# Global Information Assurance Certification Paper

# Securing SNMP in Windows

## SNMP overview

Simple Network Management Protocol (SNMP) is used to monitor, configure and send alarms from network-enabled equipment. It consists of two parts: the SNMP manager and the SNMP agent.

The SNMP manager software is typically a GUI interface (though there are command line programs that will do similar things) that shows the "state of the network." The manager retrieves configuration and performance counters from the agent software by issuing *get* commands. It can also change a network element's configuration by sending a *set* command (provided the appropriate permissions are set).

The SNMP agent responds to set and get commands issued from a management software with the correct community code. On Windows NT the agent retrieves information from the registry and converts it to the accepted format for SNMP. Agent software also has the ability to send an alarm or trap to the management console (or whatever IP address it's configured).

SNMP agents use a Management Information Base (MIB) to determine what traps are sent and what performance counters are used. These MIBs are the foundation for reporting and sending traps.[1]

If SNMP is installed on Windows NT after the application of service pack 3 or later you **must** reinstall the service pack. Microsoft recommends reinstalling service packs after installing any software, but in this situation it is mandatory as there is a .dll incompatibility that will cause the SNMP service to fail to start. Reapplication of the service pack fixes this problem.

## Built in Security

The security implementation in SNMP is very primitive. SNMP run over UDP port 161 (traps are sent over UDP 162). Authentication is accomplished through the use of a community name (or string). The community string is sent along with the SNMP command. The community string is then compared to the list the agent contains; valid permissions are checked for the community and if all is in order the command are executed.

The default community name in Windows NT, and in general, is "public," as specified in RFC 1157, although some vendors are setting the default community as "private." These two as well as an empty community string are well known and the first that will be tried.

[1] For more information on MIBs see: RFC 1213 and RFC 1155.

This shared password is transmitted in clear text, as part of the UDP package, so simply sniffing the network will reveal the community.

## Default Install

With a default install of Windows NT 4.0 with SNMP the default community is set (public) and the default (and only) settings are Read/Write. This allows any and all to issue a command such as:

```
SNMPUTL walk hostname public .1.3.6.1.4.1.77.1.2.25
```

The user will receive a listing of all usernames on the machine (or Domain if a DC is targeted). SNMPUTIL is a program that ships with the Windows NT resource Kit. Another potential exploit is:

```
snmpset –v 1 ipaddress public .1.3.6.4.1.311.1.2.5.3.0 a
```

This will erase all entries in the WINS database. SNMPSET is a UNIX command using the CMU SNMP development kit. The potential for harm is easily grasped.

## Securing SNMP in Windows NT

The next question is: How does one go about securing SNMP in Windows NT. The solution is fivefold.

### *Ports*

The very first thing that should be done is to block port 161 and 162 UDP on your firewall or gateway. SNMP utilizes port 161 to issue and respond to SNMP queries and commands. Port 162 is used to send trap messages. Port 161 should be set to block both inbound and outbound, thereby preventing someone from sending or receiving information on these ports. Port 162 should be blocked for outbound at the least. If systems were compromised, or a user changes the parameters, traps could be sent out of the network.

If you really need control over where and where not messages are sent these ports could be filtered on the routers of various subnets to contain them on one or a few subnets. For example one could block 161 and 162 on all routers except the server's subnet and the monitoring station's subnet to monitor only the servers and to keep "adventurous" users from sending and receiving SNMP packages.

### *Community String*

Change the community string. By default the community string of "public" is installed and active (with Read/Write access). This is not an oversight, but expected behavior (see RFC 1157) and easily overlooked. Set a new community string and be sure to delete the

"public" community string. Public, private and NULL are the three most common public strings and should never be used.

## *Install Service Pack 4 or better*

The option to set a community to 'Read Only' is **not** available on the default install. To change the default community to an option other then Read/Write service pack 4 or later must be installed. Remember, if the SNMP service was installed after a service pack, the service pack **must** be reinstalled or the SNMP service will not operate.

After installing service pack 4 or greater the option to set permissions by community string becomes available under: `"Control Panel" -> "Network" -> "Services" -> "SNMP, properties" -> "Security tab"`. Different permissions for different communities can be set. The options are Read/Write (default), Read Only, and Read/Create (the default setting for Windows 2000 is Read Only). Try to set these strings to "Read Only" (perfect if you're just monitoring systems). If you are using SNMP to manage the systems use one community set to "Read/Write" to make changes and another set to "Read Only" for normal monitoring activities. This will cut down on the exposure of the "Read/Write" community string.

## *Use a packet filter*

In the SNMP properties window there is an option to set packet filters. This allows an administrator to determine what IP addresses a machine is allowed to communicate with by community. After selecting a new community name and setting the permissions for the string, one can add valid IP addresses for that community string. As many IP addresses can be added as needed and one IP address can be a member of as many community strings as there are defined.

To set the packet filtering options go to `"Control Panel" -> "Network" -> "Services" -> "SNMP, properties" -> "Security tab."` Select the community string, check the "accept packets from these IP's only, type in the IP address in the box and click add. Repeat as necessary.

This doesn't prevent IP spoofing but it does prevent the responses from being sent to another machine. Unless the perpetrator has a sniffer on one of the subnets issuing a get will do them no good. They could, however, issue a set command with a spoofed IP that would be accepted if it were sent using a Read/Write community string.

## *Secure the registry and .dll*

The last step is to secure the registry. This is important as a user could edit the registry directly and modify the settings for SNMP and the .dll files associated with the MIBs. The other part of this section is securing the .dll files (the MIBs) directly. These files need to be protected to prevent the introduction of a trojan horse or other mischief.

The registry keys that need to be changed are:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\DHCPMibAgent
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\LANManagerMIB2Agent
HKEY_LOCAL_MACHINE\Software\Microsoft\RFC1156Agent
HKEY_LOCAL_MACHINE\Software\Microsoft\SNMP
```

as well as any other keys with MIB pointers. These registry entries will point to the associated files in the (typically) %systemroot%\system32 directory. These files should be set to Read and Execute permissions for the system and administrator, and no access permissions set for everyone and other accounts.

The following registry keys should be fine with the default settings, but you may want to check them:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMPTRAP
```

## *Summary*

The five basic things that need to be done to secure SNMP in Windows NT are:

- Ports: secure ports 161 and 162 on the network and at routers.
- Change community string and set permissions.
- Install the latest service pack (at leas service pack 4).
- Activate various packet filters.
- Secure registry keys and .dll files.

Be sure to reinstall any service pack you have if you install the SNMP service after applying the service pack, as there are conflicting files that will cause the service to fail to start.

## References

Taylor, Paul. "Enterprise Integration Using SNMP." Enterprise Integration Using SNMP Feature Article, July 1998 by Paul Taylor. July, 1998. URL:
http://www.ntsystems.com/db_area/archive/1998/9807/207fe2.shtml (8/22/2000)

Network Associates, Inc. "Windows NT SNMP Security Permissions." COVERT Research Center Windows NT SNMP Security Permissions. November 17, 1998. URL:
http://www.pgp.com/research/covert/advisories/030.asp (8/22/2000)

Shiva. "What is SNMP?" Shiva SNMP Reference. URL:
http://www.shiva.com/prod/docs/archive/netmod/11_snmpf.html (8/22/2000)

Rouland, Christopher. "SNMP holes in Windoze NT 4.0."(sic) October 8, 1998. URL:
http://www.insecure.org/sploits/NT.snmp.domain_users.record_deletion.html (8/22/2000)

NetIQ Corporation. "Troubleshooting tips for Hardware category products" URL:
http://www.netiq.com/support/hrdwrtips.asp (8/22/2000)