Third Time’s Not a Charm

Exploiting SNMPv3 for Router Fingerprinting

Taha Albakour, Oliver Gasser, Robert Beverly, and Georgios Smaragdakis.
What is SNMP?

- Simple Network Management Protocol (SNMP)
- De facto network management protocol
- Multiple versions over the years

<table>
<thead>
<tr>
<th>Year</th>
<th>Protocol</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>1988</td>
<td>SNMPv1</td>
<td>Poor Performance, weak security</td>
</tr>
<tr>
<td>1993</td>
<td>SNMPv2p</td>
<td>Performance and Security Improvements</td>
</tr>
<tr>
<td>1996</td>
<td>SNMPv2u</td>
<td>User-based Security Model</td>
</tr>
<tr>
<td>1996</td>
<td>SNMPv2c</td>
<td>Performance Improvements, Community-based</td>
</tr>
<tr>
<td>2002</td>
<td>SNMPv3</td>
<td>User-based Security Model</td>
</tr>
</tbody>
</table>
Research Until Now: SNMPv2c

- Currently only ~1.6M SNMPv2c responsive IPs
- No prior work investigated the adoption of SNMPv3

Figure source [https://scan.shadowserver.org/snmp/stats/](https://scan.shadowserver.org/snmp/stats/)
SNMPv3 Discovery Phase
SNMPv3 Discovery Request
- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: <MISSING>
- msgAuthoritativeEngineBoots: 0
- msgAuthoritativeEngineTime: 0
- msgUserName: 
- msgAuthenticationParameters: <MISSING>
- msgPrivacyParameters: <MISSING>
- msgData: plaintext (0)
SNMPv3 Discovery Request

- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: <MISSING>
- msgAuthoritativeEngineBoots: 0
- msgAuthoritativeEngineTime: 0
- msgUserName:
- msgAuthenticationParameters: <MISSING>
- msgPrivacyParameters: <MISSING>
- msgData: plaintext (0)
SNMPv3 Discovery Request

- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: <MISSING>
- msgAuthoritativeEngineBoots: 0
- msgAuthoritativeEngineTime: 0
- msgUserName:
- msgAuthenticationParameters: <MISSING>
- msgPrivacyParameters: <MISSING>
- msgData: plaintext (0)

SNMPv3 Discovery Response

- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: 800007c703748ef831db80
  1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
  Engine Enterprise ID: Brocade Communication Systems, Inc.
  Engine ID Format: MAC address (3)
- msgAuthoritativeEngineBoots: 148
- msgAuthoritativeEngineTime: 10043812
- msgUserName:
- msgAuthenticationParameters: <MISSING>
- msgPrivacyParameters: <MISSING>
- msgData: plaintext (0)
SNMPv3 Discovery Request

- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: <MISSING>
- msgAuthoritativeEngineBoots: 0
- msgAuthoritativeEngineTime: 0
- msgUserName:
- msgAuthenticationParameters: <MISSING>
- msgPrivacyParameters: <MISSING>
- msgData: plaintext (0)

SNMPv3 Discovery Response

- msgVersion: snmpv3 (3)
- msgGlobalData
- msgAuthoritativeEngineID: 800007c703748ef831db80
  - .... = Engine ID Conformance: RFC3411 (SNMPv3)
  - Engine Enterprise ID: Brocade Communication Systems, Inc.
  - Engine ID Format: MAC address (3)
- msgAuthoritativeEngineBoots: 148
- msgAuthoritativeEngineTime: 10043812
- msgUserName:
- msgAuthenticationParameters: <MISSING>
- msgPrivacyParameters: <MISSING>
- msgData: plaintext (0)
What can we do with SNMPv3 responses?

- Facilitate many Internet measurement tasks:
  - IP alias resolution
  - IPv4/IPv6 dual-stack detection
  - Device vendor fingerprinting
  - Device uptime analysis

- With only a single packet per IP!
Alias and Dual-Stack Detection
Alias and Dual-Stack Detection
Alias and Dual-Stack Detection

1. `snmpv3 get, dst=A, EngId=null`

Alias and Dual-Stack Detection

1. `snmpv3 get, dst=A, EngId=null`
Alias and Dual-Stack Detection

1. `snmpv3 get, dst=A, EngId=null`

Alias and Dual-Stack Detection

1. `snmpv3 get, dst=A`, `EngId=null`


3. `snmpv3 get, dst=B`, `EngId=null`
Alias and Dual-Stack Detection

1. `snmpv3 get, dst=A, EngId=null`
3. `snmpv3 get, dst=B, EngId=null`
Active Scan Results

- **Responses**
  - 31M IPv4 addresses
  - 180k IPv6 addresses

- **After extensive filtering**
  - 12.5M IPv4 addresses
  - 140k IPv6 addresses

IPv6 hitlist service: [https://ipv6hitlist.github.io/](https://ipv6hitlist.github.io/)
ZMap: [https://github.com/zmap/zmap](https://github.com/zmap/zmap)
Device Fingerprinting: Vendors Popularity

Total Number of Devices: 4.6M

Total Number of Routers: 350k
SNMPv3 Router Vendors Popularity per Network
SNMPv3 Routers Last Reboot
Why do so many devices respond?

- Lab experiments
  - Cisco IOS 15.2(4)S7 and IOS XR 6.0.1
  - Juniper JunOS 17.3
- Devices unknowingly respond to SNMPv3
SNMPv3 Measurement Service

On this website we present results from ongoing SNMPv3 measurements, provide access to raw SNMPv3 measurement results to fellow researchers, and show additional information about our IMC 2021 paper *Third Time’s Not a Charm: Exploiting SNMPv3 for Router Fingerprinting*.

We run continuous SNMPv3 measurements on the full IPv4 address space and based on the IPv6 Hitlist Service.
Summary

● SNMPv3 adoption
  ○ 31M IPs

● Lightweight technique (single packet)
  ○ IP alias and dual-stack detection
    ■ 4.6M devices
  ○ Router vendor fingerprinting and uptime analysis
    ■ 350k routers
    ■ 11k networks
Backup Slides
Device Vendor Fingerprinting

Engine ID Structure:

<table>
<thead>
<tr>
<th>Conformance Bit</th>
<th>Enterprise ID</th>
<th>Engine ID format</th>
<th>Engine ID Data</th>
</tr>
</thead>
</table>

Example EngineID: 800007c703748ef831db80

- Conformance Bit: 8000
- Enterprise ID: 07c7
- Engine ID format: 03
- Engine ID Data: 748ef831db80
## Filtering Responses

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Date</th>
<th>#IPs</th>
<th>#Engine IDs</th>
<th>#IPs w/ valid engine ID</th>
<th>#IPs w/ valid engine ID &amp; engine time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 scan 1</td>
<td>Apr. 16–20, 2021</td>
<td>31.8M</td>
<td>18.8M</td>
<td></td>
<td>27.0M</td>
</tr>
<tr>
<td>IPv4 scan 2</td>
<td>Apr. 22–27, 2021</td>
<td>31.5M</td>
<td>18.6M</td>
<td></td>
<td>12.5M</td>
</tr>
<tr>
<td>IPv6 scan 1</td>
<td>Apr. 13, 2021</td>
<td>182k</td>
<td>68k</td>
<td></td>
<td>152k</td>
</tr>
<tr>
<td>IPv6 scan 2</td>
<td>Apr. 14, 2021</td>
<td>180k</td>
<td>67k</td>
<td></td>
<td>140k</td>
</tr>
</tbody>
</table>

- **Engine ID filters:**
  - Missing engine IDs.
  - Inconsistent engine IDs across 2 scans
  - Short engine IDs
  - Format specific filters
- **Engine boot + Engine time filters:**
  - Zero Engine time or engine boot
  - Engine time in the future
  - Inconsistent engine boots
  - Inconsistent last reboot time
EngineID Formats

![Graph showing the fraction of IPs with different engine ID formats for IPv4 and IPv6. The categories include MAC addr., Octets, non-SNMPv3, Net-SNMP, IPv4 addr., with counts ranging from 7.2M82k to 20k.](image-url)
Alias Resolution: IPs per Alias Set

ECDF: Fraction of Alias Sets

Number of IPs per Alias Set

IPv6 Alias Sets
Routers Only
IPv4 Alias Sets
Fingerprinting: Router Vendors Count per AS
Fingerprinting: Router Vendors Popularity per Region