Measurement Survey of Server–Side DNSSEC Adoption

Matthäus Wander

<matthaeus.wander@uni-due.de>

TMA Conference 2017
Maynooth, Ireland, June 23, 2017
DNSSEC
Signed Response

Query: www?

Response

www A 192.0.2.1
NSEC: Denial of Existence

Query: test?

ns1 NSEC www

Not found

Proof of non-existence via nearest existing names
NSEC3: Hashed Denial of Existence

Query: test?

Proof of non-existence via nearest hash values of existing names

Not found
NSEC3: Hash Function

Domain name
Salt

Multiple hash iterations

SHA-1

NSEC3 hash value
Zone Enumeration
Research Questions

1. Can we perform zone enumeration over all top-level domains?
   - Will it work for NSEC3?

2. What is the DNSSEC deployment state?
   - How many domains are signed?
   - How prevalent are validation failures?
Methodology

- Send queries for non-existing domain names
- NSEC zone enumeration yields domain names
- NSEC3 zone enumeration yields hash values
  - Recover cleartext names with GPU hashing power
DNSSEC Domains

40% of all DNSSEC domains below .nl

92% of all DNSSEC domains below top 10 TLDs
DNSSEC vs. unsigned Domains

Universität Duisburg-Essen
Verteilte Systeme

Matthäus Wander
Total Number of DNSSEC Domains: 6.4 million

Complete* figure as of January 2017

* limitations apply
Figure includes only Second-Level Domains

- **root**
  - org
    - example.org
    - iana.org
    - ietf.org
  - uk
    - ac.uk
    - co.uk

Zone enumeration on TLD returns second-level domains.

Third-level domains not found:
- abdn.ac.uk
- google.co.uk
NSEC3 Cleartext Recovery

- 5.7 million NSEC3 hash values from 1196 TLDs
  - Partial brute-force and dictionary attack
  - 7 graphic cards running for two weeks
  - 4.5 million DNSSEC names recovered (79%)

- NSEC3 has hidden 21% DNSSEC names from us
  - At higher operational costs (server must compute NSEC3 hash value for each negative response)
Cleartext Recovery Ratio

Universität Duisburg-Essen
Verteilte Systeme

Matthäus Wander
What helps against Zone Enumeration?

- **Broken NSEC/NSEC3 chain**
  - Not practical: validation will fail on benign clients

- **Frequent re-signing with new salt**
  - Expensive: new signatures every few seconds/minutes
  - Beware: malicious attacker will increase query rate

- **Online signing with NSEC3 or NSEC5**
  - Expensive: new signature for each negative response
What helps **not** against Zone Enumeration?

- Increase hash iteration count?
  - Slows down attack but not to a degree that helps

<table>
<thead>
<tr>
<th>TLD</th>
<th>NSEC or NSEC3?</th>
<th>DNSSEC Domains</th>
<th>Cleartext Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>22. mx</td>
<td>NSEC3, opt-out i=100</td>
<td>7,924</td>
<td>80%</td>
</tr>
<tr>
<td>132. lat</td>
<td>NSEC3, opt-out i=100</td>
<td>200</td>
<td>79%</td>
</tr>
<tr>
<td>187. la</td>
<td>NSEC3, opt-out i=150</td>
<td>105</td>
<td>96%</td>
</tr>
<tr>
<td>40. name</td>
<td>NSEC3, opt-out i=0</td>
<td>1,694</td>
<td>43%</td>
</tr>
<tr>
<td>71. jp</td>
<td>NSEC3, opt-out i=8</td>
<td>453</td>
<td>39%</td>
</tr>
<tr>
<td>112. xn--3e0b707e</td>
<td>NSEC3, opt-out i=10</td>
<td>257</td>
<td>8%</td>
</tr>
</tbody>
</table>

Many iterations, high recovery

Few iterations, low recovery
Analysis of Signed Second–Level Domains

- Query 5.1 million signed second–level domains for their DNSSEC configuration (DS and DNSKEY record sets)
Signing Algorithms

Most frequent: RSA (92%)

ECDSA growing (8%)

Few DSA keys
# Validation Failures

<table>
<thead>
<tr>
<th>Result</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>No DNSKEY (dangling DS)</td>
<td>19,386</td>
</tr>
<tr>
<td>No trusted DNSKEY (dangling DS)</td>
<td>1,216</td>
</tr>
<tr>
<td>No RRSIG for trusted DNSKEY</td>
<td>380</td>
</tr>
<tr>
<td>Signature expired</td>
<td>1,799</td>
</tr>
<tr>
<td>Signature ahead of time</td>
<td>1</td>
</tr>
<tr>
<td>Signature verify failure</td>
<td>49</td>
</tr>
<tr>
<td>Validation failure</td>
<td>22,831</td>
</tr>
<tr>
<td>Validation success</td>
<td>5,092,022</td>
</tr>
</tbody>
</table>

- **DNSSEC failure**: 0.44%
- **Other failure**: 0.48%
- **No failure**: 99%
Conclusions 1/2

- DNSSEC signing is **common** among a few TLDs
  - 6.4 million signed second-level domains
- Validation **failures** are rare (0.44%) but visible
- NSEC3 **protects** minor portion of names (21%)
  - Hash iteration count does not affect the recovery ratio
- Effective protection is **expensive** (online signing)
Conclusions 2/2

- Zone enumeration is useful for debugging
  - Find broken NSEC/NSEC3 chains or erroneous servers

- TLD measurements give an incomplete picture
  - How to get a list of associated second–level domains?

- Suggestion: Use Mozilla‘s Public Suffix List
  - First section (ICANN domains), omit private domains
# Top-Level Domain Statistics

<table>
<thead>
<tr>
<th></th>
<th>TLD</th>
<th>NSEC or NSEC3?</th>
<th>DNSSEC Domains</th>
<th>Adoption Ratio</th>
<th>Cleartext Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>nl</td>
<td>NSEC3, opt-out, i=5</td>
<td>2,592,219</td>
<td>45%</td>
<td>78%</td>
</tr>
<tr>
<td>2.</td>
<td>se</td>
<td>NSEC</td>
<td>673,262</td>
<td>49%</td>
<td>all</td>
</tr>
<tr>
<td>3.</td>
<td>cz</td>
<td>NSEC3, i=10</td>
<td>655,529</td>
<td>52%</td>
<td>82%</td>
</tr>
<tr>
<td>4.</td>
<td>com</td>
<td>NSEC3, opt-out, i=0</td>
<td>614,209</td>
<td>&lt;1%</td>
<td>75%</td>
</tr>
<tr>
<td>5.</td>
<td>no</td>
<td>NSEC3, opt-out, i=5</td>
<td>409,416</td>
<td>57%</td>
<td>81%</td>
</tr>
<tr>
<td>6.</td>
<td>eu</td>
<td>NSEC3, opt-out, i=1</td>
<td>355,157</td>
<td>9%</td>
<td>91%</td>
</tr>
<tr>
<td>7.</td>
<td>fr</td>
<td>NSEC3, opt-out, i=1</td>
<td>304,663</td>
<td>10%</td>
<td>67%</td>
</tr>
<tr>
<td>8.</td>
<td>be</td>
<td>NSEC3, opt-out, i=5</td>
<td>127,177</td>
<td>8%</td>
<td>82%</td>
</tr>
<tr>
<td>9.</td>
<td>hu</td>
<td>NSEC3, opt-out, i=5</td>
<td>107,434</td>
<td>15%</td>
<td>70%</td>
</tr>
<tr>
<td>10.</td>
<td>net</td>
<td>NSEC3, opt-out, i=0</td>
<td>101,872</td>
<td>&lt;1%</td>
<td>88%</td>
</tr>
</tbody>
</table>

[1357 others omitted]  
**Total: 6,441,427**