Tracking Registrar Support for DNSSEC

It's Slowly Getting Better

Spencer Roth
Rochester Institute of Technology

Roland van Rijswijk-Deij
University of Twente and NLNetLabs

Taejoong Chung
Rochester Institute of Technology

ABSTRACT

In response to security issues in the Domain Name System (DNS), DNS Security Extensions (DNSSEC) were introduced to provide authenticity and integrity of DNS records. However, DNSSEC has been criticized for its low deployment rate both on domains (lack of signing) and resolvers (lack of validation). A study conducted in early 2017 found that the underlying reasons why DNSSEC adoption was low (e.g., 1.0% in `.com` domains) are mainly a lack of DNSSEC support from registrars, which are organizations that sell domain names to the public. For example, the authors found that only few popular registrars support DNSSEC on their nameservers and even further require domain name owners to take complex, often error prone steps in order to activate DNSSEC. In this paper, we examine if registrars have improved their support for DNSSEC and how the deployment status of DNSSEC has been impacted as a result. Through more longitudinal datasets (21 vs. 51 months) of all second level domain names of five TLDs and purchasing domains from popular registrars, we are not only able to observe more support for DNSSEC from registrars (compared to previous findings), but also find new challenges that they may face when managing and deploying DNSSEC such as algorithm rollovers, which we observed for one registrar.

ACM Reference Format:
Spencer Roth, Roland van Rijswijk-Deij, and Taejoong Chung. 2019. Tracking Registrar Support for DNSSEC: It's Slowly Getting Better. In *Internet Measurement Conference (IMC '19), October 21–23, 2019, Amsterdam, Netherlands.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3355369.3355596

1 INTRODUCTION

The DNS Security Extensions (DNSSEC) were introduced starting two decades ago, mainly to guarantee the integrity of DNS records. Unfortunately, even though more than 93% of TLDs now support DNSSEC, recent studies found that adoption by second-level domains (e.g., `google.com`) still remains low (e.g., 1.0%∼1.1% in `.com`, `.net` and `.org` [1]). A study conducted in 2016 [2] investigated the underlying reasons why DNSSEC adoption has been remarkably low; *DNS registrars—the entites that sell domain names and often operate DNS authoritative nameservers—play a critical role in the deployment of DNSSEC, but only few of them actually support DNSSEC*. Even if domain owners want to use their own authoritative nameservers to enable DNSSEC, registrars must still upload a `DS` record to the registry to complete the deployment process. The study found that only 3 out of 20 popular registrars, responsible for 54.3% of `.com`, `.net`, and `.org` domains, support DNSSEC on their nameservers and 10 registrars support DNSSEC when the domain name owner is the DNS operator.

Since then, however, there have been numerous attempts to spur greater adoption of DNSSEC; for example, Google (https://domains.google) announced DNSSEC support on their authoritative nameservers in November 2017. Also, `CDS` and `CDNSKEY`, which allow a domain owner to automate the DNSSEC deployment process, began to be implemented by DNS operators (e.g., DNSSimple [5], Cloudflare [7]), registries (e.g., `.cz` [6] and `.ch` [15]) and DNS software vendors (e.g., Knot DNS [10]).

In this study, we explore how popular registrars have improved their support for DNSSEC and how this has impacted overall DNSSEC deployment. We leverage over 4 years of daily snapshots of DNSSEC records for *all* `.com`, `.net`, `.org`, `.se`, and `.nl` second-level domains as well as purchase domains from the 20 most popular registrars to conduct apples-to-apples comparisons with the previous study [2].

2 BACKGROUND

This section provides a brief overview of DNS, DNSSEC, and various organizations involved in the deployment of DNSSEC. For more detail, we refer to the 2016/2017 studies [1, 2].

DNS and DNSSEC DNS has long been fraught with security issues such as DNS spoofing and cache poisoning [8]. To mitigate these attacks, DNSSEC was introduced to provide cryptographic signatures of DNS records to let clients verify record integrity and authenticity. There are three essential DNSSEC records to achieve the goals:

- `DNSKEY` records are public keys that clients need to verify DNSSEC signatures
- `RRSIG` records are cryptographic signatures over DNS record sets.
- `DS` records are a hash of `DNSKEY`s, which must be uploaded to the parent zone by *registrars*. A client can verify the authenticity of a `DNSKEY` by comparing a hash of the `DNSKEY` to the `DS` record provided by the parent zone.

Registries, Registrars, and DNS Operators

IMC '19, October 21–23, 2019, Amsterdam, Netherlands

ACM ISBN 978-1-4503-6948-0/19/10…$15.00
https://doi.org/10.1145/3355369.3355596

TLD	Measurement Period	Domains	
		Number	Percent with DNSKEY (Δ)
.com	2015-03-01 – 2019-06-19	140,438,505	0.8% (+0.1)
.net	2015-03-01 – 2019-06-19	13,408,301	1.1% (+0.1)
.org	2015-03-01 – 2019-06-19	10,066,388	1.1% (+0.0)
.nl	2016-02-09 – 2019-06-19	5,860,418	54.1% (+2.5)
.se	2016-06-07 – 2019-06-19	1,450,441	56.9% (+10.2)

Table 1: Overview of the datasets used for this study. The number of overall domains and percentage that have DNSKEYs published is as-of June 19, 2019; comparing to the DNSSEC deployment rate at the end of 2016, the overall DNSSEC deployment rate has increased across all TLDs.

- *Registries* are organizations that manage top-level domains (TLDs); for example, Verisign manages all second level domains of .com.
- *Registrars* are accredited organizations that sell domain names to public. They can directly access the registry to register domain names or DNS records such as NS records.
- *DNS operators* are organizations that run authoritative nameservers for a domain name. The domain name owners can use either their own nameserver (i.e., owner as a DNS operator), a nameserver provided by the registrar (e.g., registrar as a DNS operator), or a third-party nameserver such as Cloudflare (i.e., third-party as a DNS operator) to manage their DNS records. Regardless of which DNS operators to use, however, the domain name owner *must* communicate with the registrar to enable DNSSEC because it is the *only* entity that can upload a DS record to the parent zone (i.e., registry).

3 DATASETS

In this section, we present the datasets that we use in this study and compare overall DNSSEC deployment rate to that in 2016 [2]. Similar to the previous work, we have been provided access to OpenINTEL [14, 17] to scan all second-level domains from five TLDs on a daily basis: the .com, .net, and .org generic TLDs and .se and .nl country-code TLDs. Compared to the earlier studies [1, 2], we process data for a much longer period to see how DNSSEC deployment has changed. Table 1 shows a summary. We immediately notice that DNSSEC deployment has increased since 2016 across all TLDs. Interestingly, the deployment rate for the two country-code TLDs substantially increased by 2.5% (.nl) and 10.2% (.se). We believe this is due to financial incentives provided from each of the registries; a registrar receives a discount every year when it correctly signs its .nl and .se domains [3, 11, 12, 16].

4 POPULAR DNS OPERATORS

We begin by re-examining how the most popular DNS registrars have improved their support for DNSSEC. To do so, we follow the same methodology as the earlier study [2]; we focus on the most popular 31 DNS operators that serve DNS for the most domains. After purchasing a .com domain from each registrar, we re-examine

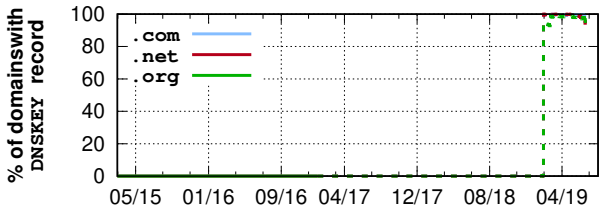

Figure 1: The percentage of NameBright-operated domains that deployed DNSKEYs; the dashed line is drawn from the new datasets (since January 1st, 2017).

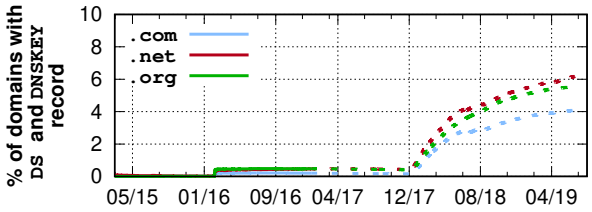

Figure 2: The percentage of Google-operated domains that fully deployed DNSSEC; since its launch in November 2017, they have deployed both of DNSKEYs and DS records correctly and its deployment rate has been increasing.

their DNSSEC policy.[1] Table 2 shows the results of this experiment. We make a number of observations below.

4.1 Registrar as a DNS operator

First, we observe that two more registrars (NameBright and Google) now support DNSSEC when they are the DNS operator. In 2016, only 3 registrars (GoDaddy, NameCheap, and OVH) supported DNSSEC on their nameservers. Interestingly, NameBright has enabled DNSSEC for almost all of its domains (99.41%), whereas Google shows a lower deployment (4.49%), suggesting they leave the choice to the user.

Next, we check if they have correctly deployed DNSSEC by checking the existence of DS records; Figure 1 shows NameBright-operated domains with DNSKEYs. The graph shows they published DNSKEYs for almost all domains (99.5%) on January 29, 2019. If we look at which fraction of domains also have matching DS records, however, we find that *none of these domains* have a DS record. Considering that domains that fail to provide a DS record signed by the parent zone cannot be validated, NameBright's DNSSEC deployment does not yet provide any security benefits to those domains.

On the other hand, Google launched DNSSEC supports in November 2017 [4] and the percentage of domains with DNSKEYs from Google increased to 4.49%. We observe that they enabled DNSSEC support on their nameservers correctly by showing that all of the domains with DNSKEYs have deployed DS records as well (Figure 2).

[1] We exclude nine domain parking services and two third-party DNS operators as they are not registrars.

Registrar (Domain of Auth. Nameservers)	% of Domains with DNSKEY	Δ	Registrar DNS operator: DNSSEC default	Registrar DNS operator: DNSSEC opt-in	Owner DNS operator: DNSSEC support	Owner DNS operator: DS upload Web	Owner DNS operator: DS upload Email	Owner DNS operator: DS Validation DNSKEY	Owner DNS operator: DS Validation Email
GoDaddy (domaincontrol.com)	0.03%	+0.01%	○	●	●	●	-	○	-
Alibaba (hichina.com)	0.00%	0.00%	○	○	◑	◑	-	○	-
1AND1 (1and1)	0.01%	+0.01%	○	○	○	-	-	-	-
Network Solution (worldnic.com)	0.01%	+0.01%	○	○	◑	-	◑	○	◑
eNom (name-services.com)	0.01%	+0.01%	○	○	●	○	●	○	●
Bluehost (bluehost.com)	0.00%	0.00%	○	○	◑	○	◑	○	◑
NameCheap (r...-servers.com)	1.03%	+0.36%	○	●	●	●	-	○	-
WIX (wixdns.net)	0.02%	+0.02%	○	○	○	-	-	-	-
HostGator (hostgator.com)	0.01%	+0.01%	○	○	●	●	-	◑	-
NameBright (namebrightdns.com)	99.41%	+99.41%	◑	◑	●	◑	◐	◑	●
register.com (register.com)	0.01%	+0.01%	○	○	◑	○	◑	◑	◑
OVH (ovh.net)	28.07%	+2.06%	○	●	●	●	-	●	-
DreamHost (dreamhost.com)	0.01%	+0.01%	○	○	●	◑	-	●	-
WordPress (wordpress.com)	0.00%	0.00%	○	○	○	-	-	-	-
Amazon (aws-dns)	0.03%	+0.03%	○	○	●	●	-	●	-
Xinnet (xincache.com)	0.00%	0.00%	○	○	○	-	-	-	-
Google (googledomains.com)	4.49%	+4.25%	○	◑	◑	◑	-	○	-
123-reg (123-reg.co.uk)	0.00%	+0.00%	○	○	●	●	-	○	-
Yahoo (yahoo.com)	0.01%	+0.01%	○	○	○	-	-	-	-
Rightside (name.com)	0.03%	0.03%	○	○	●	●	-	◑	-

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 still does not support DNSSEC, ◑ means that a DNS operator now supports DNSSEC, ● means that a DNS operator already supported DNSSEC. Note that we are not able to observe any DNSSEC operators that decided not to support DNSSEC any longer, which would be ◐. If a registrar supports uploading a DS record via its web interface, we do not email them to ask if they accept a DS record by email (hence the –). Cells with a green background show improved registrars; two registrars (Google and NameBright) now support DNSSEC on their nameservers and five registrars now support uploading a DS record; four of these now validate the uploaded DS record and one registrar checks the sender's email address.

4.2 Owner as a DNS operator

Next, we now turn our attention to how registrars have changed their policies to support DNSSEC when the owner acts as a DNS operator. We find that five more registrars (Alibaba, Network Solutions, Bluehost, register.com and Google) have enabled DNSSEC support for domains served from external nameservers; 15 of the 20 registrars now support DNSSEC for such domains. This is very promising compared to the earlier study from 2017 [2], which showed that only 10 registrars supported DNSSEC for domains operated by a third party.

We also observe that four more registrars (Hostgator, NameBright, register.com and Rightside) now validate the uploaded DS record; this is crucial as an incorrect DS record would break the chain of trust preventing users using DNSSEC-validating clients from communicating with the domain name.

In summary, we observe that DNSSEC support has generally improved over 3 years; two more registrars now support DNSSEC on their nameservers and five more registrars support DNSSEC for external nameservers. However we also observed that NameBright did not upload a DS record to the parent zone, which also reveals persisting mismanagement of DNSSEC.

5 MORE CHALLENGES FOR CORRECT DNSSEC DEPLOYMENT

Compared to the earlier studies, we are not only able to observe several challenges that DNS operators usually face, which are reported in the previous work [2] but also find a new one from the extended dataset.

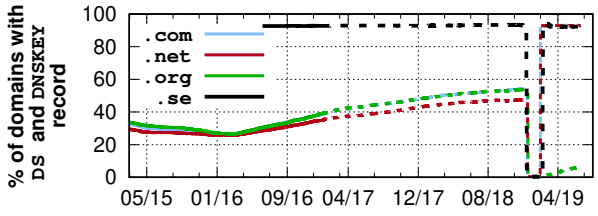

Figure 3: The percentage of domains with DNSKEY and DS records for Binero. Their algorithm rollover started on December 11, 2018 and finished on February 8, 2019.

5.1 DNSKEY Algorithm Rollover

As with any PKI, DNSSEC provides a way for DNS operators to roll their public/private key pairs to prevent potential key compromises. Thus, it is a good practice to roll DNSKEYs periodically, but it is crucial to *keep the DNSSEC chain intact* during the rollover by providing the old and new DNSKEYs and their corresponding RRSIGs together. Unlike many other PKIs, the public key pairs (i.e., DNSKEYs) can be cached at resolvers. Hence, the DNS operators should carefully choose when to drop and introduce new DNSKEYs and RRSIGs by considering the time-to-live (TTL) of DNS records because some resolvers might fetch the new DNSKEYs while preserving the unexpired old RRSIGs (or vice versa) [13].

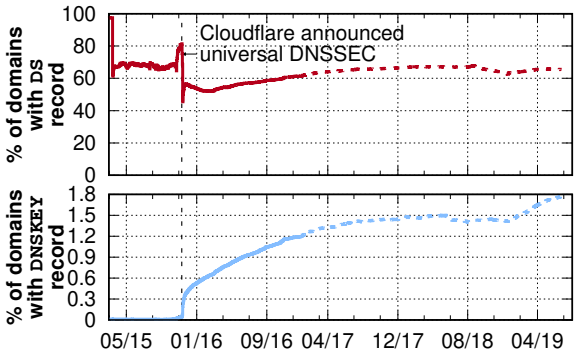

Figure 4: The percentage of Cloudflare-operated domains that enabled DNSSEC (bottom) and the percentage of these domains with DNSKEY that have a DS record as well (top). Note that the range of *y*-axis of the bottom graph is between 0 to 1.2.

During our measurement period, we notice that Binero, a Swedish registrar that supports DNSSEC for .com, .net, .org, and .se domains, began rolling their DNSKEYs on December 11, 2018 (Figure 3). They deployed a new stronger DNSKEY by switching their key algorithm from RSA (RSASHA256) to ECDSA (ECDSAP256SHA256). It took *59 days* to finish this process. We observe a number of things during the rollover.

First, they began to *withdraw only* DS *records* for nearly all of the domains that had DNSSEC enabled from December 11, 2018 while *keeping* the DNSKEYs; the number of domains with both DNSKEYs and DS records dropped to 798 from 130,765 (December 11, 2018), which implies they simply *deactivated* DNSSEC for 99.5% of their DNSSEC-enabled domains. After that, they also removed the old DNSKEYs over three days from December 26, 2018, leaving only 800 out of 160K domains with DNSKEYs. On January 27, 2019, they began to introduce only the new DNSKEYs and new DS records followed two days later. They finally completed the key and algorithm rollover on February 8, 2019, after more than 59 days. While it is understandable that they chose to go "unsigned" during the algorithm rollover (which is generally considered complex), this should not have left domains unprotected by DNSSEC for almost 2 months.

Second, after the rollover, we notice they enabled DNSSEC for a significant portion of the .com (93.7%) and .net (93.0%) domains they manage. This is encouraging given that they used to support DNSSEC only for the .se domains due to financial incentives.[2]. However, we find that the domains with DNSKEYs and DS records of the .org domains that they manage dropped to nearly zero percent after the rollover and increase marginally; in fact, they only deployed new DNSKEYs without uploading new DS records, making 93.5% of their .org domains have only DNSKEYs without DS records.

These two observations demonstrate the challenges that registrars face when trying to change their DNSKEYs, and especially when changing their signing algorithm.

[2]For .se domains, a registrar received a 10 SEK (∼$1.10) discount every year for a correctly-signed .se domain [12]

5.2 Third-party DNS operator

Finally, we examine the most popular third-party DNS operator, Cloudflare, which serves 3,270,777 domains (as-of June 19, 2019). They announced support for DNSSEC on November 11, 2015; if owners opt-in to use DNSSEC, Cloudflare will generate DNSKEYs and RRSIGs as well as DS records; the owner is responsible for uploading the DS records to their registrars. However, the previous study [2] showed that nearly half of the owners who opt-in to use DNSSEC failed to upload their DS records correctly.

From our investigation (Figure 4), we find that the percentage of domains with DNSKEYs has been increasing, but 36% of these domains still fail to upload DS records. This shows that there is an increasing demand from domain owners to deploy DNSSEC, but there are still problems doing this correctly; we believe that the CDS and CDNSKEY protocols [9, 18] would remedy this situation.[3]

6 CONCLUSION

This paper presents a study of how registrars' DNSSEC support have been improved since 2016 by monitoring 170M domains more than 4 years and registering domains at 20 registrars. Despite concerns about lacklustre support from registrars in the previous study, we now observe a decent increase in support: 15 out of 20 registrars now support DNSSEC for their own or external nameservers. However, we also observed an unsolved operational challenge for full DNSSEC deployment when using third-party DNS operators and a new issue when a DNS operator rolls their DNSKEYs.

REFERENCES

[1] 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.

[2] T. Chung, R. van Rijswijk-Deij, D. Choffnes, A. Mislove, C. Wilson, D. Levin, and B. M. Maggs. Understanding the Role of Registrars in DNSSEC Deployment. *IMC*, 2017.

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

[4] DNSSEC now available in Cloud DNS. https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns.

[5] A. Eden. Announcing CDS/CDNSKEY Support. 2019. https://blog.dnsimple.com/2019/02/cds_cdnskey/.

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

[7] S. Isasi and V. Shrestha. Expanding DNSSEC Adoption. 2018. https://blog.cloudflare.com/automatically-provision-and-maintain-dnssec/.

[8] 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.

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

[10] KnotDNS. KnotDNS Version 2.5.0 Updates. https://www.knot-dns.cz/2017-06-05-version-250.html.

[3]However, even after two years since its standardization, only the .cz and .ch registries have deployed it.

[11] T. Le, R. V. Rijswijk-Deij, L. Allodi, and N. Zannone. Economic Incentives on DNSSEC Deployment: Time to Move from Quantity to Quality. *NOMS*, 2018.
[12] A.-M. E. Löwinder. 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.
[13] M. Müller, T. Chung, A. Mislove, and R. van Rijswijk-Deij. Rolling with Confidence: Managing the Complexity of DNSSEC Operations. *IEEE Transactions on Network and Service Management*, IEEE, 2019.
[14] OpenINTEL. https://www.openintel.nl/.
[15] D. Stirnimann. Automating DNSSEC trust anchors using CDS. 2018. https://www.nic.ch/export/shared/.content/files/SWITCH_CDS_Manual_en.pdf.
[16] 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/.
[17] 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.
[18] P. Wouters and O. Gudmundsson. Managing DS Records from the Parent via CDS/CDNSKEY. RFC 8078, IETF, 2017.