Understanding the Role of Registrars in DNSSEC Deployment

Taejoong Chung
Northeastern University

Roland van Rijswijk-Deij
University of Twente and SURFnet

David Choffnes
Northeastern University

Dave Levin
University of Maryland

Bruce M. Maggs
Duke University and
Akamai Technologies

Alan Mislove
Northeastern University

Christo Wilson
Northeastern University

ABSTRACT

The Domain Name System (DNS) provides a scalable, flexible name resolution service. Unfortunately, its unauthenticated architecture has become the basis for many security attacks. To address this, DNS Security Extensions (DNSSEC) were introduced in 1997. DNSSEC's deployment requires support from the top-level domain (TLD) registries and registrars, as well as participation by the organization that serves as the DNS operator. Unfortunately, DNSSEC has seen poor deployment thus far: despite being proposed nearly two decades ago, only 1% of `.com`, `.net`, and `.org` domains are properly signed.

In this paper, we investigate the underlying reasons *why* DNSSEC adoption has been remarkably slow. We focus on registrars, as most TLD registries already support DNSSEC and registrars often serve as DNS operators for their customers. Our study uses large-scale, longitudinal DNS measurements to study DNSSEC adoption, coupled with experiences collected by trying to deploy DNSSEC on domains we purchased from leading domain name registrars and resellers. Overall, we find that a select few registrars are responsible for the (small) DNSSEC deployment today, and that many leading registrars do not support DNSSEC at all, or require customers to take cumbersome steps to deploy DNSSEC. Further frustrating deployment, many of the mechanisms for conveying DNSSEC information to registrars are error-prone or present security vulnerabilities. Finally, we find that using DNSSEC with third-party DNS operators such as Cloudflare requires the domain owner to take a number of steps that 40% of domain owners do not complete. Having identified several operational challenges for full DNSSEC deployment, we make recommendations to improve adoption.

IMC '17, November 1–3, 2017, London, United Kingdom

ACM ISBN 978-1-4503-5118-8/17/11...$15.00
https://doi.org/10.1145/3131365.3131373

CCS CONCEPTS

• **Security and privacy** → **Public key (asymmetric) techniques**; • **Networks** → **Application layer protocols**; **Security protocols**; **Naming and addressing**;

KEYWORDS

DNS; DNSSEC; DNS Security Extension; PKI; Public Key Infrastructure; Registrar; DNS Operator

ACM Reference format:
Taejoong Chung, Roland van Rijswijk-Deij, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. Understanding the Role of Registrars in DNSSEC Deployment. In *Proceedings of IMC '17, London, United Kingdom, November 1–3, 2017,* 15 pages.
https://doi.org/10.1145/3131365.3131373

1 INTRODUCTION

The Domain Name System (DNS) [33] provides name resolution for the Internet, mapping human-readable names (e.g., `example.com`) to machine-routable IP addresses (among other things). As DNS was designed without end-to-end authentication, attackers have leveraged it as a basis for myriad attacks, such as DNS hijacking [7, 27] and cache poisoning [40].

DNS Security Extensions (DNSSEC) [17] were proposed two decades ago to address threats like these. DNSSEC allows clients (typically DNS resolvers) to verify the *integrity* and *authenticity* of DNS records. It has also been leveraged to enhance the security of other protocols: For example, DANE (DNS-based Authentication of Named Entities) [43] enables domain holders to publish their public keys and authorized certificate authorities in DNS records.

DNSSEC derives its security properties from its hierarchical public key infrastructure (PKI). The DNSSEC PKI establishes chains of trust that mirror the structure of the DNS hierarchy, with the root of trust in the DNS root zone. Critically, this means that a domain in zone z can be authenticated only if *all* zones in the DNS hierarchy from the root to z support DNSSEC. Fortunately, there has been considerable work towards deployment near the top of the hierarchy. After the DNS root zone's key was created in July 2010, many top-level domains (TLDs) have become DNSSEC-enabled; recent studies [25, 42] have reported that 90.5% of generic TLDs (gTLDs, for example `.com`) and 47% of country-code TLDs (ccTLDs, for example `.nl`) are now DNSSEC-enabled.

Unfortunately, even though most TLDs now support DNSSEC, adoption by second-level domains (e.g., `example.com`) remains quite low [4, 8, 31, 42, 51]; our recent work [8] shows that only 0.6% of `.com` domains and 1.0% of `.org` domains have `DNSKEY` records[1] published. Worse, even among those domains that did attempt to deploy DNSSEC, we found significant levels of misconfiguration that resulted in incorrectly signed DNSSEC domains. For example, 31% of domains that support DNSSEC fail to publish all relevant records required for validation, meaning DNSSEC-enabled clients are unable to validate their records.

In this paper, we explore *why* DNSSEC deployment remains so small, and *why* there are high levels of misconfiguration of DNSSEC records. We focus primarily on DNS *registrars*—the entities that sell domain names and often operate the authoritative nameservers—to better understand how different registrar policies have led to the current state of affairs. Registrars play a critical role in the deployment of DNSSEC, as domains where the registrar is the DNS operator are entirely at the mercy of the registrar to support DNSSEC. Even for domains where the domain owner is the DNS operator, the registrar must still upload a `DS` record to the registry to complete the DNSSEC deployment.

Most prior studies of DNS registrar behavior have relied on active scans or large-scale data from zone files. Understanding what registrars allow and how they behave, however, requires a different form of measurement study: in this work, we examine large-scale, longitudinal DNS measurements and provide the first systematic study of the entire DNSSEC deployment process from a customer's perspective (by purchasing domains from leading domain name providers). Only by using this hands-on approach can we observe what domain owners experience. Overall, we purchased domains from the most popular 20 registrars (responsible for 54.3% of all `.com`, `.net`, and `.org` domains), as well as the 10 registrars that operate the large number of domains with `DNSKEY`s (covering 84.6% of such domains in `.com`, `.net`, and `.org`). In many cases, we find that we have to file support tickets or email the registrar in order to successfully deploy DNSSEC.

We couple our hands-on registrar measurements with 21 months of daily snapshots of DNSSEC records for *all* signed `.com`, `.net`, and `.org` second-level domains, 11 months of daily snapshots of DNSSEC-enabled `.nl` second-level domains, and seven months of daily snapshots of DNSSEC-enabled `.se` second-level domains. We choose `.nl` and `.se` as these have some of the highest levels of DNSSEC support among TLDs [12]. Looking at this historical data allows us to see how the policies we observe as a customer are correlated with each registrar's DNSSEC track record.

Individually, many of our results are anecdotal, but taken together, they paint a picture of why DNSSEC deployment remains at 1% of second-level domains, even though DNSSEC was originally proposed 20 years ago. Concretely, we observe that:

- The support for DNSSEC is skewed to a small number of registrars. Covering 50% of all `.com`, `.net`, and `.org` domains requires the top 26 registrars, but covering the top 50% of those domains that properly support DNSSEC requires *just two* registrars.
- Among the top 20 registrars, only three support DNSSEC when the registrar is the DNS operator. Only one (NameCheap) does so by default, and then only does so for some of their more expensive plans. The other two registrars either require the customer to opt-in (OVH) or to pay $35 per year (GoDaddy).
- Not all of the registrars we study support DNSSEC even when the owner is the DNS operator. Of those that do, 12 provide a web form for customers to upload `DS` records while seven require human intervention by contacting the registrar (e.g., via email or chat) to do so. We found most web forms to be inadequate (ten of the 12 registrars do no validation), emails to present obvious security vulnerabilities (four of the seven registrars did not verify the authenticity of the incoming email, and one even accepted an email from a *different* email address than the one that registered the domain), and web chat to be error-prone (one of the registrars accidentally installed our provided `DS` record on *someone else's* domain).
- Among the top 10 DNSSEC-supporting registrars, we find many of them are from the Netherlands or Sweden. Historically, both `.nl` and `.se` have provided financial incentives for registrars to support DNSSEC (with auditing for compliance), and we observe many registrars that properly support DNSSEC for these TLDs but not for others.
- Finally, we examine how third-party DNS operators such as Cloudflare interplay with DNSSEC. We find the process of deploying DNSSEC using these services to be error-prone, as customers must obtain a `DS` record from the third-party DNS operator and upload it to their registrar. This is done successfully by only 60% of domain owners.

Taken together, our results uncover many of the reasons why DNSSEC adoption has remained low, but provide ways forward to better incentivize DNSSEC deployment. We have been responsibly disclosing security issues to the registrars we interacted with, but there is a long way to go before DNSSEC deployment becomes simple, secure, and universally available to domain name owners. To allow other researchers and administrators to reproduce and extend our work, we publicly release all of our analysis code and data (where possible[2]) to the research community at

https://securepki.org

Outline The remainder of this paper is organized as follows. Section 2 provides background on DNSSEC and Section 3 gives an overview of related work. Section 4 provides more detail on the TLDs that we study and our daily scans. Section 5 explores the behavior and policies of the most popular registrars, while Section 6 examines the behavior and policies of the registrars with the largest number of DNSSEC-enabled domains. Section 7 examines third-party DNS operators such as Cloudflare, and Section 8 concludes.

2 BACKGROUND

In this section, we provide an overview of DNS, DNSSEC, and the various entities involved in the management of the DNS infrastructure.

[1] We review all relevant DNSSEC records in Section 2.

[2] Our `.com`, `.net`, `.org` and `.nl` zone files are collected under agreement with the zone operators; while we are not permitted to release this data, we provide links where other researchers can obtain access themselves. For the `.se` zone file, which is open data, we release it through OpenINTEL [38].

DNS and DNSSEC DNS is a distributed database that stores *records* that map domain names to values. For example, the IP address of `example.com` can be obtained by looking up the `A` record associated with the name `example.com`. DNS's logical namespace is divided into *zones*, each of which represents a contiguous set of domain names controlled by a single organization (e.g., the `example.com` zone may control names like `www.example.com`, but may further delegate `*.test.example.com`, thereby creating another zone).

Unfortunately, the original DNS protocol lacked many security features (e.g., authentication of records), making DNS vulnerable to numerous attacks, such as DNS hijacking [7, 27] and cache poisoning [40]. To defend against such threats, DNS Security Extensions (DNSSEC) [1–3, 16] were introduced in 1997. DNSSEC employs cryptographic mechanisms to verify records' *integrity* and *authenticity*. To achieve these goals, it is essential for each zone to provide three record types:

`DNSKEY` records are public keys. Zones sign DNS records with the corresponding private keys, and resolvers use the `DNSKEY` to verify these signatures. Each zone usually creates two `DNSKEY` records (called the KSK and ZSK) to sign DNS records: the private key of the KSK is used to sign `DNSKEY` records, and the private key of the ZSK is used to sign all other records.

`RRSIG` (Resource Record Signature) records are cryptographic signatures of other records signed using a `DNSKEY`'s corresponding private key. `RRSIG`s are applied to the set of all records associated with a given name and type. For instance, all `NS` records for `example.org` will be authenticated by a single `RRSIG`.

`DS` (Delegation Signer) records are essentially hashes of `DNSKEY`s that are uploaded to the parent zone by registrars. To ensure integrity, `DS` records also need to be signed by the parent zone (in the `RRSIG` of `DS` records). Hence DNSSEC can only function correctly when there are valid `DS` records from root to leaf, thereby establishing a chain of trust.

For more details on the correct validation of DNSSEC records, we refer the reader to our previous work [8].

Registry, Registrar, Reseller, and DNS Operator Since much of the focus of this paper is on the organizations that sell (and often host) domains, we provide a brief overview here. There are four kinds of organizations that play a role in the domain name registration process.

Registries are organizations that manage top-level domains (TLDs); each TLD has exactly one registry. The registry maintains the TLD *zone file* (the list of all registered names within that zone), and works with registrars to sell domain names to the public. For example, Verisign serves as the registry for `.com`. In many cases, registries do not have any direct contact with customers.[3]

Registrars are organizations that are accredited by ICANN[4] and certified by registries to sell domains to the public. They have direct access to the registry, which enables them to process new registrations.

Resellers are organizations that sell domain names, but are either not accredited (by ICANN) or certified (by a given TLD's registry). Typically, resellers partner with registrars in order to sell domain names, and relay all information through the registrar. For example, if a registrar wants to sell domains of a TLD that it is not accredited to access, it can partner with a registrar for that TLD, thereby becoming a reseller. Thus, a given organization can serve as a registrar for certain TLDs and a reseller for others.

DNS Operators are organizations that run authoritative DNS servers. Each domain name has a DNS operator, and a given operator may serve as the authoritative DNS server for multiple domains.

Whenever a registrar (or a reseller, via a registrar) sells a domain name, it must update the registry. It provides several pieces of information, but the two most crucial parts (and the parts of interest to this paper) are two DNS records that get inserted into the TLD zone file: the `NS` record set (the identity of the authoritative nameservers of the DNS operator, referred to as *delegation* of the domain) and, optionally, the `DS` record set (if the domain supports DNSSEC).

Throughout the remainder of the paper, we will refer to *registrars* as the entities that sell domain names; this should be interpreted as *registrar or reseller*. When the distinction becomes important, we will note it explicitly.

Registrar vs. external DNS operator Many registrars offer customers two options when purchasing a domain: (1) the customer can ask the registrar to serve as the authoritative nameserver (i.e., the registrar is the DNS operator), or (2) the customer can run their own authoritative nameserver for its new domain (i.e., the owner is the DNS operator). In the former case, the authoritative nameserver for the domain will be listed as one in the registrar's domain, and the registrar usually provides the customer with a web-based interface where they can modify the contents of their domain. For example, if a customer purchased `example.com` from Bluehost and chose registrar hosting, the `NS` record for `example.com` would be a machine in the `bluehost.com` domain.

For domains that support DNSSEC, the responsibility for maintaining DNSSEC records (e.g., `DNSKEY`s, `RRSIG`s, `DS` records) falls on the DNS operator. If this is the registrar, and if the registrar supports DNSSEC and manages DNSSEC correctly, it is the registrar who will generate `DNSKEY`s and `RRSIG`s for DNS records. If this is the owner, the owner must generate and maintain all DNSSEC records.

Uploading `DS` records If a domain operator wishes to support DNSSEC, a `DS` record for the domain must be uploaded to the registry in order to establish a chain of trust. However, only registrars can upload `DS` records to the registry.

Thus, if the domain's DNS operator is the registrar, they can simply upload the `DS` record by directly accessing the registry. Unfortunately, if the domain's DNS operator is the owner, the situation is more complicated because the owner must somehow convey the `DS` record to the registrar. To this end, a registrar may provide customers with a web-based interface to submit `DS` records, or may allow customers to transmit `DS` records via an out-of-band mechanism such as by e-mail or telephone. Moreover, if a registrar does not support

[3] A full list of all TLDs and registries can be viewed at https://www.icann.org/resources/pages/listing-2012-02-25-en.

[4] ccTLD registries often have their own accreditation requirements.

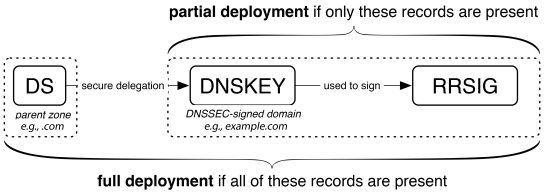

partial deployment if only these records are present
DS
parent zone e.g., .com
secure delegation
DNSKEY
DNSSEC-signed domain e.g., example.com
used to sign
RRSIG
full deployment if all of these records are present

Figure 1: A diagram of full deployment vs. partial deployment of DNSSEC by a domain. It is important to note that partially deployed domains *do not* properly validate, as they are missing DS records.

any methods for customers to upload DS records, the domain *cannot* support DNSSEC as the domain's chain of trust will be broken due to the missing DS record. Hence, the registrars' policy for uploading DS records to the registry plays a crucial role in whether domains purchased through that registrar can support DNSSEC.

For DNSSEC to function properly, it is essential that a complete chain of trust (RRSIG, DNSKEY, and DS record) exists. Unfortunately, this is often not the case. In this paper we distinguish between *partial* and *full* DNSSEC deployments: A domain that publishes DNSKEY and RRSIGs and uploads DS records is called *fully deployed* DNSSEC, while a domain that has DNSKEYs and RRSIGs but that does not upload DS record (and therefore cannot be validated) is called *partially deployed* DNSSEC as illustrated in Figure 1.

From a security perspective, a partial deployment has limited value, since there is no way to verify DNSSEC signatures.[5] This makes it all the more important that DNSSEC deployment is done correctly, as any missing link the chain would prevent a domain's records from being validated. In the remainder of this paper, we study key points in the domain registration and operation process where DNSSEC deployment breaks down and missing functionality leads to partial deployments.

Automating DS uploads Uploading DS records manually or out-of-band can be error-prone[6] and can open up security vulnerabilities (e.g., if an attacker can convince a registrar to accept an incorrect DS record). To address these problems, the CDNSKEY (child DNSKEY) and CDS (child DS) record types were introduced in 2014 [28, 48]. In brief, these records automate DNSSEC delegation trust maintenance by allowing an in-band mechanism for transmitting and updating DS records. If a customer wants to replace its DS records with a new one, the customer publishes a CDNSKEY or CDS record (or both) with its RRSIG(s).[7] Once the registry detects the presence of the CDNSKEY or CDS record in one of its customers' domains, it authenticates the record and then updates the DS record in the registry.[8] Once the old DS record is replaced with new one, the customer can remove the CDNSKEY and CDS records from their zone configuration settings.[9] Unfortunately, CDS and CDNSKEY have thus far seen very little adoption by registries, leaving us with the manual processes described above.

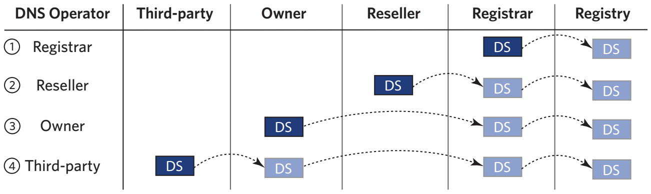


Figure 2: Steps in the process for inserting a DS record into the registry when the DNS operator is (1) a registrar, (2) a reseller, (3) the owner, and (4) a third-party. In each case, it is the DNS operator who actually generates the DS record; it then has to be handed off (potentially up to three times) to make it to the registry. Not shown is the case where a customer buys a domain from a reseller and uses a third-party DNS operator (adding yet another handoff).

Third-party DNS operators Recently, we have observed the growth in popularity of organizations that provide management of DNS records, but do not serve as registrars; we refer to these organizations as *third-party DNS operators*. These organizations serve as authoritative nameservers for customers, manage DNS records, and often provide security services such as distributed denial-of-service (DDoS) prevention. One prominent example of such a service is Cloudflare. With a third-party DNS operator, properly deploying DNSSEC is even more complicated, as it is the third-party who generates DNSKEYs and RRSIGs. Specifically, if the registry does not support CDS or CDNSKEY (which comprises all but one registrar at the time of writing), the third-party DNS operator does not have the authority to ask the registrar to upload a DS record; it must instead ask the customer to relay a DS record to the registrar. As we will see later in the paper, this convoluted process plays a role in why DNSSEC adoption remains low.

As a summary, Figure 2 shows how the process for inserting DS records into the registry varies when the DNS operator is the registrar, a reseller, the owner, and a third-party.

3 RELATED WORK

In this section, we discuss studies of DNSSEC deployment and DNS registrars.

DNSSEC deployment We first discuss related studies of DNSSEC deployment, covering both server-side (DNSSEC-enabled domain) and client-side (DNS resolver) studies.

[5] DNSKEYs for a domain could be delivered out-of-band even though the domain does not have a DS record, enabling an RRSIG to be validated by the DNSKEYs. However this is not the intended mechanism for deployment of DNSSEC.

[6] An anecdotal example is that the DS record for isoc.org was found to be incorrect at the 38'th ICANN meeting in 2010 due to a transcription error made when the DS record was *manually* entered while dictated over a phone. This was discovered shortly before the press conference announcing the ISOC (The Internet Society) DNSSEC deployment by one of our authors and fixed immediately.

[7] Since the DS record can be generated using the CDNSKEY, publishing both a CDS and CDNSKEY is redundant but not incorrect.

[8] The operational methods for the registry to notice the CDNSKEY and CDS record may differ; the registry can use tools that periodically check each of its customers' domains to see if they have a CDS and CDNSKEY record, or it can provide a web interface for the customer to signal the parent zone to fetch the records.

[9] Using CDS and CDNSKEY records, a customer can also request the registry to remove the current DS record by setting the algorithm number of CDS or CDNSKEY to zero.

Server-side support: DNSSEC has attracted much attention from both research and industrial stakeholders. In early stage of deployment of DNSSEC, several studies measured the operational status of DNSSEC [36, 37] or operational challenges for wide deployments [50]. More recently, studies found that 89% of generic TLDs (gTLDs) and 47% of country-code TLDs (ccTLDs) supported DNSSEC in 2016 [42], and that most major DNS server software supports DNSSEC [14] as well. Additionally, a number of free tools exist to help system administrators properly deploy DNSSEC, such as DNSSEC Debugger [11] and DNSViz [15]. Recent studies have also found, however, that DNSSEC adoption for second-level domains remains low. Our recent study [8] showed that DNSSEC deployment is rare in the second-level domains (roughly 1% of .com, .net and .org domains), but is growing. Some of the studies have focused on the misconfigurations of DNSSEC: Adrichem et al. [45] analyzed a sample of second-level domains and similarly found that 4% exhibited misconfigurations. Dai et al. [10] also found that 19% of second-level domains from the Alexa Top-1M could not establish a chain of trust from the root. One of the common causes was the failure to upload DS records; nearly 30% of .com, .net, and .org domains do not properly upload DS records even though they have DNSKEYs and RRSIGs [8].

Our work complements these pieces of prior work, as they measured the current status of the low DNSSEC deployment. In contrast, we focus primarily on why DNSSEC deployment remains so small and why there are high levels of DNSSEC misconfiguration. Our approach is to purchase domains from popular registrars and resellers and then examine the process of configuring DNSSEC for these domains. We also use considerably broader datasets including all second-level domains from three gTLDs (.com, .net, and .org) and two ccTLDs (.nl and .se).

Client-side support: To measure client-side support for DNSSEC, studies have used advertisements in embedded webpages to cause clients to make DNS requests [4, 31, 42]; their results showed that about 26% of clients use DNSSEC-validating resolvers, but they retry querying to non-validating resolvers if validation fails (defeating the point of DNSSEC). Using a similar technique, Lian et al. [31] showed that 1% of clients failed to resolve DNSSEC-enabled domains at all, while only 3% of clients successfully detected DNSSEC-signed domains with broken signatures. Finally, we used the Luminati proxy network [7] to induce DNS requests; we found that 83% of clients use a resolver that requests DNSSEC records, but only 12% of them actually bother to validate the response [8].

Registrars Another line of work has examined the role of registrars in the deployment of DNSSEC. Recent work has found that many second-level domains with DNSKEYs fail to upload a DS record [8, 45, 46], suggesting that certain registrars may incorrectly deploy DNSSEC. Some studies focused on the process of enabling DNSSEC. The Internet Society [24], for example, stressed the role of registrars in enabling DNSSEC, publishing a list of registrars that are known to support DNSSEC. The report by York [49] also pointed out that the low DNSSEC adoption rate is due to its complexity, and the most effective way to accelerate its deployment is to simplify the process of signing a domain, such as enabling DNSSEC *by default*.

TLD	Measurement Period	Domains	
		Number	Percent with DNSKEY
.com	2015-03-01 – 2016-12-31	118,147,199	0.7%
.net	2015-03-01 – 2016-12-31	13,773,903	1.0%
.org	2015-03-01 – 2016-12-31	9,682,750	1.1%
.nl	2016-02-09 – 2016-12-31	5,674,208	51.6%
.se	2016-06-07 – 2016-12-31	1,388,372	46.7%

Table 1: Overview of the datasets that we use for this study. The number of overall domains and percentage that have DNSKEYs published is as-of December 31, 2016.

On the other hand, several studies examined ways to increase DNSSEC deployment, primarily through financial incentives [9, 18, 20, 21]. Collectively, they showed how financial incentives for a registrar can lead to higher levels of DNSSEC adoption. Unfortunately, financial incentives are only offered by a small number of ccTLDs (e.g., .nl, .se, and .cz), and this approach has yet to expand to other TLDs.

There are also several attempts to make it easier for third-party DNS operators to use DNSSEC. For example, Cloudflare and CIRA, the registry operator for .ca, are working on a draft standard [13, 29], which essentially would allow the third-party DNS operator to identify the registrars and communicate with them directly to enable or bootstrap DNSSEC using a REST-based [41] protocol (without any effort from registrants).

4 DATASETS

In this section, we present the datasets that we use in this study and briefly examine the overall support for DNSSEC to help motivate the subsequent analysis.

4.1 TLD zone files

Our goal is to understand how different registrars have affected DNSSEC's deployment. To do so, we rely on scans from five TLDs, provided by OpenINTEL [38, 47]: the .com, .net, and .org generic TLDs and .se and .nl country-code TLDs. We choose .com, .net, and .org because they are some of the largest TLDs, and .se and .nl because they are TLDs that show some of the highest rates of DNSSEC deployment [12].

Our dataset contains daily scans of all second-level domains in these five TLDs. Because of the way the data was collected, our datasets *start* at different times: .com, .net, and .org start on March 1st, 2015, .nl starts on February 9th, 2016, and .se starts on June 7th, 2016. However, all end on December 31st, 2016. Table 1 shows a summary.

Each daily scan contains a number of pieces of information for each second-level domain in the zone: *First*, each daily scan contains the Nameserver (NS) record(s) for each domain, containing the authoritative nameserver(s) of the DNS operator. *Second*, each scan contains the Delegation Signer (DS) record for each domain, if it exists. *Third*, each scan contains the DNSKEY and DNSKEY RRSIGs for the domain, if any exist. Taken together, the scans represent one of the most comprehensive sets of DNSSEC observations.

4.2 Identifying the DNS operator

To understand how different registrars behave, we first need to know who manages each domain. One possible option is to use WHOIS

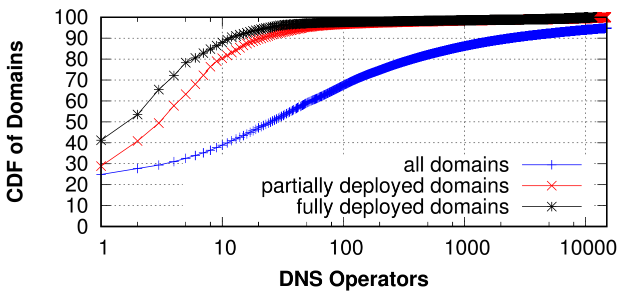


Figure 3: Cumulative distribution of `.com`, `.org`, and `.net` domains by DNS operators; shown are all, partially deployed, and fully deployed domains. We can see that 26 DNS operators are necessary to cover over 50% of all domains. However, only four DNS operators are needed to cover 57% partially deployed domains, and only two DNS operators cover 54% of fully deployed domains.

data to obtain registrar information; however the WHOIS infrastructure is distributed across registrars and resellers, is heavily rate-limited, and lacks a consistent schema [30]. Moreover, a domain could be managed by a reseller, but the WHOIS information may be served by its partner registrar; this would conflate the behavior of the reseller and the registrar.

Instead, we rely on the authoritative nameserver for each domain (from the NS record), which is present in our data sets, to indicate the DNS operator. The identity of the authoritative nameserver serves our purpose well, as the domain name of the authoritative nameserver typically identifies the organization that is actually managing the name. Specifically, we group domains if they share the same second-level domain in their NS records. For example, if two different domains have NS records of `ns01.domaincontrol.com` and `ns02.domaincontrol.com`, we group these under the DNS operator domaincontrol.com (owned by GoDaddy).

4.3 Overall DNSSEC support

We begin by quickly examining how DNSSEC is deployed across different TLDs. Table 1 shows the number of domains in each of the TLDs that we study as well as the percentage of domains that have DNSKEYs; we can immediately observe that the overall DNSSEC deployment rate in the three generic TLDs is quite low—in line with recent studies [8]—but that the percentage is much higher in `.nl` and `.se`. We explore this trend in more detail in the subsequent sections.

Next, we examine how the domains that attempt to deploy DNSSEC are distributed across registrars. Recall that to correctly deploy DNSSEC, a domain must (a) publish DNSKEYs and RRSIGs for all records, and (b) must have a DS record in the TLD zone. Thus, we examine how three subsets of the domains are distributed across registrars: (1) all domains, (2) partially deployed domains, and (3) fully deployed domains.

Figure 3 presents a cumulative distribution function (CDF) of the number of all `.com`, `.net`, and `.org` domains per registrar from the December 31, 2016 snapshot. We make two observations. *First*, we observe that partially and fully deployed domains show a much different distribution across registrars than the overall data set: 26 registrars are necessary to cover 50% of all domains, but only four registrars are necessary to cover 50% of the partially deployed domains, and only *two* registrars are necessary to cover 50% of the fully deployed domains. *Second*, the small number of registrars that host an outsized proportion of DNSSEC domains suggests that many popular registrars fail to support DNSSEC. For example, the overlap between the 25 most popular registrars overall, and the 25 most popular registrars among fully deployed domains is only three registrars, which paints a bleak picture of DNSSEC support among registrars. Hence, to better understand why and how DNSSEC is deployed, we turn our attention to study each registrar's DNSSEC deployment policy and its impact.

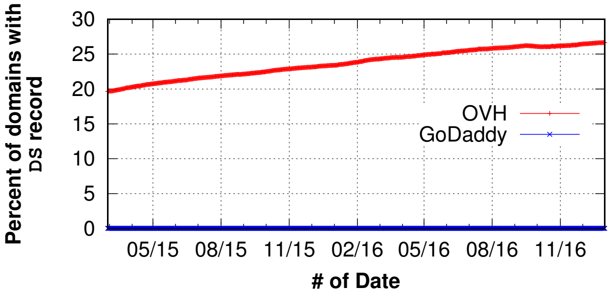


Figure 4: The percentage of all merged domains with DNSKEY and DS records for OVH (free DNSSEC with customer opt-in) GoDaddy (paid DNSSEC). OVH shows a much more robust deployment for DNSSEC.

5 POPULAR REGISTRARS

We begin by examining how the most popular DNS registrars support DNSSEC. To do so, we register domains ourselves and attempt to deploy DNSSEC, as well as look at all domains operated by the registrar to look for patterns.

5.1 Methodology

To understand how different registrars support DNSSEC, we need to register domains and try to deploy DNSSEC as a customer would. We focus on the most popular 31 DNS operators that serves DNS for the most domains across our datasets, which collectively cover 54.3% of `.com`, `.net`, and `.org` domains in the TLD zone files. For each of these 31 DNS operators, we proceed as follows:

(1) We first check whether the DNS operator is a registrar. We found nine are domain parking services[10] and two are third-party DNS operators. We do not study the domain parking services further[11]. The two third-party DNS operators, DNSPod and Cloudflare, are studied in Section 7. For the others, we purchase a `.com` domain.

(2) Next, we examine whether our purchased domain supports DNSSEC by default, or if DNSSEC is an opt-in feature. If

[10] Domain parking services are services that hold a given domain, but do not provide any services (e.g., a website). Often, such parking services simply serve ads as a way to profit from parked domains.

[11] These DNS operators are parking services: Ename (1,604,676 domains), BuyDomains (1,190,973), SedoParking (1,186,838), DomainNameSales (1,081,944), CashParking (1,012,114), HugeDomains (807,607), ParkingCrew (660,081), RookMedia (619,254), as well as the advertising domain `ztomy.com` (631,381 domains).

Registrar	Domains		Registrar DNS operator		Owner DNS operator				
(Domain of Auth. Nameservers)	All	with	DNSSEC	DNSSEC	DNSSEC	DS upload		DS Validation	
		DNSKEY	default	opt-in	support	Web	Email	DNSKEY	Email
GoDaddy (`domaincontrol.com`)	37,652,477	8,139	✗	●	●	●	-	✗	-
Alibaba (`hichina.com`)	4,292,138	3	✗	✗	✗	-	-	-	-
1AND1 (`1and1`)[13]	3,802,824	0	✗	✗	✗	-	-	-	-
Network Solution (`worldnic.com`)	2,534,673	0	✗	✗	✗	-	-	-	-
eNom (`name-services.com`)	2,525,828	10	✗	✗	●	✗	●	✗	●
Bluehost (`bluehost.com`)	2,066,503	0	✗	✗	✗	-	-	-	-
NameCheap (`r...-servers.com`)	1,963,717	13,232	▲	-	●	●	-	✗	-
WIX (`wixdns.net`)[14]	1,887,139	0	✗	✗	✗	-	-	-	-
HostGator (`hostgator.com`)	1,849,735	0	✗	✗	●	●	-	✗	-
NameBright (`namebrightdns.com`)	1,823,823	0	✗	✗	●	✗	●	✗	▲
register.com (`register.com`)	1,311,969	0	✗	✗	✗	-	-	-	-
OVH (`ovh.net`)	1,228,578	319,580	✗	●	●	●	-	●	-
DreamHost (`dreamhost.com`)	1,117,902	0	✗	✗	●	✗	●	●	▲
WordPress (`wordpress.com`)	888,174	3	✗	✗	✗	-	-	-	-
Amazon (`aws-dns`)[15]	865,065	0	✗	✗	●	●	-	▲	-
Xinnet (`xincache.com`)	836,293	0	✗	✗	✗	-	-	-	-
Google (`googledomains.com`)	813,945	1,945[12]	✗	✗	●	●	-	✗	-
123-reg (`123-reg.co.uk`)	720,435	1	✗	✗	●	●	-	✗	-
Yahoo (`yahoo.com`)	690,823	0	✗	✗	✗	-	-	-	-
Rightside (`name.com`)	663,616	0	✗	✗	●	●	-	✗	-

Table 2: Table showing the results of our study of registering domains using the 20 registrars among the top 31 DNS operators. ● means that a DNS operator supports DNSSEC and ✗ means that a DNS operator fails to support DNSSEC. If DNS operators support uploading a `DS` record via web interface, we do not email them to ask if they accept a `DS` record by email (hence the –). Only three them support DNSSEC for domains they manage, and only one of them provides DNSSEC by default for these domains (NameCheap only supports DNSSEC by default for certain plans, hence the ▲ [35]). Only 11 of the registrars support DNSSEC for external nameservers, eight providing web-based forms for uploading `DS` records and three requiring emails with `DS` records; only two of these actually validate the provided `DS` records. Of the three that require emails, two of them do not verify the validity of the incoming email (hence the ▲).

we are unable to find a way to do so, we email the registrar to ask if they support DNSSEC.

(3) If we manage to enable DNSSEC, we verify that the registrar correctly deploys all DNSSEC records by checking the existence of a `DS` record, its accordance with our `DNSKEY`, and the validity of the `RRSIG`s.

(4) We then disable the registrar hosting, and switch our domain to use an external nameserver we control. Our nameserver correctly publishes all DNSSEC records.

(5) Next, we examine whether the registrar allows us to upload a `DS` record via the web interface. If we are unable to find this feature, we email the registrar to ask whether we can provide a `DS` record some other way.

(6) If we are able to supply a `DS` record, we verify that our domain correctly deploys all DNSSEC records.

(7) Next, if possible, we upload a `DS` record that does not match our published `DNSKEY`, to check if the registrar validates supplied `DS` records.

(8) Finally, if a registrar accepts a `DS` record via e-mail, we send it with a different email address (one that was *not* used to register the domain) to see whether they check that the owner of the domain is sending the record.

Table 2 summarizes the results of this experiment. We make a number of observations below.

5.2 Registrar as a DNS operator

We first focus on what happens when we use the registrar as the DNS operator for our domain. Surprisingly, only three registrars (GoDaddy, NameCheap, and OVH) out of the 20 we studied support DNSSEC *at all* when they are the DNS operator. This situation is unfortunate, as these cases present an easy path to DNSSEC deployment, as the registrar has full control over the domain and could create `DNSKEY`s, `RRSIG`s, and upload `DS` records all on its own.

Even more alarming, among the three registrars that do support DNSSEC when they are the DNS operator, we find that *only* NameCheap enables DNSSEC by default, and they only do so for some of their DNS plans. In particular, NameCheap offers six different plans, only three of which support DNSSEC [35]. NameCheap's free plan, FreeDNS, does not support DNSSEC, partially explaining the low fraction of signed domains. The other two registrars that support DNSSEC also have different policies: GoDaddy provides

[12] DNSSEC was only available to Google Clould DNS customers participating in Alpha release [22].

[13] The nameservers from 1AND1 Internet (also hosting provider) share the same second level domain, but are dispersed over the different ccTLDs; we instead group them easily when the second level of `NS` record is "1and1."

[14] Wix does not allow an owner to use external nameservers.

[15] The nameservers from `Amazon Web Services` have a specific naming convention; awsdns-*id*.TLD (e.g., `awsdns-13.net`), which allows grouping them by using a regular expression.

DNSSEC as a premium package (at a cost of $35 per year), while OVH provides DNSSEC for free but *only* if the customer explicitly opts in.

From our December 31st, 2016 snapshot, we observe that 25.9% of domains from OVH, 0.59% of domains from NameCheap, and 0.02% of domains from GoDaddy deploy DNSSEC. As seen in Figure 4, to further explore the behavior of customers with these registrars, we compare the historic fraction of OVH and GoDaddy domains that have DNSKEYs and DS records.Unsurprisingly, we observe that OVH's overall DNSSEC adoption ratio is significantly higher and growing. However, GoDaddy's fraction of DNSSEC-support domains is minuscule by comparison: only 7,841 of their domains (0.02%) domains have a DNSKEY and DS record in our latest snapshot. Thus, we can immediately see the crucial role that free and default support for DNSSEC can have in successfully deploying DNSSEC.

We contacted an administrator of one of the registrars to inquire why they choose to make DNSSEC an opt-in feature rather than a default, and why DNSSEC adoption was still low. They reported three potential reasons: (1) the layout of their purchase page, which placed the (free) option for DNSSEC on the same page as other (paid) options; (2) misconceptions concerning DNSSEC among their customers, who believe that DNSSEC causes issues for domain name resolution for non-DNSSEC supporting clients; and (3) DNS resolution performance, where requests for records in domains that support DNSSEC may take longer to resolve.

5.3 Owner as a DNS operator

Next, we explore how registrars support DNSSEC if the owner acts as the DNS operator (e.g., by hosting their own nameserver). We find that only 11 of the 20 registrars listed in Table 2 support DNSSEC for such domains (beyond the three discussed above, this includes eNom, HostGator, NameBright, DreamHost, Amazon, Google, 123-Reg, and Rightside).

Interestingly, only three registrars in this group of twenty (Amazon, Google, and Rightside) present a DS upload menu on their site when a user switches to an external nameserver. 123-reg requires customers to submit a support ticket to upload DS records, and they must attach the desired DS record to the ticket. Similarly, HostGator's customers need to have a live web chat with an agent to copy/paste the DS record into the chat window. While all of 123-reg's and HostGator's webpages are HTTPS-secured—at least ensuring that the DS record is uploaded through a secure channel—these approaches are manual processes that present numerous opportunities for error.[16]

The remaining registrars do not provide any details on their webpages for users who want to enable DNSSEC on domains operated by a third party. We contacted each registrar to ask whether they support DNSSEC in this case, and if so, how we can send the DS record to them. We find that three of these are willing to support DNSSEC, and all of them require that the DS record be submitted via email. These case studies are particularly disappointing, as communicating DS records over email opens up security vulnerabilities due to the insecurity of email communication[17].

DS record validation We now turn our attention to see how these registrars validate DS records once they have been uploaded. As the DS record is a core piece of the trust chain, the uploading process must be carefully considered. If a domain owner uploads an incorrect DS record by mistake (e.g., the wrong record, or an incorrectly formatted record), the domain will fail to validate, potentially preventing clients from communicating with the domain.

We first check whether the registrars validate the uploaded DS record to ensure it is the hash of the domain's DNSKEY. We observe that only two registrars (OVH and DreamHost) out of the 11 registrars that support DNSSEC when the owner is the DNS operator correctly validated the DS record before accepting it. Interestingly, Amazon allows domain owners to upload their DNSKEY instead of the DS record (and generates the DS record by themselves), which is not perfect, as a domain owner could upload a different DNSKEY than the one that they are actually serving. The remaining registrars all allow us to publish arbitrary data as DS records.

Finally, we tested whether the registrars that require emailed DS records would accept an updated DS record without validating the email (as email headers can be forged). We found that two of the three registrars that require emailed DS records did not attempt to verify the authenticity of the email, meaning an attacker who wished to take control of a victim domain could simply forge an email to these registrars. We have contacted these two registrars to inform them of this security vulnerability.

5.4 Summary

In summary, we observe that DNSSEC support is quite poor among the popular registrars: only three of 20 registrars support DNSSEC for registrar-hosted domains, and only 11 of them support DNSSEC for externally hosted domains. Of the three that do support DNSSEC for registrar-hosted domains, only one is by default and even that is only for certain plans; one of the other two even charges domain owners for the service. Finally, we observe that only two providers reject a DS record that does not match the DNSKEY served from the external nameservers. The others, however, accept *anything* as a DS record so that a simple copy/paste error could make the entire zone fail to validate (and thus fail to resolve) by DNSSEC-validating resolvers.

6 DNSSEC-SUPPORTING REGISTRARS

Measuring the most popular registrars, as we did above, provides an overall view of support for DNSSEC. To better understand how registrars that *do* support DNSSEC behave, we now repeat the same experiment as above but focus on the registrars that have the largest number of domains with DNSKEYs. Specifically, we first extract .com, .net, and .org second-level domains that publish at least one DNSKEY record from our latest snapshot (December 31st, 2016). Next, we group them by registrars as we did before. We then focus on the 12 most popular nameserver domains, representing 10

[16] As an anecdotal example, we found that one of our DS records was accidentally installed by the registrar on *someone else's* domain due to a mistake by the customer service agent with whom we were chatting. This mistake was fixed right after we raised the issue, but potentially made the other domain inaccessible to DNSSEC-aware clients while the DS record was present.

[17] Ironically, deploying DNSSEC correctly can improve email security using STARTTLS [23] and DANE [43].

Registrar	Domains	Registrar DNS operator			Owner DNS operator				
(Domain of Authoritative Nameservers)	w/ DNSKEY	DNSSEC	Publish		DNSSEC	DS Upload		DS Validation	
		default	DNSKEY	DS	support	Web	E-mail	DNSKEY	Email
OVH (ovh.net)	319,580	✗	●	●	●	●	-	●	-
Loopia (loopia.se)	131,726	●	●	▲	●	✗	●	✗	●
DomainNameShop (hyp.net)	94,084	●	●	●	●	●	-	✗	-
TransIP (transip.net)	91,103	●	●	●	●	●	-	✗	-
MeshDigital (domainmonster.com)	60,425	●	●	✗	●	✗	●	✗	▲
OVH (anycast.me)	52,381	✗	●	●	●	●	-	●	-
TransIP (transip.nl)	47,007	●	●	●	●	●	-	✗	-
Binero (binero.se)	44,650	●	●	●	●	✗	●	✗	✗
KPN (is.nl)	15,738	●	●	▲	✗	-	-	-	-
PCExtreme (pcextreme.nl)	14,967	●	●	●	●	✗	●	▲	▲
Antagonist (webhostingserver.nl)	14,806	●	●	●	✗	-	-	-	-
NameCheap (registrar-servers.com)	13,232	●	●	▲	●	●	-	✗	-

Table 3: Table showing the 10 most popular unique registrars in terms of number of domains for which they serve as DNS operator (and their 12 nameserver domains) for domains that publish DNSKEYs in .com, .net, and .org; Most support DNSSEC by default, but four of them support DNSSEC partially depending on the TLD zone (indicated as ▲).

different registrars[18]; they collectively cover 81.6% of the domains with DNSKEYs.[19]

6.1 Registrar policies

Table 3 shows the results of this experiment in a format similar to Table 2. At a first glance, we notice that 9 of 10 registrars enable DNSSEC by default; the only exception is OVH (previously studied). This high level of DNSSEC-by-default behavior for registrars with high levels of DNSSEC deployment is not surprising, but shows the crucial role that default support can play. Second, we observe that a few registrars publish DNSKEYs and RRSIGs for all domains, but only publish DS records for some domains (marked ▲ in the DS column). Taking a closer look at these registrars, we find that they only publish DS records for certain TLDs: Loopia only publishes DS records for .se domains, KPN only publishes DS records for .nl domains, and NameCheap only publishes DS records for .com and .net domains. We emailed all three registrars to inquire why they fail to publish DS records for some TLDs, but were unable to get a precise explanation of this behavior.[20] We observe this partial-support behavior to an even larger degree with MeshDigital, which publishes DNSKEYs and RRSIGs for their domains but fails to upload a DS record for almost all domains for which they are the DNS operator; this is in line with recent study [8] showing that only 4 domains out of 60,425 have a DS record. We find the failure to upload DS records by these four registrars curious, as domains where DS records are not published cannot be validated, foregoing the security that DNSSEC provides.

Next, we examine how well these registrars support DNSSEC when the domain owners (registrants) themselves are the DNS operator. Overall, we find similar behavior to the popular registrars examined in the previous section: while a higher fraction of these registrars support DNSSEC when the owner is the DNS operator (8 of 10 registrars do so), only four of them allow for web-based uploads, while the other four require unauthenticated emails with DS records. In fact, in a discussion with an administrator of one of the registrars, we were informed that their decision not to support DS records for external nameservers is intentional and meant to prevent potential errors when domain owners copy and paste the DS record manually (i.e., avoiding cases where domain owners accidentally upload an incorrect DS record and make their entire zone unavailable to DNSSEC-supporting clients). This demonstrates that at least one registrar is aware that current DS record upload mechanisms are error-prone.

6.2 Registrars vs. resellers

So far, we have observed that different registrars have different DNSSEC policies. Now we dig deeper and attempt to explain *why* various registrars have chosen their policies and quantify their effect on DNSSEC deployment. To this end, we perform a longitudinal study for each registrar to answer questions that include: (1) how does different DNSSEC policies affect deployment of DNSSEC? (2) do registrars have consistent DNSSEC policies for domains in different TLDs? and (3) if they have different policies, why do they differ?

Recall that a given registrar may serve as a registrar for certain TLDs (e.g., is accredited to update the registry), may serve as a reseller for others (e.g., works with a partner registrar to facilitate registration), and may simply not support other TLDs. Thus, if a given registrar is a reseller and wishes to support DNSSEC, *both* it and its partner registrar must support DNSSEC (i.e., it must generate DNSKEYs and RRSIGs, and its partner registrar must support the uploading of DS records). It is therefore crucial to understand the role that registrars play for various TLDs to understand their behavior.

To answer these questions, we performed a small survey. We asked the 10 registrars whether they support each of the five TLDs we studied, and asked them for the identity of the third-party registrars

[18] Two of the registrars own multiple domains used to host DNS servers: OVH owns ovh.net and anycast.me, and TransIP owns transip.net and transip.nl.

[19] Note that having a DNSKEY record published does not necessarily mean that the domain has correctly deployed DNSSEC; e.g., the corresponding DS records might not be published in the parent zone.

[20] For example, one of the registrars repeatedly said that they do not sign domains automatically for all TLDs at the current time, but might starting doing so in the future.

Domain of Authoritative Nameservers	DNS Operator	Registrar				
		`.com`	`.org`	`.net`	`.nl`	`.se`
`ovh.net` & `anycast.me`	OVH	OVH	OVH	OVH	OVH	OVH
`domaincontrol.com`	GoDaddy	GoDaddy	GoDaddy	GoDaddy	GoDaddy	GoDaddy
`domainmonster.com`	Mesh Digital	Mesh Digital	Mesh Digital	Mesh Digital	Mesh Digital	*No support*
`hyp.net`	DomainNameShop	DomainNameShop	DomainNameShop	DomainNameShop	*No support*	*No support*
`transip.nl` & `.net`	TransIP	TransIP	TransIP	TransIP	TransIP	Key Systems
`registrar-servers.com`	NameCheap	NameCheap	eNom	NameCheap	*No support*	*No support*
`binero.se`	Binero	Binero	Binero	Binero	*No support*	Binero
`pcextremenl.nl`	PCExtreme	Open Provider	Open Provider	Open Provider	PCExtreme	*No support*
`webhostingserver.nl`	Antagonist	Open Provider	Open Provider	Open Provider	Antagonist	*No support*
`loopia.se`	Loopia	Ascio	Ascio	Ascio	Ascio	Loopia
`is.nl`	KPN	Ascio	Ascio	Ascio	KPN	Open Provider

Table 4: Table showing the 11 DNS operators that support DNSSEC for hosted domains, and the registrar they use for various TLDs. In many cases, these operators are registrars themselves (white background); in other cases, these operators are resellers and use registrars (shown with grey background); finally, some DNS operators do not support certain TLDs (shown with red background).

(if one is used) for each TLD. Table 4 shows the results of this survey, listing whether each registrar serves as a registrar or a reseller for each of the TLDs. As we can see, some registrars are registrars for all TLDs (e.g., OVH and GoDaddy), while others are resellers for various TLDs; additionally, a number of the registrars do not support the `.nl` and `.se` TLDs at all.

6.3 Financial incentives

A common criticism of DNSSEC has been the slow deployment. One potential way registries could incentivize greater DNSSEC deployment is by providing discounts for domains that properly support DNSSEC. We now focus on the `.nl` and `.se` TLDs, which are the TLDs with the largest fraction of DNSSEC-enabled domains [12] and which provide registrars a discount for DNSSEC-enabled domains. We compare the registrar behavior w.r.t `.nl` and `.se` to behavior w.r.t `.com`, `.net`, and `.org` to explore whether financial incentives serve as a useful tool to incentivize DNSSEC deployment.

For `.nl` domains, a registrar receives a €0.28 (∼$0.30) discount every year for a `.nl` domain if it is correctly DNSSEC signed [9, 44]. Similarly, for `.se` domains, a registrar used to receive a 10 SEK (∼$1.10) discount every year for a correctly-signed `.se` domain [18] (it is unclear whether this discount is still active at this time). To facilitate these discounts, every DNSSEC-signed `.nl` and `.se` second-level domain is tested every day by the registry to ensure it has correct `DNSKEY`s, `RRSIG`s, and `DS` records [9, 39]. Registrars that have many incorrectly configured DNSSEC records[21] may not receive future discounts.

To study how registrars behave when DNSSEC is incentivized, we focus on the six registrars that are from the Netherlands (TransIP, PCExtreme, Antagonist, and KPN) and Sweden (Loopia and Binero). We group registrars that have similar behavior together.

KPN and Loopia Figure 5 shows the fraction of the domains with `DNSKEY` and `DS` records. Interestingly, we find that Loopia only supports DNSSEC for `.se` domains, and KPN only supports DNSSEC for `.nl` domains (in fact, *none* of the domains that they are the DNS operator for in other TLDs have DNSSEC deployed). There could be two potential reasons why KPN and Loopia support DNSSEC only for `.nl` and `.se` domains, respectively, and not the others: (1) their registrar partners might not support DNSSEC, or (2) they enable DNSSEC only if there is a financial incentive.

To test our hypothesis, we purchased a `.com` domain from Loopia and asked them to serve as the DNS operator. We observed that Loopia automatically published `DNSKEY`s and `RRSIG` for our domain, but did not upload a `DS` record to the `.com` registry (thereby making DNSSEC for our domain only partially deployed). However, when we registered a `.com` domain through Loopia and used an external nameserver, Loopia was able to upload a `DS` record for our external domain. We repeated the same experiment with KPN and found exactly the same behavior: they published `DNSKEY`s and `RRSIG`s by default, but only uploaded a `DS` record after we requested it. The take-away from this experiment is that financial incentives are likely to play a role in registrar policies: the registrars clearly have the capability to upload `DS` records, but only do so by default for domains where there is a financial incentive.

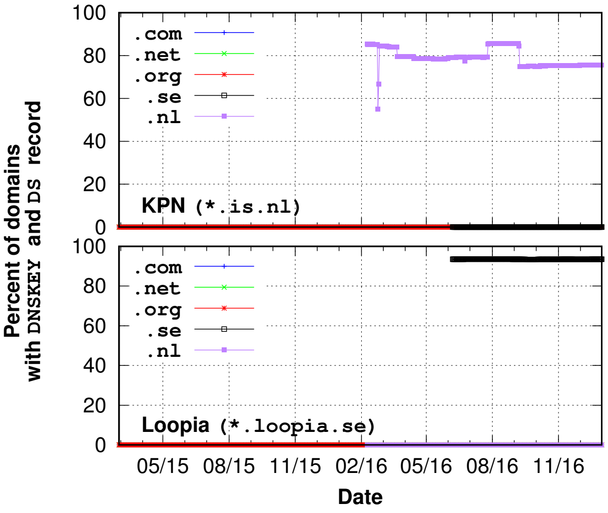
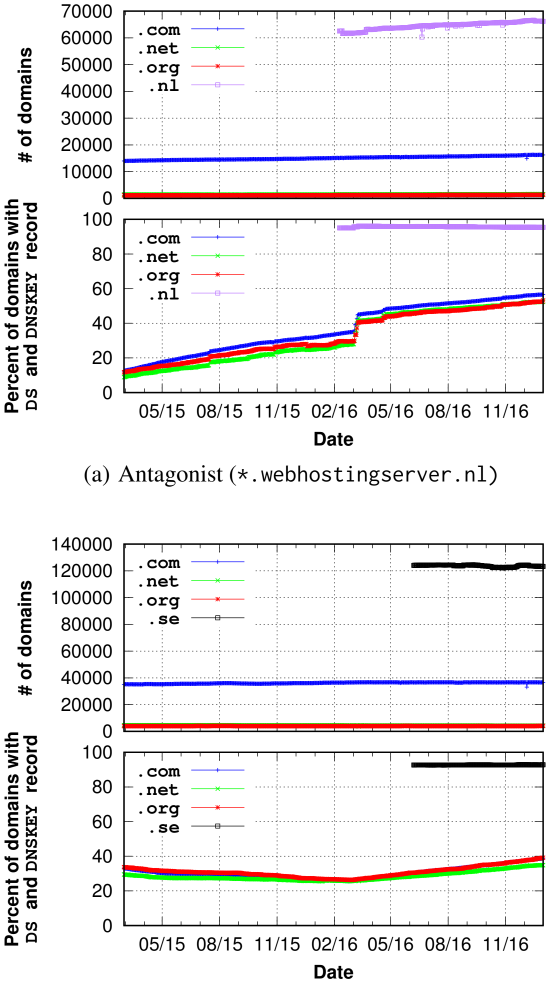


Figure 5: The percentage of fully deployed DNSSEC domains for Loopia and KPN. Each registrar supports DNSSEC only in their own country's domain (`.se` and `.nl`, respectively).

[21] For example, the `.nl` registry states that registrars should not fail validations more than 14 times in six months.



(a) Antagonist (`*.webhostingserver.nl`)

(b) Binero (`*.binero.se`)

Figure 6: The percentage of domains with DNSKEY and DS record for Antagonist and Binero. The number of domains for both registrars do not increase for our measurement period, but Antagonist gradually enabled DNSSEC over time.

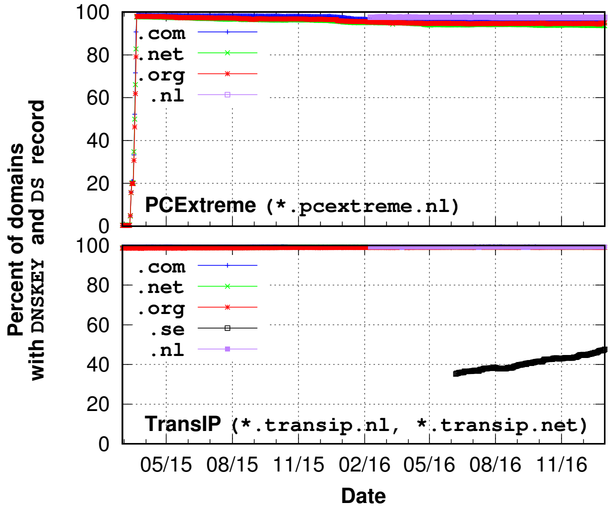


Figure 7: The percentage of domains with DNSKEY and DS record for PCExtreme and TransIP. Both of them have deployed DNSSEC for almost of their domains, but the DNSSEC adoption rate for the .se domains from TransIP is lower than the others due to the partial DNSSEC support of its registration partner (i.e., KeySystems).

Antagonist and Binero Next, we turn to two other registrars that show similar behavior. Figure 6 shows the percentage of domains with DNSSEC (bottom) and the number of domains (top) that are operated by Antagonist and Binero. Both of these registrars support DNSSEC for all TLDs, but we observe two phenomena. *First*, the percentage of domains with DNSSEC is much higher for `.nl` and `.se` domains, suggesting that the financial incentives may have encouraged their adoption. In fact, 95.4% of `.nl` domains from Antagonist and 92.9% of `.se` domains from Binero have DNSSEC deployed. However, the DNSSEC adoption ratios in other domains are much lower: 52.7% for Antagonist, and 37.8% for Binero in our latest snapshots.

Second, we observe that Antagonist's DNSSEC adoption rate has rapidly increased in all three other TLDs. However, the number of domains for which these two registrars are the DNS operator is increasing much more slowly (bottom graph), suggesting that the registrars have been enabling DNSSEC for existing customers. In an email exchange with Antagonist [26], we were informed that they are a reseller for `.com`, `.net`, and `.org`, and that they switched their `.com`, `.net`, and `.org` partner from Direct to OpenProvider in order to support DNSSEC in December 2014. However, the actual domain migration to a new registrar can only happen at the end of the current registration period of a domain, explaining why Antagonist shows gradual DNSSEC deployment. Overall, this example shows that the complex relationship between reseller and registrar can also result in slow deployment of DNSSEC.

TransIP and PCExtreme Next, we examine the two remaining registrars that serve as resellers: TransIP and PCExtreme. Figure 7 shows the percentage of domains with DNSSEC that are managed by these two. *First*, we note that these two registrars support DNSSEC very well; PCExtreme clearly enabled support for DNSSEC in March 2015 and the percentage of DNSSEC enabled `.com`, `.net`, and `.org` domains jumped from 0.44% to 98.3% in 10 days, even though they are a reseller for all three TLDs. Moreover, this high level of DNSSEC support has largely continued: in our latest snapshot, we observe that 97.0% of all their domains in these TLDs have DS and DNSKEY records. *Second*, TransIP shows an average 99.2% adoption rate of DNSSEC for the TLDs when they are themselves a registrar (`.com`, `.net`, `.org`, and `.nl`), but only 48.4% adoption rate when they are a reseller (`.se`). In an email discussion with a TransIP administrator [6], we were informed that this is due to its registrar for .se, KeySystems, which "enabled DNSSEC at a later date[22]." We suspect that the enabling of DNSSEC is only happening upon domain renewal, similar to Antagonist above. Overall, these results highlight the challenges for applying consistent DNSSEC policies for registrars who are also resellers for some TLDs.

6.4 DS record validation

As we did in Section 5.3 for the popular registrars that support the domain owner as the DNS operator, we tested whether the registrars that have the largest number of DNSSEC domains validate uploaded records. Surprisingly, we find that even among them only two (OVH and PCExtreme) checked the correctness of our uploaded DS records.

In fact, we observe that PCExtreme takes a unique approach: a domain owner can request to publish a DS record without sending them a DNSKEY nor a DS record. Instead, PCExtreme then fetches the DNSKEY records themselves from the authoritative nameserver and generates the DS records. This approach represents a trade-off between usability and security: it is less error-prone (to avoid the owner having to generate and transmit the DS record), but opens a window for an attacker to give PCExtreme an incorrect DNSKEY record. Moreover, this approach only works when publishing the *first* DS record. When a domain owner generates a new DNSKEY, PCExtreme requests the new DNSKEY by email [32] (with similar implications as for other registrars that use email-based DS uploads).

Of the four registrars that only use email to transmit DS records, we found that only one of them verified the email (by asking for a security "code" bound to the account). Two of the registrars did not verify the email was authentic and simply uploaded the DS record. Even worse, we found one registrar that accepted an updated DS record for our test domain from a *different* email address than the one we used to register the domain.[23] We have reported these vulnerabilities to the respective registrars with the hope that they will change their internal processes to properly validate updated DNSSEC records. Regardless, these examples demonstrate the challenges that registrars face when trying to properly deploy DNSSEC.

6.5 Summary

In summary, we observed that customers wishing to deploy DNSSEC face challenges even when using the registrars that have the best historic support for DNSSEC. Of the top 10 such registrars, most support DNSSEC by default when they are the DNS operator, but many only partially deploy DNSSEC (i.e., fail to upload DS records). Worse, most of the registrars do not validate DS records uploaded by the user, and fail to verify emails that request a new DS record be published. Overall, these registrars should be lauded for their support of DNSSEC, but could still improve their customer support and processes to make it easier and more secure for customers to support DNSSEC.

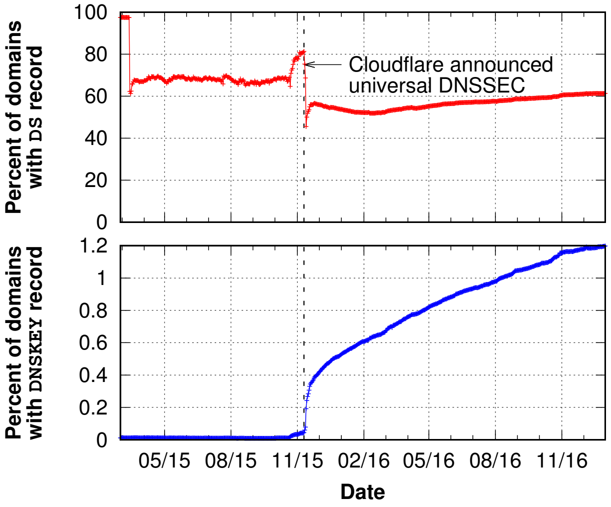


Figure 8: The percentage of Cloudflare-operated domains that enabled DNSSEC (bottom) and the percentage of these domains with DNSKEY that have a DS record as well (top). Roughly 40% of Cloudflare-operated domains that attempt to deploy DNSSEC fail to successfully do so. Note that the range of *y*-axis of the bottom graph is between 0 to 1.2.

7 THIRD-PARTY DNS OPERATORS

Finally, we examine the two most popular third-party DNS operators: DNSPod and Cloudflare, which are the DNS operators for 2,309,215 and 1,561,687 .com, .net, and .org domains, respectively. Recall that the third-party operators are *not* registrars; instead the owner of a domain contracts with these third-party operators to outsource the management of their domain.

After setting up an account with both services, we find that only Cloudflare supports DNSSEC. Cloudflare initially announced support for DNSSEC on November 11th, 2015 [5], but the domain owners must opt-in to use DNSSEC. If the owner does so, Cloudflare will generate DNSKEYs and RRSIGs, and will provide the domain owner with the DS record; the domain owner is responsible for communicating the DS record to their registrar for addition to the registry (as Cloudflare does not have the authority to do so). As a result, if a domain owner fails to properly convey the DS record, or if their registrar does not support DNSSEC, they will fail to properly deploy DNSSEC for their domain.

We find that only 29,537 (1.9%) of domains using Cloudflare have a DNSKEY record in our latest snapshot (December 31st, 2016). Interestingly, we also observe that 11,626 (39.3%) of these domains do *not* have a DS record, suggesting that they failed to upload the Cloudflare-provided DS record to their registrar.

To explore this further, Figure 8 shows the number of Cloudflare-hosted domains with DNSKEYs (bottom) and the fraction of those that

[22] Because KeySystems acts as a registrar and TransIP as a reseller for .se domain, the financial incentive that the .se registry awards will go to KeySystems.

[23] We used an address that was completely different from the name we listed in the WHOIS information to send the DS record.

also have DS records (top). We can immediately see the how this complex procedure leads to poor overall deployment of DNSSEC. We are able to observe a rapid increase in the percentage of Cloudflare domains that have DNSKEYs once Cloudflare announced universal DNSSEC. However, even today, 40% of the domain owners who enabled DNSSEC at Cloudflare did not upload their DS record to their registrar. Even worse, this portion has remained remarkably stagnant as the number of domains with DNSKEYs has increased; we observe that 38.7% of domains with DNSKEYs still do not have a DS record in our latest snapshot (December 31st, 2016).

To help remedy this situation, Cloudflare supports the CDS and CDNSKEY proposals [28, 48], which would enable Cloudfare to convey the DS record to the registry themselves (i.e., avoiding the need for the user to relay the DS record to the registrar, who relays it to the registry). However, this proposal has seen very slow uptake, and we know of only one registry (.cz) that has deployed it and one registry (.ca) that is considering deploying it.

8 CONCLUDING DISCUSSION

We began this paper noting that the low level of adoption of DNSSEC has been widely bemoaned, but relatively little appears to be changing. DNSSEC was originally proposed almost two decades ago, and today most TLD registries support it. Unfortunately, less than 1% of .com, .net, and .org second-level domains do, meaning very few DNS responses provide the authenticity and integrity that DNSSEC could in theory provide. Given the powerful attacks [27, 40], the critical role that DNS plays, and society's increasing reliance on computing infrastructure, the poor deployment of DNSSEC remains as a significant problem.

In this paper, our goal was to shed light on *why* DNSSEC adoption remains so low. To do so, we took the perspective of a customer and attempted to buy domains and deploy DNSSEC through 30 different registrars. We found the level of support for DNSSEC to be highly skewed: only three of the top 20 registrars support DNSSEC when they are the DNS operator, which is unfortunate as this is the easiest situation for DNSSEC support. Moreover, only 11 of the 20 supported DNSSEC when the owner was the DNS operator, and the processes for uploading DS records were error-prone (very few of the registrars did any validation of uploaded data) and opened the door to security attacks (most registrars that use email for transmittal of DS records did not actually validate the email, and one even accepted an email from a different address). Taken together, our results shine a light on the difficulties that domain owners face when trying to deploy DNSSEC.

Ethical Considerations Our measurements of the (in)security of uploading DS records brings up a few ethical issues, and we wish to discuss them explicitly before concluding. At all points, we took steps to ensure our measurements met community ethical standards. *First*, we note that we only tested uploading incorrect DS records for the test domains that we bought from each registrar, thus our experiment did not impact any other domains. *Second*, we responsibly disclosed our findings to all of the registrars that have potential security vulnerabilities that we found (e.g., not validating the authenticity of incoming email or accepting different email address than the one that registered) in order to help them mitigate the issues.

Recommendations Stepping back, our results indicate there are a number of steps that the various DNS entities can take to spur greater adoption of DNSSEC.

(1) Registrars play a critical role in supporting DNSSEC today, but most do so poorly. Registrars should allow *all* customers to enable DNSSEC if they wish, and should move towards a standard of DNSSEC-by-default. Today, only one registrar among the top 20 had this policy, and only did so for some of their domains.
(2) Registries largely support DNSSEC, but we know that only the .cz registry has recently announced support for CDS and CDNSKEY [19]. These proposals completely remove the friction that customers face when trying to deploy DS records, as they can effectively communicate directly with the registry. Unfortunately, we know of no other registries that support CDS and CDNSKEY today, which is unfortunate given how many domains we find have DNSKEYs deployed but fail to successfully deploy a DS record.
(3) Until CDS and CDNSKEY are fully supported, registries should work to make the process of uploading DS records easier and more secure. Of the registrars we studied, PCExtreme has the easiest and most secure approach, allowing a customer to log in and request that the registrar fetch the customer's DNSKEYs and generate and deploy a DS record. This process is much less error-prone than web-based uploads or emails, but PCExtreme can further improve this by (a) showing the customer the fetched DNSKEY so the customer can verify this process was secure, and (b) allowing customers to switch to a new key in a similar fashion as well.
(4) Certain TLD registries have employed small financial incentives for registrars to deploy DNSSEC; these same TLDs have seen dramatically higher levels of DNSSEC deployment. We encourage other registries to do the same. For example, .se offered a €0.28 discount per year off of the €3.40 price (an 8.2% discount); the .se registry observed that when they originally raised their discount from 2.5% to 5%, the number of DNSSEC-signed domains jumped "literally overnight" [34]. Even this modest discount becomes significant at the scale that many registrars operate; since a small number of registrars own much of the market, even changing just a few registrars' policies to support DNSSEC may lead to much higher adoption.

9 ACKNOWLEDGMENTS

We thank the anonymous reviewers and our shepherd, Mark Allman, for their helpful comments. This research was supported in part by NSF grants CNS-1564143 and CNS-1563320, and made possible by OpenINTEL (https://www.openintel.nl/), a joint project of SURFnet, the University of Twente, and SIDN.

REFERENCES

[1] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. RFC 4033, IETF, 2005. http://www.ietf.org/rfc/rfc4033.txt.
[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Protocol Modifications for the DNS Security Extensions. RFC 4035, IETF, 2005. http://www.ietf.org/rfc/rfc4035.txt.

[3] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Resource Records for the DNS Security Extensions. RFC 4034, IETF, 2005. http://www.ietf.org/rfc/rfc4034.txt.

[4] APNIC DNSSEC validation rate. https://stats.labs.apnic.net/dnssec.

[5] Announcing Universal DNSSEC: Secure DNS for Every Domain. https://blog.cloudflare.com/introducing-universal-dnssec.

[6] Arjan van den Berg, TransIP BV. Personal Communication.

[7] T. Chung, D. Choffnes, and A. Mislove. Tunneling for Transparency: A Large-Scale Analysis of End-to-End Violations in the Internet. *IMC*, 2016.

[8] T. Chung, R. van Rijswijk-Deij, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. *USENIX Security*, 2017.

[9] M. Davids. DNSSEC in .nl. 2016. https://www.sidnlabs.nl/downloads/presentations/SIDN-Labs-InternetNL-20160316.pdf.

[10] T. Dai, H. Shulman, and M. Waidner. DNSSEC Misconfigurations in Popular Domains. *CANS*, 2016.

[11] DNSSEC Debugger. http://dnssec-debugger.verisignlabs.com.

[12] DNSSEC Deployment Report. https://rick.eng.br/dnssecstat/.

[13] DNSSEC for Registrars. https://www.cloudflare.com/dns/dnssec/dnssec-for-registrars.

[14] DNSSEC signzone manual pages. https://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/man.dnssec-signzone.html.

[15] DNSViz. http://dnsviz.net.

[16] D. Eastlake. Domain Name System Security Extensions. IETF RFC 2535, IETF, 1999.

[17] D. Eastlake and C. Kaufman. Domain Name System Security Extensions. RFC 2065, IETF, 1997.

[18] A.-M. Eklund-Lowinder. DNSSEC Deployment in Sweden: How Do We Do It? ICANN50, 2014. https://london50.icann.org/en/schedule/wed-dnssec/presentation-dnssec-deployment-sweden-25jun14-en.pdf.

[19] O. Filip. Let's make DNS great again! 2017. https://en.blog.nic.cz/2017/06/21/lets-make-dns-great-again/.

[20] A. Fant-Eldh and M. Kirvesniemi. Economical and Political Implications of DNSSEC Deployment. Ph.D. Thesis, KTH Information and Communication Technology, 2010.

[21] Getting DNSSEC deployed: costs and benefits. https://www.powerdns.com/resources/BringingDNSSECtotheaccessproviders.pdf.

[22] Google DNS: DNSSEC Available to Test on Cloud DNS. https://groups.google.com/forum/#!topic/cloud-dns-discuss/WXNHtB9W0bg.

[23] P. Hoffman. SMTP Service Extension for Secure SMTP over Transport Layer Security. IETF RFC 3207, IEFT, 2002.

[24] How to Sign and Secure Your Domain with DNSSEC Using Domain Registrars. http://www.internetsociety.org/deploy360/resources/dnssec-registrars/.

[25] ICANN TLD DNSSEC Report. http://stats.research.icann.org/dns/tld_report.

[26] Joris de Leeuw, Antagonist. Personal Communication.

[27] D. Kaminsky. It's the End of the Cache as We Know It. Black Hat, 2008. https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf.

[28] W. Kumari, O. Gudmundsson, and G. Barwood. Automating DNSSEC Delegation Trust Maintenance. RFC 7344, IETF, 2014.

[29] J. Latour, O. Gudmundsson, P. Wouters, and M. Pounsett. Third Party DNS operator to Registrars/Registries Protocol. IETF, 2017.

[30] S. Liu, I. Foster, S. Savage, G. M. Voelker, and L. K. Saul. Who is .com? Learning to Parse WHOIS Records. *IMC*, 2015.

[31] W. Lian, E. Rescorla, H. Shacham, and Stefan. Measuring the Practical Impact of DNSSEC Deploymenta. *USENIX Security*, 2013.

[32] Loek Geleijn, PCExtreme System Operations. Personal Communication.

[33] P. Mockapetris. Domain Names - Concepts and Facilities. RFC 1034, IETF, 1987.

[34] R. Mohan. Slowly cracking the DNSSEC code at ICANN 43. https://afilias.info/blogs/ram-mohan/slowly-cracking-dnssec-code-icann-43.

[35] Nameservers and TLDs supported/unsupported by DNSSEC. https://www.namecheap.com/support/knowledgebase/article.aspx/9718/2232/nameservers-and-tlds-supportedunsupported-by-dnssec.

[36] E. Osterweil, D. Massey, and L. Zhang. Deploying and monitoring DNS security (DNSSEC). *ACSAC*, IEEE Computer Society, 2009.

[37] E. Osterweil, M. Ryan, D. Massey, and L. Zhang. Quantifying the operational status of the DNSSEC deployment. *IMC*, 2008.

[38] OpenINTEL. https://www.openintel.nl/.

[39] Report from the IAB workshop on Internet Technology Adoption and Transition (ITAT). https://tools.ietf.org/id/draft-iab-itat-report-01.xml#rfc.section.3.3.

[40] S. Son and V. Shmatikov. The hitchhiker's guide to DNS cache poisoning. *Security and Privacy in Communication Networks*, Springer, 2010.

[41] Z. Shelby. Constrained RESTful Environments (CoRE) Link Format. RFC 6690, IETF, 2012.

[42] State of DNSSEC Deployment 2016. https://www.internetsociety.org/sites/default/files/ISOC-State-of-DNSSEC-Deployment-2016-v1.pdf.

[43] The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. RFC 6698, IETF, 2012. https://tools.ietf.org/html/rfc6698.

[44] A. Veenman. SIDN extends DNSSEC discount until July 1, 2018. 2014. https://www.ispam.nl/archives/38957/sidn-verlengt-dnssec-kortingsregeling-tot-1-juli-2018/.

[45] N. L. M. van Adrichem, N. Blenn, A. R. Lua, X. Wang, M. Wasif, F. Fatturrahman, and F. A. Kuipers. A measurement study of DNSSEC misconfigurations. *Sec. Info.*, 4(8), 2015.

[46] R. van Rijswijk-Deij, M. Jonker, and A. Sperotto. On the Adoption of the Elliptic Curve Digital Signature Algorithm (ECDSA) in DNSSEC. *CNSM*, 2016.

[47] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. *IEEE Journal on Selected Areas in Communications*, 34(6), 2016.

[48] P. Wouters and O. Gudmundsson. Managing DS Records from the Parent via CDS/CDNSKEY. RFC 8078, IETF, 2017.

[49] D. York. Challenges and Opportunities in Deploying DNSSEC: A progress report on an investigation into DNSSEC deployment. *SATIN*, 2012.

[50] H. Yang, E. Osterweil, D. Massey, S. Lu, and L. Zhang. Deploying cryptography in Internet-scale systems: A case study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing*, 8(5), 2011.

[51] Y. Yu, D. Wessels, M. Larson, and L. Zhang. Check-Repeat: A New Method of Measuring DNSSEC Validating Resolvers. *TMA*, 2013.