A Characterization of IPv6 Network Security Policy

Mark Allman
International Computer Science Institute

MAPRG Meeting
April 2016

“Hey [IETF] I'm calling all stations
Blowing down the wire tonight
I'm singing through these power lines
And I'm running on time and feeling alright”
Acknowledgments

• Collaborators:
  • Matthew Luckie, CAIDA/U. Waikato
  • Michael Bailey, UIUC

• Paper:
IPv6 gaining traction
IPv6 Security

- IPv6 is not inherently more or less secure than IPv4

- IPv6 ecosystem is actually less secure
  - Lack of maturity in stacks, processes, tools, operator competency
  - In dual-stack world, IPv6 is a second attack path
IPv6 Security

“In new IPv6 deployments it has been common to see IPv6 traffic enabled but none of the typical access control mechanisms enabled for IPv6 device access.”

— Chittimaneni, et al., Internet-Draft draft-ietf-opsec-v6
Overview

• We know policy discrepancies *can happen*

• We know *via anecdote* that policy discrepancies *do happen*

• We want to know the extent to which policy discrepancies *do happen* in the wild
Methodology

1. Derive a list of dual-stack devices
2. Probe devices via IPv4 & IPv6
3. Determine fate of probes vs. network protocol utilized
Finding Dual-Stack Hosts

• Glib version:
  • Obtain lists of devices (names or IP addresses)
  • Leverage DNS to provide connective tissue between IPv4 & IPv6 addresses
  • Calibration phase to enhance confidence in connective tissue

• Full details of methodology in the paper
Dual-Stack Devices

• Device lists:
  • 25K dual-stack routers
  • 520K dual-stack servers

• Note: we verified that all identified dual-stack hosts speak both IPv4 and IPv6
Probing

- Probe each host via IPv4 and IPv6
- Use *scamper* to send:
  - basic probes
  - *traceroute*-style probes

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Router</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Echo</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SSH</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Telnet</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BGP</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SMB</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>MySQL</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RDP</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DNS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NTP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SNMPv2</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Judgment

• Crucial assumption: probes with different network protocols and different fates indicate a policy difference

• E.g., an unsuccessful IPv4 probe and a successful IPv6 probe indicates a policy difference

• Small scale independent validation, stay tuned
Router Results

Percent of Population Open

NTP
- IPv4: 0.4%
- IPv6: 15.3%
- Both: 18.0%
- Increase: +14%

SSH
- IPv4: 6.2%
- Increasing: +166%

BGP
- IPv4: 0.3%
- Increasing: +73%

Telnet
- IPv4: 3.9%
- Increasing: +156%

SNMP
- IPv4: 1.8%
- Increasing: +285%

HTTP
- IPv4: 0.4%
- Decreasing: -3%

HTTPS
- IPv4: 0.4%
- Decreasing: -12%

DNS
- IPv4: 0.2%
- Decreasing: -6%

IPv6

Allman
Server Openness

Percent of Population Open

HTTP: 4.9%
HTTPS: 4.1%
SSH: 3.1%
FTP: 0.8%
DNS: 0.4%
NTP: 0.4%
RDP: 0.3%
SMB: 0.3%
Telnet: 0.3%
MySQL: 0.1%
SNMP: 0.1%

Both: 4.9%
IPv4: 4.1%
IPv6: 3.8%

Allman

13
Intra-Network Uniformity

- Want to know how uniform policies are within networks

- For each routed prefix and each application:
  - calculate the fraction of hosts with the most popular policy (v4-only, v6-only or both)
Intra-Network Uniformity

Policy settings are generally systematic within network boundaries.

(a) Routers
(b) Servers
Policy Enforcement

• How:
  • Passive: probe is silently discarded
  • Active: probe triggers an error (TCP RST, ICMP unreachable, etc.)

• Where:
  • Target: destination of probe
  • Other: some hop on path prior to destination
### Policy Enforcement

<table>
<thead>
<tr>
<th>Mode</th>
<th>Router ($R_T$)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean IPv4</td>
</tr>
<tr>
<td>Open</td>
<td>4.17</td>
</tr>
<tr>
<td>Passive:Target</td>
<td>43.50</td>
</tr>
<tr>
<td>Passive:Other</td>
<td>10.12</td>
</tr>
<tr>
<td>Active:Target</td>
<td>30.93</td>
</tr>
<tr>
<td>Active:Other</td>
<td>3.55</td>
</tr>
</tbody>
</table>

- IPv6 uses more active blocking than IPv4
- Target host responsible for more blocking in IPv4
## Policy Enforcement

<table>
<thead>
<tr>
<th>Mode</th>
<th>Server ($S_T$) Mean IPv4</th>
<th>Mean IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>18.57</td>
<td>18.89</td>
</tr>
<tr>
<td>Passive:Target</td>
<td>36.06</td>
<td>31.17</td>
</tr>
<tr>
<td>Passive:Other</td>
<td>16.31</td>
<td>14.20</td>
</tr>
<tr>
<td>Active:Target</td>
<td>22.82</td>
<td>27.61</td>
</tr>
<tr>
<td>Active:Other</td>
<td>2.09</td>
<td>2.79</td>
</tr>
</tbody>
</table>

- IPv6 uses more active blocking
- Policy enforcement equally shared between target and other
Notification & Validation

- Wanted to know if our findings were …
  - … correct?
  - … intentional?
Notification & Validation

- 16 operators contacted, 12 responded
- All confirmed our results
- All indicated different policy was unintentional

<table>
<thead>
<tr>
<th>Operator</th>
<th>Host-App Pairs w/Only IPv6 Open</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global CDN 1</td>
<td>3</td>
<td>✓</td>
</tr>
<tr>
<td>Tier1 ISP 1</td>
<td>498</td>
<td></td>
</tr>
<tr>
<td>Global Transit Pro. 1</td>
<td>201</td>
<td>✓</td>
</tr>
<tr>
<td>Large Hosting Pro. 1</td>
<td>≈800</td>
<td></td>
</tr>
<tr>
<td>Large University 1</td>
<td>5</td>
<td>✓</td>
</tr>
<tr>
<td>Large University 2</td>
<td>6</td>
<td>✓</td>
</tr>
<tr>
<td>Large University 3</td>
<td>989</td>
<td>✓</td>
</tr>
<tr>
<td>National ISP 1</td>
<td>4757</td>
<td>✓</td>
</tr>
<tr>
<td>National ISP 2</td>
<td>89</td>
<td>✓</td>
</tr>
<tr>
<td>Research/Ed. ISP 1</td>
<td>1</td>
<td>✓</td>
</tr>
<tr>
<td>Research/Ed. ISP 2</td>
<td>523</td>
<td>✓</td>
</tr>
<tr>
<td>Research/Ed. ISP 3</td>
<td>77</td>
<td>✓</td>
</tr>
<tr>
<td>Research/Ed. ISP 4</td>
<td>17</td>
<td>✓</td>
</tr>
<tr>
<td>Small Hosting Pro. 1</td>
<td>17</td>
<td>✓</td>
</tr>
<tr>
<td>Small ISP 1</td>
<td>12</td>
<td>✓</td>
</tr>
<tr>
<td>Small Transit Pro. 1</td>
<td>2</td>
<td>✓</td>
</tr>
</tbody>
</table>
Final Bits

- Unintentionally open services are a *symptom* of a less mature IPv6 ecosystem
- So, be diligent beyond ACLs

- Our test modules are available as part of *scamper*
- So, test your own networks/devices
Questions? Comments?

Mark Allman, mallman@icir.org
http://www.icir.org/mallman/
@mallman_icsi
References

• NDSS paper:
  http://www.icir.org/mallman/pubs/CLAB16/

• Google’s IPv6 Statistics:

• SIGCOMM paper on IPv6 adoption:
  http://www.icir.org/mallman/pubs/CAZ+14/