

OARC 47 · 2026

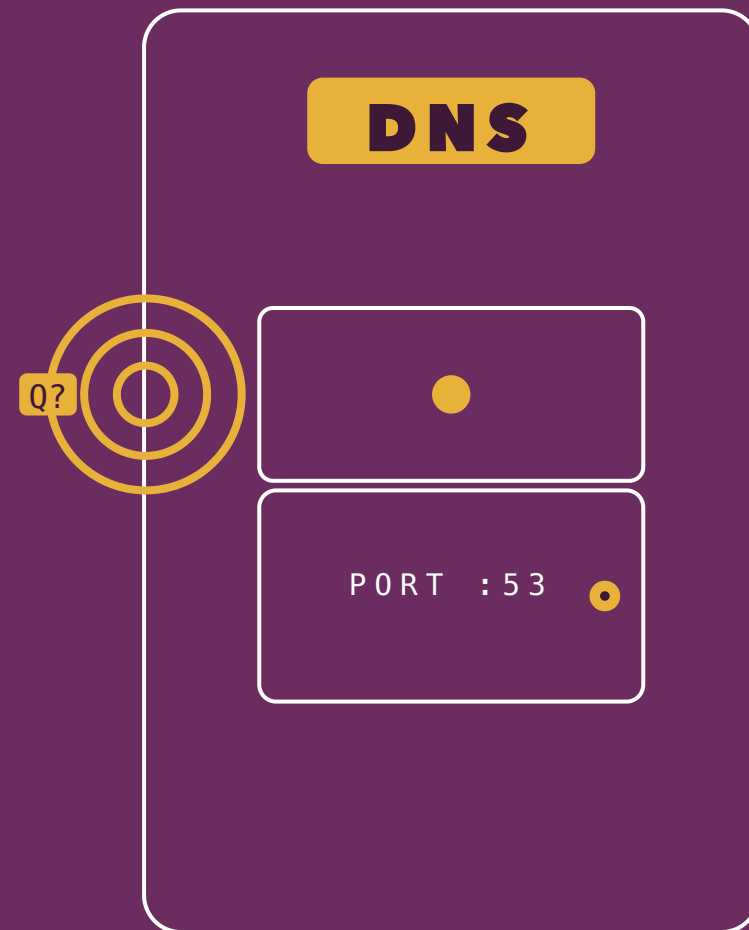
JIGGLE Attack

What Malformed Queries Reveal About DNS Resolver Security

Yuqi Qiu · Xiang Li · Zheli Liu

Nankai University

Nov, 2026



– MOTIVATION

The query-processing attack surface

What does a resolver **actually** do with a malformed query ?

The “back door”

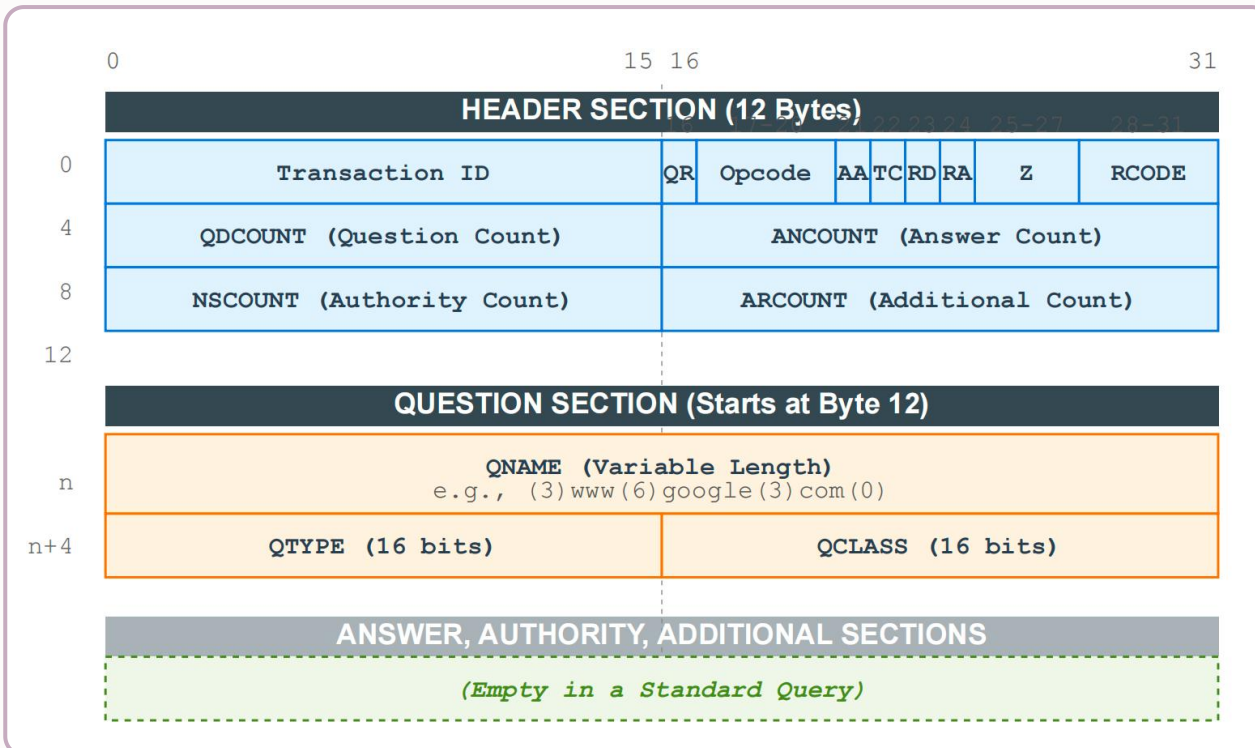
Response processing has received substantial security attention, including TuDoor.

The “front door”

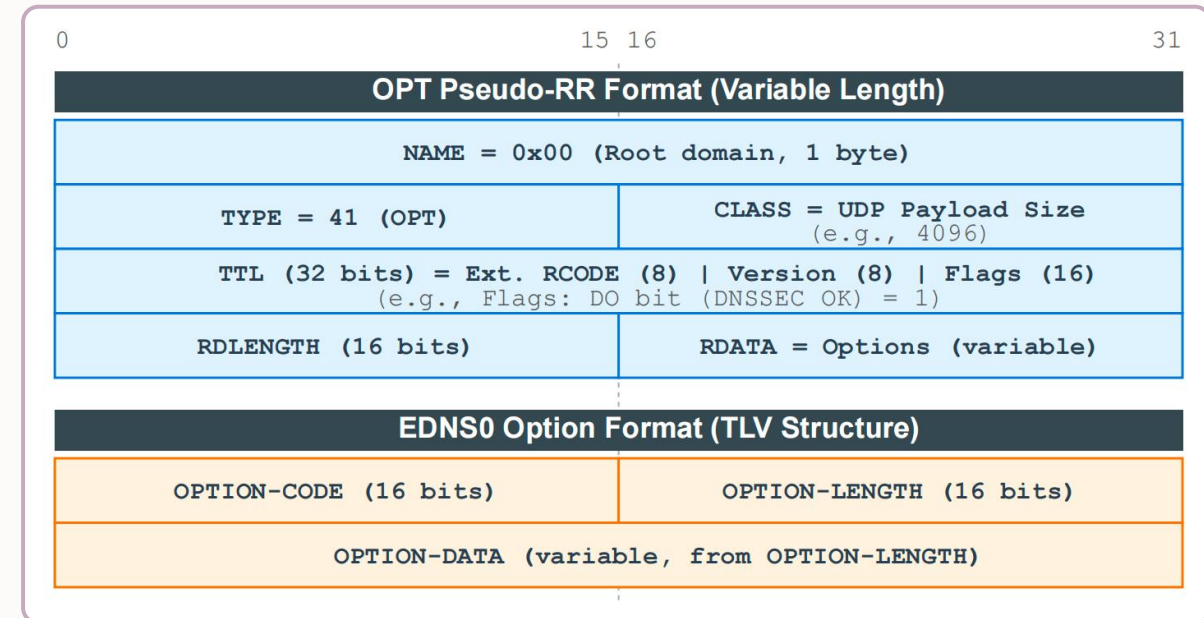
Logic vulnerabilities in query-processing pipelines:
an underexplored DNS attack surface.

– BACKGROUND

DNS Message Format



The structure of a Standard Common DNS Query packet (based on RFC 1035)



The EDNS0 extension mechanism (RFC 6891)

– BACKGROUND

The DNS Query Processing Pipeline

P1 Network Reception

queue check · IP-based ACL

P2 Protocol Validation

RFC 1035 header · pre-EDNS rate-limit · parse

P3 EDNS Parsing

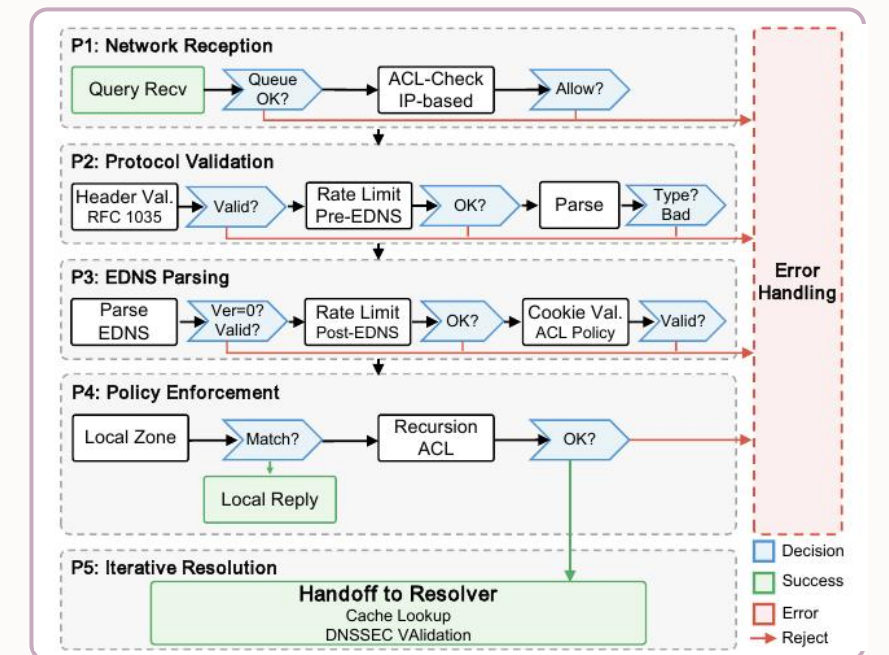
OPT RR · version · cookies · post-EDNS rate-limit

P4 Policy Enforcement

local zones · recursion ACL · RPZ

P5 Iterative Resolution

cache · DNSSEC · the back door



GENERIC DNS QUERY PROCESSING PIPELINE

Divergence in query validation, error handling or forwarding can create an attack surface.

– BACKGROUND

Why Resolvers Diverge

Ambiguous and fragmented specifications

- **Natural language, not formal grammar**
 - RFC use elastic terms – MUST, SHOULD, MAY
 - Same QDCOUNT=0 query → different behaviors
- **Inter-RFC dependency**
 - Parsing one packet may invoke 5 RFCs from different decades
 - RFC 2181 amends 1035; DNSSEC RFCs 4034/4035 add new logic

A complex parsing environment

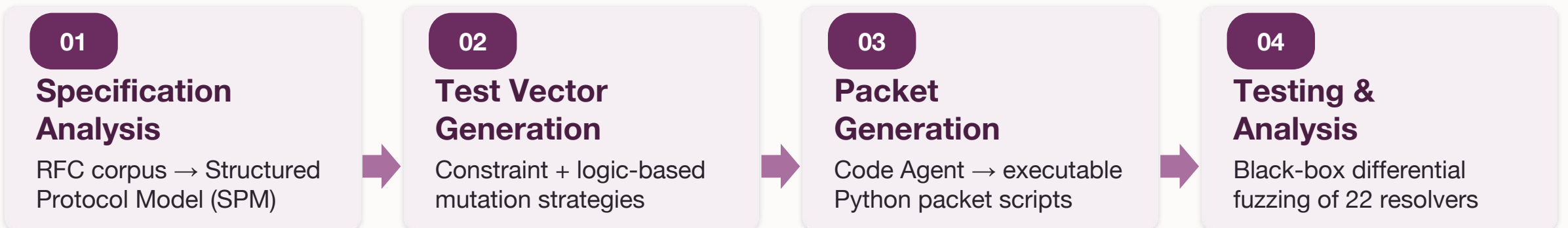
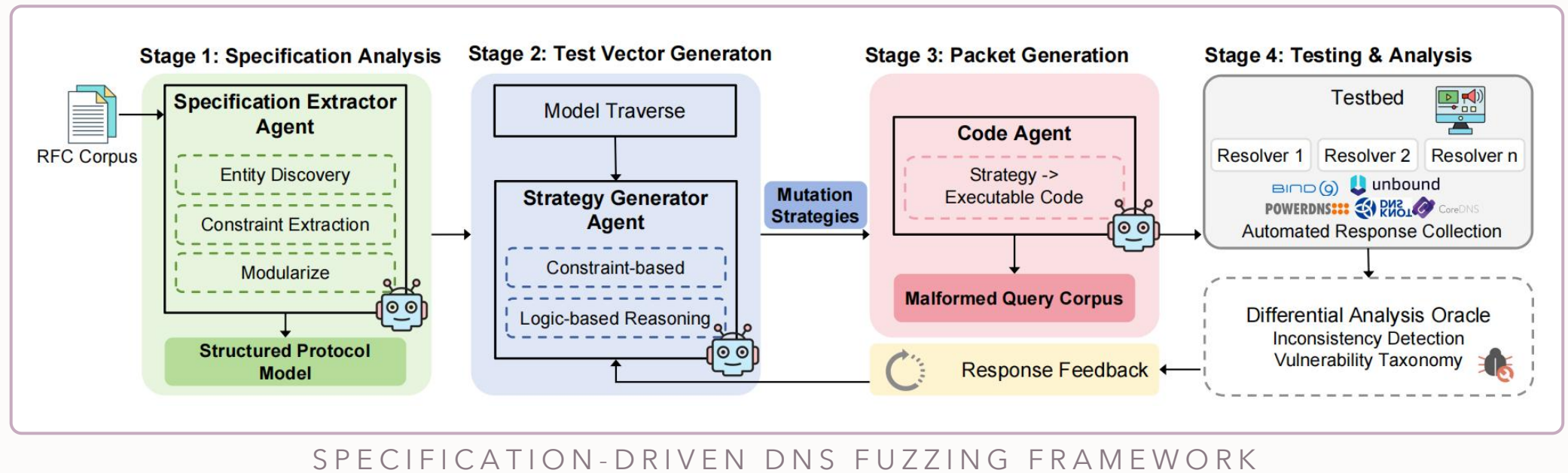
- **EDNS0 nested TLV options**
 - OPT RDATA holds variable-length, nested options (e.g., ECS)
 - Validity of one field depends on multi-pass parsing of others

– DNS CAMEL

"Each new RFC adds another straw to a protocol whose complexity already exceeds what any single implementer can internalise."

METHODOLOGY

QuerySynth: An LLM-Guided Specification-to-Test Pipeline



— METHODOLOGY

Stage 1: Building the Structured Protocol Model

RFCs to machine-readable constraints

NotebookLM

Step 1: Broad-Spectrum Entity Discovery

Q: Analyze the entire 299-RFC corpus. Scan all documents and generate a complete list of all defined protocol entity types.

A: Analysis complete. A comprehensive index of various DNS protocol entity types has been identified and categorized.

Step 2: Constraint-Focused Extraction

Q: Focus on [Current_Entity]. Analyze all RFCs to list all sub-fields, their names, lengths, types, and all constraints.

A: Extraction for [Current_Entity] complete.

Agent: Iterating Entity ...

Step 3: Synthesis and Materialization

Q: Synthesize all fields and constraints into the final SPM.

A: All entities extracted. Synthesizing all fields and constraints into the final SPM...



Source: 299 RFCs

- RR Types: [A, NS, CNAME, SOA, MX, TXT, AAAA, SRV, CAA, RRSIG, DNSKEY, ...]
- Query Types: [ANY (255), AXFR (252), ...]
- Meta-Types: [OPT (41), TSIG (250), TKEY, ...]
- Classes: [IN (1), CS (2), CH (3), ANY (255), ...]

Additional entities like Opcodes also noted in full output



Save to note

- Field: Flags, Constraint: 'Bit 0 is Issuer Critical...'
- Field: Tag Length, Constraint: 'Must be at least 1'
- Field: Tag, Constraint: 'Must be ASCII alphanumeric' ..."



Save to note



Convert all notes to source

Final Output (SPM) Snippet:

```
"Part1_Header": {
  "Field_Name": "ID (Transaction ID)",
  "Defined_RFC": "RFC 1035, RFC 5936",
  "Length": "16 bits (2 octets)",
  "Constraints_and_Handling_Rules": [
    "Assigned by the program generating the query.",
    "Must be copied into the corresponding response.",
    "Resolvers SHOULD check the ID...",
    "..."],
  ...
},
"Part2_Question": "...",
"Part3_Resource_Record": "...",
"Part4_EDNS_OPT_Pseudo_RR": "...",
"Part5_Encodings": "...",
```

RFC corpus

NotebookLM grounds extraction in the 299-RFC corpus.

Three extraction steps

Entity discovery → constraint extraction
→ hierarchical JSON model

Expert review

All 134 constraints manually audited
≈10 hours of expert effort.

Q&A FLOW FOR SPM EXTRACTION

– METHODOLOGY

Stage 2 • Constraint and logic-based strategies

The Strategy Generator Agent

Constraint-Based Mutation

- **Systematic violation of every documented MUST / MUST NOT / max-min**
- **Reserved Bit Violation**
 - e.g., set DNS-header Z bit to 1
- **Boundary Violation**
 - e.g., QDCOUNT = 2 in a standard query
- **Encoding Violation**
 - e.g., domain label of 64 bytes (limit is 63)
- **Semantic Constraint Violation**
 - e.g., compression pointer in CHAIN FQDN

Logic-Based Reasoning

- **Cross-field semantic contradictions a grammar-fuzzer cannot reach**
- **Structural Integrity Mismatch**
 - a count field that contradicts the actual data
- **Internal Consistency Mismatch**
 - RDLENGTH inconsistent with nested options
- **Protocol State Contradiction**
 - syntactically valid, semantically absurd
- **Encoding Abuse**
 - compression pointer pointing back to itself

– METHODOLOGY

Stage 3: PACKET GENERATION

Strategies → executable Python packet scripts

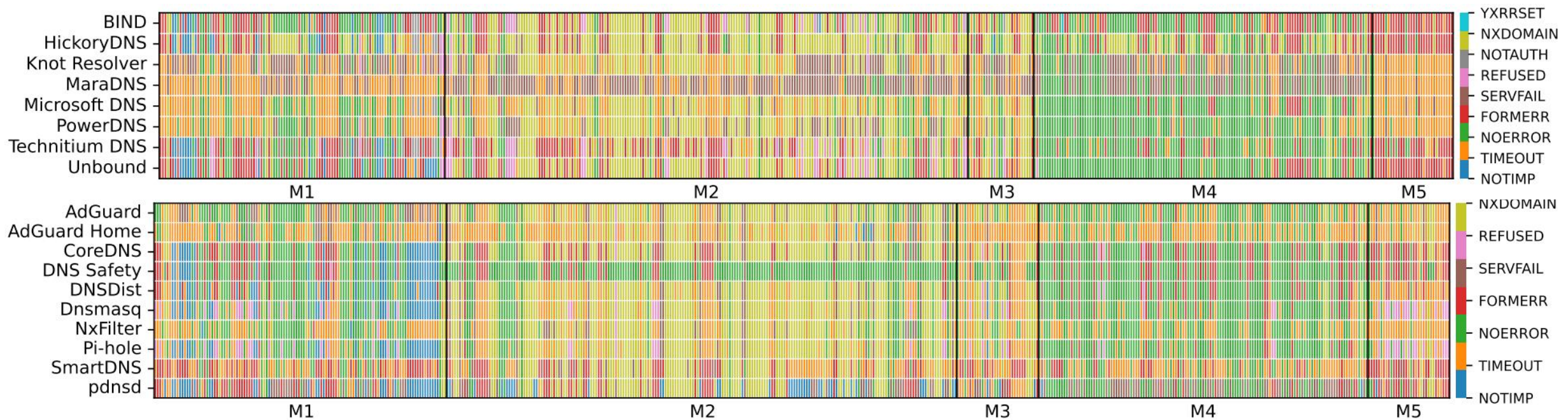
756 normalized mutation vectors in six categories

ID	Part	Count	Example
M1	Header	123	Query with ANCOUNT=N (answer records in quey)
M2	Question	213	QNAME label with length N containing only null
M3	Resource	56	Query asks for A but answer section contains AAAA
M4	EDNS	136	COOKIE option with too short Client Cookie length
M5	Encoding	33	Compression pointer to offset N(last byte of header)
M6	Mixed	195	Query with authority containing self-referential NS

— METHODOLOGY

Stage 4: TESTING

- 8 recursive + 10 forwarders.
- Black-box principle
- Differential Analysis Oracle



676 / 756 vectors triggered inconsistent behavior · 89.41%

– FINDINGS

Three classes of inconsistency

I.

Semantic

Different RCODEs for the same packet.

M4 EDNS: BIND → FORMERR
Microsoft DNS → NOERROR
MaraDNS → SERVFAIL.

II.

Content

Same RCODE, but radically different content.

Echo symmetry: Unbound returns a 65,535-byte FORMERR mirroring the malformed query.

III.

Decision

Some reject; others go silent.

REJECT vs. TIMEOUT asymmetry opens a multi-second deterministic vulnerability window.

– ATTACKS

JIGGLE. the act of disturbing a lock without precise tools.

A1

Echo-Based Pulsing DoS

1,083× bandwidth amplification: low-rate input into a high-bandwidth pulse.

A2

Echo Covert Channel

Resolver becomes an unwitting C2 relay and no domain registration needed.

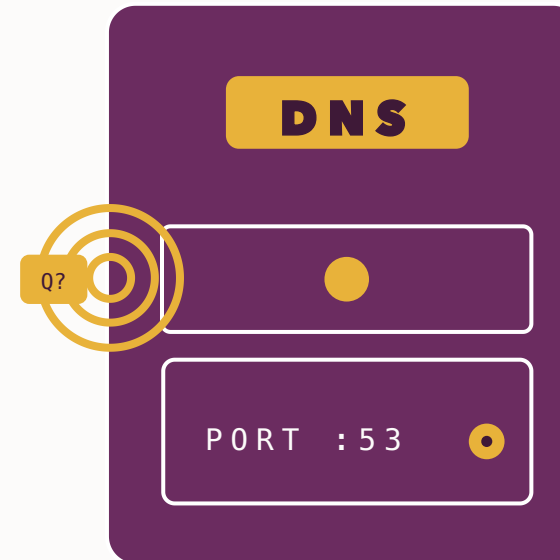
B

Asymmetric-Parsing Poisoning

Silence switch → multi-second deterministic cache-poisoning window.

Two attack channels, mapped to response status

- **Responsive (Replied) → Data-plane exploitation**
 - the resolver leaks anomalous data back
- **Silent (No reply) → Control-plane manipulation**
 - upstream silence opens internal-state flaws

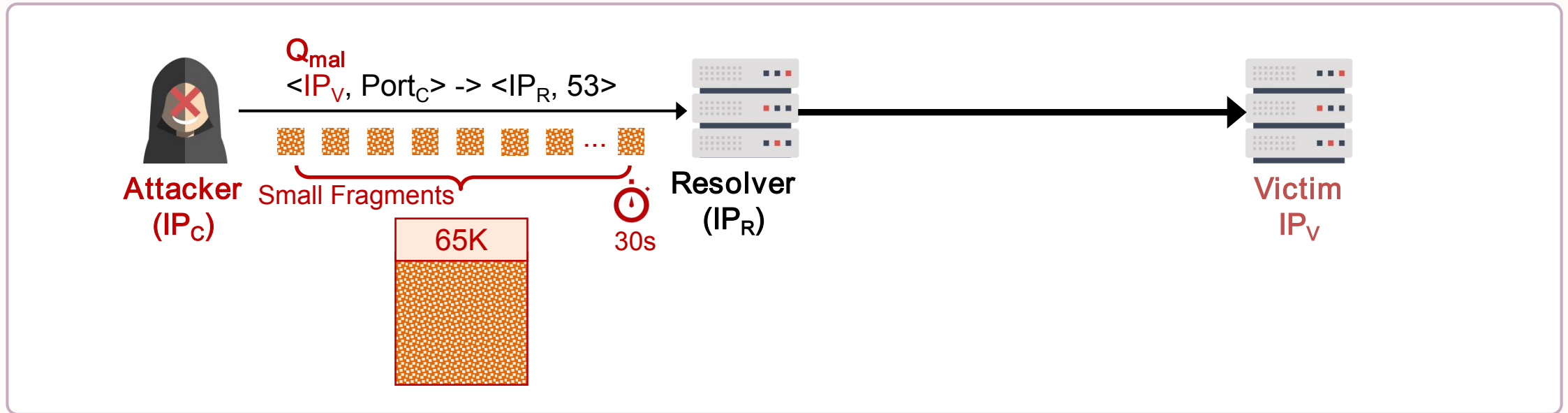


– ATTACKS

Resolver			Echo				Silent			Vulnerability		
Actor	Software	Version	#	max size	Mutation Field	Rcode	#	Vectors [†]	Mutation Field*	V_{EP}	V_{EC}	$V_{APP}^{\ddagger}$
Recursive	BIND	9.20.15	X	-	-	-	✓	8	M4	X	X	✓
	Unbound	1.24.1	✓	65535	M1+M2/M3,M4	FORMERR	✓	2	M2	✓	✓	✓
	PowerDNS	5.2.5	X	-	-	-	✓	185	M1	X	X	✓
	Knot Resolver	5.7.6	X	-	-	-	✓	201	M2	X	X	✓
	Microsoft DNS	2025	✓	4000	M4	FORMERR	✓	207	M2	✓	✓	✓
	Technitium DNS	13.6	X	-	-	-	✓	55	M4	X	X	✓
	MaraDNS	3.5.0036	✓	512	M1+M2/M3	SERVFAIL	✓	211	M1	✓	✓	✓
	Hickory DNS	0.26.0-alpha.1	✓	4096	M1+M2/M3	FORMERR	✓	9	M1	✓	✓	X
Forwarder	Dnsmasq	2.91	✓	1232	M1+M2/M3	REFUSED	✓	114	M2	✓	✓	✓
	Pi-hole	6.2.2	✓	1232	M1+M2/M3	REFUSED	✓	111	M2	✓	✓	✓
	SmartDNS	47	X	-	-	-	✓	275	M6	X	X	✓
	CoreDNS	1.13.1	X	-	-	-	X	-	-	X	X	X
	DNSDist	2.1.0-alpha0	X	-	-	-	✓	98	M2	X	X	✓
	AdGuard	7.2	X	-	-	-	✓	154	M4	X	X	✓
	DNS Safety	2.1	X	-	-	-	X	-	-	X	X	X
	AdGuard Home	107.69	X	-	-	-	✓	430	M6	X	X	✓
	pdnsd	1.2.9a	✓	512	M1+M2/M3	NOERROR	✓	13	M1	✓	✓	✓
	NxFilter	4.7.3.9	X	-	-	-	✓	214	M4	X	X	✓

– ATTACKS

Primitive A1 · Echo-Based Fragmentation Pulsing DoS

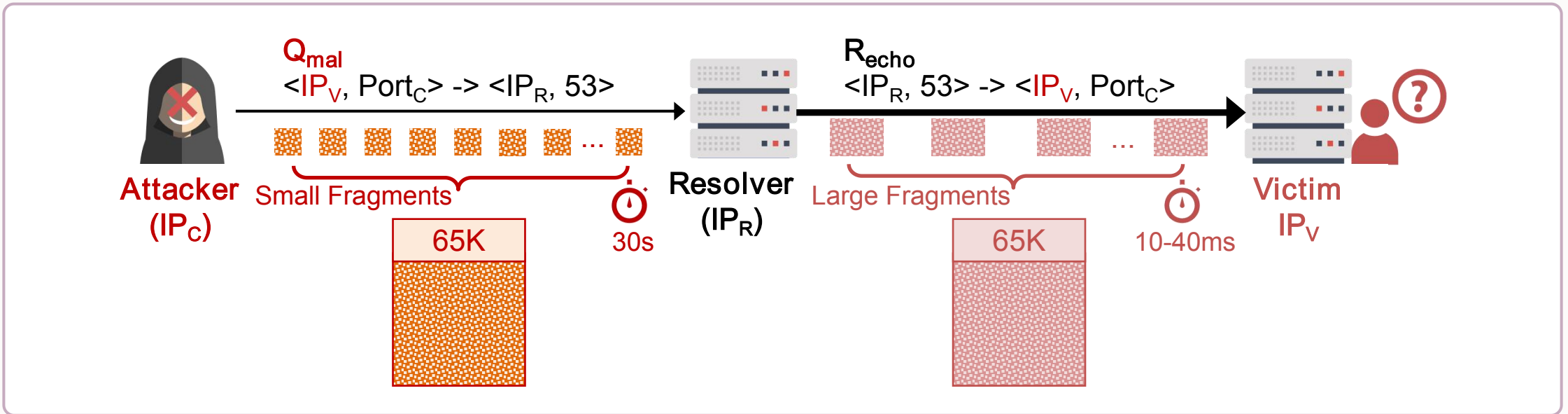


MECHANISM

- Craft a 65,535-byte malformed query → echo defect.
- Spoof victim IP · split into 24-byte fragments · 10 ms apart.
- Resolver reassembles via 30 s timeout · bursts 65 KB FORMERR.

– ATTACKS

Primitive A1 · Echo-Based Fragmentation Pulsing DoS



MECHANISM

- Craft a 65,535-byte malformed query → echo defect.
- Spoof victim IP · split into 24-byte fragments · 10 ms apart.
- Resolver reassembles via 30 s timeout · bursts 65 KB FORMERR.

BANDWIDTH AMPLIFICATION FACTOR

1,083×

validated against Unbound 1.24.1

48.4
Kb/s
attacker

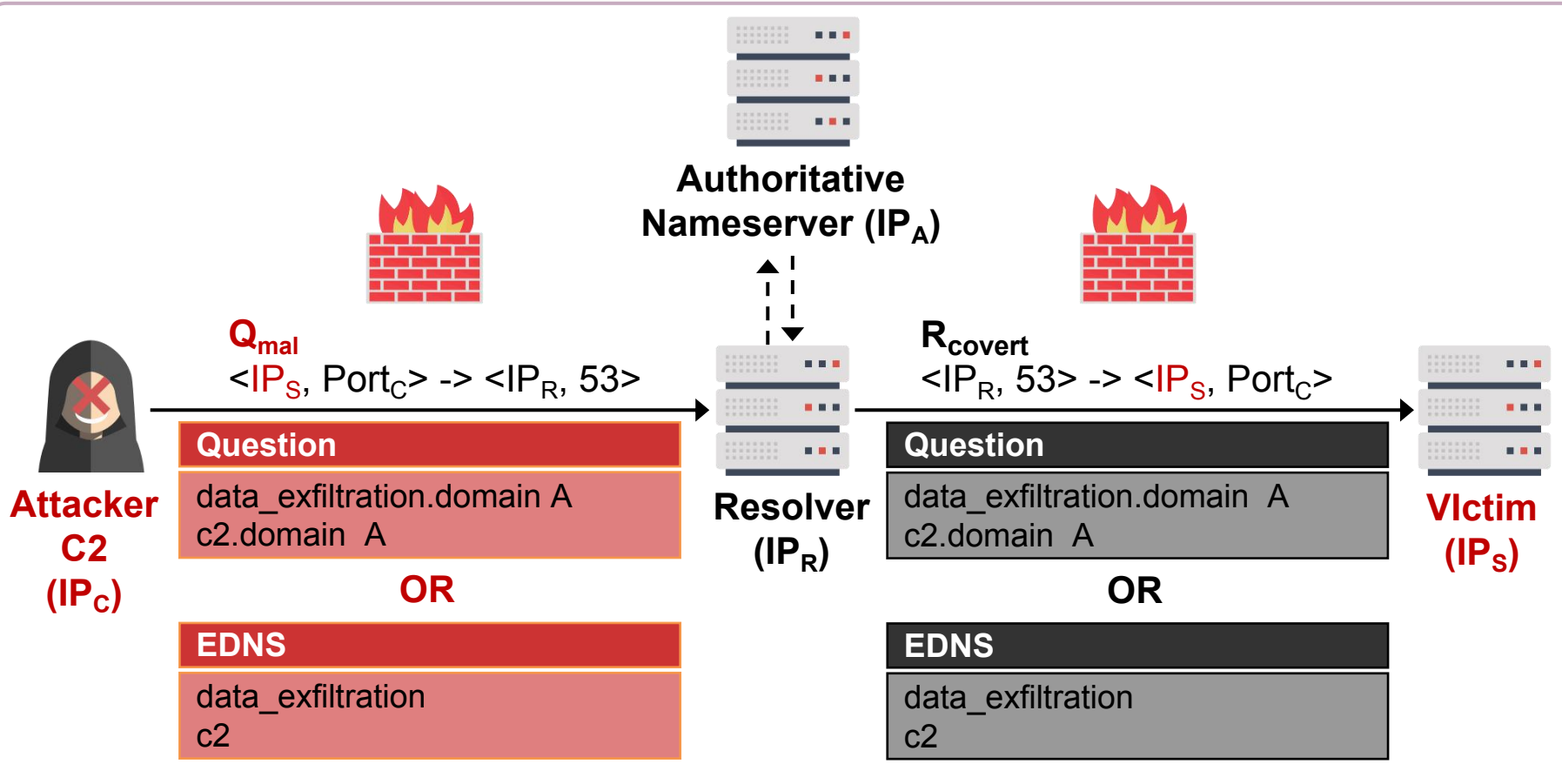
51.2
Mb/s
victim pulse

>1.5
Gb/s
coordinated

– ATTACKS

Primitive A2 · Echo-Based Covert Channel

The resolver becomes an **unwitting** one-way C2 relay.



HOW IT WORKS

- Embed exfil data in malformed query fields.
- Spoof the receiver as source IP.
- Echo defect → FORMERR copies data into response.
- Reflected response delivered to spoofed receiver.

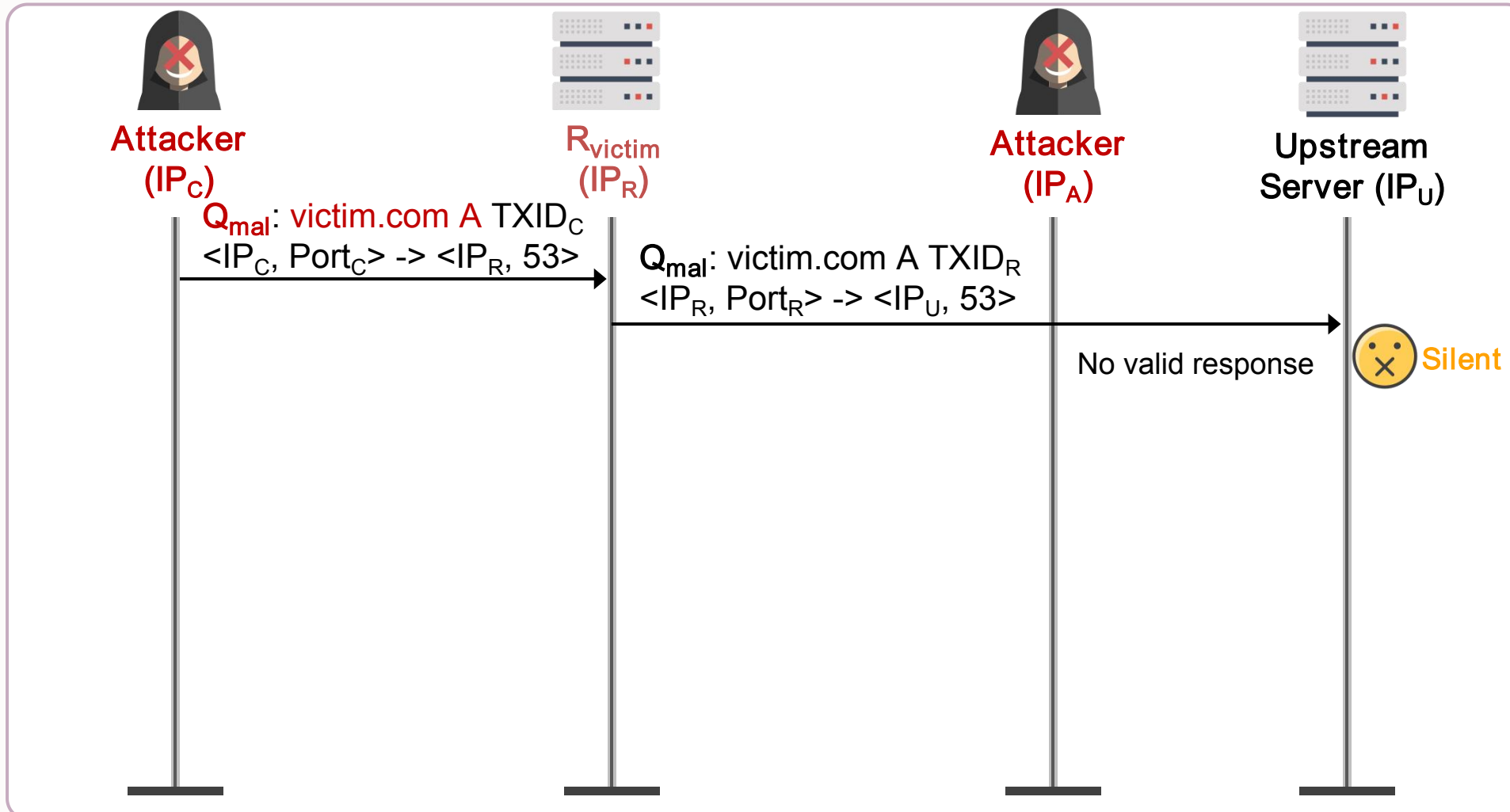
WHY IT'S HARD TO DEFEND

- No domain registration → DNS-name detection fails.
- Rides legitimate FORMERR → blends into benign error noise.

– ATTACKS

Primitive B · Asymmetric-Parsing Poisoning

Turning silent rejection into a deterministic, multi-second poisoning window



SILENCE SWITCH

- Q_{mal} · valid Question + anomalous flags / EDNS.
- Lenient forwarder forwards, while strict upstream drops silently.
- Forwarder trapped in long timeout → deterministic window.

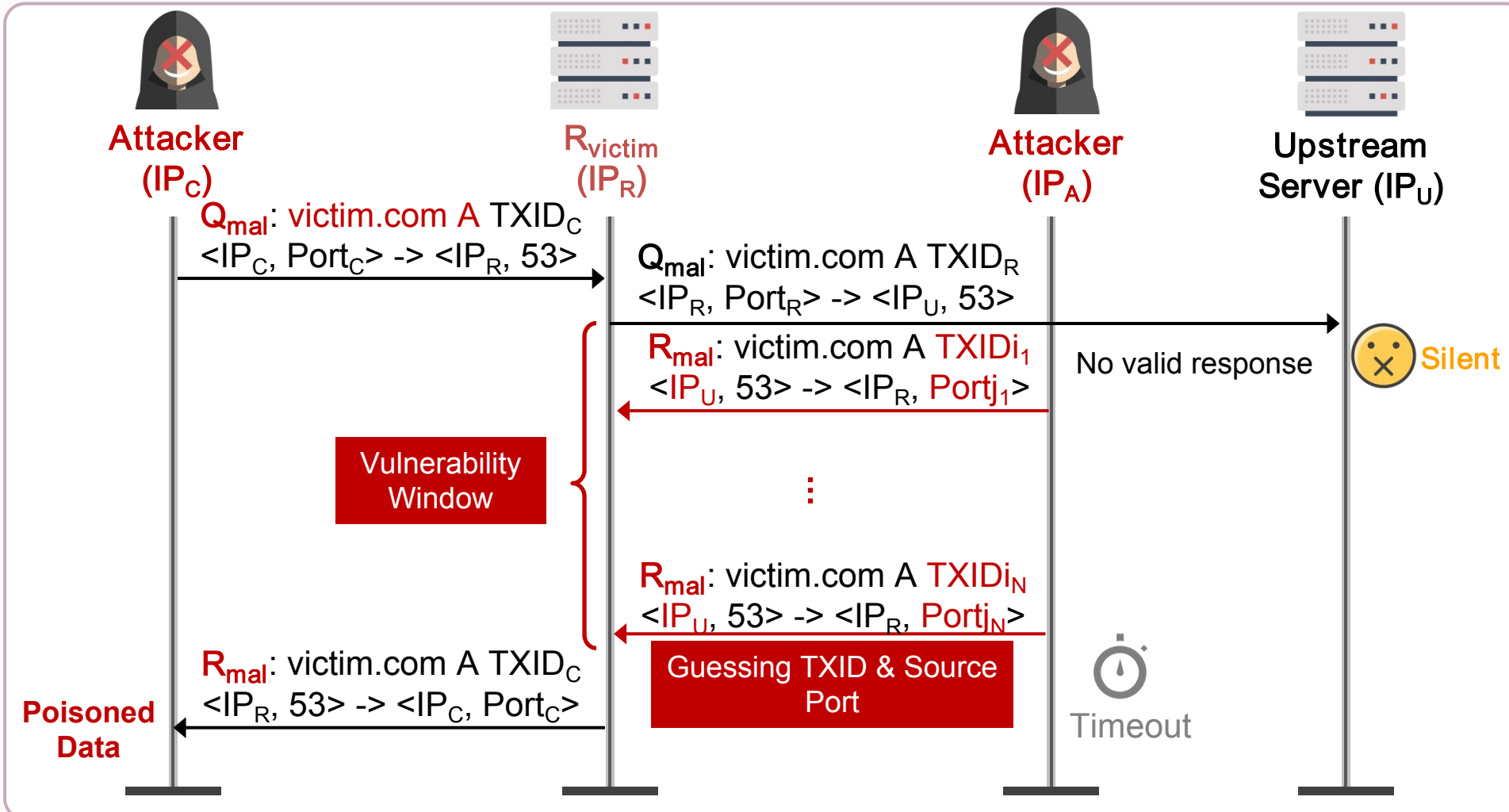
FORCE-MULTIPLIERS

- 60× larger window – race timeout, not sub-ms response.
- Weaponises 12 known cache-poisoning attacks (2002 – 2025).

– ATTACKS

Primitive B · Asymmetric-Parsing Poisoning

Turning silent rejection into a deterministic, multi-second poisoning window



SILENCE SWITCH

- Q_{mal} · valid Question + anomalous flags / EDNS.
- Lenient forwarder forwards, while strict upstream drops silently.
- Forwarder trapped in long timeout → deterministic window.

FORCE-MULTIPLIERS

- 60x larger window – race timeout, not sub-ms response.
- Weaponises 12 known cache-poisoning attacks (2002 – 2025).

– Vulnerable Resolvers in the Wild

44 Major Public DNS Services

18 / 44 (40.90%) exhibit responsive (echo) behavior: vulnerable to A1 + A2.

40/44 silently drop and vulnerable to B.

Affected: Ali DNS, Quad9, Comodo, ControlD, Yandex, etc.

1.31 M Open Resolvers (XMap scan)

924,808 (70.33%)

vulnerable to ≥ 1 JIGGLE primitive.

Echo : 75,711 (5.76%)

Silent: 852,770 (64.84%)

Public DNS Service		Echo				Silent		Vulnerability		
DNS	IP	#	max size	Mutation Field	Rcode	# Vectors [†]	Mutation Field*	V _{EP}	V _{EC}	V _{APP}
114DNS	114.114.114.114	✗	-	-	-	✓ 288	M2	✗	✗	✓
360 Secure DNS	218.30.118.6	✗	-	-	-	✓ 274	M1	✗	✗	✓
AdGuard DNS	94.140.14.14	✗	-	-	-	✓ 138	M4	✗	✗	✓
Ali DNS	223.5.5.5	✓	1232	M1+M2/M3	FORMERR	✓ 74	M1	✓	✓	✓
AhaDNS	45.67.219.208	✓	512	M1+M2/M3	FORMERR	✓ 506	M2	✓	✓	✓
Akamai Vantio DNS	23.56.160.142	✗	-	-	-	✓ 179	M1	✗	✗	✓
Baidu DNS	180.76.76.76	✗	-	-	-	✓ 24	M4	✗	✗	✓
ByteDance DNS	180.184.1.1	✓	512	M1+M2/M3	REFUSED	✓ 189	M4	✓	✓	✓
CIRA Shield DNS	149.112.121.10	✗	-	-	-	✓ 13	M1	✗	✗	✓
CNNIC sDNS	1.2.4.8	✓	1232	M1+M2/M3	FORMERR	✓ 34	M2	✓	✓	✓
CZ.NIC ODVR	193.17.47.1	✗	-	-	-	✓ 202	M2	✗	✗	✓
CenturyLink DNS	205.171.3.66	✗	-	-	-	✓ 33	M2	✗	✗	✓
Cisco OpenDNS	208.67.222.222	✗	-	-	-	✓ 13	M1	✗	✗	✓
CleanBrowsing	185.228.168.9	✗	-	-	-	✓ 531	M2	✗	✗	✓
CloudFlare DNS	1.1.1.1	✗	-	-	-	✓ 102	M2	✗	✗	✓
Comodo Secure DNS	8.26.56.10	✓	4096	M2	FORMERR	✓ 160	M1	✓	✓	✓
ControlD DNS	76.76.2.5	✓	1500	M4	FORMERR	✓ 307	M2	✓	✓	✓
DNS Forge	176.9.93.198	✗	-	-	-	✓ 200	M1	✗	✗	✓
DNS for Family	94.130.180.225	✗	-	-	-	✓ 94	M2	✗	✗	✓
DNS.SB	185.222.222.222	✗	-	-	-	✓ 171	M1	✗	✗	✓
DNS.WATCH	84.200.69.80	✓	65535	M4	FORMERR	✓ 470	M2	✓	✓	✓
DNSPod Public DNS+	119.28.28.28	✗	-	-	-	✓ 217	M1	✗	✗	✓
Dyn DNS	216.146.36.36	✓	512	M1+M2/M3	FORMERR	✓ 125	M2	✓	✓	✓
Freenom World	80.80.81.81	✗	-	-	-	✓ 594	M2	✗	✗	✓
G-Core DNS	95.85.95.85	✗	-	-	-	✓ 171	M1	✗	✗	✓
Hurricane Electric DNS	74.82.42.42	✗	-	-	-	✓ 176	M1	✗	✗	✓
Google DNS	8.8.4.4	✗	-	-	-	✓ 36	M1	✗	✗	✓
Level3 DNS	209.244.0.3	✓	65535	M4	FORMERR	✓ 13	M2	✓	✓	✓
LibreDNS	88.198.92.222	✗	-	-	-	✓ 170	M1	✗	✗	✓
Neustar UltraDNS	156.154.70.1	✓	512	M1+M2/M3	FORMERR	✓ 198	M4	✓	✓	✓
NextDNS	45.90.28.118	✓	512	M1+M2/M3	FORMERR	✓ 156	M4	✓	✓	✓
Norton ConnectSafe	199.85.126.10	✓	512	M1+M2/M3	FORMERR	✓ 203	M4	✓	✓	✓
OneDNS	117.50.10.10	✗	-	-	-	✓ 299	M2	✗	✗	✓
OpenNIC DNS	103.1.206.179	✗	-	-	-	✓ 1	M6	✗	✗	✗
Quad101	101.101.101.101	✗	-	-	-	✓ 4	M6	✗	✗	✓
Quad9 DNS	9.9.9.9	✓	4096	M1+M2/M3	FORMERR	✓ 131	M2	✓	✓	✓
SafeDNS	195.46.39.39	✓	65535	M4	FORMERR	✓ 1	M6	✓	✓	✗
SafeSurfer DNS	104.155.237.225	✗	-	-	-	✓ 213	M1	✗	✗	✓
SkyDNS	193.58.251.251	✓	65535	M4	FORMERR	✓ 1	M6	✓	✓	✗
Strongarm DNS	54.174.40.213	✗	-	-	-	✓ 205	M1	✗	✗	✓
Tiarap Public DNS	174.138.21.128	✓	65535	M4	FORMERR	✓ 1	M6	✓	✓	✗
Verisign Public DNS	64.6.64.6	✓	512	M1+M2/M3	FORMERR	✓ 354	M2	✓	✓	✓
Yandex DNS	77.88.8.1	✓	512	M1+M2/M3	FORMERR	✓ 31	M4	✓	✓	✓

– Disclosure & Remediation

Responsible Disclosure · 8 vendors + 38 public DNS providers

- Fixes & improvements – Unbound and AdGuard: fixes released with public attribution; Technitium: developer fix completed; Hickory: stricter parsing prompted; DNS Forge: service hardened.
- Bug bounty – DNSPod.
- Review & acknowledgment – Knot Resolver, PowerDNS, Quad9, Cisco OpenDNS, Yandex, ControlD, Akamai Vantio, DNS.SB, CZ.NIC ODVR, AliDNS, ByteDance DNS.

– DISCUSSION

FOR RESOLVER DEVELOPERS

→ DO

- Strict validation; generic FORMERR
- Mitigate the echo defect: error responses must be minimal.
- Avoid silent drops, prefer explicit errors.

IETF and DNS operators

→ STANDARDISE

- No standardised error-handling spec.
- Issue a BCP defining required behaviour for malformed-query classes.
- Standardise error-handling logic for invalid inputs, not just valid ones.
- Lesson: RFC ambiguity is a primary source of vulnerability.

– Wrap-up

Thanks for listening!

Yuqi Qiu

<https://www.yuqiqiu.space/>
qiuyuqi@mail.nankai.edu.cn