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...

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),

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).

Example in .FR

Example in .FR

1. November 2010: key deletion issue, zone no longer signed, monitoring did not detect it,

Example in .FR

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.

Example in .FR

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

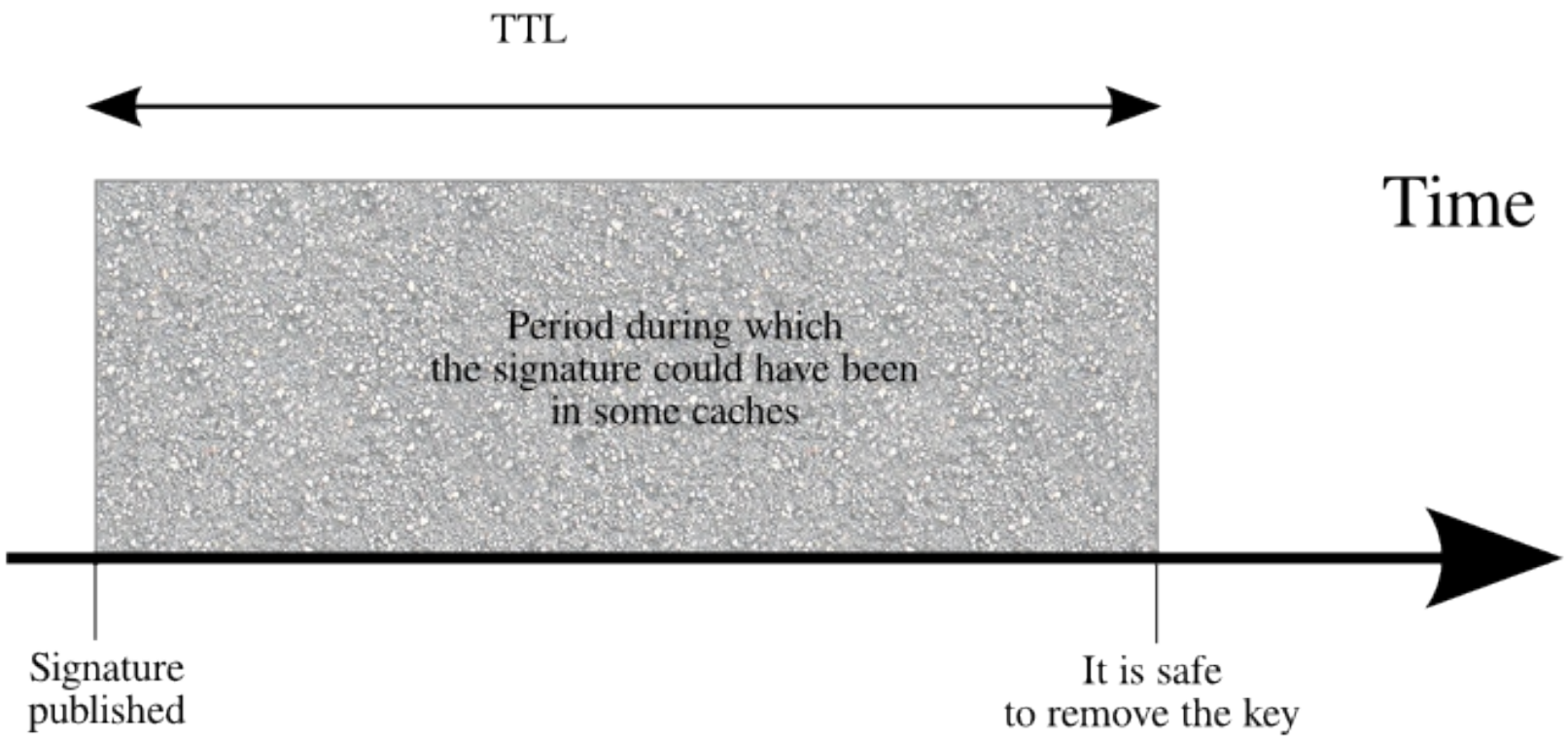
Taboo

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

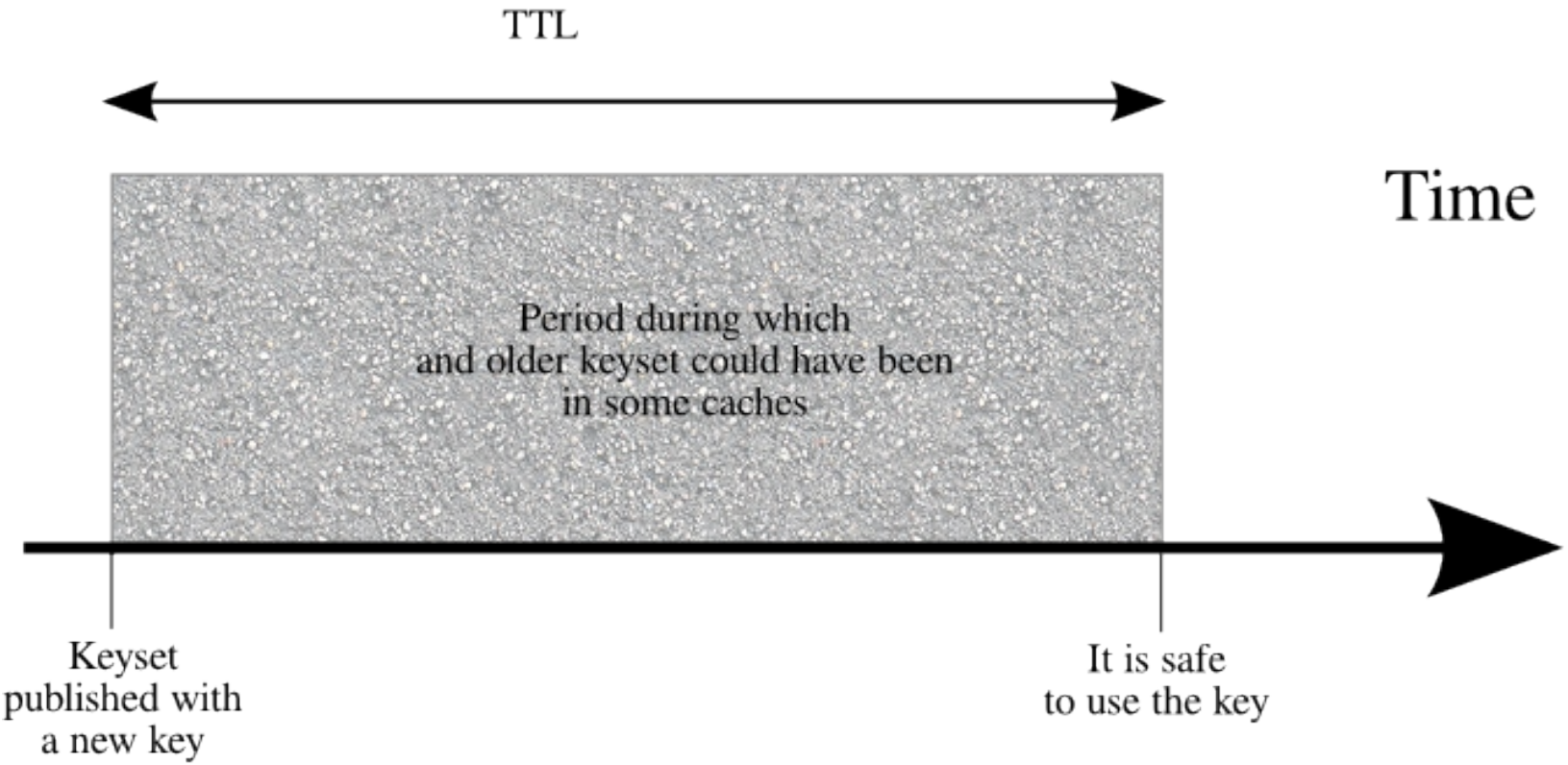
Anyway,

Without caching, key rollovers would be very simple. But without caching, would the DNS still work?

Rollovers need to be aware of caching



Caching is per set, not per record



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 focus 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.

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;
2011-03-28 17:29:30|2011-03-28 20:17:31|86400
2011-03-28 13:22:23|2011-03-28 16:25:05|86400
2011-03-28 09:19:59|2011-03-28 12:28:09|86400
```

Example of keysets

```
sqlite> SELECT first_seen,last_seen,ttl,id FROM Keysets
          WHERE  name='192.in-addr.arpa.' ORDER BY last_seen DES
2011-03-29 09:38:45|2011-03-31 08:30:30|14400|J/dCsFib6kxRer/O/e
2011-03-21 21:39:09|2011-03-29 08:38:16|14400|NgM4JKT7QacTgX+ZF7
```

Example of keys

```
sqlite> SELECT first_seen,last_seen,key_tag FROM Keys
          WHERE  name='192.in-addr.arpa.' ORDER BY last_seen DES
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
```

The observed domains and the results

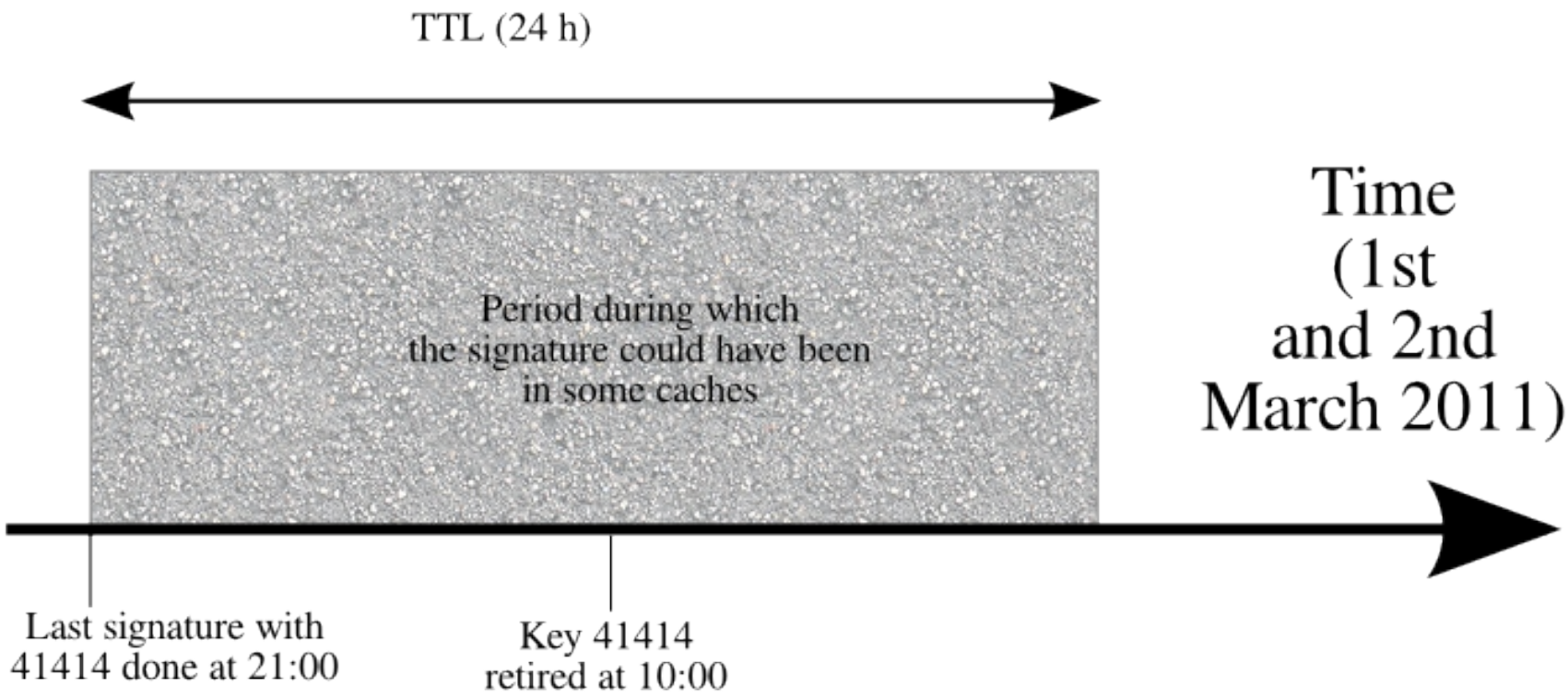
- 54 domains monitored, mostly serious domains (TLD, important sub-domains like `isoc.org`),
- In two months, seven problems detected, including two TLD,
- Six of the problems were a key retired too soon. (Only one was a new key used too early.)

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 exampe: isoc.org



All the glitches

Zone	Date	Glitch	Windo
isoc.org	2011-03-29	retired too early	11h
192.in-addr.arpa	2011-03-28	retired too early	14h
my	2011-03-26	retired too early	24h
bg	2011-03-19	retired too early	72h
isoc.org	2011-03-01	retired too early	11h
noaa.gov	2011-02-18	used too early	24h
noaa.gov	2011-02-18	retired too early	24h

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.