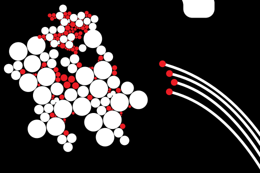
UNIVERSITY OF TWENTE.

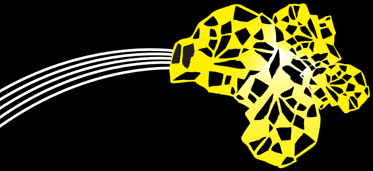
SURF NET



DNSSEC and its potential for DDoS attacks

a comprehensive measurement study

Roland van Rijswijk-Deij, *Anna Sperotto*, *Aiko Pras*

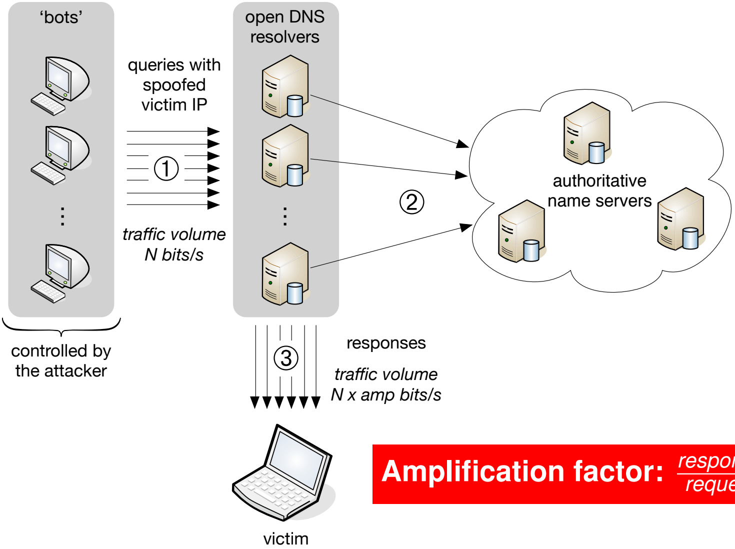


Background to this study

- SURFnet pioneered DNSSEC in the Netherlands
  - First major network operator to deploy validation (2009)
  - First signed `.nl` delegation (2010)
  - Hands-on guides, HOWTO's, blogging, . . .
- If you're the first, you are also the first to run into problems:
  - Issue #1: fragmentation (subject of another study[1])
  - Issue #2: abuse of signed domains for amplification attacks (2012) ← **the reason for this study**

[1] G. van den Broek et al. "DNSSEC Meets Real World: Dealing with Unreachability Caused by Fragmentation". In: *IEEE Communications Magazine* 52.4 (2014), pp. 154–160.

DNS amplification



'bots'

queries with spoofed victim IP

①

traffic volume N bits/s

controlled by the attacker

open DNS resolvers

②

authoritative name servers

③

responses

traffic volume N x amp bits/s

victim

Amplification factor: $\frac{\textit{response size}}{\textit{request size}}$

DNSSEC

- Goal: add authenticity and integrity to DNS
- Solution: add digital signatures to DNS
- Problem: DNSSEC makes DNS responses much bigger
- Critics of DNSSEC, e.g. Dan Bernstein[2]:

  “DNSSEC is a remote-controlled double-barreled shotgun, the worst DDoS amplifier on the Internet.”

- Intuitively, that is true, but… *How bad is it really?*

[2] D.J. Bernstein. “High-speed high-security cryptography: encrypting and authenticating the whole Internet”. In: *27th Chaos Communication Congress (27C3)*. Berlin, 2010. URL: `http://cr.yp.to/talks/2010.12.28/slides.pdf`.

Time to establish some…

100% ALL NATURAL ORGANIC

GROUND TRUTH

NET WT. 80 OZ (5LB)

MADE FROM INTERNATIONALLY RENOWNED TOP-LEVEL DOMAINS

Source data

- Source data comes from six major TLDs

  `.com`, `.net`, `.org`, `.uk`, `.se`, `.nl`
- In total, over 156 million domains
  - 57.5% of all domains on the Internet[3]*
- Almost 2.5 million DNSSEC-signed domains*
- Around 70% of all signed domains*
- **Goal:**

  measure amplification for all signed domains and for a random sample of the same size of unsigned domains

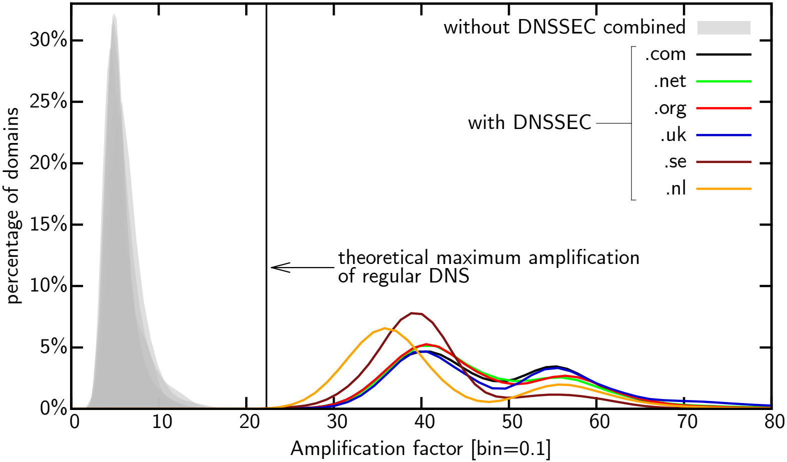
**at the time of the study in 2014*

[3] Verisign. *The Domain Name Industry Brief (Vol. 11, Iss. 1)*. Tech. rep. 2014. URL: `https://www.verisigninc.com/assets/domain-name-report-april2014.pdf`.

Measurements

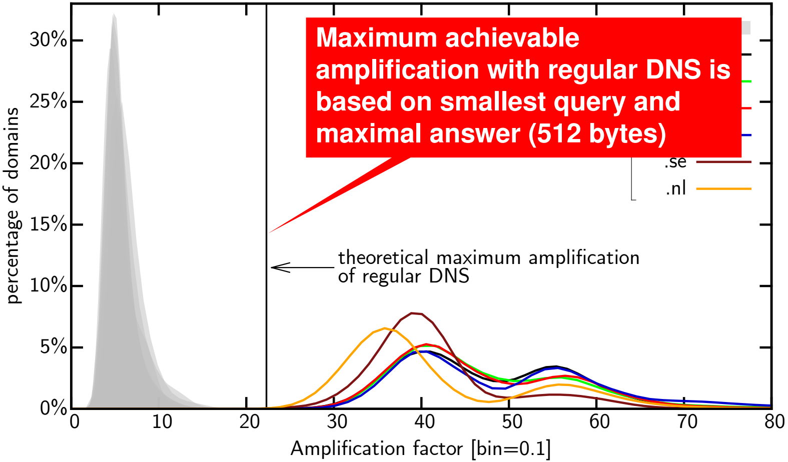
- For each domain:
  - Determine set of authoritative name servers
  - Send a set of queries to each IPv4 and IPv6 address of each authoritative name server
- Query types:
  - `ANY` – abused most for attacks
  - `TXT` – seen in 'crafted' domains
  - `MX`, `NS` – answers may be larger
  - `A`, `AAAA` – most common queries
  - `DNSKEY`, `NSEC(3)` – DNSSEC specific
- We measured:
  - Query and response size → **amplification**
  - Number of answers, authority and additional records
  - Some other data, e.g. number of different record types

ANY queries



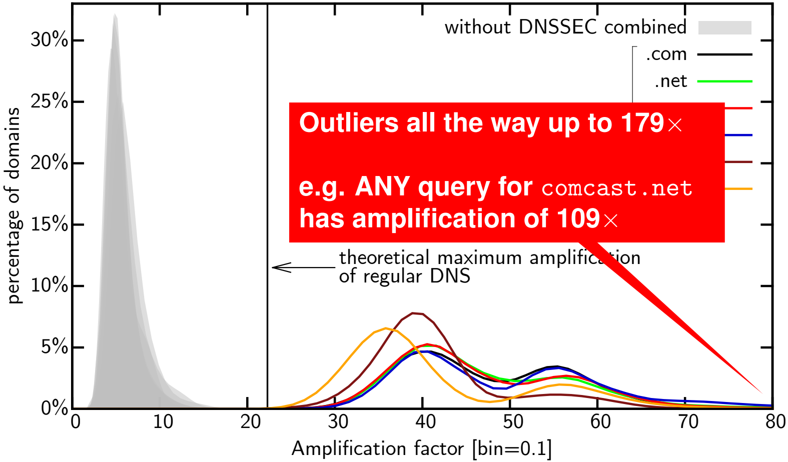
without DNSSEC combined
with DNSSEC
.com
.net
.org
.uk
.se
.nl
theoretical maximum amplification of regular DNS
percentage of domains
0%
5%
10%
15%
20%
25%
30%
0
10
20
30
40
50
60
70
80
Amplification factor [bin=0.1]

ANY queries



Maximum achievable amplification with regular DNS is based on smallest query and maximal answer (512 bytes)

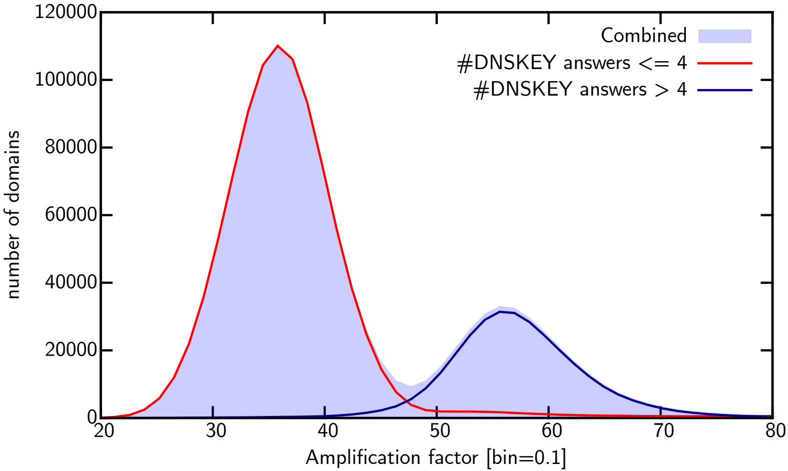
ANY queries



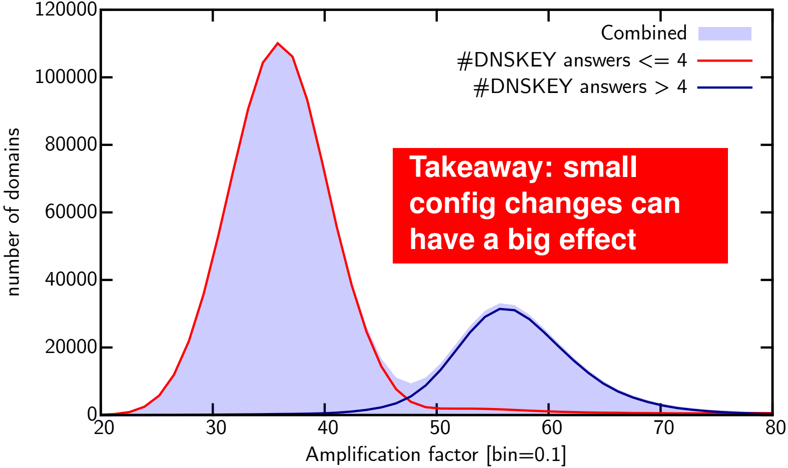
Outliers all the way up to 179×

e.g. ANY query for `comcast.net` has amplification of 109×

Twin Peaks

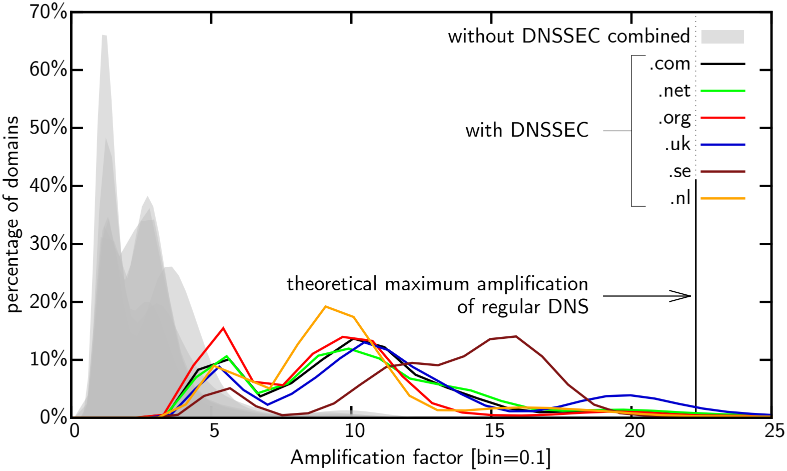

Combined
#DNSKEY answers <= 4
#DNSKEY answers > 4
number of domains
120000
100000
80000
60000
40000
20000
0
20
30
40
50
60
70
80
Amplification factor [bin=0.1]

Twin Peaks



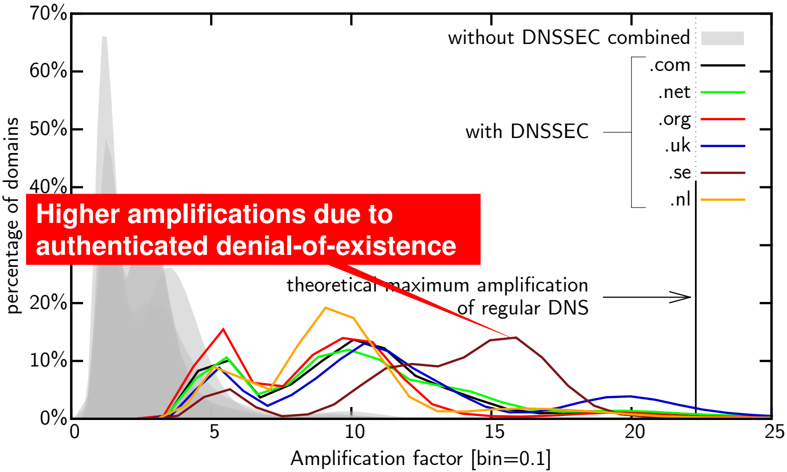
Takeaway: small config changes can have a big effect

A queries



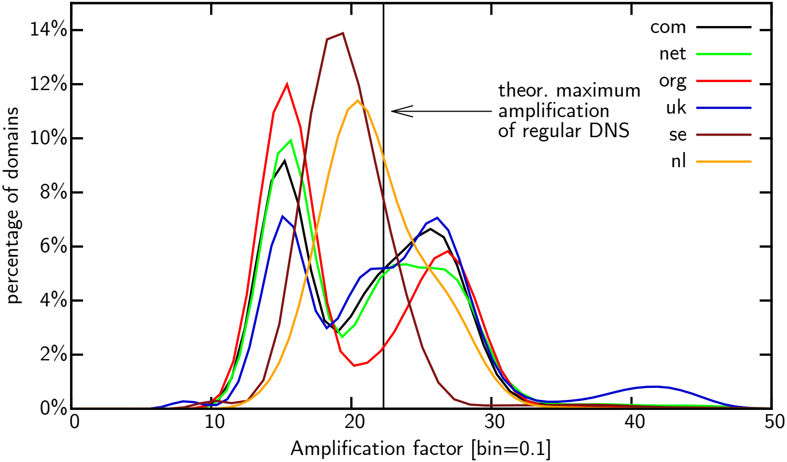
70%
60%
50%
40%
30%
20%
10%
0%
percentage of domains
0
5
10
15
20
25
Amplification factor [bin=0.1]
without DNSSEC combined
with DNSSEC
.com
.net
.org
.uk
.se
.nl
theoretical maximum amplification of regular DNS

A queries

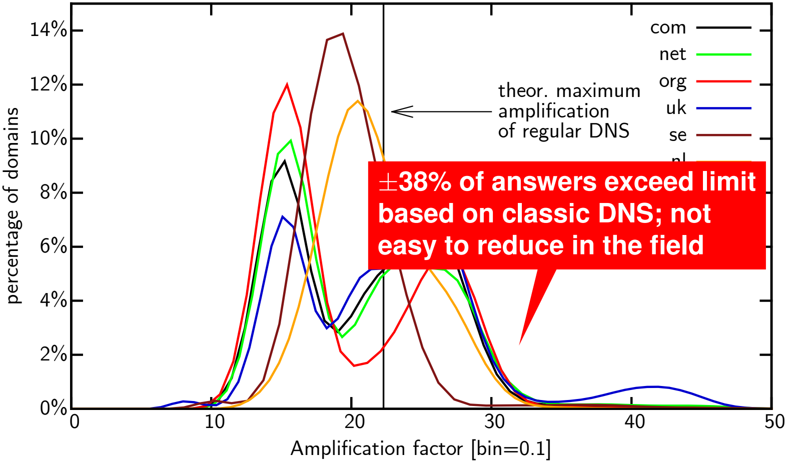


Higher amplifications due to authenticated denial-of-existence

DNSKEY queries

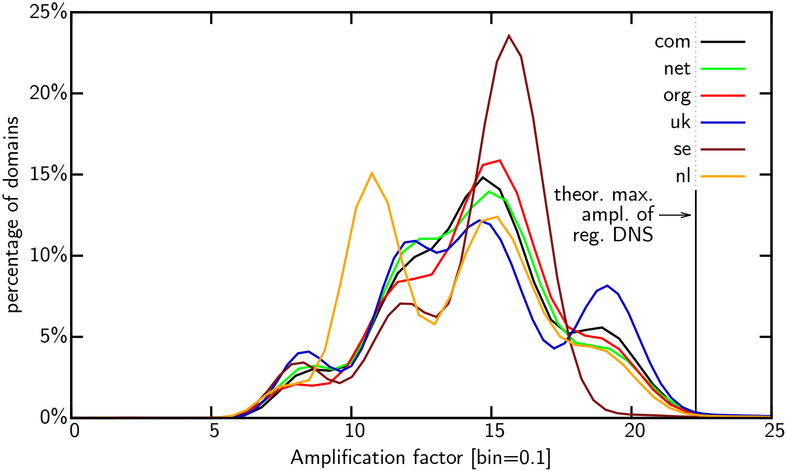


DNSKEY queries

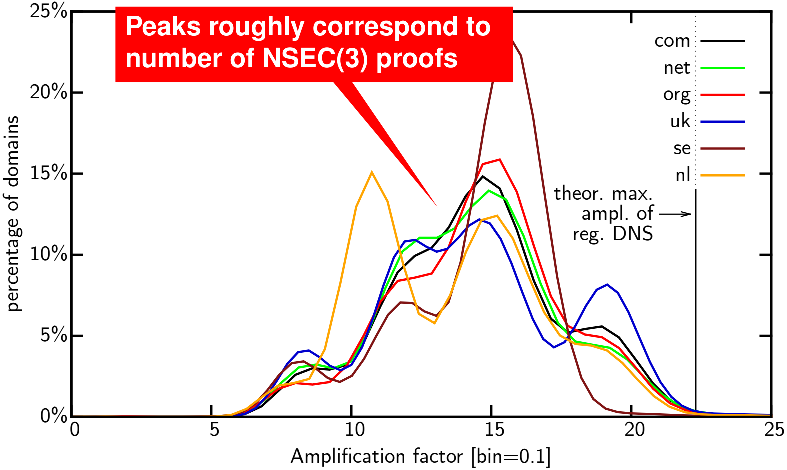


±38% of answers exceed limit based on classic DNS; not easy to reduce in the field

Authenticated Denial-of-Existence



Authenticated Denial-of-Existence



Peaks roughly correspond to number of NSEC(3) proofs

So it’s really bad?

image courtesy of `zombiecrisis.org`

- At first glance DNSSEC **is** that double-barreled shotgun
- But that is only true if we look at `ANY` queries
- On average other query types incur much more limited amplification increases
- Authenticated denial-of-existence is responsible for the worst increase in amplification for non-`ANY` queries
- `DNSKEY` queries are the biggest worry since there is no straightforward way to reduce the response size

Mitigation

- Restricting or blocking `ANY` queries[4]
- DNS cookies[5]
- Ingress filtering (BCP 38 & BCP 84)
- Response Rate Limiting (RRL)
- Response Size Limiting (RSL)

- No single deployed strategy effectively mitigates the threat

[4] Joe Abley, Ólafur Guðmundsson, and Marek Majkowski. *(draft) - Providing Minimal-Sized Responses to DNS Queries with QTYPE=ANY*. . 2015. URL: `https://tools.ietf.org/html/draft-jabley-dnsop-refuse-any-01`.

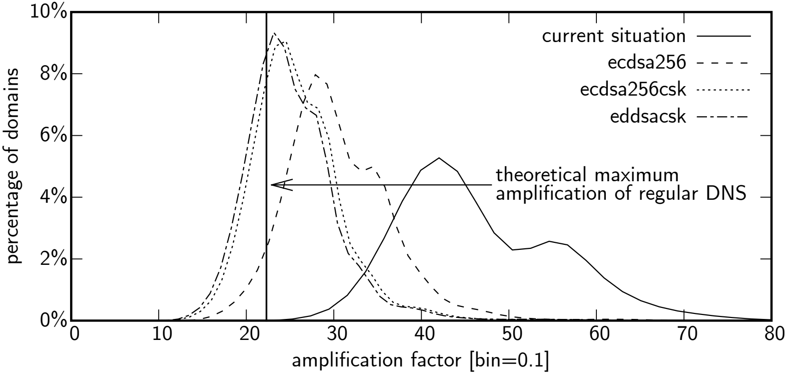
[5] Donald Eastlake and Mark Andrews. *(draft) - Domain Name System (DNS) Cookies*. 2015. URL: `https://tools.ietf.org/html/draft-ietf-dnsop-cookies-06`.

Alternative: dampen DNSSEC impact

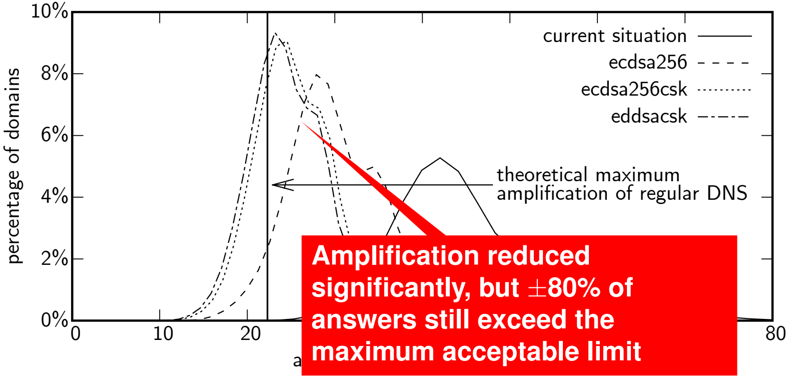
- Since a multi-tiered approach seems warranted, why not look at reducing impact of DNSSEC itself?
- What makes DNSSEC an attractive amplifier?
  Keys and **signatures**!
- Arguable root cause: RSA
  - 1024-bit RSA → 128-byte signature, ±132 byte `DNSKEY`
  - 2048-bit RSA → 256-byte signature, ±260 byte `DNSKEY`
- Alternatives exist based on elliptic curve cryptography
  - ECDSA → standardised in 2012 in RFC 6605
  - EdDSA → under discussion in `cfrg` and `dnsop` WGs
- We studied their effect on amplification (& fragmentation)[6]

[6] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. “Making the Case for Elliptic Curves in DNSSEC”. . In: *ACM Computer Communication Review* 45.5 (2015).

ANY amplification revisited

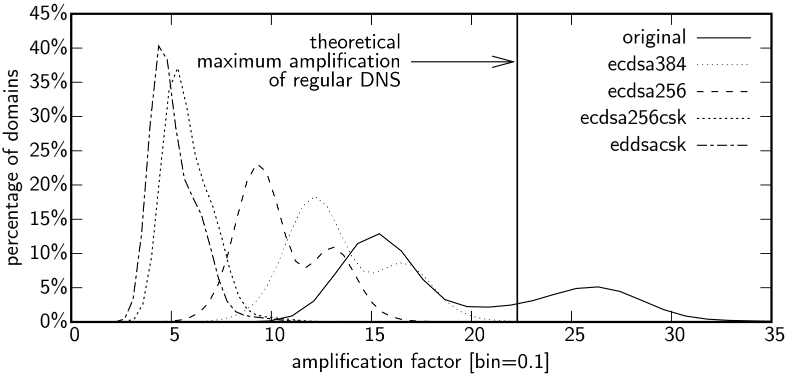


ANY amplification revisited

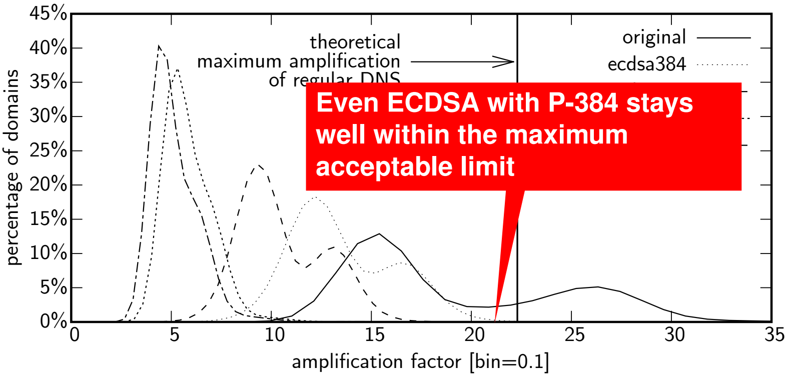


Amplification reduced significantly, but ±80% of answers still exceed the maximum acceptable limit

DNSKEY amplification revisited

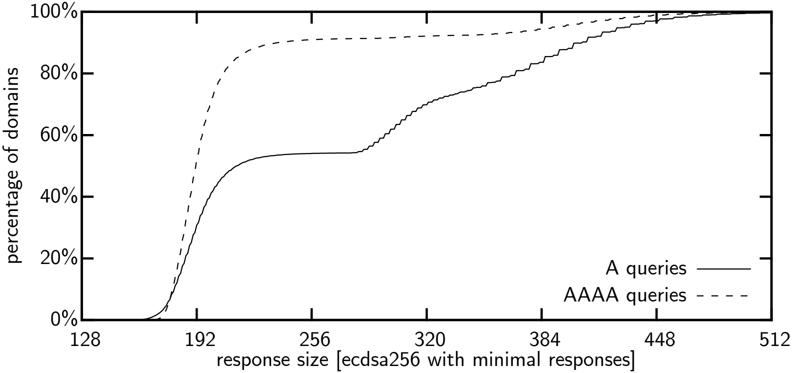


DNSKEY amplification revisited



Even ECDSA with P-384 stays well within the maximum acceptable limit

A & AAAA fit in classic DNS!



- Also holds for DNSKEY in some cases, see paper

ECC considerations

- ECC algorithms show promise for use in DNSSEC
- Potential to virtually eliminate amplification potential
- Eliminate fragmentation*
- Enable simpler key management strategies*

- Remaining worry: **validation** of ECC signatures **is (much) slower than RSA**, thus a risk of pushing load to the edges (validating resolvers)

  → also studying that, initial result: not a problem[7], expect a paper soon!

*for more information, see the paper

[7] Kaspar Hageman. *The Performance of ECC Algorithms in DNSSEC: A Model-based Approach*. 2015. URL: `http://essay.utwente.nl/68358/`.

Conclusions

- We confirmed the intuition that DNSSEC is an attractive amplification source for attackers
  - On average 6×-12× the amplification of regular domains
- . . . not the whole truth; only `ANY` queries are really bad, and `DNSKEY` is worrying
- Mitigation requires a multi-tiered approach
- We are studying changes in DNSSEC itself → switching to elliptic curve crypto is a worthwhile approach
- Interesting times: lots of mitigations strategies under consideration, we are keen to study their roll-out

Questions?

Our data sets are available as open data, get them at:

`http://traces.simpleweb.org/`

Part of this work has been supported by the EU-FP7 FLAMINGO Network of Excellence Project (318488)

Part of this work was supported by the GigaPort3 programme funded by the Dutch Economic Structure Enhancing Fund (FES)

With thanks to the Internet Society for sponsoring travel to IETF 94 in Yokohama as part of the Applied Networking Research Prize 2015

✉ r.m.vanrijswijk@utwente.nl

in nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil