DNSSEC 101

Ulrich Wisser
ulrich@wisser.se
Agenda

- DNSSEC Overview
- Public Key Cryptography
- Signing
- Validation
- Non-existence
- Key management
- Policy Considerations
• Ulrich Wisser
• Formerly Senior DNS Expert at .SE
• Developer, father of four, judo black belt
DNSSEC History

- 1993: Discussion of secure DNS begins
- 1994: First draft of possible standard published
- 1997: RFC 2065 published DNSSEC is an IETF standard
- 1999: RFC 2535 published DNSSEC standard is revised
- 2005: Total rewrite of standards published RFCs 4033, 4034 and 4035
- 2005: First TLD signed (.SE)
- 2010: Root zone signed
- 2011: .com zone signed
- current: 1363 TLDs signed, 113 TLDs unsigned (9 IDN, 104 ccTLDs)
Problem Description

- DNS uses UDP (one packet request, one packet answer)
- No assurance that the source address in the packet is the real source
DNSSEC

DNSSEC does not

- protect against DDoS attacks
- Encrypt DNS data (no privacy)

DNSSEC does

- Protect against spoofed answers
- Proofs data origin
Public Key Cryptography

Private Key
Used for signing

Public Key
Used for Validation
Signing

text extracted from image
Cryptographic Algorithms

RSA – Rivest–Shamir–Adleman

ECDSA

EdDSA

https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

example.com. 3600 IN  DNSKEY  256   3   13
QWNloZpo3yvMOM50yUnWlypnRVd6YRHM0nFXCkOeGwdDI7DL
LMx1MOMRggFBO351vhsOXT2HEqL4tDjmFGMucTA==

example.com. 3600 IN  RRSIG  DNSKEY  13 2 3600
20221111101743 20221021012705 45620 example.com.
55MrjDXJfsJ3nDxsYi8apWj0wdiyl1mYZdVyRvfHB85mAbP59sVo
Uo2qVn03kupugNjSYXpGUvD43JwTYkACw==
Chain of Trust

.COM

AUTHENTICATES

EXAMPLE.COM
Chain of Trust

- Cryptographic Hash function

https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml
DS Records

example.com. 300 IN DS 31406 13 2
F78CF3344F72137235098ECBBD08947C2C9001C7F6A085A17F518B5D8F6B916D
Key Types

- **KSK - Key Signing Key**
  - Signes the DNSKEY set
- **ZSK – Zone Signing Key**
  - Signes zone data
- **CSK – Combined Signing Key**
  - Signed both, the DNSKEY set and zone data
Chain of Trust

Root

KSK  Signs  ZSK  Signs  .com DS

.com

KSK  Signs  ZSK  Signs  example.com DS

Example.com

KSK  Signs  ZSK

www.example.com  A
Validation

root hints

trust anchor

root

.com

example.com
Short Summary

- Public Key Cryptography
- Cryptographic Hash Functions
- KSK, ZSK
- DNSKEY, DS, RRSIG resource records
- Validation
Non-Existence
NSEC
NSEC

    2018041700 3600 600 86400 600
example.com. NS ns.example.com.
example.com. A 10.0.0.1
example.com. MX 0 mail.example.com.

east.example.com. NS ns.east.example.com.
ns.east.example.com. A 10.0.0.5
ns.example.com. A 10.0.0.1
www.example.com. A 10.0.0.3
www.example.com. AAAA 2001:DB80::CAFE
<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>SOA</td>
<td>ns.example.com. hostmaster.example.com.</td>
</tr>
<tr>
<td>example.com</td>
<td>NS</td>
<td>ns.example.com.</td>
</tr>
<tr>
<td>example.com</td>
<td>A</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>example.com</td>
<td>MX</td>
<td>0 mail.example.com.</td>
</tr>
<tr>
<td>example.com</td>
<td>NSEC</td>
<td>east.example.com. A NS SOA MX NSEC</td>
</tr>
<tr>
<td>east.example.com</td>
<td>NS</td>
<td>ns.east.example.com.</td>
</tr>
<tr>
<td>east.example.com</td>
<td>NSEC</td>
<td>ns.east.example.com. NS NSEC</td>
</tr>
<tr>
<td>ns.east.example.com</td>
<td>A</td>
<td>10.0.0.5</td>
</tr>
<tr>
<td>ns.example.com</td>
<td>NSEC</td>
<td>ns.example.com. A NSEC</td>
</tr>
<tr>
<td>ns.example.com</td>
<td>A</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>ns.example.com</td>
<td>NSEC</td>
<td><a href="http://www.example.com">www.example.com</a>. A NSEC</td>
</tr>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>A</td>
<td>10.0.0.3</td>
</tr>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>AAAA</td>
<td>2001:DB80::CAFE</td>
</tr>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>NSEC</td>
<td>example.com. A AAAA NSEC</td>
</tr>
</tbody>
</table>
Zone Walking

domain.example.com.

SOA ns.example.com. hostmaster.example.com.
2018041700 3600 600 86400 600

domain.example.com.

NS ns.example.com.
domain.example.com.

A 10.0.0.1
domain.example.com.

MX 0 mail.example.com.
domain.example.com.

NSEC east.example.com. A NS SOA MX NSEC
east.example.com.

NS ns.east.example.com.
east.example.com.

NSEC ns.east.example.com. NS NSEC
east.example.com.

A 10.0.0.5
east.example.com.

NSEC ns.example.com. A NSEC

ns.east.example.com.

A 10.0.0.1
nen.example.com.

NSEC www.example.com. A NSEC

www.example.com.

A 10.0.0.3

www.example.com.

AAAA 2001:DB80::CAFE

www.example.com.

NSEC example.com. A AAAA NSEC
NSEC3

tjlb7qbojvmlf1s6gdriru7vsms1lg16.example.com 300 IN NSEC3
1 1 15 CA12B74ADB90591A tjlfs98uj0vbvg6md2klgv0gi2gu6kj5
NS SOA RRSIG DNSKEY NSEC3PARAM
Key management

- Offline KSK
- HSM – Hardware Security Module
Policy Considerations
Timing Considerations

RRSIG Lifetime  12 days
RRSIG Refresh   4 days

Days

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
</table>

refresh

Lifetime
Timing Considerations

RRSIG Lifetime: 12 days
RRSIG Refresh: 4 days
Timing Considerations

- RRSIG Lifetime: 12 days
- RRSIG Refresh: 4 days
- SOA Expire: 10 days

Days: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Lifetime, Refresh, and Days are depicted in the diagram.
Policy Considerations

- RFC 6841 - A Framework for DNSSEC Policies and DNSSEC Practice Statements
  https://www.rfc-editor.org/rfc/rfc6841.html
- RFC 9276 - Guidance for NSEC3 Parameter Settings
Summary

- Public Key Cryptography
- Cryptographic Hash Functions
- KSK, ZSK
- DNSKEY, DS resource records
- Validation
- NSEC / NSEC3
- Policy and Timing Considerations
Advanced DNSSEC

- ZSK Rollover
- KSK Rollover
- CDS/CDNSKEY support
- Multi-signer DNSSEC
- Trust Anchors for non-root zones
Thank You!