DNSSEC and DANE Deployment
Trends, Tools And Challenges

Dan York, Senior Content Strategist
Internet Society

ENOG 6, Kiev, Ukraine
October 2, 2013
About Deploy360

The Challenge:
- The IETF creates protocols based on open standards, but some are not widely known or deployed
- People seeking to implement these protocols are confused by a lack of clear, concise deployment information

The Deploy360 Solution:
- Provide hands-on information on IPv6, DNSSEC and routing resiliency/security to advance real-world deployment
- Work with first adopters to collect and create technical resources and distribute these resources to fast following networks
Deploy360 Components

Web Portal
(Online Knowledge Repository)
- Technical documents
- Audience-specific information
- Blogs & social media

Social Media
(Constant Audience Engagement)
- Twitter
- Facebook
- Google+
- YouTube
- RSS Feeds

Speaking Engagements
(Come Meet Us or Invite Us to Speak)
- Consumer Electronics Show
- IPv6 Summits
- Interop
- Network Operators’ Groups

ION Conferences
(Hands-on Educational Events)
- Slovenia
- India
- USA
- Canada
- Argentina
A Quick Overview of DNSSEC
A Normal DNS Interaction

Web Server

Web Browser

https://example.com/

10.1.1.123

example.com?

1

DNS Resolver

DNS Svr root

.example.com

DNS Svr .com

DNS Svr example.com

10.1.1.123

1

2

3

4

5

6

web page

web page
Attacking DNS

1. DNS Resolver queries root DNS server for example.com.
2. Root DNS server returns com domain server IP address.
3. DNS Resolver queries com domain server for example.com.
4. Com domain server returns 192.168.2.2 as example.com IP address.

DNS Svr for example.com forwards query to another DNS Svr.

Attacking DNS Svr example.com responds with 192.168.2.2.
A Poisoned Cache

Web Server

https://example.com/

Web Browser

example.com?

192.168.2.2

DNS Resolver

Resolver cache now has wrong data:
example.com 192.168.2.2

This stays in the cache until the Time-To-Live (TTL) expires!
A DNSSEC Interaction

1. DNS Resolver queries .com NS DS
2. DNS Resolver queries example.com NS DS
3. DNS Resolver receives 10.1.1.123 DNSKEY RRSIGs
4. DNS Resolver queries 10.1.1.123
5. Web Browser receives https://example.com/
6. Web Browser receives web page
Attempting to Spoof DNS

Web Server
- to Web Browser
  - https://example.com/

Web Browser
- to DNS Resolver
  - example.com?

DNS Resolver
- to DNS Svr .com
  - .com NS
  - .com DS
- to DNS Svr root
  - .com NS
  - .com DS

DNS Svr .com
- to DNS Svr example.com
  - example.com NS
  - example.com DS

DNS Svr example.com
- to Attacking DNS Svr example.com
  - SERVFAIL

DNSKEY RRSIGs
- 192.168.2.2 DNSKEY RRSIGs
- 0.1.1.123 DNSKEY RRSIGs
The Two Parts of DNSSEC

Signing
- Registries
- Registrars
- DNS Hosting

Validating
- Applications
- Enterprises
- ISPs
DNSSEC Signing - The Individual Steps

- **Registry**
  - Signs TLD
  - Accepts DS records
  - Publishes/signs records

- **Registrar**
  - Accepts DS records
  - Sends DS to registry
  - Provides UI for mgmt

- **DNS Hosting Provider**
  - Signs zones
  - Publishes all records
  - Provides UI for mgmt

- **Domain Name Registrant**
  - Enables DNSSEC (unless automatic)
DNSSEC Signing - The Players

- Registries
- Registrars
- DNS Hosting Providers
- Domain Name Registrants

Registrar also provides DNS hosting services
DNSSEC Signing - The Players

- Registries
- Registrars
- DNS Hosting Providers
- Domain Name Registrants

Registrant hosts own DNS
A Quick Overview of DANE
The Typical TLS (SSL) Web Interaction

1. The Web Browser sends a request to a DNS Resolver for the domain example.com?
2. The DNS Resolver queries higher-level DNS servers (DNS Svr root) for the authoritative DNS Svr example.com.
3. The DNS Resolver receives the IP address 10.1.1.123 from the DNS Svr example.com.
4. The Web Browser connects to the IP address 10.1.1.123.
5. The DNS Resolver sends the request to the DNS Svr example.com?
6. The Web Server responds to the DNS Resolver with the IP address 10.1.1.123.

The Web Browser requests the HTTPS:// URL: https://example.com/

The Web Server responds with a TLS-encrypted web page.
The Typical TLS (SSL) Web Interaction

Web Server

Web Browser

https://example.com/

TLS-encrypted web page

DNS Resolver

example.com?

1

2

3

10.1.1.123

DNS Svr root

DNS Svr .com

DNS Svr example.com

10.1.1.123

Is this encrypted with the CORRECT certificate?
Problems?

- Web Server
- DNS Server
- Firewall
- Web Browser

SSL-encrypted web page with CORRECT certificate

SSL-encrypted web page with NEW certificate (re-signed by firewall)

www.example.com?

1 1.2.3.4

1

www.internetsociety.org/deploy360/
DANE

Web Server

TLS-encrypted web page with CORRECT certificate

Firewall (or attacker)

TLS-encrypted web page with NEW certificate (re-signed by firewall)

Log files or other servers

DNS Server

10.1.1.123 DNSKEY RRSIGs TLSA

delete

example.com?

Web Browser w/DANE

DANE-equipped browser compares TLS certificate with what DNS / DNSSEC says it should be.
DNS-Based Authentication of Named Entities (DANE)

• Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

• A: Store the certificate (or fingerprint) in DNS (new TLSA record) and sign them with DNSSEC.

A browser that understand DNSSEC and DANE will then know when the required certificate is NOT being used.

Certificate stored in DNS is controlled by the domain name holder. It could be a certificate signed by a CA – or a self-signed certificate.
DANE – Not Just For The Web

• DANE defines protocol for storing TLS certificates in DNS
• Securing Web transactions is the obvious use case
• Other uses also possible:
  • Email via S/MIME
  • VoIP
  • Jabber/XMPP
  • PGP
  • ?
DANE Resources

DANE and email:

DANE Operational Guidance:
• http://tools.ietf.org/id/draft-dukhovni-dane-ops-01.txt

DANE and SIP (VoIP):
• http://tools.ietf.org/id/draft-johansson-dane-sip-00.txt

Other uses:
• http://tools.ietf.org/id/draft-wouters-dane-openpgp-00.txt
• http://tools.ietf.org/id/draft-wouters-dane-otrfp-00.txt
DNSSEC Deployment Trends - Signing
DNSSEC Deployment – Top-Level Domains

Source: http://www.internetsociety.org/deploy360/dnssec/maps/
DNSSEC Deployment – Top-Level Domains

EUR ccTLD DNSSEC Status on 2013-09-09

Source: http://www.internetsociety.org/deploy360/dnssec/maps/
DNSSEC Deployment – Second-Level Domains

Source: https://xs.powerdns.com/dnssec-nl-graph/
DNSSEC Deployment – .COM

Source: http://scoreboard.verisignlabs.com/count-trace.png
DNSSEC Deployment – .GOV

USG DNSSEC Enabled Domains
- 1313 tested on 2013.09.30 -

- 86% Operational
- 12% In Progress
- 2% No Progress

Source: http://fedv6-deployment.antd.nist.gov/snap-all.html
DNSSEC Deployment – Fortune 1000 and U.S. Alexa Top 100 Sites

Industry DNSSEC Enabled Domains
- 1070 tested on 2013.09.23 -
  - Operational
  - In Progress
  - No Progress

Source: http://fedv6-deployment.antd.nist.gov/snap-all.html
DNSSEC Deployment – New Statistics Site

Source: http://www.statdns.com/
DNSSEC Deployment Trends - Validation
Availability of DNSSEC-Validating Resolvers

Consumers need easy availability of DNSSEC-validating DNS resolvers. Examples:

- Google's Public DNS now performing DNSSEC validation by default
- Comcast in North America rolled out DNSSEC-validating resolvers to 18+ million customers
- Almost all ISPs in Sweden provide DNSSEC-validating resolvers
Impact of Google Public DNS

Geoff Huston's measurements of DNSSEC validation:

- "Since March 2013 we've seen the proportion of end users who use DNSSEC resolvers that perform DNSSEC validation rise from 3.3% to 8.1%, or a rise of some 4.7%.


- July 2013
# Geoff Huston's Measurements – July 2013

## Where is DNSSEC? - The Top 20

<table>
<thead>
<tr>
<th>Rank</th>
<th>CC</th>
<th>Count</th>
<th>% D</th>
<th>% X</th>
<th>% A</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SE</td>
<td>5,349</td>
<td>77.92</td>
<td>3.38</td>
<td>18.70</td>
<td>Sweden</td>
</tr>
<tr>
<td>2</td>
<td>SI</td>
<td>4,758</td>
<td>58.85</td>
<td>4.90</td>
<td>36.25</td>
<td>Slovenia</td>
</tr>
<tr>
<td>3</td>
<td>LU</td>
<td>651</td>
<td>43.87</td>
<td>6.90</td>
<td>49.23</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>4</td>
<td>VN</td>
<td>26,665</td>
<td>38.28</td>
<td>4.04</td>
<td>57.69</td>
<td>Vietnam</td>
</tr>
<tr>
<td>5</td>
<td>FI</td>
<td>2,476</td>
<td>37.01</td>
<td>16.29</td>
<td>46.70</td>
<td>Finland</td>
</tr>
<tr>
<td>6</td>
<td>CZ</td>
<td>30,817</td>
<td>33.20</td>
<td>8.08</td>
<td>58.72</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>7</td>
<td>CL</td>
<td>46,181</td>
<td>30.26</td>
<td>8.34</td>
<td>61.41</td>
<td>Chile</td>
</tr>
<tr>
<td>8</td>
<td>JM</td>
<td>1,545</td>
<td>28.22</td>
<td>3.11</td>
<td>68.67</td>
<td>Jamaica</td>
</tr>
<tr>
<td>9</td>
<td>IE</td>
<td>8,079</td>
<td>27.94</td>
<td>3.11</td>
<td>68.96</td>
<td>Ireland</td>
</tr>
<tr>
<td>10</td>
<td>BB</td>
<td>1,312</td>
<td>24.24</td>
<td>1.52</td>
<td>74.24</td>
<td>Barbados</td>
</tr>
<tr>
<td>11</td>
<td>ID</td>
<td>54,816</td>
<td>23.87</td>
<td>8.58</td>
<td>67.55</td>
<td>Indonesia</td>
</tr>
<tr>
<td>12</td>
<td>UA</td>
<td>26,309</td>
<td>21.65</td>
<td>2.75</td>
<td>65.60</td>
<td>Ukraine</td>
</tr>
<tr>
<td>13</td>
<td>ZA</td>
<td>2,959</td>
<td>21.15</td>
<td>9.36</td>
<td>69.48</td>
<td>South Africa</td>
</tr>
<tr>
<td>14</td>
<td>TR</td>
<td>49,418</td>
<td>18.06</td>
<td>2.10</td>
<td>79.84</td>
<td>Turkey</td>
</tr>
<tr>
<td>15</td>
<td>US</td>
<td>140,214</td>
<td>17.32</td>
<td>3.57</td>
<td>79.11</td>
<td>United States of America</td>
</tr>
<tr>
<td>16</td>
<td>EG</td>
<td>36,061</td>
<td>14.68</td>
<td>10.32</td>
<td>75.01</td>
<td>Egypt</td>
</tr>
<tr>
<td>17</td>
<td>GH</td>
<td>97</td>
<td>14.59</td>
<td>8.12</td>
<td>77.29</td>
<td>Ghana</td>
</tr>
<tr>
<td>18</td>
<td>AZ</td>
<td>7,409</td>
<td>14.55</td>
<td>30.34</td>
<td>55.11</td>
<td>Azerbaijan</td>
</tr>
<tr>
<td>19</td>
<td>BR</td>
<td>179,424</td>
<td>14.43</td>
<td>6.13</td>
<td>79.44</td>
<td>Brazil</td>
</tr>
<tr>
<td>20</td>
<td>PS</td>
<td>2,893</td>
<td>14.00</td>
<td>36.85</td>
<td>49.15</td>
<td>Occupied Palestinian Territory</td>
</tr>
</tbody>
</table>

SURFnet Validating Server Whitepaper

- Steps through cost/benefit, requirements, planning
- Provides instructions for:
  - BIND 9.x
  - Unbound
  - Windows Server 2012
DNSSEC Deployment Challenges
Key Questions

• What needs to be done to get more domains signed with DNSSEC?

• How can DNSSEC validation be more widely deployed?

• Are there technical issues or are the issues more of communication and awareness?

• How can we as a community address these challenges to increase the usage and availability of DNSSEC?
Opportunities to Accelerate Deployment

1. Registrar / DNS hosting provider engagement
   - Encouraging more registrars to provide DNSSEC and making it easier for domain name holders.

2. Validating name servers
   - Expanding the deployment of DNSSEC-validating name servers at multiple levels, including ISPs, operating systems and applications.

3. Enterprise signing of domains
   - Helping enterprises and other large organizations understand the added security value they can achieve with DNSSEC, particularly with the new capabilities of DANE.

4. Government activity with DNSSEC
   - Encouraging governments to expand their promotion and usage of DNSSEC
Registrars and DNSSEC - RAA

• New ICANN Registrar Accreditation Agreement (RAA) will have section on DNSSEC
  • Specifically the "Additional Registrar Operations Specification"
  • Impact will be that any registrars wishing to continue their ICANN accreditation will need to learn about DNSSEC and accept records
  • Must be implemented by January 1, 2014
Registrars and DNSSEC - RAA

New specification states:

1. DNSSEC

Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices. Registrars shall accept any public key algorithm and digest type that is supported by the TLD of interest and appears in the registries posted at: <http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml> and <http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml>. All such requests shall be transmitted to registries using the EPP extensions specified in RFC 5910 or its successors.

Specification also covers IPv6 and IDNs.
Helping Accelerate DNSSEC Deployment

Public mailing list, “dnssec-coord”, available and open to all:

https://elists.isoc.org/mailman/listinfo/dnssec-coord

Focus is on better coordinating promotion / advocacy / marketing activities related to DNSSEC deployment.

Monthly conference calls and informal meetings at ICANN and IETF events.
DNSSEC Resources
DNSSEC Workshop at ICANN 48

- November 20, 2013
  Buenos Aires, Argentina

- Topics to be discussed include:
  - Automation of DNSSEC
  - Root key rollover
  - Guidance for registrars in supporting DNSSEC
  - Interfaces between registrars and registries
  - Regional activities

- Will be streamed live over the Internet
Resources

To learn more about DNSSEC and how to get started:
http://www.internetsociety.org/deploy360/dnssec/basics/
http://www.internetsociety.org/deploy360/resources/dane/

Specific resources that may be of interest:
• SURFnet whitepaper about deploying validating servers
• DNSSEC HOWTO
• NIST "Secure DNS Deployment Guide"
Comcast Case Study

• Presentation at October 2012 DNSSEC Deployment Workshop at ICANN 45

• Slides and audio for workshop:
  • [toronto45.icann.org/node/34375](http://toronto45.icann.org/node/34375)

• Comcast presentation:
  • Customer interaction
  • Lessons learned
  • Next steps
Increased Number Of DNSSEC Tools

Lists of tools:

http://www.internetsociety.org/deploy360/dnssec/tools/

http://www.internetsociety.org/deploy360/blog/tag/tools/

DNSSEC Tools Project

http://www.dnssec-tools.org/
DANE Resources

DANE Overview and Resources:

• http://www.internetsociety.org/deploy360/resources/dane/

IETF Journal article explaining DANE:


RFC 6394 - DANE Use Cases:

• http://tools.ietf.org/html/rfc6394

RFC 6698 – DANE Protocol:

• http://tools.ietf.org/html/rfc6698
Three Requests For Network Operators

1. Deploy DNSSEC-validating DNS resolvers

2. Sign your own domains where possible

3. Help promote support of DANE protocol
   • Allow usage of TLSA record. Let browser vendors and others know you want to use DANE. Help raise awareness of how DANE and DNSSEC can make the Internet more secure.
Can You Help Us With:

- Case Studies?
- Tutorials?
- Videos?

How Can We Help You?

www.internetsociety.org/deploy360/
Thank You!