Measuring DNSSEC validation deployment with RIPE ATLAS

Willem Toorop (presenting)
Willem@NLnetLabs.nl
Nicolas Canceill
nicolas.canceill@os3.nl

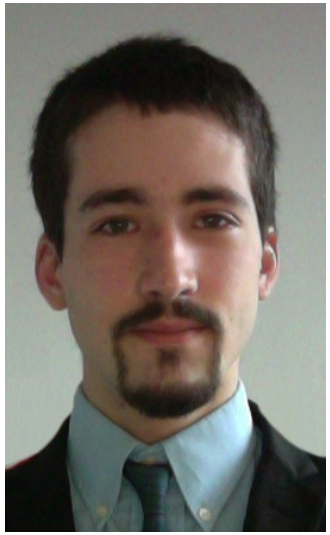
25 Jun 2014

Research scope

Research question

What is the status of DNSSEC deployment over the Internet and how does it impact Internet users?

- Which DNS resolvers can be queried from clients?
- What methods can properly assess DNSSEC support?
- How does DNSSEC support influence user experience?



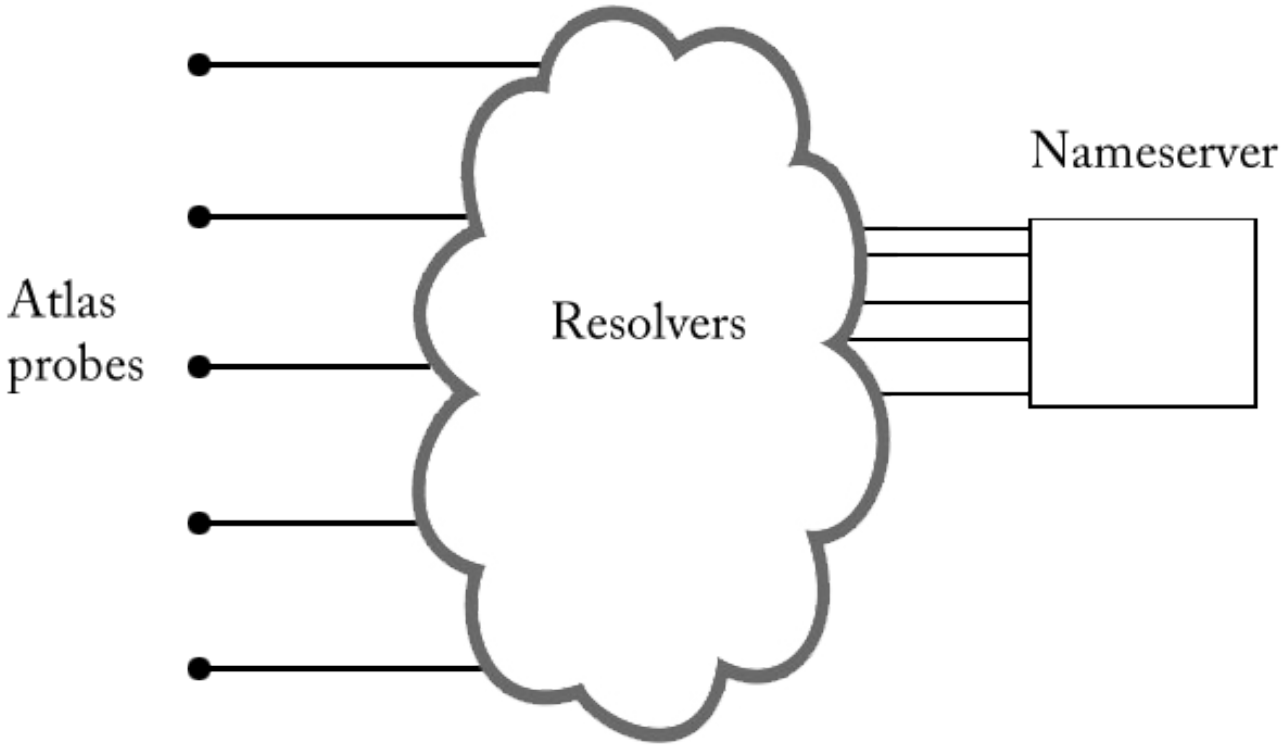
- One month master student project
- System & Network Engineering master

  University of Amsterdam
- Executed by Nicolas Canceill at NLnet Labs
- Report almost finished
  (pending corrections in methods and results)

The Atlas network

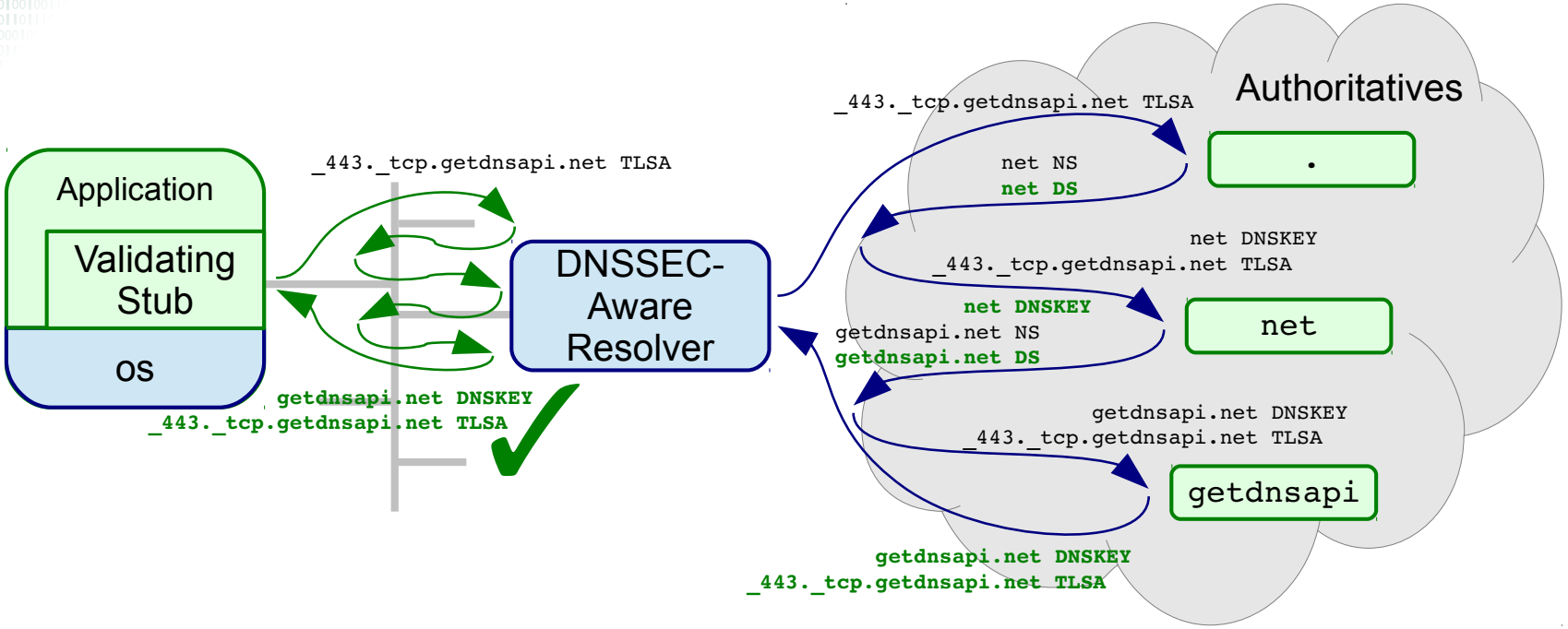
- 6,250 active probes
- Worldwide — mostly Europe

Setup



- Atlas probes: presence in client network
- Controlled nameserver with packet capture

Setup



- Atlas probes: presence in client network
- Is the nameserver DNSSEC-aware?
- Controlled nameserver with packet capture

Challenges

Probes-resolvers

- IP address seen by the probe: `8.8.8.8`
- IP address seen by the nameserver: `74.125.18.209`

Solution: pre-pend probe ID and use wildcards
Probe `1234` requests `1234.example.com`

Resolving setup

- Probes with multiple resolvers
- Probes using forwarders
- Misconfigured resolvers

Limitations

Atlas $\neq$ Internet

Atlas Top10

Country	Probes
United States	853
Germany	819
Russia	724
United Kingdom	605
Netherlands	457
France	397
Ukraine	364
Belgium	184
Italy	166
Czech Republic	161

Internet Top10

Country	Internet users (in 2012)
China	568,192,066
United States	254,295,536
India	151,598,994
Japan	100,684,474
Brazil	99,357,737
Russia	75,926,004
Germany	68,296,919
Nigeria	55,930,391
United Kingdom	54,861,245
France	54,473,474

Process

Steps

1. List all active probes
2. Start packet capture at the nameserver
3. Launch measurement on Atlas probes
4. Wait for measurement results
5. Stop packet capture
6. Repeat steps 2-5 until all active probes have been used

Zones

`secure` `insecure` `badlabel`, `badrrsigs`, `norrsigs`

Software

Python, `atlas`, `dpkt` `nsd`, `ldns` Wireshark

Resolvers

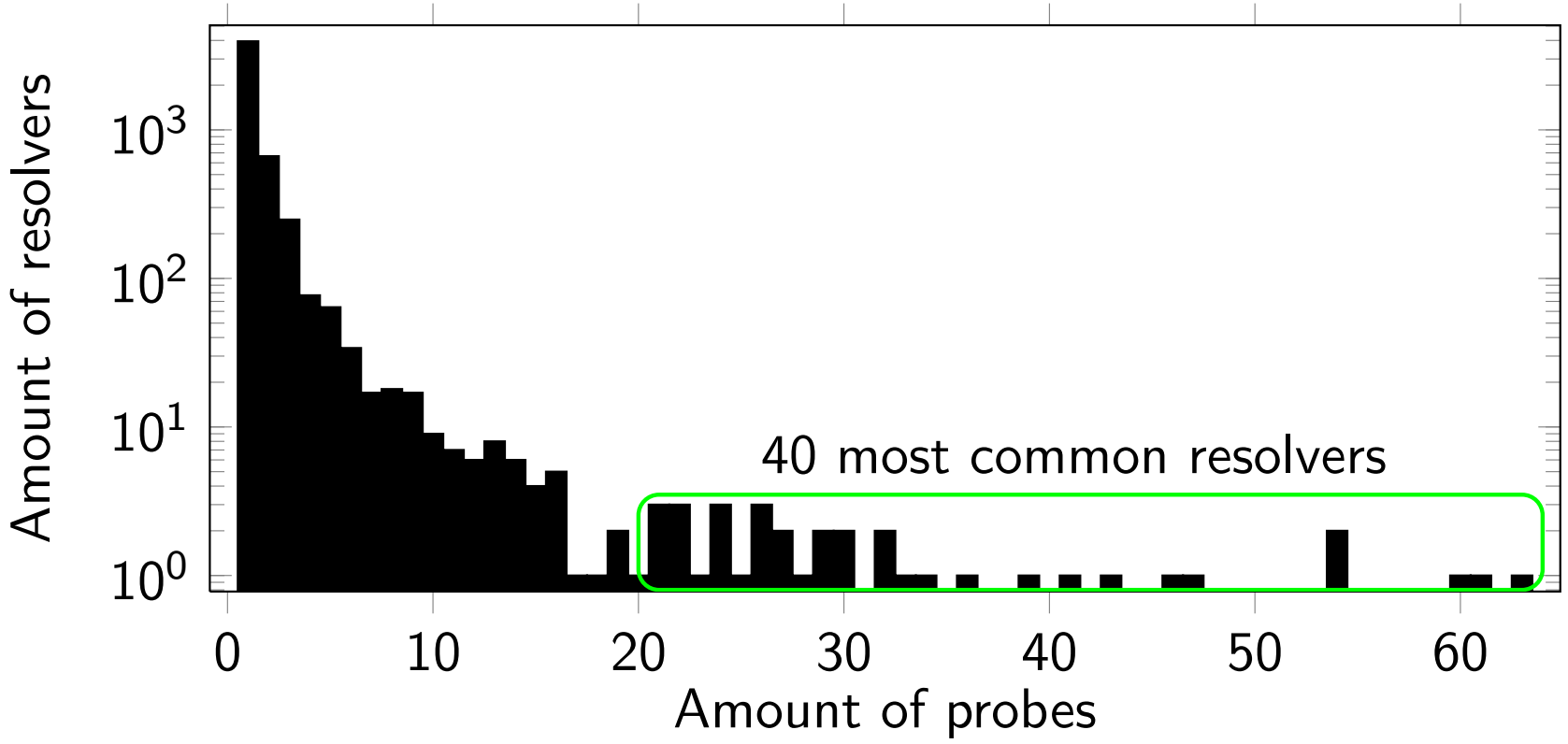
DO bit support

Requests on TXT record from secure zone with DO bit set

Probes	Resolvers	Setting DO bit	Including RRSIG
4673	5139	4534 [88.23%]	3448 [67.09%]

Resolvers

Resolvers distribution



40 most common resolvers: Google (38), OVH (2)

Validation and Protection

Protection

Zone	Probes	Answer Total	AD bit	RRSIGs+NSEC	RRSIGs only	Just answer
secure	5457	5160 [94.55%]	1472 [26.97%]	1109 [20.32%]	967 [17.72%]	1612 [20.54%]
badlabel	5366	3631 [67.66%]	0 [0.00%]	1014 [18.90%]	1004 [18.71%]	1613 [30.06%]
badrrsig	5427	3688 [67.95%]	0 [0.00%]	1017 [18.74%]	1034 [19.05%]	1636 [30.15%]
norrsigs	5491	3754 [68.37%]	0 [0.00%]	0 [0.00%]	0 [0.00%]	3754 [68.37%]

Zone	Probes	No Answer Total	SERVFAIL	FORMERR	Parse Error
secure	5457	297 [5.44%]	12 [0.22%]	263 [4.82%]	100 [1.83%]
badlabel	5366	1735 [32.33%]	1410 [26.28%]	302 [5.63%]	81 [1.51%]
badrrsigs	5427	1739 [32.04%]	1417 [26.11%]	299 [5.51%]	67 [1.23%]
norrsigs	5491	1737 [31.63%]	1416 [25.79%]	306 [5.57%]	20 [0.36%]

Validation and Protection

Protection

Zone	Probes	Answer Total	AD bit	RRSIGs+NSEC	RRSIGs only	Just answer
secure	5457	5160 [94.55%]	1472 [26.97%]	1109 [20.32%]	967 [17.72%]	1612 [20.54%]
badlabel	5366	3631 [67.66%]	0 [0.00%]	1014 [18.90%]	1004 [18.71%]	1613 [30.06%]
badrrsig	5427	3688 [67.95%]	0 [0.00%]	1017 [18.74%]	1034 [19.05%]	1636 [30.15%]
norrsigs	5491	3754 [68.37%]	0 [0.00%]	0 [0.00%]	0 [0.00%]	3754 [68.37%]

Zone	Probes	No Answer Total	SERVFAIL	FORMERR	Parse Error
secure	5457	297 [5.44%]	12 [0.22%]	263 [4.82%]	100 [1.83%]
badlabel	5366	1735 [32.33%]	1410 [26.28%]	302 [5.63%]	81 [1.51%]
badrrsigs	5427	1739 [32.04%]	1417 [26.11%]	299 [5.51%]	67 [1.23%]
norrsigs	5491	1737 [31.63%]	1416 [25.79%]	306 [5.57%]	20 [0.36%]

RRSIGs+NSEC and RRSIGs only

- All served names were wildcards
- Proof of the nonexistance of unexpanded name necessary (NSEC)
- Missing signed NSECs makes them BOGUS

Validation and Protection

Protection

Zone	Probes	Answer Total	AD bit	RRSIGs+NSEC	RRSIGs only	Just answer
secure	5457	5160 [94.55%]	1472 [26.97%]	1109 [20.32%]	967 [17.72%]	1612 [20.54%]
badlabel	5366	3631 [67.66%]	0 [0.00%]	1014 [18.90%]	1004 [18.71%]	1613 [30.06%]
badrrsig	5427	3688 [67.95%]	0 [0.00%]	1017 [18.74%]	1034 [19.05%]	1636 [30.15%]
norrsigs	5491	3754 [68.37%]	0 [0.00%]	0 [0.00%]	0 [0.00%]	3754 [68.37%]

Zone	Probes	No Answer Total	SERVFAIL	FORMERR	Parse Error
secure	5457	297 [5.44%]	12 [0.22%]	263 [4.82%]	100 [1.83%]
badlabel	5366	1735 [32.33%]	1410 [26.28%]	302 [5.63%]	81 [1.51%]
badrrsigs	5427	1739 [32.04%]	1417 [26.11%]	299 [5.51%]	67 [1.23%]
norrsigs	5491	1737 [31.63%]	1416 [25.79%]	306 [5.57%]	20 [0.36%]

RRSIGs+NSEC and RRSIGs only

- 27% validating + 38% DNSSEC-aware = **65% stub mode validation possible**
- 65% - 19% = **46% when it is a wildcard record**

DNSSEC-awareness

DS support

- Parent is authoritative

#	Answers	AD bit	With RRSIGs	Just answer	FORMERR
5602	5323 [95.01%]	1557 [27.79%]	2176 [38.84%]	1590 [28.38%]	268 [4.78%]

DNSSEC-awareness

DS support

- Parent is authoritative

#	Answers	AD bit	With RRSIGs	Just answer	FORMERR
5602	5323 [95.01%]	1557 [27.79%]	2176 [38.84%]	1590 [28.38%]	268 [4.78%]

- But DS might be answered from parent while iterating

DNSSEC-awareness

DS support

- Parent is authoritative

#	Answers	AD bit	With RRSIGs	Just answer	FORMERR
5602	5323 [95.01%]	1557 [27.79%]	2176 [38.84%]	1590 [28.38%]	268 [4.78%]

- But DS might be answered from parent while iterating
- First query something other than DS (cache NS records for zone)
- Secondly query DS

#	Answers	AD bit	RRSIGs	No RRSIGs	FORMERR
5266	4914 [93.31%]	1508 [28.64%]	2033 [38.61%]	1373 [26.07%]	273 [5.18%]

DNSSEC-awareness

DS support

- Parent is authoritative

#	Answers	AD bit	With RRSIGs	Just answer	FORMERR
5602	5323 [95.01%]	1557 [27.79%]	2176 [38.84%]	1590 [28.38%]	268 [4.78%]

- But DS might be answered from parent while iterating
- First query something other than DS (cache NS records for zone)
- Secondly query DS

#	Answers	AD bit	RRSIGs	No RRSIGs	FORMERR
5266	4914 [93.31%]	1508 [28.64%]	2033 [38.61%]	1373 [26.07%]	273 [5.18%]

- 88% set the DO bit
- They get the DS in the AUTHORITY section and cache!

DNSSEC-awareness

DS support

- Parent is authoritative
- First query something other than DS (cache NS records for zone)
- Secondly query DS

#	Answers	AD bit	RRSIGs	No RRSIGs	FORMERR
5266	4914 [93.31%]	1508 [28.64%]	2033 [38.61%]	1373 [26.07%]	273 [5.18%]

NXDOMAIN

#	No Answer	AD bit	RRSIGs	No RRSIGs	FORMERR
5204	4844 [93.08%]	1426 [27.40%]	1833 [35.22%]	1568 [30.13%]	263 [5.05%]

Plus 65 [1.25%] spoofed answers!

DNSSEC-awareness

DS support

- Parent is authoritative
- First query something other than DS (cache NS records for zone)
- Secondly query DS

#	Answers	AD bit	RRSIGs	No RRSIGs	FORMERR
5266	4914 [93.31%]	1508 [28.64%]	2033 [38.61%]	1373 [26.07%]	273 [5.18%]

NXDOMAIN

#	No Answer	AD bit	RRSIGs	No RRSIGs	FORMERR
5204	4844 [93.08%]	1426 [27.40%]	1833 [35.22%]	1568 [30.13%]	263 [5.05%]

Plus 65 [1.25%] spoofed answers!

- Collect everything Stub DNSSEC-iterator might work in 93%, but only for existing names
- Proofs of non-existence 27.4% + 35.2% = 62.6%

Findings

Validation and protection

- AD bit indicates 26%-28% validation
- Bad zones indicate 26% protection

DNSSEC-awareness

- DO bit indicates 88%
- 93% Can get a zone's DS
- Proof of non existence available with 63%
- Signatures available for normal answers with 65%
- Signatures available for wildcard answers with 46%