EECS 4482 Mini Research Project: SNMP Security

Alex Xu, Henok Keflu, N. Panjawani

March 27, 2019

Summary

- Simple Network Management Protocol
- Access information about managed devices on IP networks (network traffic, CPU usage, disk space, temperature, etc)
- Modify information to change device behavior
- Wide support: cable modems, routers, switches, servers, workstations, printers, UPSs

Advantages

- Uniform tools and interface
- Simple design
- Sufficiently powerful for its purpose

Components

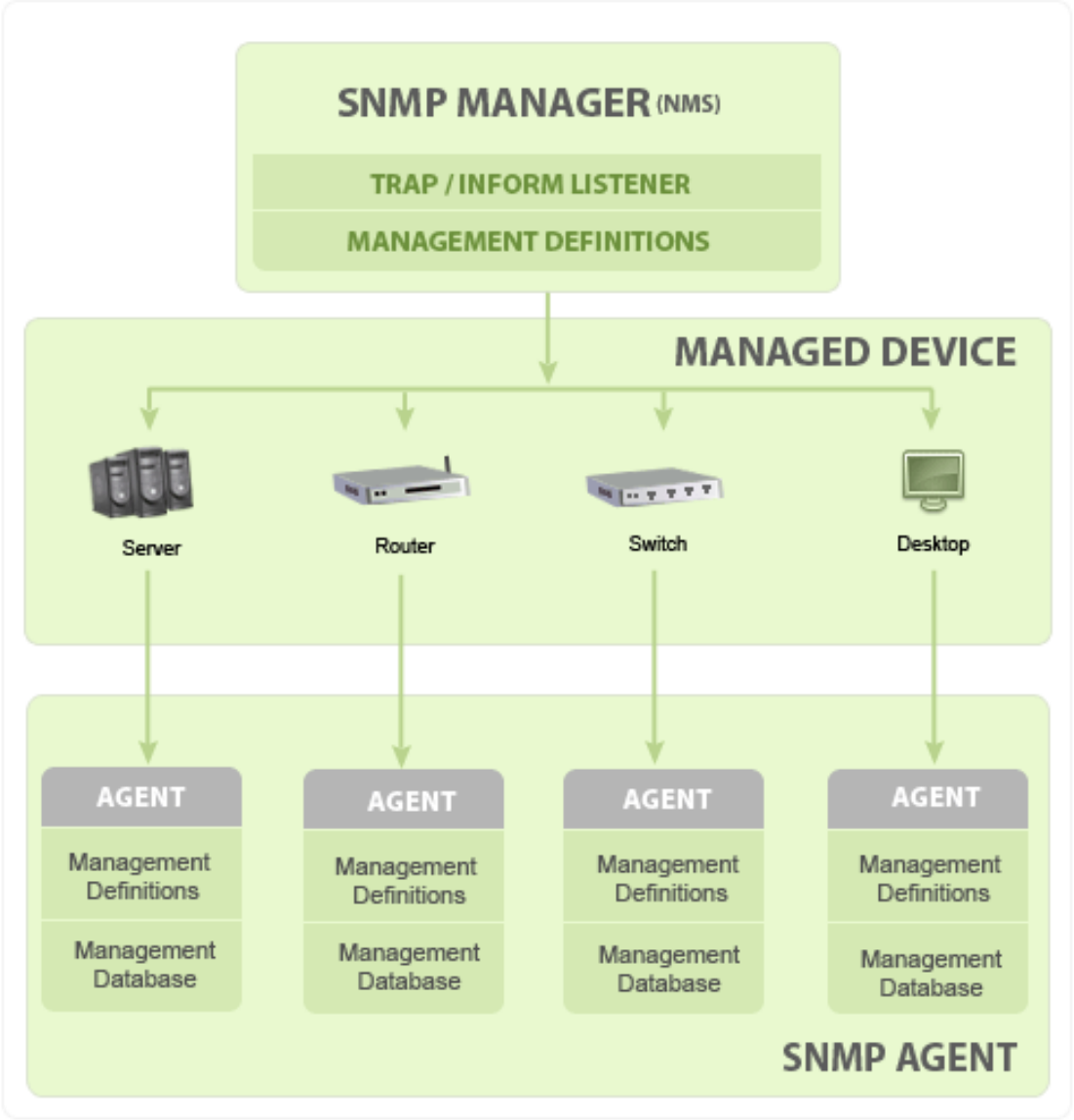
Manager

A separate entity that is responsible for communicating with the SNMP agents.

Agent

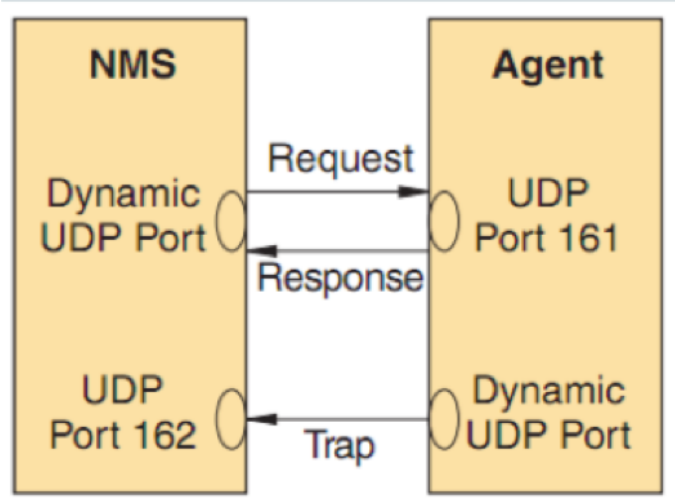
SNMP software in the managed device. Many devices have it by default.

Communication



Methods

- Polling
  1. GetRequest: read-only
  2. SetRequest: read-write
  3. Response
- Traps
  - Trap Message



Versions

- SNMPv1, SNMPv2, SNMPv2c, SNMPv2u, SNMPv3
- Similar core concepts
- Some improved features
  - GetBulkRequests
  - 64-bit counters
- Mainly different authentication

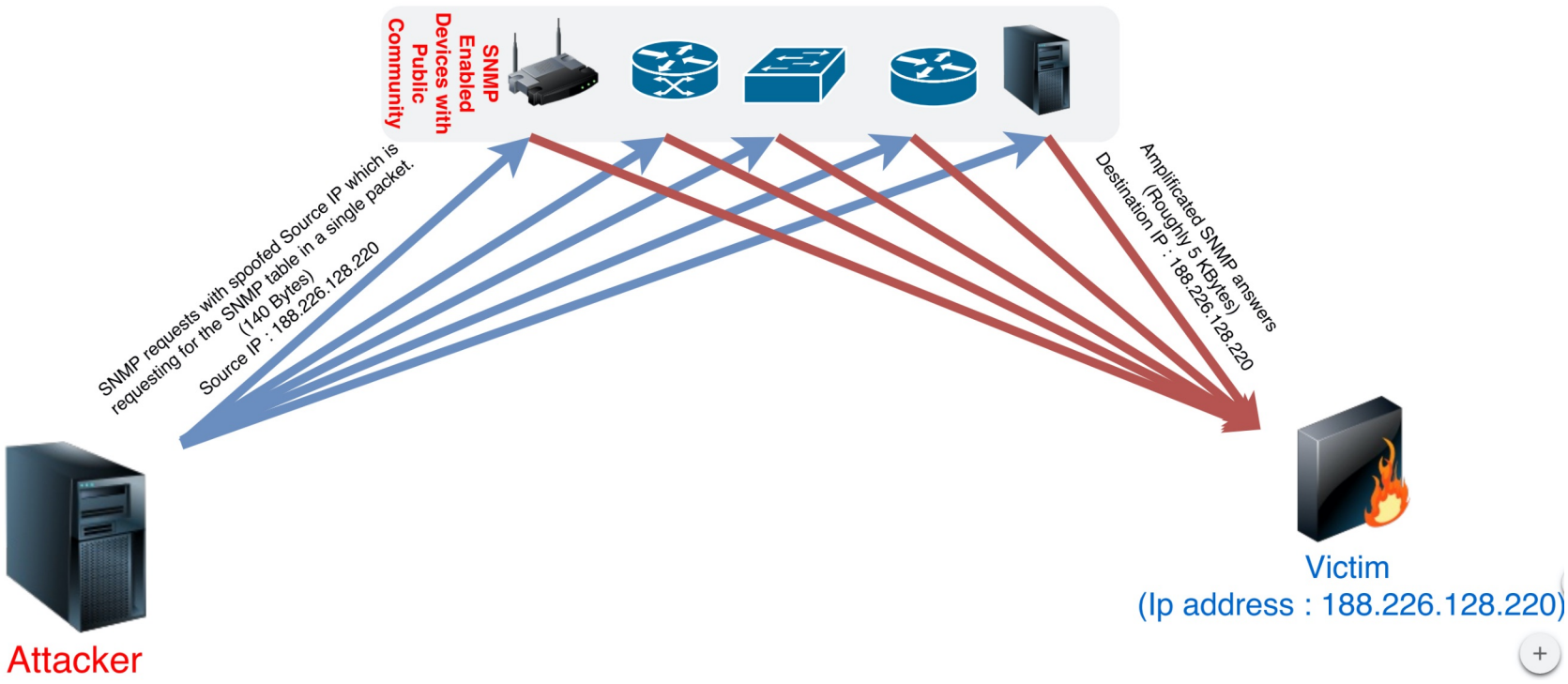
Authentication and encryption

- SNMPv1, v2c: community string
  - poorly named, really a password
- SNMPv2, SNMPv3: cryptographic security for optional confidentiality and/or integrity

Vulnerabilities

- Often preinstalled
- Default settings often insecure
- Credentials may actually be read-write

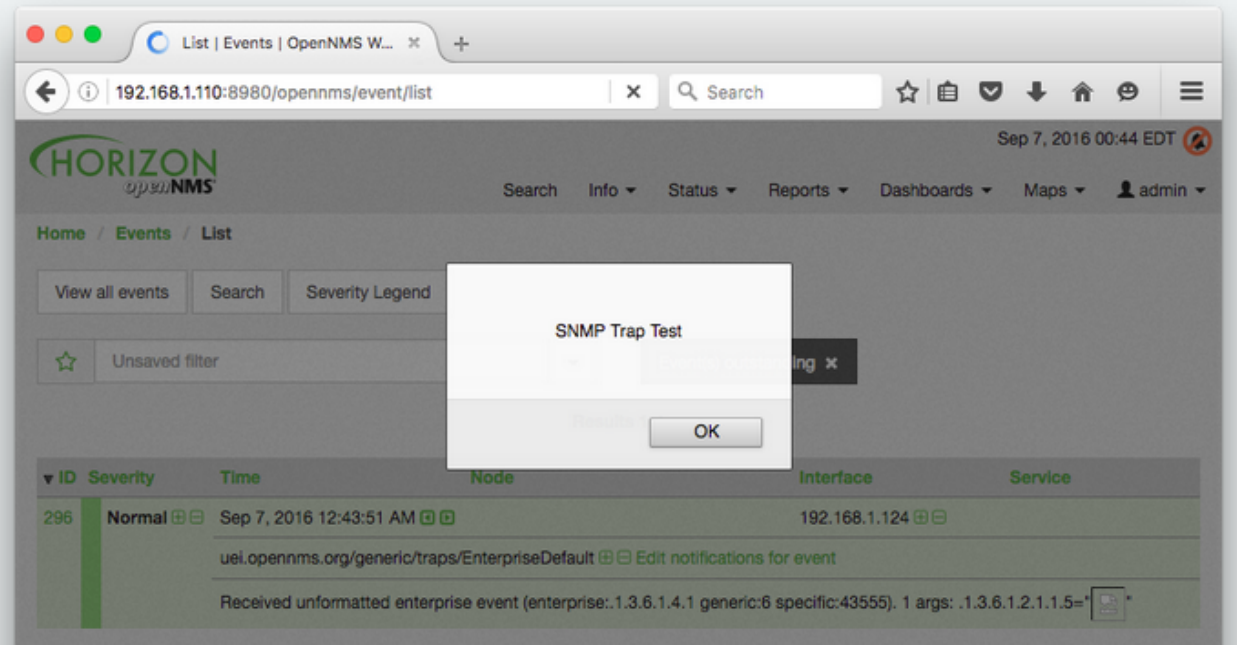
Vulnerabilities: SNMP Amplification DDOS Attack



Vulnerabilities: SNMP NMS XSS Attack

```
snmptrap -v2c -c public OpenNMS_Host '' 1.3.6.1.4.1.43555 SNMPv2-MIB::sysNa
s "<IMG SRC=/ onerror=\"alert('SNMP Trap Test')\"></IMG>"
```

When the user navigates to the events list page, the XSS payload is returned in a response to the user's browser session and executed. An alert box is displayed that contains the string "SNMP Trap Test", as shown below.



Security

- Use network scanners
- Configure SNMP properly, otherwise disable it
- Consider security requirements, use SNMPv3 with authPriv if appropriate
- Use different credentials for reading and writing

Conclusion

- Similar to other protocols, security was an afterthought
- Insecure by default, but secure options are available

Attributions, bibliography

- http://www.ists.dartmouth.edu/library/9.pdf
- https://www.btcirt.bt/snmp-vulnerability/
- https://www.esecurityplanet.com/trends/article.php/973801/SNMP-Vulnerability-A-Triple-Threat.htm
- https://nsrc.org/workshops/2015/sanog25-nmm-tutorial/materials/snmp.pdf
- https://www.manageengine.com/network-monitoring/what-is-snmp.html/snmp-manager
- https://www.excitingip.com/495/an-overview-of-snmp-simple-network-management-protocol/
- http://alibay.com.tr/?p=955
- https://blog.rapid7.com/2016/11/15/r7-2016-24-opennms-stored-xss-via-snmp-cve-2016-6555-cve-2016-6556/
- https://www.us-cert.gov/ncas/alerts/TA17-156A