Domain Name System (DNS)

A record: one of the DNS records that contains IP addresses of a domain name
DNS Spoofing

Browser

example.com

A records

1.2.3.4
Advertisement or other contents

DNS Resolver

example.com

A records

1.2.3.4

example.com's Authoritative DNS Server

✗

155.33.17.68

✗

1.2.3.4

155.33.17.68
DNSSEC 101

DNS Resolver

example.com

1.2.3.4

RRSIG

DNSKEY

.example.com's Authoritative DNS Server

.com

.(root)

Chain of Trust
DNSSEC 101

example.com's Authoritative DNS Server

dot (root)
.com
DNSSEC 101: Hierarchy Builds Trust

example.com's Authoritative DNS Server

DS Record = Hash(4c04a5 ... ff0cdd)

RRSIG
DNSSEC 101: Hierarchy Builds Trust

DNS Resolver

example.com's Authoritative DNS Server

DS Record

RRSIG

DNSKEY

DNSKEY

compare!
How to Deploy DNSSEC (Correctly)

1. Have DNSKEYs
2. Generate Signatures
3. Generate and upload DS record to the parent zone
### Scanning All Domains

<table>
<thead>
<tr>
<th>Daily Scans</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLDs</td>
</tr>
<tr>
<td>.com, .org., .net</td>
</tr>
<tr>
<td># of domains</td>
</tr>
<tr>
<td>147M domains</td>
</tr>
<tr>
<td>Interval</td>
</tr>
<tr>
<td>every day</td>
</tr>
<tr>
<td>Period</td>
</tr>
<tr>
<td>2015/03/01 ~ 2016/12/31</td>
</tr>
</tbody>
</table>

Over **750 billion** DNS Records
How DNSSEC is deployed*

DNSKEY

~1.0%

RRSIGs

DS record

Uploads

Deployment

DNSSEC deployment is rare, but growing

* A Longitudinal, End-to-End View of the DNSSEC Ecosystem [USENIX Security’17]
Generating Signatures

RRSIGs are rarely missing (0.3%)

DNSKEY

~1.0%

RRSIGs

~0.3%

DS record
Uploads

Percent of domains missing RRSIGs

0.0
0.5
1.0
1.5
2.0
2.5
02/15 05/15 08/15 11/15 02/16 05/16 08/16 11/16

.com

.net

.org

Missing RRSIGs

* A Longitudinal, End-to-End View of the DNSSEC Ecosystem [USENIX Security’17]
Building a Chain of Trust

Why does DNSSEC deployment remain so small? Why are 30% of domains w/o DS records?

* A Longitudinal, End-to-End View of the DNSSEC Ecosystem [USENIX Security’17]
Open Question
(main part of this talk)

Why is so hard to deploy DNSSEC?

How does registrar policy impact the deployment?
Open Question
(main part of this talk)

Why is so hard to deploy DNSSEC?

How does registrar policy impact the deployment?
Deploying a DNSSEC on Your Server

I need a domain

Registry (TLD)

GoDaddy Registrar

Buy example.com

Owner

DS Record

DS Record
Third Party DNS Operator

Registry (TLD)

.COM (Verisign)

Registrar

GoDaddy

Buy
example.com

Delegate

Third-Party DNS Operator

CloudFlare

DS Record

Buy example.com

Delegate
Third Party DNS Operator

Registry (TLD)

.COM (Verisign)

Registrar

GoDaddy

Third-Party DNS Operator

CloudFlare

Buy example.com

Delegate
Why is it so hard to deploy DNSSEC?

Popular registrar with lots of domains
Checking Registrar’s DNSSEC Policy

Registrar DNS Operator

Registrar Supports DNSSEC?

Registrar Supports DS upload?

Registrar Validates DS record?
## Anecdotal Examples

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>We saw the DNSKEY deployed (but not DS records) so asked why you don’t upload DS records.</td>
<td>[1] They removed a DNSSEC menu</td>
</tr>
<tr>
<td>We asked a registrar to upload a DS record by email from the different email address than the one that registered</td>
<td>[2] “Most people do not understand DNS, so imagine the white faces when I mention DNSSEC”</td>
</tr>
<tr>
<td>We asked a registrar to upload a DS record to our domain via web live chat</td>
<td>It was installed successfully</td>
</tr>
<tr>
<td></td>
<td>It was installed on someone else’s domain due to a mistake by the customer service agent</td>
</tr>
</tbody>
</table>
Details of the Last Example

3:45:32 PM tijay  hg-dnssec.com 3600 IN DS 2371 13 2 129f34c04ac58ece5218b9894148304a736a63757f58ff0cddd9b8df4989

3:56:05 PM Jeniffer S  Awesome! one moment

3:56:09 PM Jeniffer S  I have now save the request information! Manage DNSSEC paananenmusic.com Record added successfully. It can take 4–8 hours for DNS to propagate

3:57:19 PM tijay  paananenmusic.com?

3:57:28 PM tijay  my domain is hg-dnssec.com?

3:58:41 PM Jeniffer S  I apologize, you are right, silly me, one moment
## Popular Registrar’s DNSSEC Policy*

<table>
<thead>
<tr>
<th>Registrar</th>
<th>Registrar DNS Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy (domaincontrol.com)</td>
<td>✓</td>
</tr>
<tr>
<td>NameCheap (registrar-servers.com)</td>
<td>✓</td>
</tr>
<tr>
<td>OVH (ovh.net)</td>
<td>✓</td>
</tr>
<tr>
<td>Google (googledomains.com)</td>
<td>✓</td>
</tr>
<tr>
<td>Alibaba (hichina.com)</td>
<td>✗</td>
</tr>
<tr>
<td>eNom (name-services.com)</td>
<td>✗</td>
</tr>
<tr>
<td>HostGator (hostgator.com)</td>
<td>✗</td>
</tr>
<tr>
<td>NameBright (namebrightdns.com)</td>
<td>✗</td>
</tr>
<tr>
<td>DreamHost (dreamhost.com)</td>
<td>✗</td>
</tr>
<tr>
<td>Amazon (aws-dns)</td>
<td>✗</td>
</tr>
<tr>
<td>123-reg (123-reg.co.uk)</td>
<td>✗</td>
</tr>
<tr>
<td>RightSide** (name.com)</td>
<td>✗</td>
</tr>
<tr>
<td>Network Solution (worldnic.com)</td>
<td>✗</td>
</tr>
<tr>
<td>Bluehost (bluehost.com)</td>
<td>✗</td>
</tr>
<tr>
<td>register.com (register.com)</td>
<td>✗</td>
</tr>
<tr>
<td>The others (5 registrars)</td>
<td>✗</td>
</tr>
</tbody>
</table>

* The results are as of July 2019
** Rightside was acquired by Donuts Inc, in July 2017
## Popular Registrar’s DNSSEC Policy

<table>
<thead>
<tr>
<th>Registrar</th>
<th>Supports DNSSEC?</th>
<th>Supports DS Upload?</th>
<th>Validates DS Record?</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy (domaincontrol.com)</td>
<td>4/20</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>NameCheap (registrar-servers.com)</td>
<td>15/20</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>OVH (ovh.net)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Google (googledomains.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Alibaba (hichina.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>eNom (name-services.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HostGator (hostgator.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>NameBright (namebrightdns.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DreamHost (dreamhost.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Amazon (aws-dns)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>123-reg (123-reg.co.uk)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>RightSide* (name.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Network Solution (worldnic.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Bluehost (bluehost.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>register.com (register.com)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>The others (5 registrars)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### Owner DNS Operator

<table>
<thead>
<tr>
<th>Registrar</th>
<th>Web</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluehost</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>register.com</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Network Solution</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>123-reg</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>RightSide*</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Alibaba</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Amazon</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Google</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>OVH</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>NameCheap</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>GoDaddy</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
# Popular Registrar’s DNSSEC Policy

## Registrar Supports DNSSEC?

1. **GoDaddy** (domaincontrol.com)  
2. **NameCheap** (registrar-servers.com)  
3. **OVH** (ovh.net)  
4. **Google** (googledomains.com)  
5. **Alibaba** (hichina.com)  
6. **eNom** (name-services.com)  
7. **HostGator** (hostgator.com)  
8. **NameBright** (namebrightdns.com)  
9. **DreamHost** (dreamhost.com)  
10. **Amazon** (aws-dns)  
11. **123-reg** (123-reg.co.uk)  
12. **RightSide*** (name.com)  
13. **Network Solution** (worldnic.com)  
14. **Bluehost** (bluehost.com)  
15. **register.com** (register.com)  
16. **The others (5 registrars)**

## Registrar Supports DS upload?

1. **GoDaddy** (domaincontrol.com)  
2. **NameCheap** (registrar-servers.com)  
3. **OVH** (ovh.net)  
4. **Google** (googledomains.com)  
5. **Alibaba** (hichina.com)  
6. **eNom** (name-services.com)  
7. **HostGator** (hostgator.com)  
8. **NameBright** (namebrightdns.com)  
9. **DreamHost** (dreamhost.com)  
10. **Amazon** (aws-dns)  
11. **123-reg** (123-reg.co.uk)  
12. **RightSide*** (name.com)  
13. **Network Solution** (worldnic.com)  
14. **Bluehost** (bluehost.com)  
15. **register.com** (register.com)  
16. **The others (5 registrars)**

## Registrar Validates DS record?

1. **GoDaddy** (domaincontrol.com)  
2. **NameCheap** (registrar-servers.com)  
3. **OVH** (ovh.net)  
4. **Google** (googledomains.com)  
5. **Alibaba** (hichina.com)  
6. **eNom** (name-services.com)  
7. **HostGator** (hostgator.com)  
8. **NameBright** (namebrightdns.com)  
9. **DreamHost** (dreamhost.com)  
10. **Amazon** (aws-dns)  
11. **123-reg** (123-reg.co.uk)  
12. **RightSide*** (name.com)  
13. **Network Solution** (worldnic.com)  
14. **Bluehost** (bluehost.com)  
15. **register.com** (register.com)  
16. **The others (5 registrars)**

## Owner DNS Operator

### DS Upload

<table>
<thead>
<tr>
<th>Registrar</th>
<th>Web</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>NameCheap</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>OVH</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>Google</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>Alibaba</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>eNom</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>HostGator</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>NameBright</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>DreamHost</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>Amazon</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>123-reg</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>RightSide*</td>
<td>✅</td>
<td>—</td>
</tr>
<tr>
<td>Network Solution</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Bluehost</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>register.com</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>The others (5 registrars)</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>

### DS Validation

- ✅: Supports
- ✗: Does not support
- 🟢: Supports with warning

- **GoDaddy**: ✗
- **NameCheap**: ✗
- **OVH**: ✗
- **Google**: ✗
- **Alibaba**: ✗
- **eNom**: ✗
- **HostGator**: ✗
- **NameBright**: ✗
- **DreamHost**: ✗
- **Amazon**: ✗
- **123-reg**: ✗
- **RightSide***: ✗
- **Network Solution**: ✗
- **Bluehost**: ✗
- **register.com**: ✗
- **The others (5 registrars)**: ✗
# Summary: Registrar’s DNSSEC Support

<table>
<thead>
<tr>
<th>Support DNSSEC?</th>
<th>DNS Operator</th>
<th># of Registrar</th>
<th>What this means to you</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar</td>
<td></td>
<td>4/20</td>
<td>If you don’t want to run your own name server, most of the time, you CAN’T deploy DNSSEC (16/20)</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
<td>15/20</td>
<td>If you do want run your own nameserver, still you CAN’T deploy DNSSEC for 5/20</td>
</tr>
<tr>
<td>Check DS Validation</td>
<td>Owner</td>
<td>5/15</td>
<td>If you happen to upload an incorrect DS record, your domain will be inaccessible</td>
</tr>
</tbody>
</table>

Why are DNSSEC support of registrars so rare?
## Cost of Managements

<table>
<thead>
<tr>
<th></th>
<th>DNS</th>
<th>DNSSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong># of Records</strong></td>
<td>DNS</td>
<td>DNSSEC introduces much more records (e.g., need signatures for each record)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Size of Records</strong></td>
<td>DNS</td>
<td>DNSSEC: Signatures are usually 3~6 times larger than non-DNSSEC records*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>DNS</td>
<td>DNSSEC: Strong Key Unique Key Rollover</td>
</tr>
</tbody>
</table>

*DNSSEC and Its Potential for DDoS Attacks (IMC’14)

---

Operational Cost: Operational cost of DNSSEC is higher than that of DNS
Case Study: Registrar’s Policy

# of registrars: 4
- Free: 3
- Paid: 1

Registrars manage all DNS records

Registrars DO NOT need to manage DNS records at all

Support DNSSEC | Pricing
--- | ---
Free: 3
Paid: 1

Support DNSSEC | Pricing
--- | ---
15 Free
<table>
<thead>
<tr>
<th>Support DNSSEC?</th>
<th>DNS Operator</th>
<th># of Registrar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar</td>
<td>4/20</td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td>15/20</td>
<td></td>
</tr>
<tr>
<td>Check DS Validation</td>
<td>Owner</td>
<td>5/15</td>
</tr>
</tbody>
</table>

Still a way to go, but it has been improved
Outline

Why is DNSSEC deployment so rare?

How does a registrar policy impact the deployment?

We need historical dataset
## Scanning All Domains

<table>
<thead>
<tr>
<th>TLD</th>
<th>Measurement Period (Daily Scan)</th>
<th>Domains</th>
<th>Percent w/ DNSKEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>2015/03/01 ~ 2016/12/31</td>
<td>118,147,199</td>
<td>0.7%</td>
</tr>
<tr>
<td>.net</td>
<td>2015/03/01 ~ 2016/12/31</td>
<td>13,773,903</td>
<td>1.0%</td>
</tr>
<tr>
<td>.org</td>
<td>2015/03/01 ~ 2016/12/31</td>
<td>9,682,750</td>
<td>1.1%</td>
</tr>
<tr>
<td>.nl</td>
<td>2016/02/09 ~ 2016/12/31</td>
<td>5,674,208</td>
<td>51.6%</td>
</tr>
<tr>
<td>.se</td>
<td>2016/06/07 ~ 2016/12/31</td>
<td>1,388,372</td>
<td>46.7%</td>
</tr>
</tbody>
</table>
## Scanning All Domains

<table>
<thead>
<tr>
<th>TLD</th>
<th>Measurement Period (Daily Scan)</th>
<th>Domains</th>
<th>Percent w/ DNSKEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>2015/03/01 ~ 2019/06/19</td>
<td>140,438,505</td>
<td></td>
</tr>
<tr>
<td>.net</td>
<td>2015/03/01 ~ 2019/06/19</td>
<td>13,408,301</td>
<td></td>
</tr>
<tr>
<td>.org</td>
<td>2015/03/01 ~ 2019/06/19</td>
<td>10,066,388</td>
<td></td>
</tr>
<tr>
<td>.nl</td>
<td>2016/02/09 ~ 2019/06/19</td>
<td>5,860,418</td>
<td></td>
</tr>
<tr>
<td>.se</td>
<td>2016/06/07 ~ 2019/06/19</td>
<td>1,450,441</td>
<td></td>
</tr>
</tbody>
</table>
Financial gain is a huge incentive for deploying DNSSEC.
Free DNSSEC support encourages users to deploy DNSSEC
Complex relationship between reseller and registrar also result in slow deployment of DNSSEC

DNS Operator

Third-Party

CloudFlare

Owner

Reseller

Antagonist

Registrar

ASCIO

Registry

Verisign

Third-Party

DS Record

DS Record

DS Record

DS Record

DS Record

Cloudflare announced universal DNSSEC

Third-party DNS Operator

Deploying DNSSEC is even harder for users using third-party DNS Operators
Conclusion

• **Registrars** play a critical role in supporting DNSSEC today
  • Only 5 out of 20 registrars support DNSSEC on their authoritative nameservers
  • 15 out of 20 registrars support uploading a custom DS record
  • Comparing to 2017 it has been improved, but it requires more effort

• DNSSEC deployment depends on many policies
  • **Registrar**: Free
  • **Registry**: Financial incentive
  • **Reseller**: Beware to choose a partner (i.e., registrar)
  • **Third-party**: CDS/CDNSSKEY