DNSSEC Signing of .NET and .COM

Duane Wessels

2011-02-01

.NET

.NET: DUNZ

- “Deliberately Unvalidatable NET Zone”
- .NET zone signed
  - ZSK 1024-bit RSASHA256
  - KSK 2048-bit RSASHA256
  - NSEC3 optout
- KSK “blinded” before publication
- Incrementally rolled out, one site at a time
  - Oct 29 – Nov 9, 2010

.NET: Accepting DS records

- Registry system was upgraded to accept DS records (for .NET only) from registrars well in advance
- First DS records in the .NET zone appear Dec 3, 2010.

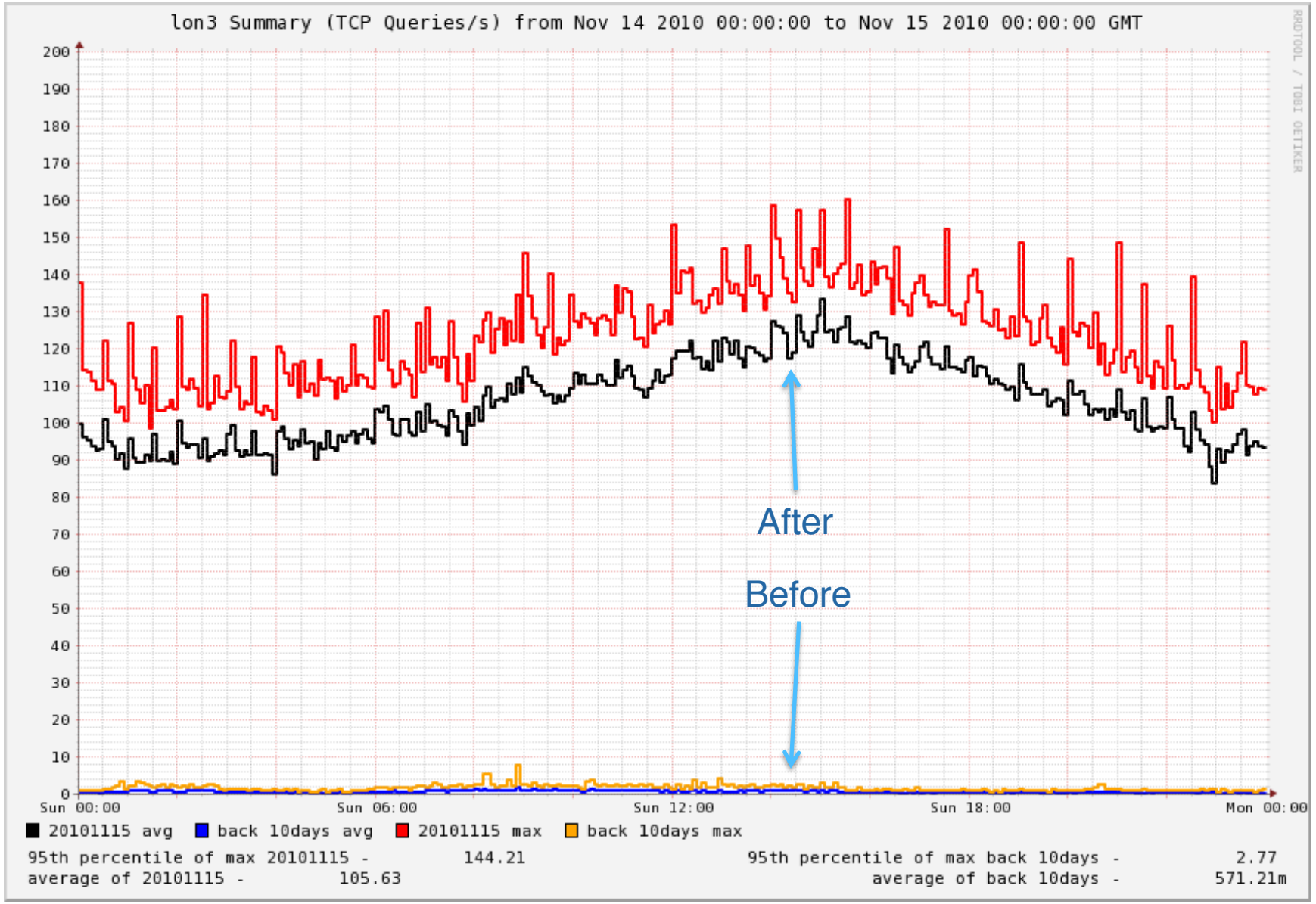
.NET: Unblinding

- KSK no longer blinded
- Incremental rollout completed by Dec 7, 2010
- Then, wait 2 days for old, blinded keys to expire from caches
- note: DNSKEY TTL = 1day

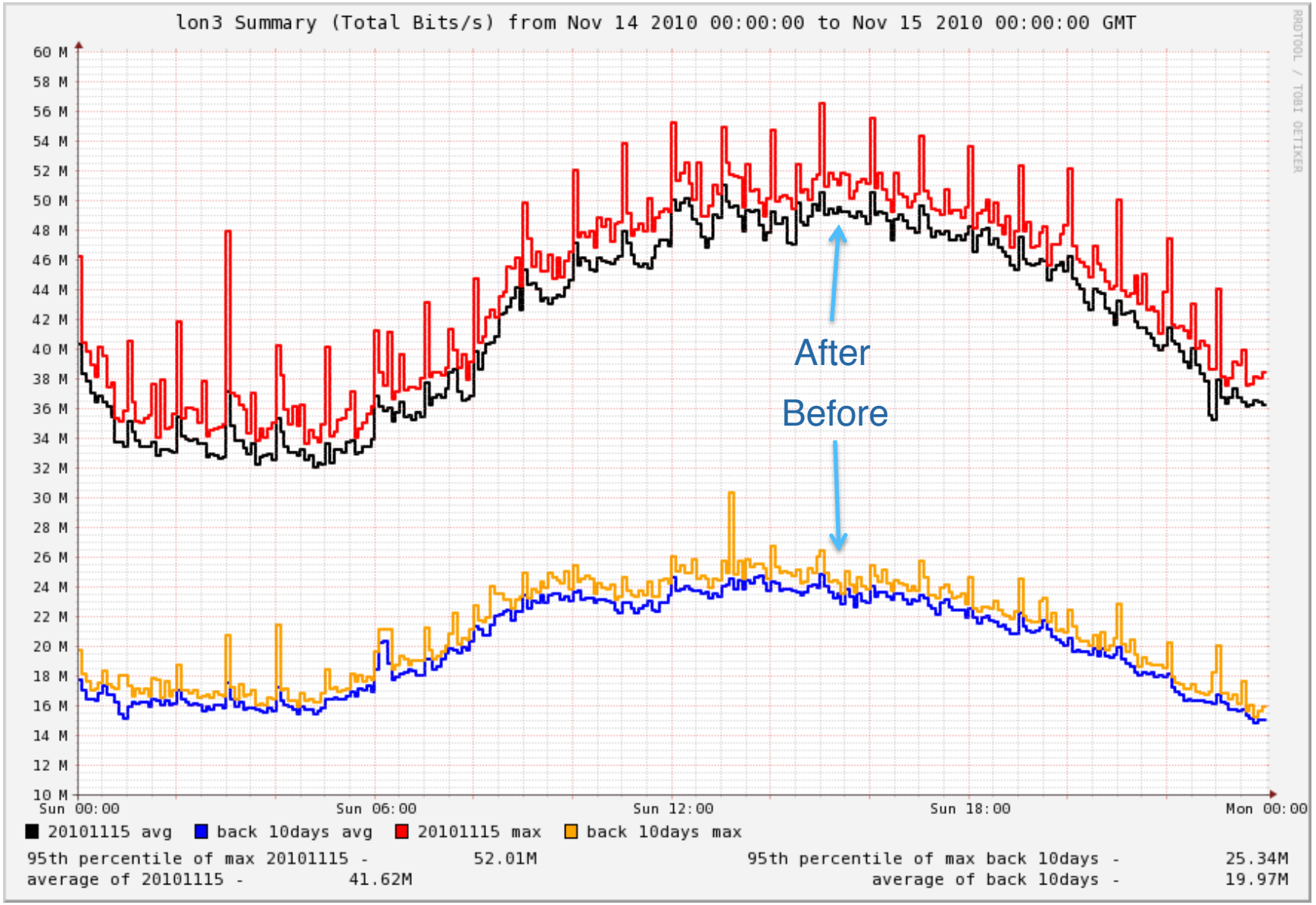
.NET: Root Zone Updated

- .NET DS record submitted through normal IANA process
- Appears in Root zone on December 9, 2010

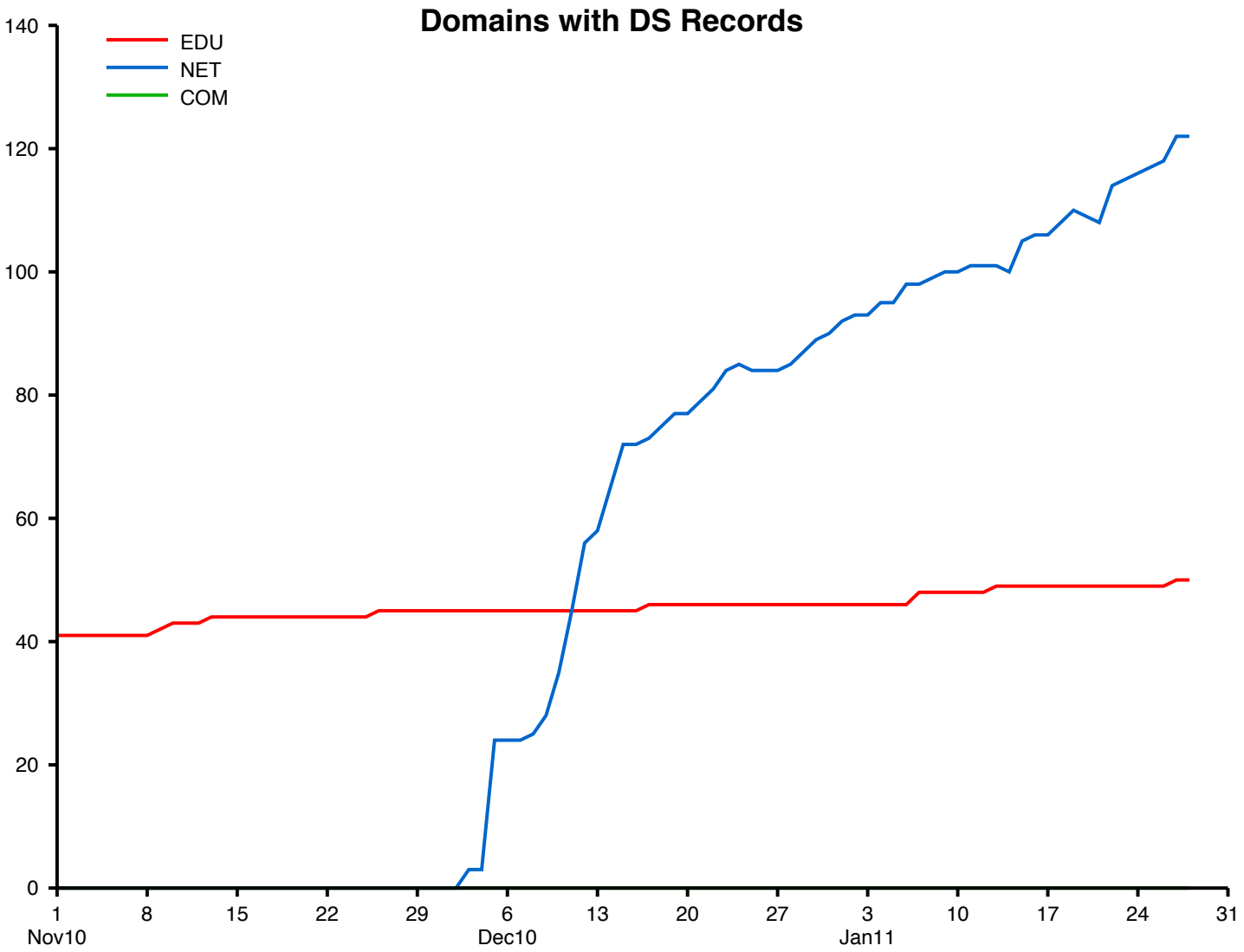
.NET: TCP Increase



.NET: Bandwidth Increase



.NET: DNSSEC Uptake

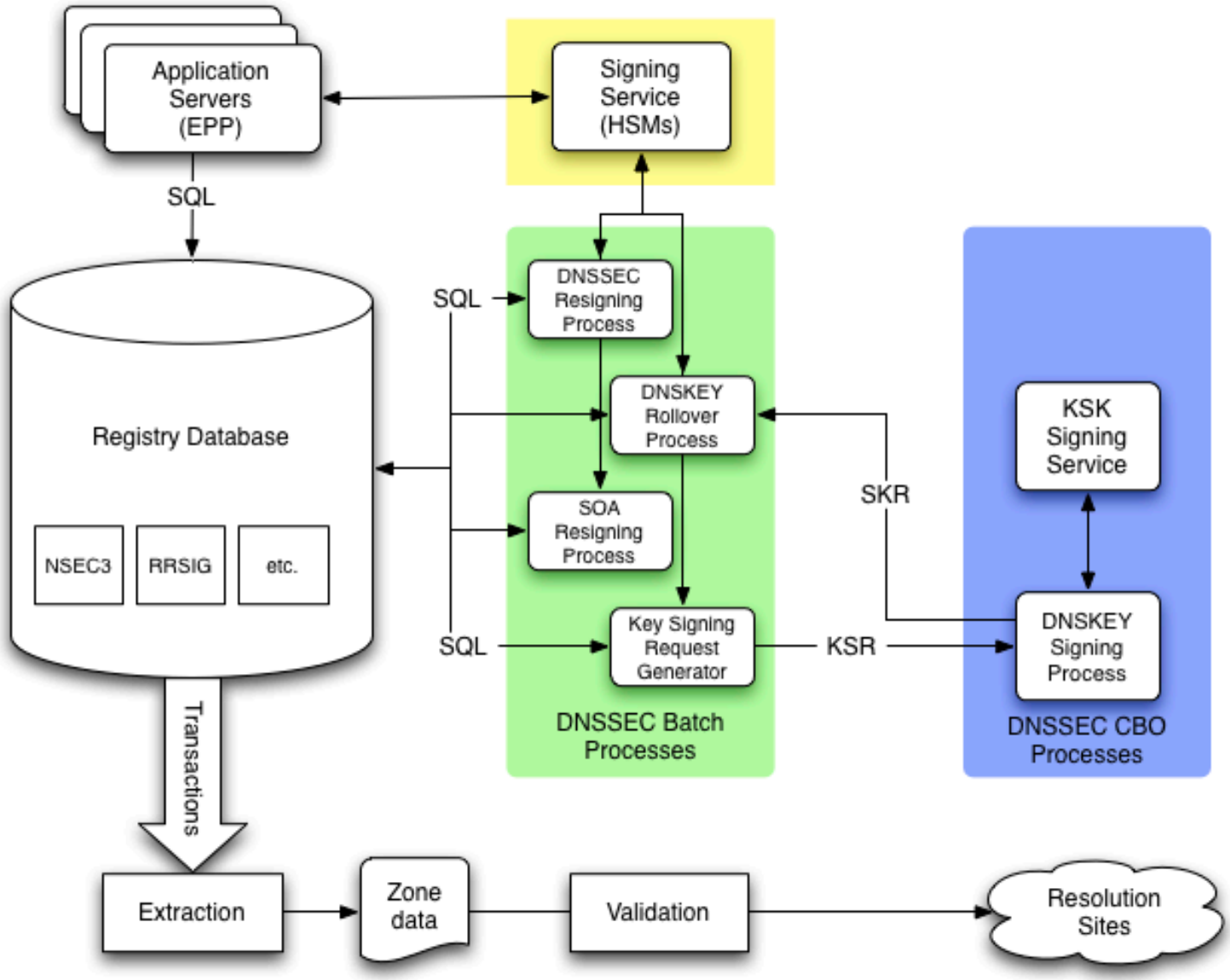


.COM

.COM: Parameters

- Same as .NET
- 2048-bit RSASHA256 KSK
  - Lifetime measured in years
  - No fixed rollover schedule
  - Not planning to use RFC5011
- 1024-bit RSASHA256 ZSK
  - Rolled every 3 months
- NSEC3 optout
- RRSIGs have 7-day validity

.COM: Provisioning Architecture



.COM: Schedule

Milestone	Date
Registry System Accepting DS	2011-02-26
Deliberately Unvalidatable Zone	2011-02-28
.COM Zone Unblinded	2011-03-28
.COM DS record published	2011-03-31

New DS may lead to SERVFAILs in some BIND versions

Problem Report

- A BIND user reported SERVFAILs for all .NET names
- Happened a few hours after .NET's DS record was published
- Looks like this in syslog:

```
2010-12-09 13:45:58 EST error (no valid RRSIG) resolving 'att.net/DS/IN': 192.41.162.30#53
2010-12-09 13:45:58 EST error (no valid RRSIG) resolving 'comcast.net/DS/IN': 192.5.6.30#53
2010-12-09 13:45:58 EST error (no valid RRSIG) resolving 'demon.net/DS/IN': 192.5.6.30#53
2010-12-09 13:45:58 EST error (no valid RRSIG) resolving 'netzero.net/DS/IN': 192.35.51.30#53
2010-12-09 13:45:58 EST error (no valid RRSIG) resolving 'verizon.net/DS/IN': 192.5.6.30#53
2010-12-09 13:45:58 EST error (no valid RRSIG) resolving 'charter.net/DS/IN': 192.12.94.30#53
```

- Solved by restarting named process

Second Guessing

- Didn’t we wait long enough after unblinding the zone?
- Some site still serving unvalidatable KSK?
- Root server propagation delay?
- Wrong key somehow in user’s cache?
- Bug in BIND?

Reproduce the problem

- BIND 9.7.0-P2 resolver
- Use real TTLs, divided by 1440
- Repeat phases of signing .NET
- Log responses to *unsigned.net* and *signed.net* queries during experiment

Bug Reproduced

```
net zone signed; keys blinded

1296243954 unsigned.net NOERROR  AD=0  127.0.0.1 30
1296243954 signed.net   NOERROR  AD=0  127.0.0.1 30
1296243969 unsigned.net NOERROR  AD=0  127.0.0.1 15
1296243969 signed.net   NOERROR  AD=0  127.0.0.1 15
1296243984 unsigned.net NOERROR  AD=0  127.0.0.1 60
1296243984 signed.net   NOERROR  AD=0  127.0.0.1 60
1296243999 unsigned.net NOERROR  AD=0  127.0.0.1 45
1296243999 signed.net   NOERROR  AD=0  127.0.0.1 45

net zone keys unblinded

1296244014 unsigned.net NOERROR  AD=0  127.0.0.1 30
1296244014 signed.net   NOERROR  AD=0  127.0.0.1 30
1296244029 unsigned.net NOERROR  AD=0  127.0.0.1 15
1296244029 signed.net   NOERROR  AD=0  127.0.0.1 15
1296244044 unsigned.net NOERROR  AD=0  127.0.0.1 60
1296244044 signed.net   NOERROR  AD=0  127.0.0.1 60
1296244059 unsigned.net NOERROR  AD=0  127.0.0.1 45
1296244059 signed.net   NOERROR  AD=0  127.0.0.1 45
1296244074 unsigned.net NOERROR  AD=0  127.0.0.1 30
1296244074 signed.net   NOERROR  AD=0  127.0.0.1 30
1296244089 unsigned.net NOERROR  AD=0  127.0.0.1 15
1296244089 signed.net   NOERROR  AD=0  127.0.0.1 15
1296244104 unsigned.net NOERROR  AD=0  127.0.0.1 60
1296244105 signed.net   NOERROR  AD=0  127.0.0.1 60
1296244120 unsigned.net NOERROR  AD=0  127.0.0.1 44
1296244120 signed.net   NOERROR  AD=0  127.0.0.1 45
```

Bug Reproduced

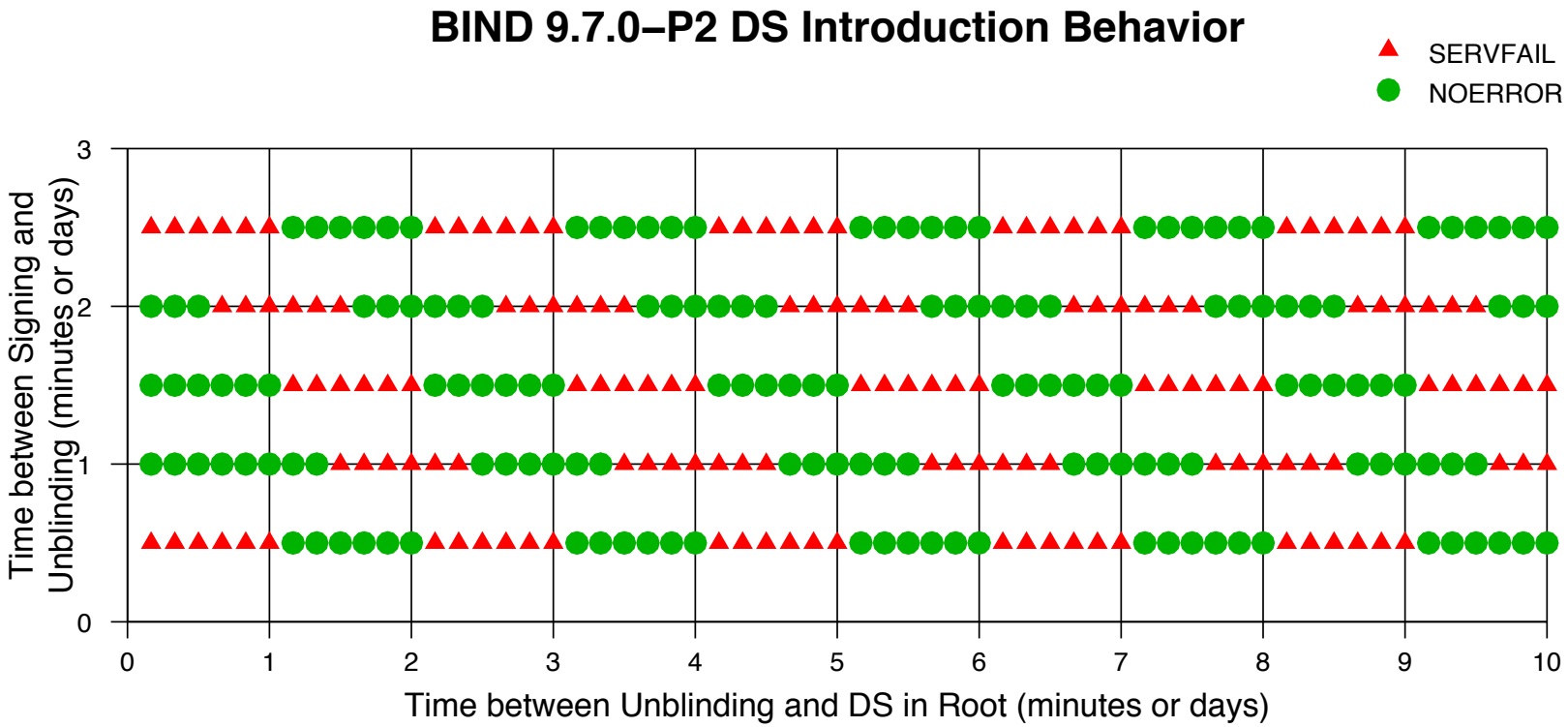
net DS published in root zone

```
1296244135 unsigned.net NOERROR  AD=0  127.0.0.1 29
1296244135 signed.net   NOERROR  AD=0  127.0.0.1 30
1296244150 unsigned.net NOERROR  AD=0  127.0.0.1 14
1296244150 signed.net   NOERROR  AD=0  127.0.0.1 15
1296244166 unsigned.net SERVFAIL AD=0
1296244166 signed.net   NOERROR  AD=0  127.0.0.1 60
1296244181 unsigned.net SERVFAIL AD=0
1296244181 signed.net   NOERROR  AD=0  127.0.0.1 45
1296244196 unsigned.net SERVFAIL AD=0
1296244196 signed.net   NOERROR  AD=0  127.0.0.1 30
1296244211 unsigned.net SERVFAIL AD=0
1296244211 signed.net   NOERROR  AD=0  127.0.0.1 15
1296244226 unsigned.net SERVFAIL AD=0
1296244226 signed.net   NOERROR  AD=1  127.0.0.1 60
1296244241 unsigned.net SERVFAIL AD=0
1296244241 signed.net   NOERROR  AD=1  127.0.0.1 45
1296244256 unsigned.net SERVFAIL AD=0
1296244256 signed.net   NOERROR  AD=1  127.0.0.1 30
1296244271 unsigned.net SERVFAIL AD=0
1296244271 signed.net   NOERROR  AD=1  127.0.0.1 15
```

(note signed domains resolve just fine, unsigned domains get SERVFAIL)

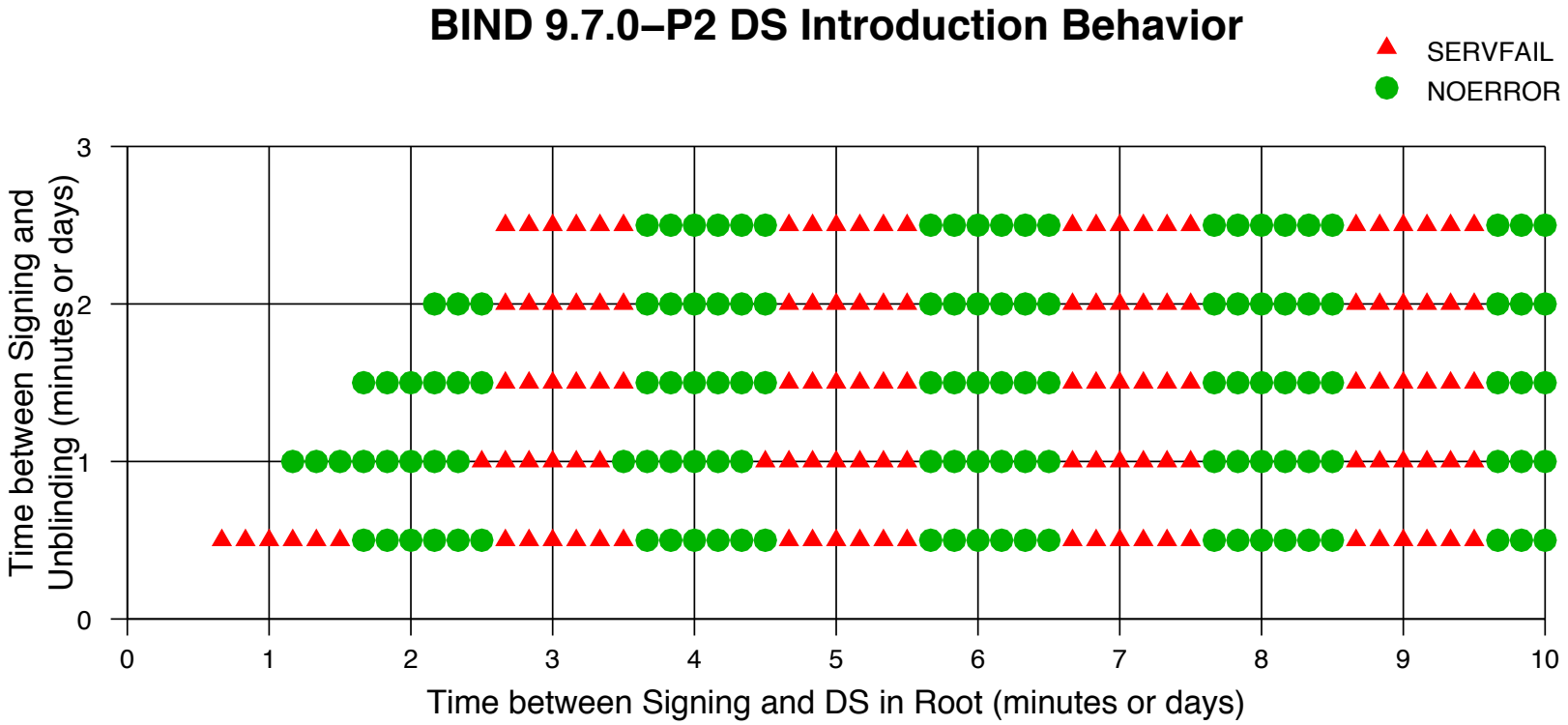
Bug isn't always triggered

- If the timing is just right, you won't see the bug
- Not avoided by waiting longer to unblind

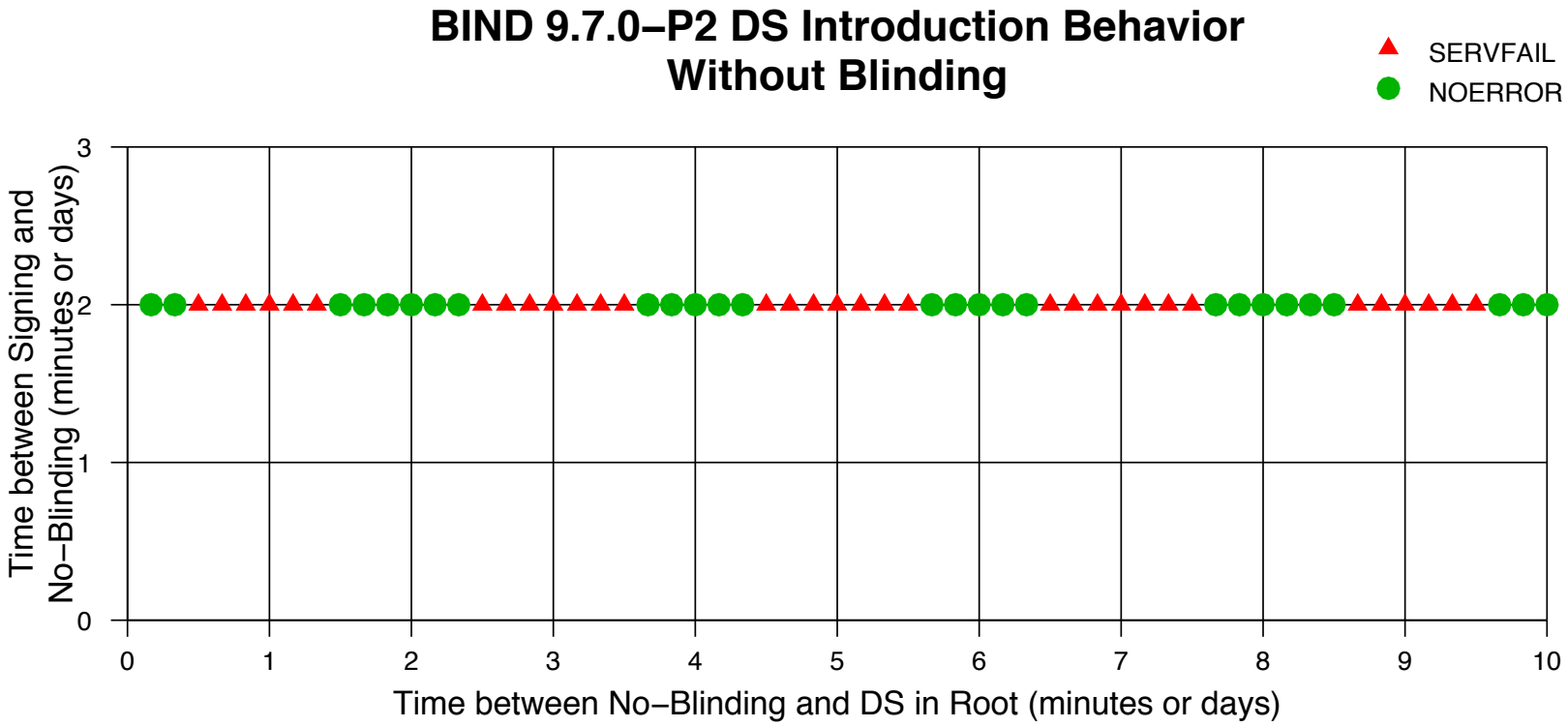


Timing

- Same data as previous, with rows shifted over
- Depends (only) on time between signing and DS in root



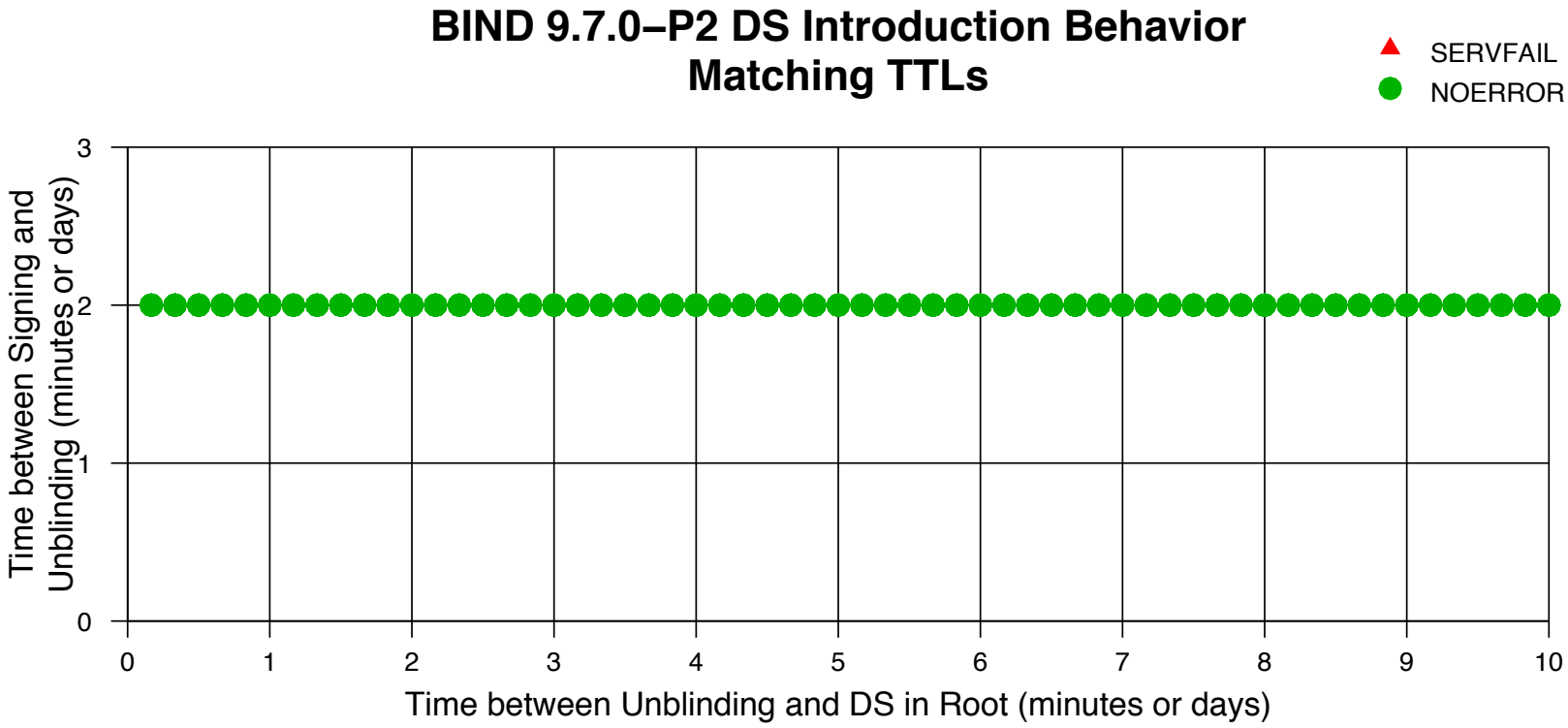
Caused by Key Blinding Process?



Periodicity

- Pattern has a period of 2 days
- With “good region” of 1 day and “bad region” of 1 day
- .NET NS TTL = 2 days
- .NET DNSKEY TTL = 1 day
- Hmm….

What if NS and DNSKEY TTLs match?



Known Bug?

- From BIND's CHANGES file:

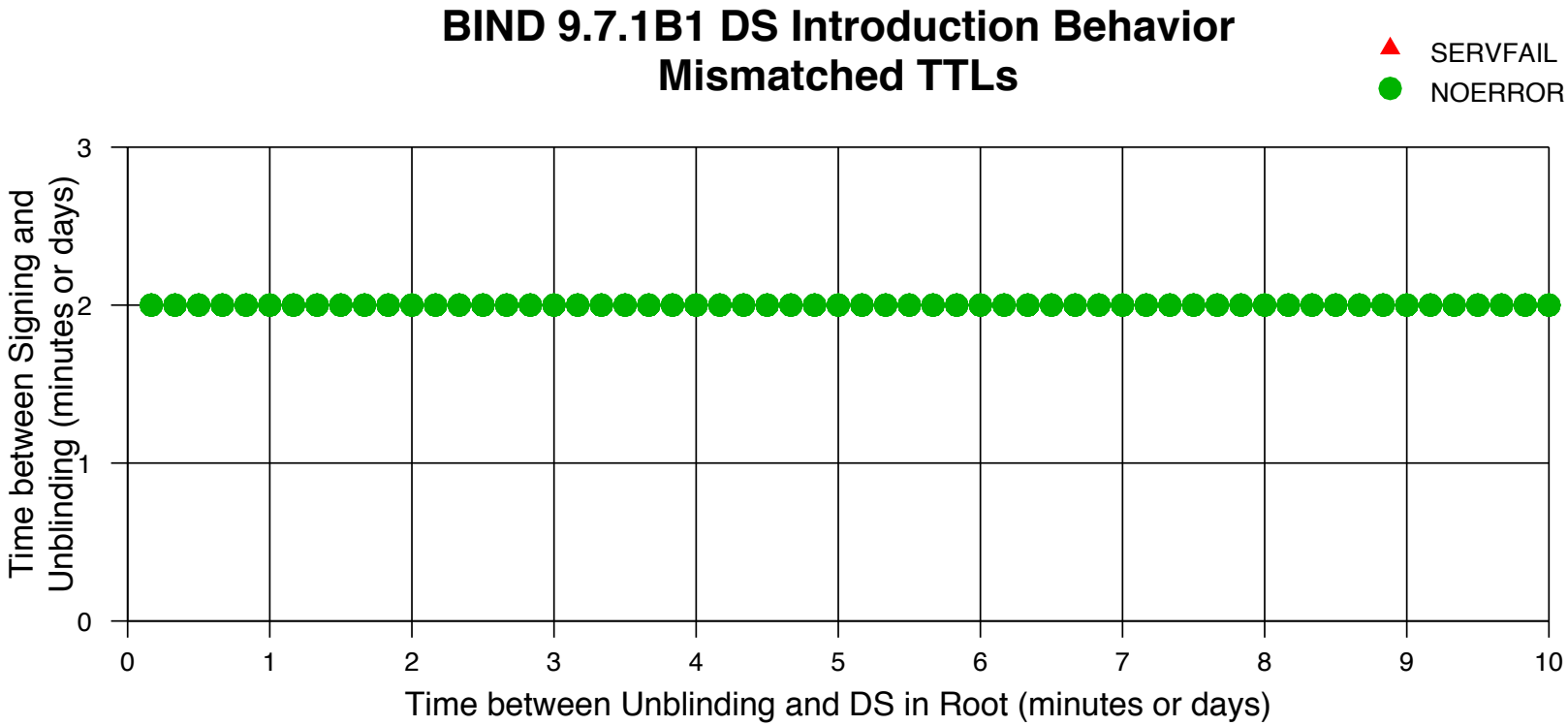
```
 --- 9.7.1b1 released ---

...

2890.   [bug]           Handle the introduction of new trusted-keys and
                        DS, DLV RRsets better. [RT #21097]
```

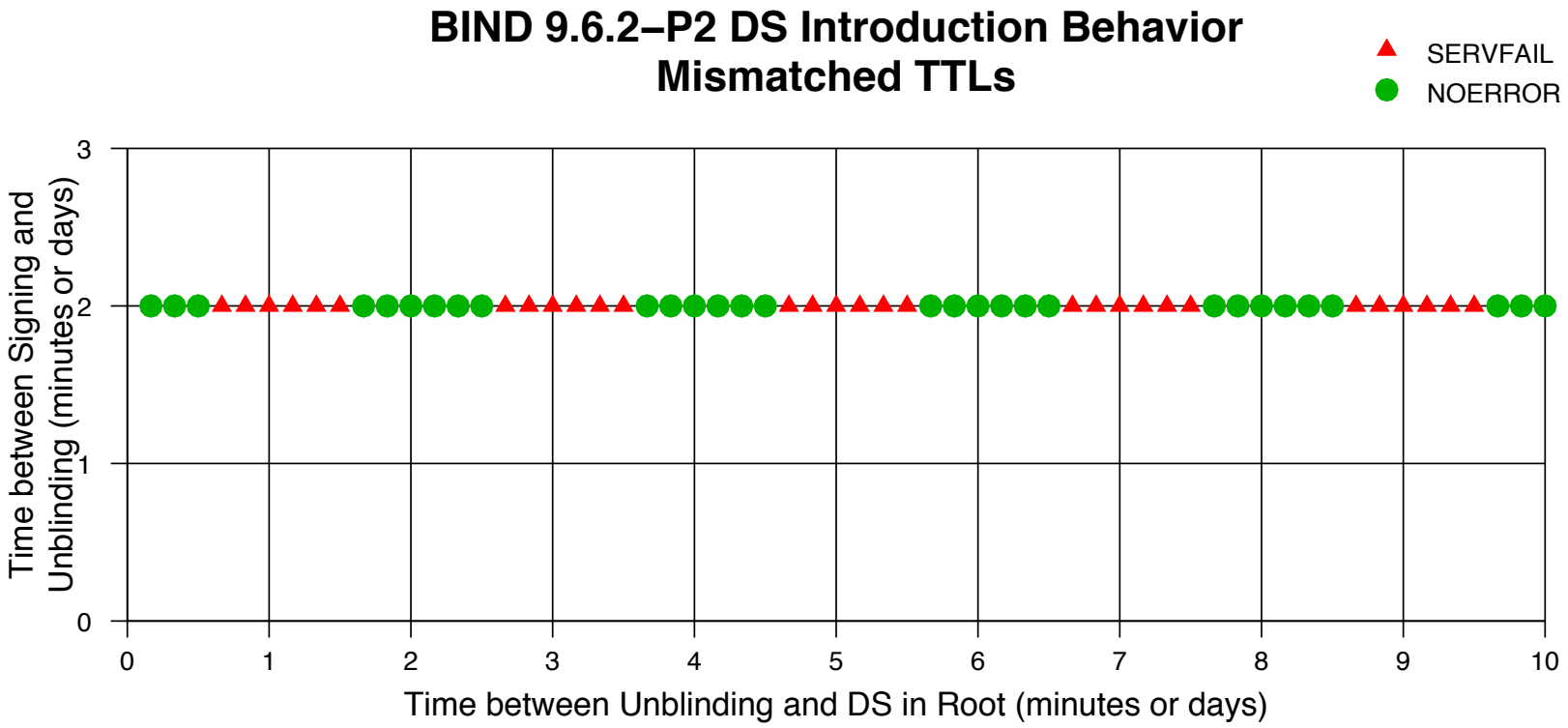
- Awaiting confirmation from ISC

Test BIND 9.7.1b1



Earlier Versions?

- 9.6.2-P2 is the earliest version with SHA-256 support



Upshot

- If you're running BIND 9.6.2 – 9.7.0 …
- With a Root Zone trust anchor …
- There is a 50% chance you'll experience SERVFAILs for all .COM queries on March 31, 2011

Workarounds

- Change .COM's DNSKEY TTLs to 2 days
  - We considered this but decided against it
- Upgrade to BIND 9.7.1 or later
- Restart your nameserver after .COM's DS record is published in the root zone
  - Hopefully before the SERVFAILs hit

Thank You