Faking EDNS Key Tag

Shane Kerr

DNS-OARC Workshop / Madrid / 2017-05

EDNS Key Tag

- RFC 8145
- Sends information about trust anchors configured by resolvers to authority servers
- Two modes:
  1. EDNS option
  2. Well-known query (not actually EDNS)

EDNS Key Tag: Coming Soon?

- Some support in BIND 9.11
  - trust-anchor-telemetry
- Scheduled for Unbound
- On the TODO list for Knot Resolver
- PowerDNS Recursor?

Even after implemented, old resolvers will not have this functionality.

EDNS Key Tag: Faking It

- The well-known query option is easy

```
dig -t null -c in _ta-4a5c.
```

- Not 100% correct
  - Supposed to be sent with DNSKEY query
  - Supposed to be cached
- Something is better than nothing

awk. Really.

- Portability a major concern
  - Any language is a potential burden
- Bourne shell is not quite enough
- awk is a real programming language
- awk is on every POSIX system
  - Even built in to busybox!
- Apologies to Joe Abley
  - I spent many years mocking his awk usage
  - But awk is actually pretty cool!

Building a Key Tag Query: Unbound

- Find the trust anchor configuration
  - Parse unbound.conf
  - Manage include files, syntax, etc.
- Extract out the key tags
  - Easy for DS records
  - Tricky for DNSKEY or BIND 9 config
- Convert tags into query string
- Note to self:
  - use **`unbound-checkconf -o`** in the future

Building a Key Tag Query: BIND 9

- Find the trust anchor configuration
  - Parse named.conf
  - Use **named-checkconf -p**
    - No need for comments, includes, and so on
  - trusted-keys, managed-keys, managed-keys-directory, dnssec-validation auto, ...
  - And of course, handle views...
  - Plus BIND 9 ships with a compiled-in key
- Left as excersise to student 😉
- Or just use BIND 9.11

Fun Bits

- 4 major modern awk implementations
  - awk, gawk, mawk, busybox awk
  - All slightly different!
- Zone file parsing
  - About 500 lines of awk
  - More-or-less correct (but not tested)
- No bit shifts in awk
  - Have to use multiple/divide/modulo for key tag generation and Base 64

Using Fake EDNS Key Tag

- Single script to add to cron

```
$ git clone ...
$ awk -f mkdtemp.awk -f unboundtag.awk
dig -t null -c in _ta-4a5c.
$ sh crontag.sh --unbound
Key tag query added to crontab
```

- Also works for Yeti roots 😉

Code

https://github.com/shane-kerr/fake-edns-keytag