Security issues and vulnerabilities of the SNMP protocol

P. Chatzimisios

School of Design, Engineering and Computing, Bournemouth University, UK

Abstract: Currently, communication networks are composed of many interconnected heterogeneous resources and network management plays a critical role. A complete network management solution must be simple, intuitive, easy to use and consistent. It also should ensure ease of deployment, security and the ability to deploy additional solutions quickly. Especially, the security of the network management is probably the most important attribute since it is likely to affect the total security of a system. In this paper, we attempt to shed some light on many issues involved with the security of network management by exploring the security vulnerabilities and threats that the current management schemes have.

1. Introduction.

The fundamentals of network and system management have changed a lot during the last years. Today, networks are global and multi-vendor networks that must provide communication services to a broad range of different applications having specific requirements. Network management is vital for optimized, controlled, and cost efficient utilization of network resources [1]. The nature of today's networking world and technologies means that there are possibly many factors that have to be considered in the selection of any technology or solution. The critical mission of network managers is to ensure that the network and its components provide the resources that applications and end users need to complete businesses processes and transactions.

A complete and ideal network management system manages a network and all its components from end-to-end. It should be able to take proactive action on its own through policy-based network management (i.e. restart a failed process). It should also alert the appropriate people to the problem through email or mobile text messages for example [1]. Ideally, a network management system will support all enterprise protocols. It will run on various types of hardware and it will not be tied closely to any particular vendor or operating system (OS). Older network management platforms tend to view the network in bits and pieces. This approach is insufficient to manage networks in today's connected world. It is essential to know and manage every component and link as well as to ensure that users get the services they need and that transactions are completed correctly. Effective network management requires the selected solution to provide an end-to-end perspective and the ability to observe, monitor and manage all devices along the way [2] [3].

Although functional classification was developed for the OSI environment, it has gained broad acceptance by many vendors of both standardized and proprietary network management systems. The OSI model breaks network management functions into the following five functional areas (FCAPS): *Fault management, Configuration management, Accounting management, Performance management and Security management.*

Nowadays, the most mature and widely used technology for managing a TCP/IP based network is the Simple Network Management Protocol [4]. The SNMP specifications define a simple and connection-less protocol to achieve the functions stated above. For the basic data structures and organization of information and parameters at managed node there is another standard called Management Information Base (MIB) [5]. Unfortunately, when designing the SNMP the security issues were mostly neglected. The result was an extremely vulnerable protocol. The security problems were not fixed in the next standard, SNMPv2, which provided mainly corrections and improvements to various issues such as bulk transfer. The standardization of a new version, SNMPv3, a security extension of SNMP [6] has finalized as an Internet standard within IETF. Table 1 presents the various standard versions of SNMP through the years and the most important corresponding RFCs (Request For Comments).

RFC	Title
1157	Simple Network Management Protocol (SNMP)
1213	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
2578	Structure of Management Information Version 2 (SMIv2)
3413	Simple Network Management Protocol (SNMP) Applications
3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

Table 1   SNMP versions and corresponding RFCs

This paper is organized as follows: Section 2 presents several issues involved with network management security and discusses the type of security threats as well as the security services that a network should provide. Section 3 examines briefly potential problems and threats of a network management system. Finally, section 4 concludes the paper and presents future research work.

2. Issues of network management security.

The significance of network security has grown with the movement towards global communications. Current network operators are enforced to provide security to their assets, the network and the network services [7]. A threat can come from either outside the organization or from inside the organization utilizing the network. A network management system is exposed to an extensive range of different threat types. These could be natural disasters, service and resource utilization by unauthorized hosts or transmission errors and system overload [8]. Moreover, illegal disclosure of sensitive information and unauthorized manipulation of data as well as denial of prior performed actions are possible threats for a network management system.

Some of the above are accidental threats (e.g. natural disaster) while others are intentional threats (e.g. theft and sabotage). To be able to protect the system from the above threat types, a security analysis of the whole network system must be performed. Based on this analysis, necessary actions to protect the system must be taken as soon as possible. The possible actions to these threats can be preventive (improvement of security services and mechanisms), detecting (discover and limit the damage) or correcting (repair the damage and restore the system) in nature. To prevent these threats, different security services can be used [9] [10]. This paper focuses to intentional threats and can in general be classified as:

- *Denial of service*: A network entity prevents other from having access to the network resources and services that they are allowed to access.

- *Masquerading*: An attacker claims to be someone else to get access to restricted information or to perform some actions on behalf of the other (e.g. spoofing).

- *Data manipulation*: A third party can intercept the transmission of a message and maliciously modify its content. Then the modified message is passed to the original receiver. For example, it is possible to modify permissions to system resources by this action.

- *Disclosure*: Confidential information is leaked someone that is not allowed to see this information. This can be done by e.g. sniffing the traffic that is not encrypted. Such confidential data can in a network environment be e.g. user passwords or accounting information.

- *Abuse of privilege*: Usually, the users of a system are not constrained within the limits of least privilege. Therefore it is possible to act beyond the scope although not exceeding the given permissions.

- *Traffic pattern analysis*: The information contents of the messages are ignored and system information is extracted from the usual patterns of the traffic flow.

A communication network in order to be characterized as a secure network, should provide several security services [4], such as:

- *Authentication*: Proof that subjects and objects are what and who they claim to be. In a network environment this is not only the identity of the user, but also the host and process.

- *Access control*: Ensures that subjects access objects in an authorized manner. It concerns access to physical system, software and data.

- *Confidentiality*: Protects the privacy of information from disclosure to unauthorized hosts. In a network environment this is achieved by encryption of the data flows.

- *Integrity*: Protects data from corruption and damage. Hence, data is protected from being corrupted, destroyed or modified.

- *Availability*: This means that the service can be provided to a requesting party that is authorized to access this service or data.

3. Vulnerabilities and threats.

Several vulnerabilities and security threats have been reported in many network management systems and some examples are given below:

- *Insecure perimeter of your network:* SNMP queries may be inadvertently allowed to firewalls and packet filters so that remote network scanners could be able to obtain the exact filter rules for your network.

- *Not securing the defaults strings:* The default name for the SNMP community string is PUBLIC and many products are shipped with this name. This is the first thing the attacker will look for.

- *Worse then PUBLIC:* Having no community name at all is worse than having just PUBLIC because now anyone can access the device, learn whatever they can from the device, and possibly alter its configuration.

- *Stop authentication trapping:* An advisory was issued about the ability to write to the snmpEnableAuthenTraps object within various systems. Potentially, an attacker could prevent the device from sending traps for failed authentication. Then the attacker could take his time to crack the admin password for the device, all without drawing attention to his activity.

- *Controlling the access:* A common problem mentioned is to not control the Read-Write community tightly, giving the wrong people the ability to alter the device. What this could lead to is having an attacker cause problems by bringing down the interface.

- *Hidden SNMP communities:* HP Openview was found to have a hidden SNMP community string that may allow unauthorized access to certain SNMP variables. Attackers may use this

hidden community to learn about network topology as well as to modify MIB variables. It was found that this problem extended to other vendors' products such as Sun Solstice and Solaris.

- *Remote Packet Capturing:* There are tools that do packet-capturing over the network using SNMP. Now this could lead to an attacker who is eavesdropping to obtain information about the network and other critical data. Two such tools come to my mind are Microsoft's NetMon and NAI's Distributed Sniffer.

- *Printer hiccups:* Some HP printers let malicious people execute DOS attack by sending SNMP gets, specifically the older firmware in the HP Series 5 printers.

- *ICMP echo requests:* Some routers, for example Cisco, can be configured to issue ICMP echo requests through the SNMP agent. If you repeat this numerous times the memory of the router can be filled. This would cause performance problems and an inability to respond to the ICMP echo requests.

4. Conclusions.

Modern network management tools have to be capable of meeting current needs and upcoming challenges. It is possible to manage networks proactively, with resource efficient and easy to use tools. While there are many management products available, network managers should check that their chosen solution provides that managed networks will be secured from any potential attacks. Security of network management is the key to the security of the entire network and strong security is needed for network management protocols and applications. Future research includes a closer study of the vulnerabilities of network management as well as the solutions to security threats. Moreover, further research will explore the latest version SNMP v3 that theoretical provides an improved security protection.

References.

[1] Stallings, W. B., "SNMP, SNMPv2, SNMPv3 and RMON 1 and 2", Third Edition, Addison Wesley Longman Inc., Reading, Massachusetts, 1999.

[2] D. Adamopoulos, G. Pavlou, C. Papandreou, "Towards the Efficient Support of Telecommunications Service Engineering Activities", Proceedings of the IEEE/IEE International Conference on Telecommunications (ICT '00), Acapulco, Mexico, May 2000.

[3] David Lewis, Chris Malbon, George Pavlou, Costas Stathopoulos and Enric Jaen Villoldo, "Integrating Service and Network Management Components for Service Fulfilment", Proc. of the 10th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM '99).

[4] Chatzimisios P., "Study and presentation of the SNMP protocol", BSc thesis, Technological Educational Institution, Thessaloniki, Greece, 2000.

[5] Pattinson, C., "A simulated network management information base", Journal of Network and Computer Applications, no 23, pp. 93–107, 2000.

[6] William Stallings, "SNMPv3: A Security Enhancement for SNMP", IEEE Communications Survey, vol. 1, no. 1, 1998.

[7] Chatzimisios P., Vafiadis A., Kamargiannis P., Stoimenos D., "A Survey of the Criteria on Selecting the Suitable Network Management System", In Proc. of 7th World Multi-conference on Systemics, Cybernetics and Informatics (SCI 2003), Orlando, USA, July 2003.

[8] Pattinson, C., "A Study of the Behaviour of the Simple Network Management Protocol" In Proc. of 12th International Workshop on Distributed Systems, Nancy, France, October, 2001.

[9] P. Astithas, G. Koutepas, A. Moralis, B. Maglaris, "Security management in large enterprise networks", In Proc. of HPOVUA Workshop, Santorini, Greece, June 2000.

[10] F. Stamatelopoulos, G. Koutepas, B. Maglaris, "System Security Management via SNMP", In Proc. of HPOVUA'97, Madrid, April 1997.