Analysis of DITL root data and comparison with a full-resolver's data

Kazunori Fujiwara
JPRS and University of Tsukuba
<fujiwara@jprs.co.jp>
DNS-OARC 2014 Spring Workshop
Updates from my previous analysis

• Analyzed DITL data from 2006 to 2010
  – Added some new graphs

• Compared with full-resolver data in 2012
  – A full-resolver sent 100,000 queries to root within 48 hours
  – It may be a typical full-resolver

• Previous analysis was reported at DNS-OARC 2013 Fall Workshop
Datasets and analysis method
DNS-OARC Root Datasets (1)

• "A Day in the Life of the Internet" (DITL) is a large-scale data collection project undertaken by CAIDA and DNS-OARC every year since 2006.

  – https://www.dns-oarc.net/oarc/data/ditl
  – 50 hours packet capture at root DNS servers and other DNS servers (48 hours are used by this analysis)
  – Source IP addresses of i.root-servers.net data are anonymized
## DNS-OARC Root Datasets (2)

<table>
<thead>
<tr>
<th>Year</th>
<th>Start (UTC)</th>
<th>End</th>
<th>List of root servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Jan 10 0000</td>
<td>Jan 12 0100</td>
<td>c,e,f,k (4/13)</td>
</tr>
<tr>
<td>2007</td>
<td>Jan 09 0000</td>
<td>Jan 11 0000</td>
<td>c,f,k,m (4/13)</td>
</tr>
<tr>
<td>2008</td>
<td>Mar 18 0000</td>
<td>Mar 20 0000</td>
<td>a,c,e,f,h,k,l,m (8/13)</td>
</tr>
<tr>
<td>2009</td>
<td>Mar 30 0000</td>
<td>Apr 02 0000</td>
<td>a,c,e,f,h,k,l,m (8/13), 72 hours</td>
</tr>
<tr>
<td>2010</td>
<td>Apr 14 0000</td>
<td>Apr 16 0000</td>
<td>a,b,c,d,e,f,g,h,i,j,k,l,m (12/13)</td>
</tr>
<tr>
<td>2011</td>
<td>Apr 12 1200</td>
<td>Apr 14 1200</td>
<td>a,c,d,e,f,h,j,k,l,m (10/13)</td>
</tr>
<tr>
<td>2012</td>
<td>Apr 17 1200</td>
<td>Apr 19 1200</td>
<td>a,c,e,f,h,j,k,l,m (9/13)</td>
</tr>
<tr>
<td>2013</td>
<td>May 28 1200</td>
<td>May 30 1200</td>
<td>a,c,d,e,f,h,j,k,l,m (10/13)</td>
</tr>
</tbody>
</table>
Analysis method of Root data

• Newly developed C program reads pcap files
• It counts number of some kinds of queries per IP address
  – All queries, RD=0 queries, EDNS0 queries,
  – DO set queries, name error queries,
  – "." DNSKEY queries (RD=0), "." NS queries,
  – "." Queries, UDP checksum off queries
  – Port number bitmaps (to analyze source port randomization trends)
  – TLD bitmaps
University of Tsukuba Dataset

- Associate researchers and the author collected packet captures at one of full-resolvers at University of Tsukuba
- Around January 2011 to August 2012
- A data exist at the same timing as DITL-2012
  - Apr 17 12:00 to Apr 19 12:00 UTC
  - 72,355,778 DNS packets captured (418 pps)
  - 28,815,955 stub queries observed (166 qps)
  - 8429 unique query source addresses
Analysis method of full-resolver data

• Newly developed perl program
  – reads pcap files
  – classifies packets into
    • Stub queries/responses
    • Full-resolver to authoritative queries/responses
  – classifies destination addresses into
    • Root, TLDs, other authoritative servers
  – parses each section
  – parses referrals (NS+glue)
  – counts characteristics
Results
## Number of IP addrs seen at root 48h

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data from</td>
<td>10 root</td>
<td>9 root</td>
<td>10 root</td>
</tr>
<tr>
<td>Total</td>
<td>7,591,031</td>
<td>8,989,786</td>
<td>8,547,065</td>
</tr>
<tr>
<td>RD0</td>
<td>5,846,612</td>
<td>5,859,493</td>
<td>6,081,035</td>
</tr>
<tr>
<td>EDNS0</td>
<td>2,340,543</td>
<td>2,906,287</td>
<td>3,572,804</td>
</tr>
<tr>
<td>DO=1</td>
<td>2,018,839</td>
<td>2,621,660</td>
<td>3,283,728</td>
</tr>
<tr>
<td>Update</td>
<td>105,131</td>
<td>138,778</td>
<td>228,633</td>
</tr>
<tr>
<td>Update Only</td>
<td>71,972</td>
<td>99,902</td>
<td>179,874</td>
</tr>
<tr>
<td>Non-existent TLD</td>
<td>2,606,340</td>
<td>2,641,072</td>
<td>2,619,836</td>
</tr>
<tr>
<td>Existing TLD</td>
<td>7,361,794</td>
<td>8,697,606</td>
<td>8,142,126</td>
</tr>
<tr>
<td>. NS</td>
<td>1,940,015</td>
<td>1,871,995</td>
<td>2,082,649</td>
</tr>
<tr>
<td>. Only</td>
<td>26,877</td>
<td>36,920</td>
<td>105,784</td>
</tr>
<tr>
<td>. DNSKEY (RD0)</td>
<td>14,092</td>
<td>43,782</td>
<td>269,390</td>
</tr>
<tr>
<td>. DNSKEY . Only</td>
<td>571</td>
<td>2,828</td>
<td>64,612</td>
</tr>
</tbody>
</table>

Copyright © 2014 Japan Registry Services Co., Ltd.
New graphs

• Horizontal axis: years from 2006 to 2013
• Graphs
  – Number of queries
  – Number of IP addresses
  – Ratio of IP addresses/queries
  – Port randomization status
• Data
  – Total, Update, EDNS0, DO
  – Repeat_port … an IP address sent from same port
    • one case of using static source port number
  – UdpSumOff
  – root: query name “.”
  – “.” DNSKEY
Ratio of addresses/queries

(update/Addresses, update/Queries, repeat_port/Addresses, repeat_port/Queries, root/Addresses, root/Queries, DNSKEY/Addresses, UdpSumOff/Addresses, UdpSumOff/Queries, EDNS0/Addresses, EDNS0/Queries, DO/Addresses, DO/Queries)
Status of port randomization

• High8 .. High 8 bits of port number
• Low8 .. Low 8 bits of port number
• OrderChange .. Number of changes of port numbers increase and decrease

• Unknown: queries from an IP address < 10
• Static: use of High8 < 4 and use of Low8 < 4
• Limited: use of High8 < 4 or use of Low8 < 4 or OrderChange < 4 (except Static)
• Random: others (port randomization enabled?)

• This classification is under concern
Source port randomization trends

Copyright © 2014 Japan Registry Services Co., Ltd.
Number of queries send from each address, at root, 48 hours

Double logarithmic chart
Horizontal axis: Ranking of IP addresses
Vertical axis: Num. of queries

Reasonable resolvers?
Number of queries from each address

• Without TLD typos,
• There were 318 TLDs and their NS TTLs were 172800 and DS TTLs were 86400 at May 2013
  – They should be cached within 1 or 2 days
• If resolvers work well, they should send only 2 * 318 + priming + root dnskey queries at most.
• However, there are 500,000 IP addresses which send over 1000 queries within 48 hours. Why?
  – They send both existing names and non-existent names
## Some known IP addresses

<table>
<thead>
<tr>
<th>IP Address Description</th>
<th>Total queries to root</th>
<th>Non-existing TLD</th>
<th>&quot;.&quot; queries</th>
<th>Existing name queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>My VPS (IPv4)</td>
<td>177</td>
<td>1</td>
<td>14</td>
<td>162</td>
</tr>
<tr>
<td>My VPS (IPv6)</td>
<td>182</td>
<td>2</td>
<td>12</td>
<td>168</td>
</tr>
<tr>
<td>My home server (IPv4)</td>
<td>1124</td>
<td>34</td>
<td>54</td>
<td>1036</td>
</tr>
<tr>
<td>One of JPRS address</td>
<td>21990</td>
<td>400</td>
<td>3</td>
<td>21587</td>
</tr>
<tr>
<td>One of full resolvers at University of Tsukuba</td>
<td>109215 Too many ?</td>
<td>12200</td>
<td>1298 Too Many?</td>
<td>95717 Too many?</td>
</tr>
</tbody>
</table>
Number of queries send from each address, at root, 48 hours

Full resolver at Univ. of Tsukuba

One of JPRS address

Reasonable resolvers?
Status of the full-resolver at the university

• Software: latest version of BIND 9.6 (April 2012)

• Configuration
  – Recursion only
  – Without DNSSEC validation
  – Without special configurations

• There are packet captures of the full-resolver at the same timing of DITL-2012
Analysis of full-resolver packets

- 72,355,778 packets captured (418 pps)
- 28,815,955 stub queries (166 qps)
  - 1,026,487 non-existing TLD queries
- 8429 unique query source addresses
- 7,499,961 authoritative queries
- 7,329,795 authoritative answers
  - 118,360 root answers
    - 105,781 (89.4%) RCODE 0 Too many
    - 12,579 (10.6%) RCODE 3 Reasonable
  - 687,365 TLD answers
Observations from packet capture (1)

• At out-of-bailiwick delegations, a modern full-resolver will start resolving all DNS server names A and AAAA simultaneously
  – If the cache is empty, it will send twice as many queries as number of NS RRs to root

• TLD typos caused 12579 error responses from root
  – Most of them were different query names
  – Some came from small (negative) cacheable time (1 hour to 3 hours)
Observations from packet capture

(2)

• The full-resolver at the university sent many DNS server name A/AAAA queries to root
  – Cacheable NS name queries are 103,024 (87%)
    • To mitigate attacks ?
    • Zone TTL is small ?
    • Why ?

• To understand this behavior more, I replayed client traffic to some full-resolvers to know that the behavior is true
Replay on some full-resolver software

• Input client traffic
  – 48 hours client query data at University of Tsukuba
  – Same timing, same qname/qtype
  – Original query source addresses are ignored
    • Sent from one IP address

• Tested full-resolvers
  – BIND 9.9.5 (with/without DNSSEC)
  – Unbound 1.4.22 (with/without DNSSEC, increased cache size, specify harden-referral)
    • large cache configuration
      – msg-cache-size: 1024m
      – rrset-cache-size: 1024m
      – infra-cache-numhosts: 500000
## Results of replay

28,815,955 client queries

<table>
<thead>
<tr>
<th></th>
<th>To root</th>
<th>To root Name error</th>
<th>To root No error</th>
<th>To TLD</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIND 9.6 / Observed data</td>
<td>118,360</td>
<td>12,579</td>
<td>105,781</td>
<td>687,365</td>
<td>6,524,070</td>
</tr>
<tr>
<td>BIND 9.9.5</td>
<td>163,187</td>
<td>12,975</td>
<td>150,212</td>
<td>842,592</td>
<td>7,377,712</td>
</tr>
<tr>
<td>BIND 9.9.5 + DNSSEC</td>
<td>663,647</td>
<td>12,727</td>
<td>650,920</td>
<td>1,061,886</td>
<td>7,235,743</td>
</tr>
<tr>
<td>Unbound</td>
<td>99,923</td>
<td>25,914</td>
<td>74,309</td>
<td>3,916,313</td>
<td>16,048,069</td>
</tr>
<tr>
<td>Unbound + large cache</td>
<td>13,300</td>
<td>11,444</td>
<td>1,856</td>
<td>870,650</td>
<td>9,102,884</td>
</tr>
<tr>
<td>Unbound + large cache + harden referral path</td>
<td>20,897</td>
<td>11,234</td>
<td>9,663</td>
<td>2,328,026</td>
<td>11,152,425</td>
</tr>
<tr>
<td>Unbound + large cache + DNSSEC</td>
<td>12,662</td>
<td>11,140</td>
<td>1,522</td>
<td>1,423,789</td>
<td>9,112,902</td>
</tr>
</tbody>
</table>
Summary of replay

- It is preliminary result
  - Need more test and detailed analysis
  - Values change at every experiment
- Both BIND 9 and Unbound generated too many (around 100,000 / 48 hours) root queries
  - 100,000 queries to root is real
- Queries to root increased 4 times when DNSSEC validation enabled on BIND 9
- Unbound with default configuration is not good for middle / large scale sites
  - Because Unbound with default configuration sent 74,309 positive queries to root
  - Unbound with large cache sent only 1,856 queries to root
- Using Unbound may decrease root queries. However queries to other servers may increase
Conclusion

• Port randomization is spreading gradually, however about 10% of IP addresses are still dangerous
• DITL data show that 30,000 IP addresses sent 100,000 or more queries to root DNS servers within 48 hours.
• A full-resolver at University of Tsukuba sent 118,360 queries within 48 hours to root.
• As a result of replay experiment, both BIND 9 and Unbound full-resolvers sent around 100,000 queries to root within 48 hours.
• BIND 9 full-resolvers may send many queries to root DNS servers
  – Unbound send smaller number of queries to root
  – Decreasing queries to root is important
Acknowledgements

• DNS-OARC as the data source of Root dataset
• Academic Computing & Communication Center offers Full-Resolver DNS servers for Campus network of University of Tsukuba