Guideline Policy on the use of SNMP in Read-Only Mode

Dr A.D. Murray
Technical Director

Edition 1.1 - July 2007

Introduction & Scope

If any organization is considering the use of the Simple Network Management Protocol (SNMP) on their network, then they should be aware of the security implications. Indeed every good security policy should contain a section on SNMP because SNMP is supported by nearly every device that can be attached to a computer network and, in some case, it may already be configured and turned on.

This document has been written to provide an introduction to good practice for an organization using the Mutiny Critical Services Monitor, which obtains most of its data use SNMP. It is equally valid for many other devices and systems that operate as SNMP monitors or data collectors, provided that read-only SNMP access is all that is required.

If an organization is considering using a device or system that requires SNMP access in either "write" or "create" modes, then it is beyond the scope of this document. It is recommended that the organization contacts Price Waterhouse Coopers (http://www.pwc.com/) or a similarly experienced and qualified IT consultancy.

Terminology

The following terminology is used in this document:

SNMP – The simple Network Management Protocol was initially defined by the IETF (http://www.ietf.org) in RFC 1157. It is widely supported and implemented by most organizations deploying TCP/IP-based networks.

Network Node - Any network-attached device that has an IP address.

Monitoring **-** The remote collection of system parameters and statistics from a network node.

Management - The remote control and modification of operating parameters on a network node.

NMS - A Network Management System is a device or system that uses SNMP (and other protocols) to monitor (and sometimes manage) network nodes.

SNMP Client - A software (or firmware) agent that runs on the network nodes. Its purpose is to respond to valid SNMP requests from the NMS and send out other SNMP information.

SNMP v1 - The original version of SNMP is still the most widely supported and implemented. Because of security weaknesses, it must not be used for management (see later).

SNMP v2c - This is defined in RFC 1905-1907 and is officially "experimental". It improves on the efficiency of SMP v1, but does not improve on its security and so it should also not be used for management functions. SNMP v2c is supported by most manufacturers (including Microsoft in Windows 2000/2003/XP).

SNMP v3 - This is a secure version of SNMP that can be used for management. It is supported by the major network vendors such as Cisco, but otherwise it is not widely implemented in the LAN environment.

Community String - (Also Community). The Community acts a type of password for SNMP. The Community strings are stored in the SNMP configuration of the SNMP client and it will only respond to SNMP requests from an NMS if it the requesting IP packet contains a matching Community String. Note that Community strings are case-sensitive.

With each Community string, there is an associated level of access to the network node which defines the management functions that can be preformed by the NMS on the network node. The most common of these are:

- Read-only - No SNMP management is allowed with this Community. SNMP information can be returned to the NMS, but it cannot be modified.
- Write - Existing data in the SNMP tables on the network node can be modified.
- Create - New entries can be created in the SNMP tales on the network node.

These modes of access can sometimes be combined under a single Community (e.g. Read/Write).

It is commonly believed that there are two "default" Community Strings:

public	- Read-only
private	- Read/Write

This is not strictly true, but these two community strings are widely used and configured as defaults on a range of devices that support SNMP v1.

In SNMP v1 and SNMP v2c, the Community String is transmitted across the network in clear text (i.e. it is not encrypted). This makes these protocols unsuitable for network management functions and use of these protocols should be restricted to monitoring (Read-only access). In SNMP v3 the SNMP packets can be encrypted and this protocol is suitable for management functions.

Access-Control lists - On a large number of devices that support SNMP, a second tier of security is provided by Access Control Lists. This is a simple list of IP addresses (or DNS names) that can be configured into the SNMP client. The network node will only respond to SNMP requests that are sourced from an IP address that is on the access-control list. Other SNMP requests will be ignored. Access-control lists should be restricted to contain only the IP addresses of the valid NMS for each network.

Classes of Network Node and SNMP threats

We can break down the network nodes that are monitored by an NMS into 4 distinct types:

Type A - Devices with an operating system. Examples include Windows Servers and workstations, UNIX systems and Novell servers. In this type of device, the SNMP client is installed as a service or process running with the operating system. The device may also support hardware-specific SNMP extensions (e.g. HP SIM or Dell OpenManage). The greatest threat posed by unauthorised SNMP read-only access to this type of system would be posed by the list of running processes or applications. This in itself is not a security risk, but it may allow the hacker to see vulnerable processes or applications to assist in targeting an attack.

Type B - Intelligent network devices such as switches or routers. Examples include Cisco, Extreme and Juniper. The greatest threat posed by unauthorised SNMP read-only access would be posed by access to the routing tables and the IP address ranges in use.

Type C - Simple network devices such as managed switches. Examples include HP proCurve, 3Com, ADSL routers etc. The greatest threat posed by unauthorised SNMP read-only access would be posed by access to the IP address ranges in use.

Type D - Other devices such as printers, environmental monitors UPS systems etc. The greatest threat posed by unauthorised SNMP read-only access would be posed by access to device-specific information such as toner levels, temperatures, battery life.

Type E - Security devices such as firewalls. All access to this type of device will be controlled by the site security policy and is therefore outside the scope of this document. The greatest threat posed by unauthorised SNMP read-only access would be posed by access to the IP address ranges in use on the network.

SNMP Configuration Guidelines

This section contains some recommendations for setting up SNMP on the 5 basic types of system defined in the previous section. If these are followed, then there will be little additional risk posed by the use of SNMP in read-only mode. In order to exploit SNMP, the hacker will have to first have to break the physical security of the network and the compromise a host on that network. The organisation's Security Policy should address these issues.

Type A - Chose Community strings using standard password rules (see Appendix). Use access control lists to define only the authorised NMS systems for each host. Wherever possible, place a firewall between the Network Node and the NMS (e.g. place hosts in a DMZ). Use the Firewall rules to control SNMP access between the Network Nodes and the NMS.

Type B - As Type A, but use different Community strings wherever possible.

Type C - Change the Community String from "public" if this is the default. Make sure that there are no "Write" or "Create Community Strings. If the system allows, use access control lists to define only the authorised NMS systems for each host.

Type D - Most of these systems will have the "public" community string set as a default and this represents little risk, so it will be easier to leave this. Make sure that there are no "Write" or "Create Community Strings. If the system allows, use access control lists to define only the authorised NMS systems for each host.

Type E - Do not allow SNMP access to these devices unless your Firewall Security Policy allows it.

Appendix – Rules for Selecting Community Strings

- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your car, the name of the street you live on, etc.

- Don't use a password of all digits, or of all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a community shorter than six characters.
- Use a community with mixed-case letters.
- In theory any printable characters can be used, but it may be best to only use letters and digits as not all characters are allowed by some systems.
- Use a community that is easy to remember, so you don't have to write it down.
- Use a community that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Further Reading

"Essential SNMP", D.R. Mauro & K.J. Schmitt, O'Reilly & Associates, 2001

"Simple Network Management Protocol (SNMP)", Cisco Systems Inc., http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

"HOW TO: Configure the Simple Network Management Protocol (SNMP) Service in Windows Server 2003", Microsoft Corporation, http://support.microsoft.com/kb/324263

"RFC 1155 - Structure and Identification of Management Information for TCP/IP-based Internets", The Internet Engineering Task Force, http://www.ietf.org/rfc/rfc1155.txt?number=1155

"RFC 1157 - A Simple Network Management Protocol (SNMP)", The Internet Engineering Task Force, http://www.ietf.org/rfc/rfc1157.txt?number=1157

"RFC 1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", The Internet Engineering Task Force, http://www.ietf.org/rfc/rfc1157.txt?number=1905