Security in the Management of Networks with SNMPv3

L. J. García Villalba, J. H. Ortiz Monedero and R. Paucar Curasma

Department of Computer Systems and Programming
Complutense University of Madrid (UCM)
Juan del Rosal, 8 – 28040 Madrid (Spain)

Abstract. This paper describes an experimental study of the security in the management or monitoring of information from a host or teams of networks through the protocol SNMP in version 3, that is characterized in regards to security authentication and access control. There is also developed an Management Information Base (MIB) in ASNI language which will be read and written using the SNMPv3 protocol in which is observed the authentication based on the user. Finally some configurations are illustrated and results obtained from the study.

1 Introduction

The proliferation of the data networks in the last decades, LANs as well as WANs, and the relationship between them makes the aspects relative to their control and management taken into account more and more each time, converting themselves into something to which all those responsible for the networks have to pay great attention.

Given that the natural tendency of any network is to grow, there are added new applications and users make use of the network, the management systems used need to be sufficiently flexible to be able to support the new elements that have been added without the necessity of making drastic changes in the network.

SNMP (Simple Network Management Protocol), in its different versions, is a group of network management applications that use the services offered by TCP/IP and that have become a standard. At the root of interests shown by the IAB (Internet Activities Board) is the finding of a management protocol that was valid for the network of the internet, with its necessities due to its large dimensions.

The SNMP protocol defines an interchange of network management information where in the most basic form exists a system manager and an agent through databases of information. This simplicity allowed deficiencies to be seen such as: problems in the transfer of large quantities of information, little or no security, as well as the weak mechanisms of authentication and privacy.

The capacities of SNMP for the basic management of the network are good. In 1993 SNMPv2 was introduced, which was revised in 1996. SNMPv2 was oriented to correct the capacities of transmission of large quantities of information, nevertheless

J. García Villalba L., H. Ortiz Monedero J. and Paucar Curasma R. (2004).
Security in the Management of Networks with SNMPv3.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 351-360
DOI: 10.5220/0002688303510360

this version continued without offering any solution in respect to security and privacy. Specifically, neither SNMPv1, nor SNMPv2 can authenticate the source of the management message, much less provide encryption for that message. In a management network where authentication does not exist or is not possible there are possibilities that unauthorized users could easily execute management functions or even worse spy information when it is past from an agent to system manager. Due to this, many implementations in SNMPv1/SNMPv2 are limited in their capacity to only reading, which as a consequence, reduces the utilities of control and monitoring of the network.

To correct this type of deficiencies, which are of such great importance due to the evolution of the internet in the market, a work group was formed to generate a series of standards that were proposed in RFCs 2271-2275 and whose result is SNMPv3 [1]. In these documents the specifications are defined for security and access control of the networks managed with SNMP, and include the functionalities of versions SNMPv1 and SNMPv2 respectively.

2 Fundamentals of SNMP

The fundamental to understand SNMP is to take into account three essential concepts that have the function of interchanging information. In figure 1 the components of a network management system are illustrated, which are a manager and an agent.

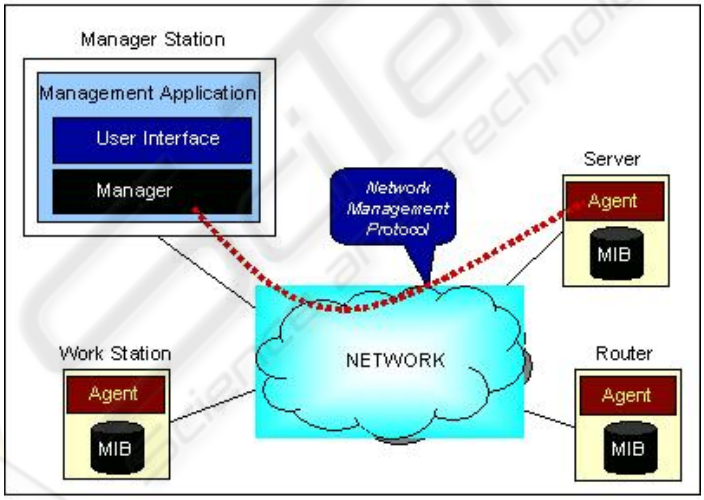

Fig. 1: Network Management System with SNMP.

In whatever configuration at least one management node has a software that supports SNMP. The management station generally provides an interface to the administrator of the network to control and observe the management processes in the network. This interface permits the user to execute commands (for example deactivate a link, read the IP address of one node and others) and provide general information of the

system. The main point of the network management system is a group of applications that join the necessities in order to execute the functions. As a minimum a system will include basic applications to develop monitoring functions, configuration control and administration of the user accounts. More sophisticated systems may include more elaborate applications for these categories with more possibilities for the correction of errors.

On the other hand, the network devices when managed, including servers, workstations, personal computers, routers, etc. are equipped with a module that includes a software agent. The agent is responsible:

- To collect and maintain information about the local environment.
- To provide information to the user of the network, either in the form of an answer to a requirement or as an advisory message that abnormal something is happening.
- To respond to the commands executed by the user to change or alter the operation parameters or local configuration.

To execute these functions each agent maintains an MIB that contains all of the information (recent as well as historical) about its local configuration and the traffic that it manages. The management station will maintain a global MIB with the summarized information from all the agents.

It is important to high-light that all management applications generally share a common protocol in the entire network. This protocol provides the fundamental functions to request information and execute commands to the agents. This protocol, in our case SNMP, makes use of communication tools such as TCP/IP.

Specifically versions SNMPv1 and SNMPv2 consist of a group of documents that define a network management protocol, a general structure MIB and a specific member of MIB structured data for management purposes. In essence protocol provides four functions:

Get	Used by the manager to execute a requirement from an agent to an MIB.
Set	Used by the manager to change some value in an MIB from an agent.
Trap	Used by an agent to send an alert message to the manager.
Inform	Used by the manager to send an alert message to another manager.

3 SNMPv3

To correct the security deficiency that SNMPv1 and SNMPv2 have presented until now, a series of recommendations were written [2]. These recommendations are oriented to define an architecture and new capacities. SNMPv3 is a interoperable network management protocol, that provides access security to the devices by way of a combination of authentication and encryption of packages that travel by the network. The security capacities that SNMPv3 provides are:

Message Integrity	Assures that the package is not violated during transmission.
Authentication	Determines that the message comes from a valid source.
Encryption	Encrypts the contents of a package as a form of prevention.

3.1 Architecture

SNMPv3 [3] provides models as well as levels of security. A model of security is a strategy of authentication that is configured for the users and groups in which those reside. The levels of security refer to the level permitted to a user inside of a model of security. The combination of the two will determine which security mechanism will be used when an SNMP package is handled. SNMPv3 includes three services: authentication, privacy and access control. To provide these services in a sufficient form, SNMPv3 introduces a new concept called Main, the which is no more than an entity in the which the greater part of the services are proportioned or processed. A Main may act in an individual form or in a particular role, as an application or a group of applications or even as a combination of all of them. Essentially a Main operates from a management station and sends SNMP commands to the agents. The identity of the Main and that of the agent together determine the security capacity that will be invoked, including authentication, privacy and access control.

It is possible to define SNMPv3 in a modular form. Each SNMP entity includes a simple SNMP Engine. An SNMP Engine implements functions to send/receive, authenticate and encrypt/decrypt messages, in addition to controlling access to the handled objects. These functions are proportioned as services for one or more applications that are configured with the SNMP Engine to thus form the SNMP Entity as illustrated in the figure 2.

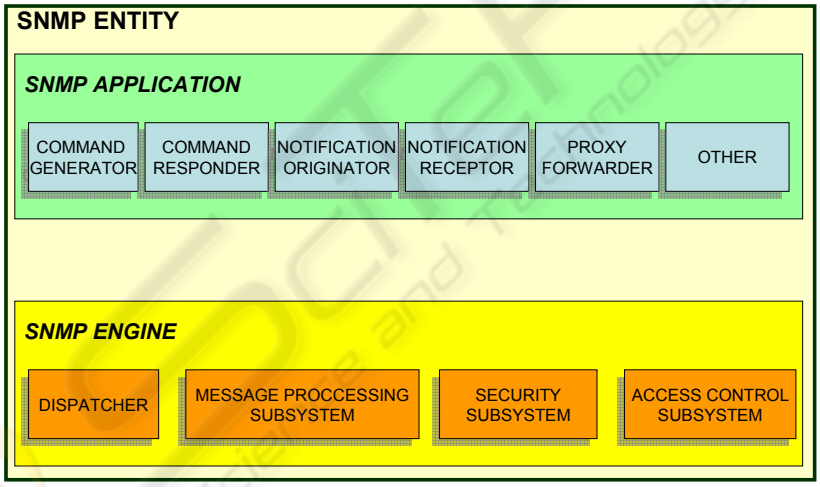

Fig. 2. Management Architecture of SNMPv3.

The modular architecture that is presented provides some advantages listed as follows:

- The role of the SNMP Entity is determined by modules that are implemented in that entity.
- The modular structure of the specifications allows the definition of different versions of each module, which makes it possible for them to take certain capacities and aspects of SNMP without the necessity of going to a new version

and taking the complete standard, in this way the co-existence of various versions are maintained.

3.2 Elements of a SNMP Entity

They are the following:

SNMP ENGINE:

Dispatcher. Permits the concurrence of multiple versions of SNMP messages in the SNMP Engine. It is responsible for:

- Accepting the PDUs (Protocol Data Units) from the applications so that later they are transmitted through the network, and sending the incoming PDUs to the applications.
- Passing the PDUs that leave to the Message Processing Subsystem so that they are prepared, and passing the incoming PDUs to the same subsystem so that they are extracted.
- Sending and receiving SNMP messages inside the network.

Message Processing Subsystem. Responsible for preparing messages to send and to extract the data of the received information.

Security Subsystem. Provides the services of authentication and privacy of the message. This subsystem potentially contains several security models.

Access Control Subsystem. Provides a set of services of authorization that an application can use for the control of access of the messages.

SNMP APPLICATION:

Command Generator. Starts the PDUs SNMP Get, GetNext, GetBulk or Set Request and processes the answer to a request that has been generated.

Command Responder. Receives the PDUs SNMP Get, GetNext, GetBulk or Set Request directed to the local system and later bring about the operation of the appropriate protocols using access control, and generates an answer message to be sent to the station that made the request.

Notification Originator. Monitors a system for a condition or a particular event and generates a Trap or an Inform message based on the condition or event. A notification originator should have a mechanism to determine where to send the message and which SNMP version and security parameters to use when the message is sent.

Notification Receptor. Waits for the notification messages and generates answers when a received message contains an Inform PDU.

Proxy Forwarder. Advances the SNMP messages. It is an optional application.

3.3 Message Processing

The model for message processing for SNMPv3 is generally defined in [3]. This model is responsible for accepting the PDUs from the dispatcher, encapsulates the messages and applies the USM (The User Security Model) [5] to insert the related parameters with the security in the heading of the message. The message processing model also takes charge of accepting incoming messages applying the USM to process the security parameters that are found in the heading of the message and sends the PDU to the dispatcher**.**

The structure of the message is illustrated in figure 4. The first five fields are generated by the incoming/outgoing message processing model. The following six fields show the security parameters used by the USM. Finally the PDU together with the ContextEngineID and ContextName constitute the PDU to be processed. The first five fields are the following:

msgVersion: Configured for SNMPv3.

msgID: An identifier used among the SNMP entities to coordinate request and answer messages. Its range is from 0 to $2^{31} – 1$.

MsgMaxSize. Refers to the maximum of a message in octets supported by the sender with a range of 484 to $2^{31}– 1$. This is the maximum size that a entity that sends can accept from another SNMP Engine.

MsgFlag. An array of octets that contains three flags in the three less significant bits.

- ReportableFlag: 1 is used for sent messages containing a request or an Inform and 0 is used for messages containing an answer Trap or Report PDU.
- PriorFlag and AuthFlag: Are configured by the sender to indicate the level of security applied to the message.

MsgSecurityModel. Is an identifier in the range of $2^{31} – 1$ that indicate the security model used by the sender, so that the receiver has the knowledge which security model he should use to process the message there exist reserved values: 1 for SNMPv1, 2 for SNMPv2, 3 for SNMPv3.

The six following fields related with the security parameters and generated by the USM include:

MsgAuthoritativeEngineID. Refers to the value of the source of a Trap, Response or Report and to the destination of a Get, GetNext, GetBulk, Set or Inform.

MsgAuthoritativeEngineTime. Is an whole value in the range of $2^{31} – 1$ that represents the number of seconds from when the snmpEngineBoots of the SNMP Engine was incremented.

MsgUserName. The principle user from which the message has been sent.

MsgAuthenticationParameters. Authentication Parameter. If the authentication is not used, this value is null. This parameters generated using an algorithm called HMAC.

MsgPrivacyParameters. Privacy Parameter. If the privacy is not used this value is null. This parameter is generated using an algorithm called DES.

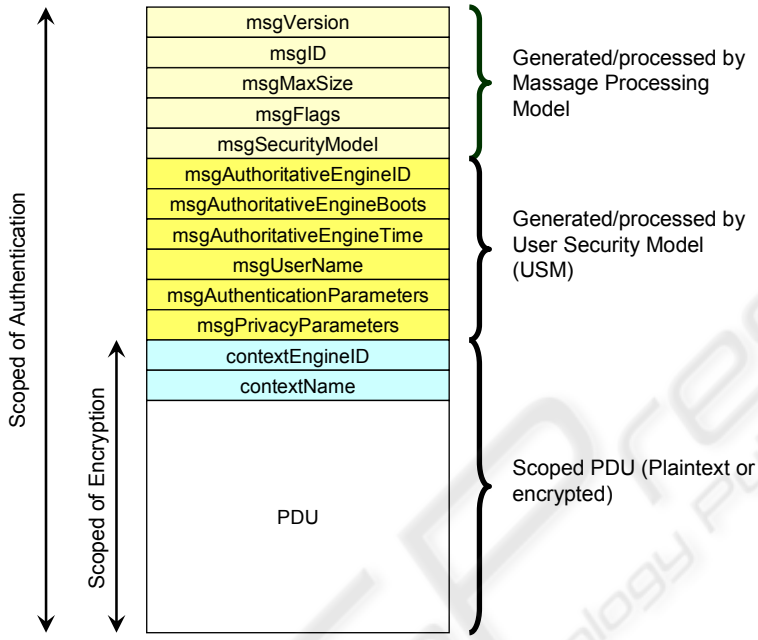

Fig. 3. Message Structure SNMP.

3.4 The Key for Authentication

The authentication mechanism in SNMPv3 assures that the message received was in reality transmitted by the principle entity source that appears in the identifying header of the message. In addition, this mechanism assures that the message was not altered during transmission and that it was not in some way delayed or captured and later resent by another source.

In the authentication process each principle and remote SNMP Engine that desires to communicate should share a secret authentication key. The entity that sends provides authentication including in the message a code. This code is a contained function of the message, of the SNMP Engine and of the principle about time of transmission and the secret key that should only be known by the sender and the receiver. The secret key should be configured initially by the administrator or user of the network, who will carry these keys in the data bases of the agents and the users. This can be done manually or using a secure form of data transmission.

When the receiving entity receives the message, it uses the same secret key to calculate the authentication code of the message. If the calculated code in the receiving side coincides with the value included with the sent message, then the receiver will know that the message originated from a authorized user and the message was not altered during transmission.

3.5 VACM (View-Based Access Control Model)

The Access Control Model makes possible the configuration of the agents to provide different access levels to the MIB and the different managers. An agent can restrict the access of its MIBs to one manager in particular in two ways: It can restrict the access to only certain parts of the MIB. The agent can limit the operation that a manager can use in certain portions of the MIB. The access control that is to be used by an agent for each manager should be pre-configured. It essentially consists of a table that details the access privileges of various authorized managers. The authentication differs in that it is done by the user, the access control is done by a group, where a group can be composed of a series of users. In figure 4 the logic of the functioning of this method of access control is illustrated

4 Implementation of the MIB Module for SNMPv3

The MIB development is done following the structure of the standard SMI [7] in one of the private nodes inside the intermediate node (internet) in figure 5 the structure of the nodes that represent the MIB created with its respective whole objects is illustrated [8]. The code written in the language ASN.1, contains the tree structure of the definition of the MIB. The final nodes indicate the whole objects that will be read or written. These will be accessed by the user of users configured in the agent that supports the protocol SNMPv3.

5 Conclusions

Now a days, the same as many other protocols used in internet, SNMP was found with the problems of security and privacy. For the which the SNMPv3 has the capacity of authentication, privacy, and access control of the information. Giving great confidence to the users of the market. As a change from the anterior versions, it is characterized by the level of security that is presented based in the user. It is for this that it has the necessity to create a user with its own respective key.

All of this was done in free distribution software such as Linux, using the SNMP package the which contains management tools, configuration files among others, being fundamental in the development of the MIB module.

Acknowledgements

Luis Javier García Villalba's work is supported by the Spanish Ministry of Science and Technology (MCYT, Spain) under Project TIC2002-04516-C03-03. This author would like to express his appreciation to the Programa Complutense del Amo for providing him a grant to stay at IBM Research Division. During part of this work he

was with the Information Storage Group at the IBM Almaden Research Center, San Jose, California, USA (javiervi@almaden.ibm.com).

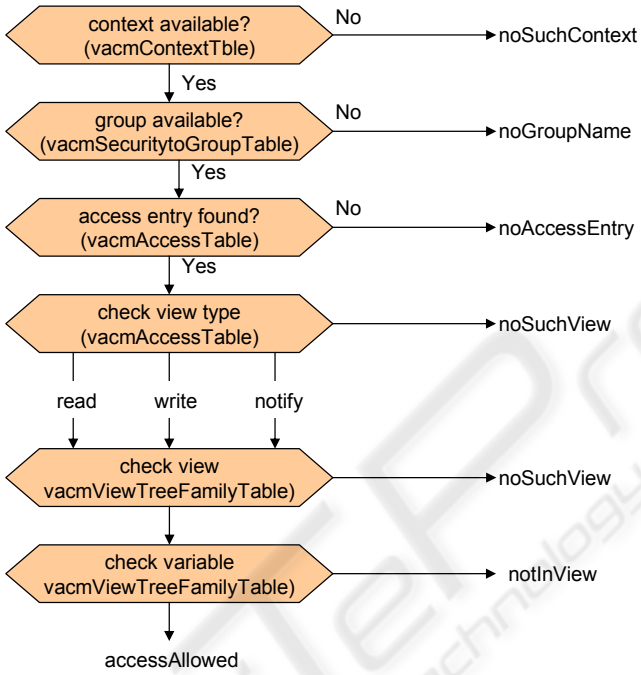

Fig. 4. Logic of the Functioning of Access Control.

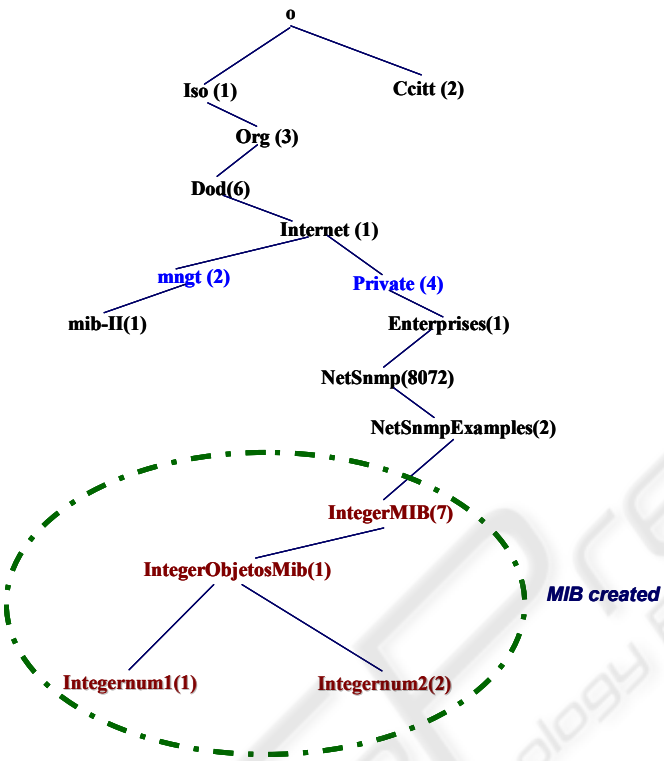

Fig. 5. Structure of the MIB Tree.

References

1. D. Harrington, R. Presuhn: “An Architecture for Describing SNMP Management Frameworks”, IETF RFC 2271, January 1998.
2. William Stallings: “Security Comes to SNMP The New SNMPv3 Proposed Internet Standards”, September 2001.
3. J. Case, D. Harrington: “Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)”, IETF RFC 2272, January 1998.
4. D. Levi, P. Meyer: “SNMPv3 Applications”, IETF RFC 2273, January 1998.
5. U. Blumenthal, B. Wijnen: “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)”, IETF RFC 2274, January 1998.
6. B. Wijnen, R. Presuhn: “View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)”, IETF RFC 2275, January 1998.
7. M. Rose, K. McCloghrie: “Structure and Identification of Management Information for TCP/IP-based Internets”, IETF RFC 1155, May 1990.
8. http://net-snmp.sourceforge.net/.