From Diagnosis to Repair: A Large-Scale Study of DNSSEC Misconfigurations and an Automated Error Resolution Framework

Md. Ishtiaq Ashiq[§], Olivier Hureau[*], Casey Deccio[†], and Tijay Chung[§]

[§]Virginia Tech, [†]Brigham Young University, [*]University of Grenoble Alpes

Speaker: Md. Ishtiaq Ashiq
Venue: 45th DNS-OARC Workshop

VIRGINIA TECH

Background

- DNSSEC is important
- Adoption rate is still hovering around 7% [1]
- Why?
  - DNSSEC is complex
    - Deployment is difficult
    - Post-deployment challenges make things harder
  - Operational challenges still remain
  - Lack of incentives

[1] https://rick.eng.br/dnssecstat/

VIRGINIA TECH

Background

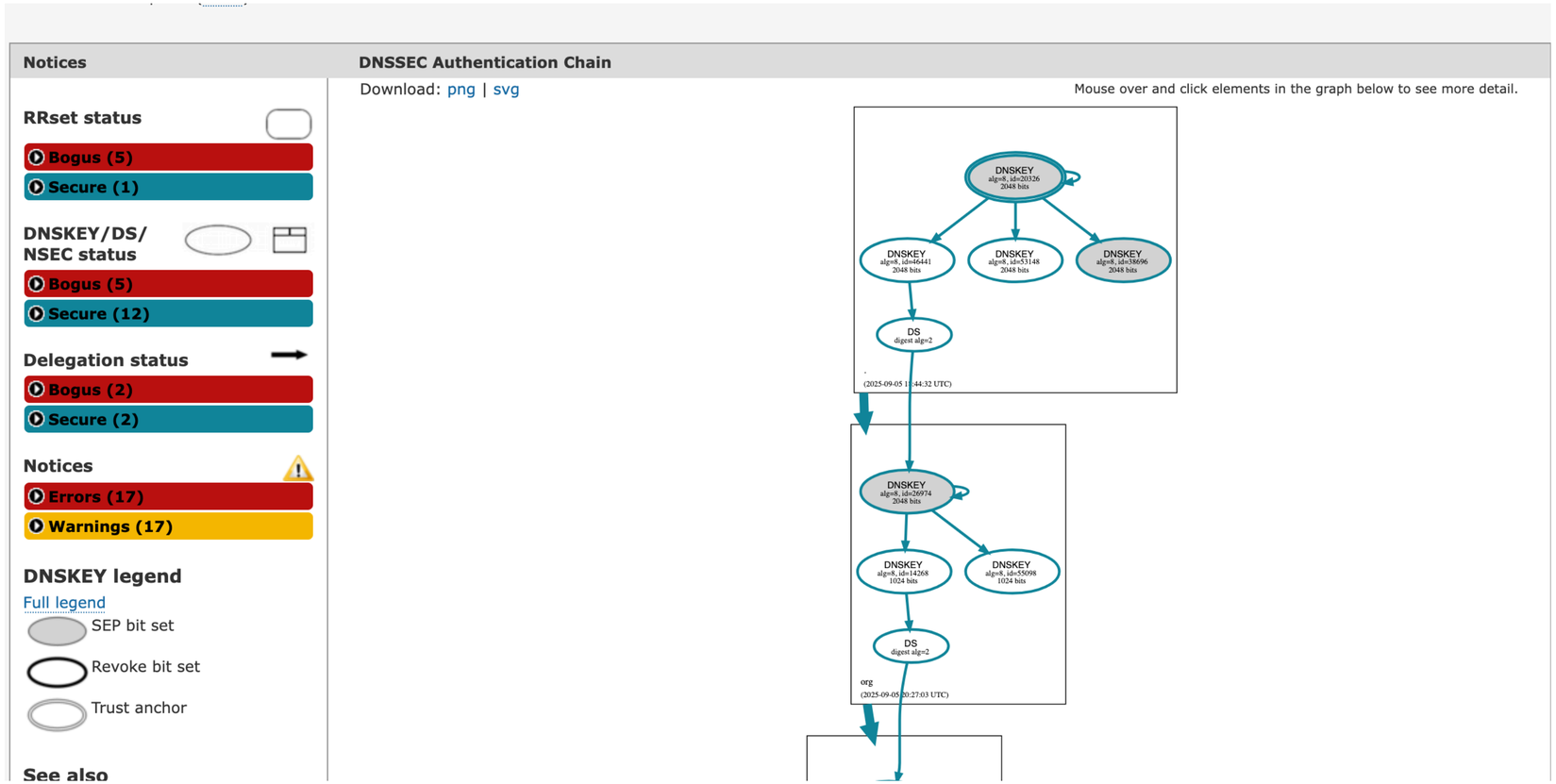
- DNSSEC is important
- Adoption rate is still hovering around 7% [1]
- Why?
  - **DNSSEC is complex**
    - **Deployment is difficult**
    - **Post-deployment challenges make things harder**
  - Operational challenges still remain
  - Lack of incentives

[1] https://rick.eng.br/dnssecstat/

VIRGINIA TECH

DNSViz

- Diagnostic website/tool
- Analyzes DNSSEC configuration
- Provides rich graphical visualization
- Assigns a set of error codes
- Has a CLI version as well



VIRGINIA TECH

Dataset

Category	Root	TLD	SLD+
Total Snapshots	6,234	356,136	747,455
Unique Domains	1	4,196	319,277
w/ at least Two Snapshots	1	2,349	84,962

Overview of our DNSViz dataset. It contains 1.1M total snapshots spanning from 2020-03-11 to 2024-09-25.

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Category Definition

Snapshot Categorization

- Signed and valid (sv)
- Signed and valid but w/ misconfigurations (svm)
- Signed and bogus (sb)
- Insecure (is)

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Category Definition

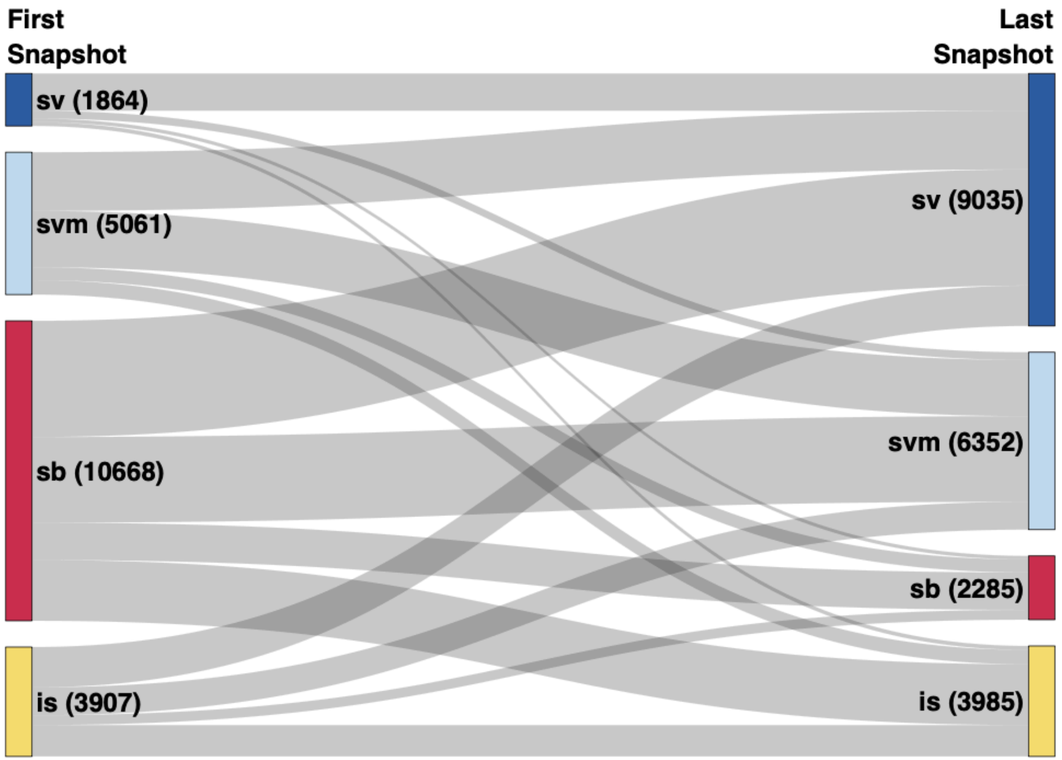
Domain Categorization

- Changing Domains (CD)
- Stable Domains (SD)

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Is DNSViz Useful?

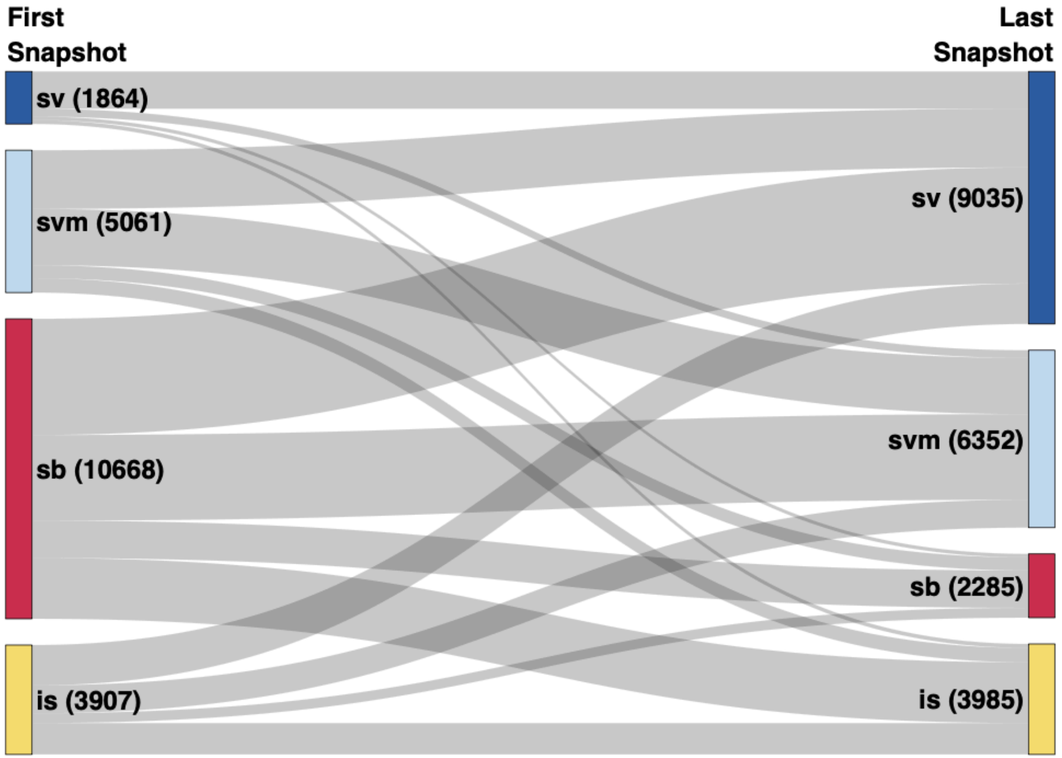


For domains in the CD category, comparing DNSSEC status between the first and last snapshots recorded by DNSViz. Note the moderate but significant fraction of domains that either enable or disable DNSSEC over time.

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Is DNSViz Useful?



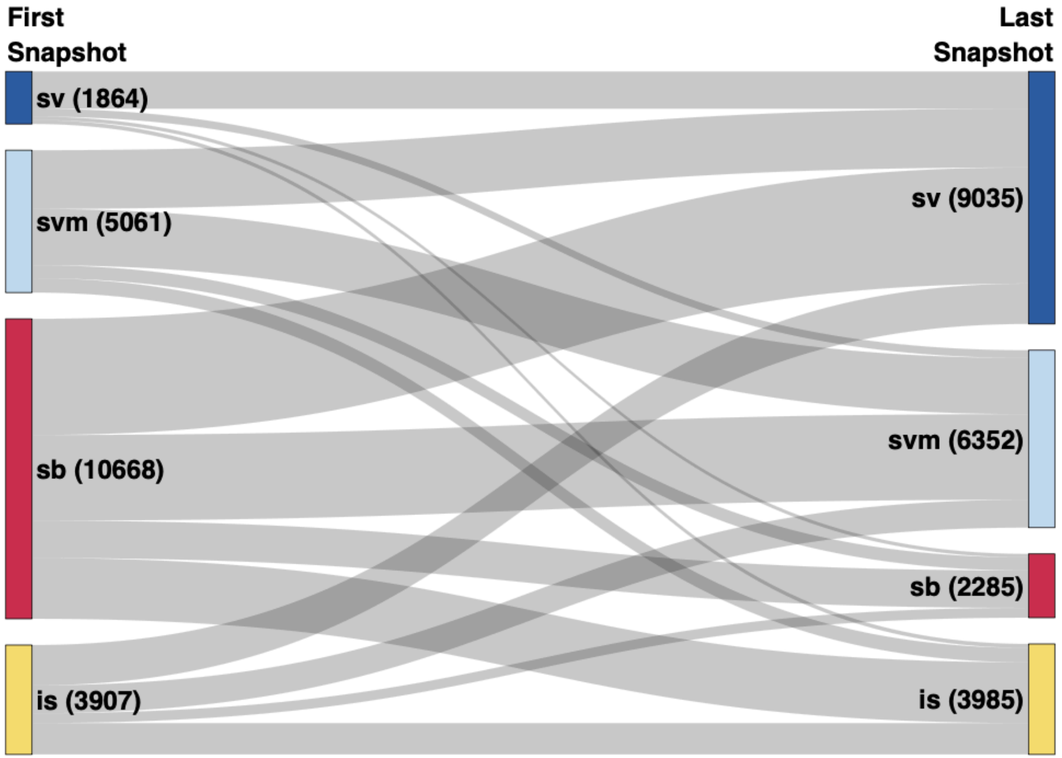
For domains in the CD category, comparing DNSSEC status between the first and last snapshots recorded by DNSViz. Note the moderate but significant fraction of domains that either enable or disable DNSSEC over time.

- 7,200 (67%) corrected errors
- 2,400 (62%) adopted DNSSEC

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Is DNSViz Useful?



For domains in the CD category, comparing DNSSEC status between the first and last snapshots recorded by DNSViz. Note the moderate but significant fraction of domains that either enable or disable DNSSEC over time.

- 7,200 (67%) corrected errors
- 2,400 (62%) adopted DNSSEC
- 650 (9.4%) disabled DNSSEC
- 588 (8.4%) transitioned to bogus

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Exploring Negative Transitions

Previous State	Transitioned State	Cause	# of domains
sv	sb	Total	4,064
		NS Update	272 (6.7%)
		Key Rollover	1,836 (45.2%)
		Algo Rollover	1,230 (30.3%)
sv	is	Total	804
		NS Update	56 (7%)
		Key Rollover	241 (30%)
		Algo Rollover	145 (18%)

Causes of negative transitions from a valid (sv) DNSSEC state to either bogus (sb) or insecure (is). Key rollovers and algorithm changes together account for roughly two-thirds of sv →sb transitions, while a smaller fraction stems from nameserver (NS) updates. We observe a similar pattern for sv →is transitions as well.

VIRGINIA TECH

Understanding DNSSEC Debugging Pattern

Error Prevalence in DNSSEC

Category	Subcategory	# of snapshots (%)	# of domains (%)
Delegation	Missing KSK for Algorithm	63,004 (8.4%)	25,102 (7.9%)
	Invalid Digest	1,103 (0.15%)	466 (0.15%)
Key	Inconsistent DNSKEY b/w Servers	19,330 (2.6%)	6,393 (2%)
Algorithm	Incomplete Algorithm Setup	6,859 (0.9%)	1,883 (0.5%)
Signature	Missing Signature	38,662 (5.2%)	18,306 (5.7%)
	Expired Signature	11,670 (1.6%)	4,494 (1.4%)
NSEC(3)	Missing Non-existence Proof	65,378 (8.7%)	17,768 (5.6%)
NSEC3 (Only)	Nonzero Iteration Count	215,036 (28.8%)	62,870 (19.7%)

Prevalence of some DNSSEC error types in our DNSViz dataset, covering 319,277 second-level and their lower-level domains (total 747,455 snapshots); for example, the “Nonzero Iteration Count” in NSEC3 appears in 215,036 snapshots (28.8%) spanning 62,870 domains (19.7%).

Observations

- Common Patterns of DNSSEC Errors
- Small Repertoire of BIND Commands

DFixer

We introduce DFixer, a semi-automated error resolution framework

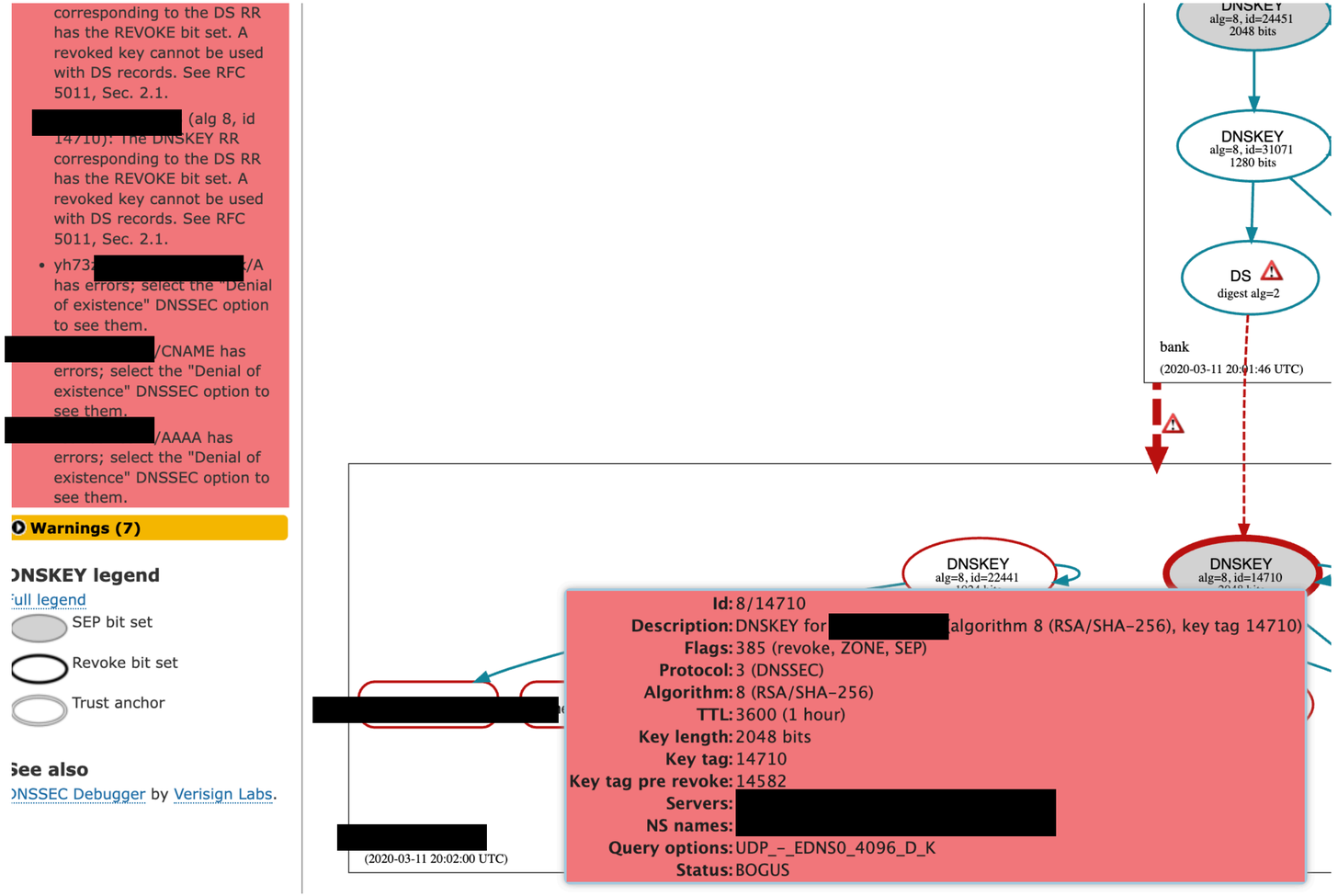
VIRGINIA TECH

Example Output from DFixer

Sample Problem

Let’s imagine a domain that have:

1. 1 KSK,
2. 1 ZSK and
3. KSK has the REVOKED bit set



Example Output from DFixer

Root Cause Identification

Root Cause: Your `DS` record is linked to a `DNSKEY` (key_tag=14, 710) with REVOKED flag on.

VIRGINIA TECH

Example Output from DFixer

Remediation Plan

Remediation Plan with `BIND` commands: Replace the path variables in angle brackets with values of your own environment. Parameters in braces and variables will be automatically populated by DFixer.

(1) Generate a new KSK key pair. Execute: `cd <key_dir> && dnssec-keygen -f KSK -a {algo} -b {key_size} -n ZONE {zone}`. This command should create two new key files inside your key directory; please note the name of the public key file (with `.key` extension).

(2) Generate the `DS` record from the generated public key file. Replace `public_key_file` with the name of the public key file from previous step and execute: `cd <key_dir> && dnssec-dsfromkey -2 <public_key_file>`. This command should show the contents of your `DS` record in standard output.

(3) Upload the `DS` record to the parent zone. This must be done manually via your registrar.

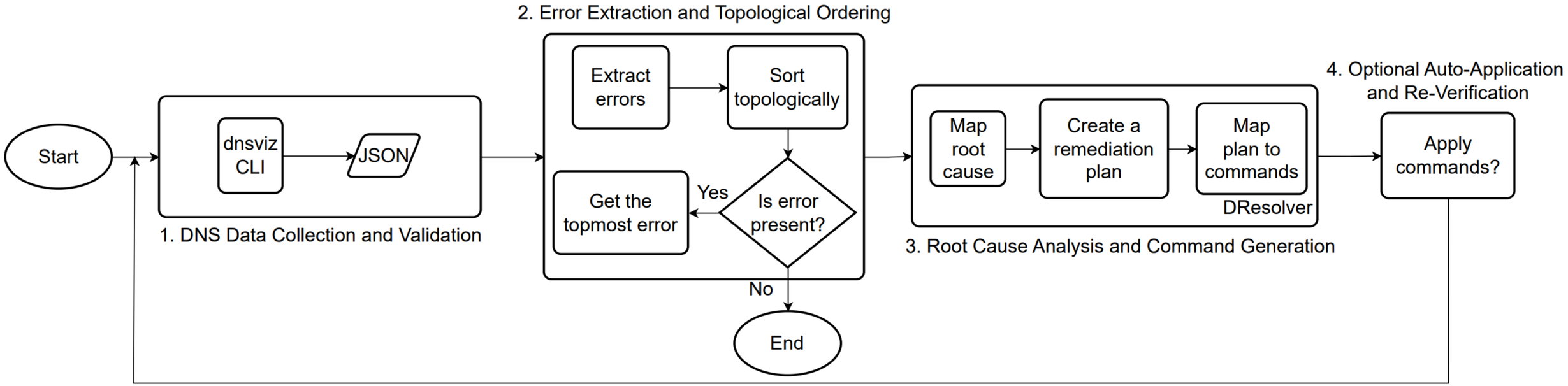
(4) Remove the `DS` record linked to the revoked DNSKEY (key_tag=14, 710) from the parent zone. This also needs to be done manually via your registrar.

(5) Wait at least one full TTL (*ttl*) for the removed `DS` record to expire from the cache of any validator. Nothing to execute; in "auto-apply" mode, DFixer will automatically infer the TTL and wait out this period before executing the next command.

(6) After *ttl* seconds, delete the DNSKEY (key_tag=14, 710, pre-revoked key_tag=14, 582) from your zone. Replace `key_file` with the name of the public key file associated with key_tag=*k*, and execute: `dnssec-settime -D {current_time} <key_dir/key_file>`

(7) Resign the zone. Execute: `cd <key_dir> && dnssec-signzone -N INCREMENT -3 {salt} -S -o {zone} -t <zone_dir/unsigned_zone_file>`

DFixer
Pipeline



Overview of the DFixer pipeline. Each iteration collects DNSSEC data with probe and grok filters relevant error codes, resolves root causes via DResolver, and produces fix commands. The process repeats until no blocking errors remain.

VIRGINIA TECH

Ok, we built DFixer...

But how would we evaluate it?

We have a lot of erroneous zones from DNSViz

VIRGINIA TECH

Can we recreate them in our own environment?

VIRGINIA TECH

ZReplicator

- Inject the exact misconfigurations (e.g., stale DS, invalid signatures) from DNSViz logs
- Run DFixer, apply suggested commands, and confirm that the zone becomes valid after re-checking

VIRGINIA TECH

ZReplicator
How?

- Create a Base Zone
- Emulate Parent and Child Zones
- Inject DNSSEC Errors

VIRGINIA TECH

Evaluation
Metrics

- Replication Rate (RR)
  - How comprehensively we can recreate real-world misconfigurations?

Evaluation
Metrics

- Fix Rate (FR)
  - How accurately DFixer resolves DNSSEC errors?

Evaluation
Results

Dataset	# of snapshots	RR	FR
Nonzero Iteration Count Only (S1)	168,482	98.81%	100%
Remaining (S2)	128,331	78.71%	99.99%
Total	296,813	90.11%	99.99%

Performance of ZReplicator and DFixer among the snapshots with DNSSEC Errors

VIRGINIA TECH

Instructions Issued By DFixer

Instructions	1st iteration	2nd iteration	3rd iteration	4th iteration
Sign the zone	62,406 (41.7%)	13,845 (90%)	1,148 (62.2%)	7 (19.4%)
Remove the incorrect DS record	46,242 (30.9%)	1,319 (8.6%)	668 (36.2%)	29 (80.6%)
Upload the DS record	14,066 (9.4%)	117 (0.8%)	12 (0.7%)	-
Generate a KSK	13,148 (8.9%)	83 (0.5%)	-	-
Synchronize the auth. servers	11,391 (7.6%)	-	-	-

Instructions issued by DFixer during its iterative remediation process in the S2 subset (i.e., zones with more complex DNSSEC errors). This highlights how DFixer repeatedly removes incorrect DS records, re-signs zones, or updates keys until all misconfigurations are resolved.

Discussion

Limitations: ZReplicator

- Some zone-file errors are unreproducible
- Only leaf-zone replication is supported
- Algorithm-distribution constraints

Discussion
Limitations: DFixer

- Requires manual update of DS record
- Optimality not guaranteed

Discussions
Extensibility

- Is DFixer extensible to other DNS Software?
  - NSD => Yes
  - PowerDNS => Yes*
  - Knot DNS => Yes

Thanks, any questions welcome!


iashiq5@vt.edu


ashiq5.github.io

VIRGINIA TECH