ID Message Exchange Format Working Group
INTERNET-DRAFT
draft-glenn-id-sensor-alert-mib-01.txt

Glenn Mansfield
Cyber Solutions Inc.
Dipankar Gupta
Hewlett Packard Company
November 20 2000

Intrusion Detection Sensor Alert MIB
<draft-glenn-id-sensor-alert-mib-01.txt>

Status of this Memo

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines the contents of messages that will be used primarily by sensors to send alerts to managers when an intrusion related event is detetcted.

Table of Contents

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.

2. The Intrusion detection Message Exchange model.

An Intrusion Detection system (Fig. 1) generally comprises an sensor which scans Data Sources for signs of intrusions. When it detects a sign or a signature the sensor sends a Message or Alert to the Manager(s). Managers in turn may exchange Messages or Alerts for cooperative or collaborative purposes. (A different MIB will be used for that purpose.)

ID Message Exchange Model

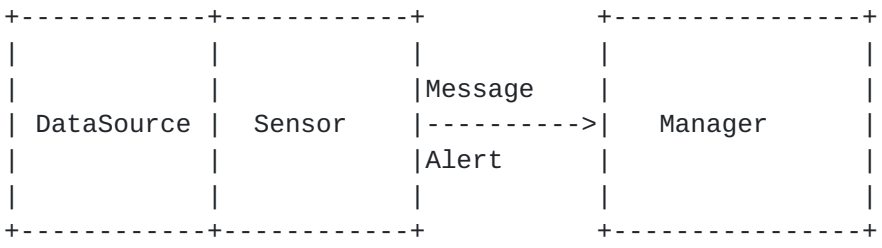

Fig. 1

3. MIB Model for ID Message Exchanges.

In Intrusion detection and management, the communication between the different components of the system will essentially be event based. Sensors will be assigned the tasks of watching some data-sources and looking out for signs of (attempted) intrusions or attacks. In case any such sign is detected it is brought to the notice of the Manager. The Manager will then take the appropriate action which may involve relaying the notification and/or carrying out further investigation by talking to peers, higher level managers and/or the entity that originated the notification.

This note relates to the alert from the sensor to the manager. The alert describes the intrusion in terms of a set of managed objects [MOs] and their values. The managed objects are defined in a MIB [Management Information Base] - the Intrusion Detection Sensor Alert MIB. A primary design constraint that needs to be met by the Intrusion MIB is that sensors are lightweight. They are not expected to do any involved processing and or archiving of events and/or data. Some of the managed objects are required to describe the sensor itself. Others are required to describe the intrusion.

4. MIB design.

The basic design principle has been to keep the MIB as simple as possible. The generic requirements are

- Alerts should contain the minimum information required by the manager to assess the situation correctly and to take appropriate defensive or investigative steps.
- Alerts, if carried in UDP datagrams, should not be too large as to require IP fragmentation. [If SNMP is used as as the application protocol, some managers may not accept SNMP-PDUs that are larger than 484 bytes.]

The MIB comprises of two parts, the idsaSensorObjects and idsaAlerts described below.

- The idsaSensorObjects subtree defines the objects that describe the sensor itself - The idsaAlerts subtree defines the objects that describe the alerts It is a table the size of which is decided by implementations.

5. The Intrusion Detection Sensor Alert MIB.

```
INTRUSION-DETECTION-SENSOR-ALERT-MIB DEFINITIONS ::= BEGIN

 IMPORTS
   MODULE-IDENTITY,  Counter32, Gauge32, OBJECT-TYPE,
   OBJECT-IDENTITY,  mib-2      FROM SNMPv2-SMI
   DateAndTime, TimeStamp
              FROM SNMPv2-TC
   MODULE-COMPLIANCE, OBJECT-GROUP
              FROM SNMPv2-CONF
   SnmpEngineID, SnmpAdminString
              FROM SNMP-FRAMEWORK-MIB
   InetAddressType, InetAddress
              FROM INET-ADDRESS-MIB
   URLString
              FROM NETWORK-SERVICES-MIB;

idsaMIB MODULE-IDENTITY
    LAST-UPDATED "200011160000Z"        --  16th November 2000
    ORGANIZATION "IETF Intrusion Detection Message Exchange Format
                  Working Group"
    CONTACT-INFO
   "                      Glenn Mansfield
                  Postal: Cyber Solutions Inc.
                          6-6-3, Minami Yoshinari
                          Aoba-ku, Sendai, Japan 989-3204.

                     Tel: +81-22-303-4012
                     Fax: +81-22-303-4015
                  E-mail: glenn@cysols.com

                          Dipankar Gupta
                  Postal: Hewlett Packard Company
                          690 East Middlefield Road, MS 31R
                          Mountain View California 94043.

                     Tel: +1-650-919-8066
                     Fax: +1-650-919-8540
                  E-mail: dipankar_gupta@hp.com

    Working Group E-mail: idwg-public@zurich.ibm.com
            To subscribe: idwg-public-request@zurich.ibm.com"

    DESCRIPTION
            " The MIB for Intrusion Detection Messages."
```

```
            ::= { mib-2 xxx }     -- to be assigned by IANA

    idsaSensorObjects OBJECT-IDENTITY
        STATUS current
        DESCRIPTION
          " This is the base object for the objects used in the
            notifications."
        ::= {idsaMIB 1}

    idsaSensorID OBJECT-TYPE
        SYNTAX  SnmpAdminString
        MAX-ACCESS  read-only
        STATUS  current
        DESCRIPTION
          " An identifier to uniquely identify the Analyzer
            in the domain."
        ::= { idsaSensorObjects 1 }

    idsaSensorDescription OBJECT-TYPE
        SYNTAX  SnmpAdminString
        MAX-ACCESS  read-only
        STATUS  current
        DESCRIPTION
          " A short description of the Sensor."
        ::= { idsaSensorObjects 2 }

    idsaSensorProductID OBJECT-TYPE
        SYNTAX  SnmpAdminString
        MAX-ACCESS  read-only
        STATUS  current
        DESCRIPTION
          "A reference to MIB definitions specific to the
           analyzer generating the message.  If this information
           is not present, its value should be set to the OBJECT
           IDENTIFIER { 0 0 }, which is a syntatically valid
           object identifier."
        ::= { idsaSensorObjects 3 }

    idsaSensorAddressType OBJECT-TYPE
        SYNTAX InetAddressType
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The type of the address which follows."
        ::= { idsaSensorObjects 4}

    idsaSensorAddress OBJECT-TYPE
        SYNTAX InetAddress
```

```
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The Internet address of the sensor."
        ::= { idsaSensorObjects 5}

    idsaSensorManufacturer   OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " the Manufacturer of the sensor that detected the event."
        ::= { idsaSensorObjects 6}

    idsaSensorProductName   OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " the name of the product that detected the event."
        ::= { idsaSensorObjects 7}

    idsaSensorVersion   OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " the version number of the sensor that detected the event."
        ::= { idsaSensorObjects 8}


    idsaSensorLocation OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " the location of the tool that detected the event."
        ::= { idsaSensorObjects 9}


    idsaAlerts OBJECT-IDENTITY
        STATUS current
        DESCRIPTION
          " This is the base object for the subtree of objects defining
            the alerts."
        ::= {idsaMIB 2}

   --  idsaAlertTable: The Table of Alerts. Each row represents an Alert.
```

```
   --  idsaAlertID is the key to the table. The size of this table will be
   --  implementation dependent - some implementors may choose to keep
   --  a maximum of one messages in this table.

    idsaAlertTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF IdsaAlertEntry
        MAX-ACCESS  not-accessible
        STATUS  current
        DESCRIPTION
          " Each row of this table contains information
            about an alert indexed by idsaAlertID."
        ::= { idsaAlerts 1 }

    idsaAlertEntry OBJECT-TYPE
        SYNTAX  IdsaAlertEntry
        MAX-ACCESS  not-accessible
        STATUS  current
        DESCRIPTION
          " Entry containing information pertaining to
            an alert."
        INDEX { idsaAlertID}
        ::= { idsaAlertTable 1 }

    IdsaAlertEntry ::= SEQUENCE {
       idsaAlertID
                 INTEGER,
       idsaAlertLocalAddressType
                 InetAddressType,
       idsaAlertLocalAddress
                 InetAddress,
       idsaAlertInterfaceIndex
                 INTEGER,
       idsaAlertTimeStamp
                 DateAndTime,
       idsaAlertActionsTaken
                 INTEGER,
       idsaAlertAttackName
                 SnmpAdminString,
       idsaAlertMoreInfo
                 URLString,
       idsaAlertSrcAddressType
                 InetAddressType,
       idsaAlertSrcAddress
                 InetAddress,
       idsaAlertDstAddressType
                  InetAddressType,
       idsaAlertDstAddress
                  InetAddress,
```

```
       idsaAlertSrcPort
                  INTEGER,
       idsaAlertDstPort
                  INTEGER
       }


    idsaAlertID OBJECT-TYPE
        SYNTAX INTEGER (1..65535)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The AlertID uniquely identifies each alert generated
            by the sensor."
        ::= {idsaAlertEntry 1}

    idsaAlertLocalAddressType OBJECT-TYPE
        SYNTAX InetAddressType
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The type of the address which follows."
        ::= { idsaAlertEntry 2}

    idsaAlertLocalAddress OBJECT-TYPE
        SYNTAX InetAddress
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The Internet address associated with the alert ."
        ::= { idsaAlertEntry 3}

    idsaAlertInterfaceIndex OBJECT-TYPE
        SYNTAX INTEGER (1..65535)
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The ifIndex of the interface on which the event was
            detected  by the sensor."
        ::= {idsaAlertEntry 4}

    idsaAlertTimeStamp OBJECT-TYPE
        SYNTAX DateAndTime
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The local date and time when this alert was generated."
        ::= { idsaAlertEntry 5}
```

```
    -- the actions will probably be a comma separated list of action
    -- codes or a pointer to another MIB table from which the actions
    -- may be fetched.
    --
    idsaAlertActionsTaken OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The list of automatic actions taken by the sensor"
        ::= { idsaAlertEntry 6}

    -- SnmpAdminString length is 255 characters max. It contains
    -- information represented using the ISO/IEC IS 10646-1 character
    -- set, encoded using the UTF-8 transformation format to facilitate
    -- internationalization.

    idsaAlertAttackName OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " the name of the atack, if known. If not known this field will
                  be inaccessile."
        ::= { idsaAlertEntry 7}

    idsaAlertMoreInfo OBJECT-TYPE
        SYNTAX  OBJECT IDENTIFIER
        MAX-ACCESS  read-only
        STATUS  current
        DESCRIPTION
          "A reference to MIB definitions specific to this
          message.  If this information is not
          present, its value should be set to the OBJECT
          IDENTIFIER { 0 0 }, which is a syntatically valid
          object identifier."
        ::= { idsaAlertEntry 8}

    idsaAlertSrcAddressType OBJECT-TYPE
        SYNTAX InetAddressType
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The type of the Internet address that was the attack source."
        ::= { idsaAlertEntry 9}

    idsaAlertSrcAddress OBJECT-TYPE
        SYNTAX InetAddress
```

```
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The Internet addresses of the entity from which the attack
            originated, if known. "
        ::= { idsaAlertEntry 10}

    idsaAlertDstAddressType OBJECT-TYPE
        SYNTAX InetAddressType
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The type of the Internet address that was the attack target."
        ::= { idsaAlertEntry 11}

    idsaAlertDstAddress OBJECT-TYPE
        SYNTAX InetAddress
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The Internet address of the entity to which the attack
            was destined, if known."
        ::= { idsaAlertEntry 12}

    idsaAlertSrcPort OBJECT-TYPE
        SYNTAX INTEGER
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The port number from where the attack has originated "
        ::= { idsaAlertEntry 13}

    idsaAlertDstPort OBJECT-TYPE
        SYNTAX INTEGER
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " The port number to which the attack is destined "
        ::= { idsaAlertEntry 14}
```

```
    -- Conformance information

    idsaConformance OBJECT IDENTIFIER ::= {idsaMIB 3 }

    idsaGroups      OBJECT IDENTIFIER ::= { idsaConformance 1 }
    idsaCompliances OBJECT IDENTIFIER ::= { idsaConformance 2 }

    -- Compliance statements

    idsaAlertCompliance MODULE-COMPLIANCE
        STATUS  current
        DESCRIPTION
                "The compliance statement for SNMP entities
                 which implement the
                            INTRUSION-DETECTION-SENSOR-ALERT-MIB."

        MODULE  -- this module
            MANDATORY-GROUPS { idsaAlertGroup }

        ::= { idsaCompliances 1 }
```

```
    -- Units of conformance

    idsaAlertGroup    OBJECT-GROUP
        OBJECTS {
                    idsaSensorID,
                    idsaSensorDescription,
                    idsaSensorProductID,
                    idsaSensorAddressType,
                    idsaSensorAddress,
                    idsaSensorManufacturer,
                    idsaSensorProductName,
                    idsaSensorVersion,
                    idsaSensorLocation,
                    idsaAlertID,
                    idsaAlertLocalAddressType,
                    idsaAlertLocalAddress,
                    idsaAlertInterfaceIndex,
                    idsaAlertTimeStamp,
                    idsaAlertActionsTaken,
                    idsaAlertAttackName,
                    idsaAlertMoreInfo,
                    idsaAlertSrcAddressType,
                    idsaAlertSrcAddress,
                    idsaAlertDstAddressType,
                    idsaAlertDstAddress,
                    idsaAlertSrcPort,
                    idsaAlertDstPort

       }
        STATUS  current
        DESCRIPTION
                " A collection of objects for generation and despatch of
                  alerts pertaining to intrusions detected."
        ::= { idsaGroups 1 }

   END
```

6. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. Acknowledgements

This draft is the product of discussions and deliberations carried out in the IETF intrusion detection message exchange format working group (ietf-idwg-wg).

References

[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

[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

[INETMIB] http://www.ietf.org/internet-drafts/draft-ops-endpoint-mib-00.txt - work in progress.

Security Considerations

There are management objects defined in this MIB that have a MAX-ACCESS clause of read-write and read-create. There is the risk that an intruder can alter or create any management objects of this MIB via direct SNMP SET operations. So, care must be taken to put in place the security provisions of SNMP for authentication and access control. Not all versions of SNMP provide features for such a secure environment.

SNMPv1 by itself is such an insecure 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 (read) and SET (write) the objects in this MIB.

It is strongly recommended that the implementors consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model RFC 2274 [RFC2274] and the View-based Access Control Model RFC 2275 [RFC2275] 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 those objects only to those principals (users) that have legitimate rights to access them.

Authors' Addresses

Glenn Mansfield
Cyber Solutions Inc.
6-6-3 Minami Yoshinari
Aoba-ku, Sendai 989-3204
Japan

Phone: +81-22-303-4012
EMail: glenn@cysols.com

Dipankar Gupta
Hewlett Packard Company
690 East Middlefield Road, MS 31R
Mountain View California 94043.

Phone: +1-650-919-8066
E-mail: dipankar_gupta@hp.com

Full Copyright statement