Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment: Version 1.4b Option 1

Title: Securing Network Management Information

Author: Ronald Menardo
Date: September 24, 2003

TABLE OF CONTENTS

Securing Network Management Information

I. Introduction

Simple Network Management Protocol (SNMP) has become the de facto standard for monitoring and managing network devices. The purpose of this document is to understand the importance of securing SNMP-based network management across the enterprise, and how security is implemented and enhanced as the Simple Network Management Protocol evolves.

This document is organized into two basic parts. The first part (Sections II and III) provides an overview and the basic concepts of SNMP. The second part (Sections IV, V, VI, VII) covers the importance of securing network management, SNMP vulnerabilities, implementing secure network management system, and an overview of SNMPv3.

II. SNMP Overview

A. What is SNMP?

Simple Network Management Protocol (SNMP) is a widely used network management standard. It enables the delivery of management information across the enterprise network. SNMP has three elements: Network Management System (NMS), managed devices, and agents. A Network Management System polls the network and collects information such as performance statistics, error counters, configuration, etc. from managed devices. An NMS can also perform remote configuration of managed devices. Managed devices (e.g. routers, switches, hubs) must have an SNMP agent software responsible for providing access to management information requested by a Network Management System. An SNMP agent can be configured to send unsolicited notification (trap) to a Network Management System when a network event or condition occurs.

B. Evolution of SNMP

The first version of SNMP was introduced in the late 1980's and subsequent versions were released to enhance capabilities and address security deficiencies. The first revision was SNMPv2, released in 1993 and later revised in 1996. Revisions continued with SNMPv3, drafted in 1998 and approved in December of 2002.

All SNMP versions of the Internet Standard Management Framework share the same basic structure, components and architecture. The original framework that was intended for a smooth migration from SNMP-based management to OSI protocols did not materialize. As it stands today, the de facto standard is still SNMP management based. The simplicity of the original framework made it easier for the development and release of later versions of SNMP. It also enabled the coexistence of the three SNMP versions and multi-vendor interoperability.

SNMPv2 provided several advantages from the previous version such as:[1]

- Expanded data types: 64 bit counter
- Improved efficiency and performance: get-bulk operator
- Confirmed event notification and inform operator
- Richer error handling errors and exceptions
- Improved sets: especially row creation and deletion
- Fine tuned data language

However, SNMPv2 did not meet the original goals and requirements for enhanced security and administration. Instead, SNMPv3 (described in RFC's 2570-2575) was drafted to focus on security (authentication, authorization, access control, and privacy) and administration (naming of entities, principals, and policies).

III. SNMP Basic Concepts

A. SNMP Components

The three basic components of SNMP are: managed device, agent, and Network Management System. Below are brief descriptions of the SNMP components.[2]

A *managed device* is a network node that contains an SNMP agent. Managed devices are sometimes referred as *clients* and can be routers, switches, hubs, computer hosts, printers, or other network devices.

An *agent* is network-management software that is installed in a managed device. An agent has local knowledge of the management information base (MIB) and responds to the requests (polls) from the NMS. It also sends notifications (traps) when network events or conditions occur.

A *Network Management System (NMS)* polls the network by sending requests or it receives notifications (traps) from managed devices. An NMS has network management applications that enable monitoring and remote management of network devices. An NMS is sometimes referred as a Network Manager where applications such as HPOpenView or NetView are installed.

B. SNMP Operations

The exchange of management information between SNMP components is categorized into three operations: read, write, and notify. In SNMPv1 and SNMPv2, these operations are sent and included in a PDU (Protocol Data Unit). These operations are

[1] SNMP Research International, Inc. "SNMPv3 White Paper". 21 Feb. 2003. URL http://www.snmp.com/snmpv3/v3white.html

[2] Reference Document. "Simple Network Management Protocol". 20 Feb. 2002. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm - xtocid2

executed using SNMP commands such as:[3] **GET**, **GETNext**, **GETBulk, GetReply, SET,** and **Trap** as shown in Figure1.

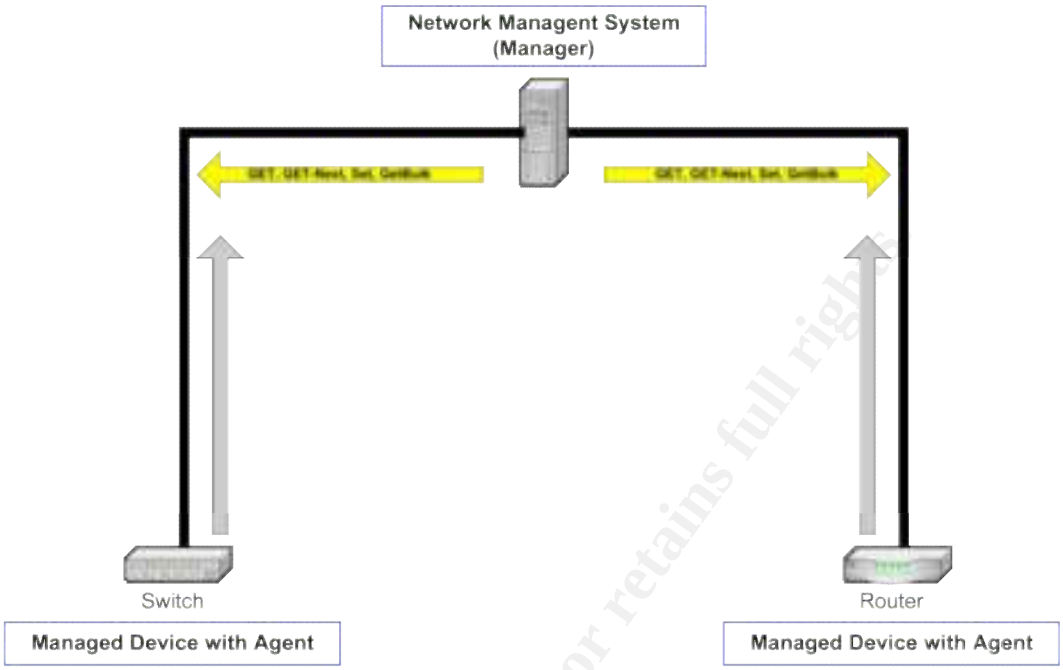

Figure 1: SNMP Commands

READ - Operation executed by a Network Management System to retrieve information from managed devices. This is a solicited request that expects a response from a managed device. (Get, GetNext, Get Bulk)

For example, when an NMS polls the network to retrieve MIB information from a managed device it uses the Get command. GetNext command is used to retrieve an incremental update from the information previously received from a Get command. GetBulk command is used to retrieve a report or detailed information.

WRITE - Operation executed by a Network Management System to configure or change settings on managed devices. This is a solicited request that requires an action to be performed by a managed device. (SET)

For example, when an NMS performs a task to change the configuration of a managed device, it uses the SET command.

NOTIFY - Operation executed by managed devices to send asynchronous notification messages popularly known as traps to a Network Management System. Unlike the

[3] Knapp, Laura Jeanne. "SNMP Version 3: Securing Your Management Structure". URL: http://www.lauraknapp.com/images/snmpv3.pdf

other SNMP operations, “notify” is an unsolicited request sent by managed devices to inform NMS that an event occurred. (Trap)

For example, when a managed device exceeded a pre-defined threshold and is required to inform the NMS, it uses Trap for notification.

What is a MIB?[4]
MIB stands for Management Information Base. It is a collection of managed objects where management information is stored. These managed objects are uniquely identified as Object Identifiers (OID). A Network Management Station queries the agent for MIB values when executing “read” or “write” operations. The MIB’s are accessed via SNMP agents and are arrange in hierarchical order similar to a tree.

C. SNMP Transport

Simple Network Management Protocol is an application layer protocol that is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP messages are transported via User Datagram Protocol (UDP) using destination ports 161 and 162.[5] Using UDP as a transport mechanism is unreliable and does not guarantee the delivery of information. This method is similar to a conversation across a public telephone network. There is no guarantee the caller’s voice message was heard by the called party. It’s up to the called party to request the calling party to repeat the message.

D. SNMP Message Structure

An SNMP message contains a header and Protocol Data Unit (PDU) as shown in Figure 2. The message header has two fields: SNMP version and community string. The PDU contains specific SNMP operations (read, write or notify) that are used to retrieve management information, send configuration changes, and send traps.

Figure 2: SNMP Message Structure

E. Simple SNMP Authentication

The exchange of management information between SNMP components uses an SNMP community string that acts similar to a password. An SNMP community string establishes a logical relationship between the NMS and managed devices.[6] The string is given a name that will be used to validate membership and is used for authentication. Managed devices will only respond to messages from an NMS with a valid community string. This prevents an unauthorized NMS from sending or receiving messages. All

---

[4] Solarwinds. “SNMP Overview and SNMP Security”. URL: http://www.solarwinds.net/Tools/SNMP.htm
[5] Cohen, Yoram. “SNMP-Simple Network Management Protocols”. URL: http://www2.rad.com/networks/1995/snmp/snmp.htm - snmp
[6] Bay Networks. “SNMP Overview”. 12 April 1996. URL: http://support.baynetworks.com/library/tpubs/html/router/soft1000/snmp/2923A-15.html

members of the community have the same access privileges, either ***read only*** (members can only view information) or ***read-write*** (members can view and also modify information). The community strings are transmitted across the network in clear text and this is a known weakness in SNMPv1 and SNMPv2.

IV. Importance of Securing Network Management

Network Management provides significant contributions in managing network devices in an enterprise. The growth of the Internet and networked services has increased the demands for network management. In the past, managing an enterprise faced multiple challenges because of limited visibility of the entire network. The lack of indicators, statistics, and baselines made it difficult to effectively determine the health of the network and forecast the network growth. As a result, uncertainties in the environment could potentially impact the production and delivery of services to customers. Today, these challenges are addressed by implementing a network management solution, which will help network administrators to proactively and effectively manage the enterprise.

Using SNMP, a network administrator is now able to discover the network topology, remotely manage network devices, and receive prioritized alerts that are critical in the fault isolation process. The International Standard Organization (ISO) has defined five functional areas of network management to keep up with these growing demands: Fault Management, Performance Management, Configuration and Name Management, Accounting Management, and Security Management.

Unfortunately, this growing dependency on enterprise network management has a downside. There are SNMP vulnerabilities and threats that can be exploited by malicious attackers. Listed below are the potential impacts and associated risks when external or internal attackers exploit SNMP vulnerabilities:[7]

- An unauthorized person could obtain the read-only or read-write community strings configured in the NMS and SNMP agents. An attacker who obtained the community string can modify the management information and use it for malicious purposes.

- SNMP is transported across the network using User Datagram Protocol (UDP) and is subject to IP source address spoofing. An unauthorized user able to assume the identity of the Network Management System could perform malicious operations to learn and disclose information contained in the data stream.

[7] Reference Document. “Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities”. Revision 2.1. 14 March 2002. URL: http://www.cisco.com/en/US/products/products_security_advisory09186a00800945b4.shtml

- The processing of requests or traps may result in a denial of service. Malformed SNMP messages received by an affected device could crash an SNMP device such as a router or cause it to continuously reload.

These associated risks could be very costly and might cause extended outages in the production environment. Securing Network Management is a must and this should not be taken for granted. The Internet industry has taken several steps to strengthen SNMP security and this is evident in the recent SNMPv3. Many vendors are actively working to make sure their products address the SNMP vulnerabilities to reduce these risks. Network administrators should know their systems and ensure that best practices and workarounds are implemented to protect against malicious attacks in the enterprise.

V. SNMP Vulnerabilities and Threats

A. SNMPv1 Vulnerabilities

The Oulu University Security Programming Group (OUSPG) conducted a research project and found multiple vulnerabilities in the SNMPv1 implementations from different vendors. The testing was focused in the way SNMP managers and SNMP agents decode and process traps and requests. Their testing discovered that the decoding and processing of traps and requests might result in denial of service, community string vulnerabilities, buffer overflows and an unauthorized access. These vulnerabilities are categorized as follows:[8]

> **"*VU#107186 – Multiple vulnerabilities in SNMPv1 trap handling.***
> *SNMP trap messages are sent from agents to managers. A trap message may indicate a warning or error condition or otherwise notify the manager about the agent's state. SNMP managers must properly decode trap messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP managers decode and process SNMP trap messages".*
>
> ***"VU#854306 – Multiple vulnerabilities in SNMPv1 request handling.***
> *SNMP request messages are sent from managers to agents. Request messages might be issued to obtain information from an agent or instruct the agent to configure the host device. SNMP agents must properly decode request messages and process the resulting data. In testing, the OUSPG found multiple vulnerabilities in the way many SNMP agents decode and process SNMP request messages".*

[8] CERT Coordination Center. "CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the SNMP". 18 Aug. 2003. URL: http://www.cert.org/advisories/CA-2002-03.html

B. Threats[9]

- *Modification of Information* – Accidental or intentional alteration of management information while in transit on behalf of an unauthorized user to cause malicious SNMP operations.

- *Masquerade* – An unauthorized user assuming the identity of a user with appropriate authorization to perform SNMP operations.

- *Message stream modification* – Intentional or accidental delay, re-order, or replay of management information to cause unauthorized management operations.

- *Disclosure* – An unauthorized user capturing a message while in transit to obtain information (e.g., community string) contained in the stream.

- *Denial of Service* – An unauthorized user exploits SNMP vulnerabilities by sending malformed SNMP packets, which may cause a SNMP device to crash, or making it unresponsive.

- *Traffic Analysis* – An unauthorized user able to analyze traffic pattern and use it for malicious intent.

VI. Securing Network Management System

Best Practices

A. Disable Services That Are Not Needed

Today, most organizations use the Internet as a major resource to stay competitive. The Internet connection is where the external (public) network is logically segmented from the internal (private) corporate network. It is very important to understand the types of traffic that should be allowed across this perimeter because it is one of the vulnerable sections in the corporate network where potential malicious attacks may originate. It is highly recommended to block SNMP or consider SNMP filtering at this perimeter. However, there is an exception as some organizations might have a requirement to manage the network connectivity with their business partners. Most likely, this network connection terminates outside the perimeter or at the edge routers of both organizations. In this situation, it is advisable to enable SNMP at the perimeter but only allow the IP address of a trusted Network Management System across the specific network connection. Configuring an access-list to allow a trusted NMS is covered later.

- Disable SNMP using the configure command in Cisco router. This will remove the SNMP management capability of the device.

---

[9] Alcatel. "SNMPv3 Simple Network Management Protocol". Feb. 2003. URL: http://www.ind.alcatel.com/library/e-briefing/eBrief_SNMPv3.pdf
SNMP Research International, Inc. "SNMP Security Pack". 9 July 2003. URL: http://www.snmp.com/products/snmpsecpack.html - Intro

no snmp-server

- Apply an extended access (ACL) to deny protocol UDP, port 161, and 162 at the interface level. This can be done using the following configure commands in Cisco router:

access-list 150 deny udp any any eq snmp
access-list 150 deny udp any any eq snmptrap
access-list 150 permit ip any any

The access-list statement containing "snmp" will prevent snmp messages bound for port 161 from entering the network when it is applied at the perimeter router

The access-list statement containing "snmptrap" will prevent notification messages bound for port 162 from entering the network when it is applied at the perimeter router.

In the example below, access-list 150 is applied to interface serial 1/0 using the following configure commands in Cisco router:

Interface serial 1/0
access-group 150 in

B. Eliminate Default Configuration

Eliminating the default configuration for SNMP community strings is always a good practice. It will prevent unauthorized access by a malicious attacker using the default *public* and *private* community strings for *read only* and *read-write* access. Unfortunately, many network administrators do not change the default SNMP community strings configured in their network devices. Below are examples of how to change the default *public* and *private* community strings in Cisco routers:

no snmp-server community *public* **RO**
snmp-server community *d3onottry!* **RO**

In the above example, the default read only *"public"* community string is removed and replaced with a new password of *d3onottry!*

no snmp-server community *private* **RW**
snmp-server community *d2onotuse#* **RW**

In the above example, the default read-write *"private"* community string is removed and replaced with a new password of *d2onotuse#*

C. Principle of Lease Privilege

Apply the principle of lease privilege by providing the proper levels of access and authorization to trusted users and devices in the network. Applying a community access-list is recommended to control access and authorization level in Network Management System. This will reduce the risk in SNMPv1 and SNMPv2

implementations where community strings are transported in clear text during information exchange. Below is an example of how to implement a community access list in a Cisco router:

```
access-list 11 permit 10.12.14.16
snmp-server community d3onottry! RO 11
snmp-server community d2onotuse# RW 11
```

In the above example, when access-list 11 is applied to the read-only and read-write community strings, it only allows the trusted network management system with an IP address of 10.12.14.16 to access SNMP information on the router.
Best practices also recommend community strings for requests (polling) and notifications (traps) should **not** be the same. This will add another layer of security in combination with other security measures that were already in place. It will help protect the SNMP community strings for read-only and read-write access against unauthorized disclosure when a notification (trap) message is in transit.

```
snmp-server host 10.12.14.16 notsimilar
```

In the above example, the community string "*notsimilar*" is use only for notifications (traps) and will be sent only to host 10.12.14.16

For Cisco IOS, an additional requirement is needed when a different community string is configured for notifications (traps). The router should be set to deny all SNMP requests to prevent notification messages from being viewed or changed using the configured community string. Below is an example of the Cisco router configuration commands:

```
access-list 13 deny any
snmp-server community notsimilar RO 13
```

It is advisable to verify SNMP configuration using the command "**show snmp group**." This command displays the configured community strings for read only, read-write, and notifications, access-lists number, SNMP version of notifications, and security model. Below is an example showing the output of the "show snmp group" command.

```
groupname: d2onotuse#                 security model:v1
readview : v1default                  writeview: v1default
notifyview: <no notifyview specified>
row status: active     access-list: 11

groupname: d2onotuse#                 security model:v2c
readview : v1default                  writeview: v1default
notifyview: <no notifyview specified>
row status: active     access-list: 11

groupname: notsimilar                 security model:v1
```

readview : v1default **writeview: <no writeview specified>**
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active access-list: 13

groupname: notsimilar **security model:v2c**
readview : v1default **writeview: <no writeview specified>**
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active access-list: 13

groupname: d3onottry! **security model:v1**
readview : v1default **writeview: v1default**
notifyview: <no notifyview specified>
row status: active access-list: 11

groupname: d3onottry! **security model:v2c**
readview : v1default **writeview: <no writeview specified>**
notifyview: <no notifyview specified>
row status: active access-list: 11

D. Business Continuity

In today's business environment, companies need to achieve business continuity, where critical business processes, applications, data, and networks are always available for support. Network Management should be one of the critical resources considered in implementing risk mitigation plans. It is advisable to configure a backup Network Management System located in another subnet in the enterprise. The backup NMS should provide a partial or full capability to support the network. Below is an example router configuration allowing for a backup network management subnet.

In the following example, the primary subnet for the Network Management System is 172.16.30.0 and the backup subnet is 172.16.40.0.

```
access-list 16 permit 172.16.30.0 0.0.0.255
access-list 16 permit 172.16.40.0 0.0.0.255
snmp-server community d3onottry! RO 16
snmp-server community d2onotuse# RW 16
```

E. Stay Current

Information security is a continuously evolving process that heavily relies on latest events for prevention and detection. There are many resources where to find the latest updates, advisories, and tools concerning Information Security. The evolution of SNMP is an example of how the SNMP Work Group stays up to date to address the security weaknesses of the earlier SNMP implementations. Vendors are constantly providing patches, upgrades, and recommendations to reduce or eliminate the associated risks from vulnerabilities and threats.

VII. SNMPv3 Overview

The SNMPv3 Management Framework follows the same architecture that was used in versions 1 and 2. The enhancements in security and administration[10] are major improvements from the previous SNMP versions. The SNMPv3 security implementation is simple but it requires an understanding of the new concept of SNMP Entity. This new concept replaced the SNMP Manager and SNMP Client notion in the earlier versions. In the next section, the administrative framework is described to understand the concept of SNMP Entity.

A. Administrative Framework

As shown in Figure 3, an SNMP entity is composed of an SNMP engine and application modules. The SNMP engine employs subsystems to process outgoing and incoming messages, support authentication and encryption, and provide access control. The application modules in the SNMP engine execute SNMP operations similar to the tasks perform by the legacy SNMP manager and SNMP client. Below are functional descriptions of the subsystems and application modules.[11]

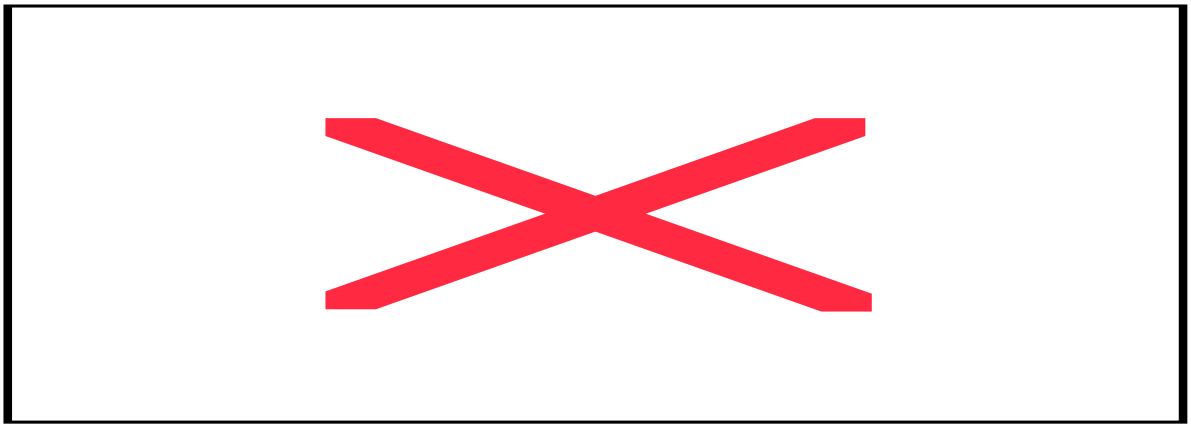

Figure 3: SNMP Entity

- **Dispatcher** – Sends and receives SNMP messages to/from the network. It allows concurrent support of multiple versions of SNMP by acting as interpreter for the different Message Processing models.

- **Message Processing Subsystem** – Prepares or processes SNMP messages for transmission or reception by the Dispatcher. Provides the proper encapsulation (message header) for transmission and de-encapsulation for

[10] Case, J.; Mundy, R.; Partain, D.; Stewart, B. "Request For Comments 2570". URL: http://www.isi.edu/in-notes/rfc2570.txt

[11] Harrington, D.; Presuhn, R.; Wijnen, B. "Request For Comments 2571". URL: http://www.isi.edu/in-notes/rfc2571.txt

Levi, D.; Meyer, P.; Stewart, B.; "Request For Comments 2573". URL: http://www.isi.edu/in-notes/rfc2573.txt

reception of an SNMP message. This subsystem includes message processing models for each versions of SNMP.

- **Security Subsystem** - Provides security services in the form of authentication and encryption. This subsystem is using the User-based Access Model (USM).

- **Access-Control Subsystem** – Provides control mechanism to restrict access to the MIB by authorized principals. This subsystem is using the View-based Access Control Model (VACM).

- **Command Generator** – SNMP application that sends SNMP requests (Get, GetNext, GetBulk, or Set) to retrieve or modify MIB information. It also processes the reply from the command responder.

- **Command Responder** – SNMP application that receives and processes the SNMP requests destined for the local system. It also generates a response to the request initiated by the command generator.

- **Notification Originator** – SNMP application that generates notifications (traps) for specific events or conditions. It is configurable to define the criteria for a trap, destination of the trap, and SNMP version to use.

- **Notification Receiver** – SNMP application that listens to notifications and generates acknowledgment of the receipt for confirmation if required.

- **Proxy Forwarder** – SNMP application that receives and forwards SNMP requests or notifications to/from SNMP entities. The use of proxy forwarder is optional and can be advantageous to save bandwidth as it aggregates the transfer of management information to/from a central location.

The SNMPv3 message format is expanded to support authentication, encryption, access control and co-existence with the earlier versions of SNMP. Figure 4 shows the SNMPv3 message format that conforms to the Message Processing Model and Security Models (User-based Security Model and View-based Access Control Model).

The first five fields of the message header are parameters used in the generation and processing of a message. These message parameters are: (1) SNMP version, (2) unique identifier, (3) maximum size supported by the sending entity, (4) state or condition of SNMP operation, authentication and encryption, and (5) security model. The next six fields of the message header are security components essential in authentication, timeliness verification, and encryption. The last three fields describe the “scoped PDU” which includes the PDU, ContextEngineID, and ContextName. The “scoped PDU” can be encrypted or it can be sent as a plain text and it is where the access control mechanism is applied.

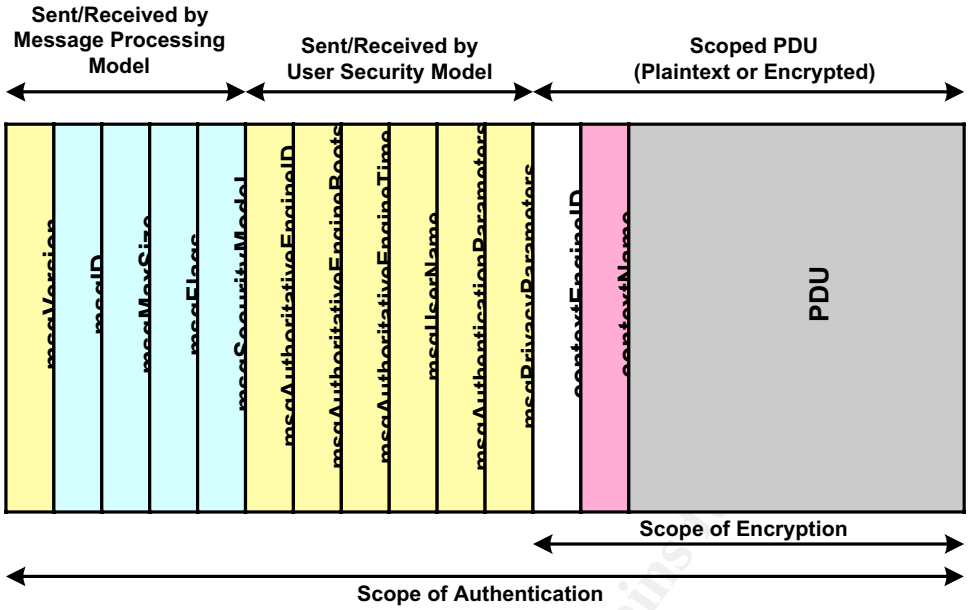

Figure 4: SNMPv3 Message Format[12]

SNMPv3 introduced the concept of EngineID to identify an SNMP entity. An EngineID is a unique identifier configured by a network administrator or manufacturer to an SNMP agent installed in a managed device. Previous SNMP versions rely on IP address or domain name of a managed device, which can be obtained by outsiders and may lead to security risks. The EngineID concept adds another layer in security and is used at two instances in the processing of an SNMP message. First, it is used to create an authentication key and second, to identify the source and destination of the message payload.

ContextEngineID and ContextName are extensions of the EngineID. These extensions are commonly used in complex devices with multiple components or modules. Figure 5 is an example of a Layer 3 Switch with a router module and a supervisor engine. When an NMS polls the switch to retrieve MIB information from the router module, it will use the ContextEngineID of the physical switch, which is the same as the EngineID. Then, the SNMP agent in the switch will use the ContextName of the router module to get the specific MIB information. The same logical approach is taken to get MIB information from the supervisor engine but in this case the switch will use the ContextName of the supervisor engine.

[12] Stallings, William. "Security Comes To SNMP: The New SNMPv3 Proposed Internet Standards". URL: http://www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_snmpv3.html
Harrington, D.; Presuhn, R.; Wijnen, B. "Request For Comments 2572". URL: http://www.isi.edu/in-notes/rfc2572.txt

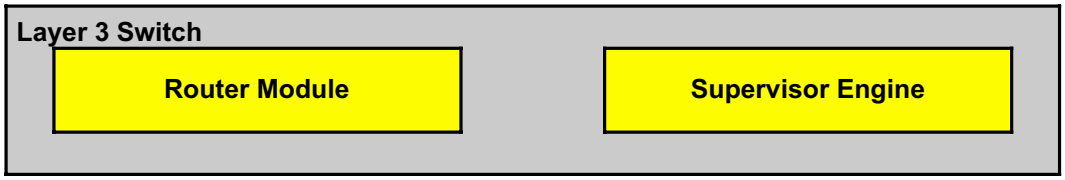

Figure 5: Layer 3 Switch with a Router Module and a Supervisor Engine

B. Security Concept

SNMPv3 security mechanism is based on two design models: User-based Security Model (USM) and View-based Access Control Model (VACM). USM is implemented in the form of **authentication** and **encryption** and VACM in the form of **access control**.

Authentication and encryption are primarily used for message-level security. Access control is a mechanism applied to restrict access to the Management Information Base (MIB). It is similar in the way a network administrator grants access privileges to a user or a group. To deliver security services, SNMPv3 introduces the concept of a principal on whose behalf services are rendered and processing takes place. The term principal can be an individual or a set of individuals, an application or a set of applications, and various combinations thereof.

1. Authentication

The authentication process assures that the message came from a valid message originator, the data was not modified during transit, and the message was delivered in a timely manner.[13] When a message passed the authentication process, it is certain the message came from an authorized origin, the management information was not changed, and the message was not delayed or replayed intentionally.

Authentication is accomplished using a pre-configured secret key that is shared between the sending entity and the receiving entity. Hashing the password of the principal and the EngineID forms a secret key. The secret key is delivered between SNMP entities outside SNMPv3 using a secure data transfer.

The sending entity provides authentication by inserting an “authentication code” in the SNMPv3 message. The “authentication code” is hashed using MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). The code is comprised of the timestamp, secret key, EngineID, and the contents of the message. Upon receipt of the SNMP message, the receiving entity will use the same secret key to compute the value of the “authentication code.” If the computed value is equal to the embedded “authentication code” from the sending entity, then it is assured the message came from an authorized entity and was not altered during transit.

The second aspect of authentication is the timeliness of the message delivery. The timing indicator (timestamp) included in the incoming message is verified upon receipt. The embedded timestamp is examined by the receiving entity by comparing the time

[13] Blumenthal, U.; Wijnen, B. “Request for Comments 2574”. URL: http://www.isi.edu/in-notes/rfc2574.txt

values from its internal clock. The message is rejected if the value exceeds the specified window. Please note that the process of timing synchronization between SNMP entities is beyond the scope of this document.

SNMPv3 User Security Model has three levels and these are listed below:[14]

1. *No Authentication and No Encryption* – This level has no provision for security, privacy, and confidentiality. This is usually used for application development or debugging.

2. *Authentication and No Encryption* – This level requires an authentication from the SNMP entities but encryption of the message payload is not required.

3. *Authentication and Encryption* – This level requires an authentication from the SNMP entities and the message payload needs encryption for confidentiality.

The authentication process is done in both directions to establish trust relationship between SNMP entities.

2. Encryption (Privacy)

The SNMP message is encrypted using DES (Data Encryption Standard) in the cipher block-chaining mode to prevent eavesdropping and ensure privacy of the management information. When encryption is enabled, the administrator issues two sets of passwords to an SNMP entity. The first password is use for authentication and the second password is for encryption (privacy)[15]. The secret "privacy key" is created using the same hash algorithm in the authentication process.

Similar to the authentication process, both the sending entity and receiving entity use the same or shared "privacy key" to encrypt and decrypt the message properly. This will prevent unauthorized persons from getting confidential management information while it is in transit.

Encryption is an option and some companies may not implement it due to bandwidth constraints and associated cost factors. When encryption is enabled there is additional overhead traffic across the network.

3. Access Control[16]

Access Control is a significant enhancement from the earlier SNMP implementations. It addresses the security principle of least privilege. SNMP agents are configured to

---

[14] Routhier, Shawn; Wellens, Chris. "Beginner's Guide to SNMPv3 Security". 2003. URL: http://www.iwl.com/Resources/Papers/snmpv3_security.html

[15] Routhier, Shawn; Wellens, Chris. "Beginner's Guide to SNMPv3 Security". 2003. URL: http://www.iwl.com/Resources/Papers/snmpv3_security.html

[16] Wijnen, B.; Presuhn, R.; McCloghrie, K. "Request for Comments". URL: http://www.isi.edu/in-notes/rfc2575.txt

provide different access levels to its MIB. Authorized principals are restricted based on the control policies defined in the SNMP agents. For example, principals from the operations team are only allowed to read (view) the MIB's, whereas principals from the engineering team can be granted read and write access. Each SNMP agent maintains a pre-configured access control table where security policies are defined for authorized principals.

VIII. Summary

SNMP has become the standard network protocol used for Network Management implementations. Like any network protocol, SNMP has vulnerabilities that could be exploited and threats that could potentially compromise network integrity and stability.

In this document we discussed the importance of securing Network Management, the vulnerabilities and threats surrounding SNMP, how to secure SNMP and how SNMP evolves to address the weaknesses in security and administration. This document also demonstrated the fundamental principles of securing a network (Know your System, Defense in Depth, Principle of Least Privilege and Prevention and Detection) to protect confidentiality, integrity, and availability.

IX. References

SNMP Research International, Inc. “SNMPv3 White Paper”. 21 Feb. 2003. URL http://www.snmp.com/snmpv3/v3white.html

Reference Document. “Simple Network Management Protocol”. 20 Feb. 2002. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm - xtocid2

Reference Document. “Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities”. Revision 2.1. 14 March 2002. URL: http://www.cisco.com/en/US/products/products_security_advisory09186a00800945b4.shtml

CERT Coordination Center. “CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the SNMP”. 18 Aug. 2003. URL: http://www.cert.org/advisories/CA-2002-03.html

Alcatel. “SNMPv3 Simple Network Management Protocol”. Feb. 2003. URL: http://www.ind.alcatel.com/library/e-briefing/eBrief_SNMPv3.pdf

Harrington, D.; Presuhn, R.; Wijnen, B. “Request For Comments 2571”. URL: http://www.isi.edu/in-notes/rfc2571.txt

Stallings, William. “Security Comes To SNMP: The New SNMPv3 Proposed Internet Standards”. URL: http://www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_snmpv3.html

Routhier, Shawn; Wellens, Chris. “Beginner’s Guide to SNMPv3 Security”. 2003. URL: http://www.iwl.com/Resources/Papers/snmpv3_security.html

SNMP Research International, Inc. “SNMP Security Pack”. 9 July 2003. URL: http://www.snmp.com/products/snmpsecpack.html - Intro

Knapp, Laura Jeanne. “SNMP Version 3: Securing Your Management Structure”. URL: http://www.lauraknapp.com/images/snmpv3.pdf

Cohen, Yoram. “SNMP-Simple Network Management Protocols”. URL: http://www2.rad.com/networks/1995/snmp/snmp.htm - snmp

Bay Networks. “SNMP Overview”. 12 April 1996. URL: http://support.baynetworks.com/library/tpubs/html/router/soft1000/snmp/2923A-15.html

Solarwinds. “SNMP Overview and SNMP Security”. URL: http://www.solarwinds.net/Tools/SNMP.htm

Case, J.; Mundy, R.; Partain, D.; Stewart, B. “Request For Comments 2570”. URL: http://www.isi.edu/in-notes/rfc2570.txt

Harrington, D.; Presuhn, R.; Wijnen, B. “Request For Comments 2572”. URL: http://www.isi.edu/in-notes/rfc2572.txt

Levi, D.; Meyer, P.; Stewart, B.; “Request For Comments 2573”. URL: http://www.isi.edu/in-notes/rfc2573.txt

Blumenthal, U.; Wijnen, B. “Request for Comments 2574”. URL: http://www.isi.edu/in-notes/rfc2574.txt

Wijnen, B.; Presuhn, R.; McCloghrie, K. “Request for Comments”. URL: http://www.isi.edu/in-notes/rfc2575.txt