            **Using Authentication, Authorization, and Accounting Services
              to Dynamically Provision View-Based Access Control Model
                            User-to-Group Mappings**

Abstract

   This memo defines a portion of the Management Information Base (MIB)
   for use with network management protocols. It describes the use of
   information provided by Authentication, Authorization, and Accounting
   (AAA) services, such as the Remote Authentication Dial-In User
   Service (RADIUS), to dynamically update user-to-group mappings in the
   View-based Access Control Model (VACM).

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6065.

Copyright Notice

Table of Contents

1. Introduction

   This memo specifies a way to dynamically provision selected View-
   based Access Control Model (VACM) [RFC3415] Management Information
   Base (MIB) objects, based on information received from an
   Authentication, Authorization, and Accounting (AAA) service, such as
   RADIUS [RFC2865] and [RFC5607]. It reduces the need for security
   administrators to manually update VACM configurations due to user
   churn, allowing a centralized AAA service to provide the information
   associating a given user with the access control policy (known as a
   "group" in VACM) governing that user's access to management
   information.

   This memo requires no changes to the Abstract Service Interface for
   the Access Control Subsystem, and requires no changes to the Elements
   of Procedure for VACM. It provides a MIB module that reflects the
   information provided by the AAA service, along with elements of
   procedure for maintaining that information and performing
   corresponding updates to VACM MIB data.

   The reader is expected to be familiar with [RFC3415], [RFC5607],
   [RFC5608], and their supporting specifications.

2. The Internet-Standard Management Framework

   For a detailed overview of the documents that describe the current
   Internet-Standard Management Framework, please refer to section 7 of
   RFC 3410 [RFC3410].

   Managed objects are accessed via a virtual information store, termed
   the Management Information Base or MIB. MIB objects are generally
   accessed through the Simple Network Management Protocol (SNMP).
   Objects in the MIB are defined using the mechanisms defined in the
   Structure of Management Information (SMI). This memo specifies a MIB
   module that is compliant to the SMIv2, which is described in STD 58,
   RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580
   [RFC2580].

3. Conventions

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in RFC
   2119 [RFC2119].

4. Overview

4.1. Using AAA services with SNMP

   There are two use cases for AAA support of management access via
   SNMP. These are (a) service authorization and (b) access control
   authorization. The former is discussed in detail in [RFC5608]. The
   latter is the subject of this memo.

   The use case assumption here is that roles within an organization
   (which are represented in VACM as groups, which in turn name access
   control policies) change infrequently, while the users assigned to
   those roles change much more frequently. This memo describes how the
   user-to-role (group) mapping can be delegated to the RADIUS server,
   avoiding the need to re-provision managed devices as users are added,
   deleted, or assigned new roles in an organization.

   This memo assumes that the detailed access control policies are pre-
   configured in VACM, and does not attempt to address the question of
   how the policy associated with a given role is put in place.

   The only additional information obtained from the AAA service is the
   mapping of the authenticated user's identifier to a specific role (or
   "group" in VACM terminology) in the access control policy. Dynamic
   user authorization for MIB database access control, as defined
   herein, is limited to mapping the authenticated user to a group,
   which in turn is mapped to whatever access control policies are
   already in place in VACM.

   The SNMP architecture [RFC3411] maintains strong modularity and
   separation of concerns, separating user identity (authentication)
   from user database access rights (authorization). RADIUS, on the
   other hand, allows for no such separation of authorization from
   authentication. Consequently, the approach here is to leverage
   existing RADIUS usage for identifying a principal, documented in
   [RFC5608], along with the RADIUS Management-Policy-Id Attribute
   [RFC5607].

   A unique identifier is needed for each AAA-authorized "session",
   corresponding to a communication channel, such as a transport
   session, for which a principal has been AAA-authenticated and which
   is authorized to offer SNMP service. How these identifiers are
   assigned is implementation dependent. When a RADIUS Management-
   Policy-Id Attribute (or equivalent) is bound to such a session and
   principal authentication, this binding provides sufficient
   information to compute dynamic updates to VACM. How this information
   is communicated within an implementation is implementation dependent;
   this memo is only concerned with externally observable behavior.

The key concept here is that what we will informally call a "AAA
binding" binds:

1. a communications channel

2. an authenticated principal

3. service authorization

4. an access control policy name

Some of the binding is done via other specifications. A transport
model, such as the Secure Shell Transport Model [RFC5592], provides a
binding between 1 and 2 and 3, providing a securityName. In turn,
[RFC5607] provides a binding between (1+2+3) and 4. This document
extends that further, to create a binding between (1+2+3+4) and the
local (VACM MIB) definition of the named policy, called a group in
VACM.

4.2. Applicability

Though this memo was motivated to support the use of specific
Transport Models, such as the Secure Shell Transport Model [RFC5592],
it MAY be used with other implementation environments satisfying
these requirements:

o   use an AAA service for sign-on service and data access
    authorization;

o   provide an indication of the start of a session for a particular
    authenticated principal in a particular role, based on information
    provided by the AAA service. The principal will be identified
    using an SNMP securityName [RFC3411]. The role will be identified
    by the name of the corresponding VACM group.

o   provide an indication of the end of the need for being able to
    make access decisions for a particular authenticated principal, as
    at the end of a session, whether due to disconnection, termination
    due to timeout, or any other reason.

Likewise, although this memo specifically refers to RADIUS, it MAY be
used with other AAA services satisfying these requirements:

o   the service provides information semantically equivalent to the
    RADIUS Management-Policy-Id Attribute [RFC5607], which corresponds
    to the name of a VACM group;

o the service provides an authenticated principal identifier (e.g.,
   the RADIUS User-Name Attribute [RFC2865]) that can be transformed
   to an equivalent principal identifier in the form of a
   securityName [RFC3411].

5. Structure of the MIB Module

5.1. Textual Conventions

This MIB module makes use of the SnmpAdminString [RFC3411] and
SnmpSecurityModel [RFC3411] textual conventions.

5.2. The Table Structure

This MIB module defines a single table, the
vacmAaaSecurityToGroupTable. This table is indexed by the integer
assigned to each security model, the protocol-independent
securityName corresponding to a principal, and the unique identifier
of a session.

6. Relationship to Other MIB Modules

This MIB module has a close operational relationship with the SNMP-
VIEW-BASED-ACM-MIB (more commonly known as the "VACM MIB") from
[RFC3415]. It also relies on IMPORTS from several other modules.

6.1. Relationship to the VACM MIB

Although the MIB module defined here has a close relationship with
the VACM MIB's vacmSecurityToGroupTable, it in no way changes the
elements of procedure for VACM, nor does it affect any other tables
defined in VACM. See the elements of procedure (below) for details
of how the contents of the vacmSecurityToGroupTable are affected by
this MIB module.

6.2. MIB modules Required for IMPORTS

This MIB module employs definitions from [RFC2578], [RFC2579], and
[RFC3411].

6.3. Documents Required for REFERENCE Clauses

This MIB module contains REFERENCE clauses making reference to
[RFC2865], [RFC3411], and [RFC5590].

7. Elements of Procedure

   The following elements of procedure are formulated in terms of two
   types of events: an indication of the establishment of a session, and
   an indication that one has ended. These can result in the creation
   of entries in the vacmAaaSecurityToGroupTable, which can in turn
   trigger creation, update, or deletion of entries in the
   vacmSecurityToGroupTable.

   There are various possible implementation-dependent error cases not
   spelled out here, such as running out of memory. By their nature,
   recovery in such cases will be implementation dependent.
   Implementors are advised to consider fail-safe strategies, e.g.,
   prematurely terminating access in preference to erroneously
   perpetuating access.

7.1. Sequencing Requirements

   These procedures assume that a transport model, such as [RFC5592],
   coordinates session establishment with AAA authentication and
   authorization. They rely on the receipt by the AAA client of the
   RADIUS Management-Policy-Id [RFC5607] Attribute (or its equivalent)
   from the RADIUS Access-Accept message (or equivalent). They also
   assume that the User-Name [RFC2865] from the RADIUS Access-Request
   message (or equivalent) corresponds to a securityName [RFC3411].

   To ensure correct processing of SNMP PDUs, the handling of the
   indication of the establishment of a session in accordance with the
   elements of procedure below MUST be completed before the
   isAccessAllowed() Abstract Service Interface [RFC3415] is invoked for
   any SNMP PDUs from that session.

   If a session termination indication occurs before all invocations of
   the isAccessAllowed() Abstract Service Interface [RFC3415] have
   completed for all SNMP PDUs from that session, those remaining
   invocations MAY result in denial of access.

7.2. Actions upon Session Establishment Indication

7.2.1. Required Information

   Four pieces of information are needed to process the session
   establishment indication:

   o the SnmpSecurityModel [RFC3411] needed as an index into the
      vacmSecurityToGroupTable;

   o the RADIUS User-Name Attribute;

   o a session identifier, as a unique, definitive identifier of the
      session that the AAA authorization is tied to;

   o the RADIUS Management-Policy-Id Attribute.

   All four of these pieces of information are REQUIRED. In particular,
   if either the User-Name or Management-Policy-Id is absent, invalid,
   or a zero-length string, no further processing of the session
   establishment indication is undertaken.

   As noted in [Section 4.2](#), the above text refers specifically to RADIUS
   attributes. Other AAA services can be substituted, but the
   requirements imposed on the User-Name and the Management-Policy-Id-
   Attribute MUST be satisfied using the equivalent fields for those
   services.

[7.2.2](#). Creation of Entries in vacmAaaSecurityToGroupTable

   Whenever an indication arrives that a new session has been
   established, determine whether a corresponding entry exists in the
   vacmAaaSecurityToGroupTable. If one does not, create a new row with
   the columns populated as follows:

   o vacmAaaSecurityModel = value of SnmpSecurityModel corresponding to
      the security model in use;

   o vacmAaaSecurityName = RADIUS User-Name Attribute or equivalent,
      the securityName that will be used in invocations of the
      isAccessAllowed() Abstract Service Interface [[RFC3415](#)];

   o vacmAaaSessionID = session identifier, unique across all open
      sessions of all of this SNMP engine's transport models;

   o vacmAaaGroupName = RADIUS Management-Policy-Id Attribute or
      equivalent.

   Otherwise, if the row already exists, update the vacmAaaGroupName
   with the RADIUS Management-Policy-Id Attribute or equivalent
   supplied.

[7.2.3](#). Creation of Entries in vacmSecurityToGroupTable

   Whenever an entry is created in the vacmAaaSecurityToGroupTable, the
   vacmSecurityToGroupTable is examined to determine whether a
   corresponding entry exists there, using the value of
   vacmAaaSecurityModel for vacmSecurityModel, and the value of
   vacmAaaSecurityName for vacmSecurityName. If no corresponding entry
   exists, create one using the vacmAaaGroupName of the newly created

   entry to fill in vacmGroupName, using a value of "volatile" for the
   row's StorageType, and a value of "active" for its RowStatus.

[7.2.4](7.2.4-ref). **Update of vacmGroupName**

   Whenever the value of an instance of vacmAaaGroupName is updated, if
   a corresponding entry exists in the vacmSecurityToGroupTable, and
   that entry's StorageType is "volatile" and its RowStatus is "active",
   update the value of vacmGroupName with the value from
   vacmAaaGroupName.

   If a corresponding entry already exists in the
   vacmSecurityToGroupTable, and that row's StorageType is anything
   other than "volatile", or its RowStatus is anything other than
   "active", then that instance of vacmGroupName MUST NOT be modified.

   The operational assumption here is that if the row's StorageType is
   "volatile", then this entry was probably dynamically created; an
   entry created by a security administrator would not normally be given
   a StorageType of "volatile". If the value being provided by RADIUS
   (or another AAA service) is the same as what is already there, this
   is a no-op. If the value is different, the new information is
   understood as a more recent role (group) assignment for the user,
   which should supersede the one currently held there. The structure
   of the vacmSecurityToGroupTable makes it impossible for a
   (vacmSecurityModel, vacmSecurityName) tuple to map to more than one
   group.

[7.3](7.3-ref). **Actions upon Session Termination Indication**

   Whenever a RADIUS (or other AAA) authenticated session ends for any
   reason, an indication is provided. This indication MUST provide
   means of determining the SnmpSecurityModel, and an identifier for the
   transport session tied to the AAA authorization. The manner in which
   this occurs is implementation dependent.

[7.3.1](7.3.1-ref). **Deletion of Entries from vacmAaaSecurityToGroupTable**

   Entries in the vacmAaaSecurityToGroupTable MUST NOT persist across
   system reboots.

   When a session has been terminated, the vacmAaaSecurityToGroupTable
   is searched for a corresponding entry. A "matching" entry is any
   entry for which the SnmpSecurityModel and session ID match the
   information associated with the session termination indication. Any
   matching entries are deleted. It is possible that no entries will
   match; this is not an error, and no special processing is required in
   this case.

7.3.2. Deletion of Entries from vacmSecurityToGroupTable

   Whenever the last remaining row bearing a particular
   (vacmAaaSecurityModel, vacmAaaSecurityName) pair is deleted from the
   vacmAaaSecurityToGroupTable, the vacmSecurityToGroupTable is examined
   for a corresponding row. If one exists, and if its StorageType is
   "volatile" and its RowStatus is "active", that row MUST be deleted as
   well. The mechanism to accomplish this task is implementation
   dependent.

8. Definitions

SNMP-VACM-AAA-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-COMPLIANCE, OBJECT-GROUP   FROM SNMPv2-CONF
    MODULE-IDENTITY, OBJECT-TYPE,
    mib-2,
    Unsigned32   FROM SNMPv2-SMI
    SnmpAdminString,
    SnmpSecurityModel   FROM SNMP-FRAMEWORK-MIB;

vacmAaaMIB   MODULE-IDENTITY
    LAST-UPDATED "201012090000Z"   -- 9 December 2010
    ORGANIZATION "ISMS Working Group"
    CONTACT-INFO "WG-email: isms@ietf.org"

    DESCRIPTION "The management and local datastore information
                  definitions for the AAA-Enabled View-based Access
                  Control Model for SNMP.

                  Copyright (c) 2010 IETF Trust and the persons
                  identified as the document authors. All rights
                  reserved.

                  Redistribution and use in source and binary forms,
                  with or without modification, is permitted pursuant
                  to, and subject to the license terms contained in,
                  the Simplified BSD License set forth in Section
                  4.c of the IETF Trust's Legal Provisions Relating
                  to IETF Documents
                  (http://trustee.ietf.org/license-info).

                  This version of this MIB module is part of RFC 6065;
                  see the RFC itself for full legal notices."

    REVISION "201012090000Z"
    DESCRIPTION "Initial version, published as RFC 6065."

     ::= { mib-2 199 }

vacmAaaMIBObjects   OBJECT IDENTIFIER ::= { vacmAaaMIB 1 }

vacmAaaMIBConformance OBJECT IDENTIFIER ::= { vacmAaaMIB 2 }

vacmAaaSecurityToGroupTable OBJECT-TYPE
    SYNTAX   SEQUENCE OF VacmAaaSecurityToGroupEntry
    MAX-ACCESS   not-accessible
    STATUS   current
    DESCRIPTION "This table provides a listing of all currently active
                 sessions for which a mapping of the combination of
                 SnmpSecurityModel and securityName into the name of
                 a VACM group has been provided by an AAA service.
                 The group name (in VACM) in turn identifies an access
                 control policy to be used for the corresponding
                 principals."
    REFERENCE   "RFC 3411, Section 3.2.2, defines securityName."
    ::= { vacmAaaMIBObjects 1 }

vacmAaaSecurityToGroupEntry OBJECT-TYPE
    SYNTAX   VacmAaaSecurityToGroupEntry
    MAX-ACCESS   not-accessible
    STATUS   current
    DESCRIPTION "An entry in this table maps the combination of a
                 SnmpSecurityModel and securityName into the name
                 of a VACM group defining the access control policy
                 that is to govern a particular session.

                 Each entry corresponds to a session.

                 Entries do not persist across reboots.

                 An entry is created whenever an indication occurs
                 that a new session has been established that would
                 not have the same index values as an existing entry.

                 When a session is torn down, disconnected, timed out
                 (e.g., following the RADIUS Session-Timeout Attribute),
                 or otherwise terminated for any reason, the
                 corresponding vacmAaaSecurityToGroupEntry is deleted."
    REFERENCE   "RFC 3411, Section 3.2.2, defines securityName."
    INDEX   {
                   vacmAaaSecurityModel,
                   vacmAaaSecurityName,
                   vacmAaaSessionID
                  }
    ::= { vacmAaaSecurityToGroupTable 1 }

VacmAaaSecurityToGroupEntry ::= SEQUENCE
    {
        vacmAaaSecurityModel   SnmpSecurityModel,
        vacmAaaSecurityName   SnmpAdminString,
        vacmAaaSessionID   Unsigned32,
        vacmAaaGroupName   SnmpAdminString
    }

vacmAaaSecurityModel OBJECT-TYPE
    SYNTAX   SnmpSecurityModel(1..2147483647)
    MAX-ACCESS   not-accessible
    STATUS   current
    DESCRIPTION "The security model associated with the AAA binding
                 represented by this entry.

                 This object cannot take the 'any' (0) value."
    ::= { vacmAaaSecurityToGroupEntry 1 }

vacmAaaSecurityName OBJECT-TYPE
    SYNTAX   SnmpAdminString (SIZE(1..32))
    MAX-ACCESS   not-accessible
    STATUS   current
    DESCRIPTION "The securityName of the principal associated with the
                 AAA binding represented by this entry. In RADIUS
                 environments, this corresponds to the User-Name
                 Attribute."
    REFERENCE   "RFC 3411, Section 3.2.2, defines securityName, and
                 RFC 2865, Section 5.1, defines User-Name."
    ::= { vacmAaaSecurityToGroupEntry 2 }

vacmAaaSessionID OBJECT-TYPE
    SYNTAX   Unsigned32
    MAX-ACCESS   not-accessible
    STATUS   current
    DESCRIPTION "An implementation-dependent identifier of the session.

                 This value MUST be unique among all currently open
                 sessions of all of this SNMP engine's transport models.
                 The value has no particular significance other than to
                 distinguish sessions.

                 Implementations in which tmSessionID has a compatible
                 syntax and is unique across all transport models MAY
                 use that value."
    REFERENCE   "The Abstract Service Interface parameter tmSessionID
                 is defined in RFC 5590, Section 5.2.4."
    ::= { vacmAaaSecurityToGroupEntry 3 }

vacmAaaGroupName   OBJECT-TYPE
    SYNTAX   SnmpAdminString (SIZE(1..32))
    MAX-ACCESS   read-only
    STATUS   current
    DESCRIPTION "The name of the group to which this entry is to belong.
                In RADIUS environments, this comes from the RADIUS
                Management-Policy-Id Attribute.

                When the appropriate conditions are met,
                the value of this object is applied the vacmGroupName
                in the corresponding vacmSecurityToGroupEntry."
    REFERENCE   "RFC 3415"
    ::= { vacmAaaSecurityToGroupEntry 4 }

-- Conformance information **

vacmAaaMIBCompliances
                OBJECT IDENTIFIER ::= {vacmAaaMIBConformance 1}
vacmAaaMIBGroups
                OBJECT IDENTIFIER ::= {vacmAaaMIBConformance 2}

-- compliance statements

vacmAaaMIBBasicCompliance MODULE-COMPLIANCE
    STATUS   current
    DESCRIPTION "The compliance statement for SNMP engines implementing
                the AAA-Enabled View-based Access Control Model for
                SNMP."
    MODULE   -- this module
        MANDATORY-GROUPS { vacmAaaGroup }

    ::= { vacmAaaMIBCompliances 1 }

-- units of conformance

vacmAaaGroup OBJECT-GROUP
    OBJECTS {
            vacmAaaGroupName
          }
    STATUS   current
    DESCRIPTION "A collection of objects for supporting the use of AAA
                services to provide user-to-group mappings for VACM."
    ::= { vacmAaaMIBGroups 1 }

END

9. Security Considerations

   The algorithms in this memo make heuristic use of the StorageType of
   entries in the vacmSecurityToGroupTable to distinguish those
   provisioned by a security administrator (which would presumably not
   be configured as "volatile") from those dynamically generated. In
   making this distinction, it assumes that those entries explicitly
   provisioned by a security administrator and given a non-"volatile"
   status are not to be dynamically overridden. Furthermore, it assumes
   that any active entries with "volatile" status can be treated as
   dynamic, and deleted or updated as needed. Users of this memo need
   to be aware of this operational assumption, which, while reasonable,
   is not necessarily universally valid. For example, this situation
   could also occur if the SNMP security administrator had mistakenly
   created these non-volatile entries in error.

   The design of VACM ensures that if an unknown policy (group name) is
   used in the vacmSecurityToGroupTable, no access is granted. A
   consequence of this is that no matter what information is provided by
   the AAA server, no user can gain SNMP access rights not already
   granted to some group through the VACM configuration.

9.1. Principal Identity Naming

   In order to ensure that the access control policy ultimately applied
   as a result of the mechanisms described here is indeed the intended
   policy for a given principal using a particular security model, care
   needs to be applied in the mapping of the authenticated user
   (principal) identity to the securityName used to make the access
   control decision. Broadly speaking, there are two approaches to
   ensure consistency of identity:

   o Entries for the vacmSecurityToGroupTable corresponding to a given
      security model are created only through the operation of the
      procedures described in this memo. A consequence of this would be
      that all such entries would have been created using the RADIUS
      User-Name (or other AAA-authenticated identity) and RADIUS
      Management-Policy-Id Attribute (or equivalent).

   o Administrative policy allows a matching pre-configured entry to
      exist in the vacmSecurityToGroupTable, i.e., an entry with the
      corresponding vacmSecurityModel and with a vacmSecurityName
      matching the authenticated principal's RADIUS User-Name. In this
      case, administrative policy also needs to ensure consistency of
      identity between each authenticated principal's RADIUS User-Name
      and the administratively configured vacmSecurityName in the
      vacmSecurityToGroupTable row entries for that particular security
      model.

In the latter case, inconsistent re-use of the same name for
different entities or individuals (principals) can cause the
incorrect access control policy to be applied for the authenticated
principal, depending on whether the policy that is configured using
SNMP or the policy that is applied using the procedures of this memo
is the intended policy. This may result in greater or lesser access
rights than the administrative policy intended. Inadvertent
misidentification in such cases may be undetectable by the SNMP
engine or other software elements of the managed entity.

9.2. Management Information Considerations

There are no management objects defined in this MIB module that have
a MAX-ACCESS clause of read-write and/or read-create. So, if this
MIB module is implemented correctly, then there is no risk that an
intruder can alter or create any management objects of this MIB
module via direct SNMP SET operations.

Some of the readable objects in this MIB module (including some
objects with a MAX-ACCESS of not-accessible, whose values are exposed
as a result of access to indexed objects) may be considered sensitive
or vulnerable in some network environments. It is thus important to
control even GET and/or NOTIFY access to these objects and possibly
to even encrypt the values of these objects when sending them over
the network via SNMP. These are the tables and objects and their
sensitivity/vulnerability:

o vacmAaaSecurityToGroupTable - the entire table is potentially
   sensitive, since walking the table will reveal user names,
   security models in use, session identifiers, and group names;

o vacmAaaSecurityModel - though not-accessible, this is exposed as
   an index of vacmAaaGroupName;

o vacmAaaSecurityName - though not-accessible, this is exposed as an
   index of vacmAaaGroupName;

o vacmAaaSessionID - though not-accessible, this is exposed as an
   index of vacmAaaGroupName;

o vacmAaaGroupName - since this identifies a security policy and
   associates it with a particular user, this is potentially
   sensitive.

SNMP versions prior to SNMPv3 did not include adequate security.
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 module.

It is RECOMMENDED that implementers consider the security features as
provided by the SNMPv3 framework (see [\[RFC3410\], section 8](#)),
including full support for the SNMPv3 cryptographic mechanisms (for
authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT
RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to
enable cryptographic security. It is then a customer/operator
responsibility to ensure that the SNMP entity giving access to an
instance of this MIB module 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.

[10](#). IANA Considerations

The MIB module in this document uses the following IANA-assigned
OBJECT IDENTIFIER value recorded in the SMI Numbers registry:

```
   Descriptor        OBJECT IDENTIFIER value
   ----------        -----------------------
   vacmAaaMIB        { mib-2 199 }
```

[11](#). Contributors

The following participants from the ISMS working group contributed to
the development of this document:

o Andrew Donati

o David Harrington

o Jeffrey Hutzelman

o Juergen Schoenwaelder

o Tom Petch

o Wes Hardaker

During the IESG review, additional comments were received from:

o Adrian Farrel

o Amanda Baber

o Dan Romescanu

o David Kessens

o Francis Dupont

o Glenn Keeni

o Jari Arkko

o Joel Jaeggli

o Magnus Nystrom

o Mike Heard

o Robert Story

o Russ Housley

o Sean Turner

o Tim Polk

12. References

12.1. Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC2579]   McCloghrie, K., Ed., Perkins, D., Ed., and J.
            Schoenwaelder, Ed., "Textual Conventions for SMIv2",
            STD 58, RFC 2579, April 1999.

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

   [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson,
              "Remote Authentication Dial In User Service (RADIUS)",
              RFC 2865, June 2000.

   [RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An
              Architecture for Describing Simple Network Management
              Protocol (SNMP) Management Frameworks", STD 62, RFC 3411,
              December 2002.

   [RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based
              Access Control Model (VACM) for the Simple Network
              Management Protocol (SNMP)", STD 62, RFC 3415,
              December 2002.

   [RFC5590] Harrington, D. and J. Schoenwaelder, "Transport Subsystem
              for the Simple Network Management Protocol (SNMP)",
              RFC 5590, June 2009.

   [RFC5607] Nelson, D. and G. Weber, "Remote Authentication Dial-In
              User Service (RADIUS) Authorization for Network Access
              Server (NAS) Management", RFC 5607, July 2009.

   [RFC5608] Narayan, K. and D. Nelson, "Remote Authentication Dial-In
              User Service (RADIUS) Usage for Simple Network Management
              Protocol (SNMP) Transport Models", RFC 5608, August 2009.

12.2. Informative References

   [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart,
              "Introduction and Applicability Statements for Internet-
              Standard Management Framework", RFC 3410, December 2002.

   [RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure
              Shell Transport Model for the Simple Network Management
              Protocol (SNMP)", RFC 5592, June 2009.

Authors' Addresses

    Kaushik Narayan
    Cisco Systems, Inc.
    10 West Tasman Drive
    San Jose, CA 95134
    USA

    Phone: +1 408-526-8168
    EMail: kaushik_narayan@yahoo.com

    David Nelson
    Elbrys Networks, Inc.
    282 Corporate Drive, Unit #1,
    Portsmouth, NH 03801
    USA

    Phone: +1 603-570-2636
    EMail: d.b.nelson@comcast.net

    Randy Presuhn (editor)
    San Jose, CA 95120
    USA

    EMail: randy_presuhn@mindspring.com