Extended Security Options for Standards-Based Network Management

SNMP Research International, Inc.
Knoxville, Tennessee

1 Overview

Security was initially not addressed in standards-based network management. The original Simple Network Management Protocol (SNMP) specifications included only a very simple “community string” mechanism for specifying access restrictions to management data. Because of this, the use of SNMP was frequently limited to read-only monitoring of network health and performance information.

The introduction of SNMP version 3 (SNMPv3) added authentication and privacy (encryption) features to the communication of management information to provide vastly improved security. SNMPv3 also includes a flexible and powerful administrative framework to implement the security infrastructure. This administrative framework contains configuration information for the usernames, access rights, and keys used to limit access to management data. Today, access to management information can be made much more secure, and the risk of malicious damage through the use of network management commands is reduced. The improved security provided by SNMPv3 has also facilitated the use of SNMP for configuration changes (write operations). SNMPv3 has become popular in government, military, and security-conscious commercial enterprises.

The SNMPv3 specification documents define standard implementations of two cryptography technologies for authentication (MD5 and SHA1), and one technology for encryption (56-bit DES in CBC mode). However, the specification documents define extensibility techniques for both authentication and encryption, so organizations may implement the cryptography technologies required for their environments. Several vendors have implemented stronger cryptography (in the prescribed manner) to meet the security needs of their customers. This paper is a brief overview of the security mechanisms currently available for SNMPv3. Please reference the IETF specification documents (RFCs) and documents published by SNMP Research International for implementation details.

2 Authentication

Authentication is the process of reliably verifying the source and validity of a request or response. Agents and managers need to verify that the requests being made of them come from a known party, have not been corrupted or modified, and are not replays of requests sent earlier.

In the SNMPv3 framework, authentication protects against the following threats:

- Masquerade, where the sender of a message is pretending to be another entity;
- Modification of information, where the content of a message has been changed or corrupted;
- Modification of the message stream, where a previous message is being sent again, or an intercepted message is sent at a later time.

For each packet where authentication is requested, the sender computes a message digest based on the contents of the request or response, and includes it in the request header. On receipt of the request or response, the receiver computes the message digest, and verifies that it matches the digest computed by the sender. The key used in the digest algorithm is known only to the sender and receiver, so third-party reproduction of the digest is not feasible. The User-based Security Model (USM) specifies that either the MD5 or the SHA1 digest algorithms may be used in computing the message digest.

A shared secret key (i.e. the same key for the manager and for the agent) is used when generating the digest. Each manager must know the authentication key for each agent for which it must communicate. Each user might have only one authentication pass-phrase that is used across an administrative domain, but a localized key for each agent is automatically generated from the user’s pass-phrase. The key is localized for each agent, so for a well-implemented agent (i.e., an agent that does not store pass-phrases in plaintext) inadvertent disclosure of an agent’s secrets will not breach security for the entire administrative domain.

The choice of digest algorithm is made when the SNMPv3 user used to send and receive messages is created. Since the digest algorithm is identified by name (object identifier), agents and managers can be extended to use other digest algorithms, though, to the knowledge of the authors of this document, there has been no market requirement to do so. The security provided by MD5 and SHA1 authentication is sufficient to address the needs of the network management community for the foreseeable future.

The User Security Model (USM) is the standard security and management framework for SNMPv3. USM specifies the use of shared symmetric secrets, and the use of a digest-base authentication mechanism. However, as the security model is specified in each packet, it is feasible to extend the security models, so that nonstandard models can be used in a standard way. This allows implementation of third-party authentication services such as RADIUS. In this model, an authentication service is consulted by the network management system to verify the validity of the message.

3 Privacy (Encryption)

In the SNMPv3 framework, privacy is protection from the unauthorized disclosure of data. In this case the data is the message being sent between SNMP entities (e.g., a routing table being retrieved from a networking element). Privacy is implemented by encrypting the payload of the SNMP message.

The User-based Security Model (USM) of the SNMPv3 standards specifies the use of the Data Encryption

Standard (DES-CBC) with 56-bit keys as the encryption protocol. Each manager must know the privacy key for each agent for which it must communicate. Each user might have only one privacy pass-phrase that is used across an administrative domain, but a localized key for each agent is automatically generated from the user's pass-phrase. As previously explained for authentication, the key is localized for each agent, so for a well-implemented agent, inadvertent disclosure of an agent's secrets will not breach security for the entire administrative domain.

As in the user of authentication digest algorithms, the choice of the privacy protocol is made when the SNMPv3 user is created in the agent and in the manager. Since the encryption algorithm is identified by name (object identifier), agents and managers can be extended to use other encryption algorithms in an interoperable manner. There is much interest in adding additional security protocols to SNMPv3, as there is concern about the viability of 56-bit DES as an encryption algorithm. As 56-bit DES is theoretically breakable in a reasonable amount of time using current computing technology, some network operators require stronger cryptography.

Two encryption algorithms have drawn interest as additional SNMPv3 encryption protocols. The Advanced Encryption Standard (AES) has been adopted by the United States National Institute of Standards and Technology (NIST) for both government and business use (**http://www.nist.gov/aes**). Work is in progress in the Internet Engineering Task Force (IETF) to adopt the AES algorithm as an alternative SNMPv3 encryption protocol (**http://www.snmp.com/eso**). While AES is defined with three possible key lengths (128, 192 and 256 bit), at this point only the 128 bit version is being considered for SNMPv3, as it is likely to be sufficiently strong for many years. Triple-DES using a 168 bit key (abbreviated 3DES or TDEA) is currently a popular algorithm in government and business, and has been implemented by SNMP Research and others as an encryption protocol for SNMPv3. 3DES is identified in Federal Information Processing Standard (FIPS) 46-3 as the FIPS-recognized encryption algorithm of choice, and therefore is used by U.S. government entities that need to comply with FIPS 140-1 and FIPS 140-2. 3DES has a proven track record in field deployments, but the algorithm takes more computing time than any of the AES protocols.

Several networking equipment and management technology vendors have already implemented the extended security options of 3DES and AES in their SNMPv3 implementations. Known implementers of 3DES include Juniper, Marconi, and SNMP Research. Known implementers of AES include Juniper, SNMP Research, MGSoft, and the NetSNMP open software project. Other encryption technologies may be used with SNMPv3, but none are known to the authors to be in wide use.

4 Sources for More Information

- SNMPv3 Specifications
  http://www.snmp.com/snmpv3/.
- Internet Engineering Task Force (IETF)
  The User-based Security Model is defined in the IETF RFC 3414. Refer to **http://www.ietf.org** for information on receiving the freely available IETF standards.
- Extended Security Consortium
  The AES and 3DES security protocol definition documents are available at the Extended Security Consortium web site (**http://www.snmp.com**) at the following page:
  http://www.snmp.com/protocol/eso.shtml.
- Federal Information Processing Standard (FIPS)

http://www.itl.nist.gov/fipspubs/

5 Contact Information

For further information about this whitepaper or SNMP Research's products, please contact SNMP Research, Inc.

SNMP Research International
3001 Kimberlin Heights Road
Knoxville, TN, USA 37920-9716
Phone: +1 865 579 3311
Fax: +1 865 579 6565

Sales Query: http://www.snmp.com/salesquery.shtml

Information E-mail: info@snmp.com

Sales E-mail: sales@snmp.com