DNSSEC and its potential for DDoS attacks
a comprehensive measurement study

Roland van Rijsijk-Deij, Anna Sperotto, Aiko Pras
DNS amplification

'bots' controlled by the attacker

queries with spoofed victim IP

traffic volume $N$ bits/s

open DNS resolvers

responses

traffic volume $N \times \text{amp}$ bits/s

authoritative name servers

Amplification factor: \( \frac{\text{response size}}{\text{request size}} \)
DNSSEC

- DNS Security Extensions (DNSSEC)
- Development started in late 90s, large-scale roll-out since ‘Kaminsky’ vulnerability in 2008
- 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:

  “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?
Time to establish some...
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\(^1\)
- 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

---

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

The graph illustrates the amplification factor for different domains with and without DNSSEC. The theoretical maximum amplification of regular DNS is indicated by the black line.

The domains shown are: .com, .net, .org, .uk, .se, and .nl.
ANY queries

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

Theoretical maximum amplification of regular DNS

DNSSEC and its potential for DDoS attacks November 7, 2014 7 / 16
Outliers all the way up to $179 \times$

e.g. ANY query for comcast.net has amplification of $109 \times$

theoretical maximum amplification of regular DNS
Twin Peaks

Combined

#DNSKEY answers <= 4
#DNSKEY answers > 4

Takeaway: small config changes can have a big effect
A queries

Theoretical maximum amplification of regular DNS with DNSSEC.

Without DNSSEC combined.

With DNSSEC:
- .com
- .net
- .org
- .uk
- .se
- .nl

This graph shows the percentage of domains and the amplification factor over time, indicating the potential for DDoS attacks with and without DNSSEC.
A queries

Higher amplifications due to authenticated denial-of-existence

Amplification factor [bin=0.1]
DNSKEY queries

DNSSEC and its potential for DDoS attacks
DNSKEY queries

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

Amplification factor [bin=0.1] theor. max. ampl. of reg. DNS

percentage of domains

Amplification factor [bin=0.1]

DNSSEC and its potential for DDoS attacks November 7, 2014 11 / 16
Authenticated Denial-of-Existence

Peaks roughly correspond to number of NSEC(3) proofs

Amplification factor [bin=0.1]

percentage of domains

com
net
org
uk
se
nl

0% 5% 10% 15% 20% 25%

0 5 10 15 20 25

ampl. of reg. DNS

theor. max. ampl. of reg. DNS
So it’s really bad?

- 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

- Ingress filtering (BCP 38 & BCP 84)
- Response Rate Limiting (RRL)
- Restricting or blocking ANY queries
- Response Size Limiting (RSL)
- EDNS0 Cookies

- No single deployed strategy effectively mitigates the threat
- Performed exploratory work combining RSL with EDNS0 cookies; results are promising but needs more work
Conclusions

► We confirmed the intuition that DNSSEC is an attractive amplification source for attackers
  ► On average $6 \times -12 \times$ the amplification of regular domains

► ... not the whole truth; only ANY queries are really bad
  ► Raises the question: should we stop supporting these
  ► Some DNSSEC-specific queries also pose a problem

► Given the growing DNSSEC deployment this needs to be addressed

► There are many mitigation approaches; those currently implemented do not deal effectively with the problem
Future work

- Further examine effectiveness of EDNS0 cookies, especially combined with Response Size Limiting
- Investigate effect of switching to other cryptographic signature algorithms, specifically ECDSA
  - Assess impact on infrastructure
  - Possible input for IETF standardisation process
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)

r.m.vanrijswijk@utwente.nl

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil