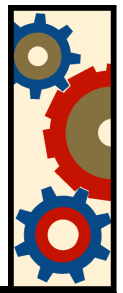
Deploying DNSSEC. Pulling yourself up by your bootstraps

João Damas

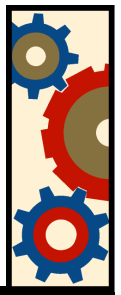
ISC

DNSSEC status



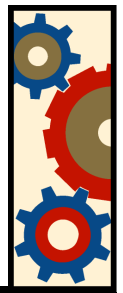
- Standard is complete and usable
  - Minor nits with regards to some privacy issues in some contexts (nsec3, online signing)
- There are at least 2 implementations of servers (BIND and NSD)
- There is at least 1 implementation of a DNSSEC aware resolver (BIND 9.3.2 and later)

Bootstrapping



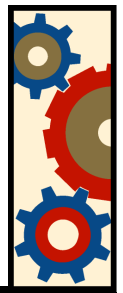
- DNSSEC follows a hierarchical model for signatures
  - Sign the root zone
  - Get the root zone to delegation-sign TLDs
  - Get TLDs to delegation-sign SLDs
  - …..

Unsigned root and TLDs



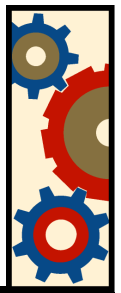
- Today the root zone remains unsigned
  - Likely this way for some time
- Very few TLDs have signed their zones and offer delegation signatures
  - .se, .pr, .bg, .br

But I want my zone signed



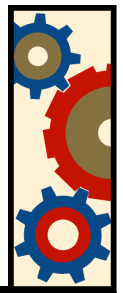
- DNSSEC provides for local implementations to be able to insert local trust anchors, entry points into the secure system
  - E.g. Trust-anchors clause in BIND
- Problem: If you have too many it becomes a nightmare to maintain, so it doesn't get used

DLV



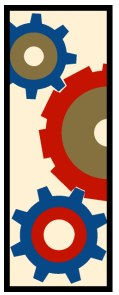
- Enter DLV, Domain Lookaside Validation
  - Is an implementation feature, not a change to the protocol. A matter of local policy.
  - It enables access to a remote, signed, repository of trust anchors, via the DNS
- Implemented in BIND's resolver so far. More to follow?

DLV lookup



- A DLV enabled resolver will try to find a secure entry point using regular DNSSEC processes and **IF IT FAILS**, and has DLV configured, will issue a search on the specified DLV tree

Enabling DLV



- On the resolver (so far only BIND)
  - Add to named.conf
    - In the options section:

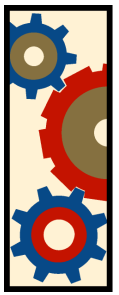
```
// DNSSEC configuration
 dnssec-enable yes;
 dnssec-lookaside . trust-anchor dlv.isc.org.;
```

      In BIND 9.4 add dnssec-validation yes;
    - By itself

```
trusted-keys {
   dlv.isc.org. 257 3 5 "BEAAAAPp1USu3BecNerrrd78zxJIslqFaJ9csRkxd9LCMzvk9Z0wFzoF
    kWAHMmMhWFpSLjPLX8UL6zDg85XE55hzqJKoKJndRqtncUwHkjh6zERN
    uymtKZSCZvkg5mG6Q9YORkcfkQD2GIRxGwx9BW7y3ZhyEf7ht/jEh01N
    ibG/uAhj4qkzBM6mgAhSGuaKdDdo40vMrwdv0CHJ74JYnYqU+vsTxEIw
    c/u+5VdA0+ZOA1+X3yk1qscxHC24ewPoiASE7XlzFqIyuKDlOcFySchT
    Ho/UhNyDra2uAYUH1onUa7ybtdtQclmYVavMplcay4aofVtjU9NqhCtv f/dbAtaWguDB";
};
```

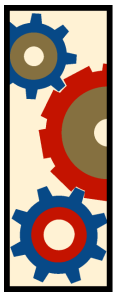
- Get the Key from ISC's web (http://www.isc.org/ops/dlv)

Using DLV



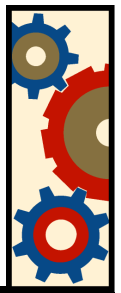
- BIND debugging is a bit hellish and user unfriendly.
- Working on tools to automate checks and make life easier
- BEWARE: If you want your zone to be signed and available **ALL** of your zone's nameservers must be DNSSEC enabled

Registering



- To make your DNSSEC information available you must register with the DLV registry.
  - In ISC's case, go to http://www.isc.org/ops/dlv and follow the instructions
  - Two authentication methods:
    - Cookie exchange
    - In person authentication

DLV registries



- ISC is operating a DLV registry free of charge for anyone who wants to secure their DNS.
  - See https://secure.isc.org/ops/dlv/
- Have a look and use it!

Questions?