Monitoring DNSSEC, not everything is perfect, yet

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

SATIN, 4 April 2011
DNSSEC shakes monitoring

1. We all know that a serious DNS zone must be monitored continuously and automatically...
We all know that a serious DNS zone must be monitored continuously and automatically...

Many tests were not done before the introduction of DNSSEC, for instance a clean path for all sizes of packets (my talk at the OARC workshop in Denver),
DNSSEC shakes monitoring

1. We all know that a serious DNS zone must be monitored continuously and automatically...

2. Many tests were not done before the introduction of DNSSEC, for instance a clean path for all sizes of packets (my talk at the OARC workshop in Denver),

3. DNSSEC-specific tests are typically far from complete, leading to embarassing publications of failures on public mailing lists,
DNSSEC shakes monitoring

1. We all know that a serious DNS zone must be monitored continuously and automatically...

2. Many tests were not done before the introduction of DNSSEC, for instance a clean path for all sizes of packets (my talk at the OARC workshop in Denver),

3. DNSSEC-specific tests are typically far from complete, leading to embarassing publications of failures on public mailing lists,

4. Some tests detect failures only when too late (signature expiration).
1. November 2010: key deletion issue, zone no longer signed, monitoring did not detect it,
2. 12 February 2011: “TYPE65534” bug. Invalid signature on a NSEC3 record. The monitoring was only done on the apex, which was correct. But requests for unsigned sub-domains failed.
3. 13 March 2011: “Missing signature” bug. The SOA record was no longer signed. This time, the monitor detected it (good reason to monitor several types).

Monitoring DNSSEC, not everything is perfect, yet /
1. November 2010: key deletion issue, zone no longer signed, monitoring did not detect it,
1. November 2010: key deletion issue, zone no longer signed, monitoring did not detect it,

2. 12 February 2011: “TYPE65534” bug. Invalid signature on a NSEC3 record. The monitoring was only done on the apex, which was correct. But requests for unsigned sub-domains failed.
1. November 2010: key deletion issue, zone no longer signed, monitoring did not detect it,

2. 12 February 2011: “TYPE65534” bug. Invalid signature on a NSEC3 record. The monitoring was only done on the apex, which was correct. But requests for unsigned sub-domains failed.

3. 13 March 2011: “Missing signature” bug. The SOA record was no longer signed. This time, the monitor detected it (good reason to monitor several types).
The specific case of key rollovers

Taboo
Do we really need to do these complicated rollovers? We break many things to solve a security problem which is quite far away.
The specific case of key rollovers

Taboo
Do we really need to do these complicated rollovers? We break many things to solve a security problem which is quite far away.

Anyway,
Without caching, key rollovers would be very simple. But without caching, would the DNS still work?
Rollovers need to be aware of caching

Period during which the signature could have been in some caches

Time

Signature published

It is safe to remove the key

TTL
Caching is per set, not per record

Time

Keyset published with a new key

Period during which and older keyset could have been in some caches

TTL

It is safe to use the key

Time

Monitoring DNSSEC, not everything is perfect, yet /
Time-aware monitoring

Because of caching, monitoring has to take time into account. The monitor needs a memory, to remember what was done and when.
What do we store

Everything is obtained from authoritative name servers, for freshness.

- Signatures of SOA, NS and DNSKEY (discussion welcome), with their TTL,
- Keys,
- Keysets, with their TTL,
What do we compute

This tool focuses on one thing: timing in key rollovers. Not a substitute for comprehensive monitoring. We check:

1. That every “potentially in caches” signature has a published key,
2. That every published signature has a key which is in the keyset(s) that is(are) in all the caches.

Monitoring DNSSEC, not everything is perfect, yet...
Example of signatures

```
sqlite> SELECT first_seen, last_seen, ttl FROM Signatures
      WHERE type=6 AND name='192.in-addr.arpa.'
          AND key_tag=20918 ORDER BY last_seen DESC;
```

Monitoring DNSSEC, not everything is perfect, yet /
Example of keysets

sqlite> SELECT first_seen, last_seen, ttl, id FROM Keysets
    WHERE name='192.in-addr.arpa.' ORDER BY last_seen DESC;

2011-03-29 09:38:45|2011-03-31 08:30:30|14400|J/dCsFib6kxRer/O/eh1ZbI/Un8=
2011-03-21 21:39:09|2011-03-29 08:38:16|14400|NgM4JKT7QacTgX+ZF7bNo2owK
Example of keys

```
sqlite> SELECT first_seen, last_seen, key_tag FROM Keys
       WHERE name='192.in-addr.arpa.' ORDER BY last_seen DESC;
2011-03-01 15:34:17 | 2011-03-31 08:30:30 | 39318
2011-03-21 21:39:09 | 2011-03-31 08:30:30 | 60494
2011-03-01 15:34:17 | 2011-03-29 08:38:16 | 20918
```

12 Monitoring DNSSEC, not everything is perfect, yet /
The observed domains and the results

- 54 domains monitored, mostly serious domains (TLD, important sub-domains like isoc.org),
- In two months, seven problems detected, including two TLD,
- Six of the problems were a key retired too soon. (Only one was a new key used too early.)
An example: 192.in-addr.arpa

% ./examine-history.py 192.in-addr.arpa
ERROR: signature of zone 192.in-addr.arpa.
    last seen at 2011-03-28 20:17:31 (with a TTL of 86400)
    while the key 20918 was retired at 2011-03-29 09:23:54

The key was withdrawn 11 hours before it was safe to do so.
An example: isoc.org

- Last signature with 41414 done at 21:00
- Key 41414 retired at 10:00
- Period during which the signature could have been in some caches
## All the glitches

<table>
<thead>
<tr>
<th>Zone</th>
<th>Date</th>
<th>Glitch</th>
<th>Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>isoc.org</td>
<td>2011-03-29</td>
<td>retired too early</td>
<td>11h</td>
</tr>
<tr>
<td>192.in-addr.arpa</td>
<td>2011-03-28</td>
<td>retired too early</td>
<td>14h</td>
</tr>
<tr>
<td>my</td>
<td>2011-03-26</td>
<td>retired too early</td>
<td>24h</td>
</tr>
<tr>
<td>bg</td>
<td>2011-03-19</td>
<td>retired too early</td>
<td>72h</td>
</tr>
<tr>
<td>isoc.org</td>
<td>2011-03-01</td>
<td>retired too early</td>
<td>11h</td>
</tr>
<tr>
<td>noaa.gov</td>
<td>2011-02-18</td>
<td>used too early</td>
<td>24h</td>
</tr>
<tr>
<td>noaa.gov</td>
<td>2011-02-18</td>
<td>retired too early</td>
<td>24h</td>
</tr>
</tbody>
</table>
Conclusions

- The tools for key rollovers are not stable yet,
- More monitoring would be a good idea,
- DNSSEC is a sensitive thing: handle with care. Do not put into the hands of children.