Network Working Group
Internet-Draft
Updates: 3411,3412,3414,3417
(if approved)
Intended status: Informational
Expires: December 31, 2007

D. Harrington
Huawei Technologies (USA)

June 29, 2007

Security Requirements for MIB Access
draft-harrington-mib-access-security-00

Status of This Memo

Copyright Notice

Abstract

Management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. This document describes requirements related to protecting the information in the Management Information Base when the data is being accessed or transported.

Table of Contents

1. Introduction

Management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. This document describes requirements related to protecting the information in the Management Information Base when the data is being accessed or transported.

MIB modules are written in the SMIv1 and SMIv2 data definition language, defined in STD 16, RFC 1155 and STD 58, RFCs 2578, 2579, 2580.

Management protocols provide for the exchange of messages which convey management information between between entities such as SNMP managers and SNMP agents. SNMP has typically been the protocol for transferring MIB data, and SNMP version 3 is an IETF Standard that describes security requirements related to transporting MIB data, the related threats, and mechanisms to mitigate those threats.

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].

It is expected that readers of this document will have read RFC3410 and RFC3411, and have a general understanding of the security-related functionality defined in RFCs 3412-3418.

1.2. 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].

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are not to be interpreted as described in RFC2119. They will usually, but not always, be used in a context relating to compatibility with the RFC3411 architecture or the subsystem defined here, but which might have no impact on on-the-wire compatibility. These terms are used as guidance for designers of proposed IETF models to make the designs compatible with RFC3411 subsystems and Abstract Service Interfaces (see section 3.2). Implementers are free to implement differently. Some usages of these lowercase terms are simply normal English usage.

Some terminology used in this document was defined as part of the IETF SNMPv3 Standard (STD62) or existed in normal English before the informational 'Internet Security Glossary' (RFC2828) was published. For consistency with related specifications, where necessary, this document favors terminology consistent with STD62 rather than with the Internet Security Glossary.

2. Motivation

The specifications of the Internet Standard Management Framework are based on a modular architecture. This framework is more than just a protocol for moving data. It consists of:

* a data definition language,
* definitions of management information (the Management Information Base, or MIB),
* a protocol definition, and
* security and administration.

Over time, as the Framework has evolved from SNMPv1, through SNMPv2, to SNMPv3, the definitions of each of these architectural components have become richer and more clearly defined, but the fundamental architecture has remained consistent. One prime motivator for this modularity was to enable the ongoing evolution of the Framework, as is documented in RFC 1052 [2].

When originally envisioned, this capability was to be used to ease the transition from SNMP-based management of internets to management based on OSI protocols. To this end, the framework was architected with a protocol-independent data definition language and Management Information Base along with a MIB-independent protocol. This separation was designed to allow the SNMP-based protocol to be replaced without requiring the management information to be redefined or reinstrumented.

SNMP has proven itself useful for certain management tasks, especially fault and performance management. but not for all management tasks. The IETF has therefore chosen to develop or standardize additional protocols to meet the needs of other management tasks, such as Netconf for configuration, IPFIX for flow accounting, and syslog for logging. Additional protocols may eb developed for other purposes.

When RFC1052 was written, security was less of a problem in the Internet than it is today. The first and second versions of SNMP included only trivial security, but it was soon recognized that access to management information could be a serious network security vulnerability. SNMP version theree was developed to provide a secure transport for management data, plus controls to allow operators to configure policies regarding who is authorized to do what to which

subsets of the MIB.

3. Requirements of a MIB Data Transport Protocol

3.1. Message Security Requirements

Protocols used to transport MIB data SHOULD provide protection against the following message-oriented threats [RFC3411]:

1. modification of information
2. masquerade
3. message stream modification
4. disclosure

These threats are described in section 1.4 of [RFC3411]. It is not required to protect against denial of service or traffic analysis, but it should not make those threats significantly worse.

3.1.1. Security Protocol Requirements

There are a number of standard protocols that could be proposed as possible solutions for transporting MIB data securely. Some factors SHOULD be considered when selecting a protocol.

Using a protocol in a manner for which it was not designed has numerous problems. The advertised security characteristics of a protocol might depend on it being used as designed; when used in other ways, it might not deliver the expected security characteristics.

Protocols used to transport MIB data MUST be able to coexist with each other.

3.2. Access Control Requirements

RFC3411 made some design decisions related to the support of an Access Control Subsystem. These include a securityName and securityLevel mapping, the separation of Authentication and Authorization, and the passing of model-independent security parameters.

3.3. Session Requirements

Some protocls might have a notion of sessions, while other protocols might provide channels or other session-like mechanism. Throughout this document, the term session is used in a broad sense to cover sessions, channels, and session-like mechanisms. Session refers to an association between two protocol engines that permits the

transmission of one or more messages within the lifetime of the session. How the session is actually established, opened, closed, or maintained is specific to a particular protocol.

Sessions may be considered desirable because the cost of authentication and integrity checking can be amortized over potentially many transactions.

3.3.1. Message security versus session security

A session is associated with state information that is maintained for its lifetime. This state information allows for the application of various security services to multiple messages.

Cryptographic keys established at the beginning of the session SHOULD be used to provide authentication, integrity checking, and encryption services for data that is communicated during the session. The cryptographic protocols used to establish keys for a Transport Model session SHOULD ensure that fresh new session keys are generated for each session. In addition sequence information might be maintained in the session which can be used to prevent the replay and reordering of messages within a session. If each session uses new keys, then a cross-session replay attack will be unsuccessful; that is, an attacker cannot successfully replay on one session a message he observed from another session. A good security protocol will also protect against replay attacks _within_ a session; that is, an attacker cannot successfully replay a message observed earlier in the same session.

Implementations SHOULD be able to maintain some reasonable number of concurrent sessions.

4. Integrating with SNMPv3

[discuss] One approach to providing access controls for protocols other than SNMPv3 is to design the protocol to utilize existing SNMP subsystems, such as the Access Control Subsystem.

The Access Control Subsystem can theoretically be accessed via the architectural ASI known as isAccessAllowed. Implemneters may or may not support an actual function call to match this ASI.

[discuss] Discuss what would be needed to utilize the existing isAccessAllowed ASI, how the parameters could be provided by the calling protocol, and the implications of using this approach.

[discuss] some transports might be able to be managed within the SNMPv3 architecure as new Transport Models, as described in the ISMS

documents.

[discuss] Some new protocols might be able to be designed as new message models in the RFC3411 architecture, possibly supported by new "Applications", which would permit reuse of existing secure Transport Models, the Transport Security Model, and existing Access Control Models.

4.1. Architectural Modularity Requirements

SNMP version 3 (SNMPv3) is based on a modular architecture (defined in [RFC3411] section 3) to allow the evolution of the SNMP protocol standards over time, and to minimize side effects between subsystems when changes are made.

[todo] describe how a new protocol could fit into the existing architecture.

5. Security Considerations

This document discusses the security requirements that should be considered for all protocols which will carry MIB data. The text of this document is, in effect, filled with Security Considerations.

6. IANA Considerations

This document requires no action by IANA.

7. Acknowledgments

The auithor would like to thank the following people for their contributions:

8. References

8.1. Normative References

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

[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.

[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.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

8.2. Informative References

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

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

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC4422] Melnikov, A. and K.

Zeilenga, "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4741] Enns, R., "NETCONF Configuration Protocol", RFC 4741, December 2006.

[I-D.ietf-isms-transport-security-model] Harrington, D., "Transport Security Model for SNMP", draft-ietf-isms-transport-security-model-04 (work in progress), May 2007.

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

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).