DNSSEC Roadblock avoidance

Wes Hardaker
Olafur Gudmundsson
Suresh Krishnaswamy

Motivation

- DNSSEC validation is not always possible
  - Network links cause problems
    - (size, filtering, etc)
  - Middle box nightmares
  - Upstream resolvers not DNSSEC aware or worse
  - Time synchronization issues
  - Configured trust anchors have changed
- How does a DNSSEC Host Validator:
  - Check if it can validate?
  - Work around problems it may find

Purpose Of The Draft

- Define a set of tests that can:
  - Test neighboring resolvers for DNSSEC awareness
  - Test network infrastructure for DNSSEC usability
- Aggregating test results into “support levels”
  - Not DNSSEC capable
  - DNSSEC Aware
  - Validator
- Define “work around options”
  - What to do with a resolver that isn’t DNSSEC-aware
  - What to do when middle boxes are in the way
  - etc

Roadblock Next Steps

- Continue with lessons learned
  - From libraries
  - From network managers
  - From applications
  - etc
- Publish within DNSOP?
  - Useful?
  - Publish as BCP/Informational ?
- Extra slides in the slide deck!

Extra Slides

- (if time permits or for downloaders)

Experience: In-library Intelligence

- Libval and libunbound:
  - Try to do intelligent fallbacks
  - Have policies to help distinguish minimum requirements

Experience: Network Managers DNSSEC Trigger

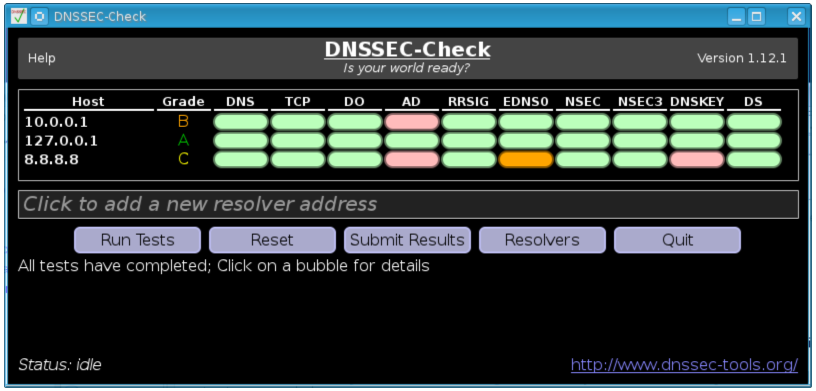
- This is a host validator that attempts to use network configured resolvers for resolution
  - Performs number of checks and falls back on
    - Full recursion if possible
    - DNS over HTTP or
    - DNS over HTTPS
- DNSSEC validation does not work all the time, what should it do?
  - FAIL all queries, Silently disable DNSSEC, ask User?

Experience: Unbound on home router

- If resolver is configured to start in validator mode, box will not work
  - Router has no battery backup for clock, time at boot is 1970/jan/1
  - NTP needs DNS to work
  - Signatures are wrong until NTP succeeds
- Resolvers SHOULD check before enabling DNSSEC validation

Experience: Testers
Testers that assess upstream resolvers

- **DNSSEC-check:** http://www.dnssec-tools.org/download/



DNSSEC-Check
Is your world ready?
Version 1.12.1

Host	Grade	DNS	TCP	DO	AD	RRSIG	EDNS0	NSEC	NSEC3	DNSKEY	DS
10.0.0.1	B	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩
127.0.0.1	A	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
8.8.8.8	C	🟩	🟩	🟩	🟥	🟩	🟧	🟩	🟩	🟥	🟩

Click to add a new resolver address

All tests have completed; Click on a bubble for details

Status: idle
http://www.dnssec-tools.org/

- **DNSSEC_Resolver_Check:**

  https://github.com/ogud/DNSSEC-resolver-check

  <pic>

Contents:

- Aggregations can be augmented by a extra information:
  - Partial and add one or more failures to it
  - NSEC3, NoBig, SlowBig, TCP, DNAME, Unknown, Permissive
    - Example: Partial Validator[DNAME]