On-the-Fly Signing of Wildcard Zones

Ray Bellis, Nominet R&D

Nov 9th 2014, IEPG

APNIC has a problem

- Their DNSSEC experiments require a separate zone for each Google Ad served:
  - Currently memory limited to 750k signed zones
  - And a signed parent zone with DS records
  - Creating these is slow
  - Re-loading BIND is slow (3 – 4 hours)

Proposed Solution

- Use evldns to build a bespoke authoritative server
  - Dynamically synthesize and sign the child zones on a per-request basis (pseudo-wildcard)
  - Dynamically synthesize and sign DS records for the parent zone too
  - Cache the above for 60 seconds

"Oh, BTW, did we mention that we want some of these zones to have deliberately broken DS records?"

Unsigned Zone Contents

- Parent zone
  - Delegation only, NS and SOA records at the APEX
  - No other RRs – so the NS records must point out-of-zone
  - All child-related records (NS records, DS records) synthesized
- Child zone
  - Same records in every child zone
  - Any records you like except wildcards and CNAMEs
  - Has to contain the same NS records as the parent

Effective Parent Zone Contents

```
@ IN  SOA …
  IN  NS  <out-of-zone NS>
* IN  NS  <as above>
  IN  DS  <synthesized,variable!>
```

Some shortcuts

These only work because parent and children are on the same NS:

- No NSEC records needed for the wildcard delegations, because queries for `<foo.example.com>` end up in the child zone handler and the child has its own NSECs

- As above, queries for `<foo.example.com> DS?` are passed to the child handler, where they're correctly calculated as if they had been served by the parent (i.e. with the parent's DNSKEY)

- Possible buglet on query for non-existing QTYPEs at the parent apex:
  - the generated NSEC denies existence of any other names
  - but it passes every DNSSEC checker, anyway ☺

Future Work

- Support truncation
- Allow wildcards and CNAMEs in the child zone
  - ldns doesn't support wildcard lookups
  - CNAMEs need Additional Section processing
- Fixup the parent apex NSEC record
  - does it matter?
  - should it point at `<*.example.com>`?
- Improve performance (currently ~200 qps)
- Applicability for ip6.arpa ?

The Code!

https://github.com/raybellis/apnic

nominet®

innovation

Any Questions?