Motivation

• DNS is critical infrastructure
  – The Internet needs DNS
  – The DNS root is part of this infrastructure

• But can users talk to the real DNS root?
  – Implications for security and Internet governance
What is the DNS root?

- DNS root is top of hierarchy
- 13 logical servers
- Servers anycasted to varying degrees
  - L root has 144 instances
  - B root has one instance
Do we care about unauthorized roots?

- **We care because DNSSEC is not enough**
  - DNSSEC only provides integrity, not availability

- **Censorship** is an attack on availability
  - Countries can and do attack DNS

- **Masquerading roots affect Internet Governance**
  - Countries could create their own version of DNS
What are we looking for?

ISP or National Internet

Host → DNS Proxy (1) → DNS Root Mirror (2) → Actual DNS Root
Problem Statement

• Problem:
  – Can users talk to the real DNS root?

• Solution:
  – Collect data from a large set of users
  – Look for anomalous response times and server identities
  – Focus on B root because there is only 1 instance
Outline

• Motivation
• Dataset and Methods
• Results
### Dataset

#### RIPE Atlas

<table>
<thead>
<tr>
<th>Measurements</th>
<th>Dates</th>
<th>Manipulation that can be Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>July 6-13, 2014</td>
<td>Proxies and root mirrors</td>
</tr>
<tr>
<td>HOSTNAME.BIND</td>
<td>July 22, 2014</td>
<td>Proxies and root mirrors</td>
</tr>
<tr>
<td>Traceroutes</td>
<td>July 6, 2014</td>
<td>Root mirrors</td>
</tr>
</tbody>
</table>

#### BGP

<table>
<thead>
<tr>
<th>Measurements</th>
<th>Dates</th>
<th>Manipulation that can be Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE RIS</td>
<td>July 6-13, 2014</td>
<td>Root mirrors</td>
</tr>
<tr>
<td>RouteViews</td>
<td>July 7, 2014</td>
<td>Root mirrors</td>
</tr>
</tbody>
</table>
Methods

• Response time
  – Did the response beat the speed of light?
  – Use RIPE Atlas pings

• Server identity
  – Is the user talking to the real root?
  – Use RIPE Atlas HOSTNAME.BIND queries, traceroutes, and BGP data
Response time

• Did the response beat the speed of light?
  – Geolocate probes with RIPE and MaxMind
  – Find the **minimum RTT** from a week of pings for each probe from RIPE Atlas
  – Compare all responses from a region with expected RTT and look for outliers
Server identity: HOSTNAME.BIND

• Does the server identity match B root?
  – Collect server identity and DNS response time
  – Compare HOSTNAME.BIND identity to expected value for B root

• Compare ping and DNS response times
  – Expect DNS and ping response time to be similar
  – If DNS response time is substantially lower, then DNS proxy in use
Server identity: traceroutes

- Hypothesis: root mirrors may have different last hop (Penultimate Router or PR)
  - Extract and compare the last hop/ PR from traceroutes
• Hypothesis: an ISP may redirect multiple root addresses to the same instance
  – Compare the similarity in paths to different roots
Server identity: BGP

• What if an ISP tried used BGP to redirect to their root mirror?
  – What if their route was propagated?

• Is anyone doing a prefix hijack on B root?
  – Collected RIBS from RouteViews and updates and RIBs from RIPE RIS
  – Looked for unexpected announcements for B root’s prefix
Outline

• Motivation
• Dataset and Methods
• Results
Comparing HOSTNAME.BIND responses

• We saw 11 anomalous responses
  – B root responses have the form \( b[0-9] \)
  – 3 responses with no answer, 3 with name of ISP, and 5 other responses

• What is the purpose of the DNS proxy?
  – Servers identifying with the ISP may be intended to improve performance
  – Other servers appear to be placed by end user, e.g. in one ISP, 1/4 probes had a DNS proxy
Detecting DNS proxies

The outlier with a much smaller DNS response time is a DNS proxy
Detecting unauthorized roots

The outlier with a much smaller ping time is a DNS root mirror
Detecting root mirrors is not easy

- Need to differentiate between errors and legitimately low ping times
  - 1 probe incorrectly geolocated with both sources
  - 2 probes incorrectly interpreted ICMP errors as ping responses
- We manually explored the low ping times to ensure accuracy
Results summary

<table>
<thead>
<tr>
<th>Analysis Method</th>
<th>Manipulation Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTNAME.BIND</td>
<td>10 DNS proxies and 1 root mirror</td>
</tr>
<tr>
<td>DNS and ping response time</td>
<td>10 DNS proxies</td>
</tr>
<tr>
<td>Ping response time</td>
<td>1 root mirror</td>
</tr>
<tr>
<td>Traceroute penultimate routers</td>
<td>No evidence of manipulation</td>
</tr>
<tr>
<td>Traceroute path sharing</td>
<td>No evidence of shared paths between roots</td>
</tr>
<tr>
<td>BGP hijack analysis</td>
<td>No evidence of hijacks</td>
</tr>
</tbody>
</table>
Conclusion

• Addressed important research question: DNS root manipulation
• Developed novel measurement techniques
• Analyzed data from RIPE Atlas to find 10 DNS proxies and 1 root mirror

• Ben Jones: bj6@cs.princeton.edu
Root mirror pings