Measuring DNSSEC validation
i.e. how to do it

Ólafur Guðmundsson
Steve Crocker
ogud, steve at shinkuro.com
Outline

- Theory of measurement
- Reality of measurements
- Results and questions
Do DNSSEC validators behave differently from regular DNS resolvers?

- Ask for DNSSEC records
  - DNSKEY
  - DS
- Needs to refresh these records once in a while
  - DNSKEY about once every TTL
  - DS
    - Resolver needs to resolve RRset that is not in cache AND
    - If TTL’s on DNSKEY and DS have expired BUT
    - Not on NS
Theory 201: Complications

- Validators not only ones:
  - DNSSEC measurement tools
  - DNSSEC key mangers for trust anchors
  - “Rollover and Die” validators
  - DDoS tools
    - Need to exclude most of above.

- Validator will ask for DNSKEY
  - Separated by at least DNSKEY TTL
  - Asked for non-DNSSEC record just before
  - Cue on RRtype or name?
Theory 202: Validator Draft rules

1. Asks for DNSKEY multiple times in a sample at least DNSKEY TTL apart
2. Asks for info, followed by DNSKEY query
3. Asks for multiple DS records
4. Rule 1 and 3 combined
Measurements: ORG traffic

- TTL’s:
  - 900 for SOA, NSEC3, DNSKEY
  - 84600 for NS and DS

- By simple measure:
  - 10% of queries originate from suspected DNSSEC validators
    - BUT:
      - includes DNSKEY + DS traffic
      - Excludes: some only using dlv.isc.org
Measurement Reality:

- Saw traffic for some of DNS servers for ORG
  - 2/3 NS records, ~ 50% of traffic
- Queries are scattered
  - Some resolvers ask a narrow band of servers
    - Busy ones
  - Some ask random ones and no subsequent questions to the same one.
    - Sporadic ones
- Multiple validators/resolvers behind an address
  - All classified as one,
- Traces
  - short < 1 hour
  - Time 2000-2050 UTZ
How good are the samples

- Are validators over/under represented?
  - Do the validators we see do more/less DNSSEC than others?
  - Do DNSSEC validators scatter queries different?
    - DNSKEY set size > 1500 effects:
      - Validator tries multiple UDP servers before falling back on TCP → Overrepresented
  - Do measurement tools trick us?

- What to exclude in calculations?
  - DNSKEY?
  - DS?
  - DLV?
  - SOA?
Discussion

- How to measure
- What to measure
- Where to measure
- How to tune TTL’s