An End-to-End View of DNSSEC Ecosystem Management

TAEJOONG CHUNG, ROLAND VAN RIJSWIJK-DEIJ, BALAKRISHNAN CHANDRASEKARAN, DAVID CHOFFNES, DAVE LEVIN, BRUCE M. MAGGS, ALAN MISLOVE, AND CHRISTO WILSON

Taejoong Chung is a Postdoctoral Researcher in the College of Computer and Information Science at Northeastern University. His work focuses on Internet security, privacy implications, and big data analysis through large-scale measurements. t.chung@neu.edu

Roland van Rijswijk-Deij is an enthusiastic Internet researcher, specializing in measurement-based research with a focus on DNS, DNSSEC, and network security. Roland has a PhD in computer science from the University of Twente in The Netherlands. He works for SURFnet, the National Research and Education Network in The Netherlands, and as Assistant Professor in the Design and Analysis of Communication Systems group at the University of Twente. r.m.vanrijswijk@utwente.nl

Balakrishnan Chandrasekaran is a Senior Research Scientist at Technische Universität Berlin. He received his PhD in computer science from Duke University. His research focuses on making the Internet faster, reliable, and more secure, and his work spans network measurements and mapping, network security, and software-defined networking. balac@inet.tu-berlin.de

The Domain Name System (DNS) provides name resolution for the Internet, and DNS's Security Extensions (DNSSEC) allow clients and resolvers to verify that DNS responses have not been forged. DNSSEC can operate securely only if each of its principals performs its management tasks correctly: authoritative name servers must generate and publish their keys and signatures, domains that support DNSSEC must be signed with their parent's keys, and resolvers must actually validate the chain of signatures. We perform the first large-scale measurement study into how well DNSSEC's PKI is managed, studying the behavior of domain operators, registrars, and resolvers. Our investigation reveals pervasive mismanagement of the DNSSEC infrastructure: only 1% of the .com, .org, and .net domains attempt to deploy DNSSEC; many popular registrars that support DNSSEC fail to publish all relevant records required for validation; and only 12% of resolvers that request DNSSEC records actually attempt to validate them.

The Domain Name System (DNS) is the Internet's equivalent of the "yellow pages": it translates human-readable domain names to machine-friendly Internet Protocol (IP) addresses. Unfortunately, the original DNS protocol did not include any security mechanisms. This lack of security allows an adversary to forge DNS records, and such attacks can have significant effects on end users, who may end up unknowingly communicating with malicious servers.

To address these problems, the DNS Security Extensions (DNSSEC) were introduced nearly two decades ago. At its core, DNSSEC is a hierarchical public key infrastructure (PKI) that largely mirrors the DNS hierarchy and is rooted at the DNS root zone. To enable DNSSEC, the owner of a domain signs its DNS records (using its private key) and publishes the signatures along with its public key; this public key is then signed by its parent domain, and so on up to the DNS root zone, resulting in a *chain of trust*. As of early 2017, more than 90% of top-level domains (TLDs), such as .com, and 47% of country-code TLDs (ccTLDs), such as .nl, are DNSSEC-enabled [4, 8]. DNS resolvers that perform recursive DNS lookups on behalf of end users validate DNSSEC signatures in order to ensure that the response to a query they handle is authentic and was not modified in flight. These so-called *validating resolvers* perform signature verification along the chain of trust, from the signature on the record that was requested all the way to the top of the PKI at the root of the DNS. But like any PKI, DNSSEC can only function correctly when all principals—every signatory from root to leaf and the resolver validating the signatures—fulfill their respective responsibilities. Unfortunately, DNSSEC is complex, creating many opportunities for mismanagement.

On the authoritative server side, a single error such as a weak key or an expired signature can weaken or completely compromise the integrity of a large number of domains. *On the resolver side,* mismanaged or buggy DNS resolvers can obviate all server-side efforts by simply failing to catch invalid or missing signatures.

David Choffnes is an Assistant Professor in the College of Computer and Information Science and a member of the Cybersecurity and Privacy Institute at Northeastern University. His research is primarily in the areas of distributed systems and networking, focusing on mobile systems, privacy, and security. His research has been supported by the NSF, DHS, Comcast Innovation Fund, Google Research Awards, the Data Transparency Lab, M-Lab, and a Computing Innovations Fellowship. choffnes@ccs.neu.edu

Dave Levin is an Assistant Professor of Computer Science and Chair of the Computer Science Honors program at the University of Maryland, from which he also received his BS and PhD. His research combines measurement and systems building to improve the security of the Internet, including the Web's public key infrastructure, DNS, and censorship avoidance. dml@cs.umd.edu

Bruce Maggs is the Pelham Wilder Professor of Computer Science at Duke University and Vice President for Research at Akamai Technologies. His research interests focus on distributed systems, including content delivery networks, computer networks, and computer and network security. bmm@cs.duke.edu

In this article, we present a comprehensive study of the entire DNSSEC ecosystem—encompassing signers, authoritative name servers, registrars, and validating DNS resolvers—to understand how DNSSEC is (mis)managed today. To study server-side behavior, our work relies on 21 months of daily snapshots of DNSSEC records for *all* signed .com, .net, and .org second-level domains. To study resolver-side behavior, 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 most domains with "DNSKEY"s (covering 84.6% of such domains in .com, .net, and .org). To study client-side behavior, we leverage the Luminati HTTP proxy service, which allows us to perform repeated, controlled tests from 403,355 end hosts and their 59,513 distinct DNS resolvers around the world.

Our analysis reveals troubling, persistent mismanagement in the DNSSEC PKI:

- First, we find that nearly *one-third* of DNSSEC-enabled domains produce records that *cannot be validated* due to missing or incorrect records. The vast majority of these missing records are due to registrars that host many domains but fail to publish the correct records for domains they manage.
- Second, we find that registrar support for DNSSEC varies widely. Among the top 20 registrars, only three support DNSSEC when the registrar runs the authoritative DNS server (referred to as being the *DNS operator*); only one does so by default, and then only for some of its more expensive plans. Moreover, not all of the registrars we study support DNSSEC when the domain owner is the DNS operator. Of those that do, many require cumbersome and insecure steps for domain owners to deploy DNSSEC, such as requiring that domain information be sent over insecure email channels.
- Third, we find that although 58% of observed resolvers request DNSSEC records during their queries, only 12% of them actually validate the records. This means that the majority of resolvers pay the overhead to download DNS records for DNSSEC, while not reaping the security benefits.

In summary, our results paint a distressing picture of widespread mismanagement of keys and DNSSEC records that violate best practices in some cases and completely defeat the security guarantees of DNSSEC in others. On a more positive note, our findings demonstrate several areas of improvement where management of the DNSSEC PKI can be automated and audited. To this end, we have publicly released all of our analysis code and data (where possible) to the research community at https://securepki.org, thereby allowing other researchers and administrators to reproduce and extend our work.

Background

DNS

The Domain Name System (DNS) is based on *records* that map *domain names* (e.g., "example.com") to Internet Protocol (IP) addresses (e.g., "10.0.0.1"). DNS is a distributed system, and there are three primary kinds of organizations involved in the domain name registration process:

- *Registries* are organizations that manage top-level domains (TLDs). They maintain their TLD *zone file* (the list of all registered names in that TLD). For example, Verisign serves as the registry for .com.
- *Registrars* are organizations that sell domains to the public. Because they are accredited by ICANN, they can directly access the registry, which enables them to process new registrations.
- *DNS operators* are organizations that run *authoritative* DNS servers. Each domain has a DNS operator; the most common cases are (1) the domain owner asks their registrar to run the authoritative DNS server (registrar DNS operator), or (2) the domain owner runs their own authoritative DNS server (owner DNS operator).

An End-to-End View of DNSSEC Ecosystem Management

Alan Mislove is an Associate Professor and Associate Dean and Director of Undergraduate Programs at the College of Computer and Information Science at Northeastern University, which he joined in 2009. He received his BA, MS, and PhD in computer science from Rice University. Prof. Mislove's research focuses on the security and privacy implications of today's distributed systems, often centered around large-scale measurement and analysis. amislove@ccs.neu.edu

Christo Wilson is an Assistant Professor in the College of Computer and Information Science at Northeastern University and a member of the Cybersecurity and Privacy Institute at Northeastern. His work focuses on Web security, privacy, and algorithmic transparency. His work is funded by the NSF, the Russell Sage Foundation, the European Commission, and the Data Transparency Lab. cbw@ccs.neu.edu

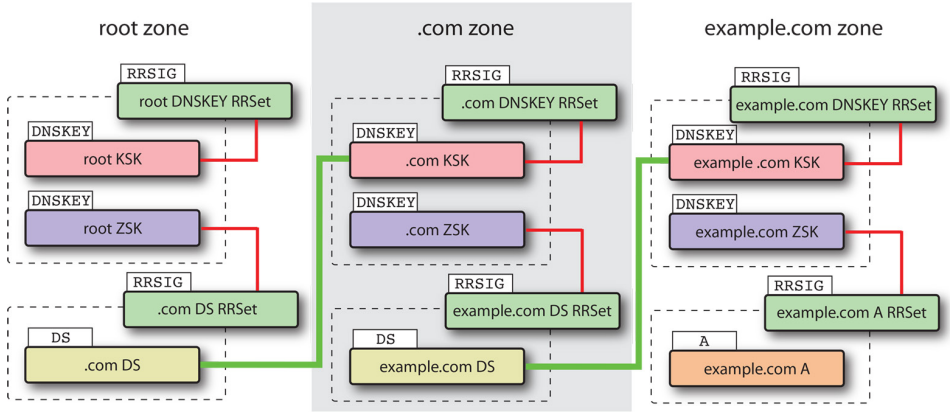

Figure 1: Overview of DNSSEC records necessary to validate example.com's "A" record. Each RRSIG is the signature of a record set (dashed lines) verified with a DNSKEY (thinner solid lines). Each DS record is the hash of a child zone's KSK, or key-signing key (thicker solid lines).

Whenever a registrar sells a domain name, it must insert an "NS" (name server) record for the new domain into the registry's TLD zone file; the "NS" record contains the identity of the authoritative DNS server (i.e., the DNS operator).

DNSSEC

Unfortunately, the original DNS protocol did not include authenticity mechanisms, allowing an adversary to forge DNS responses. The DNS Security Extensions (DNSSEC) are designed to address this vulnerability. DNSSEC provides integrity for DNS records using three primary record types:

- "DNSKEY" records are public keys used to validate DNS records in DNSSEC.
- "RRSIG" (Resource Record Signature) records are cryptographic signatures of other records. Each RRSIG is created using the private key that matches a DNSKEY; all records need to carry signatures to ensure that they are not forged.
- "DS" (Delegation Signer) records are essentially hashes of DNSKEYs. These records must be uploaded to the parent zone, where they are signed by the parent's DNSKEY.

Resolvers

Most Internet hosts are configured to use a local DNS *resolver*, which looks up domain names for them. The resolver iteratively determines the authoritative DNS server for a domain, obtains the requested record, and forwards it back to the requesting host. If the resolver supports DNSSEC, it will also fetch all DNSSEC records (DNSKEYs and RRSIGs) and validate them. Finally, the resolver returns the (validated) record back to the requesting host.

A resolver indicates that it would like to receive DNSSEC records by setting the "DO"(DNSSEC OK) bit in its DNS requests. Then the responding authoritative DNS server will include the RRSIGs corresponding to the record type of the request in its response. Once it receives the RRSIGs, the resolver can then fetch the necessary DNSKEYs and DS records to validate the response.

Validating a DNSSEC Record

All DNSSEC-aware resolvers must be provided with the root zone's key. There is a logical chain of DNSKEYs, starting from the root zone's key through the desired zone's DNSKEY record. Once a domain's DNSKEY has been authenticated, the record in question can be validated using this key and the record's RRSIG. Figure 1 shows example records and how they are related.

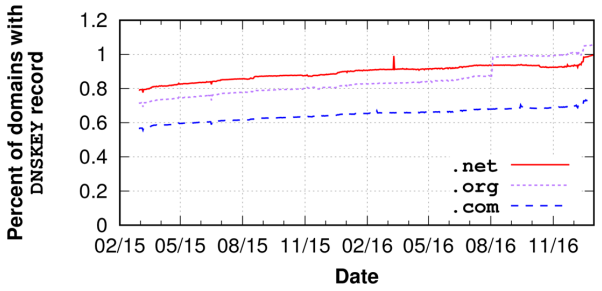

Figure 2: The percentage of all .com, .org, and .net second-level domains that have a DNSKEY record. Between 0.75% and 1.0% of all domains publish a DNSKEY record in our latest snapshot.

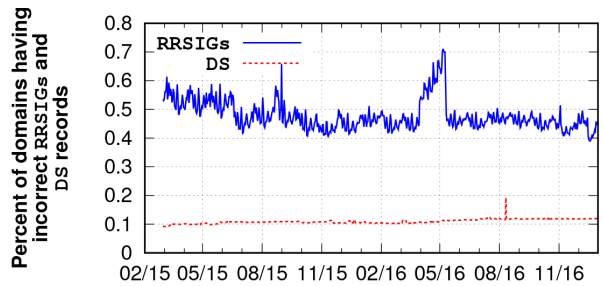

Figure 3: The percent of signed domains for which the RRSIG signatures or DS records are invalid

Uploading DS Records

If a DNS operator wishes to support DNSSEC, a DS record for the domain must be uploaded to the registry (along with the NS record) 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, the operator 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 since the registrar does not know the DS record. 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 email or telephone. Moreover, if a registrar does not support any methods for customers to upload DS records, the domain *cannot* support DNSSEC since it will have a broken chain of trust due to the missing DS record.

Authoritative Name Servers

We begin our analysis of the DNSSEC PKI by focusing on the deployment and management of DNSSEC records by domains and how this has changed over time.

Data Sets

This section describes a large-scale, longitudinal, and detailed study of DNSSEC adoption and deployment at authoritative name servers. To this end, we use data from OpenINTEL [7, 9] concerning domains listed in zone files for the .com, .net, and .org TLDs; together, these contain approximately 150M domains and cover 64% of the Alexa Top-1M (and 75% of the Alexa Top-1K sites). OpenINTEL collects daily snapshots of key DNS records for all of these 150M domains. For this study, we used the NS, DS, SOA, DNSKEY, and RRSIG records that OpenINTEL collected for .com, .net, and .org domains. These daily snapshots span 21 months (between March 1, 2015 and December 31, 2016).

DNSSEC Prevalence

We begin by examining how support for DNSSEC has evolved over time. Specifically, we focus on the number of second-level domains (e.g., amazon.com) that publish at least one DNSKEY record; we refer to these as *signed domains*. Note that having a DNSKEY record published does not by itself imply that the domain has correctly deployed DNSSEC; there could be other missing records or invalid signatures; rather, this indicates that the domain *attempted* to deploy DNSSEC.

Figure 2 plots the fraction of .com, .net, and .org second-level domains that publish at least one DNSKEY record. One key observation is that DNSSEC deployment is rare: between 0.6% (.com) and 1.0% (.org) of domains have DNSKEY records published in our latest snapshot. The fraction of domains that have DNSKEYs is, however, steadily growing. Because the trends of deployment and growth for each TLD are similar, for the remainder of this section, we combine the TLDs into a single data set; breakdowns into different TLDs are available in our recent paper [2].

Incorrect Records

Next, we study whether the DS records and RRSIGs published by signed domains are *correct*: the DS record should match the hash of the DNSKEY, and the RRSIGs should not be expired and should validate against the DNSKEYs. Figure 3 presents the results. We find that the results are largely positive. Almost 99.9% of signed domains have DS records that match their DNSKEY. (The spike that occurred in August 2016 was caused by domains hosted by one authoritative name server, transip.net. This name server suddenly changed DNSKEYs for over 400 domains without switching the DS record, and the problem was corrected the following day.) Similarly, we find that over 99.5% of signed domains have correct RRSIGs and that the majority of the incorrect RRSIGs are due to signature expirations (RRSIGs, unlike DS records, have an expiry timestamp built in).

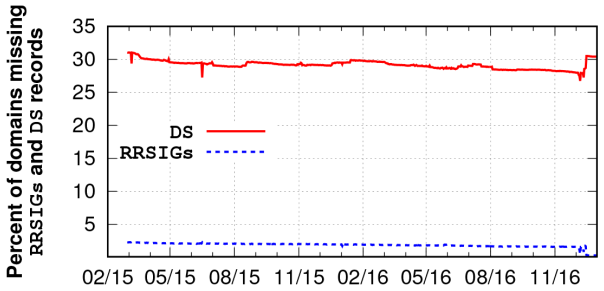

Figure 4: The percentage of signed domains that fail to publish a DS record in the parent zone and RRSIG for SOA and DNSKEY

Missing Records

We now examine whether signed domains are publishing all necessary DNSSEC records. Recall that properly deploying DNSSEC for a domain means that it must have a DS record in the parent zone, DNSKEY records, and RRSIG records for every published record type.

Figure 4 shows the percentage of domains that have DNSKEYs but are missing DS or RRSIG records. We can immediately observe that while a surprisingly low fraction of signed domains are missing RRSIGs (2%, on average), between 28%–32% of signed domains do not have a DS record, meaning they cannot be validated.

Recall that, unlike other DNSSEC record types, DS records are published in the *parent* zone (e.g., .com), along with the domain's NS record. Thus, correctly installing a DS record often requires use of an out-of-band channel, where the administrator contacts its registrar and requests that the registrar adds a DS record. To shed light on why so many domains fail to deploy DS records, we group domains by authoritative name servers (i.e., the DNS operator) to see if certain DNS operators are behind the failures. Table 1 shows the results for the 15 most common domains listed in NS records for authoritative name servers, which cover 83% of the signed domains we study. We find a highly skewed distribution, with most of the name servers publishing DS records for almost all signed domains, but with four failing to upload a DS record for nearly all of their domains. For example, Loopia (a Swedish hosting provider) is authoritative for more than 131,000 domains that publish DNSKEYs, but only *one* of these domains actually uploads a DS record, which is invalid.

Registrars

Having observed that DNSSEC is supported by only 1% of .com, .net, and .org domains, and that over 30% of those domains that try to support DNSSEC fail to do so correctly, we now turn to examine the role that registrars play. To do so, we register domains ourselves and attempt to deploy DNSSEC, both with the registrar as the DNS operator and with ourselves as the DNS operator. We focus on the 31 most popular DNS operators across our data sets, which collectively cover 54.3% of .com, .org, and .net domains in the TLD zone files. Table 2 summarizes the results of this experiment. We make a number of observations below.

Name Servers	Signed	w/DS	Ratio
*.ovh.net	316,960	315,204	99.45%
*.loppia.se	131,726	1	0.00%
*.hyp.net	94,084	93,946	99.85%
*.transip.net	91,103	91,009	99.90%
*.domainmonster.com	60,425	4	0.01%
*.anycast.me	52,381	51,403	98.13%
*.transip.nl	47,007	46,971	99.92%
*.binero.se	44,650	17,099	38.30%
*.ns.cloudflare.com	28,938	17,483	60.42%
*.is.nl	15,738	11	0.07%
*.pcextreme.nl	14,967	14,801	98.89%
*.webhostingserver.nl	14,806	10,655	71.96%
*.registrar-servers.com	13,115	11,463	87.40%
*.nl	12,738	12,674	99.50%
*.citynetwork.se	11,660	13	0.11%

Table 1: Table showing the 15 most popular common domains listed in NS records for authoritative name servers, the total number of signed domains, and the number of domains with a DS record for our latest snapshot (December 31, 2016). The shaded rows represent registrars that fail to publish DS records for nearly all of their domains.

Registrar as 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 because these cases present an easy path to DNSSEC deployment, since the registrar has full control over the domain and could create DNSKEYs, RRSIGs, and upload DS records all on its own. Even more alarming, the three registrars that do support DNSSEC when they are the DNS operator only do so for some of their DNS plans, and *only* NameCheap enables DNSSEC by default. The other two registrars that support DNSSEC also have different policies: GoDaddy provides 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 31, 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, suggesting that the low DNSSEC adoption rates may be heavily influenced by default options and cost.

Registrar	Domains		Registrar DNS operator		Owner DNS operator				
	All	with DNSKEY	DNSSEC default	DNSSEC opt-in	DNSSEC support	DS upload Web	DS upload Email	DS Validation DNSKEY	DS Validation Email
GoDaddy	37,652,477	8,139	✗	●	●	●	-	✗	-
Alibaba	4,292,138	3	✗	✗	✗	-	-	-	-
1AND1	3,802,824	0	✗	✗	✗	-	-	-	-
Network Solution	2,534,673	0	✗	✗	✗	-	-	-	-
eNom	2,525,828	10	✗	✗	●	✗	●	✗	●
Bluehost	2,066,503	0	✗	✗	✗	-	-	-	-
NameCheap	1,963,717	13,232	▲	-	●	●	-	✗	-
WIX	1,887,139	0	✗	✗	-	-	-	-	-
HostGator	1,849,735	0	✗	✗	✗	-	-	-	-
NameBright	1,823,823	0	✗	✗	●	✗	●	✗	▲
register.com	1,311,969	0	✗	✗	✗	-	-	-	-
OVH	1,228,578	319,580	✗	●	●	●	-	●	-
DreamHost	1,117,902	0	✗	✗	●	✗	●	●	▲
WordPress	888,174	3	✗	✗	✗	-	-	-	-
Amazon	865,065	0	✗	✗	●	●	-	▲	-
Xinnet	836,293	0	✗	✗	✗	-	-	-	-
Google	813,945	1,945	✗	✗	●	●	-	✗	-
123-reg	720,435	1	✗	✗	●	●	-	✗	-
Yahoo	690,823	0	✗	✗	✗	-	-	-	-
Rightside	663,616	0	✗	✗	●	●	-	✗	-

Table 2: Table showing the results of our study of registering domains using the 20 registrars among the top 29 DNS operators. The other nine DNS operators are parking services or malware domains. Only three of the 20 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 △s [6]). Only 11 of the registrars support DNSSEC for external name servers, 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 △s).

Owner as DNS operator

Next, we explore how registrars support DNSSEC if the owner acts as the DNS operator (e.g., by hosting their own name server). We find that only 10 of the 20 registrars support DNSSEC for such domains.

Interestingly, only three of the 10 registrars present a DS upload menu on their Web interface when a user switches to an external name server; others use mechanisms such as support tickets or require emails to allow customers to provide DS records. Using email is particularly distressing, since communicating DS records over email opens up security vulnerabilities due to the insecurity of email communication.

DS Record Validation

We now turn our attention to see whether these registrars validate submitted DS records. While registrars are not *required* to validate DS records, they are best positioned to help their customers deploy DNSSEC. We first checked whether the registrars validate the uploaded DS record to ensure it is the hash of the domain's DNSKEY; only two registrars correctly validated the DS record before accepting it. The remaining registrars all allowed us to publish arbitrary data as DS records. We then tested whether the registrars that require emailed DS records would accept an updated DS record without confirming the update. We found that two of the three registrars that require emailed DS records did not attempt to verify the email, meaning an attacker who wished to take control of a victim domain could do so by forging an email to these registrars. We have contacted these two registrars to inform them of this security vulnerability.

DNS Resolvers

Even if domains properly manage their DNSSEC records, end hosts do not enjoy the benefits of DNSSEC unless their DNS resolver requests and validates these records properly. We now examine the DNSSEC behavior of resolvers.

Methodology

A challenge when studying the behavior of resolvers is that most will respond only to local clients (i.e., most are not open resolvers). To address this limitation, we use the Luminati proxy network [1] to issue DNS requests. Luminati is composed of nodes that act as HTTP proxies, which allow us to (1) select the country where the node (managed by Luminati) is located and (2) route HTTP traffic via the node. The node then makes a DNS request for the domain we specify, makes the HTTP request, and returns the response back via the Luminati proxy network.

For this section, we only focus on (1) nodes that are configured with a single resolver and (2) resolvers that we were able to measure with at least 10 different nodes; this represents total 7,599 resolvers covering 328,666 total nodes in 3,582 autonomous systems (ASes). See [1, 2] for more details on this service and the methodology we used for this measurement.

Domain Configuration

For these experiments, we built an authoritative DNS server and Web server for a testbed domain under our control. Our testbed domain (a second-level domain) fully supports DNSSEC functionality with a chain of trust by uploading its DS record to the .com zone.

One of our goals is to examine whether DNSSEC resolvers properly validate DNSSEC records. To do so, we configured our DNS server with 10 different subdomains, each of which simulates a different kind of DNSSEC misconfiguration, along with a single *valid* zone. These misconfigurations include missing, incorrect, and expired RRSIGs, missing DNSKEYs, incorrect DS records, etc.

Results

Of the 7,599 resolvers we examined, we found that 4,427 (58.3%) of them send requests with the DO bit set, suggesting that a majority of resolvers support DNSSEC. We refer to this set of resolvers that request DNSSEC records as *DNSSEC-aware resolvers*. Setting the DO bit by itself, however, does not indicate that the resolvers actually *validate* the DNSSEC responses they receive. To test for proper validation, we look at whether each HTTP request made via a node was successful; because all but one of our DNSSEC records are misconfigured, we would expect all of our HTTP requests (except for those to a single valid domain) to fail validation.

Incorrectly Validating Resolvers

We found that 3,635 of the DNSSEC-aware resolvers (82.1%) from 301 ASes consistently fail to validate the DNSSEC responses, even though they issue the DNS requests with the DO bit set; these resolvers cover 149,373 (78.0%) of the nodes with DNSSEC-aware resolvers. This is especially surprising, as these resolvers all pay the overhead for DNSSEC responses but do not bother to reap DNSSEC's benefits by validating the results they receive.

Country	Hosting ISP	Resolvers	Nodes
Indonesia	PT Telekomunikasi	1,319	2,695
U.S.	Level 3 Communications	522	79,303
U.S.	Time Warner Cable Internet	148	1,133
Germany	Deutsche Telekom AG	104	2,682
Canada	Bell Canada	89	1,120
U.K.	TalkTalk Communications	76	878
U.K.	Sky UK Limited	74	1,535
U.S.	Frontier Communications	63	241
China	China Telecom	56	344
Canada	Rogers Cable Communications	49	1,250
Spain	Telefonica de Espana	48	1,982
U.S.	Charter Communications	46	355
Austria	Liberty Global Operations	40	10,554
U.S.	SoftLayer Technologies	37	2,559
Czech	Avast Software s.r.o.	33	2,731

Table 3: The top 15 ISPs in terms of the number of DNS resolvers that do not validate our DNSSEC response. Level 3 (shaded) has 522 resolvers that do not validate the DNSSEC response, while six do (not shown).

Table 3 shows the top 15 ASes where we observe resolvers that set the bit but do not validate DNSSEC responses; we can immediately observe that these networks include large, popular ISPs in the U.S., the U.K., Canada, and Germany.

Correctly Validating Resolvers

Only 543 of the DNSSEC-aware resolvers (12.2%) from 129 ASes consistently correctly validate DNSSEC responses; these resolvers cover 31,811 (16.6%) of the nodes covered by DNSSEC-aware resolvers. We found surprisingly few large ASes that validate DNSSEC responses; the largest ones include Comcast (U.S.), Orange (Poland), Bahnhof Internet AB (Sweden), Free SAS (France), and EarthLink (Iraq). Interestingly, we found that all validating resolvers successfully validate all misconfigured scenarios; we did not find any resolvers that failed some of our misconfiguration tests but passed others. This is in contrast to client behavior for other PKIs, such as the Web [5], where browsers pass different subsets of validation tests.

Conclusion

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

- First, DNS resolver software should enable DNSSEC validation by default; many popular implementations request DNSSEC records by default, but then completely ignore them.
- Second, 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 has this policy.
- Third, registries should support the "CDS" and "CDNSKEY" proposals [10], which allow domain owners to directly communicate DS records to the registry; unfortunately, we know of very few registries that support CDS and CDNSKEY today.
- Fourth, until CDS and CDNSKEY are fully supported, registrars should work to make the process of uploading DS records easier and more secure.

We also encourage interested readers to read our recent papers on DNSSEC [2, 3], which collectively explore this topic in greater detail.

References

[1] T. Chung, D. Choffnes, and A. Mislove, "Tunneling for Transparency: A Large-Scale Analysis of End-to-End Violations in the Internet," IMC, 2016: https://mislove.org/publications/Luminati-IMC.pdf.

[2] 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," in *Proceedings of the 26th USENIX Security Symposium (Security '17)*: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-chung.pdf.

[3] 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.

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

[5] Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, A. Schulman, and C. Wilson, "An End-to-End Measurement of Certificate Revocation in the Web's PKI," IMC, 2015: https://www.cs.umd.edu/~dml/papers/revocations_imc15.pdf.

[6] Name servers and TLDs supported/unsupported by DNSSEC: http://bit.ly/2fbNjAp.

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

[8] State of DNSSEC Deployment 2016: http://bit.ly/2ye4vfX.

[9] 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*, vol. 34, no. 6, 2016.

[10] P. Wouters and O. Gudmundsson, "Managing DS Records from the Parent via CDS/CDNSKEY," RFC 8078, IETF, 2017: https://datatracker.ietf.org/doc/rfc8078/.