-IND-MON-MIB DEFINITIONS ::= BEGIN

     IMPORTS
         MODULE-IDENTITY, OBJECT-TYPE, Counter32, Gauge32,
```

```
        Integer32, Counter64, NOTIFICATION-TYPE, OBJECT-IDENTITY
-- delete this and next line before release
        , experimental
                                    FROM SNMPv2-SMI
        TEXTUAL-CONVENTION, TruthValue
                                    FROM SNMPv2-TC
        OBJECT-GROUP, NOTIFICATION-GROUP, MODULE-COMPLIANCE
                                    FROM SNMPv2-CONF
        InetAddressType, InetAddress
                                    FROM INET-ADDRESS-MIB
        IsakmpDOI, IsakmpExchangeType
                                    FROM IPSEC-ISAKMP-IKE-DOI-TC;

    isakmpDoiIndMonModule MODULE-IDENTITY
    LAST-UPDATED "0110031200Z"
    ORGANIZATION "IETF IPsec Working Group"
    CONTACT-INFO
                "   Tim Jenkins
                    Catena Networks
                    307 Legget Drive
                    Kanata, ON
                    Canada
                    K2K 3C8
                    +1 (613) 599-6430
                    tjenkins@catena.com

                    John Shriver
                    Intel Corporation
                    28 Crosby Drive Bedford, MA
                    01730
                    +1 (781) 687-1329
                    John.Shriver@intel.com
                "

    DESCRIPTION
        "The MIB module to describe the DOI-independent part of
        ISAKMP objects; to be used for monitoring purposes."
    REVISION    "9906031200Z"
    DESCRIPTION
        "Initial revision."
    REVISION    "9910211200Z"
    DESCRIPTION
        "Compliances and groups added.
         OID value under experimental tree added.
         Removed SA expiration objects.
         Added invalid cookie count and trap."
    REVISION    "0007101200Z"

    DESCRIPTION
        "Change addresses to use format from INET-ADDRESS-MIB.
         Add explicit trap objects.
```

```
         Other minor changes."
    REVISION    "0102071200Z"
    DESCRIPTION
        "Change MAX-ACCESS clause of index objects to
        not-accessible. This lead to other changes due to
        restrictions on the use of objects with MAX-ACCESS clause
        values of not-accessible."
    REVISION    "0110031200Z"
    DESCRIPTION
        "A number of typo errors corrected. Also:
        - isakmpInvalidCookieCount changed to isakmpInvalidCookies
        - add (SIZE(4|16|20)) to localIpAddress
        - explain why first six members of isakmpSaGroup are
          commented out
        - allow localIpAddressType and remoteIpAddressType to be
          only IPv4 and Ipv6 addresses"

-- replace xxx in next line before release, uncomment before release
    --  ::= { mib-2 xxx }
    -- delete this and next line before release
    ::= { experimental 99 }

isakmpDoiIndMIBObjects OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION
        "This is the base object identifier for all ISAKMP
        branches."
    ::= { isakmpDoiIndMonModule 1 }


--
-- significant branches
--

isakmpSaTable OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for the security
        associations table."
    ::= { isakmpDoiIndMIBObjects 1 }

isakmpGlobals OBJECT-IDENTITY
    STATUS  current


    DESCRIPTION
        "This is the base object identifier for all objects which
        are global values for ISAKMP."
    ::= { isakmpDoiIndMIBObjects 2 }

isakmpNegStats OBJECT-IDENTITY
```

```
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all objects which
        are global counters for ISAKMP negotiation statistics."
    ::= { isakmpDoiIndMIBObjects 3 }

isakmpTrafStats OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all objects which
        are global counters for ISAKMP security association traffic
        statistics."
    ::= { isakmpDoiIndMIBObjects 4 }

isakmpErrors OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all objects which
        are global error counters for ISAKMP."
    ::= { isakmpDoiIndMIBObjects 5 }

isakmpGroups OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all objects which
        describe the groups in this MIB."
    ::= { isakmpDoiIndMIBObjects 6 }

isakmpConformance OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all objects which
        describe the conformance for this MIB."
    ::= { isakmpDoiIndMIBObjects 7 }

isakmpTrapControl OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all trap controls
        for this MIB."
    ::= { isakmpDoiIndMIBObjects 8 }

isakmpTraps OBJECT-IDENTITY
    STATUS  current
    DESCRIPTION
        "This is the base object identifier for all traps for this
        MIB."
    ::= { isakmpDoiIndMIBObjects 9 }

isakmpTrapObjects OBJECT-IDENTITY
    STATUS  current
```

```
    DESCRIPTION
        "This is the base object identifier for all objects used by
        traps for this MIB."
    ::= { isakmpDoiIndMIBObjects 10 }

--
-- textual conventions
--

IsakmpCookie ::= TEXTUAL-CONVENTION
    DISPLAY-HINT    "x"
    STATUS          current
    DESCRIPTION
        "This data type is used to model ISAKMP cookies. This is a
        binary string of 8 octets in network byte-order."
    SYNTAX  OCTET STRING (SIZE (8))

-- the ISAKMP DOI-independent SA MIB-Group
--
-- a collection of objects providing information about the
-- DOI-independent portion of SAs generated using ISAKMP
--

saTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SaEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The (conceptual) table containing the DOI-independent
        portion of ISAKMP SAs.

        There should be one row for every phase 1 security
        association that exists in the entity that uses ISAKMP. The
        maximum number of rows is implementation dependent."
    ::= { isakmpSaTable 1 }

saEntry OBJECT-TYPE
    SYNTAX      SaEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry (conceptual row) containing the DOI-independent
        information on a particular ISAKMP SA.

        A row in this table cannot be created or deleted by SNMP
        operations on columns of the table."
    INDEX       {
        saLocalIpAddressType,
        saLocalIpAddress,
        saRemoteIpAddressType,
        saRemoteIpAddress,
```

```
        saInitiatorCookie,
        saResponderCookie }
    ::= { saTable 1 }

SaEntry::= SEQUENCE {

-- identification
    saLocalIpAddressType    InetAddressType,
    saLocalIpAddress        InetAddress,
    saRemoteIpAddressType   InetAddressType,
    saRemoteIpAddress       InetAddress,
    saInitiatorCookie       IsakmpCookie,
    saResponderCookie       IsakmpCookie,

-- communication information
    saLocalUdpPort          Integer32,
    saRemoteUdpPort         Integer32,

-- peer version information
    saPeerMajorVersion      Integer32,
    saPeerMinorVersion      Integer32,

-- creation/status/type
    saDoi                   IsakmpDOI,
    saLocallyInitiated      TruthValue,
    saStatus                INTEGER,
    saExchangeType          IsakmpExchangeType,

-- statistics
    saTimeSeconds           Counter32,
    saInPackets             Counter32,
    saOutPackets            Counter32,
    saInOctets              Counter32,
    saOutOctets             Counter32
}


saLocalIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The type of the local address used to negotiate the ISAKMP
        phase 1 SA."
    ::= { saEntry 1 }

saLocalIpAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16|20))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
        "The local address used to negotiate the ISAKMP phase 1 SA."
    ::= { saEntry 2 }

saRemoteIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The type of the remote address used to negotiate the ISAKMP
        phase 1 SA."
    ::= { saEntry 3 }

saRemoteIpAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16|20))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The remote address used to negotiate the ISAKMP phase 1
        SA."
    ::= { saEntry 4 }

saInitiatorCookie OBJECT-TYPE
    SYNTAX      IsakmpCookie
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The value of the cookie used by the initiator for the
        ISAKMP phase 1 SA."
    ::= { saEntry 5 }

saResponderCookie OBJECT-TYPE
    SYNTAX      IsakmpCookie
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The value of the cookie used by the responder for the
        ISAKMP phase 1 SA.

        Note that this value may be 0 if the ISAKMP phase 1 SA has
        been initiated but not responded to by the peer entity.

        It must never be 0 if this entry represents an ISAKMP phase
        1 SA establishment attempt that has been initiated by the
        peer. This rule prevents index collisions in the (unlikely)
        event that two peers simultaneously initiate with the same
        cookie at the same time."
    ::= { saEntry 6 }

saLocalUdpPort OBJECT-TYPE
    SYNTAX      Integer32 (0..65535)
    MAX-ACCESS  read-only
```

```
        STATUS      current
        DESCRIPTION
            "The local UDP port number that this ISAKMP phase 1 SA was
            negotiated with."
        ::= { saEntry 7 }

    saRemoteUdpPort OBJECT-TYPE
        SYNTAX      Integer32 (0..65535)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The remote UDP port number that this ISAKMP phase 1 SA was
            negotiated with."
        ::= { saEntry 8 }

    saPeerMajorVersion OBJECT-TYPE
        SYNTAX      Integer32 (0..15)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The major version number from the ISAKMP packet header used
            by the peer."
        REFERENCE   "Section 3.1 of RFC 2408"
        ::= { saEntry 9 }

    saPeerMinorVersion OBJECT-TYPE
        SYNTAX      Integer32 (0..15)
        MAX-ACCESS  read-only
        STATUS      current

        DESCRIPTION
            "The minor version number from the ISAKMP packet header used
            by the peer."
        REFERENCE   "Section 3.1 of RFC 2408"
        ::= { saEntry 10 }

    saDoi OBJECT-TYPE
        SYNTAX      IsakmpDOI
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The specific DOI value that this ISAKMP SA is using.

            Note that this value MAY be 0, as allowed by Section 3.4 of
            RFC 2408"
        REFERENCE   "Section 3.3 of RFC 2408"
        ::= { saEntry 11 }

    saLocallyInitiated OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "This value is 'true' if the ISAKMP phase 1 SA was initiated
        by the local entity, and 'false' if initiated by the remote
        entity."
    ::= { saEntry 12 }

saStatus OBJECT-TYPE
    SYNTAX      INTEGER { negotiating(1), established(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The status of the ISAKMP phase 1 SA.

        If the state is 'negotiating', it means that processing of
        the final packet of the phase 1 exchange is not yet
        complete.

        If the state is 'established', it means that processing of
        all packets associated with ISAKMP phase 1 SA negotation is
        complete, and the entities involved in the ISAKMP phase 1 SA
        are authenticated."
    ::= { saEntry 13 }

saExchangeType OBJECT-TYPE
    SYNTAX      IsakmpExchangeType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The exchange type used to negotiate the ISAKMP phase 1 SA."
    REFERENCE   "Section 3.1 of RFC 2408"
    ::= { saEntry 14 }

saTimeSeconds OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "seconds"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of seconds the SA has existed. In other words,
        how old the SA is."
    ::= { saEntry 15 }

saInPackets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets received by the ISAKMP phase 1
        SA, including un-encrypted packets used to negotiate the
```

```
        ISAKMP phase 1 SA, and any re-transmissions."
    ::= { saEntry 16 }

saOutPackets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets sent by the ISAKMP phase 1 SA,
        including un-encrypted packets used to negotiate the ISAKMP
        phase 1 SA, and any re-transmissions sent."
    ::= { saEntry 17 }

saInOctets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "bytes"
    MAX-ACCESS  read-only
    STATUS      current




    DESCRIPTION
        "The amount of traffic measured in bytes received by the
        ISAKMP phase 1 SA. This includes encrypted and un-encrypted
        traffic used to negotiate the ISAKMP phase 1 SA, and any re-
        transmissions received."
    ::= { saEntry 18 }

saOutOctets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "bytes"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The amount of traffic measured in bytes sent by the ISAKMP
        phase 1 SA. This includes encrypted and un-encrypted traffic
        used to negotiate the ISAKMP phase 1 SA, and any re-
        transmissions."
    ::= { saEntry 19 }


--
-- the ISAKMP Entity MIB-Group
--

isakmpMajorVersion OBJECT-TYPE
    SYNTAX      Integer32 ( 0..15 )
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "The maximum major version number value capable of being
        supported by the entity."
    ::= { isakmpGlobals 1 }

isakmpMinorVersion OBJECT-TYPE
    SYNTAX      Integer32 ( 0..15 )
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum minor version number value capable of being
        supported by the entity."
    ::= { isakmpGlobals 2 }


--
-- ISAKMP phase 1 SA statistics
--


isakmpCurrentSAs OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of ISAKMP SAs in the entity."
    ::= { isakmpNegStats 1 }

isakmpCurrentInitiatedSAs OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of ISAKMP SAs successfully negotiated in
        the entity that were initiated by the entity."
    ::= { isakmpNegStats 2 }

isakmpCurrentRespondedSAs OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of ISAKMP SAs successfully negotiated in
        the entity that were initiated by the peer entity."
    ::= { isakmpNegStats 3 }

isakmpTotalSAs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "The total number of ISAKMP SAs successfully negotiated in
        the entity since boot time."
    ::= { isakmpNegStats 4 }

isakmpTotalInitiatedSAs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP SAs successfully negotiated in
        the entity since boot time that were initiated by the
        entity."
    ::= { isakmpNegStats 5 }

isakmpTotalRespondedSAs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP SAs successfully negotiated in
        the entity since boot time that were initiated by the peer
        entity."
    ::= { isakmpNegStats 6 }

isakmpTotalAttempts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP SAs negotiation attempts made
        since boot time. This includes successful negotiations."
    ::= { isakmpNegStats 7 }

isakmpTotalAsInitAttempts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP SAs negotiation attempts made
        where the entity was the initiator since boot time. This
        includes successful negotiations."
    ::= { isakmpNegStats 8 }

isakmpTotalAsRespAttempts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP SAs negotiation attempts made
        where the entity was the responder since boot time. This
        includes successful negotiations."
```

```
    ::= { isakmpNegStats 9 }


--
-- traffic statistics
--

isakmpTotalInPackets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current


    DESCRIPTION
        "The total number of ISAKMP packets received by the entity
        since boot time, including re-transmissions and un-encrypted
        packets."
    ::= { isakmpTrafStats 1 }

isakmpTotalOutPackets OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP packets sent by the entity since
        boot time, including re-transmissions and un-encrypted
        packets."
    ::= { isakmpTrafStats 2 }

isakmpTotalInOctets OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "bytes"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total amount of ISAKMP traffic received by the entity
        since boot time, measured in bytes, including any re-
        transmitted packets received, and including encrypted and
        un-encrypted packets."
    ::= { isakmpTrafStats 3 }

isakmpTotalOutOctets OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "bytes"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total amount of ISAKMP traffic sent by the entity since
        boot time, measured in bytes, including any re-transmissions
```

```
        and including encrypted and un-encrypted packets."
    ::= { isakmpTrafStats 4 }


--
-- global error counts
--

isakmpTotalInitFailures OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of attempts to initiate an ISAKMP phase 1
        SA that failed since boot time, when there was a response
        from the peer entity.

        This value may be used to detect clogging or denial-of-
        service attacks."
    ::= { isakmpErrors 1 }

isakmpTotalInitNoResponses OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of attempts to initiate an ISAKMP phase 1
        SA that failed since boot time, when there was no response
        from the peer entity.
        This should only be incremented if the peer does not repond
        to the first packet of attempted negotiations."
    ::= { isakmpErrors 2 }

isakmpTotalRespFailures OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of attempts to initiate an ISAKMP phase 1
        SA that failed since boot time, when the initiation attempt
        came for the peer entity."
    ::= { isakmpErrors 3 }

isakmpInvalidCookies    OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of ISAKMP packets with invalid cookies
        received by the entity since boot time."
```

```
    ::= { isakmpErrors 4 }


--
-- ISAKMP Traps and Control
--


invalidCookieTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Indicates whether invalidCookieTrap traps should be
        generated."
    DEFVAL { false }
    ::= { isakmpTrapControl 1 }

localIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The type of the local IP address used in an ISAKMP message,
        to be associated with a trap."
    ::= { isakmpTrapObjects 1 }

localIpAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16|20))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The local IP address used in an ISAKMP message, to be
        associated with a trap."
    ::= { isakmpTrapObjects 2 }

localUdpPort OBJECT-TYPE
    SYNTAX      Integer32 (0..65535)
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The local port UDP number used in an ISAKMP message, to be
        associated with a trap."
    ::= { isakmpTrapObjects 3 }

remoteIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The type of the remote IP used in an ISAKMP message, to be
```

```
        associated with a trap."
    ::= { isakmpTrapObjects 4 }

remoteIpAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16|20))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The remote IPaddress used in an ISAKMP message, to be
        associated with a trap."
    ::= { isakmpTrapObjects 5 }

remoteUdpPort OBJECT-TYPE
    SYNTAX      Integer32 (0..65535)
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The remote UDP port number used in an ISAKMP message, to be
        associated with a trap."
    ::= { isakmpTrapObjects 6 }

initiatorCookie OBJECT-TYPE
    SYNTAX      IsakmpCookie
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The initiator cookie used in an ISAKMP message, to be
        associated with a trap."
    ::= { isakmpTrapObjects 7 }

responderCookie OBJECT-TYPE
    SYNTAX      IsakmpCookie
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The responder cookie used in an ISAKMP message, to be
        associated with a trap."
    ::= { isakmpTrapObjects 8 }

invalidCookieTrap NOTIFICATION-TYPE
    OBJECTS {
        localIpAddressType,
        localIpAddress,
        localUdpPort,
        remoteIpAddressType,
        remoteIpAddress,
        remoteUdpPort,
        initiatorCookie,
        responderCookie,
        isakmpInvalidCookies
    }
```

```
    STATUS  current

    DESCRIPTION
        "ISAKMP packets with invalid cookies were detected from the
        specified source, intended for the specified destination.

        The initiator and responder cookies are also sent with the
        trap.

        The current count is sent to allow the trap to accurately
        relfect dropped and throttled traps.

        Implementations SHOULD send one trap per peer (within a
        reasonable time period, rather than sending one trap per
        packet."
    ::= { isakmpTraps 0 1 }


--
-- Units of Conformance (Object Groups)
--

isakmpSaGroup OBJECT-GROUP
    OBJECTS {
        --
        -- Authors' note: The first six objects are commented
        -- out, since the current SMI does not allow objects with
        -- a MAX-ACCESS clause of not-accessible to be put in
        -- groups.
        --
        -- saLocalIpAddressType, saLocalIpAddress,
        -- saRemoteIpAddressType, saRemoteIpAddress,
        -- saInitiatorCookie, saResponderCookie,
        saLocalUdpPort, saRemoteUdpPort, saPeerMajorVersion,
        saPeerMinorVersion, saDoi, saLocallyInitiated, saStatus,
        saExchangeType, saTimeSeconds, saInPackets, saOutPackets,
        saInOctets, saOutOctets
    }
    STATUS  current
    DESCRIPTION
        "A collection of objects that describe the state of the
        security associations of the ISAKMP protocol."
    ::= { isakmpGroups 1 }

isakmpGlobalsGroup OBJECT-GROUP
    OBJECTS {
        isakmpMajorVersion, isakmpMinorVersion, isakmpCurrentSAs,
        isakmpCurrentInitiatedSAs, isakmpCurrentRespondedSAs,
        isakmpTotalSAs, isakmpTotalInitiatedSAs,
        isakmpTotalRespondedSAs, isakmpTotalAttempts,
        isakmpTotalAsInitAttempts, isakmpTotalAsRespAttempts,
```

```
        isakmpTotalInPackets, isakmpTotalOutPackets,
        isakmpTotalInOctets, isakmpTotalOutOctets,
        isakmpTotalInitFailures, isakmpTotalInitNoResponses,
        isakmpTotalRespFailures, isakmpInvalidCookies
    }
    STATUS  current
    DESCRIPTION
        "A collections of objects that describe the global state of
        the ISAKMP protocol."
    ::= { isakmpGroups 2 }

isakmpTrapControlGroup OBJECT-GROUP
    OBJECTS {
        invalidCookieTrapEnable
    }
    STATUS  current
    DESCRIPTION
        "Trap control for the ISAKMP protocol."
    ::= { isakmpGroups 3 }

isakmpTrapDataGroup OBJECT-GROUP
    OBJECTS {
        localIpAddressType, localIpAddress, localUdpPort,
        remoteIpAddressType, remoteIpAddress, remoteUdpPort,
        initiatorCookie, responderCookie
    }
    STATUS  current
    DESCRIPTION
        "Trap data for the ISAKMP protocol."
    ::= { isakmpGroups 4 }

isakmpTrapGroup NOTIFICATION-GROUP
    NOTIFICATIONS   {
        invalidCookieTrap
    }
    STATUS  current
    DESCRIPTION
        "The traps for the ISAKMP protocol."
    ::= { isakmpGroups 5 }

--
-- Compliance Statements
--

isakmpDoiIndependentMonitorCompliance MODULE-COMPLIANCE
    STATUS  current

    DESCRIPTION
        "The compliance statement for the SNMPv3 entities which
        implement the ISAKMP DOI-Indpendent Monitoring MIB."
    MODULE    -- this module
```

```
    MANDATORY-GROUPS {
         isakmpSaGroup, isakmpGlobalsGroup, isakmpTrapControlGroup,
        isakmpTrapDataGroup, isakmpTrapGroup
    }

    -- Allows the trap control to be read-only.

OBJECT invalidCookieTrapEnable
    MIN-ACCESS read-only
    DESCRIPTION
        "If an implementation cannot properly secure this variable
        against unauthorized write access, it SHOULD implement it as
        read-only, to prevent the security risk of enabling the
        traps.  Of course, there must be other means of controlling
        the generation of the associated trap."

    -- Don't require support for dns(16) address type

OBJECT  localIpAddressType
    SYNTAX INTEGER { ipv4(1), ipv6(2) }
    DESCRIPTION
        "An implementation is only required to support IPv4 and IPv6
         addresses."

OBJECT remoteIpAddressType
    SYNTAX INTEGER { ipv4(1), ipv6(2) }
    DESCRIPTION
        "An implementation is only required to support IPv4 and IPv6
         addresses."

    -- Authors' note: The following statements are commented out,
    -- since the current SMI does not allow objects with a
    -- MAX-ACCESS clause of not-accessible to be put in groups,
    -- and objects that are not in groups cannot be in
    -- compliance statements.

-- OBJECT   saLocalIpAddressType
--  SYNTAX INTEGER { ipv4(1), ipv6(2) }
--  DESCRIPTION
--      "An implementation is only required to support IPv4 and IPv6
--       addresses."

-- OBJECT  saRemoteIpAddressType
--  SYNTAX INTEGER { ipv4(1), ipv6(2) }
--  DESCRIPTION
--      "An implementation is only required to support IPv4 and IPv6
--       addresses."

    ::= { isakmpConformance 1 }


END
```

4. Security Considerations

This MIB contains readable objects whose values provide information related to IPsec SAs. While some of the information is readily available by monitoring the traffic into an entity, other information may provide attackers with more information than an administrator may desire.

Of particular concern is the ability to disable the transmission of traps. The traps defined in this MIB may appear due to badly configured systems and transient error conditions, but they may also appear due to attacks. If an attacker can disable these traps, they reduce some of the warnings that may be provided to system administrators.

While unauthorized access to the readable objects is relatively innocuous, unauthorized access to those objects through an insecure channel can provide attackers with more information about a system than an administrator may desire.

A specific example of this includes, but is not limited to, the monitoring of global statistic counts by attackers that provides feedback on the progress of an attack.

It is thus important to control even GET access to these objects and possibly to even encrypt the values of these object when sending them over the network via SNMP. Not all versions of SNMP provide features for such a secure environment.

SNMPv1 by itself is not a secure environment. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model RFC 2574 [RFC2574] and the View-based Access Control Model RFC 2575 [RFC2575] is recommended.
It is then a customer/user responsibility to ensure that the SNMP entity giving access to an instance of this MIB, is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

5. Acknowledgments

This document was begun and mostly developed by Tim Jenkins and John Shriver. The editor listed for this document (Paul Hoffman) only sheparded the last steps before final publication.

This document is based in part on an earlier proposal titled "draft-ietf-ipsec-mib-xx.txt". That series was abandoned, since it included application specific constructs in addition to the IPsec only objects.

Portions of the original document's origins were based on the working paper "IP Security Management Information Base" by R. Thayer and U. Blumenthal.

Contribution to the IPsec MIB series of documents comes from D. McDonald, M. Baugher, C. Brooks, C. Powell, M. Daniele, T. Kivinen, J. Walker, S. Kelly, J. Leonard, M. Richardson and R. Charlet, M. Zallocco, and others participating in the IPsec working group.

6. References

6.1 Normative references

[ADDRMIB] Daniele, M., Haberman, B., Routhier, S., Schoenwaelder, J., "Textual Conventions for Internet Network Addresses", RFC 2851, June, 2000

[IPSECTC] Shriver, J., "IPSec DOI Textual Conventions MIB, draft-ietf-ipsec-doi-tc-mib, work in progress

[RFC2571] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", RFC 2571, April 1999

[RFC1155] Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", STD 16, RFC 1155, May 1990

[RFC1212] Rose, M., and K. McCloghrie, "Concise MIB Definitions", STD 16, RFC 1212, March 1991

[RFC1215] M. Rose, "A Convention for Defining Traps for use with the SNMP", RFC 1215, March 1991

[RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999

[RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999

[RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", STD 15, RFC 1157, May 1990.

[RFC1901] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to Community-based SNMPv2", RFC 1901, January 1996.

[RFC1906] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1906, January 1996.

[RFC2572] Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2572, April 1999

[RFC2574] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2574, April 1999

[RFC1905] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1905, January 1996.

[RFC2573] Levi, D., Meyer, P., and B. Stewart, "SNMPv3 Applications", RFC 2573, April 1999

[RFC2575] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 2575, April 1999

[RFC2570] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", RFC 2570, April 1999

6.2 Non-normative references

[ISAKMP]Maughan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998

A. Changes from -05 to -06

[[To be removed when published as an RFC]]

- Changed the authors' names to the editor's name.

- Added acknowledgement for the original authors.

- Minor formatting changes.

- Split the references into normative and non-normative.

NOTE: There are still lines that talk about things that need to be changed before release of the RFC (search for "release").