DANE/SMTMP
Usage Report

Viktor Dukhovni  
Two Sigma  
<ieth-dane@dukhovni.org>

Wes Hardaker  
USC/ISI  
<hardaker@isi.edu>
Overview

1. Background

2. E-Mail Security without DANE

3. E-Mail Security with DANE

4. DNSSEC and DANE deployment statistics

5. Appendix
DANE SMTP Monitoring
https://stats.dnssec-tools.org

- https://stats.dnssec-tools.org/
  - Created by Viktor Dukhovni and Wes Hardaker
  - A continually updating web-page

Recent changes:
- New data sources added
- More graphs added
  - DNSSEC growth
- Tables are sortable (click on the column name)
DNSSEC / DANE Survey
(all work by Viktor Dukhovni)

- Monitors domains delegated from public suffixes
- Notifies operators of botched key/cert rotation
- Sourced from ICANN CZDS, Verisign, https://scans.io/, open access for .se, .nu, .fr, .nl, ...
  (more ccTLD data wanted), FarSight Security

- Covers ~200 million candidate domain names
- Captures DS, DNSKEY, MX, A, AAAA, TLSA records
- Captures certificate chains of MX hosts
Survey Stats
(as of 2019-06-20)

• 9.87 million domains with DNSSEC-validated MX

• **1.18 million** domains with DANE-enabled SMTP
  - (was only 300 thousand in Barcelona!!)

• Millions of users (gmx.de, web.de, comcast.net)

• DANE-enabled MX servers in 4468 zones
DANE/DNSSEC Deployment Awards

- Best improvement
  - .bank 58.10% → 98.48% DNSSEC problem free!
- Best DANE deployment
  - one.com published 707k DANE/TLSA records
- TLDs with 100% working DNSKEY records
  - .boston
  - .bible
- Large-volume TLD working DNSKEY records
  - .br → 99.6% working
  - Via active monitoring
From LAST TIME

#Domains using SMTP/DANE
# Zones of DANE MX hosts

![Chart showing the growth of zones hosting DANE/SMTP servers from 2016/07 to 2019/07. The graph indicates a steady increase in the number of zones over time.](chart.png)
# Zones with DS Records

![Graph showing the number of zones with DS records over time. The graph indicates a steady increase in the number of zones with DS records from 2018 to 2019.](image-url)

- **ICANN Barcelona**: The graph includes a vertical line indicating the ICANN Barcelona event, which occurred in 2018.
- **DS record sets**: The graph shows the trend of DS record sets over time, with a clear upward trend from 2018 to 2019.
# Zones with DS Records

Notes:
1) Gentle downslopes are from zones disappearing over time
2) Sharp increases are from new weekly/monthly data imports
## Noteworthy new SMTP/DANE providers

<table>
<thead>
<tr>
<th>Provider</th>
<th>Deployed SMTP/DANE Records</th>
<th>Initial Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>one.com</td>
<td>706,991</td>
<td>2018-11-23</td>
</tr>
<tr>
<td>web4u.cz</td>
<td>27,341</td>
<td>2019-05-30</td>
</tr>
<tr>
<td>flexfilter.nl</td>
<td>15,759</td>
<td>2019-03-26</td>
</tr>
<tr>
<td>onebit.cz</td>
<td>12,994</td>
<td>2019-01-16</td>
</tr>
<tr>
<td>zxcs.nl</td>
<td>12,311</td>
<td>2019-04-09</td>
</tr>
<tr>
<td>netzone.ch</td>
<td>6,007</td>
<td>2019-03-26</td>
</tr>
<tr>
<td>ips.nl</td>
<td>3,760</td>
<td>2019-03-09</td>
</tr>
</tbody>
</table>
## Top DNSSEC TLDs

<table>
<thead>
<tr>
<th>DNSSEC domains x1000</th>
<th>TLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,144</td>
<td>NL</td>
</tr>
<tr>
<td>1,205</td>
<td>COM</td>
</tr>
<tr>
<td>764</td>
<td>SE</td>
</tr>
<tr>
<td>698</td>
<td>CZ</td>
</tr>
<tr>
<td>560</td>
<td>BR</td>
</tr>
<tr>
<td>492</td>
<td>EU</td>
</tr>
<tr>
<td>450</td>
<td>PL</td>
</tr>
<tr>
<td>408</td>
<td>FR</td>
</tr>
<tr>
<td>382</td>
<td>NO</td>
</tr>
<tr>
<td>286</td>
<td>BE</td>
</tr>
<tr>
<td>152</td>
<td>NET</td>
</tr>
<tr>
<td>123</td>
<td>HU</td>
</tr>
<tr>
<td>111</td>
<td>ORG</td>
</tr>
<tr>
<td>109</td>
<td>NU</td>
</tr>
<tr>
<td>87</td>
<td>CH</td>
</tr>
<tr>
<td>500</td>
<td>other</td>
</tr>
</tbody>
</table>
Leader of the Pack: .nl

nl DNSSEC Domains

Count

Time

ICANN65 | Marrakech, Morocco | June 2019
Consistency is Key: .app

app DNSSEC Domains
Smooth Operations: .dev

dev DNSSEC Domains
Big Jump: .be

be DNSSEC Domains
Big Jump: .de

de DNSSEC Domains

Count

Time

2018/11/02 00:00
2018/12/22 00:00
2019/02/10 00:00
2019/04/01 00:00
2019/05/21 00:00
Lots of Small Big Jumps: .cz

cz DNSSEC Domains

Count

Time

2018/11/02 00:00 2018/12/22 00:00 2019/02/10 00:00 2019/04/01 00:00 2019/05/21 00:00

ICANN65 | Marrakech, Morocco | June 2019
Some Loss Of Course Too

nu DNSSEC Domains
Some Disable and Re-enables Of Course

se DNSSEC Domains
DNSSEC checklist

• Keep name-server software up to date
• Test zones with apex wildcard A or CNAMEs
• Test zones with empty non-terminals
• Always sign after changing SOA serial numbers
• Avoid NSEC3 opt-out in most zones
• Avoid high NSEC3 (extra) iteration counts
  - (0 is BCP!)

https://lists.dns-oarc.net/pipermail/dns-operations/2017-December/017127.html
https://lists.dns-oarc.net/pipermail/dns-operations/2018-January/017173.html
DNSSEC Hygiene

• All nameservers need:
  - EDNS(0) support
  - NSEC3 support

• Don't block IP fragments

• Reply NODATA or NXDomain
  - (not NOTIMP, REFUSED, ...)

• Test correct denial-of-existence for each edge case

• Monitor nameservers for correct DNSSEC handling
Rolling Your TLS Keys

• Use multiple TLSA records to publish current and future keys
  - Publish **TLSA records of keys** well in advance of using new certificates
  - Required by DNS caching (publish 2xTTL ahead)

• Two pre-publishing models:
  - EE Key + Next EE Key: \((3 \ 1 \ 1 + 3 \ 1 \ 1)\)
  - EE Key + TA Key: \((3 \ 1 \ 1 + 2 \ 1 \ 1)\)

• Deploy new chain, and publish new TLSA records:
  _25._tcp.mx.example.com. IN TLSA 3 1 1 curr-pubkey-sha256
  _25._tcp.mx.example.com. IN TLSA 3 1 1 next-pubkey-sha256
Automate

• Automate:
  - TLSA record updates and zone re-signing
  - Key rollover
  - Acquiring any certs ...
  - ... and converting to TLSA records

• Have working contacts in WHOIS, SOA, postmaster
DANE Resources

Dane implementation resources:
- https://github.com/baknu/DANE-for-SMTP/wiki/2.-Implementation-resources

Reasons for 3 1 1, and 3 1 1 + 3 1 1 key rollover info:
- https://github.com/danefail/list/issues/47#issuecomment-456623996
- https://mail.sys4.de/pipermail/dane-users/2018-February/000440.html

NYLUG talk slides and video:
- https://youtu.be/A8SgW9y__io

Internet.nl "toolbox" DANE wiki (Work in progress):
- https://github.com/internetstandards/toolbox-wiki
Help wanted

• More ccTLD lists of signed delegations

• Fix any DNSSEC issues
  - Including ones centered on Denial of Existence!

• Please enable DANE **outbound**
  - (even if your own domain is unsigned)

• Please enable DNSSEC and DANE on hosting MX servers
  - Especially when hosting thousands signed domains
    • e.g. ovh.net, googlemail.com, ...
Questions?
https://stats.dnssec-tools.org/

Viktor Dukhovni  
<ietf-dane@dukhovni.org>  

Wes Hardaker  
<hardaker@isi.edu>