Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 2, 2010

K. Narayan
Cisco Systems, Inc.
D. Nelson
Elbrys Networks, Inc.
R. Presuhn, Ed.
None

January 29, 2010

Extensions to View-based Access Control Model for use with RADIUS
draft-ietf-isms-radius-vacm-02.txt

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols. In particular, it describes a backward-compatible extension to the View-based Access Control Model (VACM) for SNMPv3 for use with RADIUS and other AAA services to provide authorization of MIB database access, and defines objects for managing this extension. This extension is intended to be used in conjunction with secure SNMP Transport Models that facilitate RADIUS authentication, such as the Secure Shell Transport Model.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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.

This Internet-Draft will expire on August 2, 2010.

Copyright Notice

Table of Contents

1. Introduction

1.1. General

This memo specifies the integration of several protocols to operationally simplify the administration of the access rights granted to users of network management data. In this environment:

- The View-Based Access Control Model (VACM) [RFC3415] provides a means to manage users' access rights to management information accessed using SNMP.
- The Simple Network Management Protocol version 3 (SNMPv3) provides message security services through the Security Subsystem.
- The Transport Subsystem for the Simple Network Management Protocol [RFC5590] defines a Transport Subsystem.
- The Transport Security Model for SNMP [RFC5591] defines a Transport Security Model.
- The Secure Shell Transport Model for SNMP [RFC5592] defines a Secure Shell Transport Model and Remote Authentication Dial-In User Service (RADIUS).
- RADIUS Usage for Simple Network Management Protocol (SNMP) Transport Models [RFC5608] defines a method for authenticating SNMPv3 users via RADIUS.

It is possible to authenticate SNMPv3 messages via a RADIUS when those messages are sent over the SSH transport. As originally envisioned, VACM authorizes a given SNMP transaction using on-device, pre-existing authorization configuration. In order to leverage a centralized RADIUS service to its full extent, the access control decision in the Access Control Subsystem needs to be able to make use of authorization information received from RADIUS as well. This document defines an extension to the View-based Access Control Model to obtain authorization information for an authenticated principal, from RADIUS.

Additional introductory material on the RADIUS operational model and RADIUS usage with SNMP may be found in Sections 1.3 and 1.5 of [RFC5608].

It is important to understand the SNMP architecture and the terminology of the architecture to understand where the Extended

View-based Access Control Model described in this memo fits into the architecture and how it interacts with other subsystems and models within the architecture. It is expected that reader will have also read and understood RFC3411 [RFC3411], RFC3412 [RFC3412], RFC3413 [RFC3413], RFC3415 [RFC3415]and RFC3418 [RFC3418]. As this document describes an extension to VACM, a thorough understanding of RFC3415 [RFC3415] is assumed.

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].

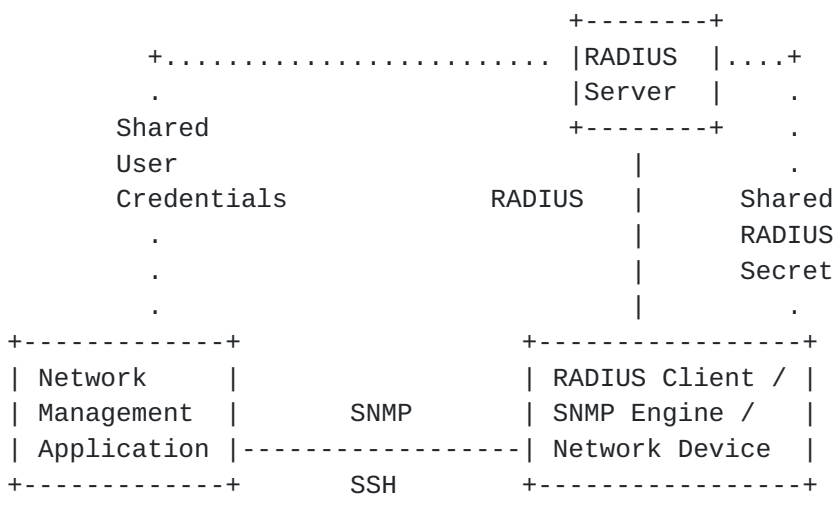
3. Conventions

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

4. Overview

4.1. System Block Diagram

A block diagram of the major system components referenced in this document may be useful to understanding the text that follows.



Block Diagram

This diagram illustrates that a network management application communicates with a network device, the managed entity, using SNMP over SSH. The network devices uses RADIUS to communicate with a RADIUS Server to authenticate the network management application (or the user whose credentials that application provides) and to obtain authorization information related to access via SNMP for purpose of device management. Other secure transport protocols might be used instead of SSH.

4.2. Using RADIUS with SNMP

There are two use cases for RADIUS support of management access via SNMP. These are (a) service authorization and (b) access control authorization. RADIUS almost always involves user authentication as prerequisite to authorization, and there is a user authentication phase for each of these two use cases. The first use case is discussed in detail in [RFC5608]. The second use case is the subject of this document. This document describes how RADIUS attributes and messages are applied to the specific application area of SNMP Access Control Models, and VACM in particular.

This document assumes that Extended VACM will be used in conjunction with an SNMP secure Transport Model and the SNMP Transport Security Model. The rationale for this assumption is as follows. The RFC 3411 SNMP architecture maintains strong modularity and separation of concerns, extending to separating user identity (authentication) from user database access rights (authorization). The former is the business of the Security Subsystem and the latter is the business of the Access Control Subsystem. RADIUS, on the other hand, allows for no such separation of authorization from authentication. In order to

use RADIUS with SNMP, binding of user authentication to user authorization must be achieved, without violating the modularity of the RFC 3411 SNMP architecture.

RADIUS does support a limited form of Authorize-Only operations. The RADIUS "Authorize Only" Service-Type Attribute can be specified in an Access-Request message, but only when accompanied by a RADIUS State Attribute, which contains an implementation specific "cookie" representing the successful outcome of a previous authentication transaction. For that reason, it is not possible to completely separate the use of RADIUS by the Access Control Subsystem from the use of RADIUS by other subsystems. This suggests that the most straightforward approach is to leverage the existing RADIUS usage, as documented in [RFC5608], and the tmStateReference cache, as documented in Section 5.2 of [RFC5590].

This document also assumes that the detailed access control rules are pre-configued in the NAS. Dynamic user authorization for MIB database access control, as defined herein, is limited to mapping the authenticated user to a pre-existing group, which in turn is mapped to the pre-existing rules. The operative use case assumption is that roles within an organization (i.e. groups and rules) change infrequently while the users assigned to those roles change much more frequently. It is the user to role mapping that is outsourced to the RADIUS server.

5. Structure of the MIB Module

5.1. Textual Conventions

This MIB module makes use of the RowStatus, StorageType, SnmpAdminString, and SnmpSecurityModel textual conventions.

5.2. The extVacmCounters Subtree

The extVacmCounters subtree contains all of this module's counters.

5.3. The Notifications Subtree

No notifications are defined in this MIB module

5.4. The Table Structures

6. Relationship to Other MIB Modules

6.1. Relationship to the VACM MIB

6.1.1. Extended VACM for RADIUS Authorization

This document will rely on implementation specific integration of the RADIUS client for user authentication and authorization. Further, it will rely on implementation specific caching of MIB database access policy information, in the form of the RADIUS Management-Policy-Id Attribute, such that it will be available to Extended VACM.

A NAS that is compliant to this specification, MUST treat any RADIUS Access-Accept message that provisions a specific policy for MIB database access control that cannot be provided as if an Access-Reject message had been received instead.

The RADIUS Management-Policy-Id Attribute MUST be used in an Access-Accept message to provision a user-specific access control policy for use in conjunction with Extended VACM. The syntax and semantics of the Management-Policy-Id attribute are described in Section 6.3 of [RFC5607].

The intended use of the content of the Management-Policy-Id attribute is to provision a mapping between the authenticated user, associated with the secure transport session, and an access control group pre-provisioned in the VACM MIB module. Details of this mapping are described in following sections.

6.1.2. VACM Extension for RADIUS Authorization

The extension to VACM [RFC3415] described in this document is a method for one or more of its MIB module objects to be dynamically provisioned based on information received from RADIUS, or some similar AAA service. This extension requires no changes to the Abstract Service Interface (ASI) for the Access Control Subsystem, nor any changes in the Elements of Procedure (EOP) for VACM. A new MIB module that augments the vacmSecurityToGroupTable is defined in this document, as well as supplemental EOP for Extended VACM to follow. It does require that a module of code somewhere in the NAS be able to write to the VACM MIB module and Extended VACM MIB Module, and that it reliably and consistently do so in immediate response to access control policy information received from RADIUS.

6.1.2.1. Dynamic Update of VACM and Extended VACM MIB Module Objects

The implementation-dependent interface between the RADIUS Client function and the SNMP Engine is responsible for updating the

vacmSecurityToGroupTable table within the VACM MIB Module [RFC3415] and the corresponding rows of the extVacmSecurityToGroupTable. Specifically, the RADIUS User-Name Attribute is used as the vacmSecurityName and the RADIUS Management-Policy-Id Attribute is used as the vacmGroupName. The vacmSecurityModel is the encoding for the Transport Security Model. The vacmSecurityToGroupStorageType should be (2) volatile.

In creating a row entry in the vacmSecurityToGroupTable, there are three cases to consider:

- No existing row has a matching vacmSecurityName.
- An existing row has a matching vacmSecurityName.
- No additional rows can be created, e.g. because of resource constraints, etc.

The second and third cases require special consideration. The second case may represent a conflict between dynamic access control authorization from RADIUS and local access control configuration by a security administrator, e.g. via remote or local SNMP MIB module updates. If one assumes that the security administrator intentionally configured a table entry for the "conflicting" vacmSecurityName, with full knowledge that it might over-ride dynamic authorization information from RADIUS, the right thing to do would be nothing. That is to say, do not update the table based on RADIUS authorization information. On the other hand, it is possible that the "name collision" is the result of a mistake, or the result of stale configuration information.

The behavior specified for Extended VACM is to make no update to the vacmSecurityToGroupTable, and to increment the extVacmSecurityNameConflict counter.

The third case is likely to be rare, and SHOULD result in a notification of some sort being logged for action by the system administrator.

It is expected that the value of the RADIUS Management-Policy-Id Attribute match an existing vacmGroupName that can be sucessfully used as an index to the vacmAccessTable. If no matching vacmGroupName exists, then the access control defaults to this will result in the default access rights of "no access", which is the desired result. The NAS should increment the extVacmMissingGroupName counter, for troubleshooting purposes, as this most likely indicates

an administrative misconfiguration.

In addition to creating a new row in the vacmSecurityToGroupTable, the NAS creates a corresponding new row in the extVacmSecurityToGroupTable, using the same values for index as were used to create the row in the vacmSecurityToGroupTable. The value of the extVacmRowCreatedBy object is set to RADIUS (1), and the value of extVacmRowLifetime is set to the value of the RADIUS Session-Timeout Attribute, if one was received by the RADIUS Client for this session, or to zero (0) otherwise.

6.1.2.2. Purging Volatile Entries in the Extended VACM MIB Module

When the secure transport session is torn down, disconnected or times out, any volatile table rows created in the vacmSecurityToGroup table by the Extended VACM function MUST be removed. The mechanism to accomplish this task is implementation specific.

6.1.3. Elements of Procedure for Extended VACM

This section describes the Elements of Procedure for Extended VACM. The function of the VACM extension is to manage the creation and deletion of rows in the vacmSecurityToGroupTable, based on the outcome of RADIUS authorization. All access control decision functions are taken by VACM, as defined in [RFC3415]. The EOP for VACM remains as listed in Section 3 of that document.

When a RADIUS (or other AAA service) authorizes SNMP data access control for a user-authenticated secure transport session, the NAS causes the RADIUS provisioning information to be made available to the Extended VACM facility, which populates the vacmSecurityToGroupTable, as follows:

1. If the the RADIUS Management-Policy-Id Attribute is not available, increment the extVacmNoPolicy counter. Do not create a table row.

2. If the the RADIUS Management-Policy-Id Attribute is available, and if no existing row has a vacmSecurityName matching the RADIUS User-Name Attribute, create a new row with the columns populated as follows:

   A. vacmSecurityModel = (x) secureTransportSecurityModel

   B. vacmSecurityName = RADIUS User-Name Attribute

   C. vacmGroupName = RADIUS Management-Policy-Id Attribute

D. vacmSecurityToGroupStorageType = volatile(2)

E. vacmSecurityToGroupStatus = createAndGo ???

F. extVacmRowCreatedBy = (1)

G. extVacmRowLifetime = RADIUS Session-Timeout Attribute | zero (0)

H. extVacmTransportSessionID = ID provided by the Secure Transport Model

3. If an existing table row has a matching vacmSecurityName, increment the extVacmSecurityNameConflict counter. Do not create a table row. If no additional table rows can be created, e.g. because of resource constraints, increment the extVacmResourceError counter.

When a RADIUS-authenticated secure transport session is disconnected by the remote peer, the NAS causes the Extended VACM to remove the corresponding table row from the vacmSecurityToGroupTable. The NAS provides an implementation dependent identifier of the session in question to Extended VACM.

1. Search for a row with a matching extVacmTransportSessionID.

2. If found, check to see that the extVacmRowCreateby value is (1) radius. If not, ignore the request.

3. If a table row exists with a matching value of extVACMTransportSessionID, that row is deleted.

6.2. MIB modules required for IMPORTS

The MIB module defined employs textual conventions from [RFC2579] and [RFC3411].

7. Definitions

```
SNMP-EXT-VACM-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-COMPLIANCE, OBJECT-GROUP       FROM SNMPv2-CONF
    MODULE-IDENTITY, OBJECT-TYPE,
```

```
    mib-2,
    Unsigned32,
    Counter32                              FROM SNMPv2-SMI
    RowStatus, StorageType                 FROM SNMPv2-TC
    SnmpAdminString,
    SnmpSecurityModel                      FROM SNMP-FRAMEWORK-MIB;

snmpExtVacmMIB    MODULE-IDENTITY
    LAST-UPDATED "200912020000Z"           -- 1 Dec. 2009, midnight
    ORGANIZATION "ISMS Working Group"
    CONTACT-INFO "WG-email:   isms@ietf.org"

    DESCRIPTION  "The management and local datstore information
                  definitions for the Extended View-based Access
                  Control Model for SNMP.

                  Copyright (C) The Internet Society (2009)."

    REVISION "200912020000Z"
    DESCRIPTION "Initial version,published as RFCZZZZ."
     ::= { mib-2 XXX }

extVacmMIBObjects   OBJECT IDENTIFIER ::= { snmpExtVacmMIB 1 }

extVacmMIBConformance OBJECT IDENTIFIER ::= {snmpExtVacmMIB 2 }

extVacmCounters     OBJECT IDENTIFIER ::= { extVacmMIBObjects 1 }

extVacmResourceError OBJECT-TYPE
       SYNTAX Counter32
       UNITS "lost rows"
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of VACM Security Name to Security
             Group table rows that could not be created by
             Extended VACM because of insufficient resources."
       ::= { extVacmCounters 1 }

extVacmNoPolicy OBJECT-TYPE
       SYNTAX Counter32
       UNITS "lost rows"
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of VACM Security Name to Security
             Group table rows that could not be created by
             Extended VACM because the AAA-provisioned
```

```
              group policy did not match an existing row in
              the VACM access table."
       ::= { extVacmCounters 2 }

extVacmSecurityNameConflict OBJECT-TYPE
       SYNTAX Counter32
       UNITS "lost rows"
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of VACM Security Name to Security
             Group table rows that could not be created by
             Extended VACM because the AAA-provisioned
             security name (user name) conflicted with an
             existing row in the table."
       ::= { extVacmCounters 3 }

extVacmSecurityToGroupTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF ExtVacmSecurityToGroupEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "This table maps a combination of securityModel and
                 securityName into a groupName which is used to define
                 an access control policy for a group of principals."
    ::= { extVacmMIBObjects 2 }

extVacmSecurityToGroupEntry OBJECT-TYPE
    SYNTAX       ExtVacmSecurityToGroupEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in this table maps the combination of a
                 securityModel and securityName into a groupName."
    INDEX       {
                  extVacmSecurityModel,
                  extVacmSecurityName
                }
    ::= { extVacmSecurityToGroupTable 1 }

ExtVacmSecurityToGroupEntry ::= SEQUENCE
    {
        extVacmSecurityModel           SnmpSecurityModel,
        extVacmSecurityName            SnmpAdminString,
        extVacmGroupName               SnmpAdminString,
        extVacmSecurityToGroupStorageType  StorageType,
        extVacmSecurityToGroupStatus   RowStatus,
        extVacmRowCreatedBy            INTEGER,
        extVacmRowLifetime             Unsigned32,
        extVacmTransportSessionID      Unsigned32
```

```
    }

extVacmSecurityModel OBJECT-TYPE
    SYNTAX       SnmpSecurityModel(1..2147483647)
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "The Security Model, by which the vacmSecurityName
                 referenced by this entry is provided.
                 Note, this object may not take the 'any' (0) value."
    ::= { extVacmSecurityToGroupEntry 1 }

extVacmSecurityName OBJECT-TYPE
    SYNTAX       SnmpAdminString (SIZE(1..32))
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "The securityName for the principal, represented in a
                 Security Model independent format, which is mapped by
                 this entry to a groupName."
    ::= { extVacmSecurityToGroupEntry 2 }

extVacmGroupName    OBJECT-TYPE
    SYNTAX       SnmpAdminString (SIZE(1..32))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "The name of the group to which this entry (e.g., the
                 combination of securityModel and securityName)
                 belongs.

                 This groupName is used as index into the
                 vacmAccessTable to select an access control policy.
                 A value in this table does not imply that an instance
                 with the value exists in table vacmAccesTable."
    ::= { extVacmSecurityToGroupEntry 3 }

extVacmSecurityToGroupStorageType OBJECT-TYPE
    SYNTAX       StorageType
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "The storage type for this conceptual row.
                 Conceptual rows having the value 'permanent' need not
                 allow write-access to any columnar objects in the row."
    DEFVAL      { nonVolatile }
    ::= { extVacmSecurityToGroupEntry 4 }

extVacmSecurityToGroupStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
```

```
    DESCRIPTION "The status of this conceptual row.

                 Until instances of all corresponding columns are
                 appropriately configured, the value of the
                 corresponding instance of the vacmSecurityToGroupStatus
                 column is 'notReady'.

                 In particular, a newly created row cannot be made
                 active until a value has been set for vacmGroupName.

                 The  RowStatus TC [RFC2579] requires that this
                 DESCRIPTION clause states under which circumstances
                 other objects in this row can be modified:

                 The value of this object has no effect on whether
                 other objects in this conceptual row can be modified."
    ::= { extVacmSecurityToGroupEntry 5 }

extVacmRowCreatedBy OBJECT-TYPE
    SYNTAX      INTEGER
                { radius (1), -- Row created by Extended VACM
                  other  (2)  -- ???
                }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "The source of the infromation in this row
                 is indicated by the value of this object.
                 In the case of VACM this column probably won't
                 exist."
    ::= { extVacmSecurityToGroupEntry 6 }

extVacmRowLifetime OBJECT-TYPE
    SYNTAX       Unsigned32
    UNITS        "seconds"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "The number of seconds remaining in this row's
                 lifetime.  Extended VACM SHOULD delete this
                 row when this value reaches zero."
    ::= { extVacmSecurityToGroupEntry 7 }

extVacmTransportSessionID OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "An identifier of the secure transport
                 model's session associated with this
                 authenticated user.  The identifier
```

```
                MUST be unique within the scope of the NAS.
                It's content is implementation dependant
                and it SHOULD be used merely as an index."
    ::= { extVacmSecurityToGroupEntry 8 }

-- Conformance information ****************************************

extVacmMIBCompliances
               OBJECT IDENTIFIER ::= {extVacmMIBConformance 1}
extVacmMIBGroups
               OBJECT IDENTIFIER ::= {extVacmMIBConformance 2}

-- compliance statements

extVacmMIBBasicCompliance MODULE-COMPLIANCE
    STATUS       current
    DESCRIPTION "The compliance statement for SNMP engines which
                 implement the Extensions to the View-based Access
                 Control Model for use with RADIUS.
                "
    MODULE    -- this module
        MANDATORY-GROUPS { extVacmGroup }

    ::= { extVacmMIBCompliances 1 }

-- units of conformance

extVacmGroup OBJECT-GROUP
    OBJECTS {
              extVacmResourceError,
              extVacmNoPolicy,
              extVacmSecurityNameConflict,
              extVacmGroupName,
              extVacmSecurityToGroupStorageType,
              extVacmSecurityToGroupStatus,
              extVacmRowCreatedBy,
              extVacmRowLifetime,
              extVacmTransportSessionID
            }
    STATUS       current
    DESCRIPTION "A collection of objects for supporting the use
                 of RADIUS to provide user / group mappings for VACM.
                "
    ::= { extVacmMIBGroups 1 }


END
```

8. Security Considerations

TODO

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) 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 TBD

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.

9. IANA Considerations

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

Descriptor	OBJECT IDENTIFIER value
snmpExtVacmMIB	{ mib-2 XXX }

Editor's Note (to be removed prior to publication): the IANA is

requested to assign a value for "XXX" under the 'mib-2' subtree and to record the assignment in the SMI Numbers registry. When the assignment has been made, the RFC Editor is asked to replace "XXX" (here and in the MIB module) with the assigned value and to remove this note.

10. Contributors

The following participants from the isms working group contributed to the devlopment of this document:

- David Harrington
- Juergen Schoenwaelder

11. References

11.1. 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.

[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.

[RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for the Simple Network Management Protocol (SNMP)", RFC 5591, 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.

11.2. 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.

[RFC3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[RFC3418] Presuhn, R., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, 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.

Appendix A. Open Issues

This section identifies questions and issues that have not been addressed in this version of this document. This section will probably be removed prior to publication, since there will be no questions left to address.

1. Is this document an amendment or update to RFC 3514? Or is it simply a standalone document that describes how to provision certain MIB Objects defined in RFC 3514, along with an extended

set of augmenting table columns?

2. Does this document need to make any reference to the Elements of Procedure in RFC 3514, or does is simply need its own Elements of Procedure for updating the group mapping table?

3. Dave Harrington had issued a summary email after IETF75 containing apparently contradictory statements about whether the additional columns should be in the *same* table that VACM uses or in another, separate table that augments the VACM table. Basically, we need some help in actually structuring the new MIB Module.

4. The Groups and Conformance sections of the MIB Module need to be checked and kept in alignment with the definitions.

5. Make sure that the new Elements of Procedure make sense and cover all the corner cases correctly.

6. for session tracking use tlstmSessionID?

7. Make boilerplate in MIB module agree with the legal trust incantation du jour.

8. Security considerations need to be filled in, specifically concerning trust relationships to RADIUS and the interaction with statically configured policy.

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)
None

Email: randy_presuhn@mindspring.com