Security Exposures with Simple Network Management Protocol

Korba, Larry

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

*Security Exposures with Simple Network Management Protocol **

Korba, L.
January 1999

* published in The Insider, 3(1). January 1999. NRC 41623.

Canada

Security Exposures with Simple Network Management Protocol[1]

Larry Korba

National Research Council of Canada
Larry.Korba@iit.nrc.ca

Abstract

Simple Network Management Protocol (SNMP) has become the standard for managing networks. Recently, there has been considerable activity within security-related e-mail lists regarding newly discovered security liabilities associated with many installed SNMP implementations. This article sheds some light on SNMP, providing an overview of its operation, and an outline of its development. It also describes security issues associated with SNMP from a network manager's perspective and provides recommendations in light of these issues.

Background

For most LANs, the current network management approach is modeled on an object-based, manager-agent approach using Simple Network Management Protocol. Developed about 10 years ago through the Internet Engineering Task Force (IETF) as a stop gap measure for network management, SNMP has superceded the standard that was to have been world dominant; Common Management Information Protocol (CMIP). The reason for its rapid acceptance is its simple but effective design. SNMPv1 is easily implemented, and offers a low-overhead protocol for remote management of multi-vendor routers, servers, hubs, workstations or any other network resource [1].

The Network Management Framework for SNMP is defined in several IETF request for comments (RFC) documents [1]. Information concerning the operation and control of each Network Element (NE) is contained within a Management Information Base (MIB). A software program called an SNMP Agent, usually operating within the computing environment of the Network Element provides a means for accessing and altering MIB objects associated with a NE. The SNMP Agent acts upon commands from a management process. Communication between the Manager process and the SNMP Agent follows the Simple Network Management Protocol. In essence, the MIBs of all NEs form a distributed database. The SNMP Agent does not make any decision or start any management activity on its own. Typically, a centralized management process communicates with the SNMP Agents of a network to obtain information about and control operational aspects of Network Elements.

Every NE will have some standard and some manufacturer-specific objects within its MIB. MIB object groupings are standardized across systems of particular classes. All routers for instance, conform to the router MIB as defined in IETF RFC 1812. Individual manufacturers may provide access to additional vendor-specific functionality and provide network management access to those functions with MIB extensions. MIBs are defined using Abstract Syntax Notation language (ASN.1). ASN.1 is a standard, international language for describing structured information. Often this information is conveyed across some interface or communication medium. It is a higher level language that provides an object-oriented approach for dealing with communication protocols

Schematically the operation of a network management environment using SNMP version 1 is shown in Figure 1. As an application layer protocol, SNMP uses User Datagram Protocol (UDP) as its Transport Layer. SNMP v1 defines five message types:

1. GET-REQUEST: Fetch the value of one or more objects,
2. GET-NEXT-REQUEST: Fetch the next value after one or more specific variable.
3. SET-REQUEST: Set the value of one or more variables,
4. GET-RESPONSE: Returns the value of one or more variables (i.e. response to management commands 1-3), and
5. TRAP-RESPONSE: Notify the manager when something happens within the NE associated with the agent.

The manager uses port 161 to send its three request types via UDP, while the agent sends its traps via UDP on port 162. To properly interpret objects managed by SNMP agents, the Network Management station must have access to the MIB definitions handled by the agent.

[1] NRC paper number 41623

Creation of an SNMP agent first involves compiling the MIB ASN.1 definitions to create C language source code for the core of the Agent using a MIB compiler. The second part of the process requires the addition of C language code to access the registers in the hardware or to perform the calculations required for formulating the value of MIB objects.

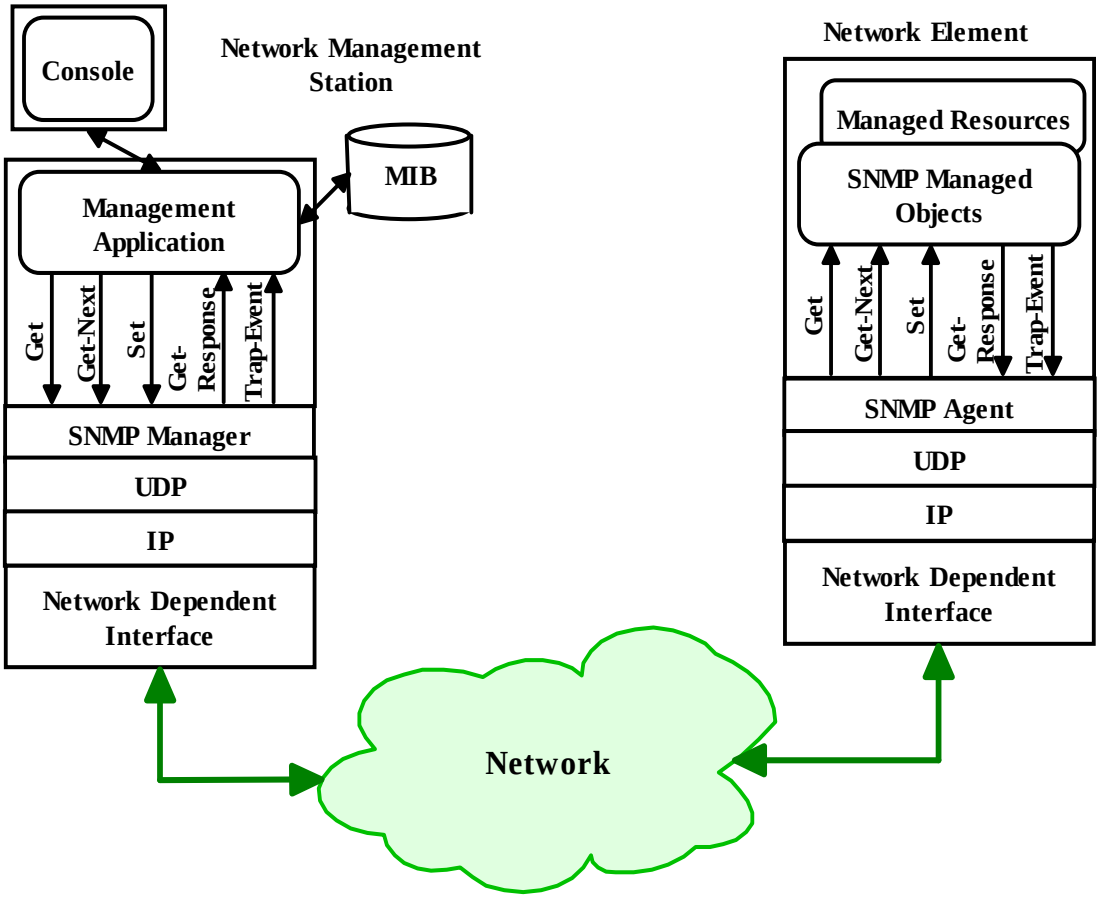

Figure 1. SNMP environment for Network Management

SNMP v1, v2, v3

The transition of SNMPv1 [1] to Version 2 [2], [3], [4], [5], [6] was not smooth or without controversy. In the references section you will find information regarding documents pertaining to the different versions of SNMP. Below is a synopsis of the development of SNMPv1.

Security problems related to SNMPv1 design were well understood. The first attempt to correct those problems became SNMPsec. No commercial packages were made available with SNMPsec. SNMPv2p or "party-based" SNMP updated SNMPv1 for the Management Interface, protocol and security. The security approach was based mainly on SNMPsec. This version was considered too complicated and saw little application. SNMPv2c, the "Community-based" version 2 of SNMP, deploys SNMPv1's community string authentication, but incorporates the added management commands of SNMPv2. This version began to gain momentum for acceptance in 1997. SNMPv2u, employs a "user-based" security model. SNMPv2*, developed by SNMP Research, combines features of SNMPv2u and SNMPv2p to provide a more manageable, strengthened security solution for SNMPv2. Neither SNMPv2u nor SNMPv2* has been extensively deployed.

All flavors of SNMPv2 and the new SNMPv3 [7], [8] support the following key features:

1. COUNTER64: A new 64 bit counter object, SNMPv1 is limited to 32 bit counters.
2. GET-BULK-REQUEST: A new Packet Datagram Unit to allow a manager to retrieve large blocks of data more efficiently as compared to SNMPv1.
3. INFORM-REQUEST Packet Datagram Unit allows one manager to send information to another manager.
4. Two new MIBs were defined to support SNMPv2 (SNMPv2 MIB) and manager-to-manager communication (SNMPv2-M2M).

The lack of a single specification for SNMPv2 led to the absence of a ubiquitous approach for securing SNMP transactions. To remedy this situation, committee work started in earnest on SNMPv3 in 1997. By January, 1998, the standards committee had settled on and published a key set of proposed standards. Rather than being a replacement for earlier SNMP versions, SNMPv3 defines a security facility for use in conjunction with SNMPv2 and SNMPv1 [9]. Presently, there are at least two

products available to support this new release: SNMP Research International Inc. [10] and AdventNet's web-based management packages [11]. SNMPv3 concentrates on strengthened security for SNMP, specifying MD5 (Message Digest 5, a one way hash function) for digital signing of SNMP datagrams, DES in Cipher Block Coding for symmetrical encryption of transactions, timing constraints for responses to requests, and administration standards. While DES encryption with 56 bit encryption key size is considered inadequate by today's security standards [12], a managed site implementing SNMPv3 would be difficult for a "low budget" hacker to attack. The key element in favor of the eventual widespread use of this version is that there is only one version 3.

Today, SNMPv1 and SNMPv2c have been widely deployed within network elements. It is used in virtually every management platform and managed device available today. Other, more secure variants of SNMPv2 are not used because of the lack of a clear security standard for version 2, and the simplicity of SNMPv2c. Since version 3 has only been recently introduced as a standard, there are very few agent or management station implementations available.

The key problems related to SNMP security pertain to SNMPv1 and SNMPv2c. Although version 3 of SNMP has provisions for more secure authentication and message interchanges, it will take considerable time for it to reach significant deployment. There will also be some reluctance to change to version 3, because of concerns over complications in the transition since both SNMP agents and network manager software must be upgraded for its support and the requirement for key management.

Security Problems with SNMPv1 and SNMPv2c

Principal security threats with which systems are analyzed include:

1. Disclosure: observing exchanges between manager and agents to learn the values of MIB objects,
2. Masquerading: unauthorized operations by a NE assuming the identity of the Management Station,
3. Modification of Information: altering in-transit messages to produce unauthorized operations,
4. Message Stream Modification: recording and replaying messages to perform unauthorized operations,
5. Traffic Analysis: observation of the traffic between management station and agents,
6. Denial of Service: preventing exchanges between management stations and agents.

No version of SNMP protects management components against Traffic Analysis or Denial of service. SNMP v3 provides a solution for the other threats, while SNMPv1 and SNMPv2 may be has security exposures through these threats. Rather than deal with each threat separately, this paper examines how several combined threats may be exploited to perform unauthorized operations. In additional to the above threats SNMPv1 and SNMPv2 have security exposures due to implementation errors.

Attack by Masquerading, Message Stream Modification, Traffic Analysis and Disclosure

A security issue related to all versions of SNMP is the UDP as a transport mechanism. UDP is connectionless. It was chosen as the transport layer for SNMP to preserve its simplicity. It was thought that a simple connectionless protocol would have a better likelihood of operation when a network is damaged.

The IP header of the SNMP packet includes the source address (Figure 2)[13]. It is easy to spoof the network manager source address using raw sockets in the construction of the SNMP packet (Masquerading via Message Stream Modification). By monitoring network traffic, one can determine a network management host address (Traffic Analysis and Disclosure). Network Management software typically use the ICMP ping command and SNMP GET-REQUESTS to discover the network. Periodically a network discovery daemon polls each node in its management domain to determine the connection and the identification of network elements. By simply monitoring and examining ICMP ping and SNMP GET-REQUESTS, the intruder may determine the address of the management workstation. With such an attack, the spoofing station will not receive a response from the agent. This of course is of little consequence to the attacker. If the intent of the attacker is to disable a router or other network element, all the attacker needs to do is send a SET-REQUEST command to the target agent. A response from the agent is irrelevant.

Attack by Masquerading, Disclosure

The authentication scheme used in forms another serious security problem. SNMPv1 and SNMPv2 may authenticate users on the basis of the source address (the agent may be arranged to only respond to requests only from a list of Internet addresses) and the use of a

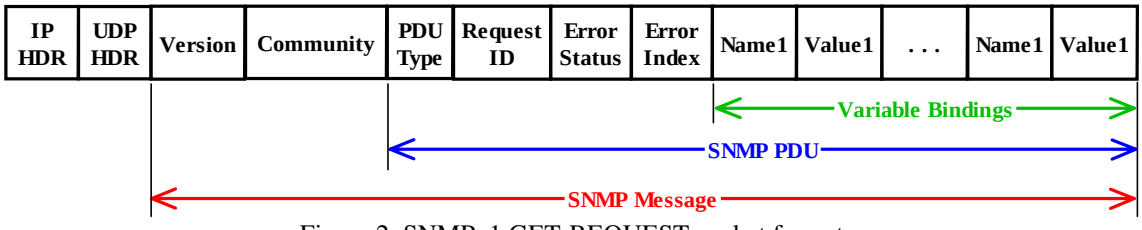

Figure 2. SNMPv1 GET-REQUEST packet format

"Community-Based Authentication" name.

Figure 2 illustrates the format of a typical SNMPv1 packet. The community name is expected as part of every SNMP message. The community name is passed in clear (unencrypted) text. An attacker need only use a packet analyzer software tool (sniffer, such as the UNIX snoop command) to filter for SNMP commands (UDP packets sent to port 161 of a target node) on the segment of interest. Every SNMP packet will contain a community name.

If sniffing a network is not possible, an attacker may simply guess the community password. The default password is "public". The network administrator may not have changed the default community name, through simply not realizing the exposure of such an omission or just being too busy. By scanning network elements in a network branch using "public" as the community name within an SNMP message, an intruder may determine which Network Elements are accessible. If the topology of the branch is known, a password-guessing program may attack SNMP passwords for the network elements. As with most password attacks, combinations of characters that include the name of the device, and/or the name or initials of the system administrator are the most logical starting points.

Attack using Implementation Errors

There is another and simpler way for an intruder to gain access to many SNMP agents. The technique involves the use of hidden manufacturer passwords. This security hole has been discovered recently (BUGTRAQ listserv). Some manufacturers of SNMP agents for network elements (3COM, HP, SUN, Microsoft) have included "back door" community names in their SNMP agent implementations. The hidden community name is part of the binary of the SNMP agent, and cannot be changed without a patch for the SNMP agent. Equipped with these passwords, a user may access (remotely, in some cases) a number of key MIB objects. The attacker may simply want to gain more information about network topology, or to determine how the network element is being used and by which computers. There have been reports of the possibility of accessing the NT Server SNMP agent to list the names of all users remotely and/or deleting all records in the WINS database, bypassing all Windows NT security. The latter operation would effectively shut down a large NT infrastructure.

Hubs and routers have MIB objects that control details concerning their operation. An intruder could determine information about network services accessed by specific network elements, e.g. routing tables. Changing the values of some MIB objects may make the network element inoperable. For instance those objects controlling filtering within the bridge MIB (RFC 1493) could be modified to limit the types of packets the bridge will pass. This action could render the network useless resulting in a denial of service attack on the whole network.

While researching SNMP security threats, the author developed a Java-based prototype for probing portions of networks to find weak SNMP security. The package tests a range of IP addresses for SNMP connectivity, using a dictionary attack on the community name. All SNMP-enabled computers on the subnetwork tested accepted GET and SET-REQUESTS using the community name "public". The simple test led to informing a tightening of SNMP access permissions, a regularly changed community name, and preventing SNMP activity across the firewall.

Recommendations

Network managers rely upon SNMP to make their job easier. If they are not using one of the more sophisticated network management tools, for automated analysis, diagnosis or configuration, they are using SNMP-based tools or browsers to remotely configure specific network elements. SNMP agents operating on computers offer a network manager a remote means for determining resources available and hardware configurations. PC MIB extensions provide a way to monitor applications. Unfortunately, the security problems associated with using SNMP are significant. In dealing with this issue, it is important to review the Security Policy of your organization in light of the potential risks of attack when using SNMP for network element monitoring and remote configuration. As with any security exposure, it is vital to take a holistic approach to finding a solution. Weigh the risks against the benefits of any policy change regarding SNMP deployment.

Approaches to dealing with the problems are:

1. Disable all SNMPv1 and SNMPv2c agents. With this approach, Network Elements would be configured at their respective consoles. This is a drastic approach, but the safest. It may not be possible because your organization relies heavily on network management for their network operation. In these cases consider the following:
2. Ensure that all of the latest patches have been applied to your network management station and all network elements. Some patches deal specifically with SNMP and other security-related problems. Apply the patches as soon as they become available.
3. If your network is connected to the Internet, ensure that your firewall is configured and operating properly to disable outside access to SNMP.
4. Monitor your network activity logs for what might be unauthorized or unusual access to SNMP objects. You might filter for access to UDP port 161 from client addresses other than those used by the network manager.
5. Change the community passwords of your network elements to hard-to-guess private names. Change these passwords often.
6. If you are using an Intrusion Detection System, configure it to monitor unauthorized or unusual SNMP activity.

7. Keep track of security-related announcements on email lists (e.g. BUGTRAQ [13], NTBUGTRAQ [14] and CERT[1] [15]).
8. Plan for a move to a more secure approach to handling SNMP. SNMP Research International for instance, has cooperated with Hewlett-Packard to develop an SNMP Security Pack [9]. This package deploys SNMPv3 for HP OpenView. Within the next year or two there will be more products offering SNMPv3 or other solutions for specific network elements or platforms. Note that management stations and network elements will require upgrading for SNMPv3. For network elements with embedded operating systems and SNMP agents, contact your vendor for information about SNMPv3 availability.

The implications of the security problems associated with using SNMP are serious. Even though the problems associated with SNMPv1 and SNMPv2c were understood when it was first developed, SNMP was embraced and deployed to promote centralized network management. With the existing security risks of SNMP, the recent exposure of implementation-related issues and the concomitant attention of this exposure, network managers must quickly take precautions to protect their SNMP-enabled networks.

References

[1] SNMPv1 Framework (key RFCs):

1155 - Structure of Management Information (SMI) ftp://ftp.isi.edu/in-notes/rfc1155.txt;

1157 - Simple Network Management Protocol (SNMP) ftp://ftp.isi.edu/in-notes/rfc1157.txt;

1212 - Concise MIB definitions ftp://ftp.isi.edu/in-notes/rfc1212.txt; and,

1213 - Management Information Base (MIB-II) ftp://ftp.isi.edu/in-notes/rfc1213.txt.

other support SNMPv1 RFCs

1089 - SNMP over Ethernet ftp://ftp.isi.edu/in-notes/rfc1089.txt

1140 - IAB Official Protocol Standards ftp://ftp.isi.edu/in-notes/rfc1440.txt

1147 - Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices ftp://ftp.isi.edu/in-notes/rfc1447.txt

1156 - (Historic) Management Information Base Network, Management of TCP/IP based internets ftp://ftp.isi.edu/in-notes/rfc1156.txt

1158 - Management Information Base Network, Management of TCP/IP based internets: MIB-II ftp://ftp.isi.edu/in-notes/rfc1158.txt

1161 - (Historic) SNMP over OSI ftp://ftp.isi.edu/in-notes/rfc1161.txt

1187 - Bulk Table Retrieval with the SNMP ftp://ftp.isi.edu/in-notes/rfc1187.txt

1215 - (Informational) A convention for Defining Traps for use with the SNMP ftp://ftp.isi.edu/in-notes/rfc1215.txt

1224 - Techniques for Managing Asynchronously-Generated Alerts ftp://ftp.isi.edu/in-notes/rfc1224.txt

1270 - (Informational) SNMP Communication Services ftp://ftp.isi.edu/in-notes/rfc1270.txt

1303 - (Informational) A convention for Describing SNMP-based Agents ftp://ftp.isi.edu/in-notes/rfc1303.txt

1470 - (Informational) A Network Management Tool Catalog ftp://ftp.isi.edu/in-notes/rfc1470.txt

1418 - SNMP over OSI ftp://ftp.isi.edu/in-notes/rfc1418.txt

1419 - SNMP over AppleTalk ftp://ftp.isi.edu/in-notes/rfc1419.txt

1420 - SNMP over IPX ftp://ftp.isi.edu/in-notes/rfc1420.txt

[2] SNMPsec (Historic, not implemented)

1351 - SNMP Administrative Model ftp://ftp.isi.edu/in-notes/rfc1351.txt

1352 - SNMP Security Protocols ftp://ftp.isi.edu/in-notes/rfc1352.txt

1353 - Definitions of Managed Objects for Administration of SNMP Parties ftp://ftp.isi.edu/in-notes/rfc1353.txt

[3] SNMPv2p (Historic, not implemented):

1441 - Introduction to SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1441.txt;

1442 - SMI for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1442.txt;

1443 - Textual Conventions for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1443.txt;

1444 - Conformance Statements for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1444.txt;

1445 - Administrative Model for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1445.txt;

1446 - Security Protocols for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1446.txt;

1447 - Party MIB for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1447.txt;

1448 - Protocol Operations for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1448.txt;

1449 - Transport Mappings for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1449.txt;

1450 - MIB for SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1450.txt;

1451 - Manager-to-Manager MIB ftp://ftp.isi.edu/in-notes/rfc1451.txt; and,

1452 - Coexistence between SNMPv1 and SNMPv2 ftp://ftp.isi.edu/in-notes/rfc1452.txt.

1. CERT is registered in the U.S. Patent & Trademark Office

[4] SNMPv2c (SomeImplementation)

1901 - Introduction to Community-based SNMPv2

1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)

1906 - Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)

[5] SNMPv2u

1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)

1906 - Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)

1909 - An Administrative Infrastructure for SNMPv2

1910 - User-based Security Model for SNMPv2

[6] SNMPv2*

Developed by SNMP Research. http://www.snmp.com/v2status.html

[7] SNMPv3 Framework (Drafts):

User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-usm-v2-02.txt

Introduction to Version 3 of the Internet-standard Network Management Framework http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-intro-02.txt

View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-vacm-01.txt

An Architecture for Describing SNMP Management Frameworks http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-arch-01.txt

SNMPv3 Applications http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-appl-v2-01.txt

Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-coex-01.txt

Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) http://www.ietf.org/internet-drafts/draft-ietf-snmpv3-mpc-01.txt

[8] SNMPv3 (RFCs)

2271 - An Architecture for Describing SNMP Management Frameworks ftp://ftp.isi.edu/in-notes/rfc2271.txt

2272 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) ftp://ftp.isi.edu/in-notes/rfc2272.txt

2273 - SNMPv3 Applications ftp://ftp.isi.edu/in-notes/rfc2273.txt

2274 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) ftp://ftp.isi.edu/in-notes/rfc2274.txt

2275 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) ftp://ftp.isi.edu/in-notes/rfc2275.txt

[9] W. Stallings, SNMPv3: A Security Enhancement to SNMP. IEEE Communications Survey, Fall, 1998, http://www.comsoc.org/pubs/surveys/4q98issue/stallings.html

[10] SNMP Research International, Inc. SNMP Security Pack http://www.snmp.com/snmpsecpack.html

[11] B. Schneier, "Applied Cryptography." John Wiley & Sons, 1996.

[12] W. Richard Stevens, "TCP/IP Illustrated, Volume 1." Addison-Wesley Publishing Company, 1994.

[13] BUGTRAQ List listserv@netspace.org

[14] NTBUGTRAQ List listserv@listserv.ntbugtraq.com

[15] CERT Coordination Center http://www.cert.org/ , cert-advisory-request@cert.org