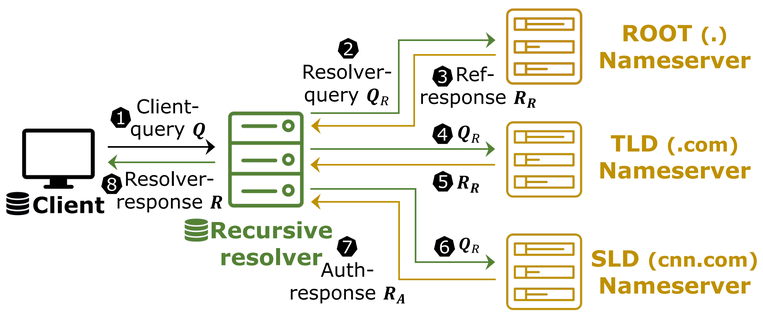
ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing

Qifan Zhang[1] Xuesong Bai[1] Xiang Li[2] Haixin Duan[2, 3, 4] Qi Li[2] Zhou Li[1]

[1]University of California, Irvine [2]Tsinghua University [3]Zhongguancun Laboratory [4]Quan Cheng Laboratory

DNS Resolution

- Translate human-friendly domains into machine-friendly IP addresses.
- **Recursive process**. Root servers, Top-Level Domain (TLD) servers, etc.
- **Multiple roles**. Forwarders, recursive resolvers, nameservers (NSes).



DNS Complexity and Vulnerability

- Over **100** RFCs.
- **Many use cases**. Web browsing, email, zero-trust network, autonomous vehicle, etc.
- **Many implementations**. 20+ widely used DNS software.
- **Fragmented service ecosystem**. Millions of NSes, open/local resolvers, and forwarders.
- **DNS failures and attacks happened a lot.**

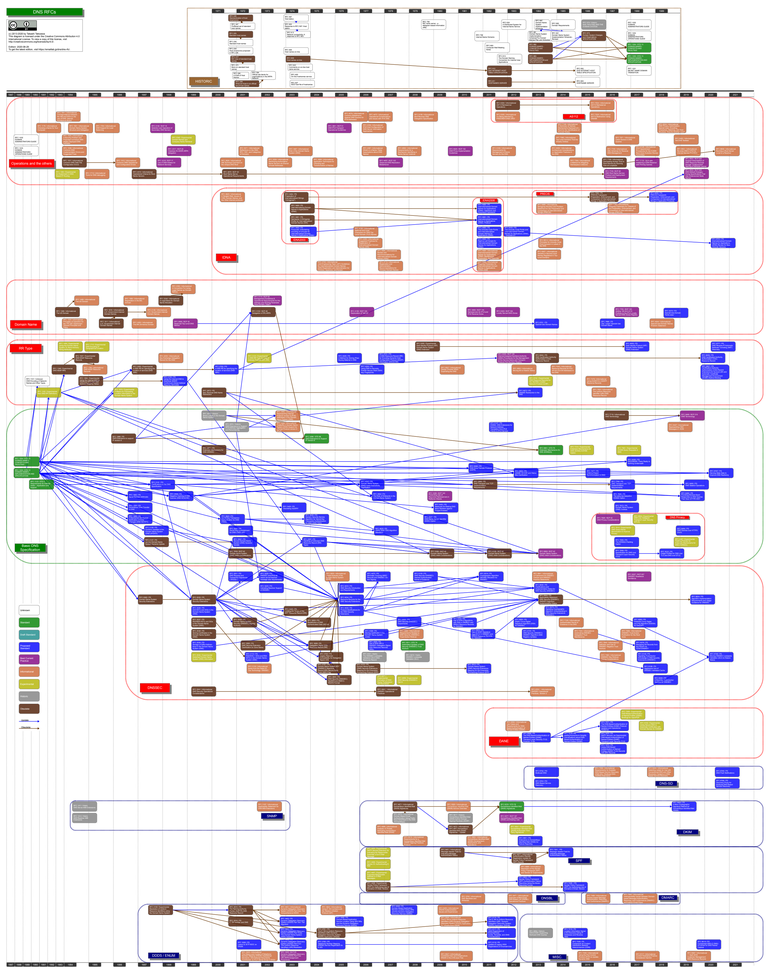
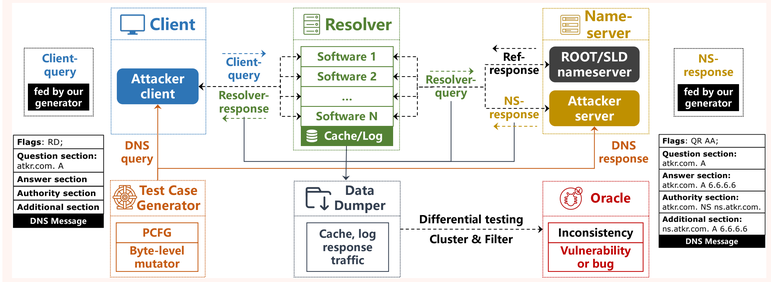


Figure 1. DNS RFCs (as of 2020) [2]

ResolverFuzz [4] Infrastructure

- **Input**: Query/Response generator.
- **Output**: response, cache dump, network traffic packets (tcpdump), system logs.
- **Oracle**: 3 oracles for each kind of vulnerabilities.

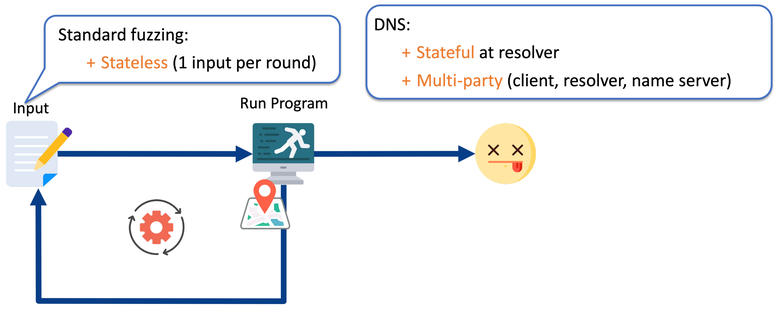


Challenges 1: Non-Crash Vulnerabilities

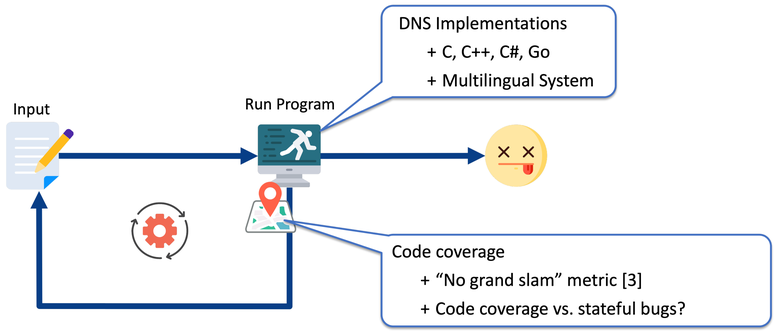
- DNS vulnerabilities **does not always lead to crashes**.
- Focus on categories of **identified bugs** via **CVE study** on CVEs ranging from 1999 to 2023.

Software*	# CVE							Total
	Non-crash				Crash			
	Cache Poisoning	Resource Consum.[1]	Others[2]	Total	Non-memory	Memory	Total	
BIND	18	18	11	47	75	22	97	144
Unbound	4	5	4	13	5	8	13	26
Knot Resolver	6	4	0	10	2	0	2	12
PowerDNS Recursor	13	8	9	30	7	6	13	43
MaraDNS	2	3	0	5	4	7	11	16
Technitium	3	1	0	4	0	0	0	4
Total	46	39	24	109	93	43	136	245

Challenges 2: Stateful Fuzzing



Challenges 3: Fuzzing Instrumentation



Identified Vulnerabilities

- Tested on **6 mainstream** DNS software.
- **23** vulnerabilities identified, **19** confirmed, **15** CVEs assigned, categorized into 3 classes.

MaginotDNS [Security'23, Black Hat USA'23] — Phoenix Domain [NDSS'23, OARC'39, Black Hat Asia'23] — TuDoor [S&P'24, OARC'42]

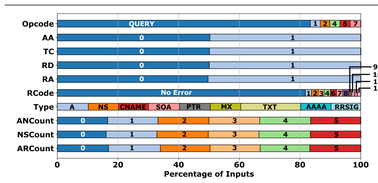
Software*	Cache poisoning					Resource consumption								Crash& Corruption	Total
	CP1	CP2	CP3	CP4[1]	Tot.[2]	RC1	RC2	RC3	RC4	RC5	RC6	RC7	Tot.	CC1	
BIND	✓†	✗	✓	✓	3	✗	✗	✗	✗	✗	✗	✗	0	✓	4
Unbound	✗	✗	✓	✓†	2	✗	✗	✓	✓	✓	✓	✗	4	-	6
Knot	✓†	✗	✓†	✓†	3	✗	✗	✗	✗	✗	✗	✓†	1	-	4
PowerDNS	✗	✓†	✗	✓†	2	✓†	✗	✓†	✗	✗	✗	✗	2	-	4
MaraDNS	✗	✗	-	✓†	1	✗	✗	✗	✓†	✗	✗	✗	1	-	2
Technitium	✓†	✗	-	✓†	2	✗	✗	✗	✓†	✗	✗	✗	1	-	3
Total	3	1	3	6	13	1	2	1	2	1	1	1	9	1	23

*: Recursive or forwarding modes. [1]: They are triggered by different responses and their cache are inconsistent. [2]: Total. ✓or ✓: Vulnerable.
✓: Discussed but no immediate action. ✓: Confirmed and/or fixed by vendors. ✗: Not vulnerable. [1]: CVEs assigned. '-': Not applicable.
Amount of test cases: *CP1* (19), *CP2* (1,422), *CP3* (111,328), *CP4* (7,856), *RC1* (539,745), *RC2* (112,126), *RC3* (88,935), *RC4* (132), *RC5* (272) *RC6* (6,264), *RC7* (4,448), and *CC1* (5).

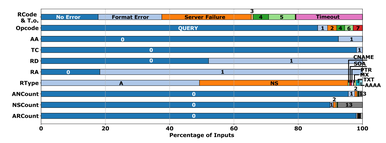
Input Generation

- **Two dimensions**. Generate a pair of query and response in each round.
- **Grammar-based fuzzing**. Generation is based on **Probabilistic context-free grammar (PCFG)**.
- **Byte-level mutation** [1]. **Special characters** (\., \000, @, /, and \) are embedded.

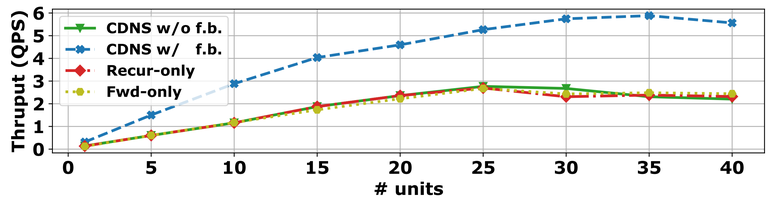
Evaluation Results



Client-queries and NS-responses.



Resolver-responses.



Throughput ("*Thruput*") of 4 modes with regard to the number of units. *CDNS w/o f.b.*, *CDNS w/ f.b.*, *Recur-only* and *Fwd-only* refers to *CDNS without fallback*, *CDNS with fallback*, *Recursive-only*, and *Forward-only*.

Project Resources

GitHub Repository — Qifan Zhang's Homepage — ResolverFuzz Homepage

References

[1] Philipp Jeitner and Haya Shulman.
Injection Attacks Reloaded: Tunnelling Malicious Payloads over DNS.
In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3165–3182, 2021.

[2] Takashi Takizawa.
DNS RFCs (2020-08-29).
`https://emaillab.jp/dns/dns-rfc/`, 2020.

[3] Jinghan Wang, Yue Duan, Wei Song, Heng Yin, and Chengyu Song.
Be sensitive and collaborative: Analyzing impact of coverage metrics in greybox fuzzing.
In *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*, pages 1–15, 2019.

[4] Qifan Zhang, Xuesong Bai, Xiang Li, Haixin Duan, Qi Li, and Zhou Li.
ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing.
In *Proceedings of the 33rd USENIX Security Symposium*, USENIX Security '24, 2024.