Defending against DNS reflection amplification attacks
What is a DNS reflection amplification attack?
“What measures can be taken to defend against DNS amplification attacks on authoritative name servers, and what is the effectiveness of Response Rate Limiting?”
Which defense mechanisms are available? Where to defend?

- Botnet controlled PC.
  - Patches, Antivirus, Antispyware etc.
- ISP.
  - BCP38: Ingress filtering.
- DNS.
  - Firewall, TCP, Dampening, RRL.
Why focus on RRL?

- Most promising;
- The only technique that is actively used and supported;
- Available for BIND and NSD;
- Research proposed by NLnet Labs.
How is the effectiveness of RRL measured?

- 5 Different attacks
  - Repeating query (ANY)
  - Varying query (25%, 50%, 75%, 100%)
- Inbound vs outbound traffic (Amplification Ratio)
- Slip settings
Lab setup.

- **Name Server**
  - BIND9.9.2-P1 + RRL
  - Cacti + RDC

- **Attacker**
  - Requests with spoofed IP

- **Victim**
  - Amplified response

- **TCPReplay + pcap file**
RRL Measurements
RRL Explained

- **MAX Responses per second = 5**
- **Window size = 5**
- **Maximum bucket = 25**
- **Minimum bucket = 0**

| 10.1.1.0/24, prague.os3.nl, status: noerror | 1/5 |
| 10.1.1.0/24, status: NXDOMAIN           | 25/5 |
Measurements 1/5 – Repeating ANY attack

\[
\begin{align*}
\text{(4 MB/s)} & \quad = 51,2 \\
\text{(80 KB/s)} & \quad = 1
\end{align*}
\]
Measurements 1/5 – Repeating ANY attack

<table>
<thead>
<tr>
<th>SLIP</th>
<th>False positives</th>
<th>In</th>
<th>Out</th>
<th>Amp. ratio</th>
<th>TCP responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slip 1</td>
<td>0%</td>
<td>80KB/s</td>
<td>81KB/s</td>
<td>≈1:1</td>
<td>100%</td>
</tr>
<tr>
<td>Slip 2</td>
<td>50%</td>
<td>79KB/s</td>
<td>39KB/s</td>
<td>≈1:0.5</td>
<td>87.5%</td>
</tr>
<tr>
<td>Slip 3</td>
<td>66.6%</td>
<td>79KB/s</td>
<td>26KB/s</td>
<td>≈1:0.3</td>
<td>66%</td>
</tr>
<tr>
<td>Slip 5</td>
<td>80%</td>
<td>80KB/s</td>
<td>16KB/s</td>
<td>≈1:0.2</td>
<td>49%</td>
</tr>
<tr>
<td>Slip 10</td>
<td>90%</td>
<td>80KB/s</td>
<td>8KB/s</td>
<td>≈1:0.1</td>
<td>27%</td>
</tr>
</tbody>
</table>
Measurements 2/5 – Varying query attack (25%)
Measurements 2/5 – Varying query attack (25%)
Measurements 3/5 – Varying query attack (50%)
Measurements 3/5 – Varying query attack (50%)

![Traffic-Kaa, NLnetLabs.nl-Lab0 graph]

- (1.19 MB/s) = 15.3
- (78 KB/s)

(469 KB/s) = 5.9

(77 KB/s)

From 2013/01/16 10:46:54 To 2013/01/16 11:16:54

- Inbound: Current: 76.68 k Average: 77.98 k Maximum: 79.42 k
- Total In: 145.04 MB
- Outbound: Current: 468.45 k Average: 782.73 k Maximum: 1.19 M
- Total Out: 1.46 GB
Measurements 4/5 – Varying query attack (75%)
Measurements 4/5 – Varying query attack (75%)

<table>
<thead>
<tr>
<th>SLIP</th>
<th>False positives</th>
<th>In</th>
<th>Out</th>
<th>Amp. ratio</th>
<th>TCP responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slip 1</td>
<td>0%</td>
<td>79KB/s</td>
<td>689KB/s</td>
<td>1:8.72</td>
<td>100%</td>
</tr>
<tr>
<td>Slip 2</td>
<td>50%</td>
<td>78KB/s</td>
<td>680KB/s</td>
<td>1:8.72</td>
<td>87.5%</td>
</tr>
<tr>
<td>Slip 3</td>
<td>66.6%</td>
<td>79KB/s</td>
<td>677KB/s</td>
<td>1:8.57</td>
<td>66%</td>
</tr>
<tr>
<td>Slip 5</td>
<td>80%</td>
<td>79KB/s</td>
<td>673KB/s</td>
<td>1:8.52</td>
<td>49%</td>
</tr>
<tr>
<td>Slip 10</td>
<td>90%</td>
<td>79KB/s</td>
<td>665KB/s</td>
<td>1:8.42</td>
<td>27%</td>
</tr>
</tbody>
</table>
Measurements 5/5 – Varying query attack (100%)

<table>
<thead>
<tr>
<th>RRL</th>
<th>In</th>
<th>Out</th>
<th>Amp. ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>80KB/s</td>
<td>891KB/s</td>
<td>1:11.14</td>
</tr>
<tr>
<td>Enabled</td>
<td>80KB/s</td>
<td>891KB/s</td>
<td>1:11.14</td>
</tr>
</tbody>
</table>
Results

RRL Effectiveness

Traffic MB/sec vs % Existing domains

- Out - RRL Enabled
- Out - RRL Disabled
- Inbound

Graph showing the impact of RRL effectiveness on traffic MB/sec as % Existing domains increase.
DNS Dampening

- Successful against distributed attacks
- Counts requests instead of responses
- Penalty points for every request
- No mechanism like slip implemented
- Most parameters cannot be changed in configuration
Conclusion

- **RRL effective:**
  - Attacks repeating the same query.

- **RRL ineffective:**
  - Varying query attacks / Distributed attacks.

- **DNS Dampening:**
  - Effective against all tested attacks.
  - No mechanism to prevent false positives.

- Need to push BCP38