Path to Encrypted DNS with DDR: Adoption, Configuration Patterns, and Privacy Implications

15 July 2025, PETS 2025

vasilis ververis, Steffen Sassalla, Felix Roth, Vaibhav Bajpai

Hasso Plattner Institute, University of Potsdam, Germany

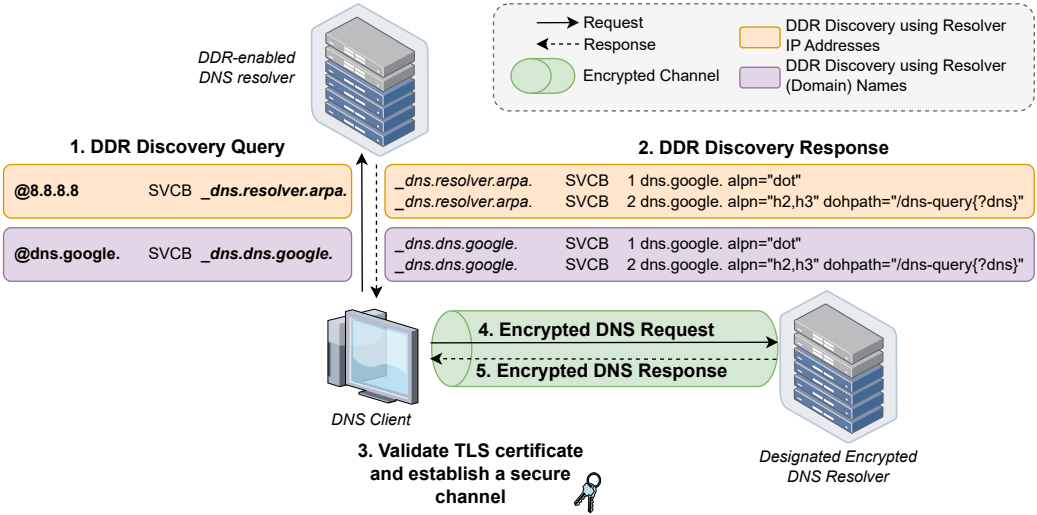
Motivation

- DNS traffic is often unencrypted, exposing users to privacy risks
- DNS over Encryption (DoE) protocols aim to secure DNS
- DDR (Discovery of Designated Resolvers) enables automatic upgrade to encrypted DNS

What is DDR? I

- RFC 9462 (November 2023)
- DDR allows clients to discover encrypted DNS resolvers
- Uses SVCB records to advertise encrypted resolvers
- Supports discovery via IP or domain name

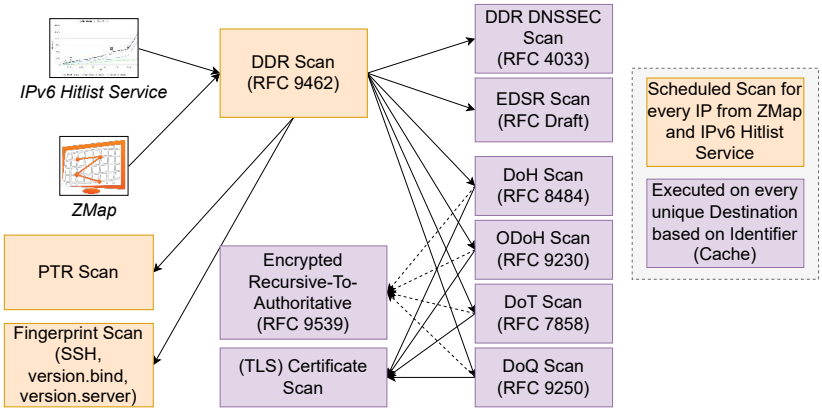
What is DDR? II



Methodology I

- **DNS Server Discovery:** ZMap (IPv4), IPv6 Hitlist
- **Measurement Period:** July - November 2024
- **Three-stage architecture**:
  1. Discover DNS servers (IPv4/IPv6)
  2. Probe for DDR support
  3. Query DoE resolvers
- **Go-based scanner**: DoE-Hunter

Mapping RFCs to their scheduled scans within our measurement architecture



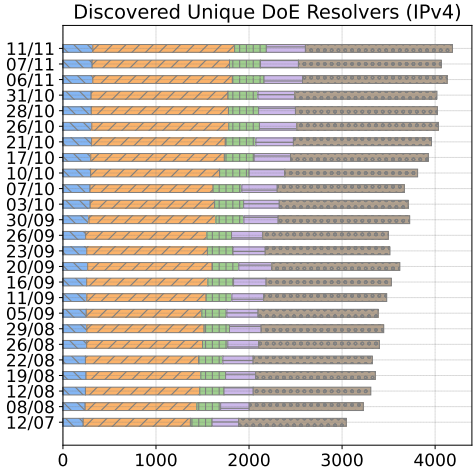
DDR Adoption Trends I

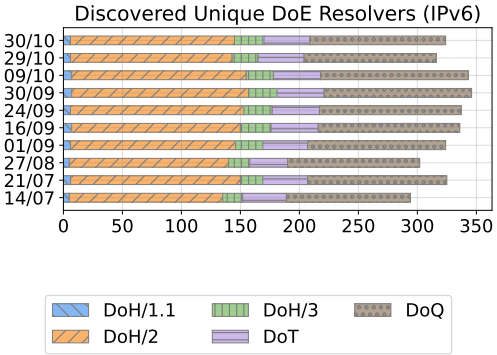
RQ1: *What are the adoption rates and trends of public DDR-enabled resolvers in IPv4 and IPv6, and how do they vary across geographical regions and network types over time?*

DDR Adoption Trends II

- 7.59% of IPv4 and 2.65% of IPv6 DNS servers support DDR.
- IPv4 adoption increased slightly; IPv6 showed proportional growth.
- Asia and Africa lead in IPv4 DDR adoption; Bolivia leads in IPv6.

DDR Adoption Trends III





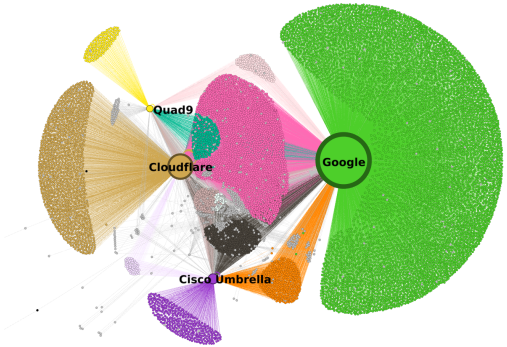
Configuration Patterns I

RQ2: *What configuration patterns are observed in DDR-enabled resolvers, and how do these patterns differ across networks and over time?*

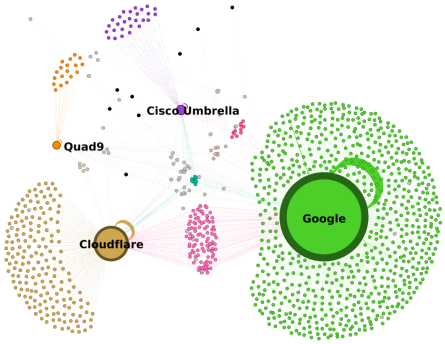
Configuration Patterns II

- Over 97% of DDR-enabled resolvers delegate to four major providers: Google, Cloudflare, Cisco, and Quad9
- Only 0.69% (IPv4) and 1.60% (IPv6) delegate within their own AS
- Privacy challenges posed by DNS centralization

Configuration Patterns III



(a) IPv4 DDR Resolver Delegation Graph



(b) IPv6 DDR Resolver Delegation Graph

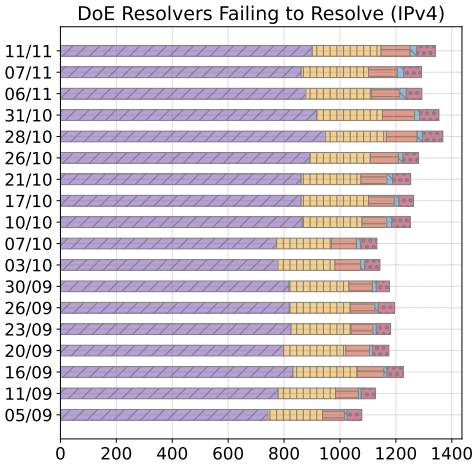
DoE Transition Challenges I

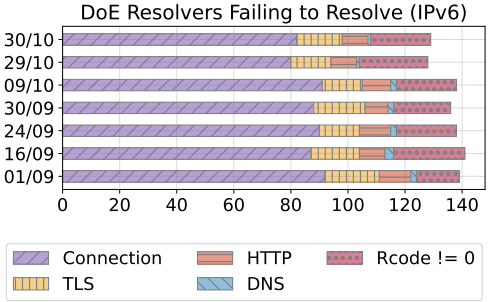
RQ3: *What observable challenges hinder clients from successfully transitioning from plain DNS to DoE protocols in real-world DDR deployments?*

DoE Transition Challenges II

- Verified discovery fails in over 99% of cases
- DoH/2 and DoQ show high error rates (38.6% and 42.2%)
- Common issues: timeouts, TLS errors, misconfigurations
- Missing IP addresses in certificate Subject Alternative Name (SAN) fields

DoE Transition Challenges III





Conclusion

- **DDR adoption is growing but uneven:**
  - IPv4: 7.6% DDR-enabled; IPv6: 2.7% (Bolivia: 98%)
- **Configuration is centralized:**
  - 97% delegate to Google, Cloudflare, Cisco, or Quad9
  - Only 0.7% (IPv4) and 1.6% (IPv6) delegate within their AS
- **Verified discovery rarely succeeds:**
  - $<$0.005% DDR-to-DoE pairs verified
  - TLS errors and timeouts dominate

Conclusion

- **DDR adoption:** Growing, but uneven (IPv4: 7.6%, IPv6: 2.7%; Bolivia: 98%)
- **Centralization:** 97% delegate to a few major providers; few within own AS
- **Verification:** $<$0.005% DDR-to-DoE pairs succeed; TLS errors/timeouts common
- **Next steps:** Improve compliance, decentralize infra, strengthen client verification

Dataset

https://zenodo.org/records/15647923

Source Code

https://zenodo.org/records/15276648

Contact: vasilis.ververis@hpi.de

Backup Slides

DNS Resolver Feature Comparison

Name	Description	DoE Support	DDR Behavior
AdGuard Home	Local DNS Proxy for Ad-Blocking	DoT and DoH support	DDR supported, designated to DoE services on the same server
BIND9	Widely used DNS software suite, including DNS resolver	DoT and DoH support	DDR can be configured
dnsmasq	Light-weight DNS resolver and proxy	Not supported	DDR is not supported, SVCB queries may be forwarded
Pi-Hole	Local DNS Proxy for Ad-Blocking	Not supported	Returns `NODATA` on DDR queries, preventing forwarding
Knot Resolver	Open-source DNS resolver	DoT and DoH support	Not supported
smartDNS	Local DNS proxy	DoT and DoH support	Not supported
unbound	Open-source DNS resolver	DoT, DoH and DoQ support	The `resolver.arpa.` zone is marked as local by default; DDR can be

DoE Resolver Analysis I

- Protocols: DoH/2, DoQ, DoT most common
- High failure rates in DoH/2 and DoQ

DoE Resolver Analysis II

Protocol	# Req.	# Errors	*Connection*	*TLS*	*HTTP*	*DNS*	*RCODE != 0*
DoH/1.1	6055	70 (1.16 %)	15 (21.43 %)	1 (1.43 %)	1 (1.43 %)	-	53 (75.71 %)
DoH/2	27 758	10 713 (38.59 %)	6052 (56.49 %)	2187 (20.41 %)	1638 (15.29 %)	300 (2.80 %)	536 (5.00 %)
DoH/3	6606	317 (4.80 %)	126 (39.75 %)	30 (9.46 %)	107 (33.75 %)	1 (0.32 %)	53 (16.72 %)
DoQ	27 074	11 433 (42.23 %)	9204 (80.50 %)	1857 (16.24 %)	-	-	372 (3.25 %)
DoT	7806	545 (6.98 %)	360 (66.06 %)	-	-	-	185 (33.94 %)

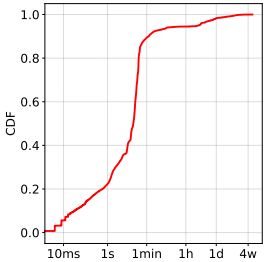
Percentages: show each category's share of total errors

Traffic Shadowing

- Repeated queries from unexpected sources
- Replay behavior observed across global ASes

Traffic Shadowing

- Repeated queries from unexpected sources
- Replay behavior observed across global ASes



CDF considers all replayed DNS queries and their time difference between the first and the last replayed query.