DNSThought

NLNETLABS

Willem Toorop

DNSSEC Workshop at the

ICANN 69 VIRTUAL ANNUAL GENERAL

21 October 2020

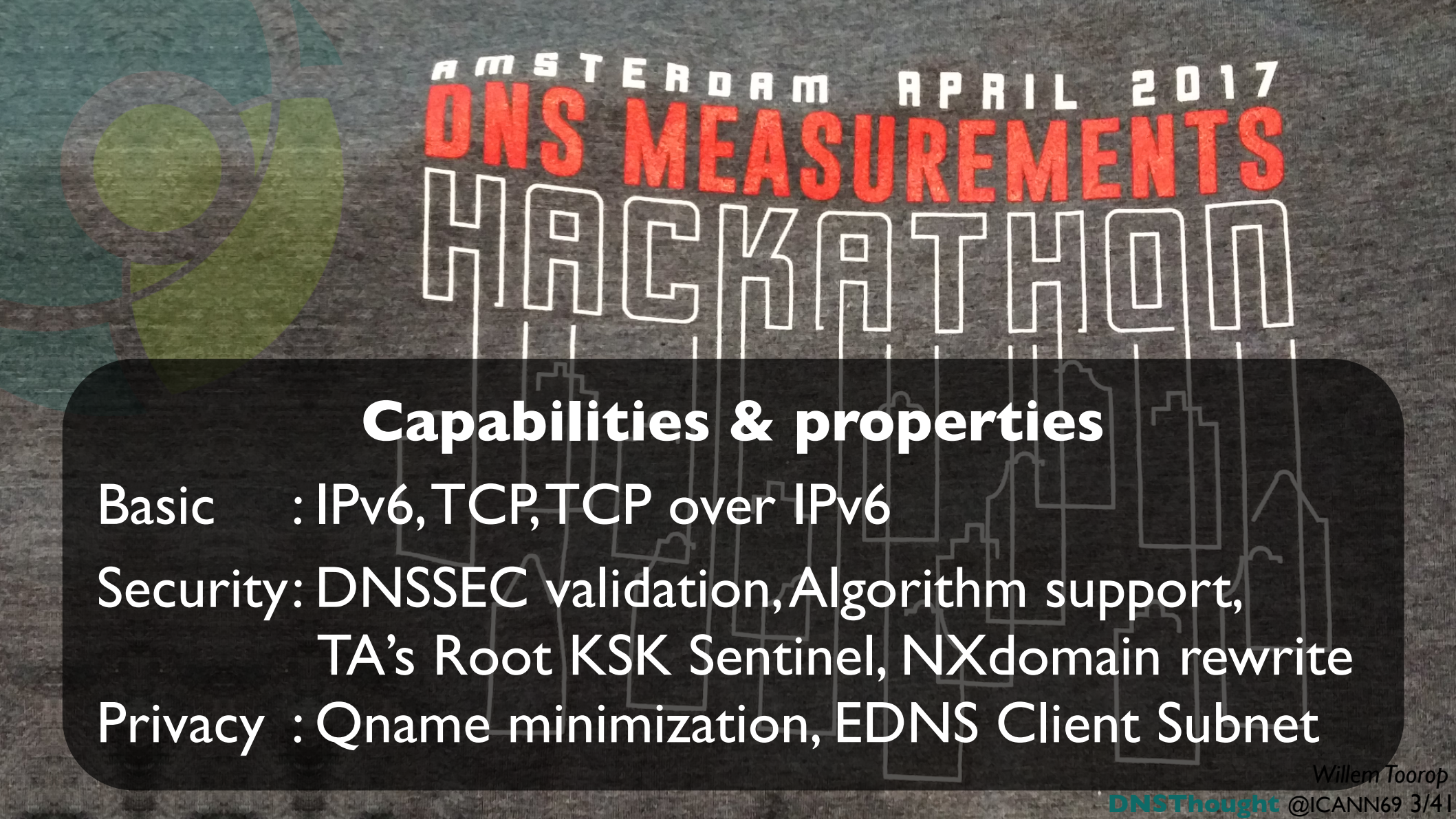
Everything you ever wanted to know about caching resolvers but were afraid to ask

Pariticpants:

Andrea Barberio, Petros Gigis, Jerry Lundström, Teemu Rytilahti, Willem Toorop

Goal:

Provide insight into caching resolver capabilities

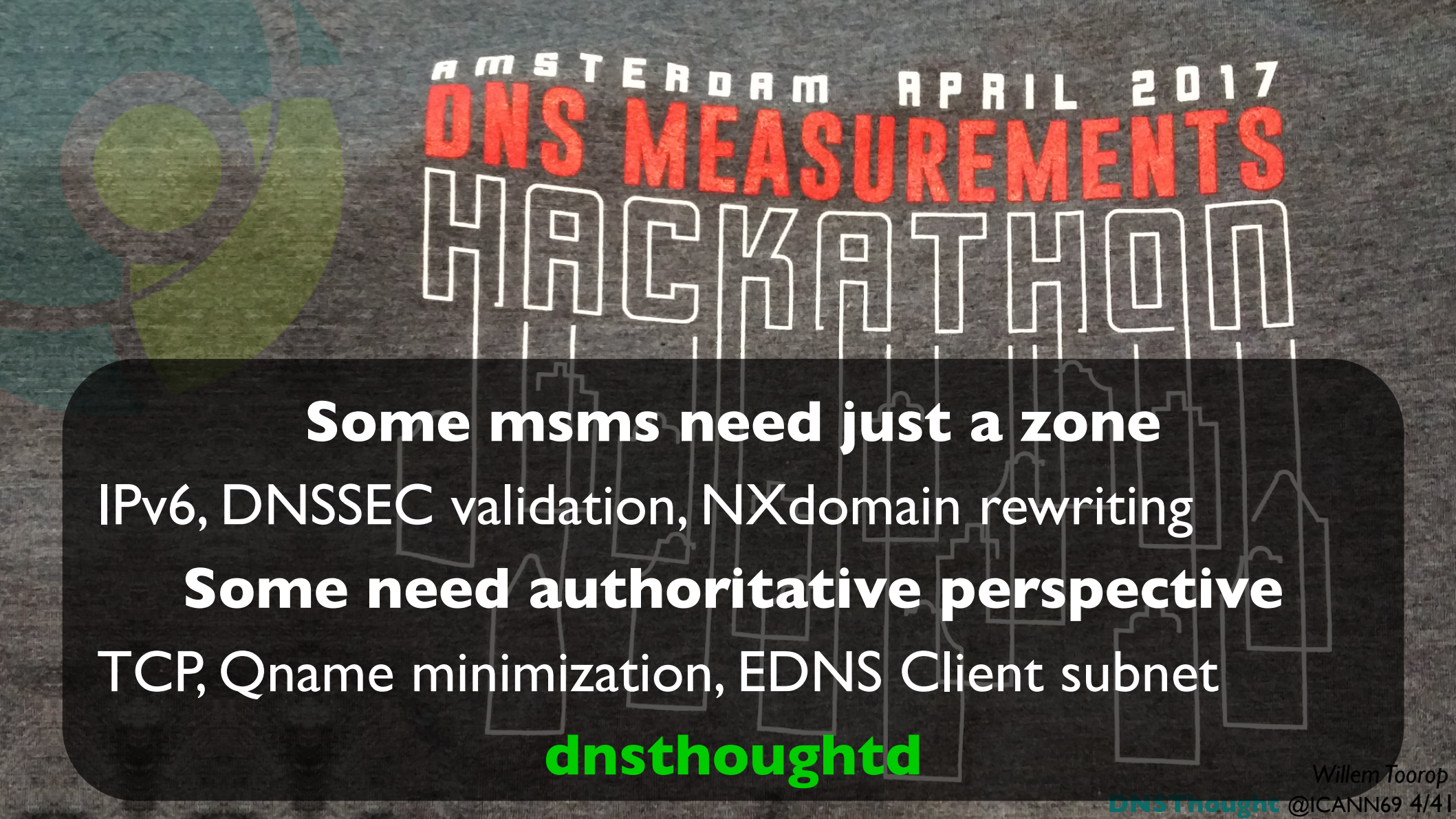


Capabilities & properties

Basic : IPv6, TCP, TCP over IPv6

Security: DNSSEC validation, Algorithm support,
TA's Root KSK Sentinel, NXdomain rewrite

Privacy : Qname minimization, EDNS Client Subnet



Some msms need just a zone

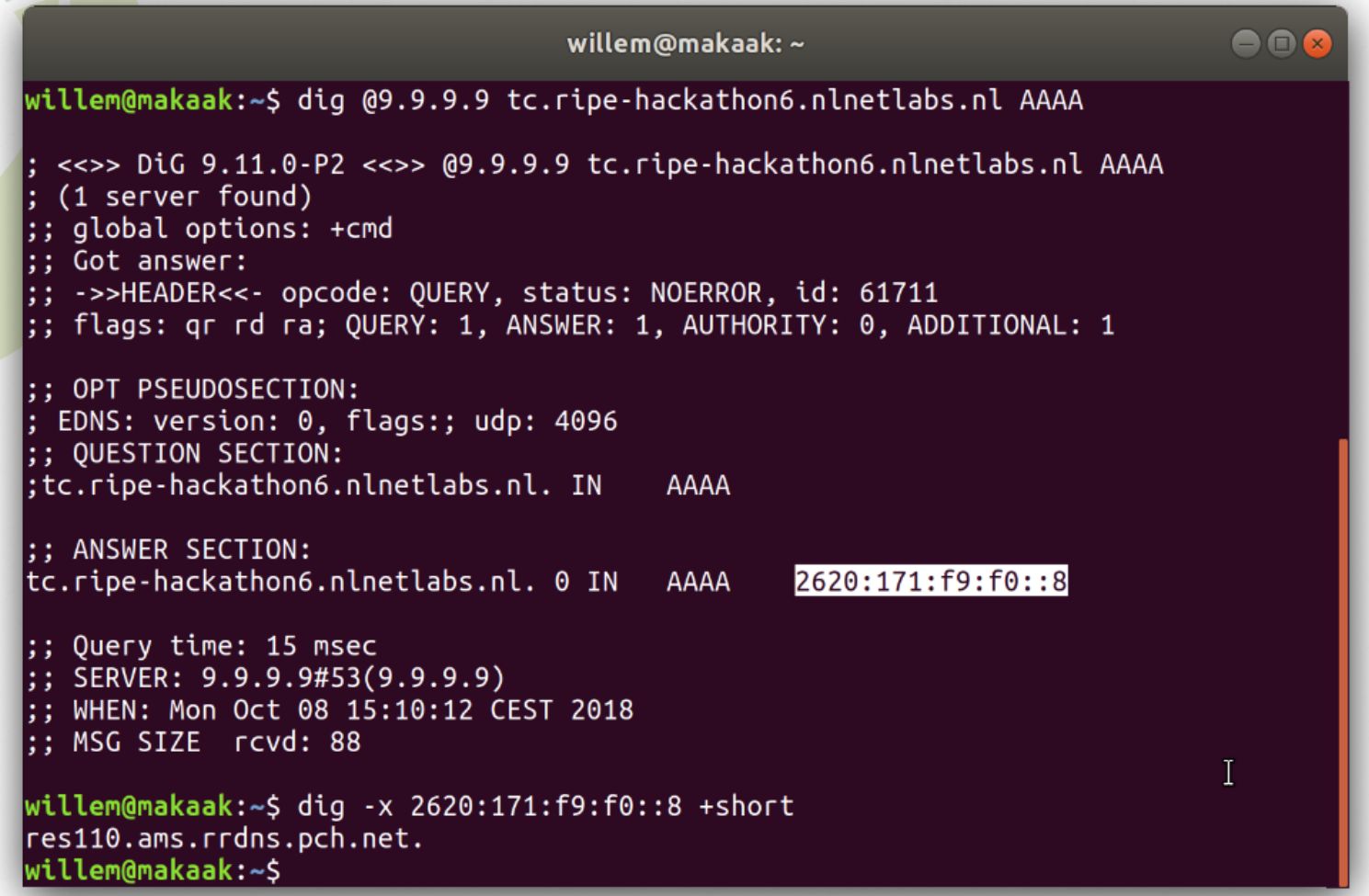
IPv6, DNSSEC validation, NXdomain rewriting

Some need authoritative perspective

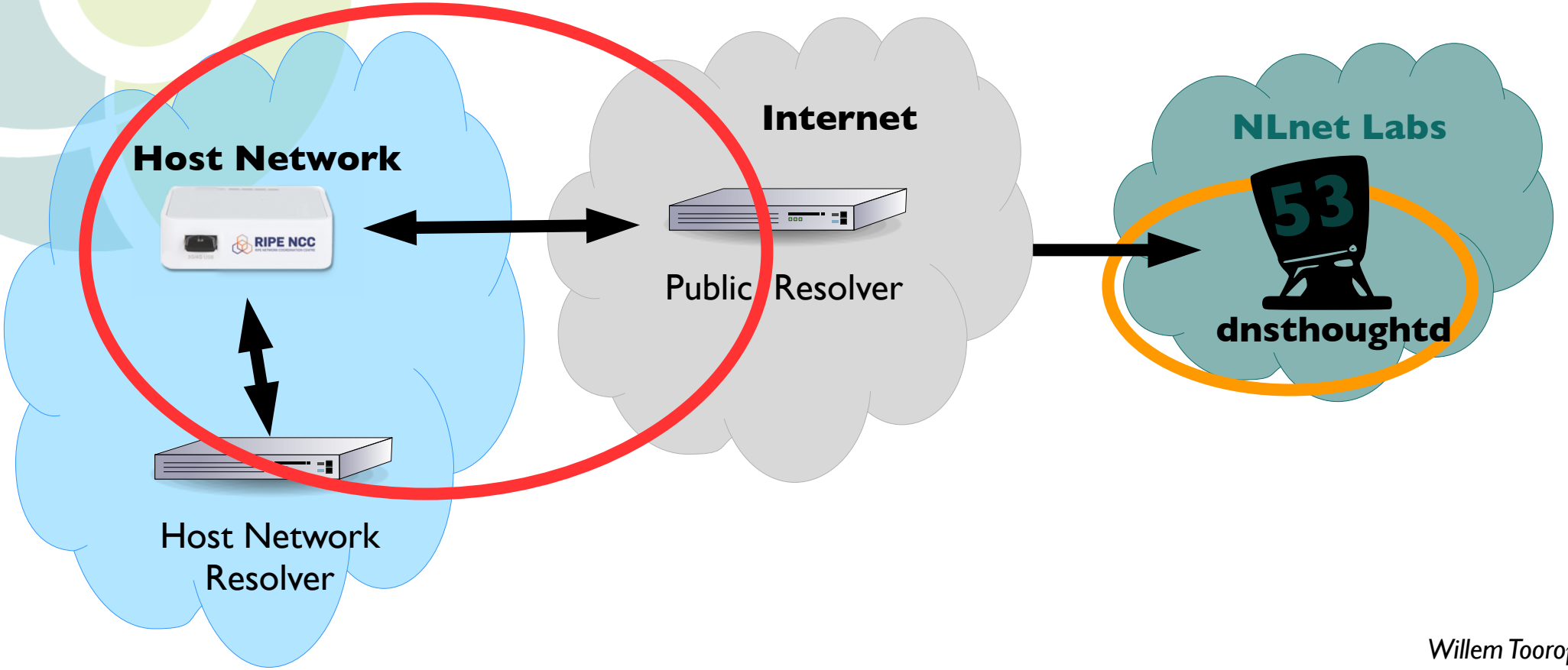
TCP, Qname minimization, EDNS Client subnet

dnsthoughtd

dnsthoughtd



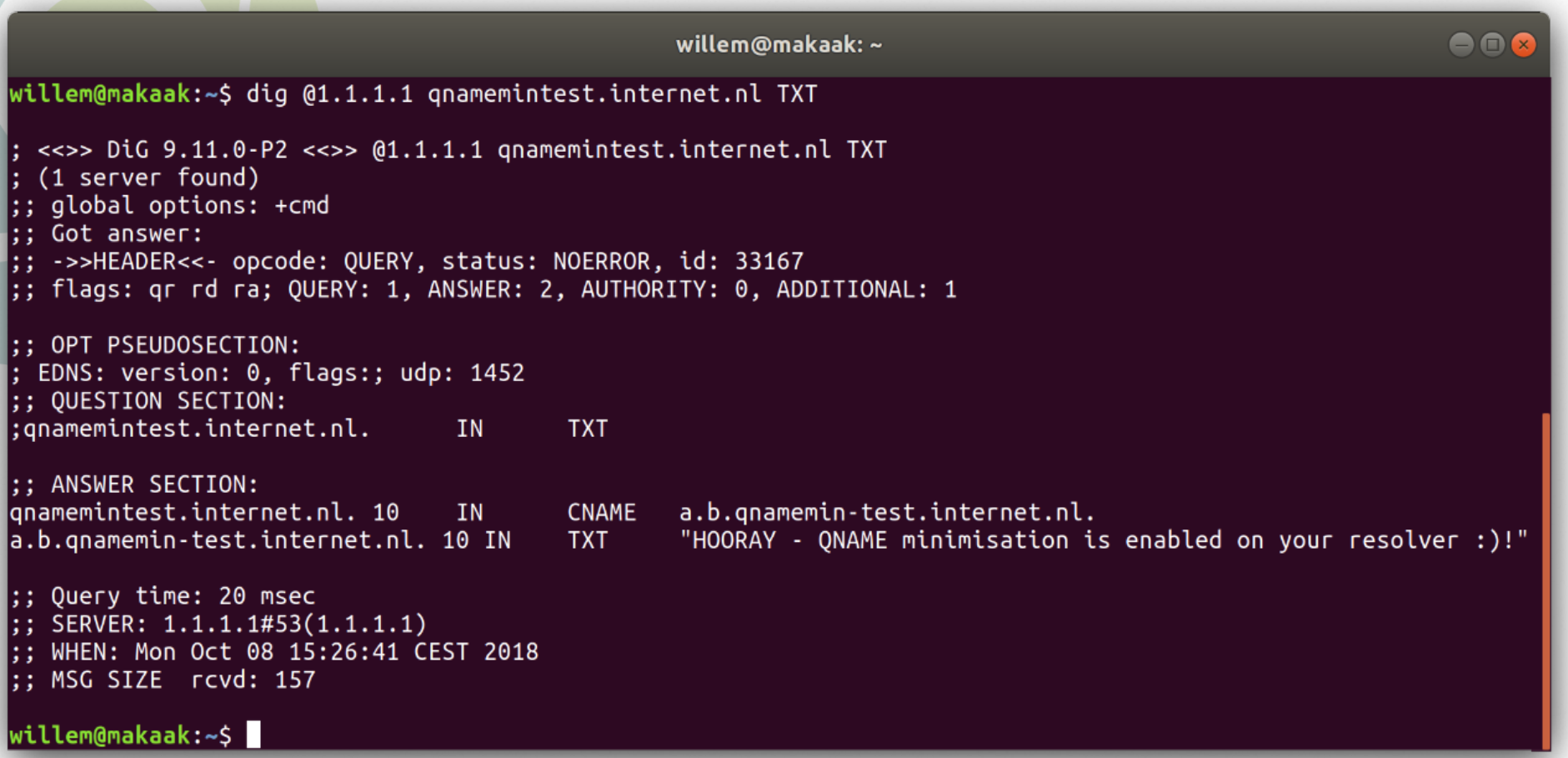
The RIPE Atlas perspective



The RIPE Atlas perspective

	Probe ASN	Resolver ASN	Authoritative ASN
Internal	X	=	X
Forwarding	X	X	Z
	X	Y	Z
External	X	Z	Z

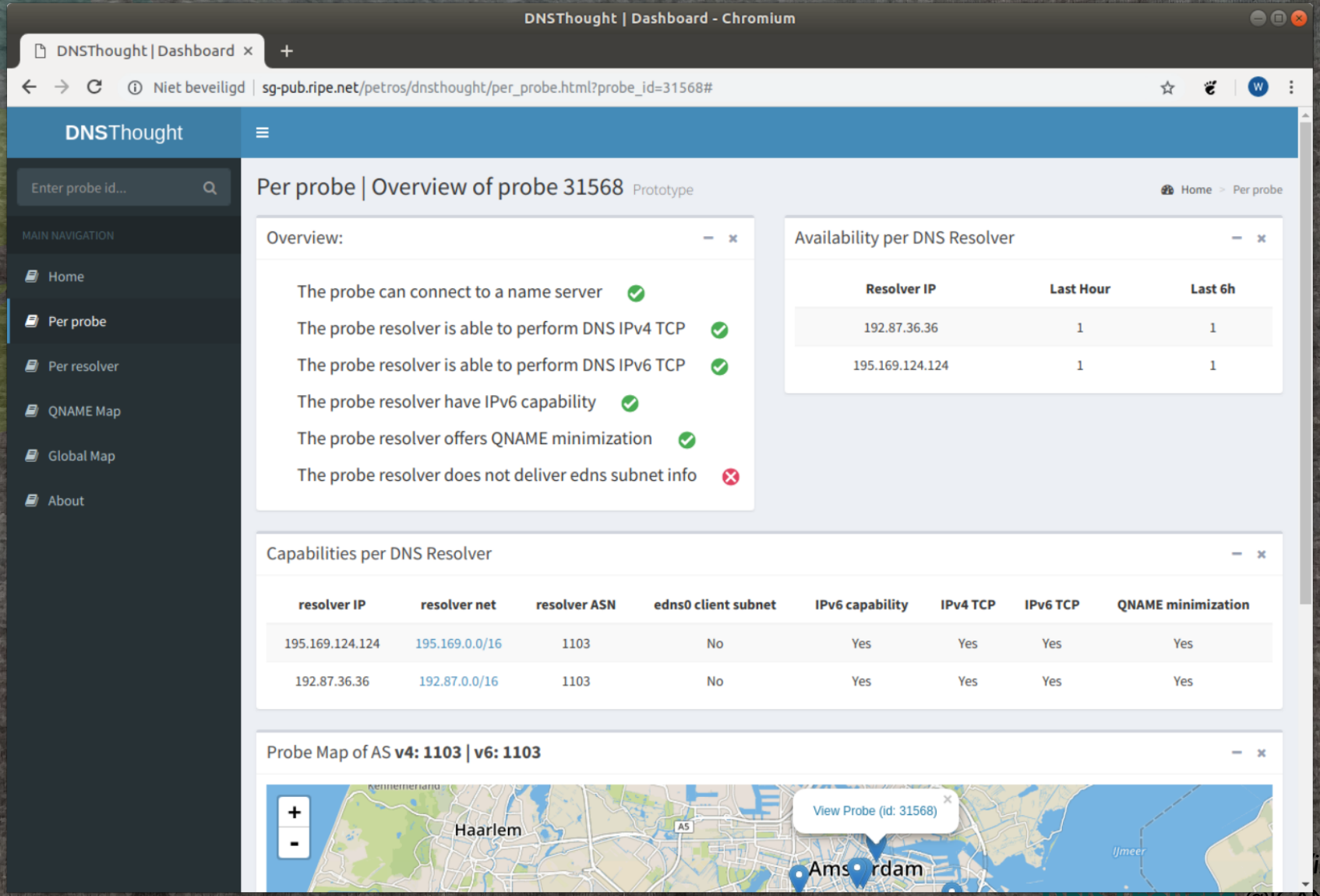
Qname minimization



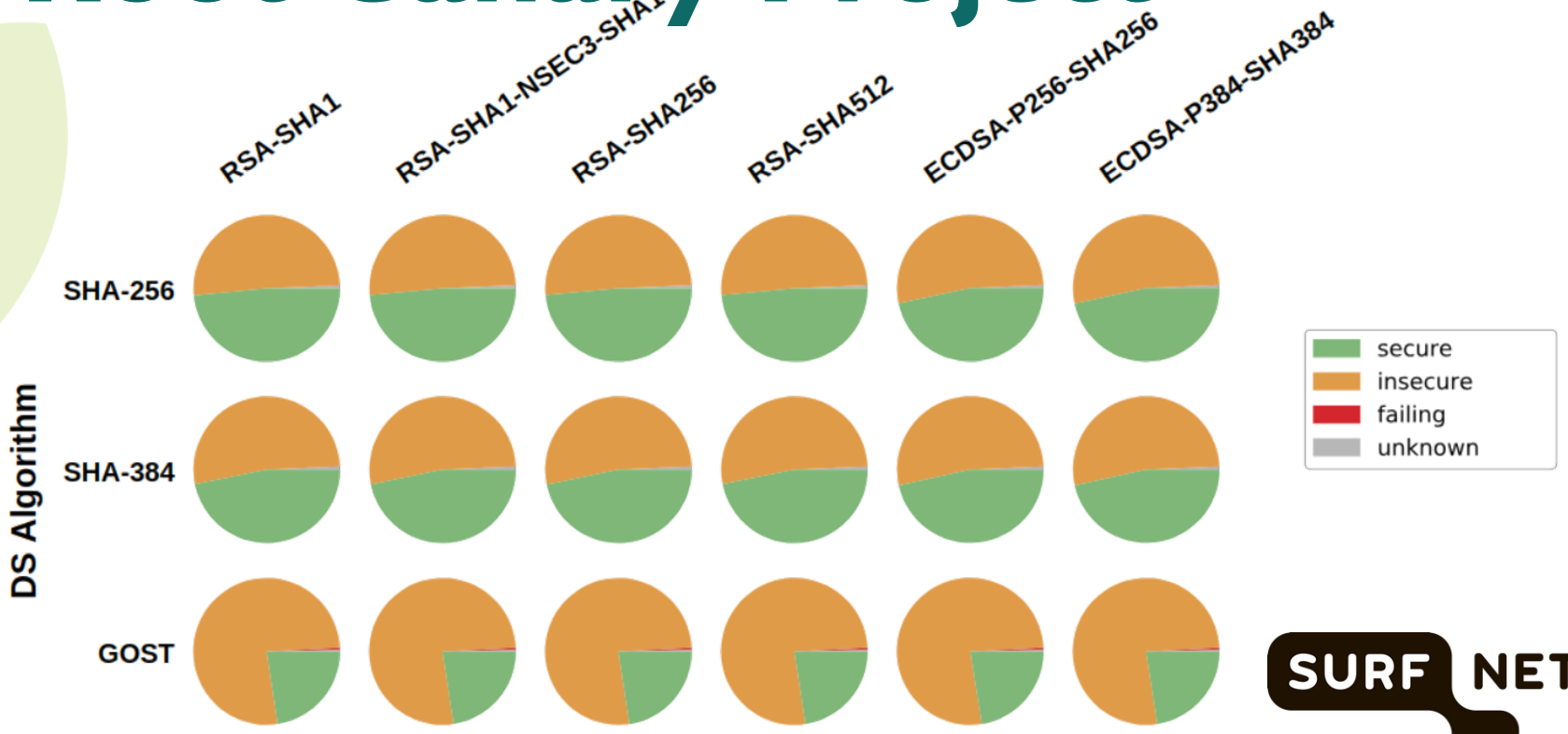
Measurements for all probes every hour

query		msm ID
<prb_id>.<time>.ripe-hackathon6.nlnetlabs.nl	AAAA	8310366
<prb_id>.<time>.tc.ripe-hackathon4.nlnetlabs.nl	A	8310360
<prb_id>.<time>.tc.ripe-hackathon6.nlnetlabs.nl	AAAA	8310364
qnamemintest.internet.nl	TXT	8310250
nxdomain.ripe-hackathon2.nlnetlabs.nl	A	8311777
whoami.akamai.net	A	8310245
o-o.myaddr.l.google.com	TXT	8310237
secure.ripe-hackathon2.nlnetlabs.nl	A	8311760
bogus.ripe-hackathon2.nlnetlabs.nl	A	8311763

Thank you Emile Aben!


DNSThought | Dashboard - Chromium
DNSThought | Dashboard
Niet beveiligd | sg-pub.ripe.net/petros/dnsthought/per_probe.html?probe_id=31568#
DNSThought
Enter probe id...
MAIN NAVIGATION
Home
Per probe
Per resolver
QNAME Map
Global Map
About
Per probe | Overview of probe 31568 Prototype
Home > Per probe
Overview:
The probe can connect to a name server
The probe resolver is able to perform DNS IPv4 TCP
The probe resolver is able to perform DNS IPv6 TCP
The probe resolver have IPv6 capability
The probe resolver offers QNAME minimization
The probe resolver does not deliver edns subnet info
Availability per DNS Resolver
Resolver IP | Last Hour | Last 6h
192.87.36.36 | 1 | 1
195.169.124.124 | 1 | 1
Capabilities per DNS Resolver
resolver IP | resolver net | resolver ASN | edns0 client subnet | IPv6 capability | IPv4 TCP | IPv6 TCP | QNAME minimization
195.169.124.124 | 195.169.0.0/16 | 1103 | No | Yes | Yes | Yes | Yes
192.87.36.36 | 192.87.0.0/16 | 1103 | No | Yes | Yes | Yes | Yes
Probe Map of AS v4: 1103 | v6: 1103
View Probe (id: 31568)
Haarlem
A5
IJmeer

Root Canary Project



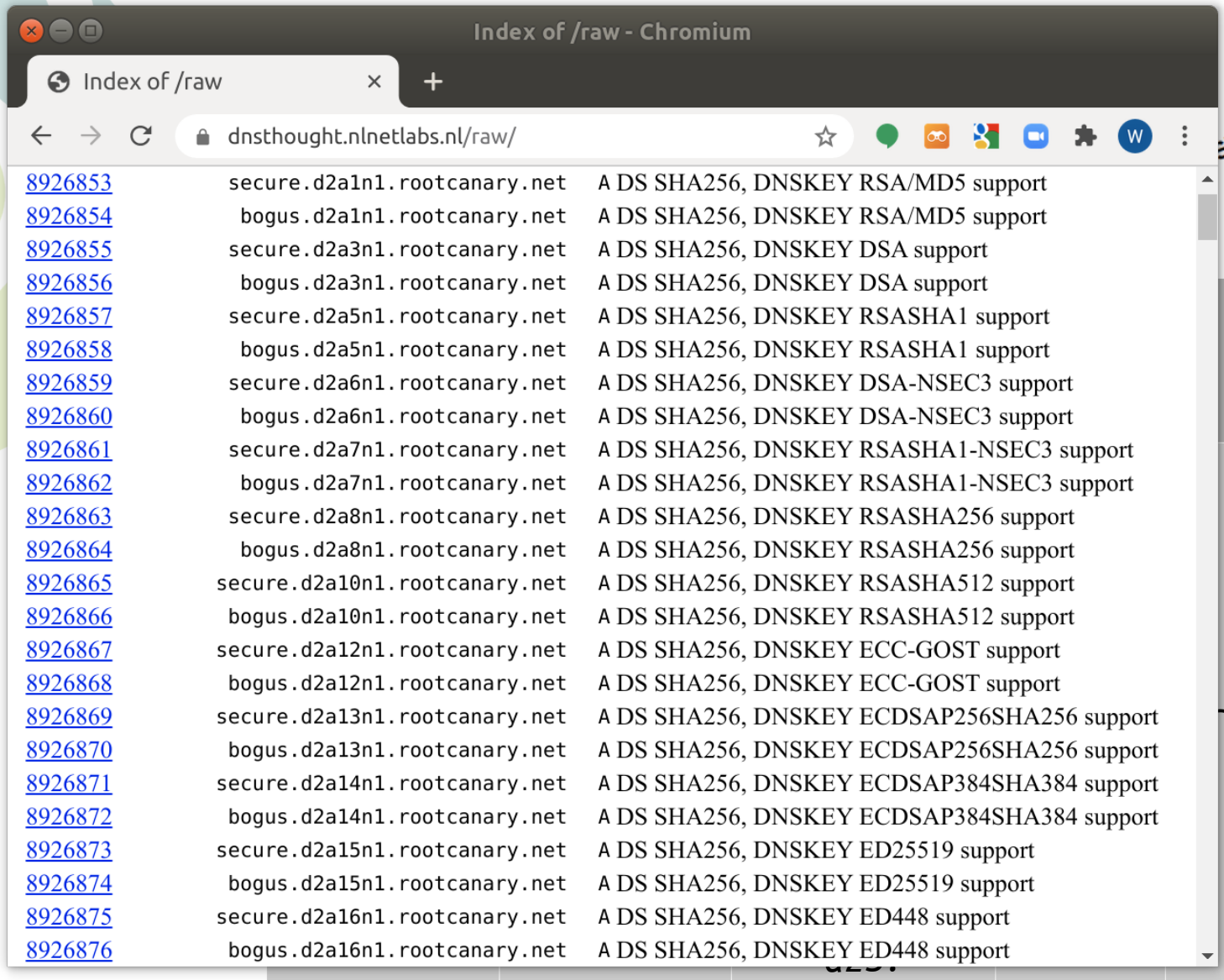
- Participation with Roland van Rijswijk - Deij
- Measurements started 20 June 2017

Root Canary Project

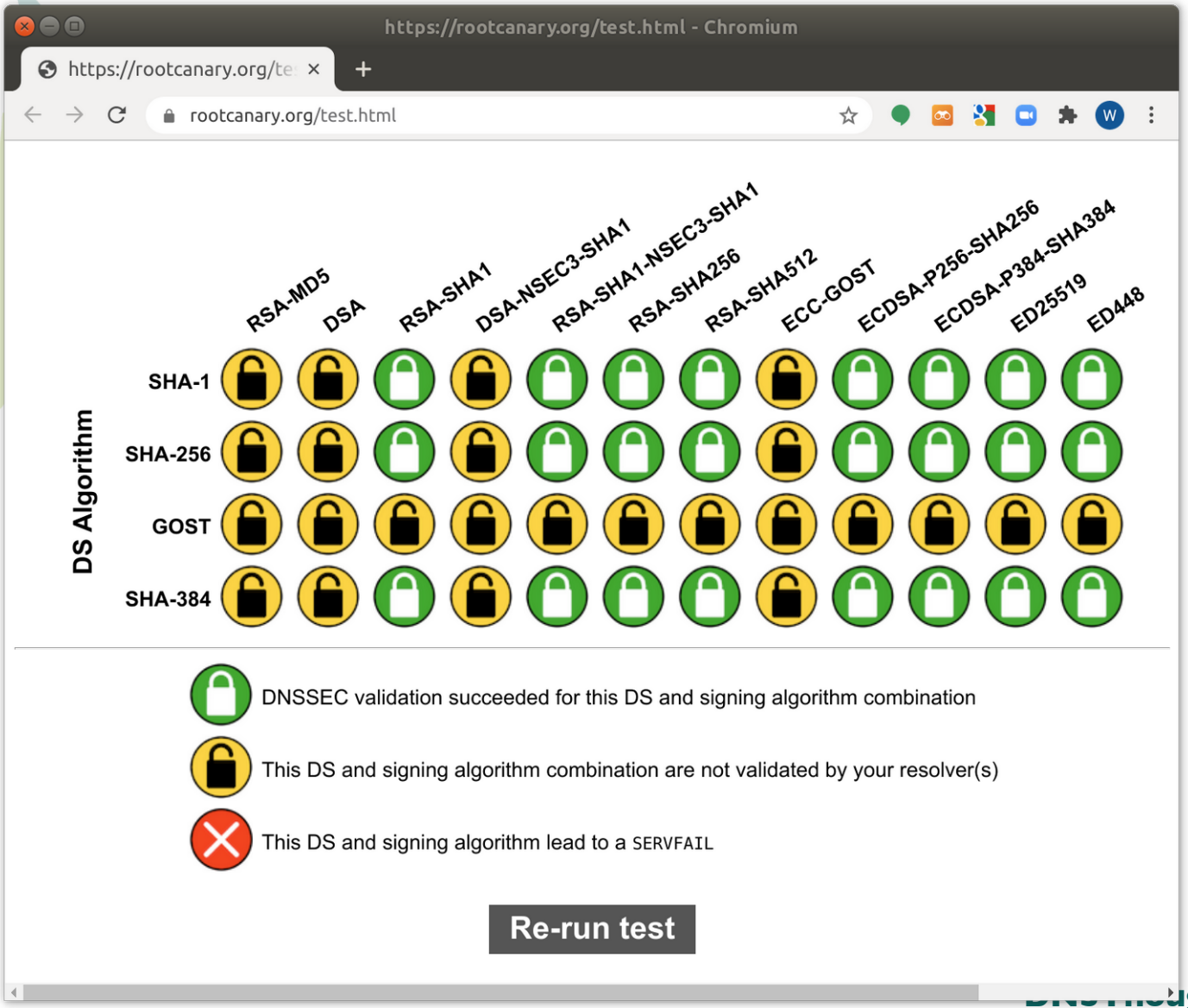
RSA-SHA1 | RSA-SHA1-NSEC3-SHA1 | RSA-SHA256 | RSA-SHA512 | ECDSA-P256-SHA256 | ECDSA-P384-SHA384

DS Algorithm: SHA-256 / SHA-384 / GOST

	DS Algorithm	DNSKEY Algorithm	NSEC version	
secure. bogus.	d1 d2 d3 d4	a1 a3 a5 a6 a7 a8 a10 a12 a13 a14 a15 a16 *a23?*	n1 n3	.rootcanary.net



8926853	secure.d2a1n1.rootcanary.net	A DS SHA256, DNSKEY RSA/MD5 support
8926854	bogus.d2a1n1.rootcanary.net	A DS SHA256, DNSKEY RSA/MD5 support
8926855	secure.d2a3n1.rootcanary.net	A DS SHA256, DNSKEY DSA support
8926856	bogus.d2a3n1.rootcanary.net	A DS SHA256, DNSKEY DSA support
8926857	secure.d2a5n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA1 support
8926858	bogus.d2a5n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA1 support
8926859	secure.d2a6n1.rootcanary.net	A DS SHA256, DNSKEY DSA-NSEC3 support
8926860	bogus.d2a6n1.rootcanary.net	A DS SHA256, DNSKEY DSA-NSEC3 support
8926861	secure.d2a7n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA1-NSEC3 support
8926862	bogus.d2a7n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA1-NSEC3 support
8926863	secure.d2a8n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA256 support
8926864	bogus.d2a8n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA256 support
8926865	secure.d2a10n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA512 support
8926866	bogus.d2a10n1.rootcanary.net	A DS SHA256, DNSKEY RSASHA512 support
8926867	secure.d2a12n1.rootcanary.net	A DS SHA256, DNSKEY ECC-GOST support
8926868	bogus.d2a12n1.rootcanary.net	A DS SHA256, DNSKEY ECC-GOST support
8926869	secure.d2a13n1.rootcanary.net	A DS SHA256, DNSKEY ECDSAP256SHA256 support
8926870	bogus.d2a13n1.rootcanary.net	A DS SHA256, DNSKEY ECDSAP256SHA256 support
8926871	secure.d2a14n1.rootcanary.net	A DS SHA256, DNSKEY ECDSAP384SHA384 support
8926872	bogus.d2a14n1.rootcanary.net	A DS SHA256, DNSKEY ECDSAP384SHA384 support
8926873	secure.d2a15n1.rootcanary.net	A DS SHA256, DNSKEY ED25519 support
8926874	bogus.d2a15n1.rootcanary.net	A DS SHA256, DNSKEY ED25519 support
8926875	secure.d2a16n1.rootcanary.net	A DS SHA256, DNSKEY ED448 support
8926876	bogus.d2a16n1.rootcanary.net	A DS SHA256, DNSKEY ED448 support


https://rootcanary.org/test.html - Chromium
https://rootcanary.org/te
rootcanary.org/test.html
RSA-MD5
DSA
RSA-SHA1
DSA-NSEC3-SHA1
RSA-SHA1-NSEC3-SHA1
RSA-SHA256
RSA-SHA512
ECC-GOST
ECDSA-P256-SHA256
ECDSA-P384-SHA384
ED25519
ED448
DS Algorithm
SHA-1
SHA-256
GOST
SHA-384
DNSSEC validation succeeded for this DS and signing algorithm combination
This DS and signing algorithm combination are not validated by your resolver(s)
This DS and signing algorithm lead to a SERVFAIL
Re-run test

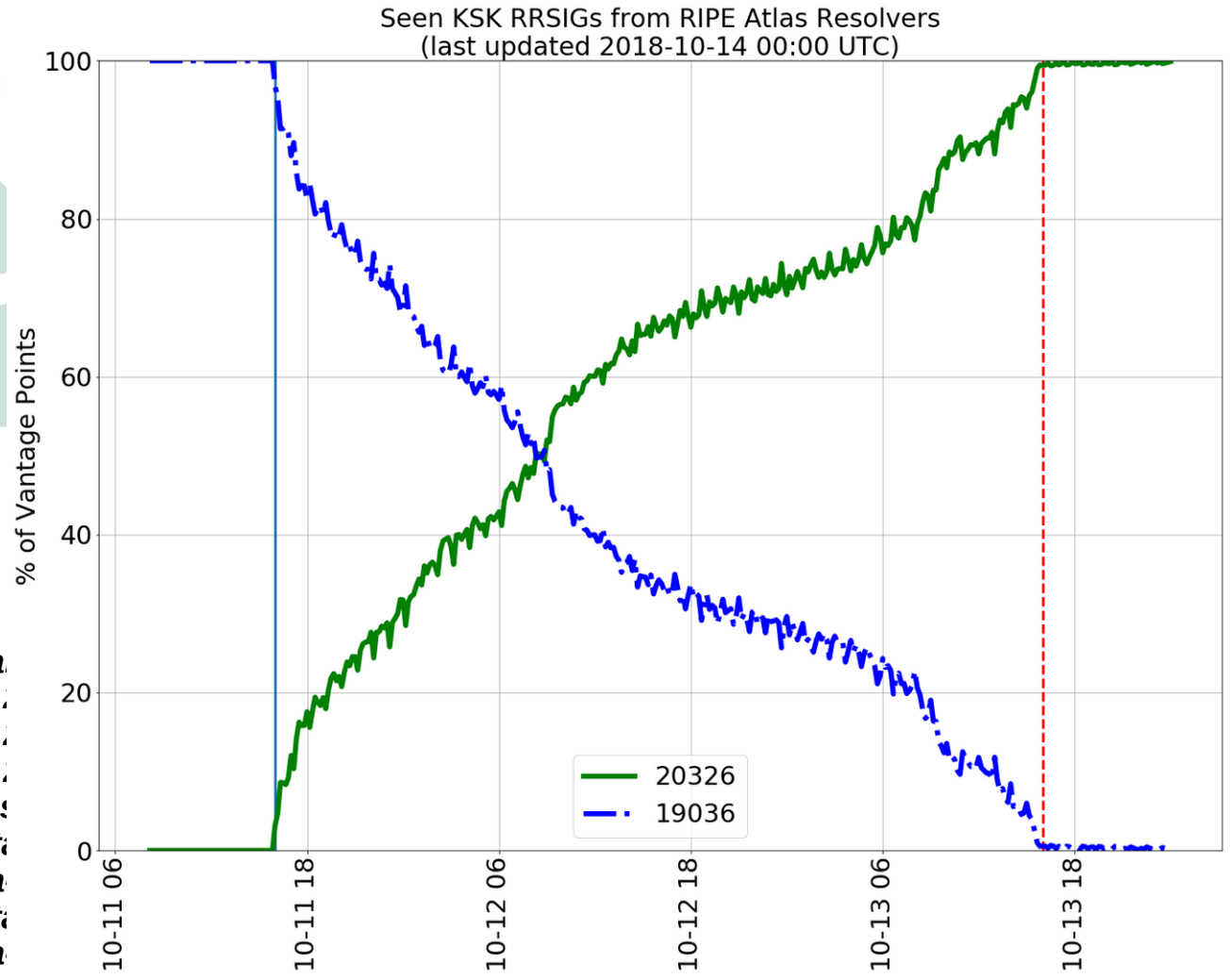
More measurements

- Moritz Muller joined too
- Root KSK Sentinel msms since 19 July 2018

query	msm ID
`root-key-sentinel-not-ta-19036.d2a8n3.rootcanary.net A`	15283670
`root-key-sentinel-not-ta-20326.d2a8n3.rootcanary.net A`	15283671

With validating resolvers we have three situations:
1. Key 20326 has not been picked up (yet)
2. Key 20326 is a valid TA, and key 19036 is still a valid TA
3. Key 20326 is a valid TA, and key 19036 is removed
For these situations (1, 2,3), measurements for:
- (not-ta-19036 is-ta-20326) results in 1: (S S), 2: (S A), 3: (A A)
- (is-ta-19036 is-ta-20326) results in 1: (A S), 2: (A A), 3: (S A)
- (not-ta-19036 not-ta-20326) results in 1: (S A), 2: (S S), 3: (A S)
- (is-ta-19036 not-ta-20326) results in 1: (A A), 2: (A S), 3: (S S)

More measurements



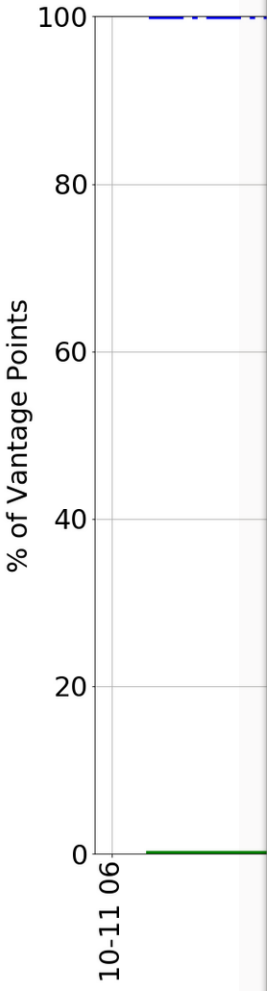
…o

…ns

	msm ID
…anary.net A	15283670
…anary.net A	15283671

With va…
1. Key …
2. Key …
3. Key …
For thes…
- (not-ta…
- (is-ta…
- (not-ta…
- (is-ta…

More measurements



With va
1. Key
2. Key
3. Key
For thes
- (not-ta
- (is-ta
- (not-ta
- (is-ta

Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover

Moritz Müller
University of Twente and SIDN Labs

Matthew Thomas
Verisign

Duane Wessels
Verisign

Wes Hardaker
USC/Information Sciences Institute

Taejoong Chung
Rochester Institute of Technology

Willem Toorop
NLnet Labs

Roland van Rijswijk-Deij
University of Twente and NLnet Labs

ABSTRACT

The DNS Security Extensions (DNSSEC) add authenticity and integrity to *the* naming system of the Internet. Resolvers that validate information in the DNS need to know the cryptographic public key used to sign the root zone of the DNS. Eight years after its introduction and one year after the originally scheduled date, this key was replaced by ICANN for the first time in October 2018. ICANN considered this event, called a *rollover*, *"an overwhelming success"* and during the rollover they detected *"no significant outages"*.

In this paper, we independently follow the process of the rollover starting from the events that led to its postponement in 2017 until the removal of the old key in 2019. We collected data from multiple vantage points in the DNS ecosystem for the entire duration of the rollover process. Using this data, we study key events of the rollover. These events include telemetry signals that led to the rollover being postponed, a near real-time view of the actual rollover in resolvers and a significant increase in queries to the root of the DNS once the old key was revoked. Our analysis contributes significantly to identifying the causes of challenges observed during the rollover. We show that while from an end-user perspective, the roll indeed passed without major problems, there are many opportunities for improvement and important lessons to be learned from events

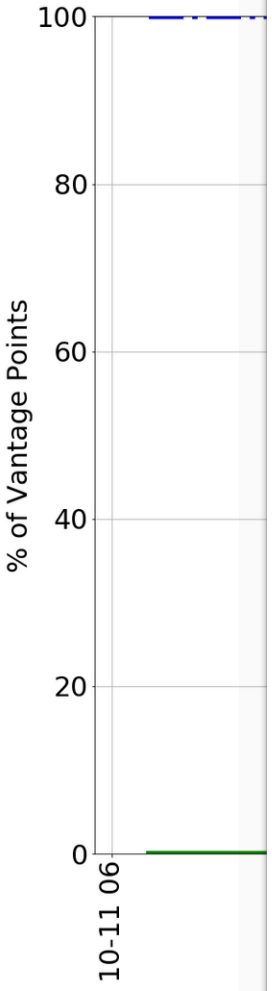
1 INTRODUCTION

The Domain Name System (DNS) is *the* naming system of the Internet. Since 2010, the root of the DNS is secured with the DNS Security Extensions (DNSSEC), adding a layer of authenticity and integrity. DNSSEC uses public-key cryptography to sign the content in the DNS and enables recursive resolvers[1] to validate that the information they receive is authentic. The sequence of cryptographic keys signing other cryptographic keys is called a *chain of trust*. The public key at the beginning of this chain of trust is called a *trust anchor*. Validators have a list of trust anchors, which they trust implicitly. The Root Key Signing Key (KSK) acts as the trust anchor for DNSSEC and this cryptographic key was added to the root zone in July 2010. Eight years later, and after a one year delay, the KSK was replaced for the very first time, following established policy that requires regular rollovers of the Root KSK [1]. This event, usually referred to as the Root KSK Rollover (hereafter "the rollover"), required years of preparation and was considered risky. Stakeholders expected, in the worst case, millions of Internet users (up to 13%) to become unable to resolve a domain name [2].

The Internet Corporation for Assigned Names and Numbers (ICANN), the organization responsible for coordinating and rolling the key, collected feedback from the community before the rollover. Two risks were most feared: (i) resolvers that would not update their

msm ID
15283670
15283671

More measurements



With va
1. Key
2. Key
3. Key

For thes
- (not-ta
- (is-ta
- (not-ta
- (is-ta

Roll, Roll, Rol

Moritz Mül
University of Twente ar

Wes Hardak
USC/Information Scien

ABSTRACT

The DNS Security Extensions
tegrity to *the* naming system o
information in the DNS need t
used to sign the root zone of
duction and one year after the
was replaced by ICANN for th
considered this event, called a
and during the rollover they d

In this paper, we independen
starting from the events that l
the removal of the old key in 2
vantage points in the DNS eco
rollover process. Using this dat
These events include telemetry
postponed, a near real-time vie
and a significant increase in c
the old key was revoked. Our
identifying the causes of chall
We show that while from an e
passed without major problem
improvement and important lessons to be learned from events
that occurred over the entire duration of the rollover. Based on
the key, collected feedback from the community before the rollover.
Two risks were most feared: (i) resolvers that would not update their

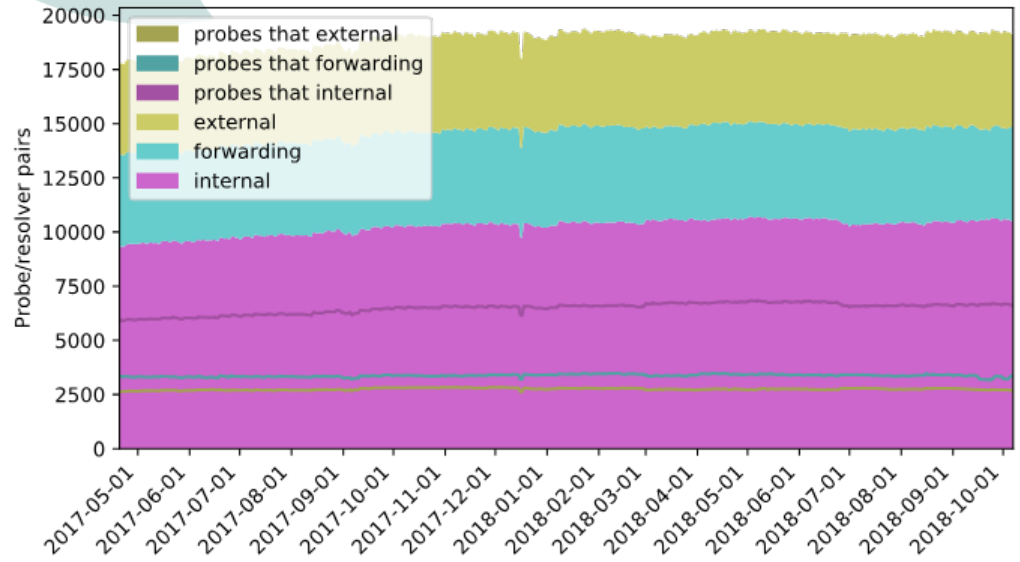
ABS

n ID
3670
3671

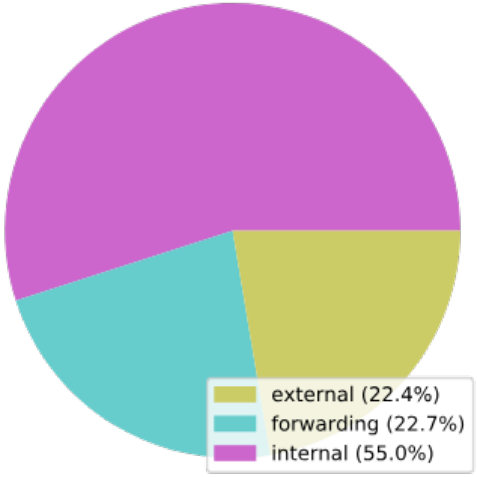
Willem Toorop
ught @ICANN69 18/41

1½ years of measurements
Internal, Forwarding & External

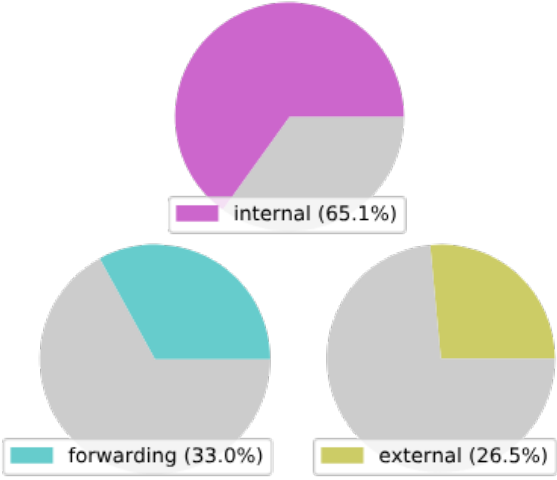
https://dnsthought.nlnetlabs.nl/#int_fwd_ext



with 19082 resolvers

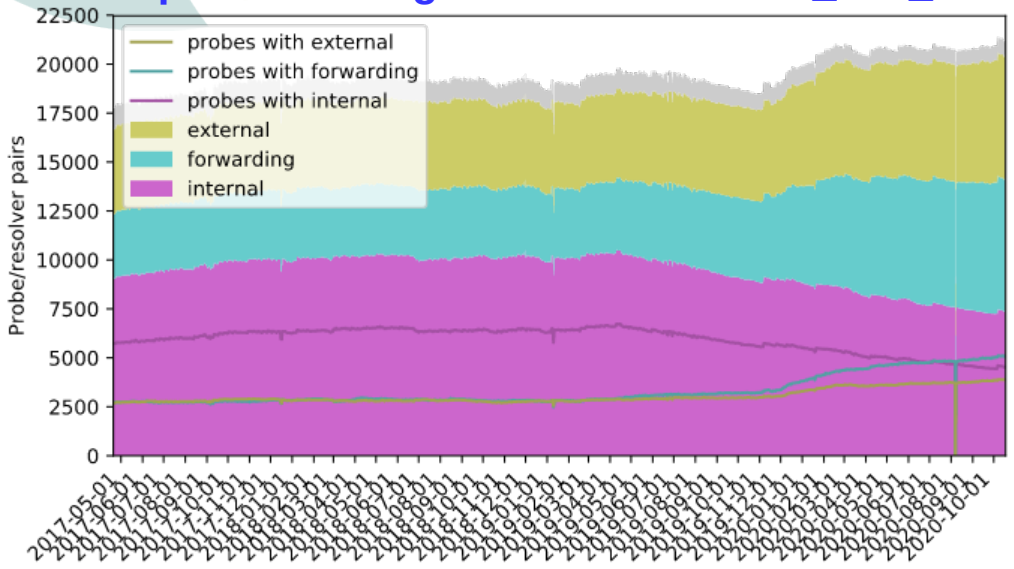


with 10155 probes

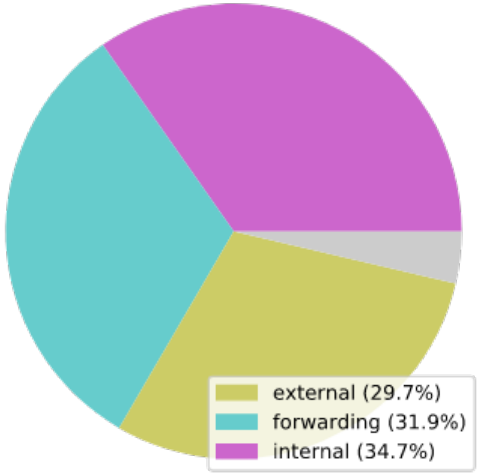


3½ years of measurements
Internal, Forwarding & External

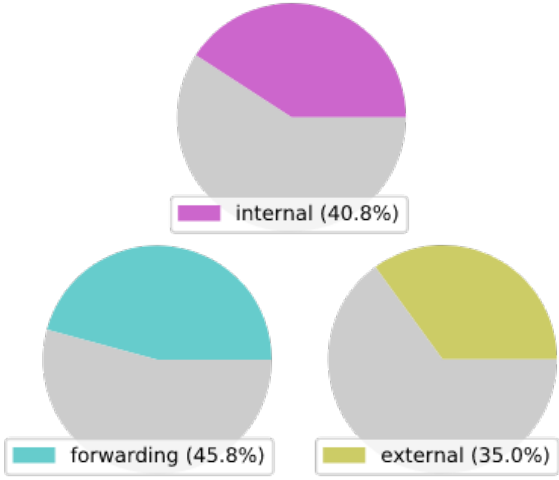
https://dnsthought.nlnetlabs.nl/#int_fwd_ext



with 21181 resolvers

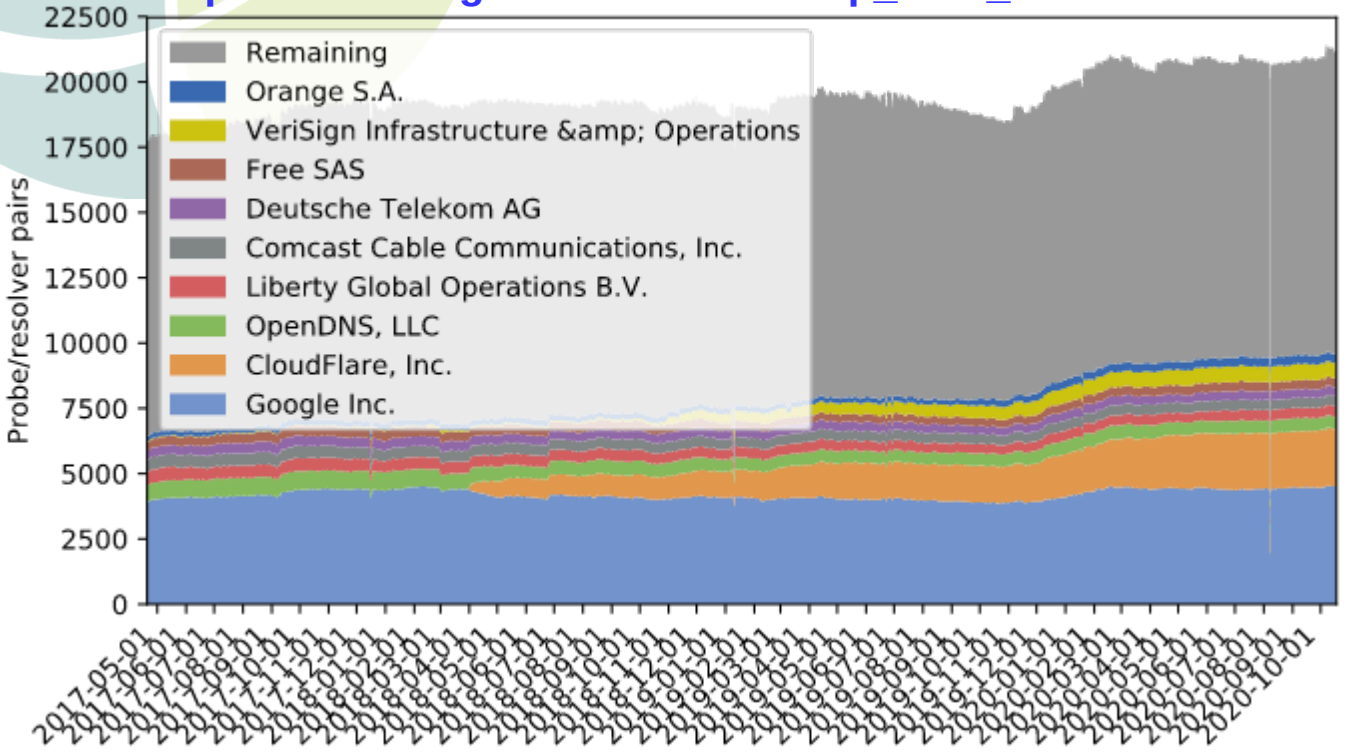


with 11095 probes

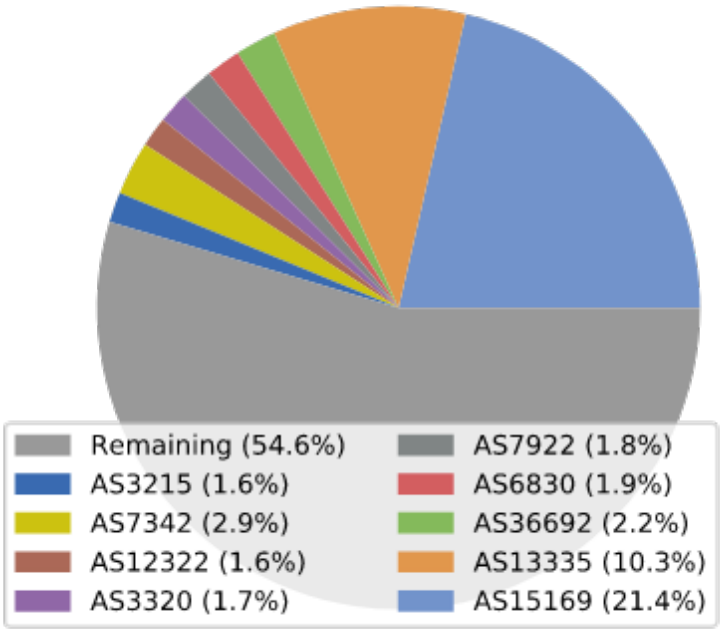


3½ years of measurements
Top 10 ASNs seen @ authoritative

https://dnsthought.nlnetlabs.nl/#top_auth_asns



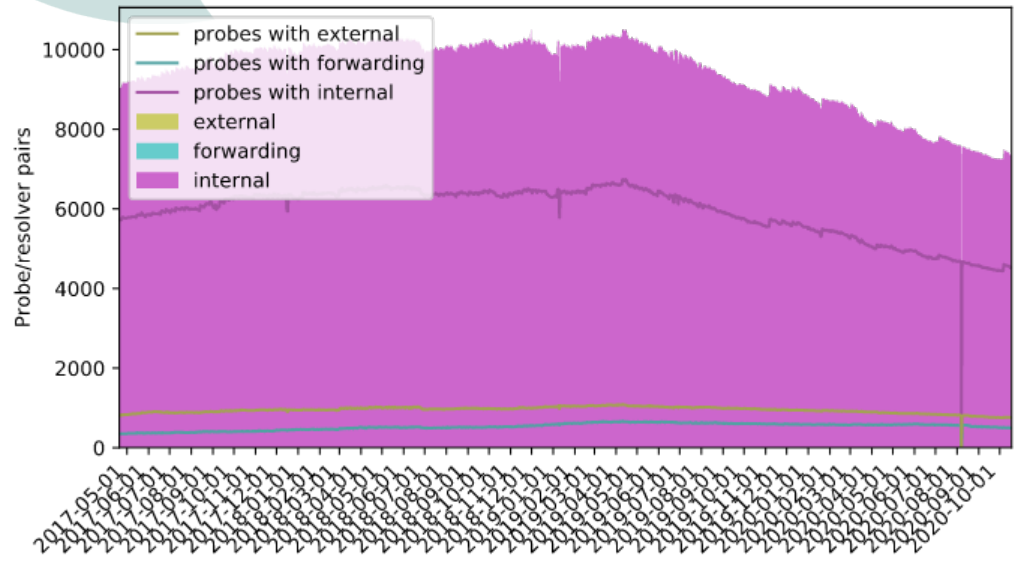
with 21181 resolvers



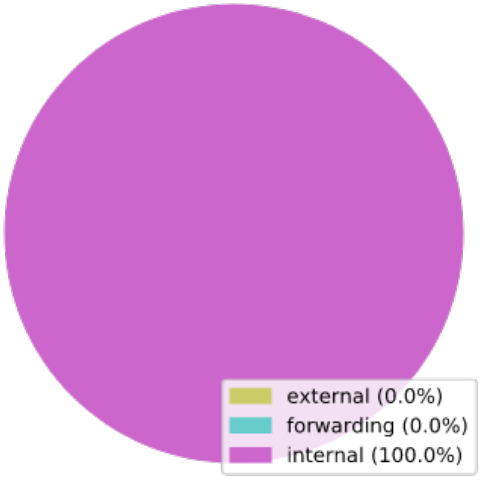
have the same ASN as the probe (internal)

https://dnsthought.nlnetlabs.nl/is_internal/#int_fwd_ext

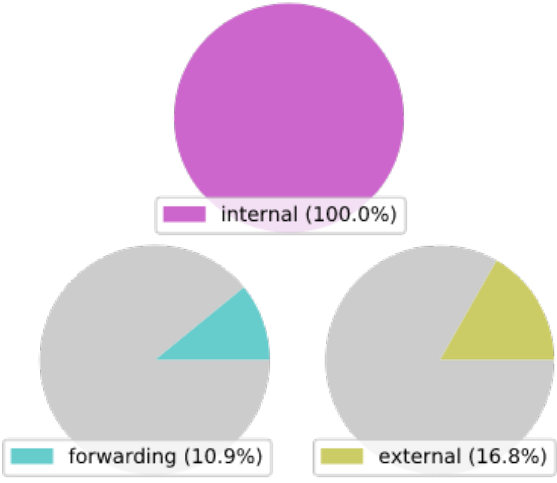
Internal



with 7358 resolvers



with 4530 probes

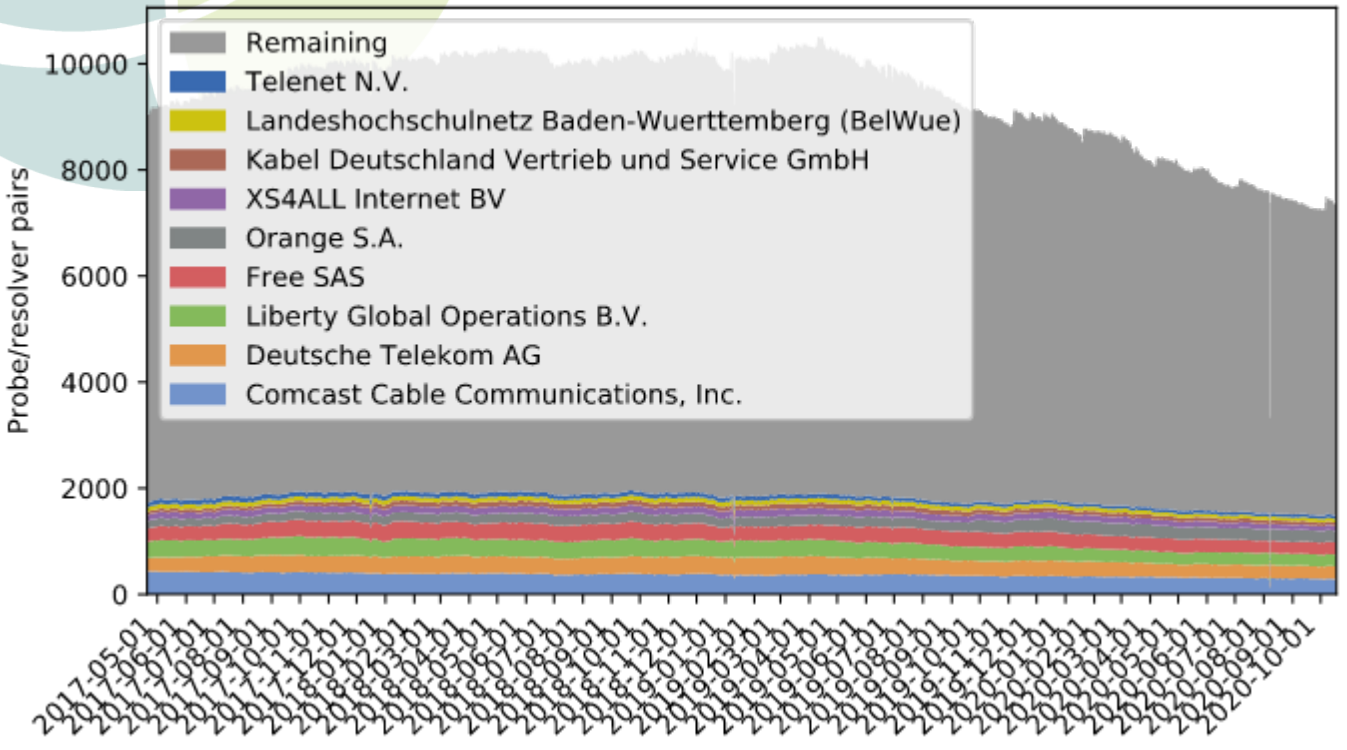


have the same ASN as the probe (internal)

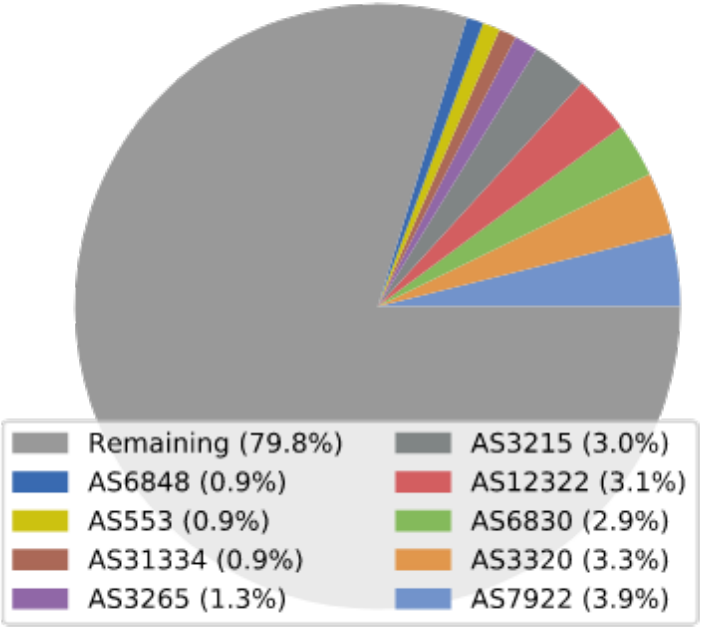
https://dnsthought.nlnetlabs.nl/is_internal/#top_auth_asns

Internal

Top 10 ASNs seen @ authoritative



with 7358 resolvers



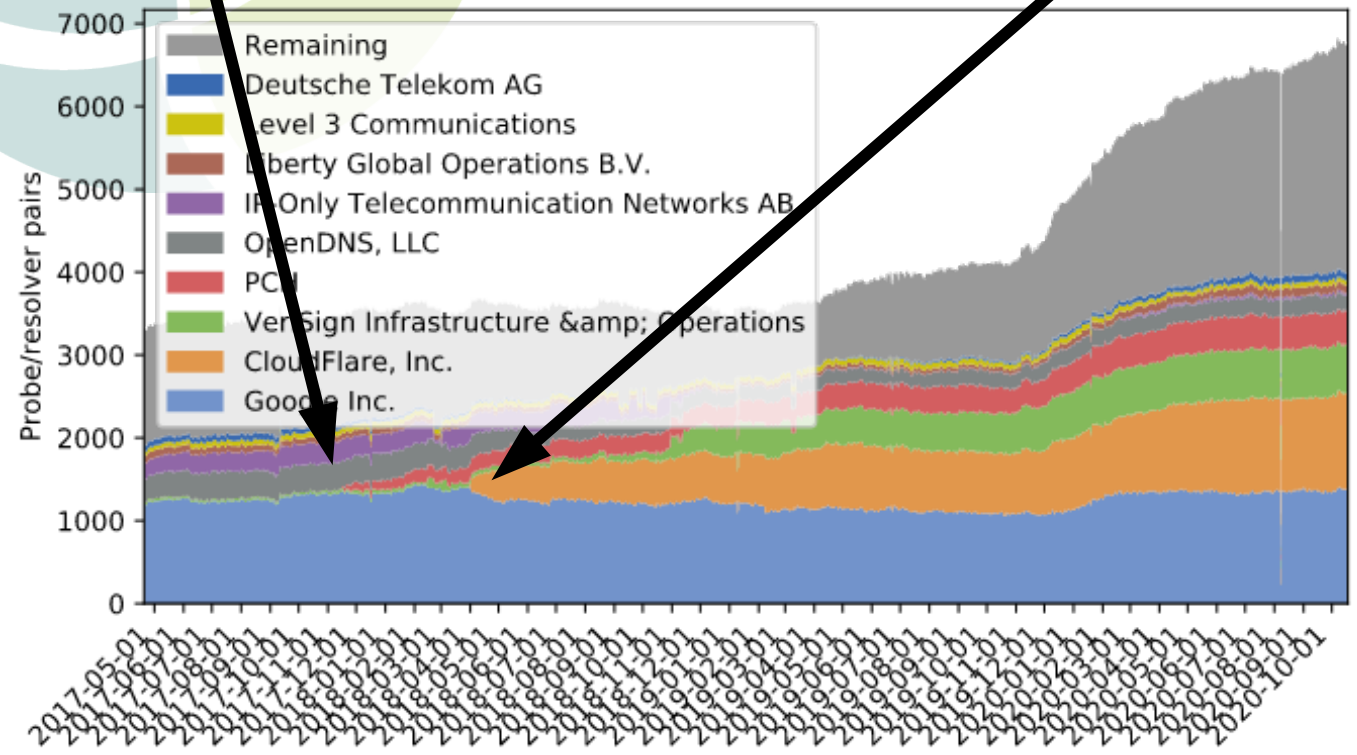
forwarding to a resolver with a different ASN
https://dnsthought.nlnetlabs.nl/is_forwarding/#top_auth_asns

Forwarding

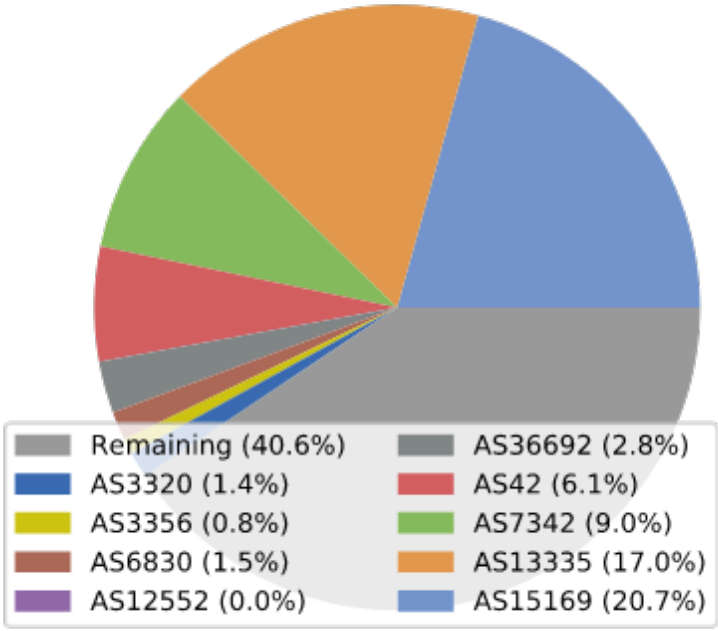
Top 10 ASNs seen @ authoritative

16 November '17
PCH = Quad9

1st April 2018 Cloudflare



with 6753 resolvers

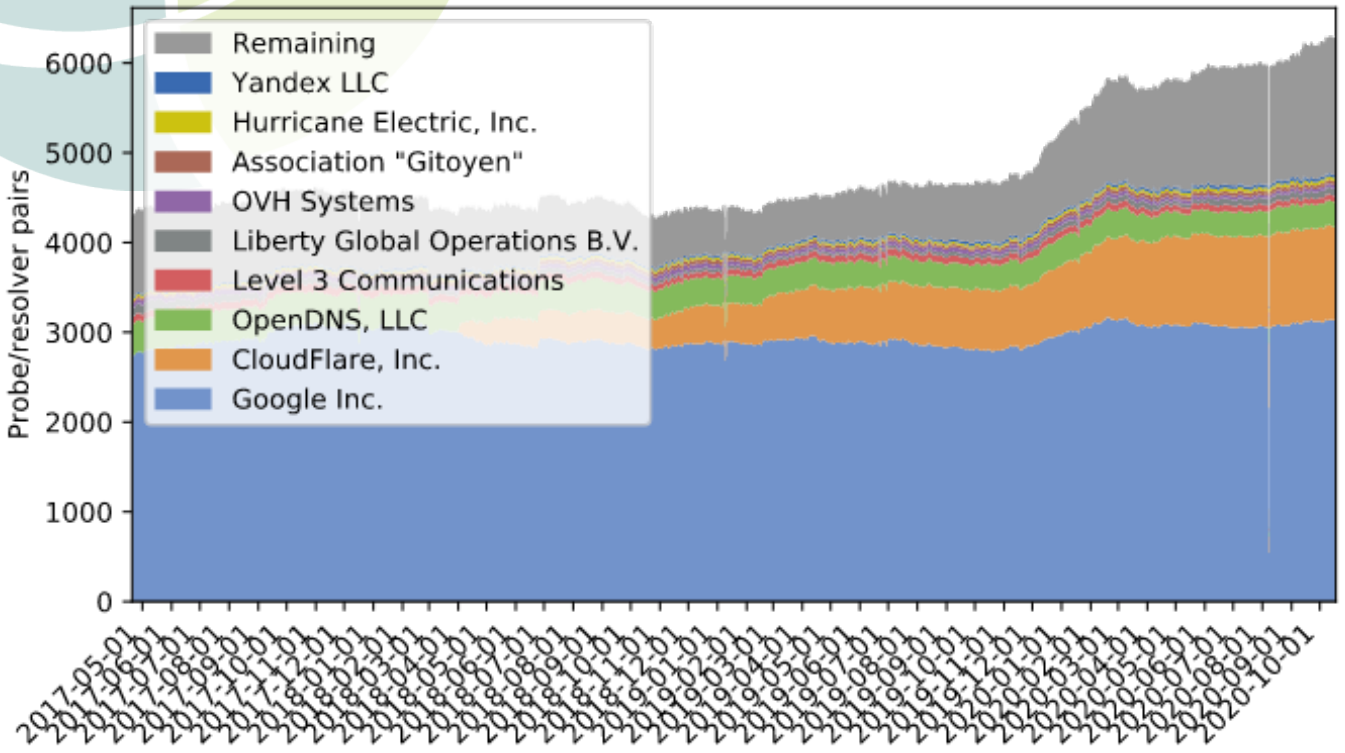


have a ASN different from the probe ASN

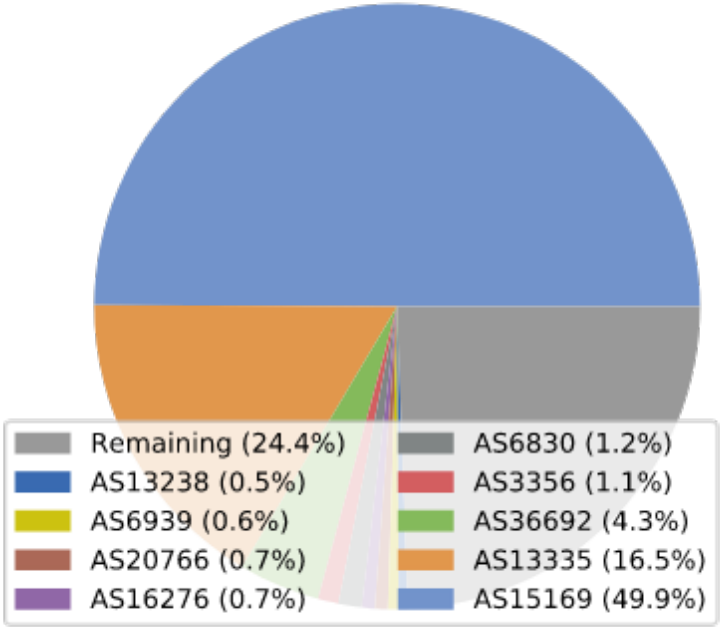
https://dnsthought.nlnetlabs.nl/is_external/#top_auth_asns

External

Top 10 ASNs seen @ authoritative



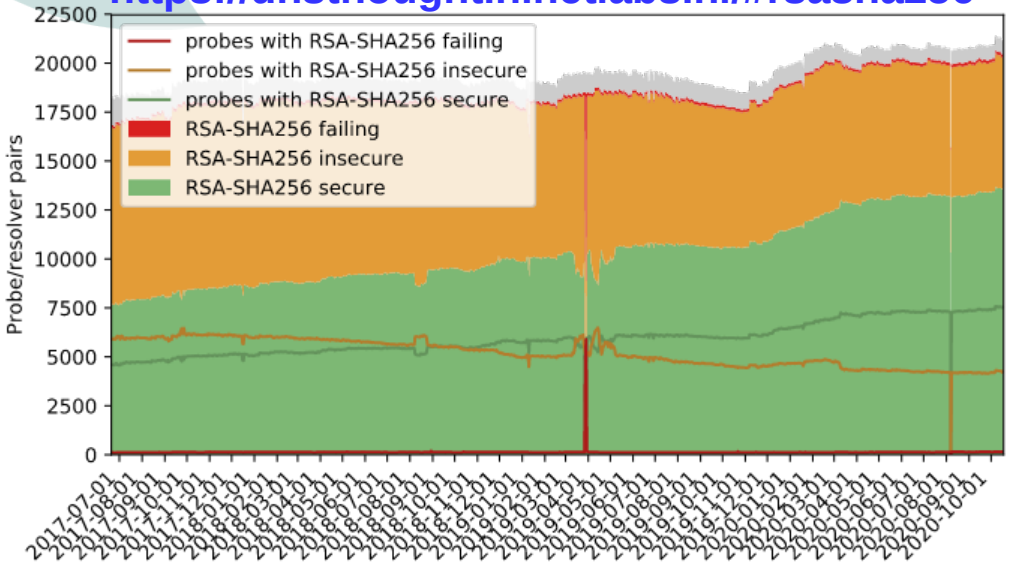
with 6291 resolvers



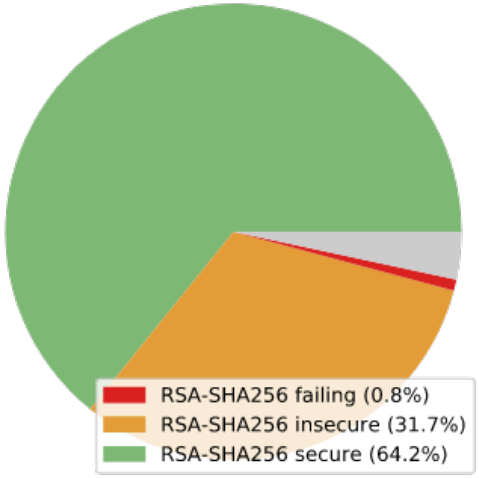
Internal, Forwarding, External

DNSSEC
RSA-SHA256 support

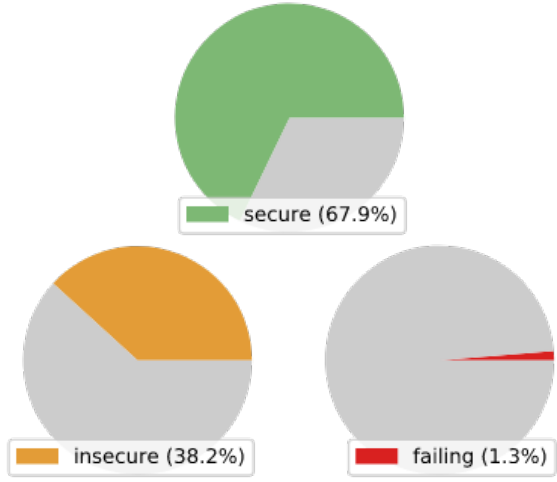
https://dnsthought.nlnetlabs.nl/#rsasha256



with 21181 resolvers



with 11095 probes

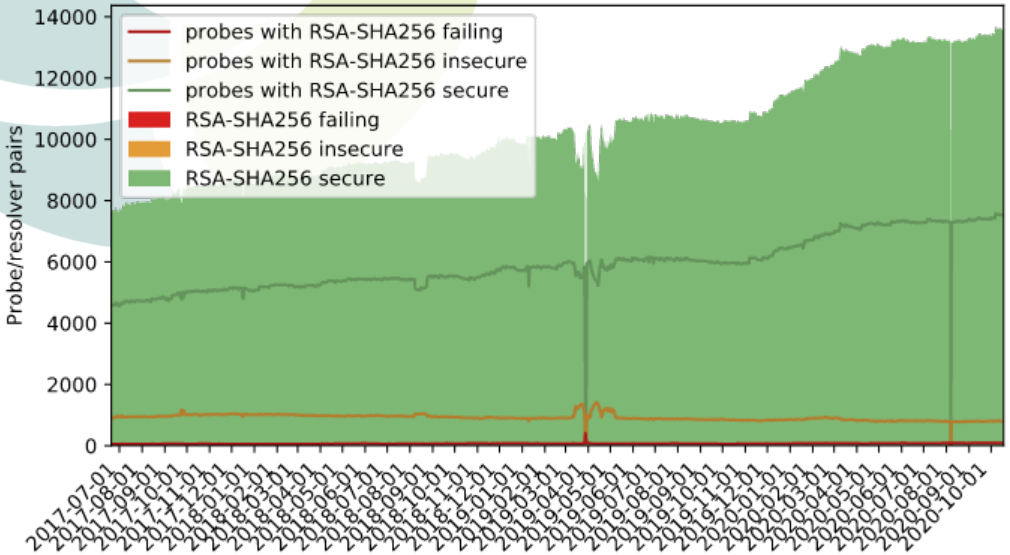


DNSSEC

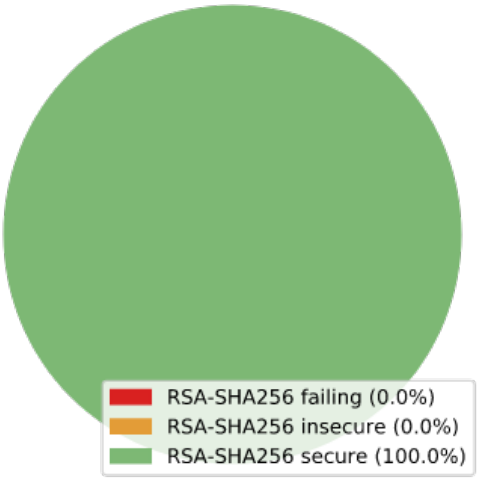
validate DNSKEY algorithm RSA-SHA256

https://dnsthought.nlnetlabs.nl/can_rsasha256/#rsasha256

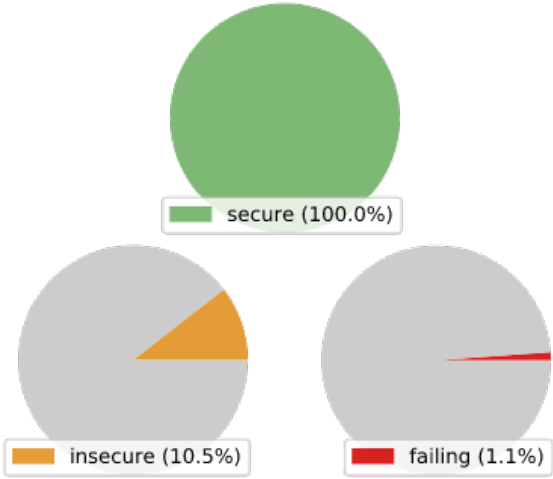
RSA-SHA256 support



with 13595 resolvers



with 7529 probes

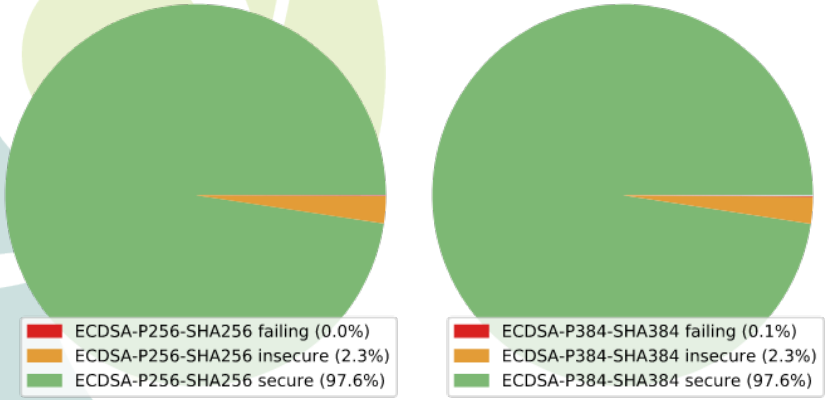


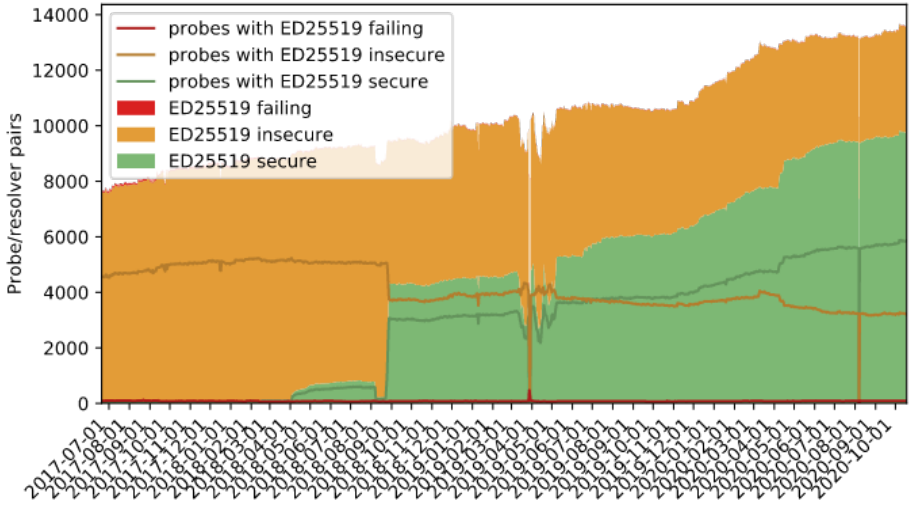
- 67.9% of probes has validating resolver
- 10.5% of those have a non validating resolver too
- So realistically only 60.77% of probes is protected

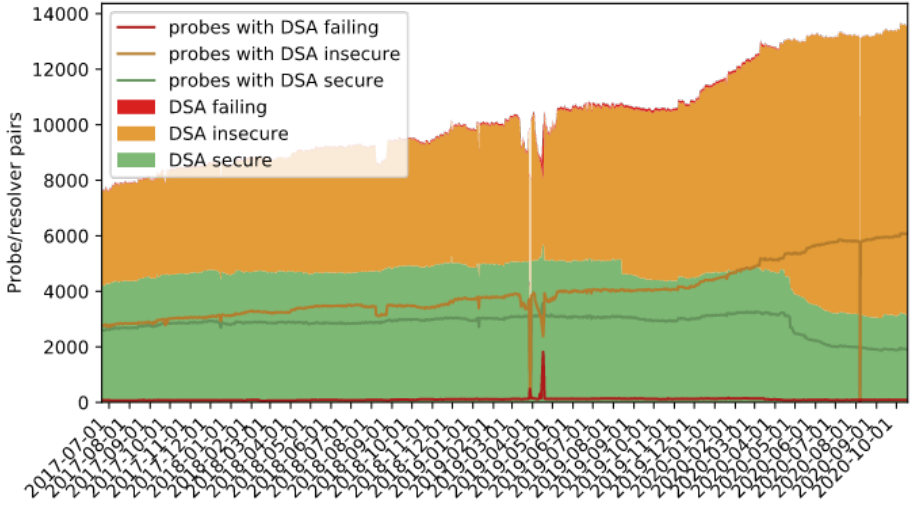
With DNSSEC validating resolvers

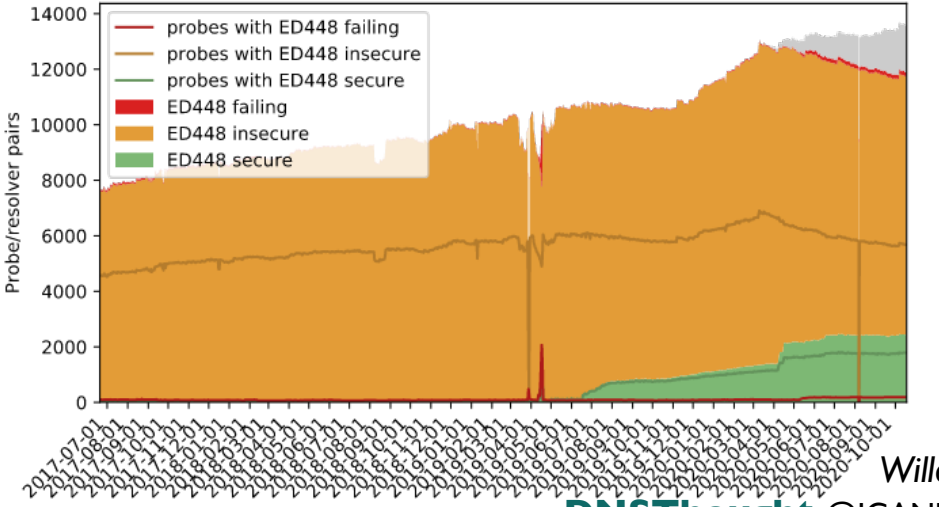
https://dnsthought.nlnetlabs.nl/can_rsasha256/#ed448

DNSSEC









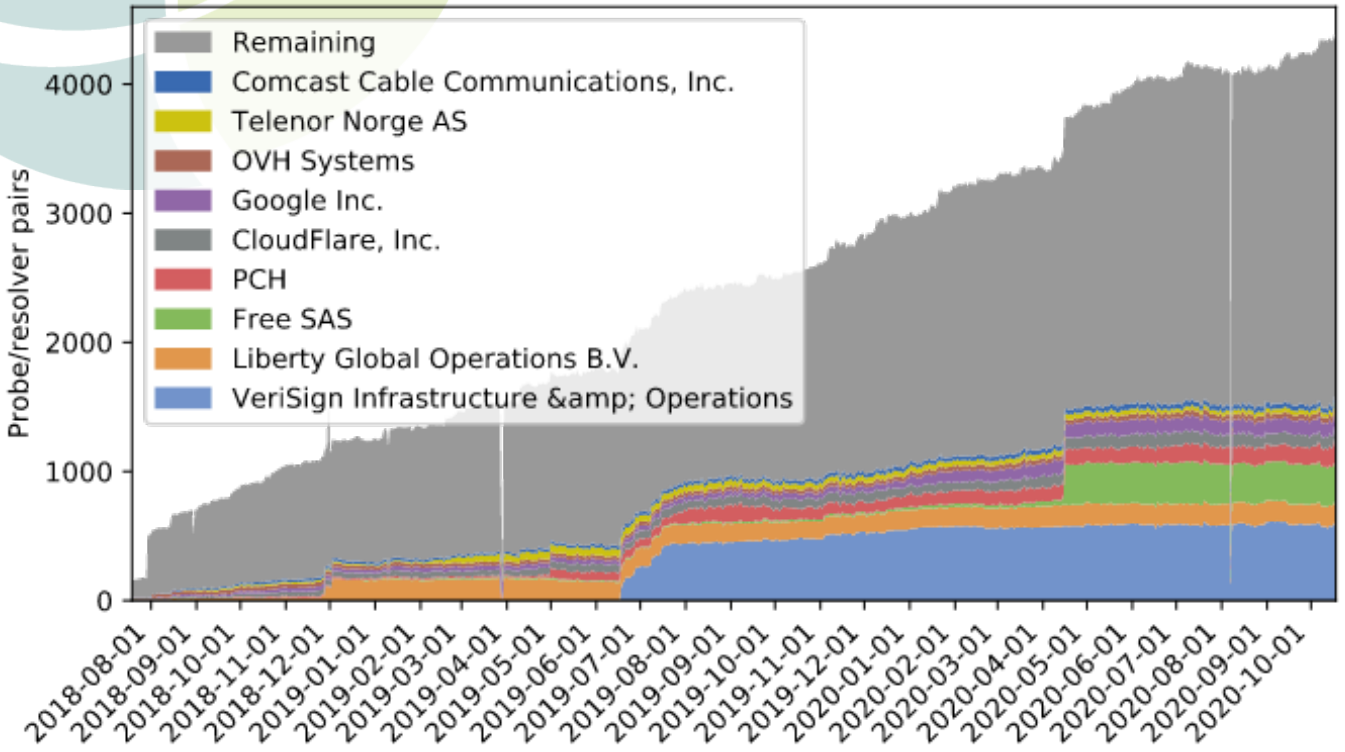
DNSSEC

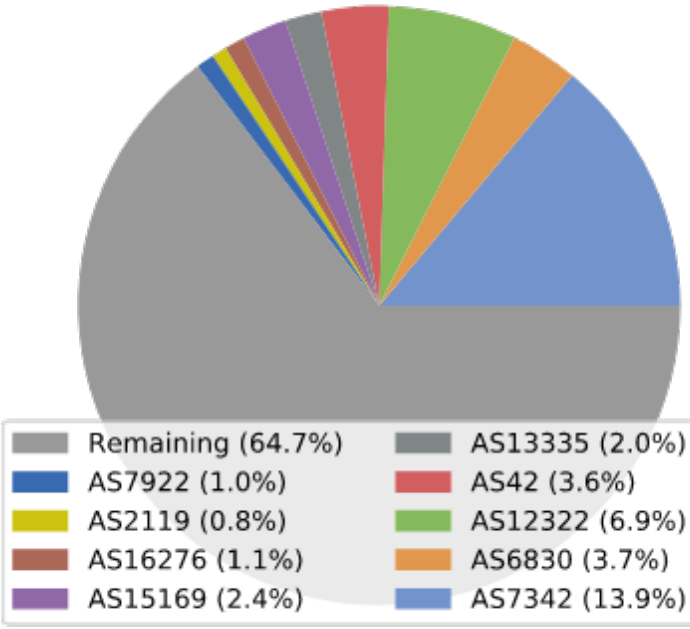
root KSK sentinel support

https://dnsthought.nlnetlabs.nl/has_ta_20326/#top_resolver_asns

Root Key Trust Anchor Sentinel

with 4344 resolvers
In 2654 probes





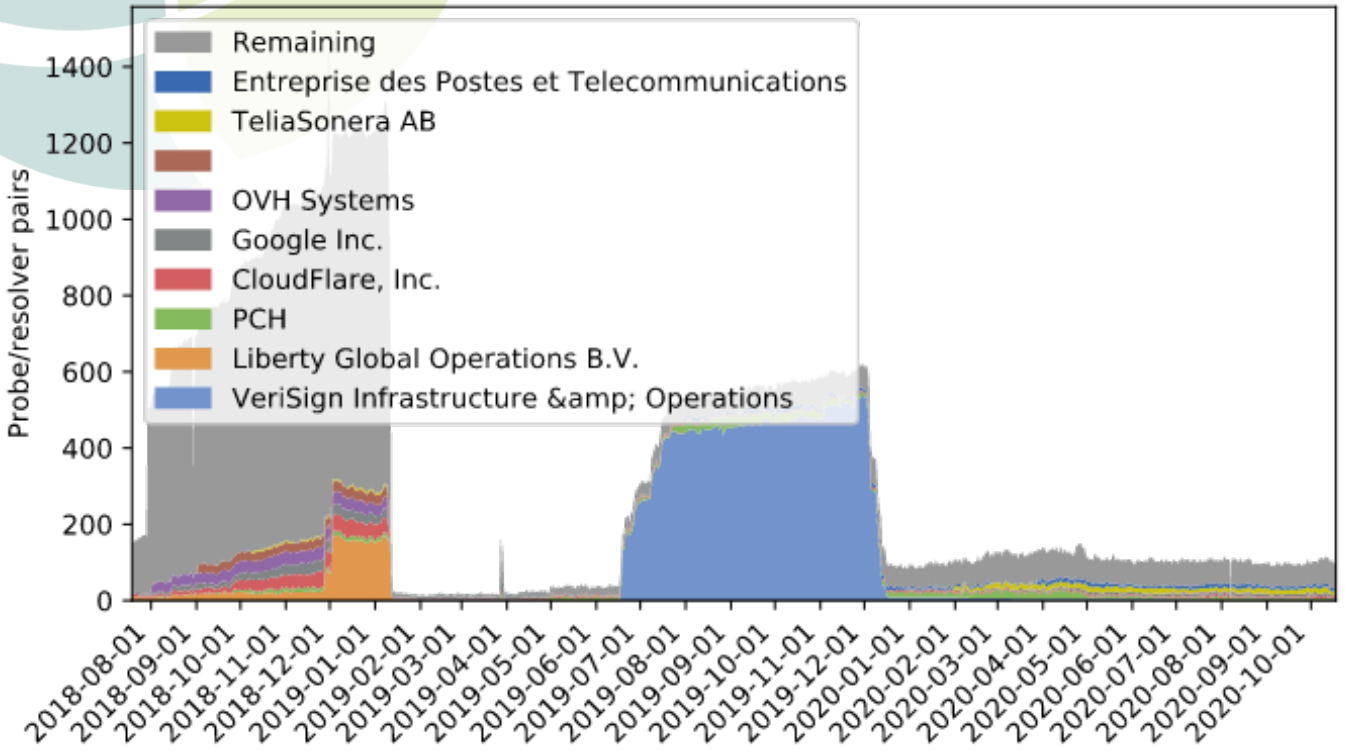
DNSSEC

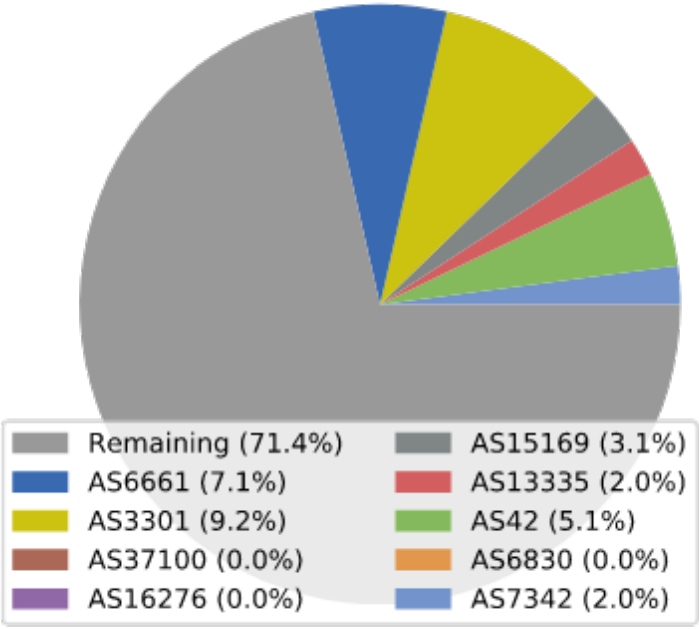
root KSK sentinel support

https://dnsthought.nlnetlabs.nl/has_ta_19036/#top_resolver_asns

Root Key Trust Anchor Sentinel

with 98 resolvers
In 74 probes





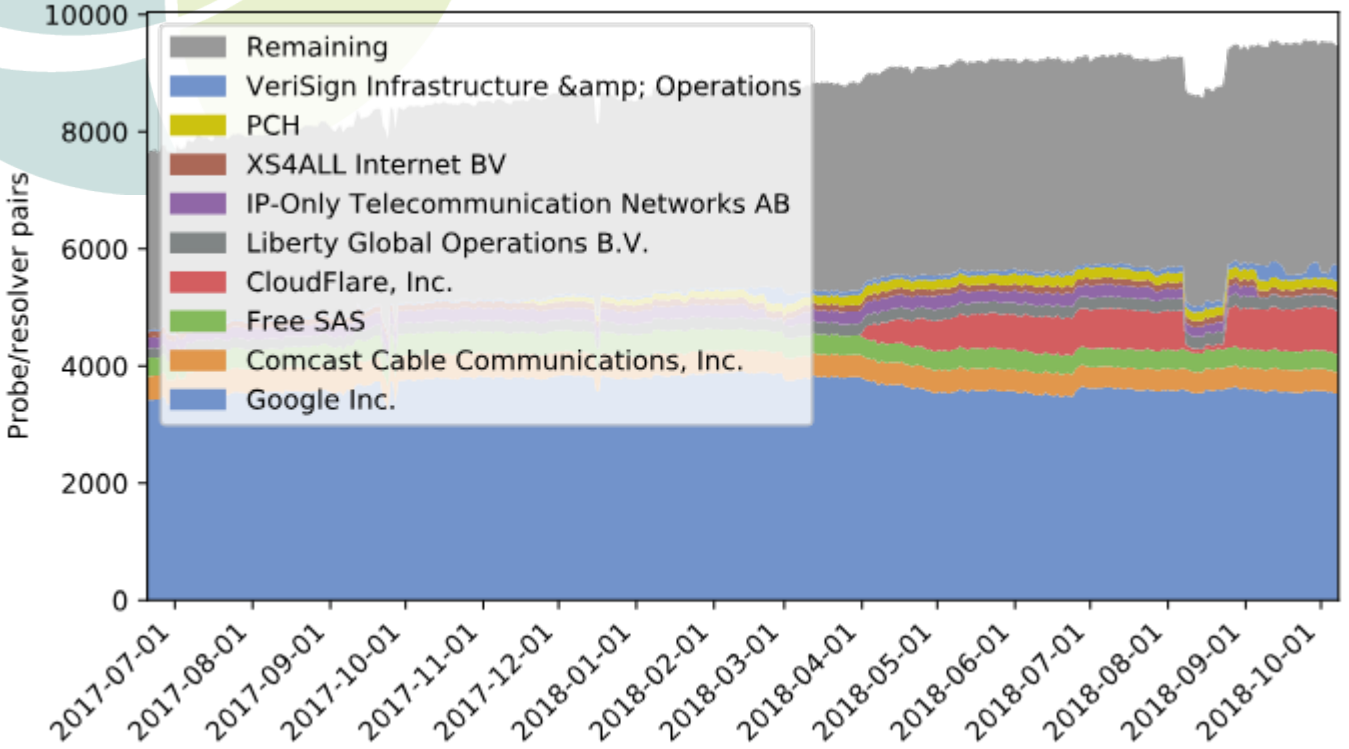
DNSSEC

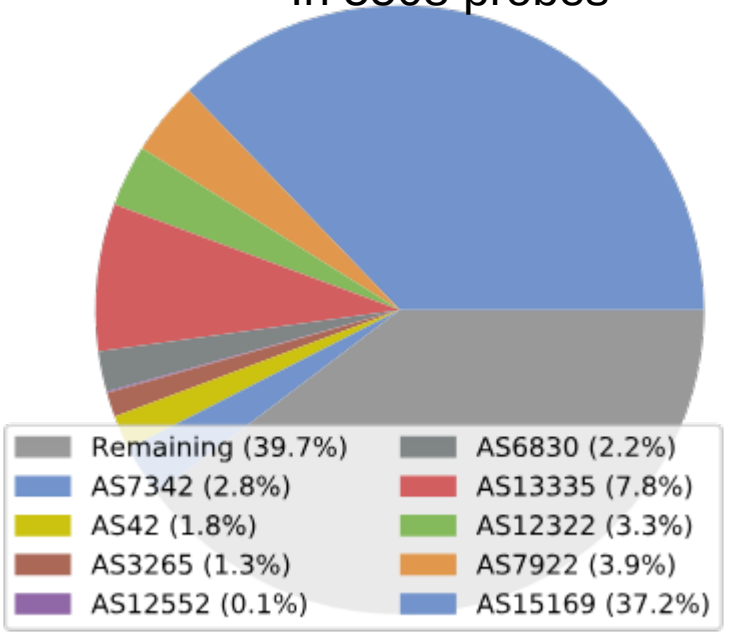
validate DNSKEY algorithm RSA-SHA256

https://dnsthought.nlnetlabs.nl/can_rsasha256/#top_auth_asns

Strange dent in August

with 9493 resolvers
In 5508 probes



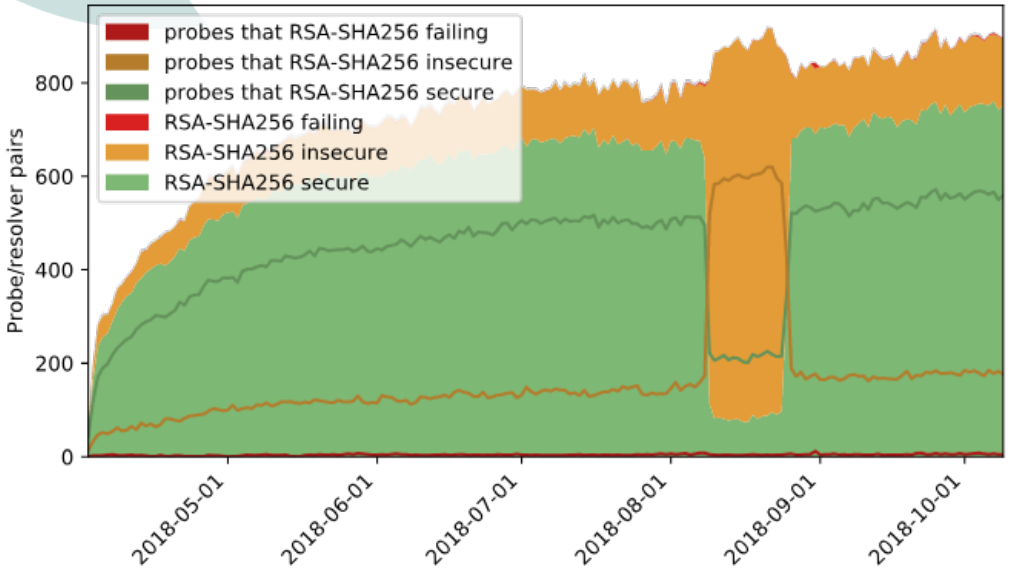


DNSSEC

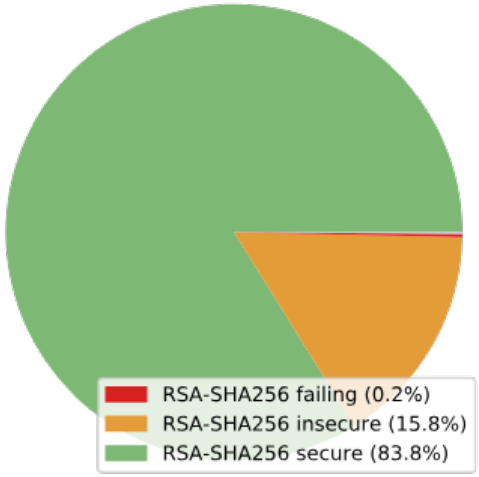
Strange dent in August

coming from AS13335

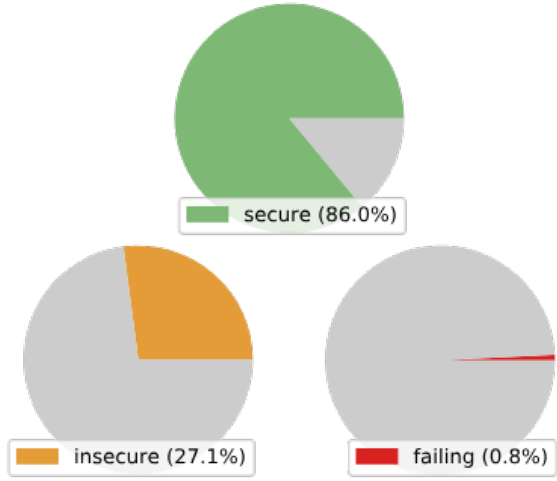
https://dnsthought.nlnetlabs.nl/auth_AS13335/#rsasha256



with 897 resolvers



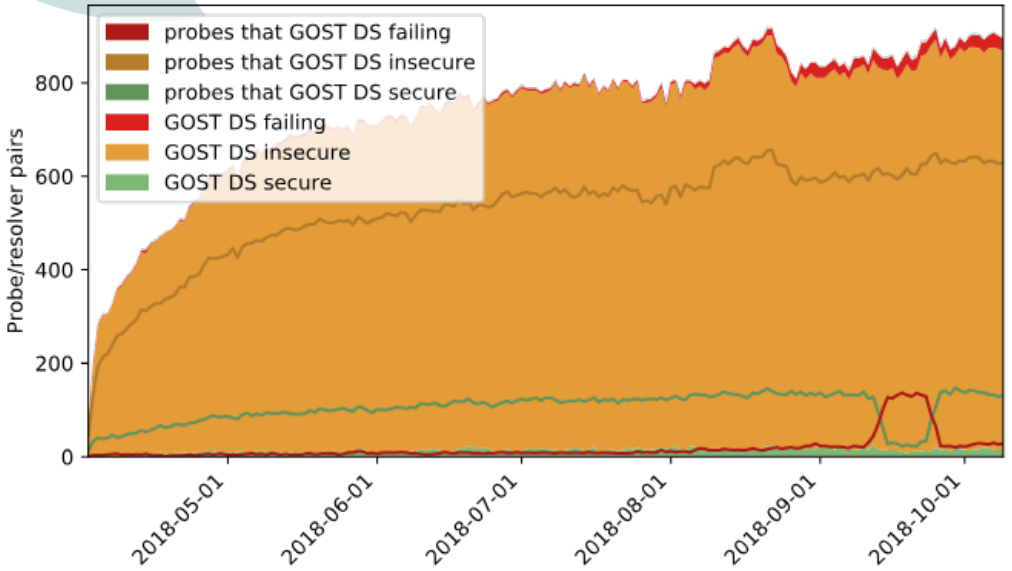
with 650 probes



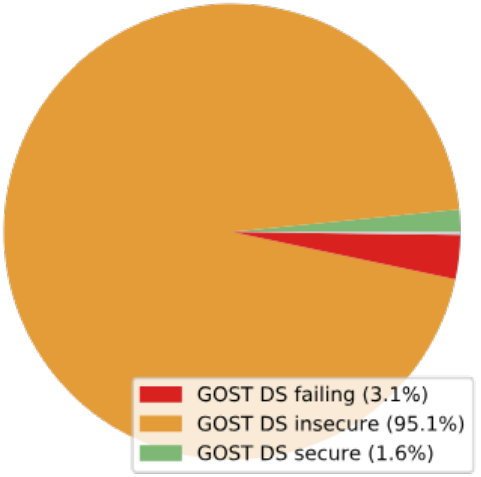
coming from AS13335

https://dnsthought.nlnetlabs.nl/auth_AS13335/#gost

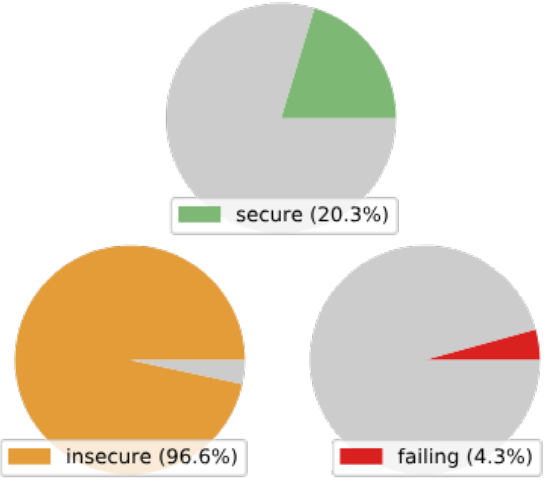
Strange broken GOST DS in September



with 897 resolvers



with 650 probes

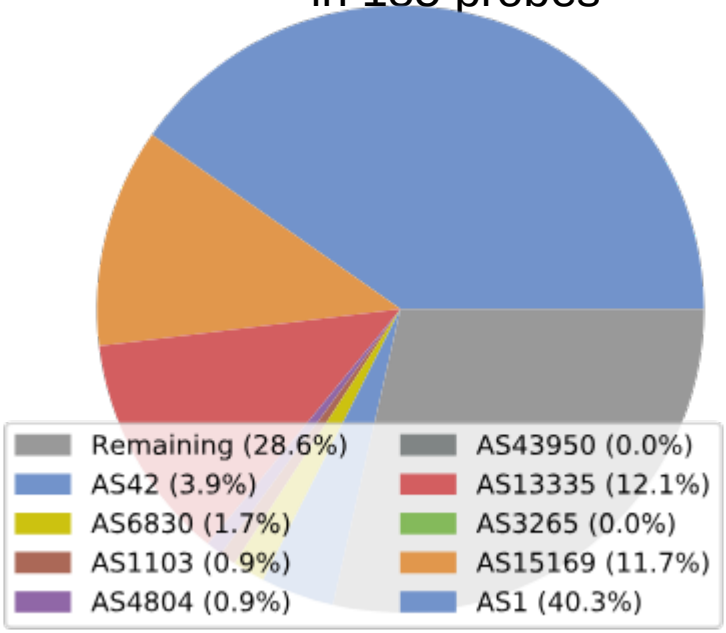


broken DS algorithm GOST validation support

https://dnsthought.nlnetlabs.nl/broken_gost/#top_auth_asns

Strange broken GOST DS in September

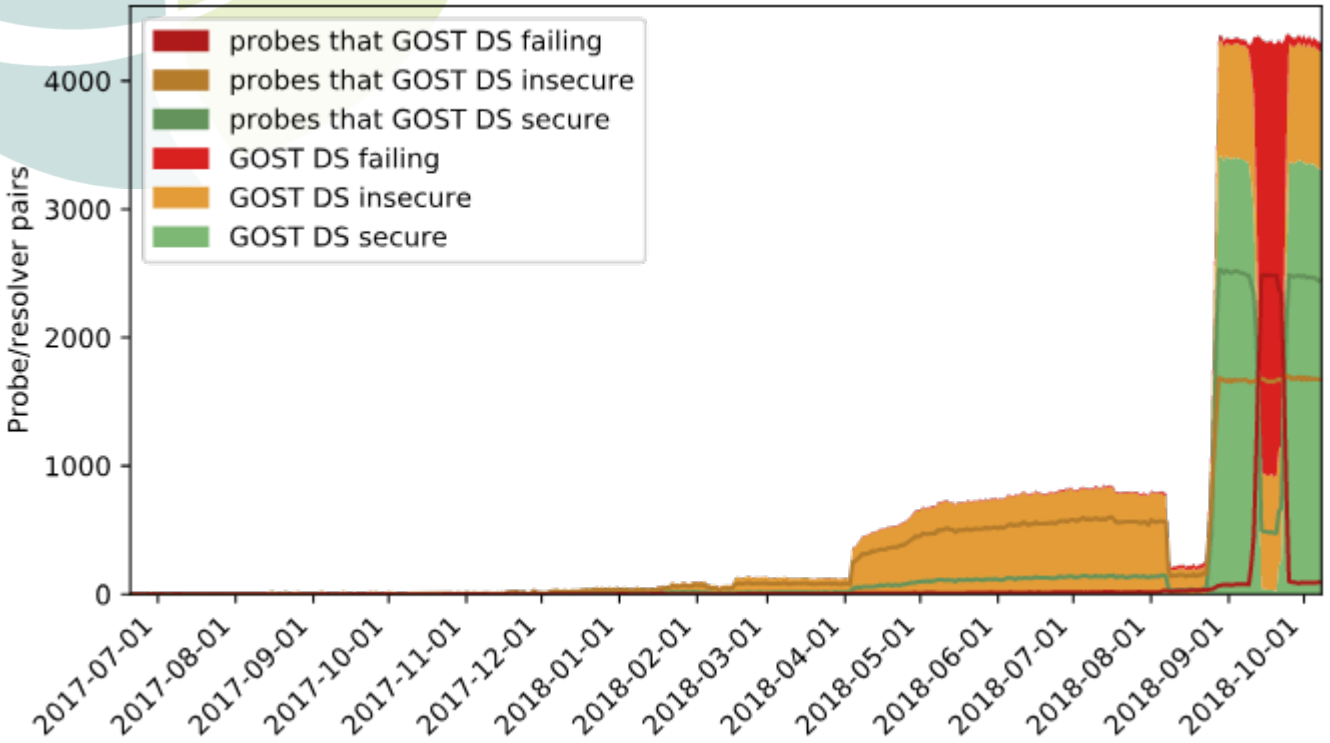
with 231 resolvers
in 185 probes



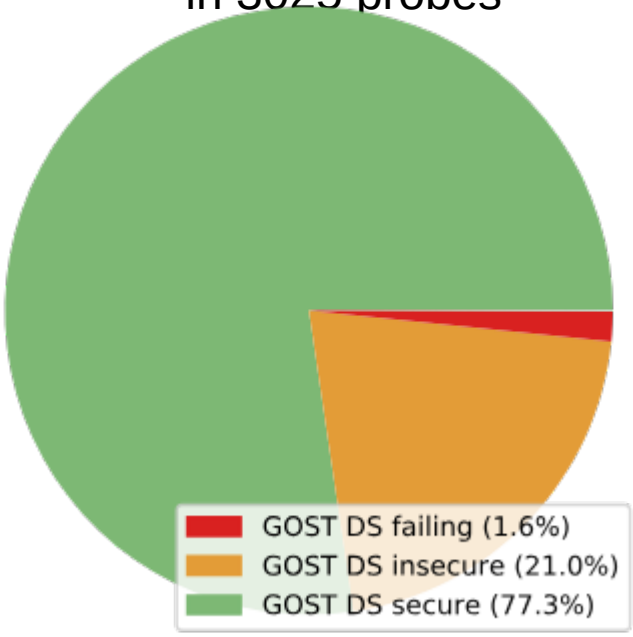
validate DNSKEY algorithm ED25519
https://dnsthought.nlnetlabs.nl/can_ed25519/#gost

DNSSEC

The two incidents side by side



with 4304 resolvers
in 3025 probes

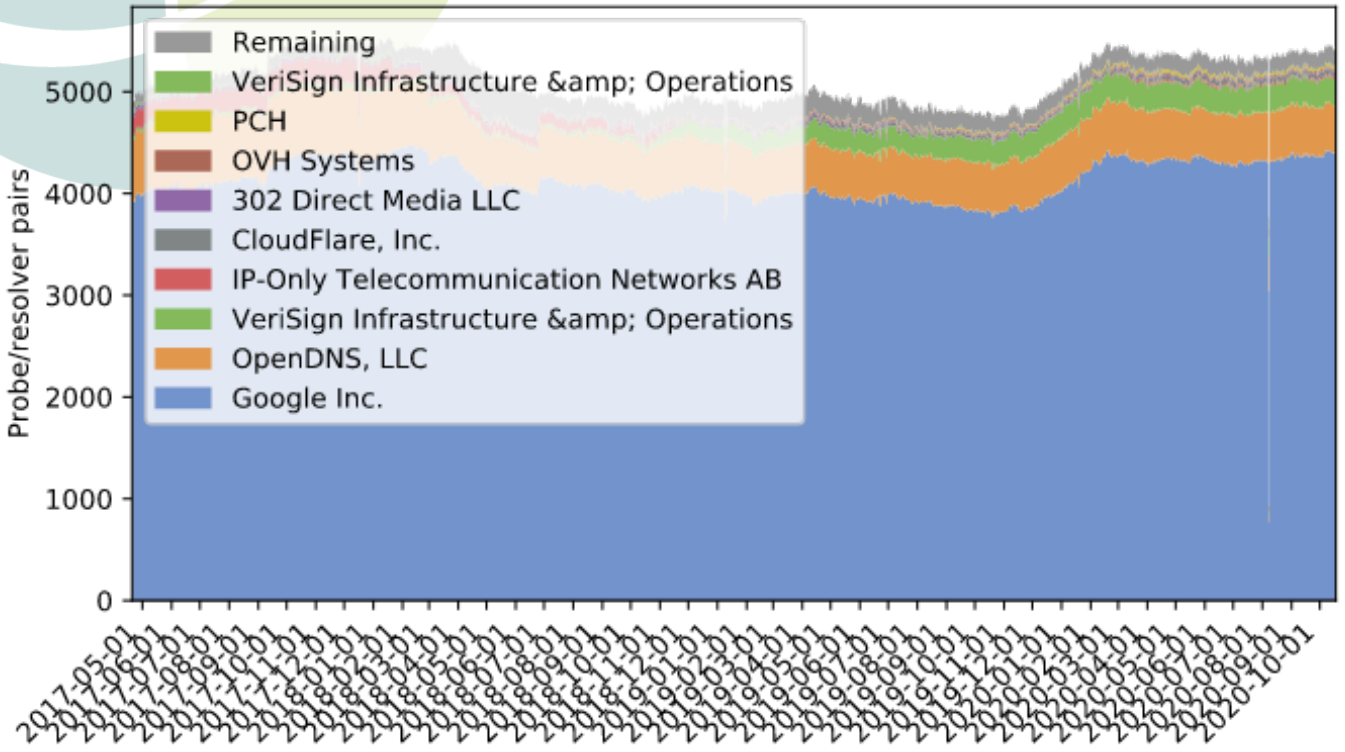


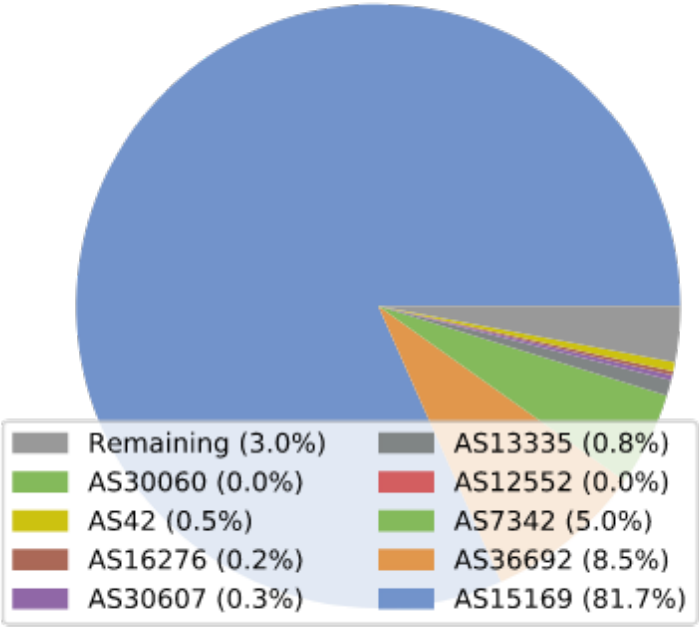
send an EDNS Client Subnet option
https://dnsthought.nlnetlabs.nl/does_ecs/#top_auth_asns

Privacy

Send an EDNS Client Subnet option

With 5417 (25.6%) resolvers
in 3720 (33.5%) probes

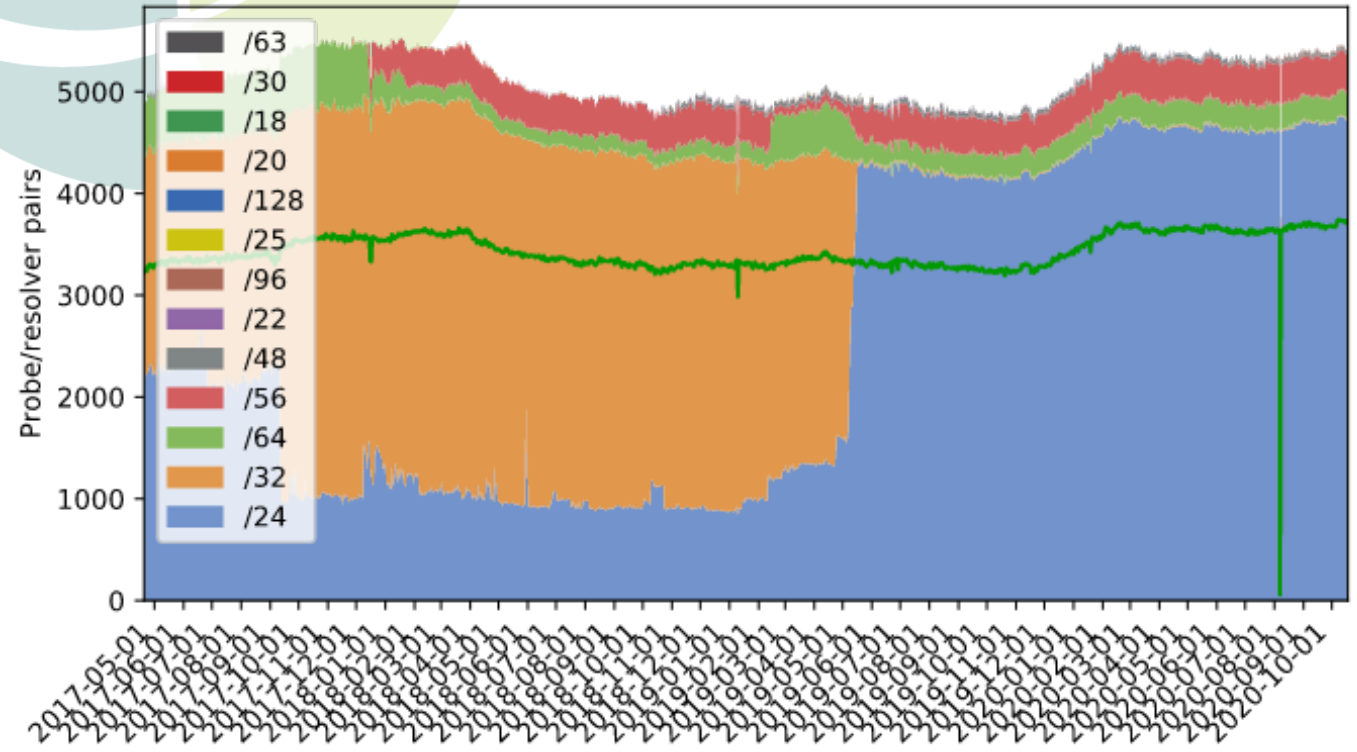




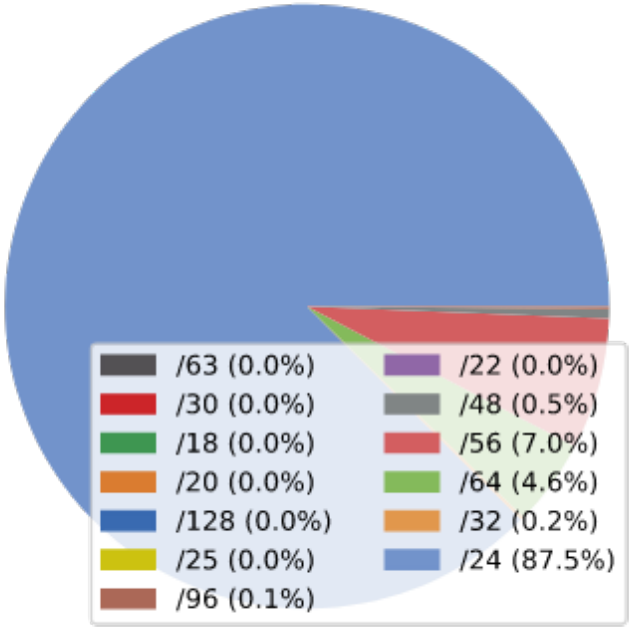
Privacy

Send an EDNS Client Subnet option

Top EDNS Client Subnet masks
https://dnsthought.nlnetlabs.nl/does_ecs/#ecs_masks



With 5417 (25.6%) resolvers
in 3720 (33.5%) probes

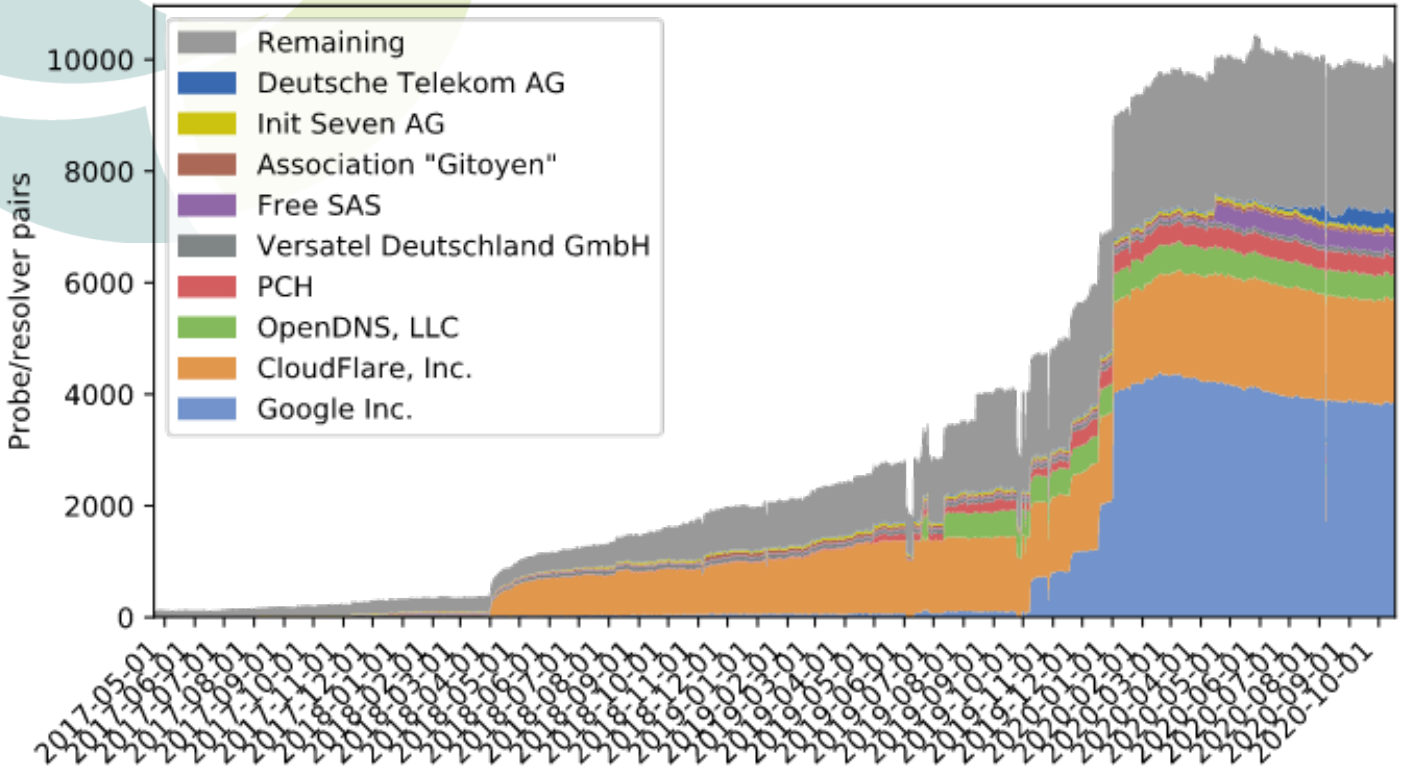


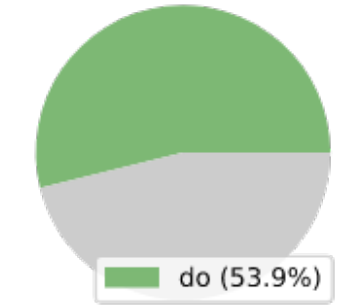
do QNAME Minimization

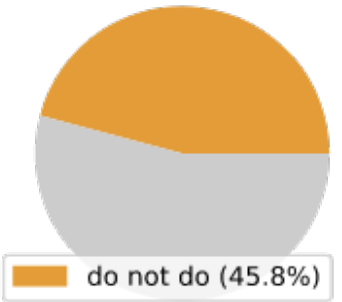
https://dnsthought.nlnetlabs.nl/does_qnamemin/#top_auth_asns

Privacy QNAME Minimization

With 9971 (8.5%) resolvers in 5976 (11.2%) probes







do QNAME Minimization

h

Privacy

inimization

olvers in 5976 (11.2%) probes

A First Look at QNAME Minimization in the Domain Name System

Wouter B. de Vries[1], Quirin Scheitle[2], Moritz Müller[1,3], Willem Toorop[4], Ralph Dolmans[4], Roland van Rijswijk-Deij[1,4]

[1]University of Twente, [2]TUM, [3]SIDN Labs, [4]NLnet L

Abstract. The Domain Name System (DNS) is a critical part
and Internet infrastructure; DNS lookups precede almost any u
DNS lookups may contain private information about the sites a
a user contacts, which has spawned efforts to protect privacy of
as transport encryption through DNS-over-TLS or DNS-over
In this work, we provide a first look on the resolver-side techniq
name minimization (*qmin*), which was standardized in Mar
RFC 7816. *qmin* aims to only send minimal information to au
name servers, reducing the number of servers that full DNS qu
are exposed to. Using passive and active measurements, we s
but steady adoption of *qmin* on the Internet, with a surpris
in implementations of the standard. Using controlled experi
test-bed, we validate lookup behavior of various resolvers, ar
that *qmin* both increases the number of DNS lookups by up t
also leads to up to 5% more failed lookups. We conclude our
a discussion of *qmin*'s risks and benefits, and give advice for

Keywords: DNS · Privacy · QNAME Minimization · Measu

1 Introduction

Willem Toorop

DNSThought

- Public, though rough, interface to data available
  https://dnsthought.nlnetlabs.nl/
- ATLAS msm ids & raw processed data available too
  https://dnsthought.nlnetlabs.nl/raw
- Wish list:
  - Auth IP from the measured property
  - Results in time series database
  - Interactive UI (zooming)
  - Better DS algorithm detection
  - Msms for: RTT, PMTU, DoT/DoH, DNS Cookies, etc. etc. etc.

Questions
Suggestions