SNMP SECURITY – A CLOSER LOOK

JEFFERY E. HAMMONDS

EAST CAROLINA UNIVERSITY

ICTN 6865

NOVEMBER 25, 2013

ABSTRACT

As a Network Monitoring System Administrator I have gained a substantial amount of experience using different versions of SNMP. The purpose of this paper is to discuss the history of SNMP over the years and the security (or lack thereof) that the different versions offer. I will discuss some of the vulnerabilities that the different versions contain, to include SNMPv3 which is the most secure version to date. I will briefly touch on configuring SNMPv3 on Cisco and Brocade devices as well as deploying agents to assist in monitoring servers using SNMPv3. After reading this paper the reader should have a better understanding of all the security options that are available to them using SNMP.

SNMP SECURITY – A CLOSER LOOK

As security concerns continue to grow in the IT field one of the commonly overlooked areas is SNMP. Administrators may not completely understand some of the risks that come with using the wrong versions of SNMP or not using the proper configuration. SNMP is a protocol used for managing devices on IP networks. SNMP relies on three major components. These are the managers, agents, and the Management Information Base (MIB). The managers are the network monitoring system (NMS) that does all the polling and receiving of traps. The agents are the SNMP services that run on the devices. The MIBS provide the "language" used for that device type so that the manager and the agent know how to communicate with each other. (Stallings, 1998)

There have been three releases of the SNMP protocol. The first release of SNMP was with SNMPv1 in 1988. The next version update occurred eight years later with SNMPv2 being released in 1996. In 2002 SNMP finally gained security features with the release of SNMPv3. SNMP is becoming a fairly dated protocol but it keeps adapting to the changing security landscape.

As I stated earlier, SNMPv1 was released in 1988 as a way for administrators to manage IP devices on their network. The only security feature included in SNMPv1 was the use of community strings. This required a string of text/numbers be input on the monitored device as well as the management system in order to get the SNMP packets. This isn't a very secure feature as the packets are sent across the network in clear text and the information can be intercepted by anyone that is eavesdropping. This clear text also includes the community string itself.

SNMPv2 didn’t add any security with its release in 1996. The community strings still existed and so did the vulnerabilities. The features that were added in SNMPv2 were more of the functional variety in that instead of with SNMPv1 only being able to perform single “get” requests you could now perform “bulk get” requests which would return information in larger quantities. What this means for information security is that you are able to give away information a lot faster than with SNMPv1.

As you can see the biggest issue with the earlier releases of SNMP was that there was no way encryption which would allow eavesdroppers to get your device information. That, however, is just one of the security issues when dealing with SNMP. Another serious security vulnerability are the two default community strings that come preloaded on most network devices. These community strings would be the “public’ and “admin” strings. The “public” community string grants users read-only access which will allow the administrator or hacker to read information off of the network device. The second string is a lot more dangerous. It grants read-write access to the device. This will allow anyone that can connect to that device using the string the ability to modify any setting on that device that they want to. (Stump, 2003)

Some of the other network vulnerabilities that come with these two earlier protocols include: masquerading, modification of information, message stream modification, disclosure, denial of service, and traffic pattern analysis (Ubizen, 2002). So if you are forced to use SNMPv1 or SNMPv2 then how can you mitigate these vulnerabilities? The first thing you need to do is move your SNMP traffic to a private network, this is called a management network. This will isolate your production network traffic from you non production traffic. It also adds a layer of security between you and the attacker since they won’t have access to this private network. This will prevent them from being able to intercept the SNMP packets since they will be routed through a private network. The next thing you need to do is add ACLs to your devices. This will limit what devices your networking device will respond to. Lastly, you want to remove the default community strings from your devices and replace them with complex community strings of your own. (Stalvig, 2008)

If your devices and network monitoring system are able to use SNMPv3 than that is your best option. Not only does SNMPv3 offer better authentication but it also offers encryption so that the SNMP traffic that is sent out can't be viewed in clear text if it is intercepted. Depending on your devices you may be able to include encryption up to SHA and AES. SNMPv3 offers three levels of security; No Authentication and No Privacy, Authentication and No Privacy, and Authentication with Privacy. The first option doesn't offer any security. The second option offers authentication but no encryption of packets traversing the network. The third option allows both authentication and privacy. From these you can tell that Authentication with Privacy offers the most security. (SNMP Research, 2013)

You may run into a couple issues trying to implement SNMP however. Not all management applications can understand SNMPv3. Not only may you run into management systems that don't understand it but unless you have newer network infrastructure then your devices might not able to be configured to use SNMPv3. On the server side Windows Server only offers support for SNMPv1 or SNMPv2. When you run into these limitations third party software may be available to bridge the gap.

Even though SNMPv3 has been around since 2002 a lot of management systems still don't provide support for it, CA eHealth and HP Performance Insight Manager to name a couple. In these situations you may feel forced to utilize SNMPv1 or SNMPv2 but that isn't the case. SNMP Research has released a product called Distributed SNMP Security Pack (DSSP) that will allow your system to receive SNMPv3 traffic. This application gets installed on the manager end to work as a liaison between the manager and the agent. Having used it at work for CA eHealth I can say that it can be a pain to setup but does offer the security that is required for my line of work. (SNMP Research, 2013)

Unfortunately, Microsoft Windows Server only provides support for SNMPv1 and SNMPv2. Fortunately, there are several companies that have produced SNMP agents that can replace the native windows SNMP agent running on your servers. Almost all of the agents provide the same functionality so I will just discuss the one that I am most familiar with and that is the CA SystemEdge agents. These agents can be deployed manually or through an application called Virtual Assurance for Infrastructure Managers (VAIM). Aside from allowing the server to communicate with the management software using SNMPv3 the SystemEdge agents can also be upgraded with Application Insight Modules (AIMs). These are application specific add-ons to the agent that provide further management information back to the management system. There are AIMs for vSphere, Cisco UCS, and several other popular server applications.

Once you are sure your management server is able to send out SNMPv3 traffic then it is time to work on configuring your devices to use SNMPv3. The major difference between the first two releases of SNMP and SNMPv3 is the addition of privacy and authentication to SNMPv3. By configuring these two settings on your device you can require advanced authentication to the device as well as encrypting the traffic as it travels across the network. The two options for authentication are MD5 and SHA, with SHA being the more secure and better option. Privacy options include DES, 3DES, AES128, AES192, and AES256. AES256 is the most secure but it is very hard to find equipment that can handle the longer key length. It is common practice to use AES128. I have had experience configuring both Cisco and Foundry devices so the next section will discuss how to configure these devices to communicate with your management server.

Cisco breaks their SNMPv3 configuration down into three steps. The first step is to enter privileged mode with the “enable” command. The second step is to enter global configuration mode by entering “configure terminal”. The last step is to enter the snmp-server command to create the user, assign the group, and specify what privacy and authentication to use. Syntax is as follows:

```
  Router(config)# snmp-server user todo kansas v3 auth sha password1 priv aes 128 password2
```

The above command would create the new user todo and assign todo to the group Kansas. It would also enable SNMPv3 for the user with Privacy and Authentication enabled and use the SHA protocol for authentication and AES 128 for privacy. The full syntax with all available options is listed below (Cisco Systems, 2007):

```
snmp-server user username group-name [remote host [udp-port port]] {v1 | v2c | v3 [encrypted]
[auth {md5 | sha} auth-password]} [access [ipv6 nacl] [priv {des | 3des | aes {128 | 192 |256}}
privpassword] {acl-number | acl-name}]
```

Foundry is very similar to Cisco as far as needing to access the global configuration mode to make the changes to SNMP. It offers a lot of the same functions as Cisco but you have to create the groups and users step by step. The first thing you will need to do is create the group with the snmp-server command. An example for creating a SNMPv3 group is listed below (Brocade, 2009):

```
snmp-server group admin v3 auth read all write all
```

The command listed above would create an admin group that requires authentication and grants read and write access to everything. After you have created the group the next thing you need to create is the SNMPv3 user account. This syntax is very similar to what we created on the Cisco devices earlier. The syntax for this command is listed below (Brocade, 2009):

```
snmp-server user dorothy admin v3 access 2 auth md5 dorothymd5 priv des dorothydes
```

The command above adds the user “dorothy” to the group “admin” that we created in the step above and enables MD5 and DES on the user account. As you can see the only major difference between this command and the Cisco command is the added “access” command. Once the user account is created the user should be able to access SNMP information using SNMPv3 with the user information and passwords created. (Brocade, 2009)

While SNMPv3 is the most secure version it is far from perfect. There aren’t currently any issues with the protocol itself but since the protocol relies on the base algorithms it is also exposed to the same weaknesses that those algorithms have. If you configure a device to us MD5 then you can expect that device to be easily hacked. This is why I recommended using at least SHA and AES128 earlier. (Lawrence, 2012)

Additional considerations that should be considered when using SNMPv3 include the additional bandwidth utilization that the handshakes generate. While this may not be an issue with smaller networks it can cause serious issues on larger networks. This is where the utilization of the private management network comes in handy again. By moving this traffic off of the production network you help ease the congestion on the network.

Another issue with the use of SNMPv3 is the affect that authentication has on the polling cycle. If you have a large number of devices then your polls may not complete before it wants to start over. Most network monitoring systems have a default polling interval of 5 minutes. If it takes the network monitoring system longer than 5 minutes to poll everything then you will get dropped packets and bad polls. If you run into this issue then you do have a couple of options.

You can increase the poll interval to a number that fits all your polls into the window or you can setup a second network monitoring system and split the polls.

As you can see, while SNMPv3 isn’t perfect it is still the only true option when it comes to SNMP traffic. SNMPv1 and SNMPv2 aren’t truly viable options if security has any importance within your organization. The information contained in these SNMP packets are enough to cripple your network and if you don’t protect it then you run the risk of an attack occurring. By combing the use of SNMPv3 with the security of a management network you will have the best of both worlds by eliminating the extra traffic that is generating by the SNMPv3 authentication.

REFERENCES

Brocade. (2009). Securing snmp access. Retrieved from http://www.foundrynet.com/services/documentation/security/current/Security_SNMP3.html

Cisco Systems. (2007, June 05). Aes and 3-des encryption support for snmp version 3. Retrieved from http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/snmpv3ae.html

Computer Associates. (2013). Guidelines for using the systemedge agent. Retrieved from https://support.ca.com/cadocs/0/CA%20Server%20Automation%2012%206-ENU/Bookshelf_Files/HTML/SE_User/index.htm?toc.htm?guidelines_for_using_the_ca_ehealth_systemedge_agent.html

*Lawrence, N. (2012, August). Vulnerabilities in snmpv3. Retrieved from https://smartech.gatech.edu/bitstream/handle/1853/44881/lawrence_nigel_r_201208_mast.pdf?sequence=2

SNMP Research. (2013). Snmpv3 with security and administration. Retrieved from http://www.snmp.com/snmpv3/snmpv3_intro.shtml

SNMP Research. (2013). Distributed snmp security pack. Retrieved from http://www.snmp.com/products/dssp.shtml

*Stallings, W. (1998). Security comes to snmp: The new snmpv3 proposed internet standards. The Internet Protocol Journal, 1(3), retrieved from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-3/snmpv3.html

Stalvig, P. (2008). Management networks— living outside of production. Retrieved from http://www.f5.com/pdf/white-papers/management-networks-wp.pdf

*Stump, M. (2003). Securing snmp: A look at net-snmp (snmpv3). Retrieved from http://www.sans.org/reading-room/whitepapers/networkdevs/securing-snmp-net-snmp-snmpv3-1051

Ubizen. (2002). Security in snmpv3 versus snmpv1 or v2c. Retrieved from http://www.aethis.com/solutions/snmp_research/snmpv3_vs_wp.pdf