Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 12, 2009

D. Harrington
Huawei Technologies (USA)

July 11, 2008

Transport Security Model for SNMP
draft-ietf-isms-transport-security-model-08

Status of This Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 January 12, 2009.

Abstract

This memo describes a Transport Security Model for the Simple Network Management Protocol.

This memo also defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP based internets. In particular it defines objects for monitoring and managing the Transport Security Model for SNMP.

Table of Contents

1. Introduction 3
  1.1. The Internet-Standard Management Framework 3
  1.2. Conventions 3
  1.3. Modularity 4
  1.4. Motivation 5
  1.5. Constraints 5
2. How the Transport Security Model Fits in the Architecture . . 5
  2.1. Security Capabilities of this Model 6
    2.1.1. Threats 6
    2.1.2. Security Levels 7
  2.2. No Sessions 7
  2.3. Coexistence 7
  2.4. Security Parameter Passing 8
  2.5. Notifications and Proxy 9
3. Cached Information and References 9
  3.1. tmStateReference 10
  3.2. securityStateReference 10
4. Processing an Outgoing Message 11
  4.1. Security Processing for an Outgoing Message 11
  4.2. Elements of Procedure for Outgoing Messages 12
5. Processing an Incoming SNMP Message 13
  5.1. Security Processing for an Incoming Message 13
  5.2. Elements of Procedure for Incoming Messages 13
6. MIB Module Overview 15
  6.1. Structure of the MIB Module 15
  6.2. The snmpTsmStats Subtree 15
  6.3. The snmpTsmLCD Subtree 15
  6.4. Relationship to Other MIB Modules 15
    6.4.1. Relationship to the SNMPv2-MIB 15
    6.4.2. Relationship to the SNMP-FRAMEWORK-MIB 15
    6.4.3. MIB Modules Required for IMPORTS 16
7. MIB module definition 16
8. Security Considerations 25
  8.1. MIB module security 25
9. IANA Considerations 26
10. References 27
  10.1. Normative References 27
  10.2. Informative References 28
Appendix A. Notification Tables Configuration 28
  A.1. Transport Security Model Processing for Notifications . . 30
Appendix B. Processing Differences between USM and Secure Transport 30
  B.1. USM and the RFC3411 Architecture 31
  B.2. Transport Subsystem and the RFC3411 Architecture 31
Appendix C. Open Issues 32
Appendix D. Change Log 32

1. Introduction

This memo describes a Transport Security Model for the Simple Network Management Protocol, for use with secure Transport Models in the Transport Subsystem [I-D.ietf-isms-tmsm].

This memo also defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP based internets. In particular it defines objects for monitoring and managing the Transport Security Model for SNMP.

It is important to understand the SNMP architecture and the terminology of the architecture to understand where the Transport Security Model described in this memo fits into the architecture and 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], and RFC3418 [RFC3418].

1.1. 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].

1.2. Conventions

For consistency with SNMP-related specifications, this document favors terminology as defined in STD62 rather than favoring terminology that is consistent with non-SNMP specifications that use different variations of the same terminology. This is consistent with the IESG decision to not require the SNMPv3 terminology be modified to match the usage of other non-SNMP specifications when SNMPv3 was advanced to Full Standard.

Authentication in this document typically refers to the English meaning of "serving to prove the authenticity of" the message, not data source authentication or peer identity authentication.

The terms "manager" and "agent" are not used in this document, because in the RFC 3411 architecture, all SNMP entities have the capability of acting as either manager or agent or both depending on the SNMP applications included in the engine. Where distinction is required, the application names of Command Generator, Command Responder, Notification Originator, Notification Receiver, and Proxy Forwarder are used. See "SNMP Applications" [RFC3413] for further information.

While security protocols frequently refer to a user, the terminology used in RFC3411 [RFC3411] and in this memo is "principal". A principal is the "who" on whose behalf services are provided or processing takes place. A principal can be, among other things, an individual acting in a particular role; a set of individuals, with each acting in a particular role; an application or a set of applications, or a combination of these within an administrative domain.

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 [RFC2119].

1.3. Modularity

The reader is expected to have read and understood the description of the SNMP architecture, as defined in [RFC3411], and the architecture extension specified in "Transport Subsystem for the Simple Network Management Protocol" [I-D.ietf-isms-tmsm], which enables the use of external "lower layer transport" protocols to provide message security, tied into the SNMP architecture through the Transport Subsystem. The Transport Security Model is designed to work with such lower-layer secure Transport Models.

In keeping with the RFC 3411 design decisions to use self-contained documents, this memo includes the elements of procedure plus associated MIB objects which are needed for processing the Transport Security Model for SNMP. These MIB objects SHOULD NOT be referenced in other documents. This allows the Transport Security Model to be designed and documented as independent and self-contained, having no direct impact on other modules, and allowing this module to be upgraded and supplemented as the need arises, and to move along the standards track on different time-lines from other modules.

This modularity of specification is not meant to be interpreted as imposing any specific requirements on implementation.

1.4. Motivation

This memo describes a Security Model to make use of Transport Models that use lower layer secure transports and existing and commonly deployed security infrastructures. This Security Model is designed to meet the security and operational needs of network administrators, maximize usability in operational environments to achieve high deployment success and at the same time minimize implementation and deployment costs to minimize the time until deployment is possible.

1.5. Constraints

The design of this SNMP Security Model is also influenced by the following constraints:

1. In times of network stress, the security protocol and its underlying security mechanisms SHOULD NOT depend solely upon the ready availability of other network services (e.g., Network Time Protocol (NTP) or Authentication, Authorization, and Accounting (AAA) protocols).

2. When the network is not under stress, the Security Model and its underlying security mechanisms MAY depend upon the ready availability of other network services.

3. It may not be possible for the Security Model to determine when the network is under stress.

4. A Security Model should require no changes to the SNMP architecture.

5. A Security Model should require no changes to the underlying security protocol.

2. How the Transport Security Model Fits in the Architecture

The Transport Security Model is designed to fit into the RFC3411 architecture as a Security Model in the Security Subsystem, and to utilize the services of a secure Transport Model.

A cache, referenced by tmStateReference, is used to pass information between the Transport Security Model and a Transport Model, and vice versa. If the Transport Security Model is used with an insecure Transport Model, then the cache will not exist or not be populated with security parameters, which will cause the Transport Security Model to return an error (see section 5.2) If another Security Model (eg Community-based Security Model) is used with a secure Transport Model, then the cache may be populated but the other Security Model

may be unaware of the cache and ignore its contents (eg deriving the securityName from the Community name in the message instead of deriving it from the tmSecurityName in the tmStateReference cache).

For incoming messages, a secure Transport Model creates a tmStateReference cache including a tmTransport, tmAddress, tmSecurityName and a tmTransportSecurityLevel, and it MAY include transport-specific information. The Transport Security Model will determine the security-model-independent securityName and securityLevel, and will verify that tmTransportSecurityLevel is at least as strong as the requested securityLevel. As with all security models, the securityName represents the principal on whose behalf a received SNMP message claims to have been generated. It is not possible to assure the specific principal that originated a received SNMP message; rather, it is the principal on whose behalf the message was originated that is authenticated.

For outgoing messages, the Transport Security Model creates a cache containing the transportDomain, transportAddress, and a tmSecurityName and tmRequestedSecurityLevel and passes the tmStateReference cache to the specified Transport Model.

To maintain the RFC3411 modularity, the Transport Model does not know which securityModel will be used for an incoming message; the Message Processing Model will determine the securityModel to be used, in a Message Processing Model dependent manner.

2.1. Security Capabilities of this Model

2.1.1. Threats

The Transport Security Model, when used with suitable secure Transport Models, provides protection against the threats identified by the RFC 3411 architecture [RFC3411].

Which threats are addressed depends on the Transport Model. The Transport Security Model does not address any threats itself, but delegates that responsibility to a secure Transport Model.

The Transport Security Model is called a Security Model to be compatible with the RFC3411 architecture. However, this Security Model does not provide security mechanisms such as authentication and encryption itself, so it SHOULD always be used with a Transport Model that provides appropriate security.

2.1.2. Security Levels

The RFC 3411 architecture recognizes three levels of security:

- without authentication and without privacy (noAuthNoPriv)
- with authentication but without privacy (authNoPriv)
- with authentication and with privacy (authPriv)

The model-independent securityLevel parameter is used to request specific levels of security for outgoing messages, and to assert that specific levels of security were applied during the transport and processing of incoming messages.

The transport layer algorithms used to provide security SHOULD NOT be exposed to the Transport Security Model, as the Transport Security Model has no mechanisms by which it can test whether an assertion made by a Transport Model is accurate.

The Transport Security Model trusts that the underlying secure transport connection has been properly configured to support security characteristics at least as strong as reported in tmTransportSecurityLevel.

2.2. No Sessions

The Transport Security Model will associate state regarding each message and each known remote engine with a combination of transportDomain, transportAddress, securityName, securityModel, and securityLevel.

The Transport Security Model does not recognize sessions of any kind, although they may be supported by a transport model.

2.3. Coexistence

There are two primary factors which determine whether Security Models can coexist. First, there must be a mechanism to select different Security Models at run-time. Second, the processing of one Security Model should not impact the processing of another Security Model.

In the RFC3411 architecture, a Message Processing Model determines which Security Model should be called. As of this writing, IANA has registered four Message Processing Models (SNMPv1, SNMPv2c, SNMPv2u/ SNMPv2*, and SNMPv3) and three other Security Models (SNMPv1, SNMPv2c, and the User-based Security Model).

The SNMPv1 and SNMPv2c message processing described in RFC3584 (BCP 74) [RFC3584] always selects the SNMPv1(1) Security Model for an SNMPv1 message, or the SNMPv2c(2) Security Model for an SNMPv2c message. Since there is no field in the message format that permits specifying a Security Model, RFC3584 message processing does not permit the selection of Security Models other than SNMPv1 or SNMPv2. Therefore, SNMPv1 or SNMPv2c messages that go through the SNMPv1 or SNMPv2 Message Processing Models **as defined in RFC3584** cannot use the Transport Security Model. (This does not mean an SNMPv1 or SNMPv2 message cannot use a secure transport model, only that the RFC3584 Message Processing Model will not invoke this security model.)

The SNMPv2u/SNMPv2* Message Processing Model is a historic artifact for which there is no existing IETF specification.

The SNMPv3 message processing defined in RFC3412 [RFC3412], extracts the securityModel from the msgSecurityModel field of an incoming SNMPv3Message. When the extracted value of msgSecurityModel is transportSecurityModel(YY), security processing is directed to the Transport Security Model. For an outgoing message to be secured using the Transport Security Model, msgSecurityModel should be set to transportSecurityModel(YY).

[-- NOTE to RFC editor: replace YY with actual IANA-assigned number, and remove this note.]

The Transport Security Model uses its own MIB module for processing to maintain independence from other Security Models. This allows the Transport Security Model to coexist with other Security Models, such as the User-based Security Model.

Note that the Transport Security Model may work with multiple Transport Models, but the isAccessAllowed() application service interfaces (ASI) only accepts a value for the Security Model, not for Transport Models. As a result, it is not possible to have different access control rules for different Transport Models that use the Transport Security Model.

The MIB module defined in this memo allows an administrator to configure the Transport Security Model to disable support for specific transport models.

2.4. Security Parameter Passing

For outgoing messages, the Transport Security Model uses parameters provided by the SNMP application to lookup or create an entry in the SNMP-TSM-MIB. From such an entry, the Transport Security Model

creates a tmStateReference. The wholeMsg and the tmStateReference are passed to the appropriate Transport Model through a series of ASIs, as described in "Transport Subsystem for the Simple Network Management Protocol" [I-D.ietf-isms-tmsm].

For incoming messages, a transport model accepts messages from the lower layer transport, and records the transport-related information and security-related information, including a human-readable name that represents the transport-authenticated identity, and a securityLevel that represents the security features provided during transport, in an implementation-dependent manner. From this information, the transport model creates a tmStateReference to pass to whichever security model is selected by the Message Processing Model. The wholeMsg and the tmStateReference are passed to the appropriate Security Model through a series of ASIs, as described in "Transport Subsystem for the Simple Network Management Protocol" [I-D.ietf-isms-tmsm].

2.5. Notifications and Proxy

The SNMP-TARGET-MIB module [RFC3413] contains objects for defining management targets, including transportDomain, transportAddress, securityName, securityModel, and securityLevel parameters, for applications such as notifications and proxy. Transport type and address are configured in the snmpTargetAddrTable, and the securityModel, securityName, and securityLevel parameters are configured in the snmpTargetParamsTable.

The default approach is for an administrator to statically configure this information to identify the targets authorized to receive notifications or perform proxy.

These parameters are passed to the security model using the appropriate ASIs. The Transport Security Model will use the parameters to determine how to create the appropriate tmStateReference for the selected transport model.

3. Cached Information and References

The RFC3411 architecture uses caches to store dynamic model-specific information, and uses references in the ASIs to indicate in a model-independent manner which cached information must flow between subsystems.

There are two levels of state that may need to be maintained: the security state in a request-response pair, and potentially long-term state relating to transport and security. This document describes caches, and differentiates the tmStateReference from the

securityStateReference, but how this is represented internally is an implementation decision.

As a general rule, if state information is available when a message being processed gets discarded, the state related to that message should also be discarded, and if state information is available when a relationship between engines is severed, such as the closing of a transport connection, the state information for that relationship might also be discarded.

3.1. tmStateReference

For each transport model, model- and mechanism-specific parameters for the transport security need to be stored in a local configuration datastore. Since the contents of this datastore are meaningful only within an implementation, and not on-the-wire, the format of this storage is implementation-specific.

To enable a security model to correlate the identity used by specific transport-model and the model-independent identity referenced by applications, a mapping is provided in the MIB module defined in this memo. A human-readable string representing the transport-specific identity is passed in the tmStateReference between a transport model and a security model.

For security reasons, the Transport Security Model REQUIRES that the security parameters used for a response are the same as those used for the corresponding request, and passes a tmSameSecurity parameter in the tmStateReference cache for outgoing messages to indicate that the same security MUST be used for the outgoing response as was used for the corresponding incoming request. It is transport-model-dependent and implementation-dependent how this is ensured at the transport layer.

3.2. securityStateReference

The securityStateReference parameter is defined in RFC3411. Its primary purpose is to provide a mapping between a request and the corresponding response. A sample model-specific cache can be found in RFC3414 [RFC3414].

Transport models do not have access to the securityStateReference. For the Transport Security Model, it is important to ensure that the security parameters used for a request match those used for the corresponding response. The Transport Security Model will conceptually add the tmStateReference to the securityStateReference cache, so the transport model can map transport-specific security parameters for a request to its corresponding response. How the

tmStateReference is added to the securityStateReference is implementation-specific.

4. Processing an Outgoing Message

An error indication may return an OID and value for an incremented counter and a value for securityLevel, and values for contextEngineID and contextName for the counter, and the securityStateReference if the information is available at the point where the error is detected.

4.1. Security Processing for an Outgoing Message

This section describes the procedure followed by the Transport Security Model.

The parameters needed for generating a message are supplied to the Security Model by the Message Processing Model via the generateRequestMsg() or the generateResponseMsg() ASI. The Transport Subsystem architectural extension has added the transportDomain, transportAddress, and tmStateReference parameters to the original RFC3411 ASIs.

```
 statusInformation =                -- success or errorIndication
       generateRequestMsg(
       IN   messageProcessingModel  -- typically, SNMP version
       IN   globalData              -- message header, admin data
       IN   maxMessageSize          -- of the sending SNMP entity
       IN   transportDomain         -- (NEW) specified by application
       IN   transportAddress        -- (NEW) specified by application
       IN   securityModel           -- for the outgoing message
       IN   securityEngineID        -- authoritative SNMP entity
       IN   securityName            -- on behalf of this principal
       IN   securityLevel           -- Level of Security requested
       IN   scopedPDU               -- message (plaintext) payload
       OUT  securityParameters      -- filled in by Security Module
       OUT  wholeMsg                -- complete generated message
       OUT  wholeMsgLength          -- length of generated message
       OUT  tmStateReference        -- (NEW)  transport info
            )
```

```
statusInformation = -- success or errorIndication
        generateResponseMsg(
        IN   messageProcessingModel  -- typically, SNMP version
        IN   globalData              -- message header, admin data
        IN   maxMessageSize          -- of the sending SNMP entity
        IN   transportDomain         -- (NEW) specified by application
        IN   transportAddress        -- (NEW) specified by application
        IN   securityModel           -- for the outgoing message
        IN   securityEngineID        -- authoritative SNMP entity
        IN   securityName            -- on behalf of this principal
        IN   securityLevel           -- Level of Security requested
        IN   scopedPDU               -- message (plaintext) payload
        IN   securityStateReference  -- reference to security state
                                     -- information from original
                                     -- request
        OUT  securityParameters      -- filled in by Security Module
        OUT  wholeMsg                -- complete generated message
        OUT  wholeMsgLength          -- length of generated message
        OUT  tmStateReference        -- (NEW) transport info
             )
```

4.2. Elements of Procedure for Outgoing Messages

1) If there is a securityStateReference, then this is a response message. Extract transportDomain, transportAddress, securityName, securityLevel, securityModel, and tmStateReference from the securityStateReference cache. Set the tmRequestedSecurityLevel to the value of the extracted securityLevel. The cachedSecurityData for this message can now be discarded. Set the tmSameSecurity parameter in the tmStateReference cache to true.

2) If there is no securityStateReference, lookup the transportDomain in the snmpTsmLCDTransformTable. If there is no entry in snmpTsmLCDTransformTable corresponding to the specified transportDomain, or the corresponding value of snmpTsmLCDPolicy is set to disable, then the snmpTsmInvalidDomain counter is incremented, an error indication is returned to the calling module, and Security Model processing stops for this message.

3) If there is no securityStateReference, use the provided parameters to lookup or create an associated entry in the snmpTsmLCDTable. Create a tmStateReference cache with tmSecurityName set to the value of securityName, tmRequestedSecurityLevel set to the value of securityLevel, tmSameSecurity set to false, and tmTransportIdentity set to the value of snmpTsmLCDTmSecurityName.

4) Fill in the securityParameters with a zero-length OCTET STRING ('0400').

5) Combine the message parts into a wholeMsg and calculate wholeMsgLength.

6) The wholeMsg, wholeMsgLength, securityParameters and tmStateReference are returned to the calling Message Processing Model with the statusInformation set to success.

5. Processing an Incoming SNMP Message

An error indication may return an OID and value for an incremented counter and a value for securityLevel, and values for contextEngineID and contextName for the counter, and the securityStateReference if the information is available at the point where the error is detected.

5.1. Security Processing for an Incoming Message

This section describes the procedure followed by the Transport Security Model whenever it receives an incoming message from a Message Processing Model. The ASI from a Message Processing Model to the Security Subsystem for a received message is:

```
statusInformation =  -- errorIndication or success
                         -- error counter OID/value if error
processIncomingMsg(
IN   messageProcessingModel    -- typically, SNMP version
IN   maxMessageSize            -- from the received message
IN   securityParameters        -- from the received message
IN   securityModel             -- from the received message
IN   securityLevel             -- from the received message
IN   wholeMsg                  -- as received on the wire
IN   wholeMsgLength            -- length as received on the wire
IN   tmStateReference          -- (NEW) from the Transport Model
OUT  securityEngineID          -- authoritative SNMP entity
OUT  securityName              -- identification of the principal
OUT  scopedPDU,                -- message (plaintext) payload
OUT  maxSizeResponseScopedPDU  -- maximum size sender can handle
OUT  securityStateReference    -- reference to security state
 )                           -- information, needed for response
```

5.2. Elements of Procedure for Incoming Messages

1) Set the securityEngineID to the local snmpEngineID.

2) If tmStateReference does not refer to a cache containing values for tmSecurityName and tmTransportSecurityLevel, then the snmpTsmInvalidCaches counter is incremented, an error indication is returned to the calling module, and Security Model processing stops

for this message.

3) If there is no entry in snmpTsmLCDTransformTable corresponding to the domain specified in tmTransportDomain, or the corresponding value of snmpTsmLCDPolicy is set to disable, then the snmpTsmInvalidDomain counter is incremented, an error indication together with the OID and value of the incremented counter is returned to the calling module, and Transport Security Model processing stops for this message.

4) Set securityName to the value of tmSecurityName from the cache referenced by tmStateReference.

5) Compare the value of tmTransportSecurityLevel in the tmStateReference cache to the value of the securityLevel parameter passed in the processIncomingMsg ASI. If securityLevel specifies privacy (Priv), and tmTransportSecurityLevel specifies no privacy (noPriv), or securityLevel specifies authentication (auth) and tmTransportSecurityLevel specifies no authentication (noAuth) was provided by the Transport Model, then the snmpTsmInadequateSecurityLevels counter is incremented, and an error indication (unsupportedSecurityLevel) together with the OID and value of the incremented counter is returned to the calling module. Transport Security Model processing stops for this message.

6)The security data is cached as cachedSecurityData, so that a possible response to this message will use the same security parameters. Then securityStateReference is set for subsequent reference to this cached data. For Transport Security Model, the securityStateReference includes a reference to the tmStateReference cache.

7) The scopedPDU component is extracted from the wholeMsg.

8) The maxSizeResponseScopedPDU is calculated. This is the maximum size allowed for a scopedPDU for a possible Response message.

9) Using the values of tmTransportDomain, tmTransportAddress, tmSecurityName, and tmTransportSecurityLevel, determine if a corresponding entry exists in the snmpTsmLCDTable. If not, create an entry. If the snmpTsmLCDTransformPolicy associated with the transportDomain is default, set the snmpTsmLCDTmSecurityName to the same value as snmpTsmLCDSecurityName. If the snmpTsmLCDTransformPolicy associated with the transportDomain is private, set the snmpTsmLCDTmSecurityName to the value provided by the private algorithm.

10) The statusInformation is set to success and a return is made to the calling module passing back the OUT parameters as specified in

the processIncomingMsg ASI.

6. MIB Module Overview

This MIB module provides management of the Transport Security Model. It defines some needed textual conventions, some statistics, and an LCD for use by the Transport Security Model.

6.1. Structure of the MIB Module

Objects in this MIB module are arranged into subtrees. Each subtree is organized as a set of related objects. The overall structure and assignment of objects to their subtrees, and the intended purpose of each subtree, is shown below.

6.2. The snmpTsmStats Subtree

This subtree contains counters specific to the Transport Security Model, that provide information for identifying fault conditions.

6.3. The snmpTsmLCD Subtree

This subtree contains transform policies and mappings between the model-independent parameters used by snmp applications, and the model-specific parameters used by transport models.

6.4. Relationship to Other MIB Modules

Some management objects defined in other MIB modules are applicable to an entity implementing the Transport Security Model. In particular, it is assumed that an entity implementing the Transport Security Model will implement the SNMPv2-MIB [RFC3418] and the SNMP-FRAMEWORK-MIB [RFC3411].

6.4.1. Relationship to the SNMPv2-MIB

The 'system' group in the SNMPv2-MIB [RFC3418] is defined as being mandatory for all systems, and the objects apply to the entity as a whole. The 'system' group provides identification of the management entity and certain other system-wide data. The snmpInASNParseErrs counter is incremented during the elements of procedure. The SNMP-TSM-MIB does not duplicate those objects.

6.4.2. Relationship to the SNMP-FRAMEWORK-MIB

The SNMP-FRAMEWORK-MIB provides definitions for the concepts of SnmpEngineID, enumeration of Message Processing Models, Security Models and Security Levels, and object definitions for snmpEngineID

These are important for implementing the Transport Security Model, but are not needed to implement the SNMP-TSM-MIB.

6.4.3. MIB Modules Required for IMPORTS

The following MIB module imports items from [RFC2578], [RFC2579], [RFC2580], [RFC3411], and [RFC3419].

7. MIB module definition

```
SNMP-TSM-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE,
    mib-2, Counter32
      FROM SNMPv2-SMI
    MODULE-COMPLIANCE, OBJECT-GROUP
      FROM SNMPv2-CONF
    TestAndIncr,
    RowStatus, StorageType
       FROM SNMPv2-TC
    SnmpAdminString, SnmpSecurityLevel
       FROM SNMP-FRAMEWORK-MIB
    TransportDomain, TransportAddress
      FROM TRANSPORT-ADDRESS-MIB
    ;

snmpTsmMIB MODULE-IDENTITY
    LAST-UPDATED "200807100000Z"
    ORGANIZATION "ISMS Working Group"
    CONTACT-INFO "WG-EMail:   isms@lists.ietf.org
                  Subscribe:  isms-request@lists.ietf.org

               Chairs:
                 Juergen Quittek
                 NEC Europe Ltd.
                 Network Laboratories
                 Kurfuersten-Anlage 36
                 69115 Heidelberg
                 Germany
                 +49 6221 90511-15
                  quittek@netlab.nec.de

                  Juergen Schoenwaelder
                  Jacobs University Bremen
                  Campus Ring 1
                  28725 Bremen
```

```
                  Germany
                  +49 421 200-3587
                  j.schoenwaelder@iu-bremen.de

               Editor:
                  David Harrington
                  Huawei Technologies USA
                  1700 Alma Dr.
                  Plano TX 75075
                  USA
                  +1 603-436-8634
                  ietfdbh@comcast.net
                    "
       DESCRIPTION  "The Transport Security Model MIB

                     In keeping with the RFC 3411 design decisions
                     to use self-contained documents, the RFC which
                     contains the definition of this MIB module also
                     includes the elements of procedure which are
                     needed for processing the Transport Security
                     Model for SNMP. These MIB objects
                     SHOULD NOT be modified via other subsystems
                     or models defined in other document..
                     This allows the Transport Security Model
                     for SNMP to be designed and documented as
                     independent and self- contained, having no
                     direct impact on other modules, and this
                     allows this module to be upgraded and
                     supplemented as the need arises, and to
                     move along the standards track on different
                     time-lines from other modules.

                     Copyright (C) The IETF Trust (2008). This
                     version of this MIB module is part of RFC XXXX;
                     see the RFC itself for full legal notices.
-- NOTE to RFC editor: replace XXXX with actual RFC number
--                     for this document and remove this note
                    "

       REVISION     "200807100000Z"
       DESCRIPTION  "The initial version, published in RFC XXXX.
-- NOTE to RFC editor: replace XXXX with actual RFC number
--                     for this document and remove this note
                    "

    ::= { mib-2 xxxx }
-- RFC Ed.: replace xxxx with IANA-assigned number and
--          remove this note
```

```
-- ---------------------------------------------------------- --
-- subtrees in the SNMP-TSM-MIB
-- ---------------------------------------------------------- --

snmpTsmNotifications OBJECT IDENTIFIER ::= { snmpTsmMIB 0 }
snmpTsmMIBObjects       OBJECT IDENTIFIER ::= { snmpTsmMIB 1 }
snmpTsmConformance   OBJECT IDENTIFIER ::= { snmpTsmMIB 2 }

-- -------------------------------------------------------------
-- Objects
-- -------------------------------------------------------------

-- Statistics for the Transport Security Model


snmpTsmStats         OBJECT IDENTIFIER ::= { snmpTsmMIBObjects 1 }

snmpTsmInvalidCaches OBJECT-TYPE
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "The number of messages dropped because the
                 tmStateReference referred to an invalid cache.
                "
    ::= { snmpTsmStats 1 }

snmpTsmInadequateSecurityLevels OBJECT-TYPE
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "The number of incoming messages dropped because
               the securityLevel asserted by the transport model was
               less than the securityLevel requested by the
               application.
                "
    ::= { snmpTsmStats 2 }

snmpTsmInvalidDomains OBJECT-TYPE
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "The number of messages dropped because the
                 specified transport domain is not supported or is
                 disabled.
                "
    ::= { snmpTsmStats 3 }

-- The snmpTsmLCD Group ************************************************
```

```
snmpTsmLCD          OBJECT IDENTIFIER ::= { snmpTsmMIBObjects 2 }

snmpTsmLCDSpinLock  OBJECT-TYPE
    SYNTAX       TestAndIncr
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION "An advisory lock used to allow several cooperating
                 Command Generator Applications to coordinate their
                 use of facilities to alter the snmpTsmLCDTable.
                "
    ::= { snmpTsmLCD 1 }

-- The table of domains for the Transport Security Model

snmpTsmLCDDomainTable     OBJECT-TYPE
    SYNTAX       SEQUENCE OF SnmpTsmLCDDomainEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "The table of transform policies.

               This table is automatically populated by the snmp
               engine, creating a conceptual row for each transport
               model supported by the engine.
               "
    ::= { snmpTsmLCD 2 }

snmpTsmLCDTransformEntry     OBJECT-TYPE
    SYNTAX       SnmpTsmLCDTransformEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Each entry specifies a transform policy for
                  automatically converting between
                  snmpTsmLCDTmSecurityNames and
                  snmpTsmLCDSecurityNames. These policies are
                 meant to be administratively assigned. In the absence
                 of an assigned policy, the default transform will be
                 used.

                 The  Transport Security Model uses the TransportDomain
                 index to identify a transport model. The Policy object
                 specifies which policy should be applied to the
                 transforms related to the corresponding transport
                 model.
                "
    INDEX       { snmpTsmLCDTransformTransportDomain
                }
    ::= { snmpTsmLCDTransformTable 1 }
```

```
SnmpTsmLCDTransformEntry ::= SEQUENCE
    {
        snmpTsmLCDTransformTransportDomain TransportDomain,
        snmpTsmLCDTransformPolicy             INTEGER
    }

   snmpTsmLCDTransformTransportDomain OBJECT-TYPE
       SYNTAX      TransportDomain
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "This object indicates the transport type of the address
            which the Transport Security Model uses to select a
            transport model. Thus, this domain is used to indicate
            the policy to be used with different transport models."
       ::= { snmpTsmLCDTransformEntry 1 }

 snmpTsmLCDTransformPolicy OBJECT-TYPE
    SYNTAX       INTEGER { default(1),
                           private(2),
                           disable(3)
                         }

       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
           "The policy that should be used to perform transforms
           between the transport model specific identity and the
           transport model independent securityName.

           default (1) - for incoming messages, the value passed in
           the tmSecurityName field of tmStateReference is assigned
           to both snmpTsmLCDSecurityName and snmpTsmLCDTmSecurityName.
           For outgoing messages, the value passed in securityName
           is assigned to both snmpTsmLCDSecurityName and
           snmpTsmLCDTmSecurityName.

            private (2) - use an implementation-specific mapping
            algorithm for the transform. If the algorithm does not yield
            a mapping, no entry should be created for the identity in
            the snmpTsmLCDTable. It is implementation-dependent
            whether a private algorithm is supported.

           disable (3) - do not allow a specific transport model to be
           used.
            "
        DEFVAL  { default }
       ::= { snmpTsmLCDTransformEntry 2 }
```

```
-- The table of users for the Transport Security Model
-- This table can support users of multiple transport models

snmpTsmLCDTable     OBJECT-TYPE
    SYNTAX       SEQUENCE OF SnmpTsmLCDEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "The table of users configured in the SNMP engine's
                 Local Configuration Datastore (LCD).

                 Rows in this table can be instantiated when an
                 authenticated identity is passed to the Transport
                 Security Model by a transport model, and they can be
                 instantiated by a command generator.

                 To instantiate a new row in this table, the
                 snmpTsmLCDSpinLock should be used to prevent conflicts.

                   1)  GET(snmpTsmLCDSpinLock.0) and save in sValue.

                   2)  SET(snmpTsmLCDSpinLock.0=sValue,
                           snmpTsmLCDTransportDomain=(desired value),
                           snmpTsmLCDTransportAddress=(desired value),
                           snmpTsmLCDSecurityName=(desired value),
                           snmpTsmLCDSecurityLevel=(desired value),
                           snmpTsmLCDTmSecurityName=(desired value),
                           snmpTsmLCDStorageType=(desired value),
                           snmpTsmLCDStatus=createAndGo)
                "
    ::= { snmpTsmLCD 3 }

snmpTsmLCDEntry     OBJECT-TYPE
    SYNTAX       SnmpTsmLCDEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "A user configured in the Local
                 Configuration Datastore (LCD) for the Transport
                 Security Model.

                 To maintain modularity of design, and to avoid
                 side-effects, only the Transport Security Model
                 (or a SET operation) should modify this table.
                 In particular, transport models should not
                 directly manipulate values in this table.
                "
    INDEX       { snmpTsmLCDTransportDomain,
                          snmpTsmLCDTransportAddress,
                          snmpTsmLCDSecurityName,
```

```
                          snmpTsmLCDSecurityLevel
                }
    ::= { snmpTsmLCDTable 1 }

SnmpTsmLCDEntry ::= SEQUENCE
    {

        snmpTsmLCDTransportDomain TransportDomain,
        snmpTsmLCDTransportAddress TransportAddress,
        snmpTsmLCDSecurityName     SnmpAdminString,
        snmpTsmLCDSecurityLevel     SnmpSecurityLevel,
        snmpTsmLCDTmSecurityName             SnmpAdminString,
        snmpTsmLCDStorageType      StorageType,
        snmpTsmLCDRowStatus           RowStatus
    }

   snmpTsmLCDTransportDomain OBJECT-TYPE
       SYNTAX      TransportDomain
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "This object indicates the transport type of the address
            contained in the snmpTsmLCDTransportAddress object."
       ::= { snmpTsmLCDEntry 1 }

   snmpTsmLCDTransportAddress OBJECT-TYPE
       SYNTAX      TransportAddress
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "This object contains a transport address.  The format of
            this address depends on the value of the
            snmpTsmLCDTransportDomain object."
       ::= { snmpTsmLCDEntry 2 }

snmpTsmLCDSecurityName      OBJECT-TYPE
    SYNTAX       SnmpAdminString (SIZE(1..32))
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "A human readable string representing the user in
                 Security Model independent format.

                 The default transformation of the Transport Security
                 Model dependent security ID to the securityName and
                 vice versa is the identity function so that the
                 securityName is the same as the LCDTmSecurityName.
                 [TODO]
                "
```

```
    ::= { snmpTsmLCDEntry 3 }

snmpTsmLCDSecurityLevel OBJECT-TYPE
    SYNTAX       SnmpSecurityLevel
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "A value representing whether the transport
                protocol provides authentication and privacy services
                for the specified UserName
                "
    ::= { snmpTsmLCDEntry 4 }

snmpTsmLCDTmSecurityName      OBJECT-TYPE
    SYNTAX       SnmpAdminString
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "A human readable string passed between the security
                 model and the transport model.
                "
    ::= { snmpTsmLCDEntry 5 }

snmpTsmLCDStorageType OBJECT-TYPE
    SYNTAX       StorageType
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "The storage type for this conceptual row.

                 Conceptual rows having the value readOnly, permanent,
                 or nonVolatile must persist across reinitializations of
                 the management subsystem.

                 Conceptual rows having the value 'volatile' must not
                 persist across reinitializations of the management
                 subsystem.

                 It is an implementation issue to decide if a SET for
                 a readOnly or permanent row is accepted at all. In
                 some contexts this may make sense, in others it may
                 not. If a SET for a readOnly or permanent row is not
                 accepted at all, then a 'wrongValue' error must be
                 returned.
                "
    DEFVAL      { volatile }
    ::= { snmpTsmLCDEntry 6 }

snmpTsmLCDRowStatus    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 snmpTsmLCDStatus
                 is 'notReady'.

                 The snmpTsmLCDTmSecurityName value should only be
                 changed when the value of this object
                 is 'active'.
                "
    ::= { snmpTsmLCDEntry 7 }

-- ************************************************************
-- snmpTsmMIB - Conformance Information
-- ************************************************************

snmpTsmCompliances OBJECT IDENTIFIER ::= { snmpTsmConformance 1 }

snmpTsmGroups OBJECT IDENTIFIER ::= { snmpTsmConformance 2 }

-- ************************************************************
-- Compliance statements
-- ************************************************************

snmpTsmCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
        "The compliance statement for SNMP engines that support
         the SNMP-TSM-MIB"
    MODULE
        MANDATORY-GROUPS { snmpTsmGroup }
    ::= { snmpTsmCompliances 1 }

-- ************************************************************
-- Units of conformance
-- ************************************************************
snmpTsmGroup OBJECT-GROUP
    OBJECTS {
        snmpTsmInvalidCaches,
        snmpTsmInadequateSecurityLevels,
        snmpTsmInvalidDomains,
        snmpTsmLCDTransformPolicy,
        snmpTsmLCDSpinLock,
        snmpTsmLCDTmSecurityName,
        snmpTsmLCDStorageType,
        snmpTsmLCDRowStatus
```

```
    }
    STATUS      current
    DESCRIPTION "A collection of objects for maintaining
                 information of an SNMP engine which implements
                 the SNMP Transport Security Model.
                "

    ::= { snmpTsmGroups 2 }

END
```

8. Security Considerations

This document describes a Security Model that permits SNMP to utilize security services provided through an SNMP Transport Model. The Transport Security Model relies on Transport Models for mutual authentication, binding of keys, confidentiality and integrity. The security threats and how those threats are mitigated should be covered in detail in the specification of the Transport Model and the underlying secure transport.

Transport Security Model relies on a Transport Model to provide an authenticated principal for mapping to securityName, and an assertion of tmTransportSecurityLevel.

The Transport Security Model is called a Security Model to be compatible with the RFC3411 architecture. However, this Security Model provides no security itself. It SHOULD always be used with a Transport Model that provides security, but this is a run-time decision of the operator or management application, or a configuration decision of an operator.

8.1. MIB module security

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/vulnerability:

- o The snmpTsmLCDTransformTable objects could be modified to disable valid domains, creating a denial of service, or to enable a transport model that was disabled by an authorized administrator.

o The snmpTsmLCDTable could be modified to map an authenticated identity to a securityName that has greater authorization than the principal should be permitted.

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 snmpTsmInvalidCaches and snmpTsmInadequateSecurityLevels and snmpTsmInvalidDomains may make it easier for an attacker to detect vulnerabilities.

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 USM and Transport Security Model 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

[DISCUSS: should we have default ports for request/response traffic and for notifications?]

IANA is requested to assign:

1. an SMI number under mib-2, for the MIB module in this document,

2. a value, preferably 4, to identify the Transport Security Model, in the Security Models registry at http://www.iana.org/assignments/snmp-number-spaces. This should result in the following table of values:

Value	Description	References
0	reserved for 'any'	[RFC3411]
1	reserved for SNMPv1	[RFC3411]
2	reserved for SNMPv2c	[RFC3411]
3	User-Based Security Model (USM)	[RFC3411]
YY	Transport Security Model (TSM)	[RFCXXXX]

-- NOTE to RFC editor: replace XXXX with actual RFC number
--   for this document and remove this note
-- NOTE to RFC editor: replace YY with actual IANA-assigned number,
                       throughout this document and remove this note.

10. References

10.1. 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.

[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.

[RFC3419] Daniele, M. and J. Schoenwaelder, "Textual Conventions for Transport Addresses", RFC 3419, December 2002.

[I-D.ietf-isms-tmsm] Harrington, D. and J. Schoenwaelder, "Transport Subsystem for the Simple Network Management Protocol (SNMP)", draft-ietf-isms-tmsm-12 (work in progress), February 2008.

10.2. 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.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3584] Frye, R., Levi, D., Routhier, S., and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework", BCP 74, RFC 3584, August 2003.

Appendix A. Notification Tables Configuration

The SNMP-TARGET-MIB and SNMP-NOTIFICATION-MIB [RFC3413] are used to configure notification originators with the destinations to which notifications should be sent.

Most of the configuration is security-model-independent and transport-model-independent.

The values we will use in the examples for the five model-independent security and transport parameters are:

```
transportDomain = snmpSSHDomain

transportAddress = 192.0.2.1:162
```

securityModel = Transport Security Model

securityName = sampleUser

securityLevel = authPriv

The following example will configure the Notification Originator to send informs to a Notification Receiver at host 192.0.2.1 port 162 using the securityName "sampleUser". The columns marked with a "*" are the items that are Security Model or Transport Model specific.

The configuration for the "sampleUser" settings in the SNMP-VIEW-BASED-ACM-MIB objects are not shown here for brevity. First we configure which type of notification should be sent for this taglist (toCRTag). In this example, we choose to send an Inform.

```
  snmpNotifyTable row:
       snmpNotifyName                 CRNotif
       snmpNotifyTag                  toCRTag
       snmpNotifyType                 inform
       snmpNotifyStorageType          nonVolatile
       snmpNotifyColumnStatus         createAndGo
```

Then we configure a transport address to which notifications associated with this taglist should be sent, and we specify which snmpTargetParamsEntry should be used (toCR) when sending to this transport address.

```
       snmpTargetAddrTable row:
          snmpTargetAddrName               toCRAddr
      *   snmpTargetAddrTDomain            snmpSSHDomain
          snmpTargetAddrTAddress           192.0.2.1:162
          snmpTargetAddrTimeout            1500
          snmpTargetAddrRetryCount         3
          snmpTargetAddrTagList            toCRTag
          snmpTargetAddrParams             toCR   (must match below)
          snmpTargetAddrStorageType        nonVolatile
          snmpTargetAddrColumnStatus       createAndGo
```

Then we configure which principal at the host should receive the notifications associated with this taglist. Here we choose "sampleUser", who uses the Transport Security Model.

```
        snmpTargetParamsTable row:
            snmpTargetParamsName             toCR
            snmpTargetParamsMPModel          SNMPv3
        *   snmpTargetParamsSecurityModel    TransportSecurityModel
            snmpTargetParamsSecurityName     "sampleUser"
            snmpTargetParamsSecurityLevel    authPriv
            snmpTargetParamsStorageType      nonVolatile
            snmpTargetParamsRowStatus        createAndGo
```

A.1. Transport Security Model Processing for Notifications

The Transport Security Model is called using the generateRequestMsg() ASI, with the following parameters (* are from the above tables):

```
 statusInformation =                -- success or errorIndication
       generateRequestMsg(
       IN   messageProcessingModel  -- *snmpTargetParamsMPModel
       IN   globalData              -- message header, admin data
       IN   maxMessageSize          -- of the sending SNMP entity
       IN   transportDomain         -- *snmpTargetAddrTDomain
       IN   transportAddress        -- *snmpTargetAddrTAddress
       IN   securityModel           -- *snmpTargetParamsSecurityModel
       IN   securityEngineID        -- immaterial; TSM will ignore.
       IN   securityName            -- snmpTargetParamsSecurityName
       IN   securityLevel           -- *snmpTargetParamsSecurityLevel
       IN   scopedPDU               -- message (plaintext) payload
       OUT  securityParameters      -- filled in by Security Module
       OUT  wholeMsg                -- complete generated message
       OUT  wholeMsgLength          -- length of generated message
       OUT  tmStateReference        -- reference to transport info
            )
```

The Transport Security Model will determine the Transport Model based on the snmpTargetAddrTDomain. The selected Transport Model will select the appropriate transport connection using the snmpTargetAddrTAddress, snmpTargetParamsSecurityName, and snmpTargetParamsSecurityLevel.

Appendix B. Processing Differences between USM and Secure Transport

USM and secure transports differ in the processing order and responsibilities within the RFC3411 architecture. While the steps are the same, they occur in a different order, and may be done by different subsystems. The following lists illustrate the difference in the flow and the responsibility for different processing steps for incoming messages when using USM and when using a secure transport. (Note that these lists are simplified for illustrative purposes, and

do not represent all details of processing. Transport Models must provide the detailed elements of procedure.)

With USM, SNMPv1, and SNMPv2c Security Models, security processing starts when the Message Processing Model decodes portions of the ASN.1 message to extract header fields that are used to determine which Security Model should process the message to perform authentication, decryption, timeliness checking, integrity checking, and translation of parameters to model-independent parameters. By comparison, a secure transport performs those security functions on the message, before the ASN.1 is decoded.

Step 6 cannot occur until after decryption occurs. Step 6 and beyond are the same for USM and a secure transport.

B.1. USM and the RFC3411 Architecture

1) decode the ASN.1 header (Message Processing Model)

2) determine the SNMP Security Model and parameters (Message Processing Model)

3) verify securityLevel. [Security Model]

4) translate parameters to model-independent parameters (Security Model)

5) authenticate the principal, check message integrity and timeliness, and decrypt the message. [Security Model]

6) determine the pduType in the decrypted portions (Message Processing Model), and

7) pass on the decrypted portions with model-independent parameters.

B.2. Transport Subsystem and the RFC3411 Architecture

1) authenticate the principal, check integrity and timeliness of the message, and decrypt the message. [Transport Model]

2) translate parameters to model-independent parameters (Transport Model)

3) decode the ASN.1 header (Message Processing Model)

4) determine the SNMP Security Model and parameters (Message Processing Model)

5) verify securityLevel [Security Model]

6) determine the pduType in the decrypted portions (Message Processing Model), and

7) pass on the decrypted portions with model-independent security parameters

If a message is secured using a secure transport layer, then the Transport Model should provide the translation from the authenticated identity (e.g., an SSH user name) to a human-friendly identifier in step 2. The security model will provide a mapping from that identifier to a model-independent securityName.

Appendix C. Open Issues

Does TSM need to have a mapping table to handle the translations from tmSecurityName to securityName?

Do we need administratively definable transform selection?

Do we need to let operators disable support for some transports?

Appendix D. Change Log

From -07- to -08-

Added tables to the MIB module to define a Transport Security Model-specific LCD, and updated the Elements of Procedure. This was because references to an abstract LCD sort of owned by both the security model and the transport model were found confusing.

Realized we referred to the MIB module in text as SNMP-TRANSPORT-SM-MIB, but SNMP-TSM-MIB in the module. Changed all occurrences of SNMP-TRANSPORT-SM-MIB to SNMP-TSM-MIB, following RFC4181 guidelines for naming.

Updated Security Considerations to warn about writable objects, and added the new counter to the readable objects list.

Changed snmpTsmLCDName to snmpTsmLCDTmSecurityName

From -05- to -06-

Fixed a bunch of editorial nits

Fixed the note about terminology consistent with SNMPv3.

Updated MIB assignment to by rfc4181 compatible

Replaced tmSameSession with tmSameSecurity to eliminate session-matching from the security model.

Eliminated all reference to the LCD from the Transport Security Model; the LCD is now TM-specific.

Added tmTransportSecurityLevel and tmRequestedSecurityLevel to clarify incoming versus outgoing

From -04- to -05-

Removed check for empty securityParameters for incoming messages

Added a note about terminology, for consistency with SNMPv3 rather than with RFC2828.

From -03- to -04-

Editorial changes requested by Tom Petch, to clarify behavior with SNMPv1/v2c

Added early discussion of how TSM fits into the architecture to clarify behavior when RFC3584 security models are co-resident.

Editorial changes requested by Bert Wijnen, to eliminate version-specific discussions.

Removed sections on version-specific message formats.

Removed discussion of SNMPv3 in Motivation section.

Added discussion of request/response session matching.

From -02- to -03-

Editorial changes suggested by Juergen Schoenwaelder

Capitalized Transport Models, Security Models, and Message Processing Models, to be consistent with RFC341x conventions.

Eliminated some text that duplicated RFC3412, especially in Elements of Procedure.

Changed the encoding of msgSecurityParameters

Marked the (NEW) fields added to existing ASIs

Modified text intro discussing relationships to other MIB modules.

From -01- to -02-

Changed transportSecurityModel(4) to transportSecurityModel(YY), waiting for assignment

cleaned up elements of procedure [todo]s

use the same errorIndication as USM for unsupportedSecurityLevel

fixed syntax of tsmInadequateSecurity counter

changed the "can and will use" the same security parameters to "can use", to allow responses that have different security parameters than the request.

removed "Relationship to the SNMP-FRAMEWORK-MIB"

cleaned up "MIB Modules Required for IMPORTS"

From -00- to -01-

made the Transport Model not know anything about the Security Model.

modified the elements of procedure sections, given the implications of this change.

simplified elements of procedure, removing most info specified in architecture/subsystem definitions.

rethought the coexistence section

noted the implications of the Transport Security Model on isAccessAllowed()

modified all text related to the LCD.

removed most of the MIB (now the TSM has no configuration parameters).

added counters needed to support elements of procedure

renamed MIB module, and registered under snmpModules

updated IANA and Security Considerations

updated references.

modified the notification configurations.

From SSHSM-04- to Transport-security-model-00

added tsmUserTable

updated Appendix - Notification Tables Configuration

remove open/closed issue appendices

changed tmSessionReference to tmStateReference

Author's Address

David Harrington
Huawei Technologies (USA)
1700 Alma Dr. Suite 100
Plano, TX 75075
USA

Phone: +1 603 436 8634
EMail: dharrington@huawei.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.