

DANE Roadblock Avoidance

Wes Hardaker
Ólafur Guðmundsson
Suresh Krishnaswamy

Motivation

- DNSSEC Validation is not always possible
 - Network links cause problems
 - (size constraints, filtering, etc)
 - Middle boxes
 - Upstream resolvers that aren't DNSSEC aware
 - Time synchronization issues
 - Changes to Trust Anchors
- How does a DNSSEC Validator:
 - Check if it can validate?
 - Work around problems it finds

Purpose of this draft: Testing

- Define a set of tests
 - Test neighboring resolvers for DNSSEC awareness
 - Test network infrastructure for DNSSEC usability
- Aggregate these results into “support levels”
 - Not DNSSEC capable
 - DNSSEC Aware
 - Validator

The screenshot shows the DNSSEC-Check application window. The title bar reads 'DNSSEC-Check'. The main window has a header with 'Help', 'DNSSEC-Check', 'Is your world ready?', and 'Version 1.12.1'. Below the header is a table with columns: Host, Grade, DNS, TCP, DO, AD, RRSIG, EDNS0, NSEC, NSEC3, DNSKEY, and DS. The table contains three rows of data. Below the table is a button labeled 'Click to add a new resolver address'. At the bottom, there are five buttons: 'Run Tests', 'Reset', 'Submit Results', 'Resolvers', and 'Quit'. A status bar at the bottom left says 'Status: idle' and the bottom right has the URL 'http://www.dnssec-tools.org/'.

Host	Grade	DNS	TCP	DO	AD	RRSIG	EDNS0	NSEC	NSEC3	DNSKEY	DS
10.0.0.1	B	Green	Green	Green	Red	Green	Green	Green	Green	Green	Green
127.0.0.1	A	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
8.8.8.8	C	Green	Green	Green	Red	Green	Orange	Green	Green	Red	Green

Purpose of this draft: Options

- Define “work around options”
 - What to do when a resolver isn't DNSSEC-aware
 - What to do when middle boxes are in the way
 - etc

Next Steps

- Continue gathering material
 - From libraries
 - From network Managers
 - From Applications
 - etc
- Publish within DNSOP?
 - Useful
 - BCP/Informational?



Questions?



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?**

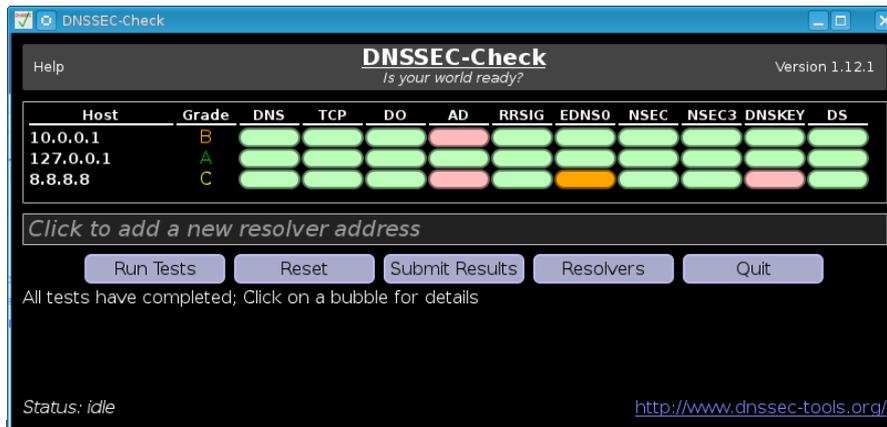
Experience: Unbound on home router

- 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_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]