

Measuring the Deployment of DNSSEC over the Internet

System & Network Engineering — Research Project

Nicolas Cancell



UNIVERSITY OF AMSTERDAM

NLnet
Labs

RIPE68 — May 14, 2014

1 Introduction

2 Methodology

3 Results

What DNSSEC?

DNS

Domain Name System

- Essential foundation of the Internet
- Translates domain names into IP addresses

Problem

DNS is notoriously insecure

Solution: DNSSEC

- Public key cryptography
- Signatures for all resources
- Hierarchical chain of trust

1 Introduction

2 Methodology

3 Results

History

DNS Development

- 1983 DNS specification published
- 1984 First TLDs defined
- 1987 DNS becomes IETF standard

DNSSEC Development

- 1997 DNSSEC specification published
- 1999 DNSSEC specification revised
- 2005 DNSSEC final revision

DNSSEC Deployment

- 2010 Root level deployment
- 2011 Most TLDs signed

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?

The Atlas network



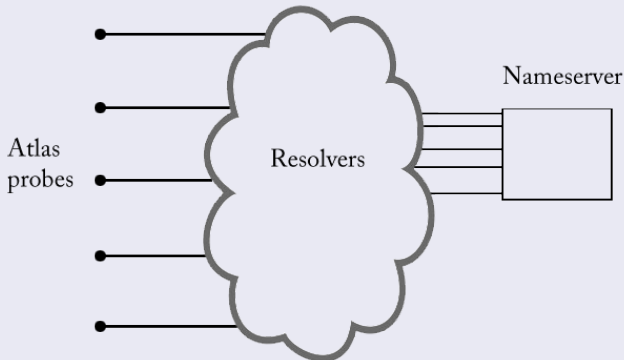
- 5,000 active probes
- Worldwide — mostly Europe

1 Introduction

2 Methodology

3 Results

Setup



- Atlas probes: presence in client network
- 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

1 Introduction

2 Methodology

3 Results

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%]

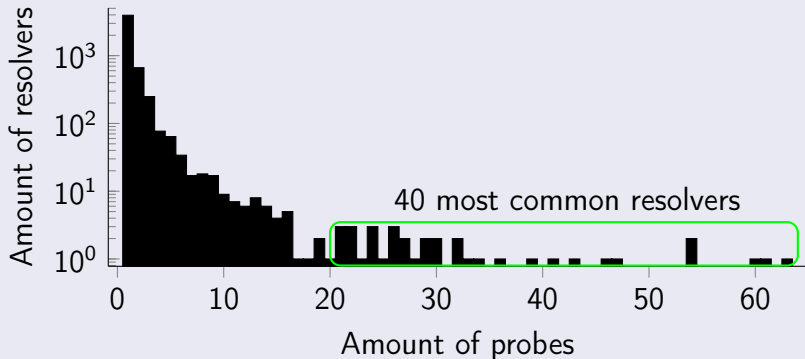
DS type support

Requests on DS record from secure zone with DO bit set

Probes	Answers	Authenticated	
4553	4228 [92.73%]	1409 [30.41%]	
Resolvers	Active	Answers	Authenticated
4586	4573	4252 [92.98%]	1374 [30.05%]

Probes (1)

Resolvers distribution



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

Probes (2)

Protection

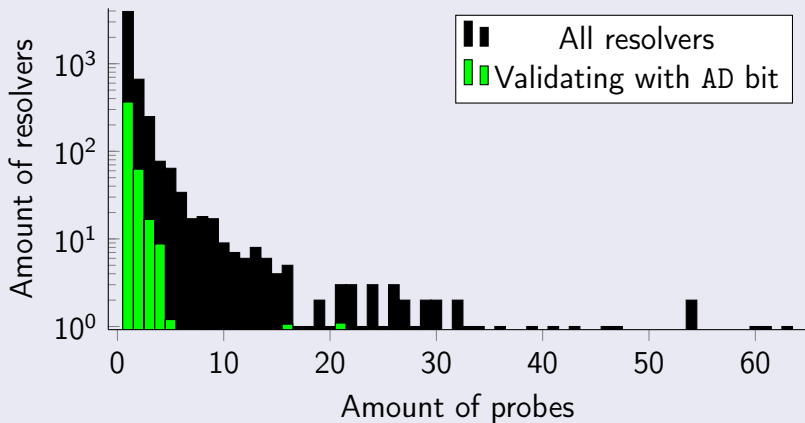
Zone	Probes	Answer	No Answer			
			NOERROR	FORMERR	SERVFAIL	REFUSED
secure	4606	3098 [67.26%]	1215 [26.38%]	252 [5.47%]	18 [0.39%]	23 [0.50%]
badlabel	4212	2381 [56.53%]	296 [7.03%]	286 [6.79%]	1224 [29.06%]	25 [0.59%]
badrrsigs	4211	2381 [56.54%]	299 [7.10%]	294 [6.98%]	1212 [28.78%]	25 [0.59%]
norrsigs	4124	2655 [64.38%]	1 [0.02%]	292 [7.08%]	1152 [27.93%]	24 [0.58%]

Compatibility

Zone	Probes	Answer	No Answer		
			with AD bit	NOERROR	SERVFAIL
secure	4606	3098 [67.26%]	822 [17.84%]	1215 [26.38%]	18 [0.39%]
insecure	4642	4350 [93.71%]	0 [0.00%]	1 [0.02%]	16 [0.34%]
secure	4695	4376 [93.20%]	1404 [29.90%]	2 [0.04%]	11 [0.23%]

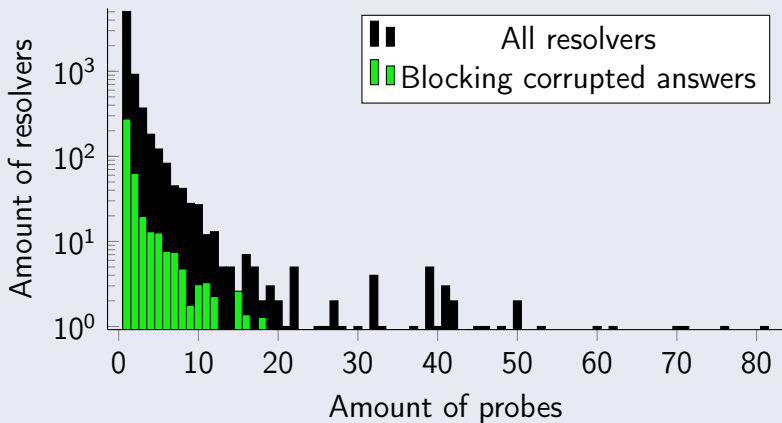
Probes (3)

Validation distribution



Probes (4)

Protection distribution



Findings

DNSSEC-awareness

- DO bit indicates 87%
- DS type indicates 93%

Validation and protection

- AD bit indicates 30% validation
- bad zones indicate 27-29% protection
- signatures available in 67% of answers

Issues

- Fallback when RRSIG missing: 1%
- Bad validation of wildcards: 26%

Thanks to...

- NLnet Labs, Amsteram
- SNE Master, University of Amsterdam

Questions?