Rollover and Die?

George Michaelson, APNIC
Geoff Huston, APNIC
Patrik Wallström, IIS
Roy Arends, Nominet UK
We’re under attack!!!

On the 16th of december, traffic more than doubled
DNSKEY amplification attack
DNSKEY response size

Response size: 990 Bytes
Query rate: 2000 qps

15.8 Mbps

Additional load
Who does this?
Who does this?
What was special about the 16th?

The latest trust anchors are available in the following two formats:

**BIND-style:**
You can download the file containing all the keys published on 16 December 2009 [here](https://www.ripe.net/projects/disi/keys/).
And the PGP signature of the file [here](https://www.ripe.net/projects/disi/keys/).

**Zone-file format:**
You can download the file containing all keys published on 16 December 2009 [here](https://www.ripe.net/projects/disi/keys/) in zone-file format.
And the PGP signature of the file [here](https://www.ripe.net/projects/disi/keys/).

As explained in the draft version of the [key maintenance procedure](https://www.ripe.net/projects/disi/keys/), new keys will be added or removed as per the schedule below.

**Most Recent Key Event:**
16 December 2009: Current (deprecated) keys are removed. One key in use.

**Future Key Roll Summary:**
23 March 2010: New keys are published, current keys are deprecated but not removed. Two keys in use.
14 June 2010: Current (deprecated) keys are removed. One key in use.
21 September 2010: New keys are published, current keys are deprecated but not removed. Two keys in use.

You can find more information on the [DISI](https://www.ripe.net/projects/disi/keys/) pages of this site. There is also more information on DNSSEC available. You should see the [DNSSEC HOWTO](https://www.ripe.net/projects/disi/keys/) and [DNSSEC Deployment at the RIPE NCC](https://www.ripe.net/projects/disi/keys/) pages.

**Important Note:**
Configuring DNSSEC on your name servers may cause problems if your firewall filters DNS packets larger than 512 bytes. DNSSEC requires support, which allows packet sizes larger than 512 bytes.

If your name server is behind a firewall that blocks these packets, you either need to configure your firewall to allow EDNS packets, or you can configure your name server to send EDNS packets smaller than 512 bytes.
What was special about the 16th?

Zone-file format:
You can download the file containing all keys published on 16 December 2009 here, in zone-file format.
And the PGP signature of the file here.

As explained in the draft version of the key maintenance procedure, new keys will be added or removed a

Most Recent Key Event:

16 December 2009: Current (deprecated) keys are removed. One key in use.

Future Key Roll Summary:

23 March 2010: New keys are published, current keys are deprecated but not removed. Two keys in use
14 June 2010: Current (deprecated) keys are removed. One key in use.
21 September 2010: New keys are published, current keys are deprecated but not removed. Two keys in

You can find more information on the DISI pages of this site. There is also more information on DNSSEC HOWTO, and DNSSEC Deployment at the RIPE NCC pages.
Hanlon’s razor

Never attribute to **malice** that which can be explained by **stupidity**.
Why so many clients?

- Fedora bug report 17th Jan 2010
  - (1 month after the roll)
- Operator reports getting 240,000 log entries in 24hr
  - “no valid key”
- Dnssec-conf tool contained a hard-configured trust anchor file
  - Obsolete after the 16th.
What was special about the 16th?
What was special about the 16th?

what a great lesson

Randy Bush’s response
Current load for in-addr.arpa

getting better, below 1000 qps right now
But decline not fast enough before new roll
The Load Projection

![Graph showing load projection from November 9, 2008 to March 4, 2010. The graph indicates the current (cur) and average (avg) values for inbound and outbound traffic.]

- **Inbound**
  - Current: 9.86M
  - Average: 7.02M
  - Maximum: 10.66M

- **Outbound**
  - Current: 32.49M
  - Average: 20.01M
  - Maximum: 41.02M
The Load Projection

![Graph showing data with annotations: Inbound current: 9.86M, average: 7.02M, max: 10.66M; Outbound current: 32.49M, average: 20.01M, max: 41.02M.](image-url)
The Load Projection

![Graph showing inbound and outbound traffic over time with specific data points for 2008-11-09 to 2010-03-04.](image)

- **Inbound**
  - Current: 9.86M
  - Average: 7.02M
  - Maximum: 10.66M

- **Outbound**
  - Current: 32.49M
  - Average: 20.01M
  - Maximum: 41.02M
The Load Projection

![Graph showing load projection with removal and addition points.](image)

- **Inbound**
  - Current: 9.86M
  - Average: 7.02M
  - Maximum: 10.66M

- **Outbound**
  - Current: 32.49M
  - Average: 20.01M
  - Maximum: 41.02M
Was this a one off event?

Swedish, June 2009
Was this a one off event?

Sweden, June 2008
Was this a one off event?

Swedish, June 2008

DNSSEC-related Queries by QType

Query Rate (q/s)

1st resolver fix
Was this a one off event?

Sweden, June 2008

1st resolver fix

2nd resolver fix
Why so many Queries?

- Resolvers are supposed to cache dnskey
- Even when those are bad
- Resolvers should be nice, not aggressive
- So many resolvers, so few servers
Why so many Queries?

• Bind bug in all versions
• Depth First Search (DFS) problem
• Chain of trust validation:
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
root
```

```
TA
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
www.dnssec.se  root
A     SIG
TA
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
dnssec.se
A    SIG    KEY
```

```
root
TA
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
+----------------+  +----------------+  +----------------+
| dnssec.se      |  | se              |  | root            |
| A   SIG        |  | KEY            |  | TA              |
+----------------+  +----------------+  +----------------+
| DS            |
+----------------+  +----------------+  +----------------+``
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
  dnssec.se  se  root
  A  SIG  KEY  DS  KEY  TA
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
      dnssec.se | se  | root  | root
      A  SIG    | DS  | KEY   | DS
      KEY       |     |       | TA
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
<table>
<thead>
<tr>
<th>dnssec.se</th>
<th>se</th>
<th>root</th>
<th>root</th>
</tr>
</thead>
<tbody>
<tr>
<td>A SIG</td>
<td>DS</td>
<td>DS</td>
<td>TA</td>
</tr>
<tr>
<td>KEY</td>
<td>KEY</td>
<td>KEY</td>
<td></td>
</tr>
</tbody>
</table>
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

```
<table>
<thead>
<tr>
<th>DNSSEC</th>
<th>A</th>
<th>SIG</th>
<th>KEY</th>
<th>DS</th>
<th>KEY</th>
<th>DS</th>
<th>KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>3</td>
<td>3</td>
<td>13</td>
<td>13</td>
<td>20</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>ROOT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Why so many Queries?

- Bind bug in all versions
- Depth First Search (DFS) problem
- Chain of trust validation:

\[
3 \times 3 \times 13 \times 13 \times 20 \times 20 = 608400 \text{ queries}
\]
• Reported the depth first search bug on februari 8th
• Reported the depth first search bug on februari 8th
• Acknowledged the problem
  – fundamental fix, needs thorough testing.
• Reported the depth first search bug on February 8th
•Acknowledged the problem
  – fundamental fix, needs thorough testing.
•released BIND 9.7.0 with bug
  – first version that can validate the root
  – “Exercise caution”, ignores the lame DS issue
• Reported the depth first search bug on februari 8th
• Acknowledged the problem
  – fundamental fix, needs thorough testing.
• released BIND 9.7.0 with bug
  – first version that can validate the root
  – “Exercise caution”, ignores the lame DS issue
• released BIND 9.6.2 with bug
  – root-validation back ported, no 5011
    • tick tock
- Reported the depth first search bug on February 8th
- Acknowledged the problem
  - fundamental fix, needs thorough testing.
- released BIND 9.7.0 with bug
  - first version that can validate the root
  - “Exercise caution”, ignores the lame DS issue
- released BIND 9.6.2 with bug
  - root-validation back ported, no 5011
  - tick tock
- Announced a patch as soon as possible.
  - still waiting
  - folks are deploying 9.7.0 and 9.6.2 right now
The Perfect Storm

- DNSSEC deployment at root (DURZ)
  - guess what: lame trust-anchor, don’t configure
• DNSSEC deployment at root (DURZ)
  – guess what: lame trust-anchor, don’t configure
The Perfect Storm
The Perfect Storm

- No automatic trust anchor roll (5011)
  - 9.7.0 implementation is buggy
    - promised fix in 9.7.1
  - 9.6.2 not planned
The Perfect Storm

• No automatic trust anchor roll (5011)
  – 9.7.0 implementation is buggy
    • promised fix in 9.7.1
  – 9.6.2 not planned

• DLV mishaps:
  – DLV registry promiscuously scrapes TLD keys
    • Just another chain of trust
  – .PR rolled its key
    • was unavailable to DLV users for days
    • caused a major packet storm
The Perfect Storm

• Multiple trust anchor problem
  – TLD Trust Anchors trumps Root Trust Anchor
    • stale TLD Trust Anchor trumps valid Root Trust Anchor
The Perfect Storm

- Multiple trust anchor problem
  - TLD Trust Anchors trump Root Trust Anchor
    - stale TLD Trust Anchor trumps valid Root Trust Anchor

- Doom scenario:
  - TLD registers DS in root
  - new policy: don’t announce rolls, depend on root
    - That is the way NS records works as well
  - Operators won’t update TLD trust anchor anymore
    - Why would they, they’ve configured root trust-anchor
A Series Of Unfortunate Events

- buggy software
A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem
A Series Of Unfortunate Events

• buggy software
• DNSSEC @ root
• multiple trust anchor problem
• no 5011 deployment
A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem
- no 5011 deployment
- opportunistic DLV scraping
A Series Of Unfortunate Events

- buggy software
- DNSSEC @ root
- multiple trust anchor problem
- no 5011 deployment
- opportunistic DLV scraping
- Frequent Rollover Syndrome
  - rolling rolling rolling, keep them DNSKEYs rolling.
Frequent Rollover Syndrome

- Advice seems to be:
  - roll the key as often as you can
  - Some roll twice a year, some roll monthly
Frequent Rollover Syndrome

• Advice seems to be:
  – roll the key as often as you can
  – Some roll twice a year, some roll monthly

• Advice is completely misguided:
  – too many sigs do not leak the key.
  – Intention is to mitigate a compromised key fallout
  – but there is no perfect forward security
Frequent Rollover Syndrome

• Advice seems to be:
  – roll the key as often as you can
  – Some roll twice a year, some roll monthly

• Advice is completely misguided:
  – too many sigs do not leak the key.
  – Intention is to mitigate a compromised key fallout
  – but there is no perfect forward security

• If a key can be compromised in 1 year, it can be compromised in 6 months for twice the cost
Frequent Rollover Syndrome

• Advice seems to be:
  – roll the key as often as you can
  – Some roll twice a year, some roll monthly

• Advice is completely misguided:
  – too many sigs do not leak the key.
  – Intention is to mitigate a compromised key fallout
  – but there is no perfect forward security

• If a key can be compromised in 1 year, it can be compromised in 6 months for twice the cost

• Other reasons: educate operators, exercise procedures
  – all irrelevant, never mess with a critical production system
Solution

• Fix the buggy software already
  – stop releasing versions that have problems
  – (Help fund BIND-10)

• Don’t roll keys (too often)
  – be practical

• Do not endorse configuration of trust-anchors when parent is signed.
  – no 5011, no web-page with listed keys, no DLV, no ITAR
  – Manage all through a signed parent.

• When parent is not signed:
  – Use proper 5011. Use ISC’s DLV.
Questions ? Remarks ? Observations ?

http://www.potaroo.net/ispcol/2010-02/rollover.html

Thanks to
  Anand Buddhdev
  Patrik Wallström
  George Michaelson
  Geoff Huston
  David Conrad
  Folks at ISC
http://www.potaroo.net/ispcol/2010-02/rollover.html

Thanks to
   Anand Buddhdev
   Patrik Wallström
   George Michaelson
   Geoff Huston
   David Conrad
   Folks at ISC

Question: If you’ve deployed DNSSEC and rolled your (ksk) key, look at the stats around that period, and (pretty) please report them back to us.