DNSSEC and Its Potential for DDoS Attacks

A Comprehensive Measurement Study

Joshua Messitte

DNSSEC

- The goal of the DNSSEC protocol is to add security to information provided by the DNS System.

- DNSSEC introduces digital signatures in DNS responses
  - *EDNS0 (DNS extension)*

DNSSEC

- The goal of the DNSSEC protocol is to add security to information provided by the DNS System.

- DNSSEC introduces digital signatures in DNS responses
  - *EDNS0 (DNS extension)*

Tradeoff: Signed Responses and Larger Response Size

DDoS Attacks

- IP Spoofing
- Reflection
- DNS Amplification

DDoS Attacks

- IP Spoofing → Attacker falsifies the IP address in a request.
- Reflection
- DNS Amplification

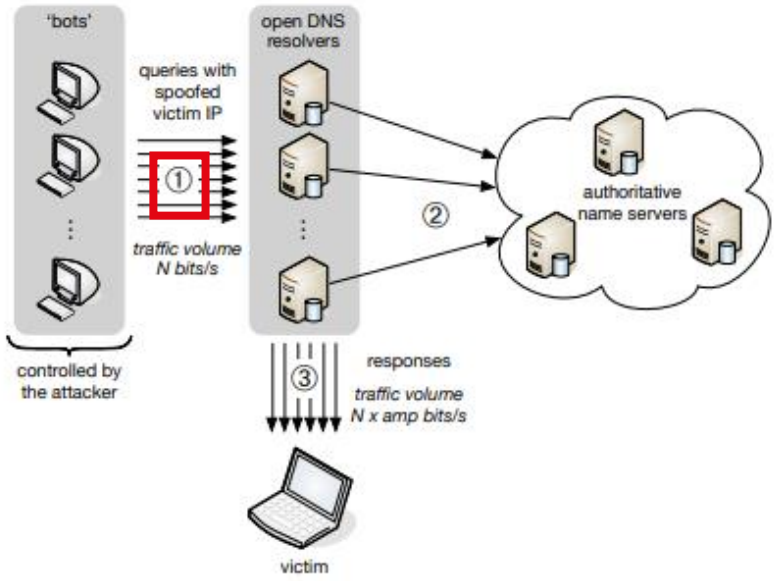


Figure 1: DNS amplification attack

DDoS Attacks

- IP Spoofing
- Reflection
- DNS Amplification

Response to this request sent to the falsified IP address.

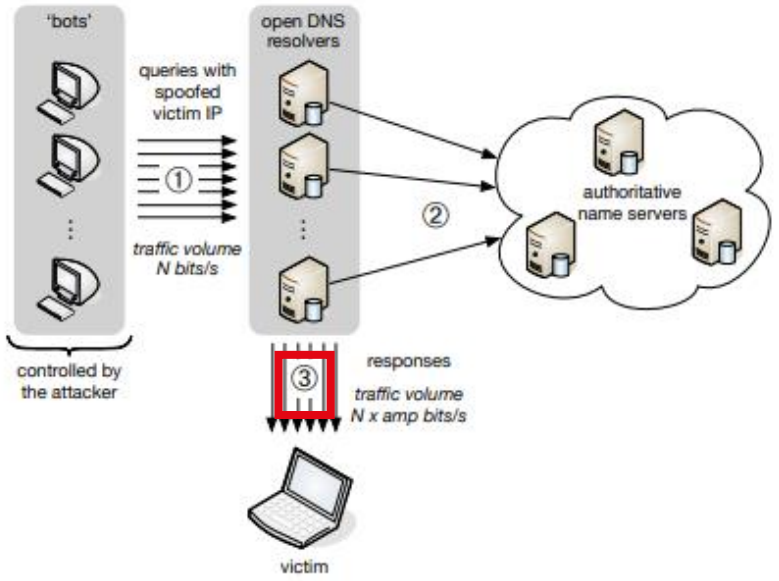
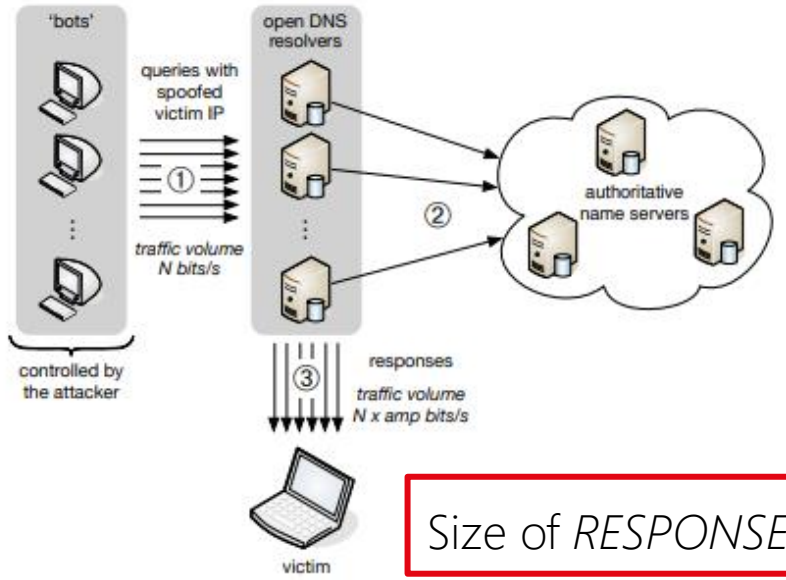


Figure 1: DNS amplification attack

DDoS Attacks

- IP Spoofing
- Reflection
- DNS Amplification

Some network protocols return a large answer to a relatively small request.



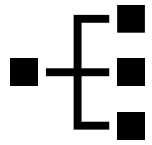
Size of *RESPONSE* > Size of *REQUEST*

Figure 1: DNS amplification attack

DDoS Amplification Attack

- Attackers use bandwidth amplification

Attack Methodology:
- Craft certain domains for which certain requests are guaranteed to return large responses.
- Large `TXT` records common
- Use of `ANY` queries common



Q-size (bytes)	R-size (bytes)	Ampl. (factor)	Attacker (bits/s)	Victim (bits/s)
40	512	12.8	100M	1.28G
40	1472	36.8	100M	3.68G
40	4096	102.4	100M	10.24G

Table 1: Theoretical effect of DNS amplification

$$\text{Amplification} = \frac{response\ size}{query\ size}$$

Motivation

Question: How bad is DNSSEC for DDoS Attacks?

1. *Tradeoff:* ***Signed Responses*** *and* ***Larger Response Size***

Potential for high amplification / DDoS Attacks

2. *Amplification Attacks*

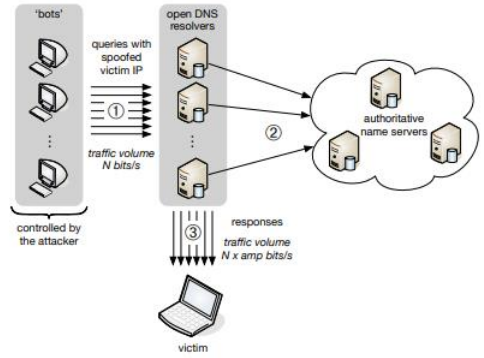


Figure 1: DNS amplification attack

DDoS Amplification *before* DNSSEC

→ Scarce bandwidth on resolvers

→ Crafted domain names can be vulnerable

→ Response Filtering on crafted domains

Attackers Benefit From DNSSEC

→ Attackers can choose from a collection of DNSEC-signed domains.

→ Less vulnerable to prosecution.

→ DNSSEC domains more stable.

→ Harder to filter.

Maximum Amplification *before* DNSSEC

Remember: EDNS0 signatures vastly increase the amplification potential in DNS.

Question: What is the max amplification factor an attacker can achieve *pre-EDNS0 ?*

Maximum Amplification *before* DNSSEC

Remember: EDNS0 signatures vastly increase the amplification potential in DNS.

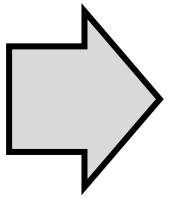
Question: What is the max amplification factor an attacker can achieve *pre-EDNS0 ?*

1. Use a query for the smallest domain name 'x.com'
   A. This yields the smallest query size (23 bytes)
2. Use a response that uses the maximum size for DNS (512 bytes)

$$\text{Pre-EDNS0 Max Amplification Factor} = \frac{512}{23} \approx 22.3$$

The Experiment

Perform a detailed measurement on a large dataset of *DNSSEC-signed* domains



Compare the potential for amplification to a second set of *non DNSSEC-signed* domains

**Note: This study covers ≈70% (2.5 million) of DNSSEC signed domains*

Query Types

- `ANY`
  - Largest possible response, returns all records.
- `MX`
  - Domains can have 1+ MX servers, DNS responses are relatively large.
- `NS`
  - Domains can have 1+ authoritative servers.
- `A`
  - Most common DNS query performed
- `AAAA`
  - Modern software look for both IPv4 and IPv6 address.
- `TXT`
  - Attackers use with crafted domains for amplification attacks.

DNSSEC-specific Query Types

- `DNSKEY`
  - Returns a set of public keys required to validate signatures in a domain. Domains can have 1+ keys which result in relatively large responses.
- `NSEC(3)`
  - *Authenticated denial of existence*

Metrics for Each Query

- Response size
- Query size
- Amplification Factor
- EDNS0 maximum response size provided by server
- Whether or not response was truncated
- Number of answers
- Number of authority records
- Number of additional records

Metrics for Each Query

Response size

÷

Query size

=

Amplification Factor 

EDNS0 maximum response size provided by server

Whether or not response was truncated

Number of answers

Number of authority records

Number of additional records

Measurement Software

Zone File Parser

1. Given size of DNS zones for different TLDs (.com, .net, etc.)
2. Extract DNSSEC and regular domains
3. Stores extracted domains in an SQLite database.

Scanner Application

1. Operates on database created by parser
2. For each domain, performs queries for each type
   A. Determines auth. Servers and IP addresses
   B. Send queries
3. Records measurements for each query

An Ethical Note

Caution was taken to ensure that these measurements do not impose an undue burden on the authoritative servers scanned.

Data Analysis

Remember: Amplification factor is the main metric

Data Analysis: **ANY** Queries

Remember: Amplification factor is the main metric

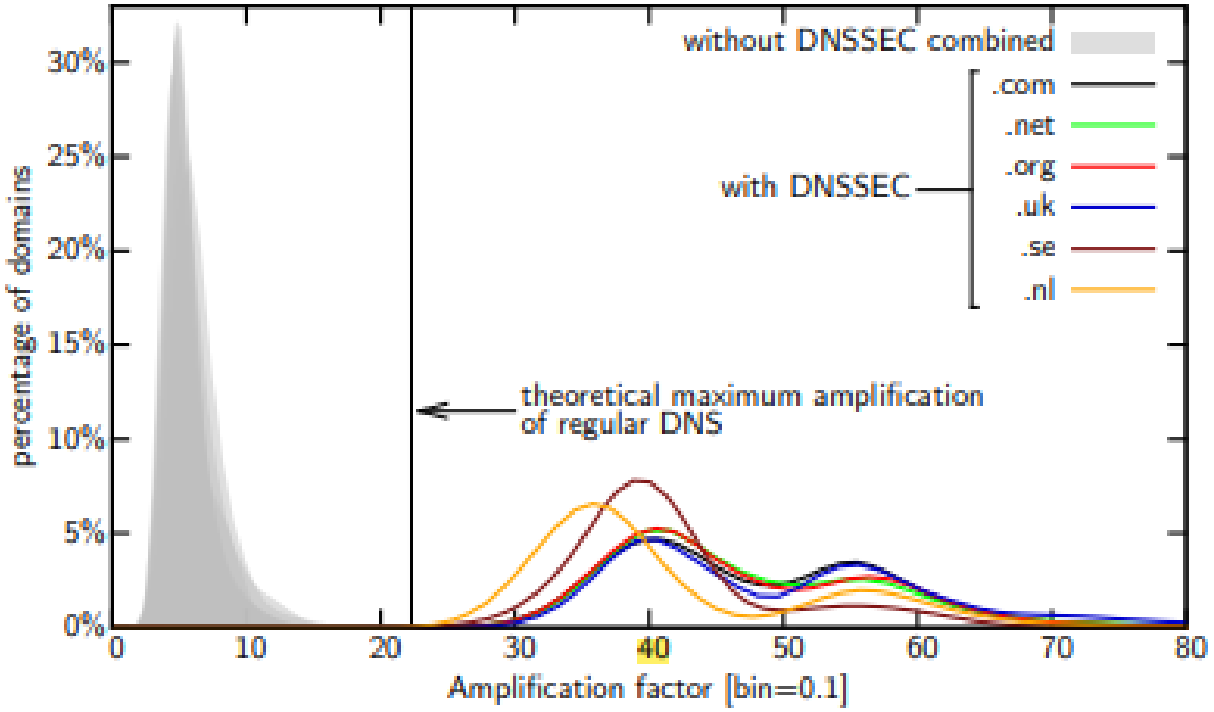
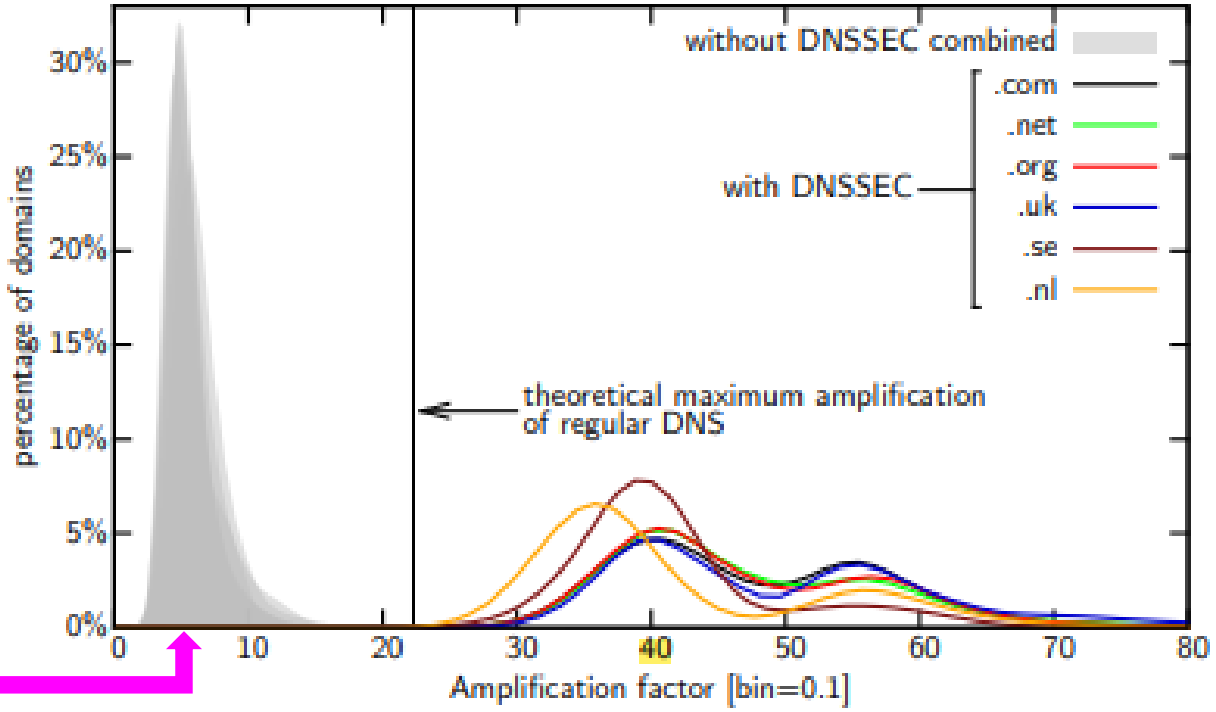


Figure 5: Amplification of ANY queries (all TLDs)

Data Analysis: **ANY** Queries

Remember: Amplification factor is the main metric



Average amplification for unsigned domains = 5.9

Figure 5: Amplification of ANY queries (all TLDs)

Data Analysis: **ANY** Queries

Remember: Amplification factor is the main metric

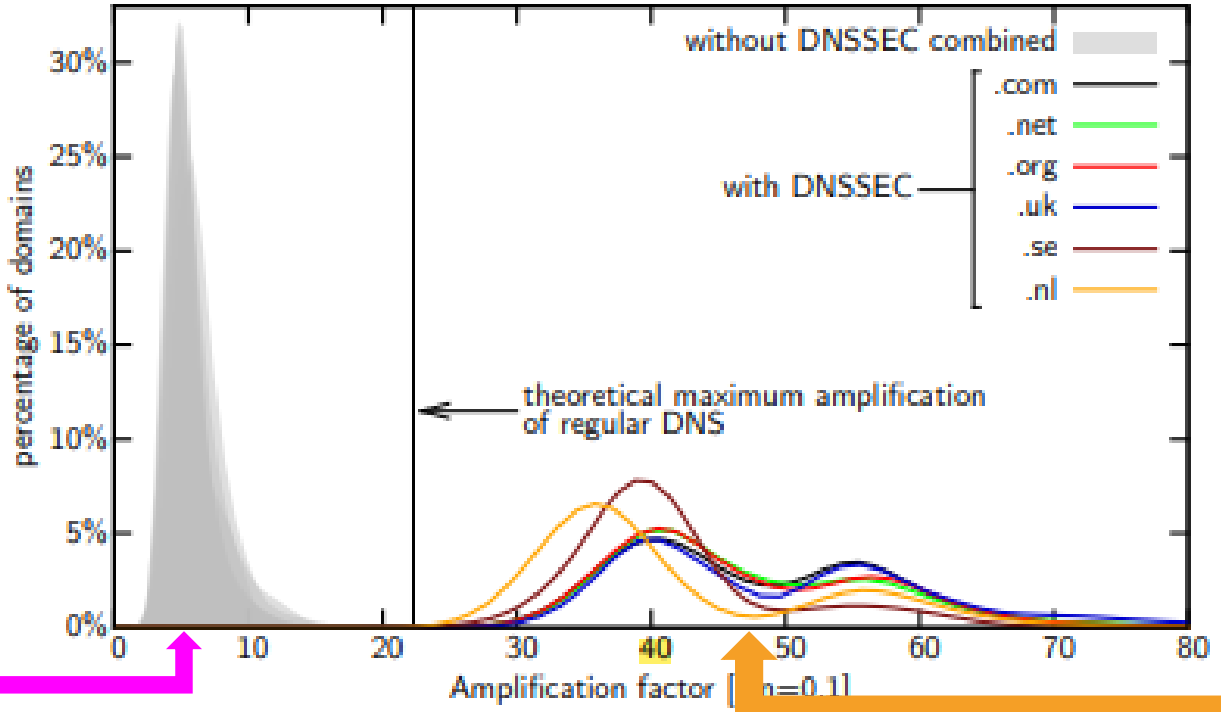


Figure 5: Amplification of ANY queries (all TLDs)

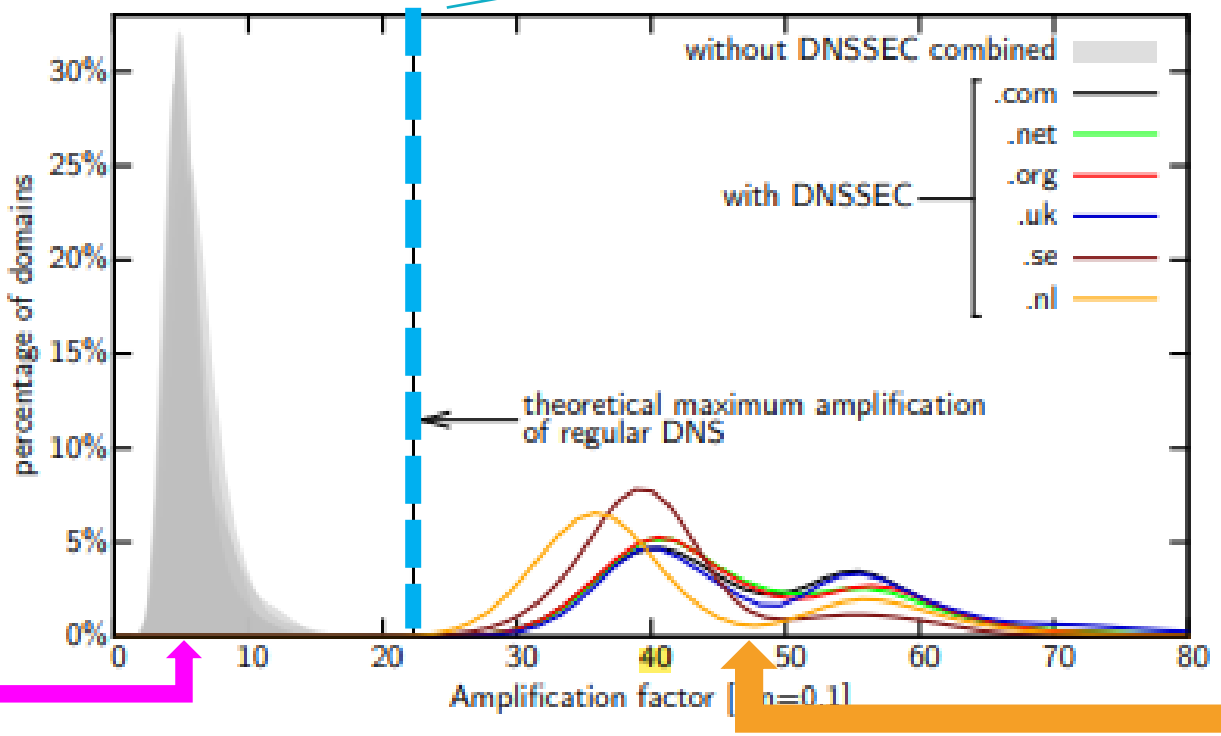
Average amplification for unsigned domains = 5.9

Average amplification for signed domains = 47.2

Data Analysis: **ANY** Queries

Remember: Amplification factor is the main metric

22.3 Amp. Factor pre-EDNS0



Average amplification for unsigned domains = 5.9

Average amplification for signed domains = 47.2

Figure 5: Amplification of ANY queries (all TLDs)

Data Analysis: **DNSKEY/NSEC** Queries

Remember: Amplification factor is the main metric

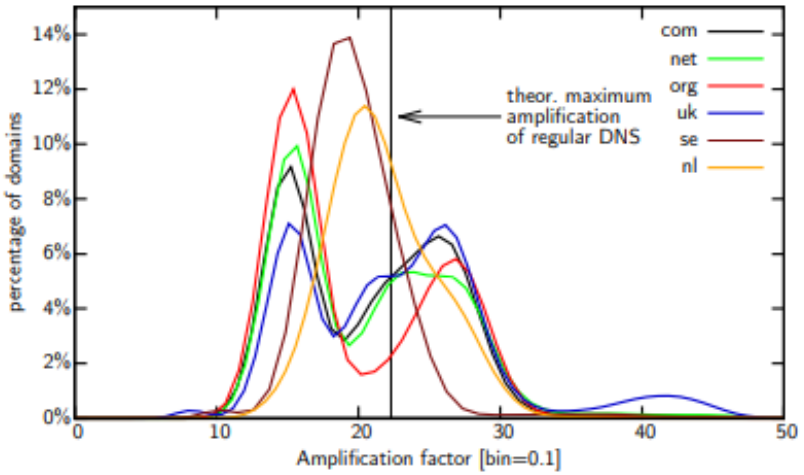


Figure 9: Amplification factor of DNSKEY queries

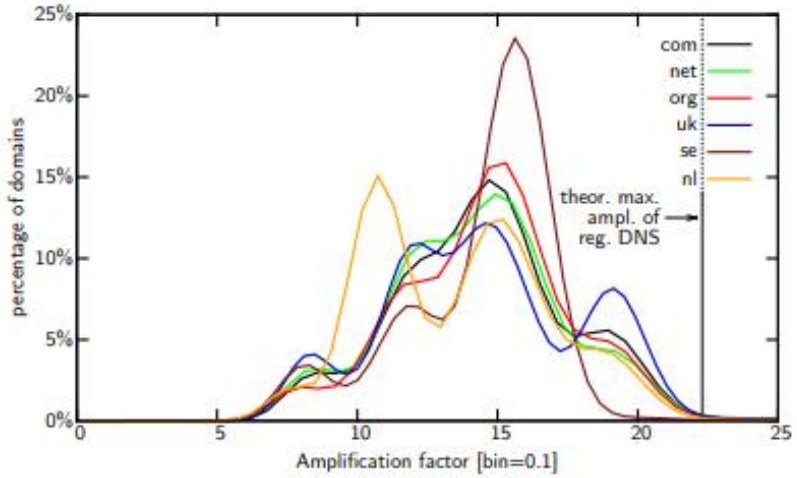


Figure 10: Amplification factor of authenticated denial-of-existence

Data Analysis: **DNSKEY/NSEC** Queries

Remember: Amplification factor is the main metric

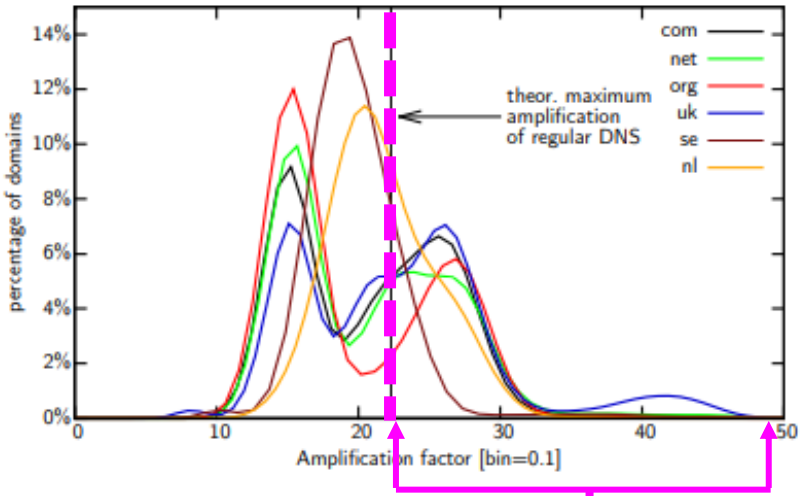


Figure 9: Amplification factor of DNSKEY queries

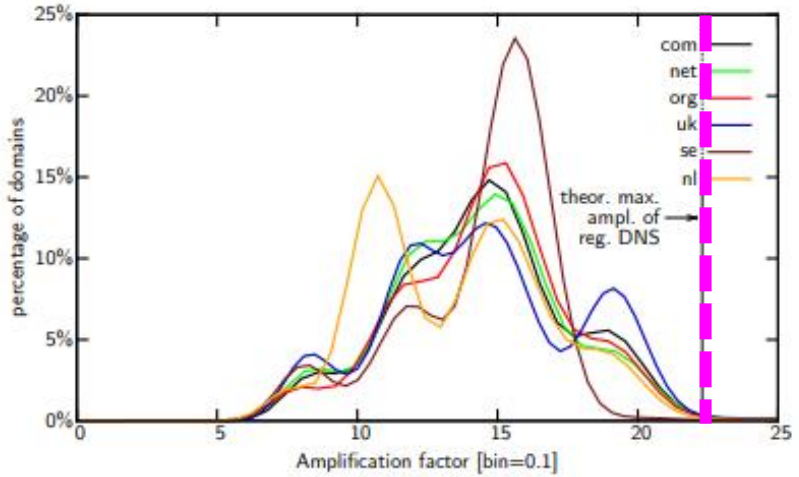


Figure 10: Amplification factor of authenticated denial-of-existence

37.8% of DNSKEY queries above upper limit

Data Analysis: `TXT,MX,NS,A,AAAA` Queries

Remember: Amplification factor is the main metric

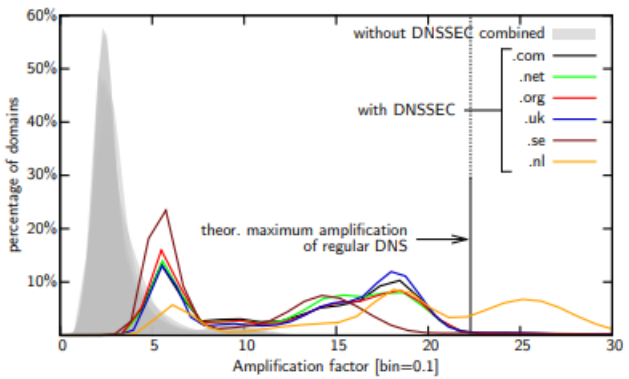


Figure 13: Amplification of `TXT` queries

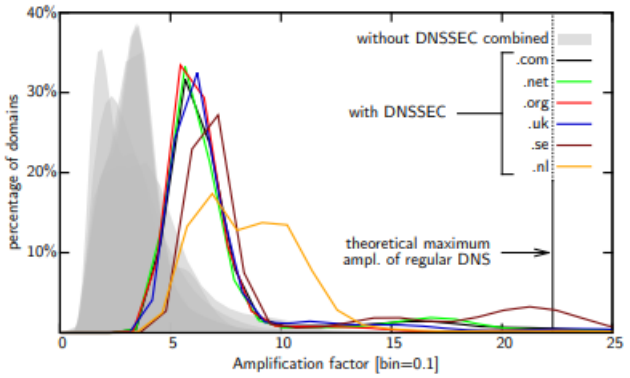


Figure 11: Amplification of `MX` queries

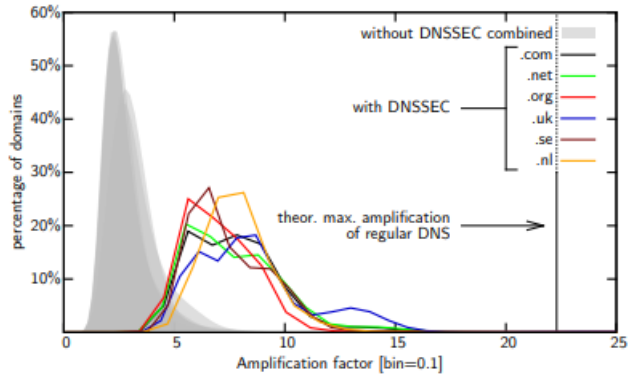


Figure 12: Amplification of `NS` queries

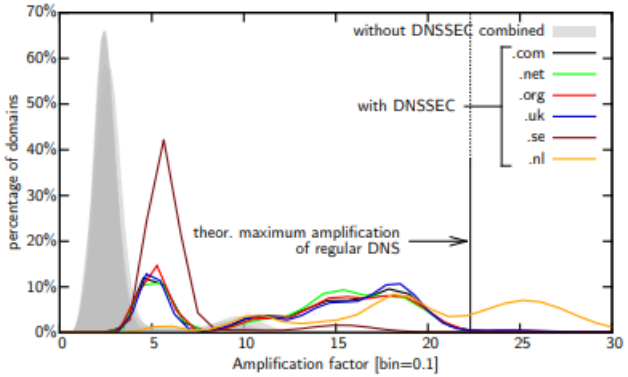


Figure 15: Amplification of `AAAA` queries

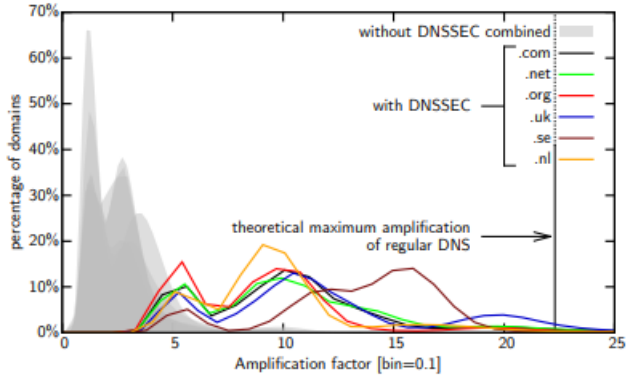


Figure 14: Amplification of `A` queries

Data Analysis: `TXT`, `MX`, `NS`, `A`, `AAAA` Queries

Remember: Amplification factor is the main metric

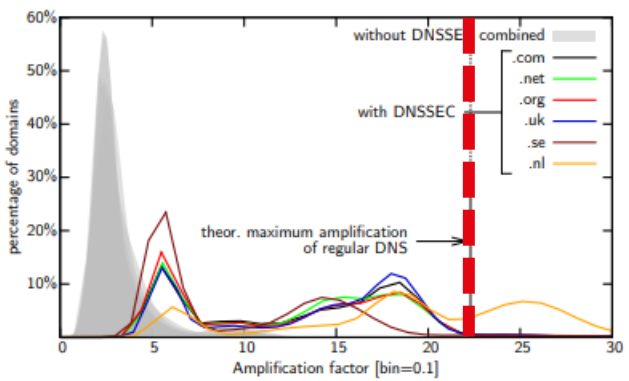


Figure 13: Amplification of `TXT` queries

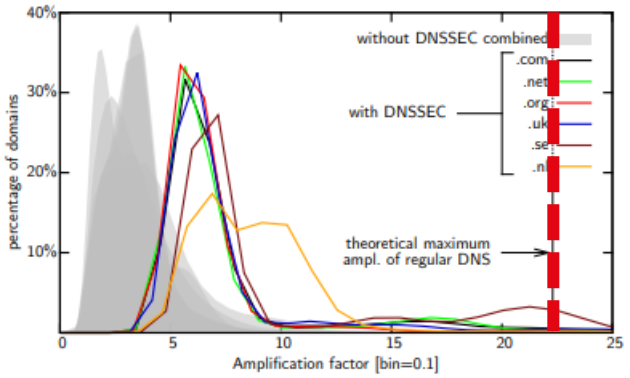


Figure 11: Amplification of `MX` queries

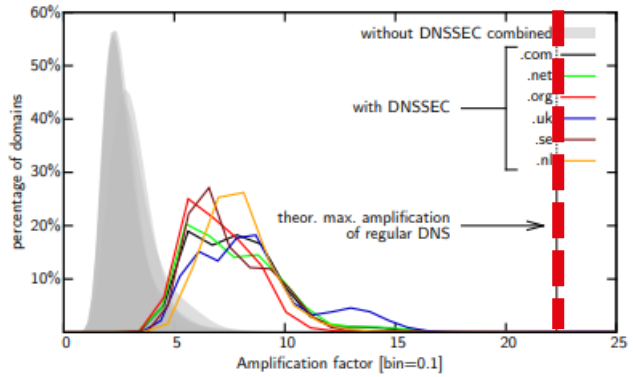


Figure 12: Amplification of `NS` queries

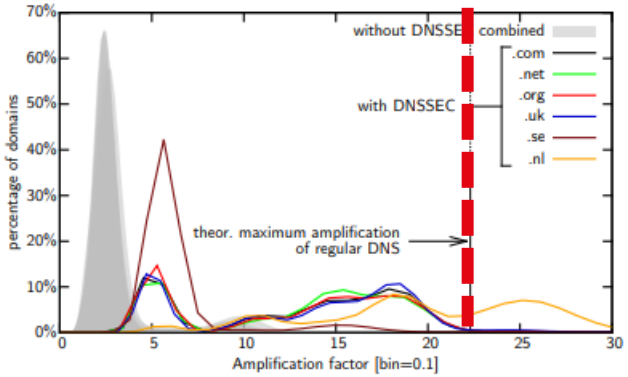


Figure 15: Amplification of `AAAA` queries

* Majority of queries below upper bound

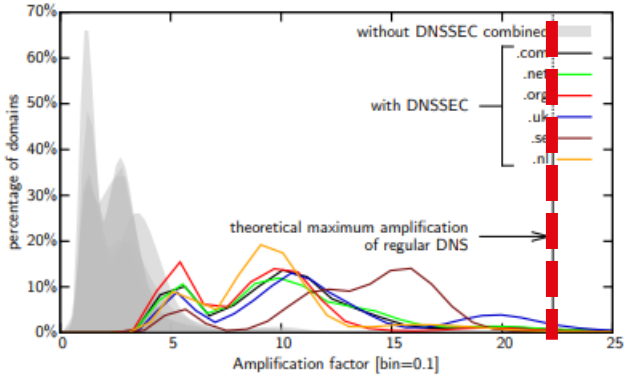


Figure 14: Amplification of `A` queries

Data Analysis: `TXT,MX,NS,A,AAAA` Queries

Remember: Amplification factor is the main metric

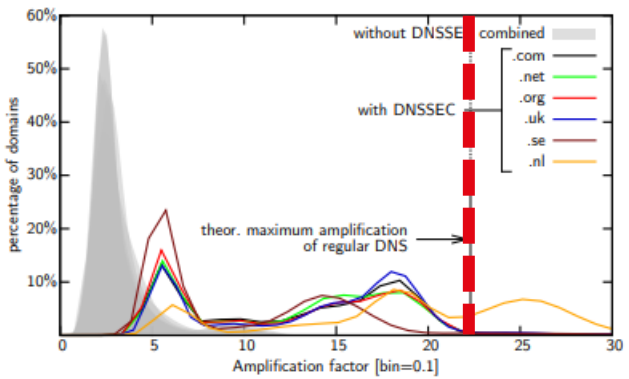


Figure 13: Amplification of `TXT` queries

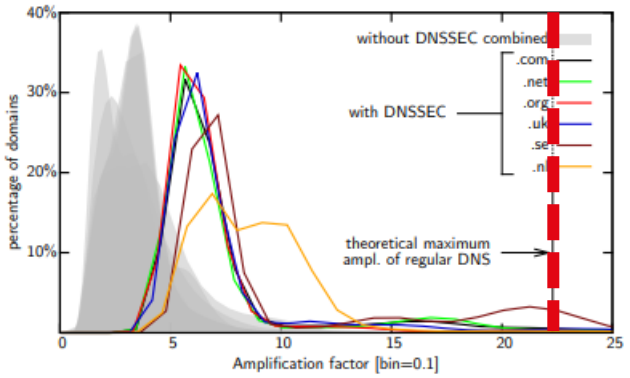


Figure 11: Amplification of `MX` queries

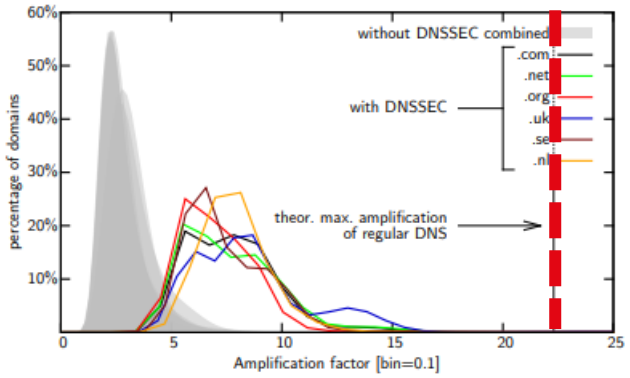


Figure 12: Amplification of `NS` queries

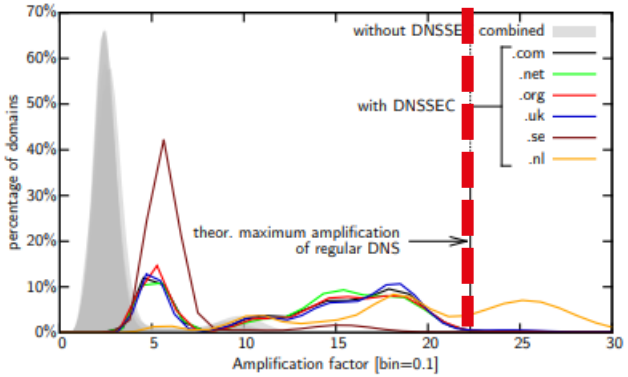


Figure 15: Amplification of `AAAA` queries

* Majority of queries below upper bound

`1)NS & MX`

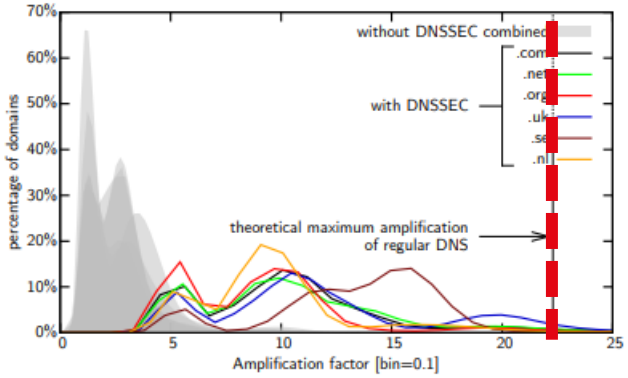


Figure 14: Amplification of `A` queries

Conclusions

Overall Conclusion: DNSSEC *is bad* for DDoS Attacks

- If we only consider **`ANY`** queries, the amplification of DNSSEC-signed domains exceeds regular DNS queries by a factor of 6-12 times, on average.
- 37.8% of **`DNSKEY`** queries are above the upper limit for amplification
- DNSSEC seems to give attackers more options

There is some nuance to this risk

- Many common DNS queries (**`MX`**, **`NS`**, **`AAAA`**) yield amplification factors that are within the upper bound.

Countermeasures

- Ingress Filtering
  - Block IP spoofing
- Response Rate Limiting (RRL)
  - Auth. servers limit rate of outgoing responses to the same IP block
- EDNS0 Cookies
  - Address authentication
- Response Size Limiting
  - Mainly affect **`ANY`** queries
- Block **`ANY`** requests

Countermeasures

- Ingress Filtering
  - Block IP spoofing
- Response Rate Limiting (RRL)
  - Auth. servers limit rate of outgoing responses to the same IP block
- EDNS0 Cookies
  - Address authentication
- Response Size Limiting
  - Mainly affect **`ANY`** queries
- Block **`ANY`** requests

Thank You!

Joshua Messitte | Joshua.Messitte@uga.edu
B.S.,M.S. Computer Science

Source

URL: https://conferences2.sigcomm.org/imc/2014/papers/p449.pdf

Roland van Rijswijk-Deij
University of Twente and
SURFnet bv
r.m.vanrijswijk@utwente.nl

Anna Sperotto
University of Twente
a.sperotto@utwente.nl

Aiko Pras
University of Twente
a.pras@utwente.nl