DNSSEC

CDBGUG
Sept 8th 2015
Patrick Muldoon
Overview

- Review of DNS
- What is DNSSEC
- Concepts
- Implementation
DNS Review

- Maps Hostname to IP (and IP to hostname)
- Two Types of Servers
  - Authoritative
  - Recursive

Authoritative Are where we create records, and provide the Answers
Recursive / Caching are used to lookup and store the answers from the Authoritative so that the system can scale. (figures out who to ask and what to ask)
Authority

• DNS is Tree Based
• Start with (.) Root Zone and work left
• . goes to the root Servers
• net. goes to the GTLD Server
• inoc.net goes to the Auth Servers that are listed
Glue Records
Let's Walk Through
| net.  | 172800 | IN    | NS    | d.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | k.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | e.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | f.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | j.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | h.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | b.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | a.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | c.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | l.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | g.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | m.gtld-servers.net. |
| net.  | 172800 | IN    | NS    | i.gtld-servers.net. |
| net.  | 86400  | IN    | DS    | 36876827F5F516EBF9668444 |
| net.  | 86400  | IN    | RRSIG | DS 8 1 86400 201509182850000 201509wBNvsQMDyMao6qYeFtXck7 CnkbAg0NgxvAb8B0rjLx7Yc70R4mmn66Ct9R93N4RBNJg0k/1m3oRlWMA |

; Received 729 bytes from 202.12.27.35#53(m.root-servers.net) in 90 ms
inoc.net. 172800 IN NS ns0.inoc.net.
inoc.net. 172800 IN NS ns1.inoc.net.
inoc.net. 172800 IN NS ns2.inoc.net.
A1RT98B55Q6C9NFI51S9HCI47ULJG66JH.net. 86400 IN NSEC3 1 1 0 - A1RUUFFJKCT2Q54F
A1RT98B55Q6C9NFI51S9HCI47ULJG66JH.net. 86400 IN RRSIG NSEC3 8 2 86400 20150913
RB248dFu4jBUEx7fQHttgQaa8uWHzqjzuBtE/ fUQBlVGrXsXxBFfZXL8v+hlpXc9RKnGgJi8dnu1HuL
LVCJ63JQ0HTSSRR1J65KFKK1FEGRRK1.net. 86400 IN NSEC3 1 1 0 - LYDQJ36ULR491FK
LVCJ63JQ0HTSSRR1J65KFKK1FEGRRK1.net. 86400 IN RRSIG NSEC3 8 2 86400 20150913
U/UpOqQ-EFikF4pId05Y2MD9HzNF61/0pM c7NPLRNS5PChgbAbdwxX+f6fzNgRCFk7056DFML;
; Received 708 bytes from 192.43.172.30#53(i.gtld-servers.net) in 83 ms
<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Class</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ioc.net.</td>
<td>A</td>
<td>IN</td>
<td>64.22.32.144</td>
</tr>
<tr>
<td>ioc.net.</td>
<td>NS</td>
<td>IN</td>
<td>ns0.ioc.net</td>
</tr>
<tr>
<td>ioc.net.</td>
<td>NS</td>
<td>IN</td>
<td>ns1.ioc.net</td>
</tr>
<tr>
<td>ioc.net.</td>
<td>NS</td>
<td>IN</td>
<td>ns2.ioc.net</td>
</tr>
</tbody>
</table>

;; Received 239 bytes from 2607:fcc50:1:500:a#53(ns1.ioc.net) in 22 ms
What is DNSSEC

- Standard Public/Private Key Crypto
- Adds Cryptographic Extensions / Signatures
- Defined in RFC 4033, 4034, 4035
Why is it “important”

- DNS primarily uses UDP, so any packet that comes back could be the answer
- Just needs right source and destination IPs, destination port, Query ID, and Bailiwick Check
- TL;DR — Easy to spoof

Bailiwick check is when resolvers determine which extra information in the response to ignore, Normally this is things that our out of zone of the responding server.

Commonly called cache Poisoning.
DNSSEC Fixes This

- Applies Cryptographic Check to each answer in resolution
- Can still Try to cache poison, but since they don’t have the correct keys the resolver will reject them
- Doesn’t Fix (D)DOS against DNS
Concepts
Authoritative

- Zone Signing
- Rollover
Authoritative

• Sign Zone with DNSSEC Records

• RRSIG - Signatures for A, AAAA, MX, NS, … (Tracks type/number)

• NSEC/NSEC3 — Used for Confirming NXDomain

• DNSKEY — Public Keys for Entire Zone

• DS Record — Given to Parent Zone to authenticate NS records
Zone Signing

- 2 Key Pairs Used
  - ZSK (Zone Signing Key)
  - KSK (Key Signing Key)
ZSK

- Signs the Zone Records, and Itself
- Public Part Becomes the DNSKEY
KSK

- Signs the Keys at the Zone
- Public Part also becomes a DNSKEY
Zone Signing Record Relationships

- DNS KEY KSK
- DNS KEY ZSK
- SOA
- NS
- A
- RRSIG by KSK
- RRSIG by ZSK

KSK Private Key Used for Signing
ZSK Private Key Used for Signing

Stolen From Online...
Rollover

- RRSIGS Have lifetime they are valid for encoded in them
- DNSKEYs also have lifetime encoded in
  - Per NIST SP800-01
    - KSK — 12 Months (1 year)
    - ZSK — 30 Days (1 Month)
  - Both Current and future keys can put published at same time to support this

NIST SP800-01: National Institute of Standards and Technology (part of Dept of Commerce) Security and Privacy Controls for Federal Information Systems and Organizations
Resolvers

• Trust Anchors
• Validation
Trust Anchors

- Records used to validate RRSIGS for DNSKEY

- Many Forms:
  - Manually Obtained
  - DS Records at parent
  - DNS Lookaside
  - Root Signed SEP

secure entry point (Now that root is signed, these are less of issue)
Validation

• DNS Query with DNSSEC enabled
• Along with Response, RRSIG is returned
• Use DNSKEY from Zone (public part of ZSK) to validate the RRSIG
• Validate that DNSKEY with RRSIG
• Validate RRSIG with Public Key from KSK (trust anchor)
• If No Trust Anchor, go upwards for DS, validate. Lather, Rinse, Repeat
Implementation

- Authoritative (NSD)
- Recursive / Caching (unbound)
Authoritative

• Assume that NSD is already installed / configured to serve Authoritative Answers

• We will be signing example.com
Generate Keys

- cd /usr/local/etc/named/zones
- export ZSK=`ldns-keygen -a RSASHA1-NSEC3-SHA1 -b 1024 example.com`
- export KSK=`ldns-keygen -k -a RSASHA1-NSEC3-SHA1 -b 2048 example.com`
• 2 private keys with .private extension
• 2 public keys with .key extension
• 2 DS records with .ds extension
Sign The Zone

- `ldns-signzone -n -s $(head -n100 /dev/random | sha1 | cut -b 1-16) example.com $ZSK $KSK`

- tell NSD to use the signed zone (edit config file and point zonefile to example.com.zone.signed)
Generate DS Keys

- rm $ZSK.ds $KSK.ds
- ldns-key2ds -n -1 example.com.zone.signed
- ldns-key2dn -n -2 example.com.zone.signed

We need these in a different format so remove them.

-n writes to standard out as opposed to file.
-1 will generate SHA1, -2 generates SHA256
Domain, TTL, IN, TYPE (DS), Keytag, Algorithm, Digest Type, Digest
Configure Registrar

Set custom name servers on your domain
Configure DNSSEC
Set up DNSSEC

Before you try to do this make sure your registrar supports this, if not find a new one :)

![Configure Registrar Screenshot](image-url)
Verify Operation

- [http://dnsviz.net/](http://dnsviz.net/)
Analyzing DNSSEC problems for `labratsoftware.com`

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Request</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>labratsoftware.com</code></td>
<td></td>
<td>Found 2 DNSKEY records for <code>labratsoftware.com</code></td>
</tr>
<tr>
<td><code>com</code></td>
<td></td>
<td>Found 1 DS record for <code>com</code> in the zone</td>
</tr>
<tr>
<td><code>labratsoftware.com</code></td>
<td></td>
<td>Found 2 DNSKEY records for <code>labratsoftware.com</code></td>
</tr>
<tr>
<td><code>com</code></td>
<td></td>
<td>Found 1 DS record for <code>com</code> in the zone</td>
</tr>
</tbody>
</table>

Move your mouse over any 🐟 or ⚡️ symbols for remediation hints.

Want a second opinion? Test `labratsoftware.com` at `digtest.net`. 
Making Changes

- editing .signed file directly will invalidate zone
- Edit unsigned Zone (making sure to increment SOA Serial) and then resign the zone file
Rollover

- Need to resign the zones every 30 days

- If you are making changes all the time, this isn’t a problem, but if your zones are static, you need to make sure to do it every 20 or so days (to account for propagation / caching). Update the SOA and resign
Recursive/Caching

- Unbound has built in support
- auto-trust-anchor-file / unbound-anchor tool
- https://data.iana.org/root-anchors/root-anchors.xml

base Install supports it, as does ports on freebsd
unbound-anchor uses the IANA cert to verify the root anchor if it changed while system was off, else it will use RFC5011 probes to keep it updated during operation