Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention

The MADDVIPR Project One Year Later

Raffaele Sommese | University of Twente

24 October 2019

Homeland Security
Science and Technology

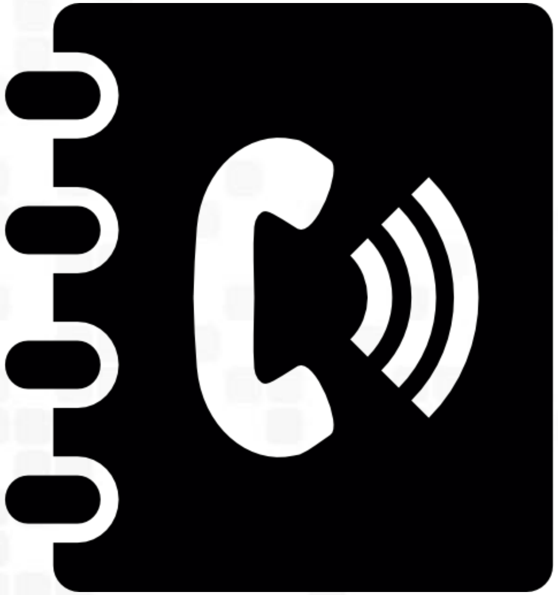
Team Profile

- Raffaele Sommese - PhD candidate - University of Twente
- Anna Sperotto - Associate Professor - University of Twente
- Roland van Rijswijk-Deij - Assistant Professor - University of Twente
- Alberto Dainotti - Research Scientist - CAIDA, UC San Diego
- KC Claffy - Research Scientist - CAIDA, UC San Diego

UNIVERSITY OF TWENTE.

Introduction: DNS nowadays

- The DNS is one of the most crucial infrastructures on the Internet.
- DNS provides the fundamental service of translation of human-readable name in IP address.
- The DNS is the phonebook of the Internet!



Introduction: DNS, not just names

- The DNS provides also other services.
- One of them is to provide information for routing the emails through different providers.
- The DNS is also fundamental in VOIP telephony.

Customer Need

- Why is important to protect DNS?
- “If you can stop the DNS, you effectively stop most Internet communication”
- DDoS attacks on DNS infrastructure can have a devastating effect.
- Understanding the nature of DDoS attacks on DNS infrastructure, and its resilience in the face of such attacks, is fundamental to protection of the system against new attacks.

Approach - Overview

1. Identify DNS single points of failure (SPoF) and vulnerabilities

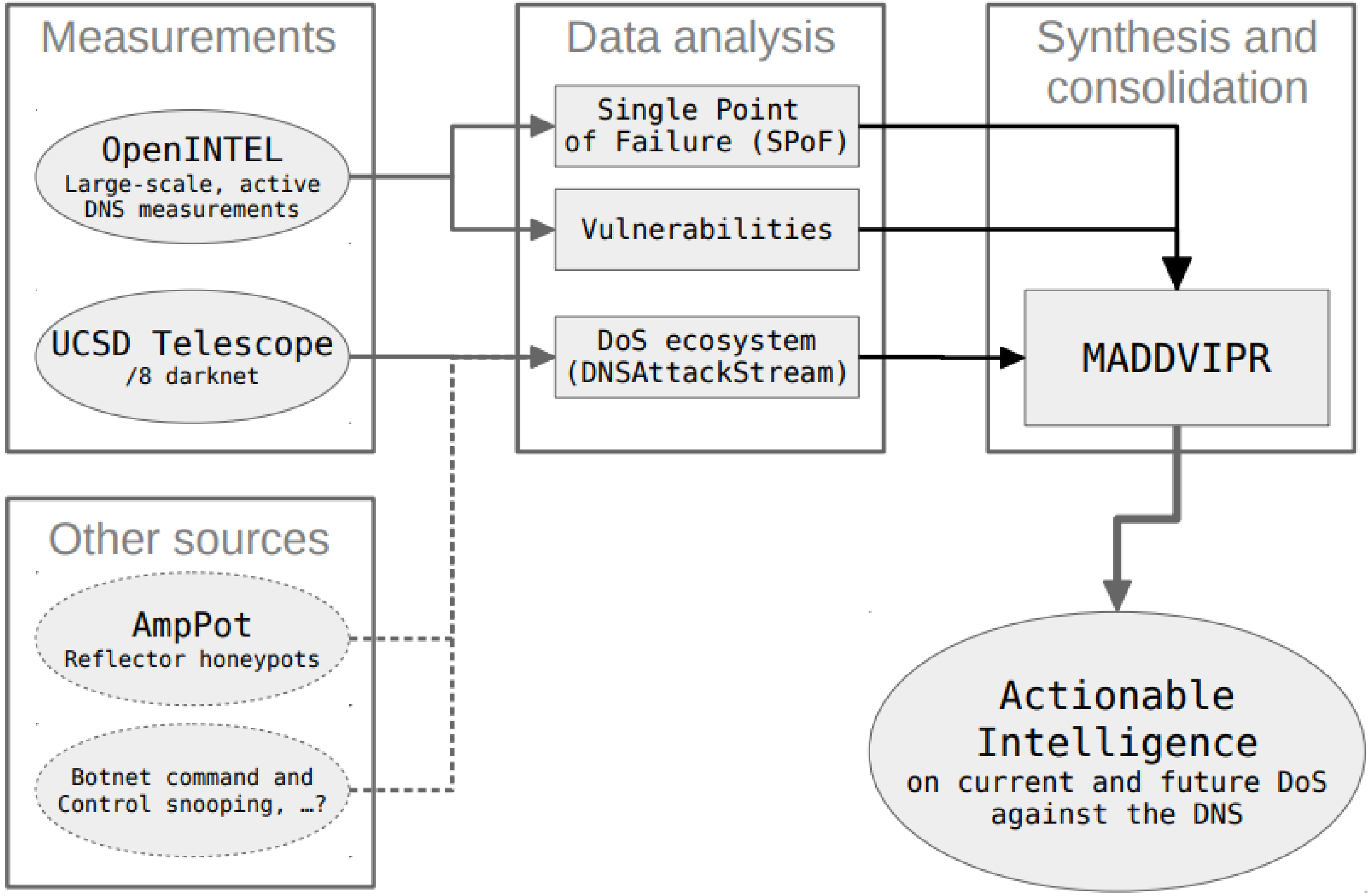
   To predict how the DNS will be the target of future attacks

2. Analyze the DNS DDoS ecosystem

   To gain a comprehensive overview of current DDoS attacks against the DNS (attackers, attacks, and targets)

3. Synthesize results of (1) and (2) into a unified view to produce actionable information (for operators and security experts) to improve DNS resilience

Approach -Architecture



Measurements

OpenINTEL
Large-scale, active DNS measurements

UCSD Telescope
/8 darknet

Other sources

AmpPot
Reflector honeypots

Botnet command and Control snooping, …?

Data analysis

Single Point of Failure (SPoF)

Vulnerabilities

DoS ecosystem (DNSAttackStream)

Synthesis and consolidation

MADDVIPR

Actionable Intelligence on current and future DoS against the DNS

Approach - Measurements

Main Datasets:

- OpenINTEL project – daily active measurements of >60% of the DNS namespace (Feb. 2015 – ongoing).
- UCSD Network Telescope – inference of DoS attack activity (Jan 2010 – ongoing).

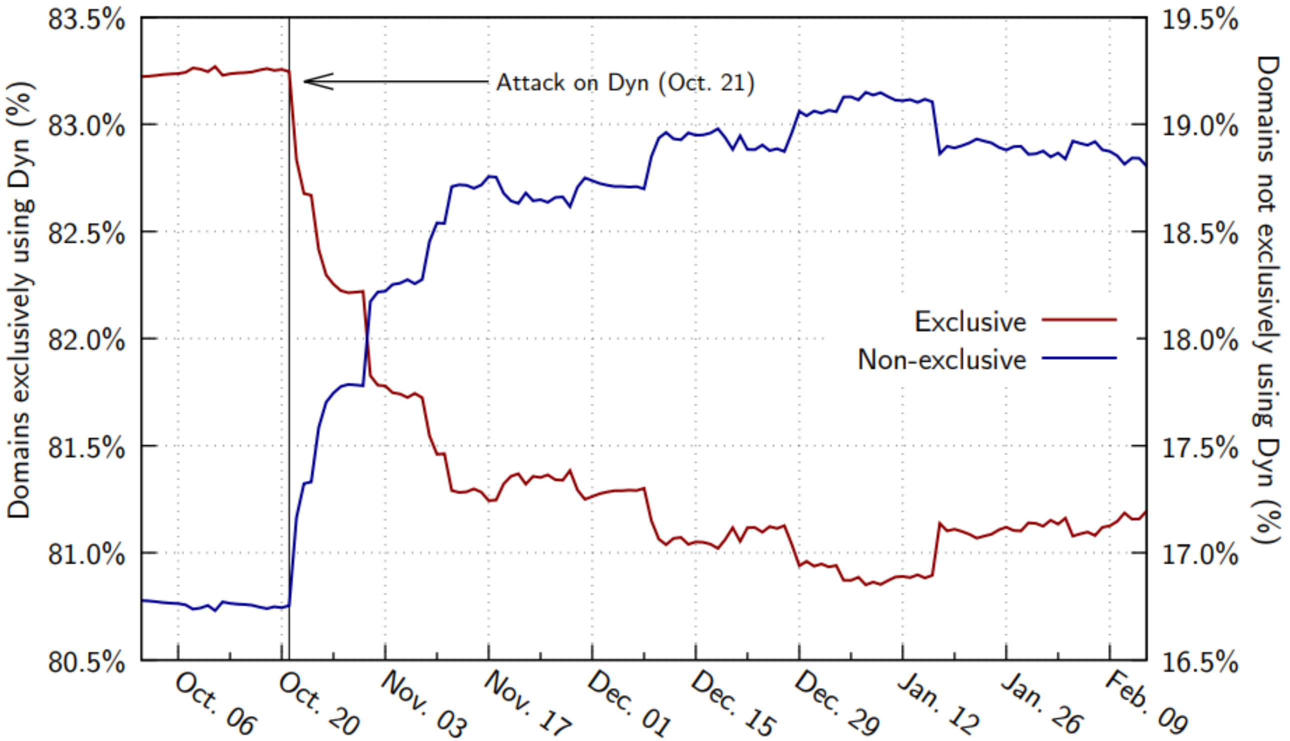
Additional Datasets:

- AmpPot reflection honeypot (University of Saarland), Botnet C&C, ...

Benefits

- Increase in DNS infrastructure resilience as strategic response to an attack

In case of Dyn, the SPoF could be detected before the attack by using the OpenINTEL data.



Benefits

- A rigorous characterization of the DNS DDoS ecosystem and of the DNS vulnerability and misconfiguration
- Operators and security experts: access to **actionable information** in form of e.g. SPoF and misconfiguration blacklists, to improve the resilience and management of their DNS solutions

Competition/Alternatives

- Active DNS measurements
  - Other DNS measurements, e.g. netray.io (RWTH Aachen) and activednsproject.org (GeorgiaTech), exist.
    - In comparisons, OpenINTEL has more comprehensive coverage (65% of the namespace) and has been collecting data the longest (4 years)
  - Alternative: passive DNS measurements; they provide a partial view

- DoS attacks
  - UCSD-NT: unique and comprehensive global view on randomly-spoofed DoS attacks
  - Others provide information about other types of DoS attacks or partial information

Current Status: First Year of MADDVIPR

- Background research on DNS-related DDoS vulnerabilities.
- Parent-Child Mismatch in the DNS hierarchy: The problem of NS and TTL mismatch.
- Orphan and Abandoned records: Dangling resources forgotten in the DNS.

Parent-Child Mismatch in the DNS hierarchy

- Some information is replicated along the hierarchy between parent and child zone.
- One of these is the NS Record.
- The NS records maintain information about the delegation of a domain.
- Each query results in a resolution against a chain of name-servers linked by NS records.
- The NS record is contained both in the parent zone file and in the child zone.

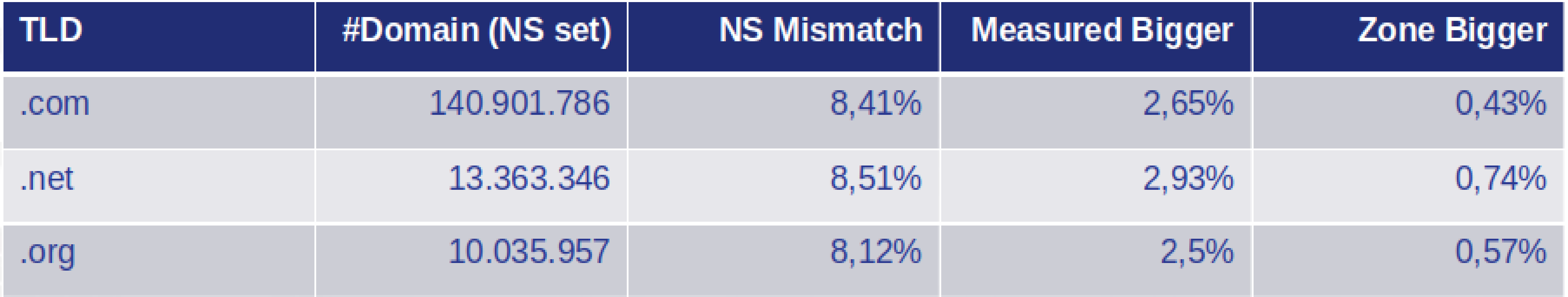
Replicated? Distributed? Consistent?

- The information replicated in the different levels of the hierarchy SHOULD BE CONSISTENT.
- Is this always true?
- Which is the impact of information mismatch on the DNS reliability?

```
raffaele@arthur:~$ dig NS @a.gtld-servers.net
17ice.com
17ice.com. 172800 IN NS 01.dnsv.jp.
17ice.com. 172800 IN NS 02.dnsv.jp.
```

```
raffaele@arthur:~$ dig NS @01.dnsv.jp. 17ice.com
17ice.com. 86400 IN NS 01.dnsv.jp.
17ice.com. 86400 IN NS 02.dnsv.jp.
17ice.com. 86400 IN NS 03.dnsv.jp.
17ice.com. 86400 IN NS 04.dnsv.jp.
```

Measuring the scope of this misconfiguration



TLD	#Domain (NS set)	NS Mismatch	Measured Bigger	Zone Bigger
.com	140.901.786	8,41%	2,65%	0,43%
.net	13.363.346	8,51%	2,93%	0,74%
.org	10.035.957	8,12%	2,5%	0,57%

Zone NS set: NS records defined in the zone file of the parent (e.g. .com), Measured set : NS records defined in the child zone file (e.g. example.com)

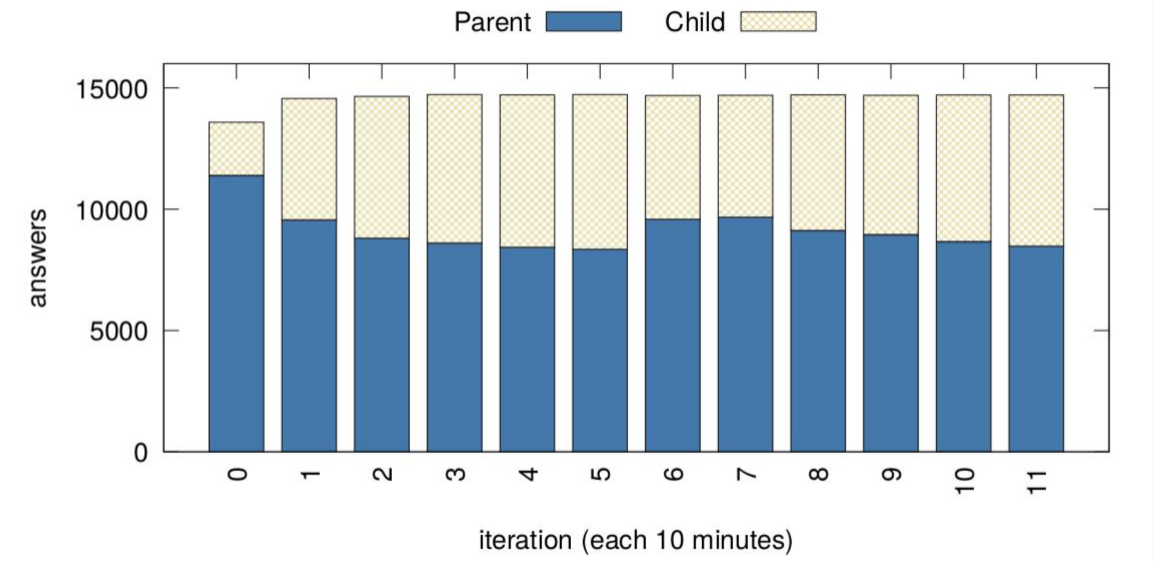
NS Mismatch: Percentage of domains for which measured NS set differs from zone NS set.

Measured Bigger (by OpenINTEL): The case shown in previous slide(measured NS set fully incorporate zone NS).

Zone Bigger: zone NS set fully incorporate measured NS.

How should resolvers behave in case of information mismatch?

- Resolvers should trust the most authoritative information obtained according to RFC 2181 Section 5.4.1
- Does this happen?



Ripe Atlas experiment: resolving a domain with NS records provided by the parent (ns1) completely different from the one provided by the child (n2).
The minimal response is disabled, the child provides the NS information to resolvers that should trust it.

How to solve this problem?

- I am a registrant, what I can do?
  - Be careful when you add your NS records to the administration panel of your domain.
  - My registrar allows me to put only two nameservers!
    - Contact your registrar
    - Change registrar
- I am a registrar, what I can do?
  - Allow users to insert a reasonable number of NS records.
  - Implement a way to check the child delegations and detect mismatches.
- I am a DNS resolver developer, what can I do?
  - Consider implementing a lazy fetcher of more authoritative information for delegation records. But be careful with CNAME on apex.

Approach Used

1. Identify the misconfiguration.
2. Study the spread of the misconfiguration using the OpenINTEL data.
3. Analyze the impact of the misconfiguration on the DNS ecosystem and the behavior of the software.
4. Provide advice and possible solutions to DNS operators.

Orphan and Abandoned Records

- Domains in DNS can be registered for a certain amount of time and expire if not renewed.
- At the expiration of a domain, all the related records should be removed from the zone file.
- In general, zone files are supposed to be clean without any orphan or dangling record.
- Is this true?

Orphan Record

- A former glue record (A record) for which the delegation records (NS records) of the related domain does not exist.
- Belonging to potentially expired domains.

```
raffaele@PreciseKoala:~$ dig  ns2.safadns.info

;; ANSWER SECTION:
ns2.safadns.info. 7178 IN A 46.4.19.73
```

```
raffaele@PreciseKoala:~$ whois safadns.info
NOT FOUND
>>> Last update of WHOIS database: 2019-10-
14T08:13:09Z <<<
```

Abandoned Record

- A former glue record (A record) for which the delegation records (NS records) of the related domain does not point anymore to it.
- Usually not resolvable.
- It could result in orphaned records at the expiring of the domain.

```
ns1.example.com IN A 42.42.42.42
example.com IN NS ns1.external.com
```

How big is the problem?

- In .info and .mobi, 25% of A glue records are orphans.
- And 40% are abandoned.
- More than half of A glue records in .info and .mobi should be deleted!

Are these records a problem?

- Orphan records can be misused for hosting malicious content without keeping the domain registered.
- Unintentionally orphaned records can be hijacked, registering the base domain.
- DO NOT POINT YOUR NAMESERVERS TO ORPHAN RECORDS!
- We discovered 39683 NS Records pointing to orphans!

How to solve the orphan and abandoned records problem?

- Clean the zone files by deleting these orphan and abandoned records!
- But this could impact other domains that rely on these records.
- A solution would be actively notifying domain owners of these misconfigurations and delete records after a period with no response.
- And in the future keep the zone clean!

Lesson Learned

- DNS is one of the most complex and precious infrastructures of the Internet.
- There are many instances of misconfiguration in the DNS system that could undercut the DNS reliability.
- Measuring DNS misconfigurations can help us to proactively identify misconfiguration and prevent or mitigate attacks.

Future Research

- Continue to analyze and study the impact of misconfigurations.
- Use OpenINTEL and UCSD Network Telescope to detect DDoS attacks against the DNS and their impact on the availability of these resources.
- Expand the OpenINTEL platform to perform monitoring of the DNS ecosystem from several vantage points and identify discrepancies.

Questions?

Contact Info

Raffaele Sommese
University of Twente
r.sommese@utwente.nl
+31 6 16 144424
https://academia.r4ffy.info | https://maddvipr.org/

UNIVERSITY OF TWENTE.