# Simple Network Management Protocol (SNMP) Vulnerabilities

William Perry

November 3, 2017

## 1 Introduction and Motivation

The recent Network Time Protocol (NTP) Distributed Denial of Service (DDoS) attack in excess of 400 Gbps [7] highlights the need for a deeper investigation into the vulnerabilities of basic networking protocols. The continued ability of malicious users to exploit network services fundamental to the continued operation of the Internet is detrimental to the industry as a whole. Without the confidence to operate under tolerable conditions, the passing of information across the Internet will be severely hampered. This is evidenced by the recent trend in government to regulate the Internet as a means to reduce the number of attacks.

Of these basic networking protocols, the Simple Network Management Protocol (SNMP) is one of the most widely implemented. The protocol is used to gather status information across a network and more generally as a situational awareness tool. As such SNMP is installed on nearly every device in a network. This presents numerous inherent problems, not least of which is the amount of traffic that this web of devices could produce if exploited. It is my goal to explore the inner-workings of SNMP and hopefully expose many of the flaws and assumptions that leave the protocol vulnerable to exploitation. I will primarily be focusing my attention on the most recent iteration of the protocol, SNMPv3, but will also provide a more concise overview of the major flaws of the still widely implemented yet older versions SNMPv1 and SNMPv2. By doing so I hope to provide network administrators and network security professionals with a succinct guide to further secure their network.

## 2 Procedure

### 2.1 Background

Vulnerabilities in network protocols are an ongoing area of research throughout the industry. Even before the exploitation of NTP to initiate a DDoS attack of extreme proportions, work was being done to examine SNMP for possible exploitation in a similar manner. Much of the research was spearheaded by organizations and entities such as Internet Service Providers (ISPs) and Internet security companies.

ISPs provide a unique insight into the state of network security because the clients that the ISPs serve are often the source of attack. This is not to

say that these clients are necessarily the initiators of the attack but may be non-consenting accomplices in the case of a bot-net or Distributed Reflected Denial of Service attack. ISPs are presented with a difficult challenge by being home to the initiator and facilitators of these attacks while still having their own infrastructure being targets of attack [6]. In this way they are caught in the middle with the only option being to secure network services as much as possible. The outright ban of some services would not be possible, especially in the case of SNMP, as their own networks rely on these same services to continue operation but also because banning any service outright could also hinder legitimate clients from accessing resources that they need. Thus, ISPs provide solutions to much of the problems inherent with basic network protocols without completely precluding the use of that service.

On the other hand, Internet security companies like Prolexic aim to provide solutions to much more secure networks like those owned by private institutions and corporations [1]. In these situations it is possible and sometimes necessary to ban services network wide when the use of these services would only result in illegitimate traffic. An example of this would be the banning of port 531 which is most commonly used for AOL instant messenger. While I am not aware of any vulnerabilities associated with this port, the disallowance of it network wide would effectively eliminate any possible exploitation from that service. While firms such as Prolexic may offer much more drastic solutions to vulnerabilities the effectiveness of these solutions should not be overlooked.

## 2.2 Statement of Work

The focus of my research was to discover avenues that malicious users could exploit in SNMP services to attack network infrastructure across the Internet. This was accomplished by gathering numerous reports from a number of different sources on their findings from attacks "in the wild." I also read much of the technical documentation relating to SNMP as a complement to these reports and to analyze the assumptions that SNMP was built with. Given the time and resource limitations I was unable to carry out simulations of my own to have direct evidence of the vulnerabilities discussed. In order to understand the terminology within this report it is first necessary to understand the basic operation of SNMP.

SNMP is loosely structured in a hierarchal manner. SNMP managers oversee and command SNMP agents or in some cases managers oversee and command master agents who then in turn oversee and command agents. Much of the time SNMP is a pull protocol with the manager requesting information from the agents through the use of several different GetRequests. However, at times the protocol operates in a push manner with agents sending information without any prompt based upon pre-configured settings in what is called a trap. SNMP agents can monitor and report on everything associated with the device that agent is installed on. This can range from the status of network interfaces to the addresses of that device's neighbors to the level of CPU usage on the device. The manager is primarily a repository for all the information that is received from traps and GetRequests and as a means for the network administrator to push configuration changes to the agents via the set command.

The information that agents can be configured to report to the manager is all dependent on the Management Information Base (MIB) module that is

associated with that device and its interfaces. In other words, the individual MIB modules define what information a device can report to the manager about and the format that that information is in. MIB modules are hierarchically structured and maintained by numerous different organizations with no central organization overseeing the administration of all MIB modules. MIB modules are semi-permanent in that once a module is published it is very difficult, and frowned upon, to alter the information defined within that module. Instead, it is common practice to publish a newer module incorporating the new information and formatting and to make the older MIB module obsolete.

## 2.3 Results

All versions of SNMP share a common vulnerability in the almost universal use of UDP as the transport layer protocol. This allows attackers to spoof the source address of traffic destined for agents and managers. Thus malicious users can use a packet crafter to masquerade themselves as the manager or agent to request or send large volumes of traffic across networks or falsify the appearance of network conditions. While spoofing the source address of the manager does not seem inherently damaging, if targets are carefully selected, it is possible to create a DRDoS attack using a networks own infrastructure. The other aspect of this vulnerability gives the attacker the means to falsify traps to the manager which lead to conditions in the network to be more favorable for attacker. For instance, an attacker could spoof source addresses of multiple agents to send traps to the manager to simulate an attack in another part of the network. The administrator would then focus the majority of their attention on this part of the network while the attacker less visibly attacks a more vulnerable part of the network. One solution to this problem is switching to using TCP. While TCP is less loss tolerant than UDP, it does have the added benefits of reliability and authentication. As shown by Wes Hardaker [5], unless UDP is configured appropriately it does not offer a much greater advantage over TCP. In a great many networks TCP would work as well as UDP in delivering SNMP traffic with the added benefit that it would not 'choke' out other traffic.

SNMPv1 and SNMPv2 (here-on referred to simply as v1 and v2) contain profuse amounts of security vulnerabilities that, unless implemented in tandem with other security such as firewalls, would be extremely easy to exploit. These vulnerabilities remain relevant because of the large numbers of devices and organizations that are either unable to update their systems to SNMPv3 or choose to continue using obsolete versions of SNMP despite the inherent security risks. V1 and v2's most obvious and easily abused vulnerability is their use of unencrypted community strings as a form of security. In SNMP community strings are used to segregate portions of the network into different areas of management. This helps to reduce complexity in network management by breaking large networks into sectors with a network administrator assigned to manage each sector. It also reduces the amount of unnecessary traffic across the network because an administrator need only request information from the desired community rather than the entire network. Community strings security strength is derived from their anonymity to everyone except the network administrator. This anonymity is compromised the first time a command is sent across a network as a result of the lack of encryption in v1 and v2. A malicious user need only capture one of these packets using a simple tool like Wireshark to find the community string

displayed in clear text.

Another common vulnerability of SNMP is the choice by device manufacturers to have platform specific configurations. This causes problems when a network is not homogenous. If only a portion of devices support certain security features it leaves holes within your network security that would require additional hardware or software to mitigate. Caveating off of this, device manufacturers further impair the ability of network administrators to secure their networks by shipping devices preconfigured with SNMP turned on. These devices most commonly have a default community string that is very easy to guess, such as 'public' or 'private.' Adding to this, when the device is not professional grade equipment it is sometimes impossible to turn off SNMP or configure it in any way. As discussed, this contributes to the problem of DRDoS attacks.

Upon a cursory inspection of RFC 3411, which defines SNMPv3, it is obvious that while SNMPv3 addresses many of the security flaws found within v1 and v2 there are still several ways to exploit SNMPv3 for malicious purposes. Ignoring Access Control Lists, security within SNMPv3 is less than ideal. Because of the vulnerabilities inherent to all versions of SNMP, SNMPv3 is still vulnerable to dictionary attacks on its community strings. However, the use of encryption, MD5 and SHA protocols, by SNMPv3 eliminates much of this threat. SNMPv3 also does very little to address the spoofing of an IP packet that is possible because of the use of UDP. Using the command AuthPriv will negate this by making agents and managers authenticate connections and encrypting the traffic so that it will be confidential.

As with almost all problems within a network, many of the vulnerabilities associated with SNMPv3 lay not within the protocol itself but with the configuration by the user. SNMPv3 does include a number of extremely powerful tools to confine the use of the resources on the network strictly to authorized personnel. Of these Access Control Lists (ACLs) are perhaps the most powerful. ACLs allow network administrators to allow only certain machines access to the device. These machines can be specified by either IP or MAC address. If configured to allow only a handful of specific machines, ACLs can be used to effectively control many of these vulnerabilities.

This leads me into a brief overview of a number of simple yet effective SNMP administration techniques that can dramatically increase network security. Network devices that have SNMP services turned on but are not being utilized should be turned off. If left on these services can be used in future DDoS attacks and contribute to unnecessary processes being run on the machine. It is highly recommended that networks disallow any SNMP traffic entering the network from the outside wherever possible. Traffic allowed to pass through a firewall destined for an SNMP agent can be used to create a DDoS attack originating from within the network. Another effective technique to make SNMP more secure is to decrease the size of communities of devices. Decreasing community sizes not only ensure that should an attacker find the correct community name he/she has access to a much smaller number of devices but also that individual communities present a much less tempting target in the first place. Finally, being highly specific with the MIBs that are able to be accessed through agents reduces the amount of needless traffic that will be passed across the network. What is meant by this is to disallow agents sending portions of MIBs that are not relevant to the management of the network. Doing this also reduces the amount of traffic that could be produced by the agents should they be exploited

in a DDoS attack.

# 3 Conclusion and How-to-Guide

In conclusion, when implemented correctly, SNMP is not overly susceptible for exploitation by malicious users. Much of the threat resides in the resistance of network administrators to switch their systems to using SNMPv3 instead of v1 and v2. The lack of awareness by device manufacturers as to the damaging nature of their continued practice of pre-configuring SNMP is something that needs to be considered by network professionals when designing a network. Security requires continued vigilance and constant correction of security practices. SNMP does not fall outside of this requirement. A network administrator must constantly be reassessing SNMP configurations to make sure the SNMP entities are operating as securely and efficiently as possible. ACLs are a powerful tool to be used. However, they are still susceptible to security vulnerabilities and need to be continually updated to ensure adequate protection.

There still remains a great deal of work in SNMP to fully understand any possible avenues that malicious users could exploit. I was unable to look at the source code of SNMP to ensure that good programming techniques were used throughout and the logic is correct. It is my suspicion that there remains a number of undiscovered flaws within SNMP that stem from errors within the code. Combing through the individual lines of code in SNMP would constitute an entirely separate project on its own right.

If someone would like to replicate my study he or she would have to do nothing more than investigate the inner workings of SNMP. The resources that I used to study SNMP are all freely available and eary to find. All one need to do is read the different studies. From these it is easy to infer the nefarious uses that the processes of SNMP could be used for.

# 4 Appendix

# References


[1] An analysis of drdos snmp/ntp/chargen reflection attacks. http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/An_Analysis_of_DrDoS_SNMP-NTP-CHARGEN_Reflection_Attacks_White_Paper_A4_042913.pdf/.

[2] Introduction to snmp and mib. http://www.cisco.com/networkers/nw04/presos/docs/NMS-1N02.pdf.

[3] A simple network management protocol. https://www.ietf.org/rfc/rfc1157.txt/.

[4] A simple network management protocol. http://www.ietf.org/rfc/rfc3411.txt/.

[5] Snmp over udp vs tcp. http://www.ietf.org/proceedings/72/slides/opsarea-2.pdf.

[6] Snmp reflected amplification ddos attack mitigation. http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf/.

[7] Technical details behind a 400gbps ntp amplification ddos attack. http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack.

[8] D. Genkov. Implementing port security feature using snmp protocol. In *Proceedings of the 14th International Conference on Computer Systems and Technologies*, CompSysTech '13, pages 38–45, New York, NY, USA, 2013. ACM.

[9] G. Jiang. Multiple vulnerabilities in snmp (supplement to computer magazine). *Computer*, 35(4):2–4, 2002.

[10] M. Pihelgas. Snmp attacks and security. http://home.cyber.ee/~ahtbu/CDS2011/MaunoPihelgasSlides.pdf.

[11] J. Romanski. Intrusion detection faq: Using snmp for reconnaissance. http://www.sans.org/security-resources/idfaq/snmp.php.