DNSSEC for the Root Zone

IEPG – IETF 77 – Anaheim, USA
March 2010

Joe Abley, ICANN           Matt Larson, VeriSign
This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA
Signing the Root
Quick Recap

- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSASHA256
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately-Unvalidatable Root Zone (DURZ)
For More Detail...

- design documentation
- copies of earlier presentations
- contact information
Signing Other Things

(a brief diversion from the root zone)
ARPA

- IAB first requested that ARPA be signed on 2006-05-09
- ICANN proposed an interim solution
  - long-term solution to follow signed root
- Signed zone published since 2010-03-17
  - interim solution
  - test deployment
IN-ADDR.ARPA

• Re-delegation planned for IN-ADDR.ARPA
  • from root to RIR/IANA servers
  • expected in the next few months

• Proposal to sign IN-ADDR.ARPA will be submitted to US DoC by ICANN following redelegation
E164.ARPA

• E164.ARPA is managed by the RIPE NCC
• RIPE NCC has advised ICANN that they intend to submit a request to add DS records to the ARPA zone in June 2010.
Other ARPA Offspring

• Proposal to sign URI.ARPA, URN.ARPA, IP6.ARPA, IN-ADDR-SERVERS.ARPA, IP6-SERVERS.ARPA submitted 2010-03-19

• Pre-production testing was completed successfully

• If proposal is acceptable, signed zones will be published in a few weeks
Operational Update
## Root Server Status

<table>
<thead>
<tr>
<th>Root Server</th>
<th>Operated by</th>
<th>Signed ARPA</th>
<th>DURZ</th>
<th>LTQC</th>
<th>DITL</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>VeriSign</td>
<td>2010-03-16</td>
<td>2010-02-10</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>B</td>
<td>ISI</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>C</td>
<td>Cogent</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>D</td>
<td>UMD</td>
<td>2010-03-16</td>
<td>2010-03-24</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>E</td>
<td>NASA</td>
<td>2010-03-16</td>
<td>2010-03-24</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>F</td>
<td>ISC</td>
<td>2010-03-17</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>G</td>
<td>US DoD</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>H</td>
<td>US Army</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>I</td>
<td>Autonomica</td>
<td>2010-03-15</td>
<td>2010-03-03</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>J</td>
<td>VeriSign</td>
<td>N/A</td>
<td>2010-05-05</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>K</td>
<td>RIPE NCC</td>
<td>2010-03-15</td>
<td>2010-03-24</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>L</td>
<td>ICANN</td>
<td>2010-03-15</td>
<td>2010-01-27</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>M</td>
<td>WIDE</td>
<td>2010-03-15</td>
<td>2010-03-03</td>
<td>submitting</td>
<td>submitting</td>
</tr>
</tbody>
</table>
KSR Processing

- KSR exchanges continue between VeriSign and ICANN
- software testing
- operational testing
Key Ceremonies

• Many rehearsals complete, more to follow
• Facility requirements continue to be refined, guided by external contributions
• Both east- and west-coast facilities expected to be on-line and tested on schedule
Trusted Community Representatives

- Proposed approach will involve TCRs as key ceremony participants and witnesses

- see Trusted Community Representatives – Proposed Approach to Root Key Management
No Harmful Effects

• No harmful effects have been reported, from DURZ or signed ARPA deployment

• Some ancilliary observations have been made
  • availability of TCP transport
  • fragmentation behaviour
Analysis
<table>
<thead>
<tr>
<th>Code</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>2010-01-27</td>
<td>✔</td>
</tr>
<tr>
<td>A</td>
<td>2010-02-10</td>
<td>✔</td>
</tr>
<tr>
<td>I,M</td>
<td>2010-03-03</td>
<td>✔</td>
</tr>
<tr>
<td>D, E, K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B,C,F,G,H</td>
<td></td>
<td></td>
</tr>
<tr>
<td>J</td>
<td>2010-05-05</td>
<td></td>
</tr>
</tbody>
</table>
Data Is Collected at DNS-OARC

• Priming queries and responses constantly since December 2009
• All queries 24h before and after a root server switches to DURZ
UDP Priming Query Rate

A significant change in priming query rate could indicate a client that’s been “cut off” from the root servers.
UDP Priming Query Rate for the previous 4h as of 2010-01-27 20:00:00

- L-root’s Maintenance Window
- First post-DURZ priming response
- Final pre-DURZ priming response

Whew, no change!
UDP Priming Query Rate for the previous 4h as of 2010-01-27 20:00:00

A typically receives more priming queries than the others.

(E has hourly spikes, not sure why)

These are lower due to missing data
UDP Priming Query Rate
for the previous 4h
as of 2010–02–10 20:00:00

A-root’s Maintenance Window
UDP Priming Query Rate
for the previous 4h
as of 2010–03–03 08:00:00

M-root’s Maintenance Window
UDP Priming Response Size

We expect the mean priming response size to increase as clients receive responses that include RRSIG records.
UDP Priming Query Mean Reply Size for the previous 4h as of 2010–01–27 20:00:00

Gradual increase in mean response size as L-root nodes switch to DURZ
UDP Priming Query Mean Reply Size for the previous 4h as of 2010–02–10 20:00:00

Mean reply size did not increase as much as it did for L.
UDP Priming Query Mean Reply Size for the previous 4h as of 2010-03-03 08:00:00

-Bytes-
Total UDP Query Rate

Significant changes in the overall UDP rate may also indicate clients having problems with DURZ responses.
UDP Query Rate

Queries Per Second

2010-01-19  Pre DURZ
2010-01-26  L DURZ
2010-02-09  A DURZ
2010-03-02  I,M DURZ

A
C
D
E
F
G
H
I
J
K
L
M

5000
10000
15000
20000
25000
30000
This spike is due to attack-like traffic.
TCP Query Rate

We expect an increase in TCP queries from clients that cannot receive response larger than 512 octets.
TCP Query Rate

M-root’s Maintenance Window
RCODE/DO

Knowing the RCODE/DO mixture helps us predict changes in bandwidth for responses.
Bufsize/DO

We look at changes in advertised Bufsize and DO values over time to see if problematic clients are migrating to non-DURZ roots.
Bufsize/DO Mix
2010–03–02.06:00:00 — 2010–03–04.18:00:00

Fraction of Queries

1.0
0.8
0.6
0.4
0.2

A
C
D
E
F
H
J
K
L
M

nodedns
bufsz<=512,DO=0
bufsz<=1500,DO=0
bufsz<=4096,DO=0
bufsz>4096,DO=0
bufsz<=512,DO=1
bufsz<=1500,DO=1
bufsz<=4096,DO=1
bufsz>4096,DO=1
DNSSEC Query Types

We look at DNSSEC query types for possible evidence of premature validation.
Client Rate Buckets

Another way to look for problem clients is to group them by how many queries they send.
Client Query Rates
For L-root

There are this many clients:
1, 3, 10, 30, 100, 300, 1000, 3000.

Making this many queries:
1/sec, 2/sec, 4/sec, 8/sec, 16/sec, 32/sec, 64/sec, 128/sec, 256/sec, 512/sec, 1024/sec.
Acknowledgements

• Thanks to the Root Server Operators that are providing data.
• Thanks to ISC for being DNS-OARC’s remote hands.
More Information

www.root-dnssec.org