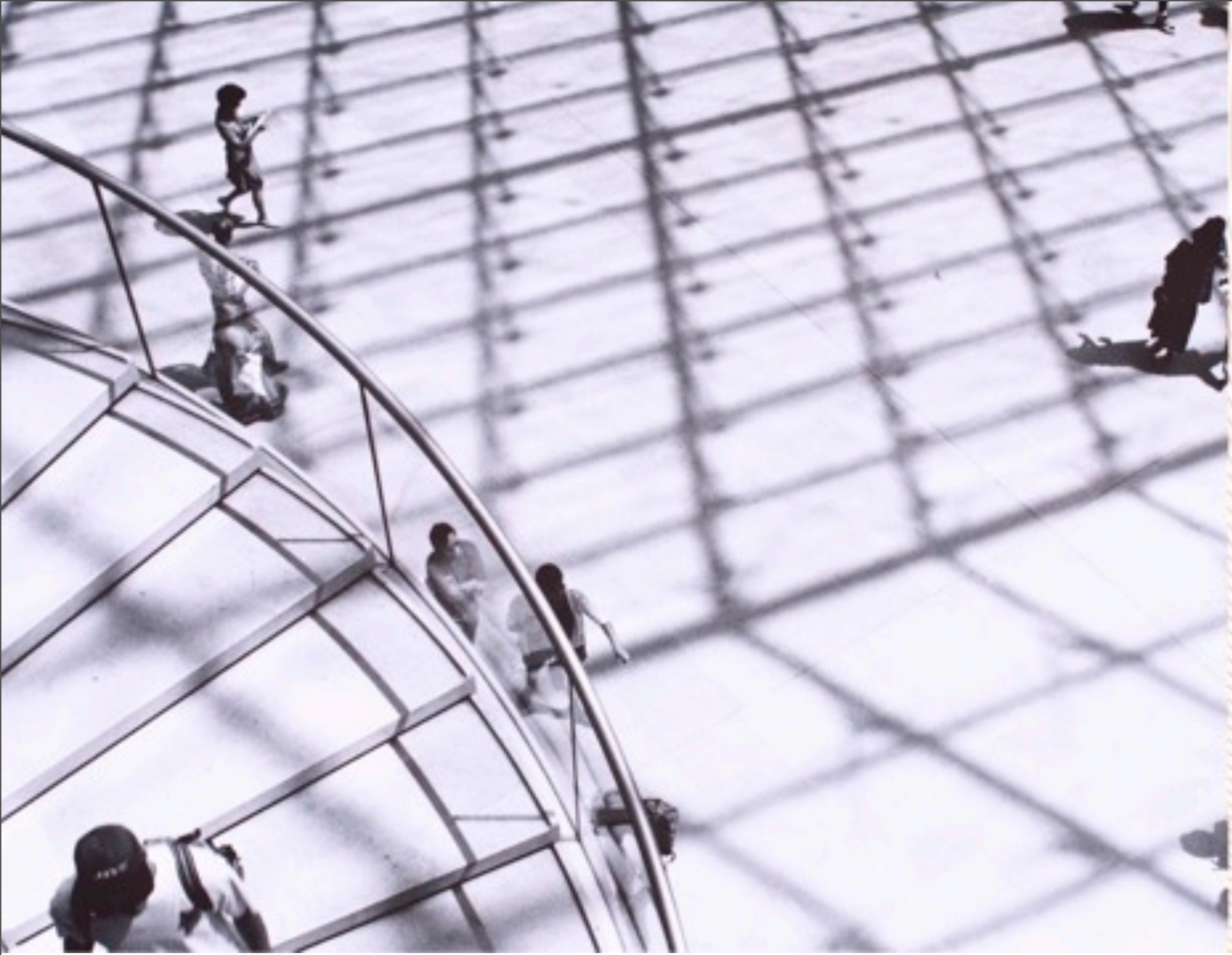


DNSSEC resolving at SURFnet

ICANN38, DNSSEC panel discussion, Brussels

Roland van Rijswijk
roland.vanrijswijk [at] surfnet.nl

June 23rd 2010

About SURFnet

National Research and Educational Network in The Netherlands

High-bandwith fiber-optic network for higher education and research

Shared ICT innovation centre

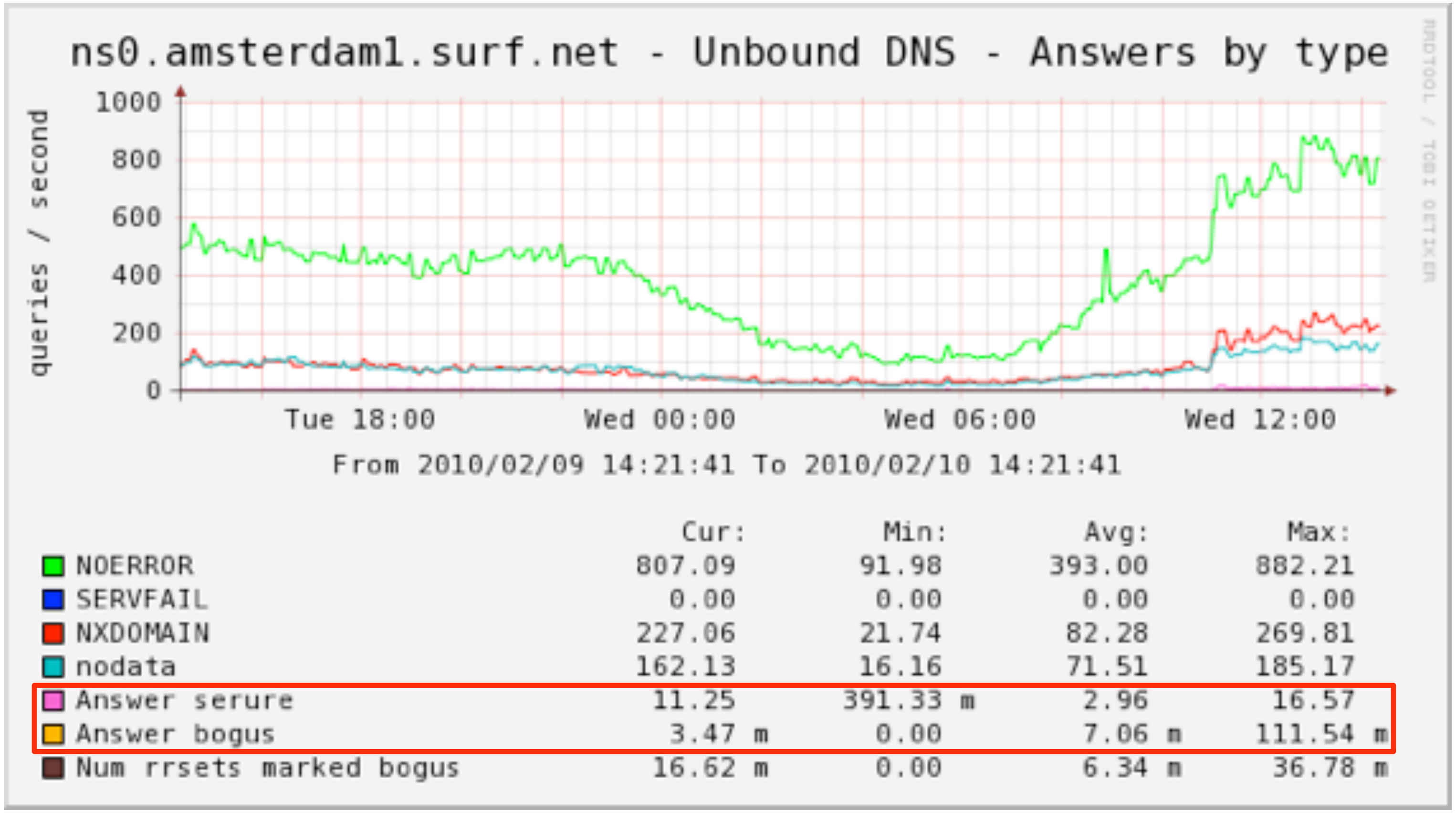
≥ 160 connected institutions and ±1 million end users

Validating resolvers

- SURFnet has DNSSEC validation enabled on all its resolvers since last year
- About 99% of validatable queries are succesful
- We use Unbound from NLnet Labs **http://www.unbound.net**

Current validation rates

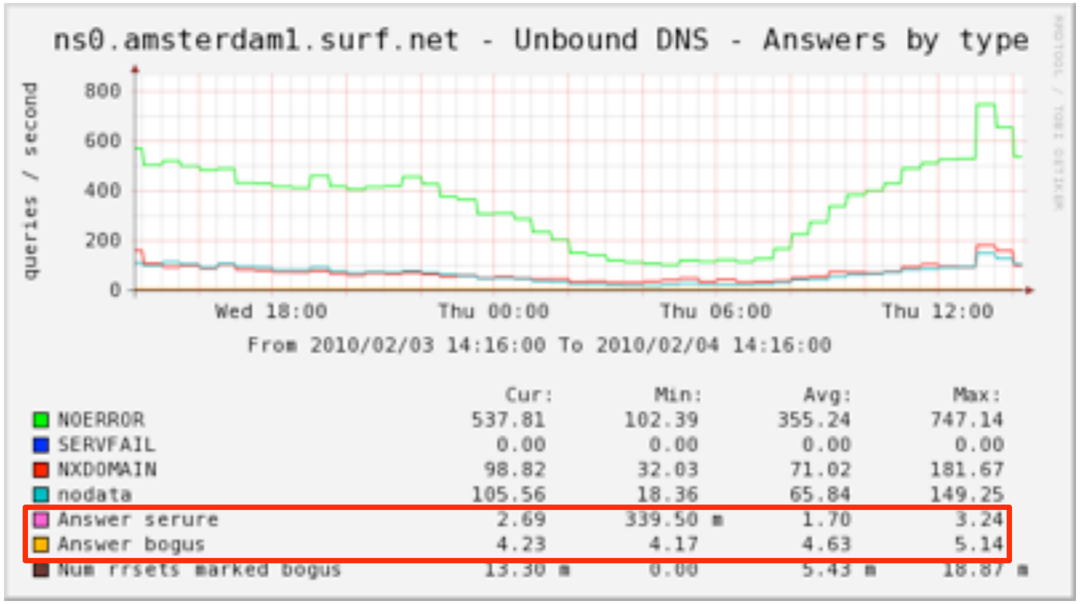
- Validation rates are around 1-2%:



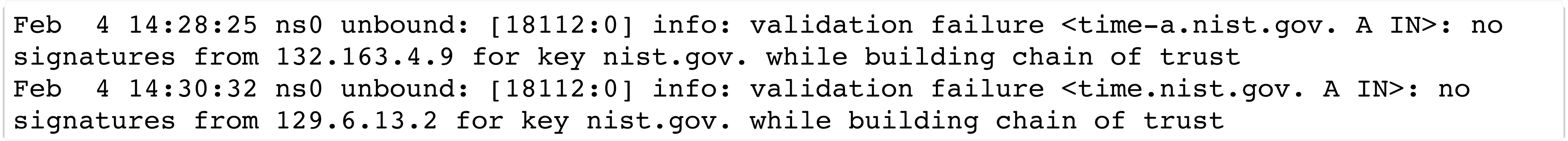
	Cur:	Min:	Avg:	Max:
🟩 NOERROR	807.09	91.98	393.00	882.21
🟦 SERVFAIL	0.00	0.00	0.00	0.00
🟥 NXDOMAIN	227.06	21.74	82.28	269.81
🟦 nodata	162.13	16.16	71.51	185.17
🟪 Answer serure	11.25	391.33 m	2.96	16.57
🟧 Answer bogus	3.47 m	0.00	7.06 m	111.54 m
🟫 Num rrsets marked bogus	16.62 m	0.00	6.34 m	36.78 m

Validation running amok

- Strange validation failures:



	Cur:	Min:	Avg:	Max:
🟩 NOERROR	537.81	102.39	355.24	747.14
🟦 SERVFAIL	0.00	0.00	0.00	0.00
🟥 NXDOMAIN	98.82	32.03	71.02	181.67
🟦 nodata	105.56	18.36	65.84	149.25
🟪 Answer serure	2.69	339.50 m	1.70	3.24
🟧 Answer bogus	4.23	4.17	4.63	5.14
🟫 Num rrsets marked bogus	13.30 m	0.00	5.43 m	18.87 m



```
Feb  4 14:28:25 ns0 unbound: [18112:0] info: validation failure <time-a.nist.gov. A IN>: no
signatures from 132.163.4.9 for key nist.gov. while building chain of trust
Feb  4 14:30:32 ns0 unbound: [18112:0] info: validation failure <time.nist.gov. A IN>: no
signatures from 129.6.13.2 for key nist.gov. while building chain of trust
```

- We’re in constant contact with NLnetLabs to solve these issues

The ARIN incident

- Around September 4th ’09 we noticed that lot’s of reverse lookups (PTR) suddenly failed to validate
- At first we thought it was an Unbound issue
- We worked with the guys from NLnetLabs for 5 days in a row
- We analysed over 500MB of DNS queries (packets are usually just 512 bytes!)
- It was not a bug in Unbound...

The ARIN incident

- **chia.arin.net** was the culprit
  - It has both an IPv4 as well as an IPv6 address
  - IPv4 (A) could be queried for
  - IPv6 (AAAA) could not be queried for
  - But the glue for arin.net contained an AAAA record
  - Once that AAAA record was cached, IPv6 is also used to access this server
  - The server gave DNSSEC answers on IPv4 but **not** on IPv6
- Made about 1 in 12 reverse validations **fail**
- At first, ARIN’s hostmaster ignored our message... but pulling some strings helped
- Issue was quietly solved on Sep. 15th ’09

Common validation failures

- Some US government agencies seem unable to get DNSSEC right:

```
Feb 10 04:16:43 ns0 unbound: [5973:1] info: validation failure <USPTO.GOV. MX IN>: no
signatures from 151.207.246.51 for key USPTO.GOV. while building chain of trust
Feb 10 04:53:00 ns0 unbound: [5973:0] info: validation failure <gk-w-mail.srvs.usps.gov. A
IN>: no signatures over NSEC3s from 56.0.141.25 for DS gk-w-mail.srvs.usps.gov. while...
Feb 10 14:21:48 ns0 unbound: [5973:1] info: validation failure <www.hud.gov. A IN>: no DS...
```

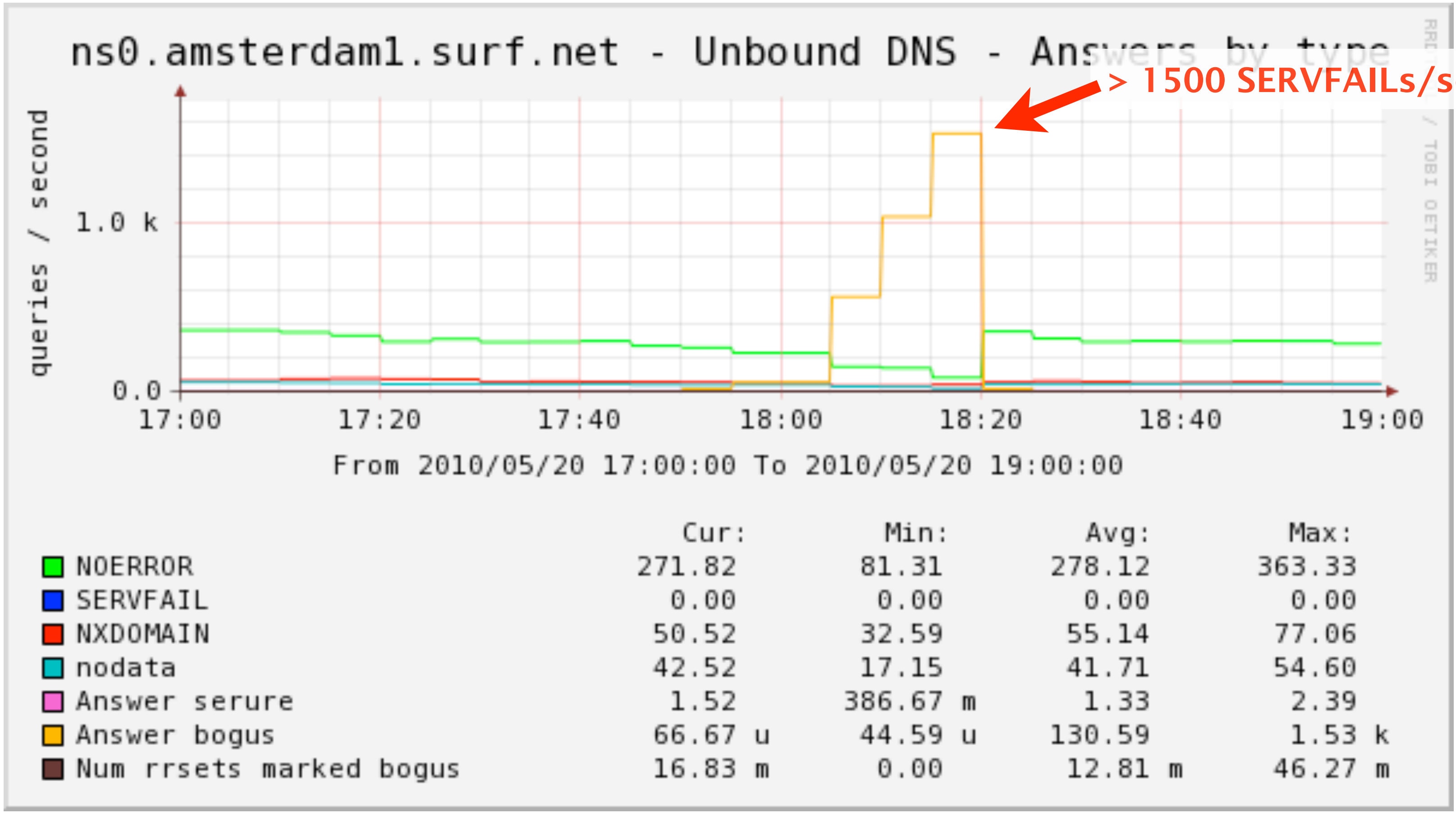
- Others include .cz and .bg domains:

```
Feb 10 13:47:35 ns0 unbound: [5973:0] info: validation failure <www.atol.bg. A IN>: No DNSK...
Feb 10 13:37:17 ns0 unbound: [5973:0] info: validation failure <ns.unicycle.cz. A IN>: no k...
```

- There were some problems in Portugal

```
Feb 15 19:10:25 ns0 unbound: [5973:1] info: validation failure <FM.UL.PT. MX IN>: [illegible] NSEC3
records from 2001:690:21c0:b::150 for DS FM.UL.PT. while building chain of trust
```

DLV is dangerous in production



> 1500 SERVFAILs/second!

	Cur:	Min:	Avg:	Max:
🟩 NOERROR	271.82	81.31	278.12	363.33
🟦 SERVFAIL	0.00	0.00	0.00	0.00
🟥 NXDOMAIN	50.52	32.59	55.14	77.06
🟦 nodata	42.52	17.15	41.71	54.60
🟪 Answer serure	1.52	386.67 m	1.33	2.39
🟧 Answer bogus	66.67 u	44.59 u	130.59	1.53 k
🟫 Num rrsets marked bogus	16.83 m	0.00	12.81 m	46.27 m

- If DLV is untrusted, all uncached queries **fail!**

International co-operation

That’s all folks... Questions?

Thank you for your attention!

?

Roland van Rijswijk

roland.vanrijswijk [at] surfnet.nl