Background research on DNS-related DDoS vulnerabilities

Raffaele Sommese[1], Anna Sperotto[1], Roland van Rijswijk-Deij[1]
Alberto Dainotti[2], Kimberly Claffy[2]
[1]) University of Twente [2]) CAIDA, UCSD
{r.sommese, a.sperotto, r.m.vanrijswijk}@utwente.nl {alberto, kc}@caida.org

1 Introduction

Distributed Denial of Service (DDoS) attacks are one of the most disruptive attacks in today's Internet. These types of attacks are even more effective and more dangerous when they target or misuse core Internet infrastructure and services, such as the Domain Name System (DNS). The DNS is a fundamental pillar of the Internet's core infrastructure, and its role is crucial not only for the translation of human-readable names into IP addresses but also for supporting plenty of widely used Internet applications, such as e-mail, VoIP, etc.

In this document, we provide an overview of the MADDVIPR (Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention) project, a collaboration between the University of Twente and the Center for Applied Internet Data Analysis (CAIDA-UCSD). In Section 2, we introduce the project's objectives and methodologies. In Section 3.1, we review the current state of the art in DNS vulnerabilities and attacks, including reflection and amplification attacks. In 3.2, we describe the most frequent attacks against the DNS system and their impact. In 3.3, we explain how typical misconfigurations that can impair DNS availability. Section 4 discusses countermeasures. Section 5 proposes some improvements.

2 The Project

In order to protect the DNS against DDoS attacks, we first analyse *what we are protecting* and *what we are protecting against.* This phase of the project has two objectives.

- Analyse the DNS resolution system, trying to identify single points of failure and vulnerabilities that can be exploited by a DDoS attack. Such vulnerabilities include DNS misconfiguration, concentrating authoritative DNS servers under a single organisation, single points of failure in the DNS chain, etc.
- Provide a comprehensive review of documented DDoS attacks that have exploited DNS infrastructure vulnerabilities, to understand trends in attack sources, types, and targets. This will provide a baseline to investigate ways to map and mitigate risks of future attacks, and reduce their prevalence.

This project will use a data-driven approach, using the dataset provided by OpenINTEL. [1] OpenINTEL collects daily active DNS lookups of over 60% of the global DNS namespace.[1] We will analyze data collected by OpenINTEL, and combine it with other data such as network topology measurements, to better understand the scope and extent of vulnerabilities.

3 DNS Vulnerabilities to Attacks

3.1 DNS as an attack vector

One use of the DNS as an attack vector is to spread amplification and reflection attacks. Distributed Denial-of-Service (DDoS) attacks create network congestion on paths to targets of the attacks. They abuse UDP-Based services in combination with spoofing to achieve reflection, and trigger large response from the UDP services to achieve amplification. Figure 1 illustrates this type of attack, which commonly uses DNS or NTP servers as reflection and amplification sources.

[1] `https://openintel.nl/coverage/`

An attacker spoofs the address of the victim and sends a request to a DNS or an NTP server, customizing queries to ensure large responses, e.g. a DNS ANY query. The amplified response traffic will be sent to the victim. This type of attack could be devastating because it can be conducted with little firepower from the attackers.

DDoS Reflection and Amplifications Attacks are often carried out using open resolvers. An OpenDNS Resolver is a publicly accessible DNS resolver, which allows the resolution of recursive DNS queries for anyone on the Internet [2]. Due to the connectionless architecture of the DNS protocol and its amplification factor, an OpenDNS Resolver introduces a significant threat to the global network. The misuse of OpenDNS resolvers to perform reflection and amplification attacks is widely described in the literature [3].

The AmpPot Project monitors reflection and amplification attacks through different HoneyPots, including DNS-based ones [4]. CAIDA monitored DNS reflection Attacks through the UCSD Network Telescope by discovering responses to spoofed queries in Internet Background Radiation [5]. Potential vectors of DNS amplification are:

- **EDNS Record**: Introduced in *RFC2671* [6], which extends DNS answers up to 4096 bytes per UDP packet for certain DNS queries.
- **DNSKEY Record**: Introduced to store DNSSEC Public Keys with a common size of 1024 or 2048 bits.
- **ANY Record**: Largest query, returns all resource records for the queried name.
- **NSEC(3)**: Introduced to provide an authenticated denial of existence.
- **TXT Record**: Textual information for queried name. Attackers can use a custom query to exploit these typically larger DNS records [7].

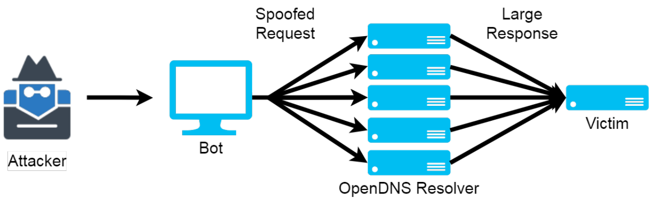

Figure 1: Reflection and Amplification Attack

Reflection and Amplification attacks rely on another vector of attack, which is the ability to spoof source addresses in packets and transmit them from the edge across the global Internet. Network Ingress Filtering (BCP 38)[8] is an IETF best practice document [**rfc2827**] that recommends adoption of a filter at the border of each edge network to permit only packets with legitimate source addresses, i.e., those owned by that network, to enter the Internet. CAIDA monitors adoption of *source address validation* through a crowdsourced Spoofer measurement platform.[2] The Spoofer Project provides a client software tool for different platforms (Windows, Linux, Mac), which allows users to test the spoofing capability of networks to which they attach, and reports results to CAIDA's servers, for aggregated public reporting.

3.2 DNS as target of attack

In July 1994, Alternic (an alternative name registry) founder, Eugene Kashpureff redirected the internic.net domain (Internic - the ancestor of ICANN) to their site, www.alternic.net. Alternic stated that they were protesting the Internic's claim to ownership of root nameservers. As a consequence, in October 1997, Eugene Kashpureff was arrested by Canadian authorities and extradited to the U.S. for wire fraud [9]. The hijacking was made possible using a DNS cache poisoning attack.

[2] https://www.caida.org/projects/spoofer/

Nowadays, different techniques can be used to prevent and mitigate this type of attack, but only DNSSEC is the definitive solution. Unfortunately, DNSSEC is still not yet widely deployed [10]. APNIC estimated that in 2018, DNSSEC-validated queries were around 12-14% of total DNS query load.[3]

We provide an overview of current exploitable attacks against the DNS:

- **DNS Cache Poisoning**: An attacker exploits system vulnerabilities or blocks legitimate answers from an authoritative nameserver (NS), intervening to place a forged answer into the DNS cache.
- **Domain Hijacking**: An attacker changes the nameservers or other fields in a DNS record for a specific domain, often redirecting DNS queries for that domain to a new (fake) destination. Attackers can use several approaches:
  - Directly compromise the authoritative nameservers.
  - Compromise any nameservers in the chain.
  - Compromise, e.g., by getting credentials of, the hosting registrar's management web interface, which then allows an attacker to modify anything about the zone.
- **Random Subdomain Attack** (Figure 2): An attacker sends a huge number of DNS queries to a nameserver for non-existent random sub-domains of a targeted domain, saturating its authoritative nameserver, due to the full resolution required for NXDOMAIN.
- **NXDOMAIN attack**: Instead of performing a DoS attack against an authoritative NS, in this case an attacker performs a DoS attack against the resolver, which must spend time and resources performing full recursion to respond to the queries.
- **Phantom Domain Attack**: In this attack, the queries are related to a specially crafted domain owned by the attacker. The nameservers of this domain never answer queries. The attacker sends a huge number of that type of query to a resolver, which must spend time and resources doing the recursion, waiting for an answer that will never come [11].
- **NSEC White Lie DoS**: In order to avoid zone walking to support NSEC(3), RFC4470 [12] proposes that DNS operators make up a previous and next name by randomly generating names that are canonically slightly before and after the requested name. This approach requires an on-demand generation of RRSIG records. The on-demand generation introduces two serious problems:
  - Zone Authoritative Nameservers need to access the DNSSEC private key, making it more vulnerable to disclosure.
  - The on-demand signing is a computationally heavy routine and can overload the authoritative nameservers, increasing their exposure to DoS Attack.
- **DDoS DNS flood attack**: An attacker sends a huge number of requests (using botnets), overloading the server to render it unreachable.
- **Distributed Reflection Denial of Service (DRDoS)**: Similar to the previous attack, but the attacker uses other DNS servers to amplify the firepower of the attack.

3.2.1 Impact of an Attack: Dyn's Case

One of the biggest DDoS attacks on the DNS infrastructure was performed in 2016 against Dyn DNS. This attack disabled many large Internet services on the East Coast of the United States, including some big name Internet brands such as Twitter, PayPal and Spotify. The attack used the Mirai Botnet, a botnet of compromised vulnerable small network devices, like router and IoT-devices, which attacked Dyn's DNS servers [13]. The affected Internet companies exclusively used Dyn as DNS provider [14], making Dyn's DNS service a single point of failure for these companies.

[3] https://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=1&w=7&g=0

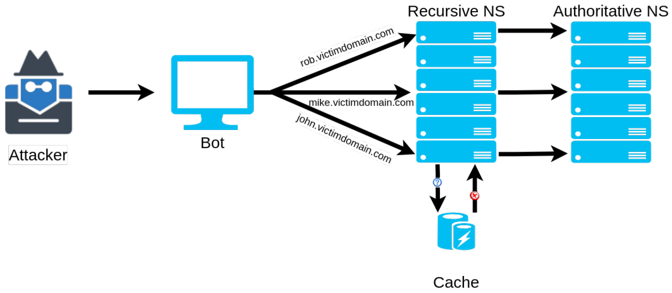

Figure 2: Random Subdomain Attack

3.3 DNS Misconfiguration and Vulnerabilities

We describe some frequent misconfigurations and vulnerabilities present in the DNS and analyzed in the literature. This background analysis is fundamental for our research. Indeed, with the result of this analysis, we can measure the spread and the impact of these vulnerabilities and the possible countermeasures that could improve the resilience of DNS.

3.3.1 Misconfiguration of DNSSEC

The DNSSEC protocol uses public key cryptography to provide protection against spoofing of DNS data by providing a means to verify the authenticity of the origin of a response to a DNS query, including verifying the integrity of the data or authenticating the absence of a hostname in a specific domain. However, DNSSEC increases the complexity of infrastructure, increasing the likelihood of mistakes and misconfiguration, which can result in loss not only of authenticity but of reachability of the domain. A 2014 study of misconfigurations for domains of four zones .bg, .br, .co, .se revealed that 4% of domains showed misconfigurations, 75% of which led to unreachability [15].

DNSSEC also introduced **NSEC** records for proof and authenticated denial of existence. The NSEC record returns the previous and next name in the zone. In this way, a nameserver can prove to the resolver that the queried name does not exist, because nothing exists between the two names listed (sorted alphabetically) in the NSEC record. This mechanism also introduced a new problem: an attacker can perform a complete zone walking and enumeration.

In order to avoid zone-walking, NSEC3 provided a hashed linked list instead of a plain text one. However, a dictionary-based enumeration attack was still possible. To solve this problem, NSEC5 used a cryptographically secure hash function through the use of a special *verifiable random function* (VRF). A VRF is the public-key version of a keyed cryptographic hash [16]. VRF intoduces a key pair (PK, SK). Only the holder of the private key SK can compute the hash, but anyone with the public key PK can verify the hash. This new key pair is different from the zone signing keypair and can be distributed on the authoritative nameserver. The public key PK is signed with the ZSK [17].

Nevertheless, we should consider the evolution of DNS services, especially high performance services. For example, CloudFlare has a custom in-house DNS server called RRDNS that does not have the concept of a zone file, but instead directly uses a key-value store. In this case, implementation of NSEC(*) as described in the standard will be extremely complicated and slow. For this reason, new solutions like NSEC White Lies (RFC7129 Appendix B) and Black Lies (developed by Cloudflare), have been introduced. This solution provides dummy online signed NSEC record to the client to avoid walking the entire database [18]. White Lie proposes to generate the NSEC answer by online signing two random records lexicographically after and before the requested name. Black Lie generates the NSEC answer by online signing a subdomain of the requested name. In this way, the wildcard NSEC record is not required.

3.3.2 Parent-Child Zone Data Mismatch

There are also misconfigurations of disagreement, i.e., mismatches, between parent and child zones, such as the following:

- **TTL and NS Record Mismatch**: The value of one of these records in the child zone does not match the corresponding one in the parent zone.
- **Ghost Glue Record**: The parent zone still has glue records for nameservers that have been removed from the zone file.
- **Lame Delegation**: The designated nameserver for a certain domain is not the authoritative nameserver for that domain (Figure 3).
- **Circular Zone Dependency**: The designated nameserver refers to another nameserver as authoritative nameserver, witch instead points to the designated nameserver (Figure 4).

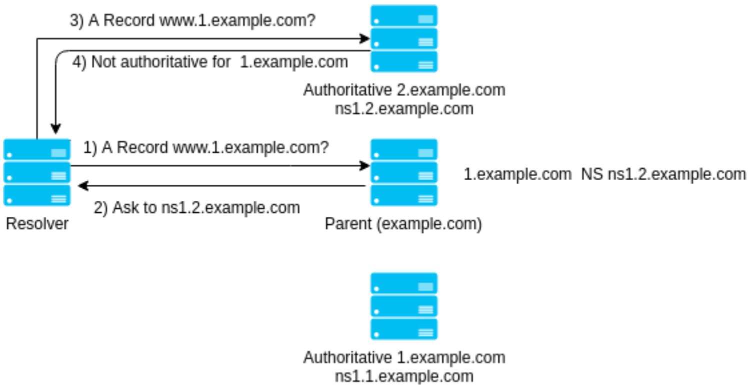
3) A Record www.1.example.com?
4) Not authoritative for 1.example.com
Authoritative 2.example.com
ns1.2.example.com
1) A Record www.1.example.com?
2) Ask to ns1.2.example.com
Resolver
Parent (example.com)
1.example.com NS ns1.2.example.com
Authoritative 1.example.com
ns1.1.example.com

Figure 3: Designated NS (ns1.2.example.org) is not authoritative for 1.example.com

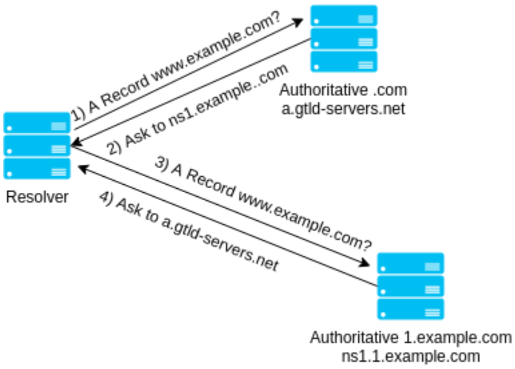
1) A Record www.example.com?
2) Ask to ns1.example..com
Authoritative .com
a.gtld-servers.net
Resolver
3) A Record www.example.com?
4) Ask to a.gtld-servers.net
Authoritative 1.example.com
ns1.1.example.com

Figure 4: Circular NS Dependency

3.3.3 Single Point of Failure (SPoF)

A Single Point of Failure (SPoF) is any component of a system that, in case of failure, causes the entire system to fail. A well-designed system should avoid SPoFs across the entire hierarchy of the system, introducing points of redundancy both in physical and logical system architecture.

- **Single or Duplicated NS Records** A single authoritative nameserver is a typical case of SPoF in the DNS system. The failure of the only authoritative nameserver leads to the unavailability of the administered zone. The case of duplicated NS records is more trivial; in this case, the use of multiple records that point to the same authoritative NS distorts choices of the DNS Round Robin server selection algorithm. For example, in a domain with 3 NS records – ns1.example.com twice and ns.example.com once – some DNS implementations will load balance the traffic on the two nameservers equally, collapsing the duplicate, while others will load balance with a proportion of 2/3 for the first and 1/3 for the second nameserver.

- **Infrastructural Single Point of Failure**:
  - Rely on only one provider for one's authoritative nameserver (Section 3.2.1.)
  - Logical redundancy but physical SPoF, e.g., all authoritative nameservers are behind the same L2 Switch [19].

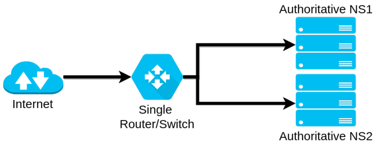

Figure 5: Logical redundancy but single physical point of failure

3.3.4 Dangling Pointer Misconfiguration

- **Dangling records and Cloud IPs**: A DNS administrator may inadvertently leave in the authoritative zone file dangling records that refer to expired resources (e.g. cloud IP addresses or names). These stale records could be exploited by an attacker trying to obtain access to the stale IP address through the same cloud services, and putting a rogue DNS server that then impersonates (hijacks) the original domain [20].
- **Expired Domain Hijacking** Another risk is re-registration of an expired domain with the aim of reselling or performing malicious activities by impersonating the previous owner.

4 Available Countermeasures

We review adoption of various countermeasures to these attacks.

4.1 Spoofing Protection

As described before, the key enabling element of reflection and amplification attacks is IP Spoofing, since source address validation (SAV) is still not pervasively deployed, and is currently incentive-incompatible for operators to maintain.[4]

4.2 Rate Limiting and Feature Disabling

Other countermeasures use rate-limiting or disabling of features such as responses answer to heavyweight **ANY** queries. However, some features are fundamental to proper operation of the DNS system (ex. DNSKEY), so this choice is not without operational cost to the infrastructure.

4.3 DNSSEC Key Shrinking

Amplification factors for RSA-signed domains average around 50x [7]. ECDSA signatures and keys are much smaller than RSA signatures and keys. Switching to ECDSA signatures can mitigate the problem of DNSSEC-based amplification attacks. ECDSA will also reduce load on authoritative nameserver for white lie answers. Unfortunately, ECDSA deployment is not widespread, recent evidence suggests a ~2% adoption for domains in {.com, .info, .net} according to the data provided by van Rijswijk-Deij *et al.* in [21] collected in 2016 over a period of 1.5 years. ECDSA also

[4] https://spoofer.caida.org/summary.php

introduced a new issue: ECC signature validation is much slower than RSA validation, although van Rijswijk-Deij *et al.* [22] found that it did not significantly increase the load on DNS resolvers, even in worst case scenarios.

4.4 DDoS Protection Services

The DDoS Protection Services (DPS) market has grown with the growth in DDoS attacks. Jonker *et al.* estimated that during their two-year measurement period (March 2015 - Feb 2017), the adoption of DPS services grew by 1.24x.[23]

4.5 Serving Stale Data

A recent Internet draft stated:

> "If the answer has not been completely determined by the time the client response timer has elapsed, the resolver SHOULD then check its cache to see whether there is expired data that would satisfy the request. If so, it adds that data to the response message with a TTL greater than 0. The response is then sent to the client while the resolver continues its attempt to refresh the data."
>
> D. Lawrence, "Serving Stale Data to Improve DNS Resiliency", 2017. [24]

In this way, if the authoritative nameserver fails, the client can receive stale data, which could still be valid.

5 Conclusion and Future Works

This analysis has provided an overview of the current state of vulnerabilities, and possible attacks and misconfigurations of today's DNS infrastructure. We have illustrated the role of DNS and its weak points. We have described how attackers misuse the DNS to perform attacks. DNS is a critical infrastructure for the Internet, and there is significant room for improvement in its resilience. We have briefly discussed several current measures to reduce the attack exposure of the DNS, and their adoption. Due to the distributed nature of DNS, it is still challenging to perform a comprehensive analysis of the health of the global DNS system. Researchers can use a combination of ICANN CZDS (Centralized Zone Data Services), OPENIntel data, and other sources to improve our state of understanding of the attack and countermeasure space on a global scale. The MADDVIPR project will pursue the following results:

1. Quantitative assessment of impacts of possible attacks and vulnerabilities as described in this document.

2. Analysis that combines historical data from OpenINTEL with knowledge developed in the first task to identify possible weak points and vulnerabilities.

3. A ranking of risks of DNS vulnerabilities, to inform operators and security experts how best to increase their resilience to future attacks.

Bibliography

[1] R. van Rijswijk-Deij et al. "A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements". In: *IEEE Journal on Selected Areas in Communications* 34.6 (June 2016), pp. 1877–1888. ISSN: 0733-8716. DOI: 10.1109/JSAC.2016.2558918.

[2] Marc Kuhrer et al. "Going Wild: Large-Scale Classification of Open DNS Resolvers". In: *Proceedings of the 2015 Internet Measurement Conference*. IMC '15. Tokyo, Japan: ACM, 2015, pp. 355–368. ISBN: 978-1-4503-3848-6. DOI: 10.1145/2815675.2815683. URL: http://doi.acm.org/10.1145/2815675.2815683.

[3] *Deep Inside a DNS Amplification DDoS Attack*. https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/.

[4] Lukas Kramer et al. "AmpPot: Monitoring and Defending Against Amplification DDoS Attacks". In: ().

[5] Karyn Benson et al. "Leveraging Internet Background Radiation for Opportunistic Network Analysis". In: *Proceedings of the 2015 Internet Measurement Conference*. IMC '15. Tokyo, Japan: ACM, 2015, pp. 423–436. ISBN: 978-1-4503-3848-6. DOI: 10.1145/2815675.2815702. URL: http://doi.acm.org/10.1145/2815675.2815702.

[6] Paul Vixie. *Extension mechanisms for DNS (EDNS0)*. Tech. rep. 1999.

[7] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. "DNSSEC and Its Potential for DDoS Attacks: A Comprehensive Measurement Study". In: *Proceedings of the 2014 Conference on Internet Measurement Conference*. IMC '14. Vancouver, BC, Canada: ACM, 2014, pp. 449–460. ISBN: 978-1-4503-3213-2. DOI: 10.1145/2663716.2663731. URL: http://doi.acm.org/10.1145/2663716.2663731.

[8] P Ferguson and D Senie. *RFC2827 (BCP38): Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. IETF, May 2000.*

[9] Antonio Lioy et al. "DNS security". In:

[10] Taejoong Chung et al. "Understanding the Role of Registrars in DNSSEC Deployment". In: *Proceedings of the 2017 Internet Measurement Conference*. IMC '17. London, United Kingdom: ACM, 2017, pp. 369–383. ISBN: 978-1-4503-5118-8. DOI: 10.1145/3131365.3131373. URL: http://doi.acm.org/10.1145/3131365.3131373.

[11] *The Most Popular Types of DNS Attacks*. https://securitytrails.com/blog/most-popular-types-dns-attacks.

[12] S Weiler and J Ihren. *Minimally covering NSEC records and DNSSEC on-line signing*. Tech. rep. 2006.

[13] Scott Hilton. "Dyn analysis summary of Friday October 21 attack". In: *Dyn Blog, Oct* (2016).

[14] Abhishta, Roland van Rijswijk-Deij, and Lambert J.M. Nieuwenhuis. "Measuring the Impact of a Successful DDoS Attack on the Customer Behaviour of Managed DNS Service Providers". In: *ACM SIGCOMM Computer Communication Review (CCR)* 48.5 (2018). DOI: 10.1145/3229598.3229599.

[15] N. L. M. v. Adrichem et al. "DNSSEC Misconfigurations: How Incorrectly Configured Security Leads to Unreachability". In: *2014 IEEE Joint Intelligence and Security Informatics Conference*. Sept. 2014, pp. 9–16. DOI: 10.1109/JISIC.2014.12.

[16] Silvio Micali, Michael Rabin, and Salil Vadhan. "Verifiable random functions". In: *40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)*. IEEE. 1999, pp. 120–130.

[17] Sharon Goldberg et al. "NSEC5: Provably Preventing DNSSEC Zone Enumeration." In: *NDSS*. 2015.

[18] Dani Grant. *Economical With The Truth: Making DNSSEC Answers Cheap*. https://blog.cloudflare.com/black-lies/.

[19] V. Pappas et al. “Impact of configuration errors on DNS robustness”. In: *IEEE Journal on Selected Areas in Communications* 27.3 (Apr. 2009), pp. 275–290. ISSN: 0733-8716. DOI: 10.1109/JSAC.2009.090404.

[20] Daiping Liu, Shuai Hao, and Haining Wang. “All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’16. Vienna, Austria: ACM, 2016, pp. 1414–1425. ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978387. URL: http://doi.acm.org/10.1145/2976749.2978387.

[21] Roland van Rijswijk-Deij, Mattijs Jonker, and Anna Sperotto. “On the adoption of the elliptic curve digital signature algorithm (ECDSA) in DNSSEC”. In: *2016 12th International Conference on Network and Service Management (CNSM)*. IEEE. 2016, pp. 258–262.

[22] R. van Rijswijk-Deij et al. “The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation”. In: *IEEE/ACM Transactions on Networking* 25.2 (Apr. 2017), pp. 738–750. ISSN: 1063-6692. DOI: 10.1109/TNET.2016.2605767.

[23] Mattijs Jonker et al. “Measuring the Adoption of DDoS Protection Services”. In: *Internet Measurement Conference*. 2016.

[24] David C Lawrence, Warren ”Ace” Kumari, and Puneet Sood. *Serving Stale Data to Improve DNS Resiliency*. Internet-Draft draft-ietf-dnsop-serve-stale-04. Work in Progress. Internet Engineering Task Force, Mar. 2019. 12 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-serve-stale-04.