Automatic DNSSEC Bootstrapping using Authenticated Signals from the Zone's Operator

draft-ietf-dnsop-dnssec-bootstrapping

IETF DNSOP Interim
May 24, 2022

Peter Thomassen (deSEC, Secure Systems Engineering)
Nils Wisiol (deSEC, Technische Universität Berlin)
Reminder: CDS Authentication via Trusted Hostname

Use an established chain of trust (left) to take a detour
- co-publish
- authenticated, immediate
- no active on-wire attacker

Extends RFC 8078 to add authentication for initial DS
Status

● Adopted by DNSOP WG in April

● Wrote post for APNIC Blog to get the word out
  ○ https://blog.apnic.net/2022/03/08/authenticated-bootstrapping-of-dnssec-delegations/

● Implementations:
  ○ Prototype implementation: github.com/desec-io/dsbootstrap
  ○ CoCCA: implementation underway for 59 ccTLDs
  ○ GoDaddy: implementation planned after CDS scanning
  ○ .cl: implementation finished, waiting for internal approval
  ○ implementations by other registries and DNS operators under way
Open Issue 1: Support requirements

- Assume that a DNS operator supports the protocol

- Should the operator be REQUIRED to serve bootstrapping records for all their domains?

- Suggestion: No, as it won’t work with zones with secondary-only service
Open Issue 2: IANA action?

- Do we need a IANA action section to reserve the `_dsauth` label?
Open Issue 3: Delegations within a bootstrapping zone

- At IETF 112, it was discussed whether owner names of bootstrapping records should be
  - “plain”, e.g. `example.co.uk._dsauth.ns1.desec.io`, or
  - “hashed”, e.g. `example.<hash(co.uk)>._dsauth.ns1.desec.io`.

There appears to be consensus to use the plain approach.

- **Plain approach causes ambiguities** with zone cuts underneath `_dsauth` label
  - CDS/CDNSKEY record ambiguous e.g. with zone cut at `co.uk._dsauth.ns1.desec.io`
  - Details: [https://mailarchive.ietf.org/arch/msg/dnsop/FE5Sm5vzZtq9VgKxgkfmy4VuV18/](https://mailarchive.ietf.org/arch/msg/dnsop/FE5Sm5vzZtq9VgKxgkfmy4VuV18/)

- **How to remove the ambiguity?**
  - Ideally, solution would preserve commonplace protocol guarantees:
    all domains are equal (from a protocol perspective), delegations are allowed everywhere
Open Issue 3: Solution options – Decision needed

1. Use a different record type
   ○ e.g. BDS/BDNSKEY (“bootstrapping DS/DNSKEY”)

2. Use a hashed naming scheme to avoid the collision
   ○ ruled out

3. Allow bootstrapping only using the leaf domain under _dsauth
   ○ implies certain assumptions on the order in which delegations are done
   ○ treats some domains special: breaks bootstrapping for non-leaf domains under _dsauth

4. Disallow CDS/CDNSKEY usage for rollovers of subzones under _dsauth
   ○ “bootstrapping has precedence”
   ○ treats some domains special: breaks rollovers for domains under _dsauth

5. Disallow zone cuts underneath a _dsauth label entirely
   ○ treats some domains special: domains under _dsauth can’t be delegated

6. Use an underscore prefix for the actual signal
   ○ _dsauth.example.co.uk._signal.ns1.desec.io
   ○ would also allow other kinds of signals (multi-signer?)
Next steps

- Authors consider the protocol rather mature
  - Some things still needed!

- Document review and suggestions for improvement, especially
  - Section 3.3 (Triggers)
  - Section 6 (Security Considerations)

- Implementations!
Backup  (some slides may be from previous revisions)
Detail: Transfer Trust from the DNS Operator

1. **Create a signaling mechanism for DNS operators**
   - **What?**
     - allow publishing *arbitrary information* about the zones they are authoritative for
     - in an *authenticated* fashion, *on a per-zone basis*
   - **How?**
     - use namespace **under each nameserver hostname**, e.g. `_boot.ns1.desec.io`
     - require **DNSSEC** under this namespace (requires nameserver domains to be secure)
     - under this namespace, **announcements** are made using *zone-specific owner names*

2. **Use this mechanism to publish an authentication signal**
   - start with **CDS/CDNSKEY records at the apex** of the target zone (RFC 8078)
   - co-publish these records using the signaling mechanism (signed with NS zone’s keys)

3. **Validate** the target domain’s CDS/CDNSKEY records **against this signal**
   - if successful: “transfer trust to the target domain” → **provision DS records** at the parent
   - **clean up** records when done
Technical Considerations

- No collision with primary use of CDS/CDNSKEY (those are apex-only)

- Add extra label: example.co.uk._dsauth.ns1.provider.net
  - to enable delegation of signaling data to separate zone

- Name scheme features:
  - removes risk of accidentally modifying the nameserver’s A/AAAA records
  - reduces churn on nameserver zone
  - allows splitting off DNS operations (e.g. online-signing with different key; delegate by parent)
Survey on Deployment Requirements

● DS bootstrapping requires that NS targets are not part of the same zone
  ○ mostly the case: > 99% of NS targets are out of bailiwick
    in bailiwick: < 0.33% for .com, < 0.72% for .net (thanks to John Levine)

● Secure signaling requires NS targets to be in securely delegated zones
  ○ How frequent is that?
  ○ For each domain in Tranco Top 1M dataset, extract
    a. whether the domain itself is secure (has validation path),
    b. all NS targets in the delegation,
    c. which NS targets are secure (if any),

... and compute things like
Bootstrappability: A domain is bootstrappable if b == c, but a == false
Survey on Deployment Requirements: Bootstrappability

Measurement failure rate..............................: 2.30%
Remaining sample size.................................: 977007
Proportion of secure zones.............................: 5.43%
Proportion of signed zones..............................: 6.84%
Proportion of zones with all nameserver targets secure: 24.63%
Proportion of zones with ≥ 1 nameserver targets secure: 25.97%

bootstrappable:
  domain is not secure and NS targets have validation path → signaling possible

Proportion of bootstrappable zones (all NS) ..........: 22.11%
Proportion of bootstrappable zones (≥ 1 NS) ..........: 23.07%

as of 22 October 2021
Survey on Deployment Requirements: by TLD, by Provider

<table>
<thead>
<tr>
<th>tld</th>
<th>zones total count</th>
<th>signed rel.</th>
<th>secure rel.</th>
<th>bootstrappable rel.</th>
<th>bootstrappable abs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>com</td>
<td>513660</td>
<td>4.5%</td>
<td>3.4%</td>
<td>23.2%</td>
<td>119195</td>
</tr>
<tr>
<td>org</td>
<td>71332</td>
<td>4.8%</td>
<td>3.7%</td>
<td>17.8%</td>
<td>12664</td>
</tr>
<tr>
<td>net</td>
<td>46232</td>
<td>6.8%</td>
<td>5.4%</td>
<td>22.1%</td>
<td>10231</td>
</tr>
<tr>
<td>ru</td>
<td>32387</td>
<td>7.3%</td>
<td>2.0%</td>
<td>13.9%</td>
<td>4511</td>
</tr>
<tr>
<td>uk</td>
<td>21003</td>
<td>4.3%</td>
<td>3.4%</td>
<td>18.8%</td>
<td>3945</td>
</tr>
<tr>
<td>in</td>
<td>9595</td>
<td>7.3%</td>
<td>5.7%</td>
<td>28.3%</td>
<td>2719</td>
</tr>
<tr>
<td>io</td>
<td>7673</td>
<td>8.6%</td>
<td>6.2%</td>
<td>34.9%</td>
<td>2677</td>
</tr>
<tr>
<td>xyz</td>
<td>4054</td>
<td>6.1%</td>
<td>5.1%</td>
<td>55.6%</td>
<td>2254</td>
</tr>
<tr>
<td>co</td>
<td>7408</td>
<td>10.6%</td>
<td>8.7%</td>
<td>29.7%</td>
<td>2201</td>
</tr>
<tr>
<td>online</td>
<td>3202</td>
<td>3.3%</td>
<td>2.4%</td>
<td>68.1%</td>
<td>2180</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ns_rname</th>
<th>zones total count</th>
<th>signed rel.</th>
<th>secure rel.</th>
<th>bootstrappable rel.</th>
<th>bootstrappable abs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.cloudflare.com</td>
<td>252145</td>
<td>6.1%</td>
<td>3.1%</td>
<td>76.5%</td>
<td>192895</td>
</tr>
<tr>
<td>dns.hostinger.com</td>
<td>4141</td>
<td>0.1%</td>
<td>0.0%</td>
<td>87.8%</td>
<td>3634</td>
</tr>
<tr>
<td>hostmaster.nsonone.net</td>
<td>19911</td>
<td>1.1%</td>
<td>0.9%</td>
<td>12.9%</td>
<td>2568</td>
</tr>
<tr>
<td>nan</td>
<td>80403</td>
<td>9.2%</td>
<td>8.6%</td>
<td>2.6%</td>
<td>2066</td>
</tr>
<tr>
<td>hostmaster.cscdnns.net</td>
<td>6041</td>
<td>1.8%</td>
<td>1.7%</td>
<td>22.8%</td>
<td>1375</td>
</tr>
<tr>
<td>dns.openprovider.eu</td>
<td>1290</td>
<td>1.0%</td>
<td>0.8%</td>
<td>91.7%</td>
<td>1183</td>
</tr>
<tr>
<td>postmaster.ii.j.ad.jp</td>
<td>935</td>
<td>2.0%</td>
<td>2.0%</td>
<td>98.0%</td>
<td>916</td>
</tr>
<tr>
<td>ntsld.verisign-grs.com</td>
<td>8531</td>
<td>90.4%</td>
<td>90.4%</td>
<td>7.5%</td>
<td>637</td>
</tr>
<tr>
<td>root.v1.wpxhosting.com</td>
<td>617</td>
<td>0.3%</td>
<td>0.3%</td>
<td>99.7%</td>
<td>615</td>
</tr>
<tr>
<td>nsadmin.nic.in</td>
<td>771</td>
<td>29.4%</td>
<td>29.4%</td>
<td>70.6%</td>
<td>544</td>
</tr>
</tbody>
</table>

*as of 22 October 2021, “nan” ns_rname means that referenced NS zones have more than one rname in their SOAs*
<table>
<thead>
<tr>
<th>BOOTSTRAPPING INVOLVES</th>
<th>MANUAL</th>
<th>BOOTSTRAPPING METHOD</th>
<th>PROPOSED</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone operator $Z$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>domain owner</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>registrar</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>registry</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**ACTORS WHO CAN INITIALIZE KEYS**

**Required parties (trusted)**

<table>
<thead>
<tr>
<th>Role</th>
<th>Manual</th>
<th>CDS/CDNSKEY</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>registrar</td>
<td>✓</td>
<td>✓²</td>
<td>✓²</td>
</tr>
<tr>
<td>NS zone operator</td>
<td>x</td>
<td>✓³ (✓)</td>
<td>(✓)</td>
</tr>
<tr>
<td>NS zone ancestors</td>
<td>x</td>
<td>✓³ (✓)</td>
<td>(✓)</td>
</tr>
<tr>
<td>NS zone owner</td>
<td>x</td>
<td>✓³ (✓)</td>
<td>(✓)</td>
</tr>
</tbody>
</table>

**Others parties (untrusted)**

<table>
<thead>
<tr>
<th>Role</th>
<th>Manual</th>
<th>CDS/CDNSKEY</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>active on-wire attacker</td>
<td></td>
<td>✓³</td>
<td>x</td>
</tr>
<tr>
<td>social engineering attacker [1]</td>
<td>✓</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Manual</th>
<th>CDS/CDNSKEY</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Comparison of methods for establishing a new secure delegation, displaying a) entities involved in the bootstrapping of an individual insecure zone, b) attack surface towards trusted and untrusted third parties, and c) prerequisites, key material authentication, and bootstrapping duration. Key initialization within parentheses (✓) requires collusion across all NS zones. ¹ For offline signing, only the signing key holder is involved. ² Registry could refuse deployment through registrar. ³ Requires knowledge of private key. ⁴ Several vantage points and long time must be covered.