Towards Operational and Security Best Practices for DNS in the Internet of Things.

Andrew Losty Anna Maria Mandalari Abhishek Mishra Mathieu Cunche

Paper accepted by Internet Research Task Force (IRTF) – for presentation at IETF123 Madrid (July 2025)

Motivation 1

Evaluate the Security, Operational behavior of DNS in IoT devices.

Security:

- DoH, DoT, DNSSEC,
- Port & Transaction ID Randomization
- DNS Extensions

Regulatory Framework:

- Identify existing guidance

Behaviour:

- Device identifiability via traffic request patterns.
- TTL adherence, caching strategies and exponential back-off
- Hardcoded DNS servers
- IPv6 support, MDNS operation.

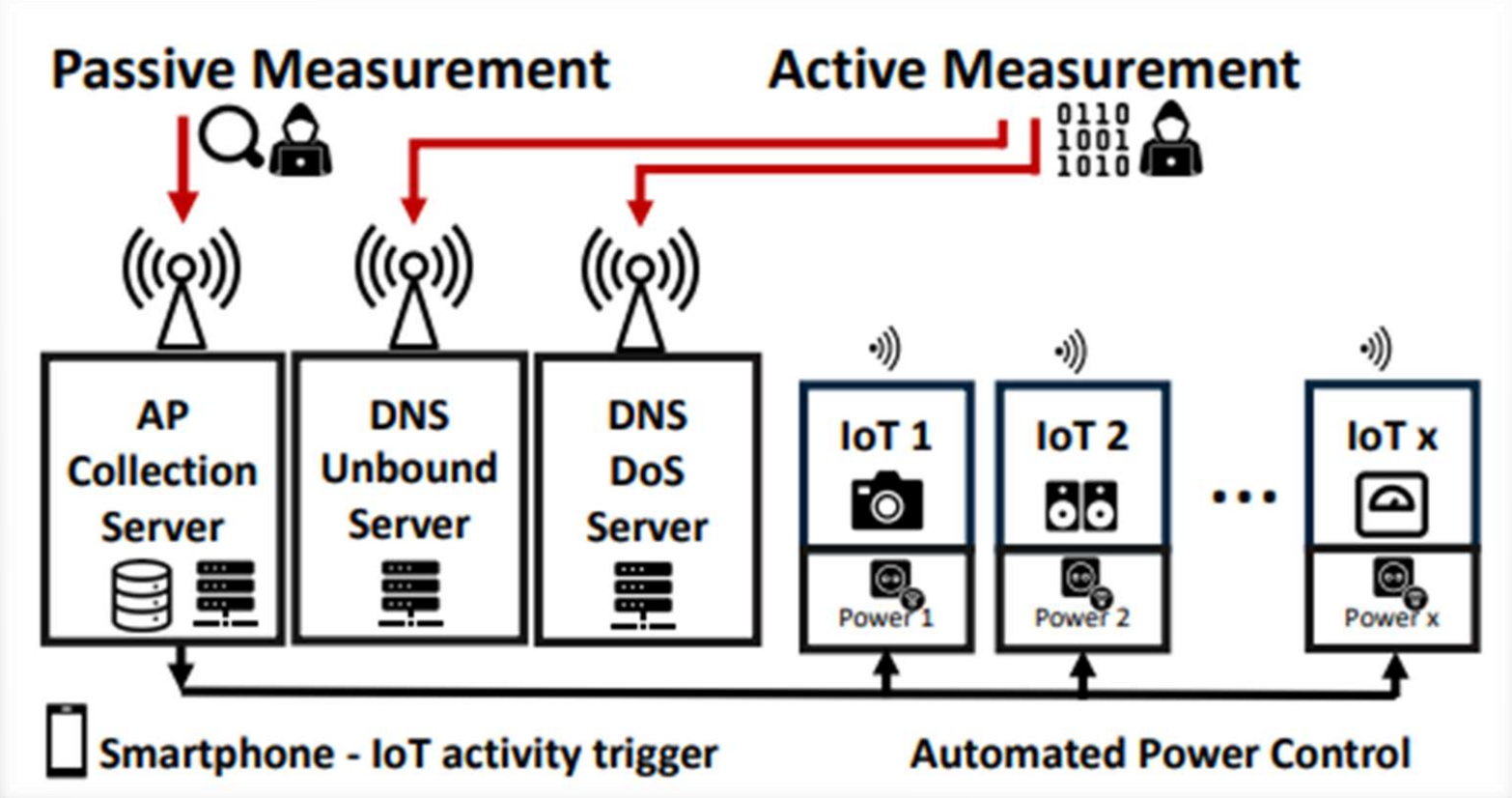
Statista reports a projected doubling of IoT devices from 19.8 billion in 2025 to over 40.6 billion by 2034.

Motivation 2

European Telecommunications Standards Institute (ETSI)			
ETSI EN 303 645	✗ DNS∩IoT ✓ DNS	ETSI TS 103 375	✗ DNS∩IoT ✗ DNS
ETSI EN 103 645	✗ DNS∩IoT ✓ DNS	ETSI TS 103 701	✗ DNS∩IoT ✓ DNS
ETSI TR 103 621	✗ DNS∩IoT ✗ DNS	ETSI TS 103 457	✗ DNS∩IoT ✗ DNS
ETSI GR IP6 008	✗ DNS∩IoT ✗ DNS		
National Institute of Standards and Technology (NIST)			
NIST SP 800-53 Rev.5	✗ DNS∩IoT ✓ DNS	NIST SP 800-53A Rev.5	✗ DNS∩IoT ✓ DNS
NIST SP 800-53B	✗ DNS∩IoT ✗ DNS	IoT NIST IR 8259	✗ DNS∩IoT ✗ DNS
NIST Cybersecurity Framework (CSF) 2.0	✗ DNS∩IoT ✗ DNS	NIST IR 8425	✗ DNS∩IoT ✗ DNS
NIST IR 8425A	✗ DNS∩IoT ✗ DNS	NIST SP800-81r3	✗ DNS∩IoT ✗ DNS
European Union Agency for Cybersecurity (ENISA)			
Good Practices for Security of IoT	✗ DNS∩IoT ✗ DNS	Guidelines for Securing the IoT	✗ DNS∩IoT ✗ DNS
Baseline Security Recommendations for IoT	✗ DNS∩IoT ✓ DNS		
European Commission			
Cyber Resilience Act (CRA)	✗ DNS∩IoT ✗ DNS		
ISO/IEC			
ISO/IEC 30141:2024	✗ DNS∩IoT ✗ DNS	ISO/IEC 21823-2:2020	✗ DNS∩IoT ✗ DNS
ISO/IEC 27001:2023+A1:2024	✗ DNS∩IoT ✗ DNS	ISO/IEC 27002:2022	✗ DNS∩IoT ✓ DNS
ISO/IEC DIS 27404:2024	✗ DNS∩IoT ✗ DNS	ISO/IEC TS 30149:2024	✗ DNS∩IoT ✗ DNS
ISO/IEC 30161-2:2023	✗ DNS∩IoT ✗ DNS	ISO/IEC TR 30164:2020	✗ DNS∩IoT ✗ DNS
ISO/IEC 29192-8:2022	✗ DNS∩IoT ✗ DNS		
ITU-T			
ITU-T Y.4806	✗ DNS∩IoT ✗ DNS	ITU-T Y.4807	✗ DNS∩IoT ✗ DNS
ITU-T Y.4808	✗ DNS∩IoT ✗ DNS	ITU-T Y.4809	✗ DNS∩IoT ✗ DNS
ITU-T Y.4810	✗ DNS∩IoT ✗ DNS	ITU-T Y.4811	✗ DNS∩IoT ✗ DNS
Internet Engineering Task Force (IETF) DNS RFCs			
RFC 1034	✗ DNS∩IoT ✓ DNS	RFC 1035	✗ DNS∩IoT ✓ DNS
RFC 8484	✗ DNS∩IoT ✓ DNS	RFC 7858	✗ DNS∩IoT ✓ DNS
Institute of Electrical and Electronics Engineers (IEEE)			
IEEE 2413-2019	✗ DNS∩IoT ✗ DNS		

Evaluate existing Regulatory Framework

Test environment



30+ Consumer IoT devices categorized as: Cameras, Doorbells, Smart Plugs, Hubs, Speakers, Sensors, Lights, Appliances, Health, and Pet Care.

DNS Unbound Server: (Active experiments Crafted DNS responses, TTL, RR)

DNS DoS Server: (Active experiments DNS Amplification and RR duplication)

Collection Server: (Passive Data collection)

DNS RFCs

Fundamentals

RFC 1034 – DNS Concepts
RFC 1035 – DNS Implementation
RFC 2181 – Specification Clarifications
RFC 2308 – Negative Caching
RFC 2671 – EDNS(0)
RFC 6891 – EDNS(0) Update
RFC 3596 – IPv6 AAAA Records
RFC 8499 – DNS Terminology

Operational

RFC 1912 – Config Best Practices
RFC 1033 – DNS Admin Guide
RFC 9210 – DNS over TCP
RFC 7766 – TCP Best Practices
RFC 7871 – Client Subnet (ECS)
RFC 8767 – Serve Stale Data
RFC 8906 – DNS Terminology Updates

Security (DNSSEC)

RFC 4033 – DNSSEC Overview
RFC 4034 – DNSSEC Records
RFC 4035 – Protocol Changes
RFC 5155 – NSEC3
RFC 5452 – TXID Randomization
RFC 8624 – Algorithm Requirements
RFC 5011 – Trust Anchor Rollover
RFC 4032 – Deployment Roadmap

Encrypted Transport

RFC 7858 – DNS over TLS
RFC 8484 – DNS over HTTPS
RFC 9250 – DNS over QUIC

rfc-editor.org - title/ keyword identifies 345 current – retired DNS RFCs

Lack of Secure Protocols

Spoofing / Cache Poisoning Protection (Client)
- RFC 5452 – Port & TXID Randomization

✅ DNSSEC: Authenticated Responses (Resolver)
- RFC 2671 – EDNS0 Extension
- RFC 6891 – EDNS0 Update (enables DNSSEC)
- RFC 4033 – DNSSEC Overview
- RFC 4034 – Security Records (DNSKEY, RRSIG)
- RFC 4035 – Protocol Changes
- RFC 8624 – Algorithm Guidance

Encrypted DNS Transport (Client)
- RFC 7858 – DNS over TLS (DoT) (853)
- RFC 8484 – DNS over HTTPS (DoH) (443)
- RFC 9250 – DNS over QUIC (DoQ)

None of the 30 IoT devices evaluated supported Secure DNS protocols or EDNS(0).

Extension mechanism for DNS - EDNS(0)

Observed Issue

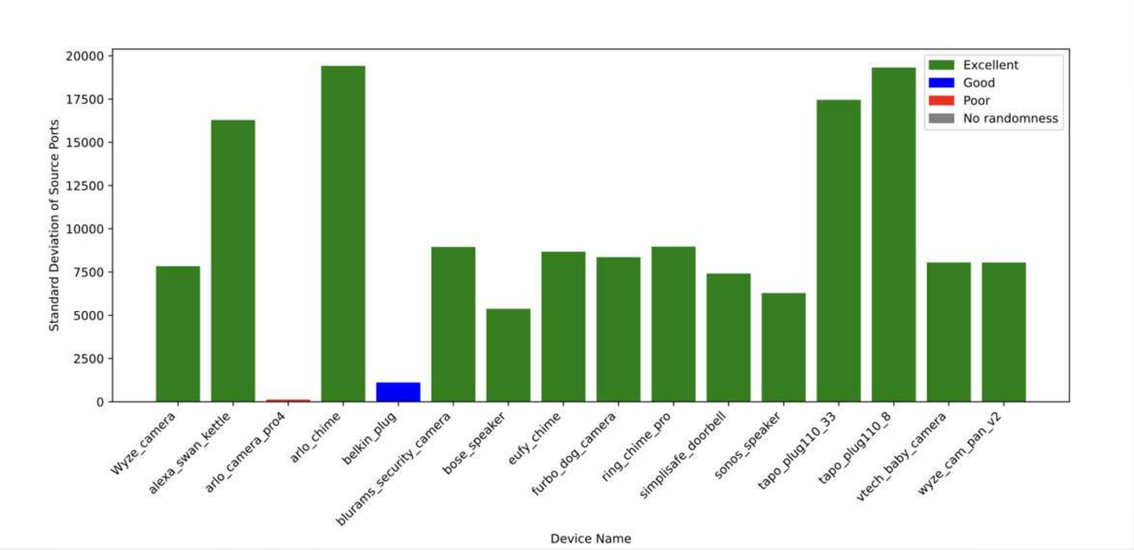
- **Non of the IoT devices support EDNS(0).**
- **Failure to support DNS UDP payloads >512B**

Security Risks / Operational behavior

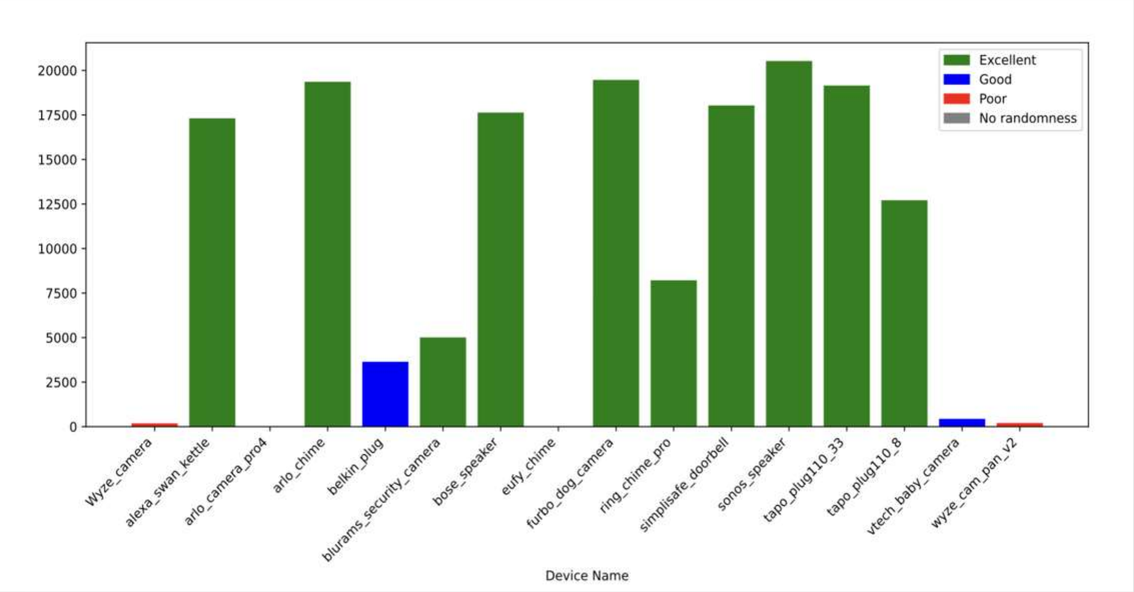
- **Possible evasion +mishandling of fragments by security devices**
- **DNS amplification** via fragmented responses (RFC 8195) (DNS Privacy Considerations)
- **Devices fail to switch to TCP for large payloads**.

IoT Device fragment at the IP layer rather than using TCP

Source Port + Transaction-ID



Source-Port Randomization



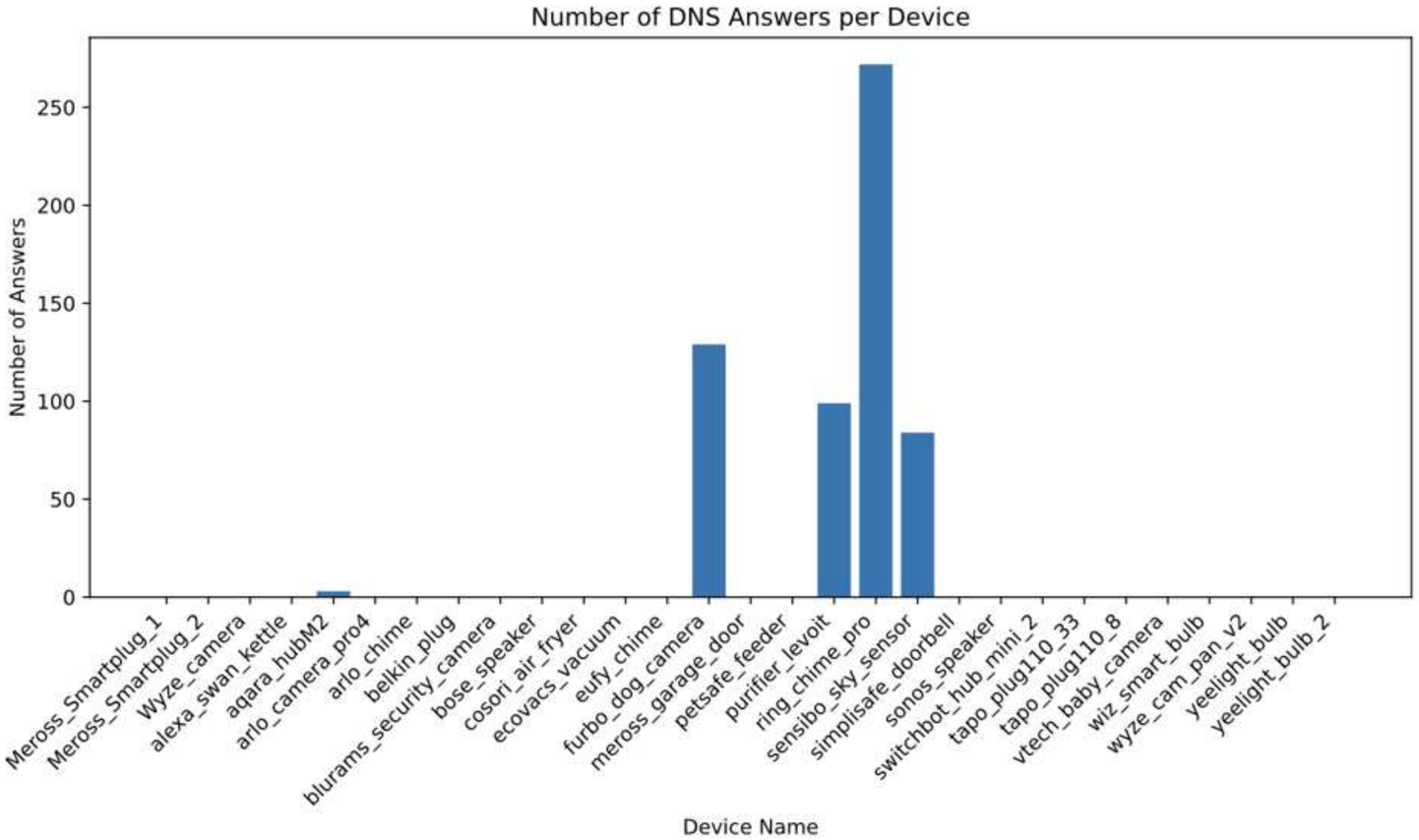
Transaction ID Randomization

Observed Issue

Devices fail to randomize Source-Ports/Transaction IDs as defined, RFC 5452 (2009)

Devices susceptible to Cache Poisoning

DNS – Hardcoded Server Addresses



Use of Hard-coded DNS servers

Observed Issue

Devices ignore DHCP - use hard-coded DNS.

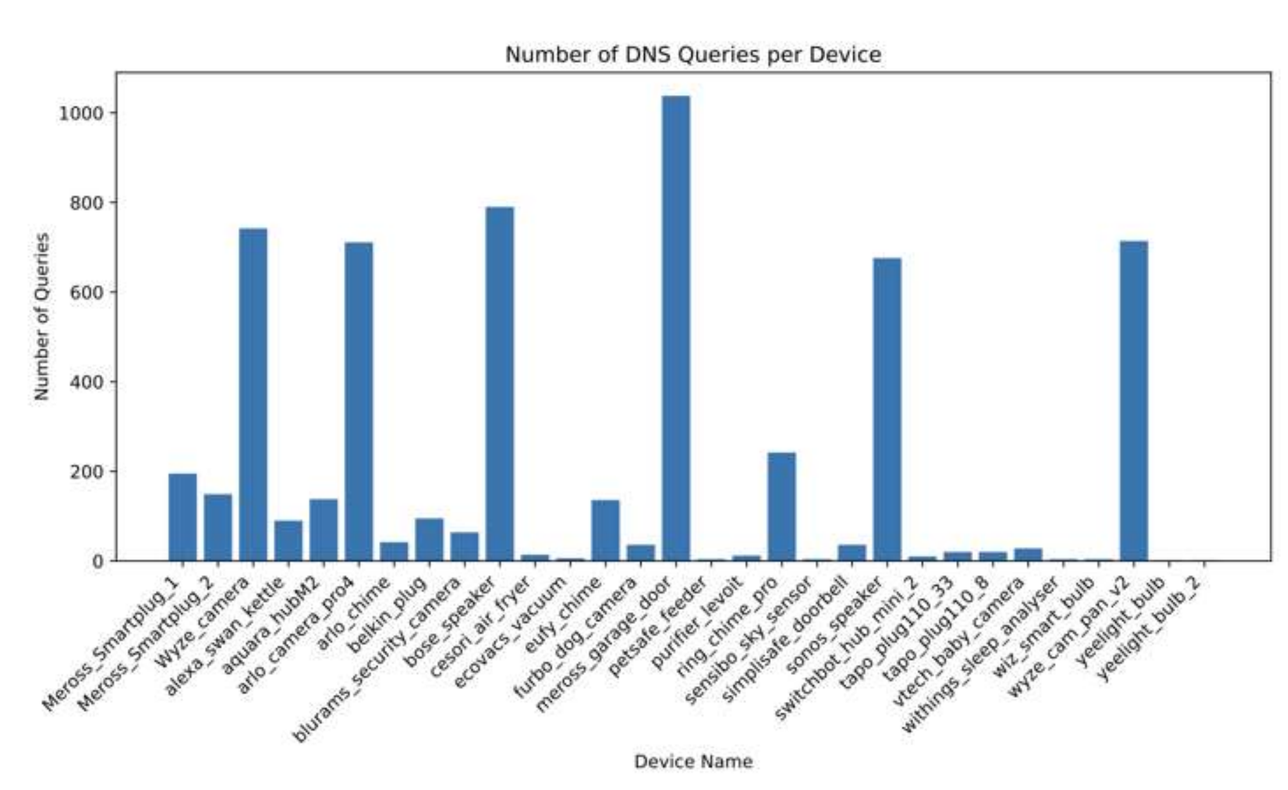
Devices Bypass inspection

Breach of policy

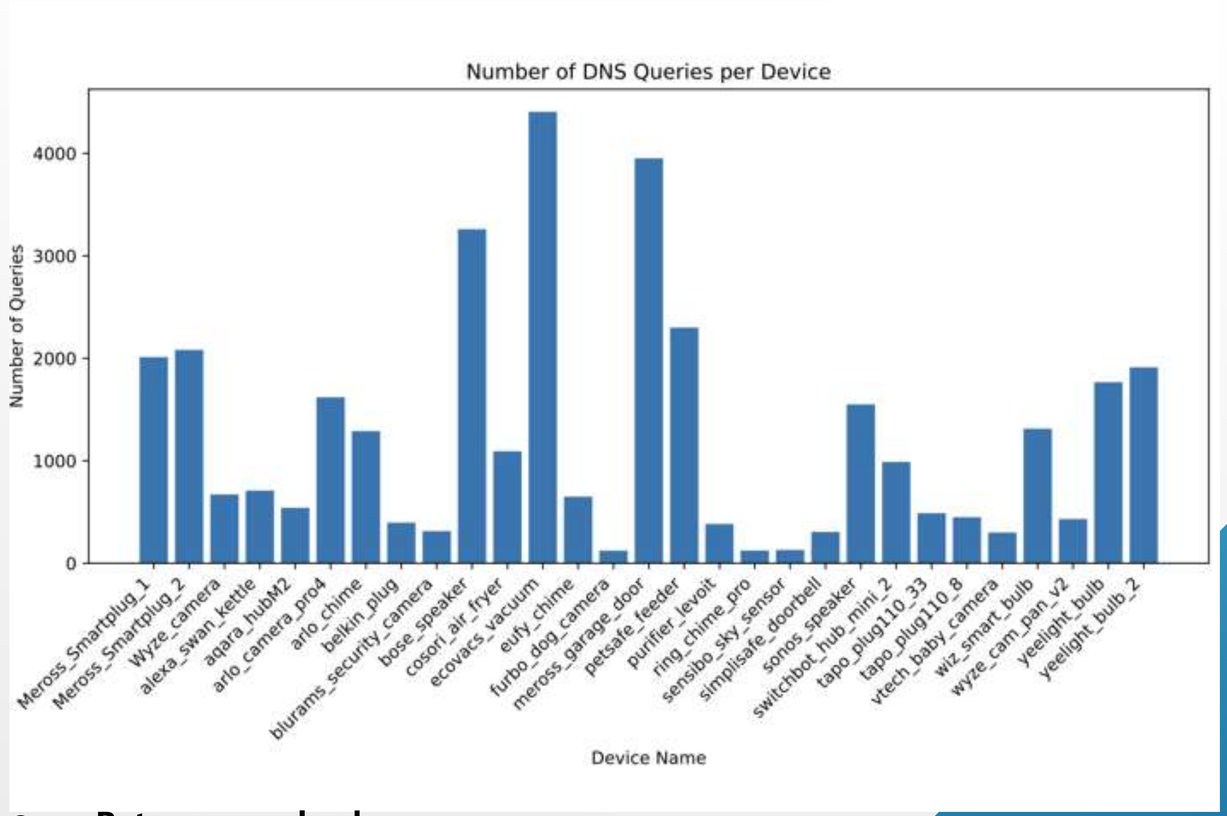
Reduction in resilience

Data leak - 3rd parties

DNS – High Retry Rate



Query rate



Query Rate - unresolved

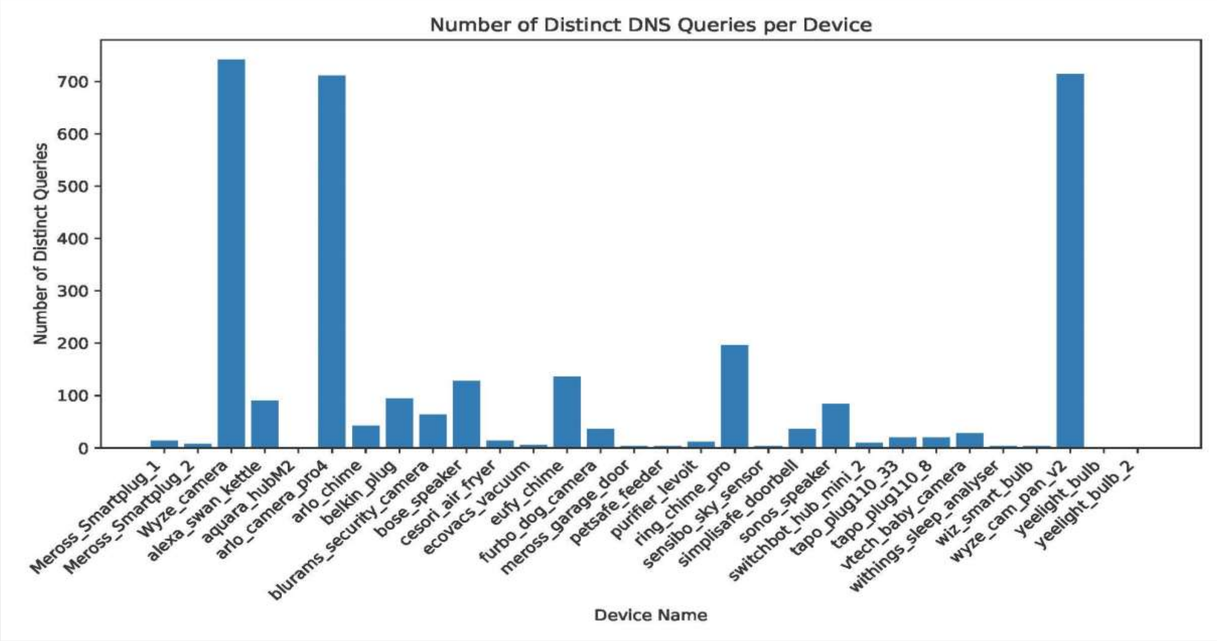
Observed Issue

10-fold increase in DNS Queries , increased load on infrastructure.

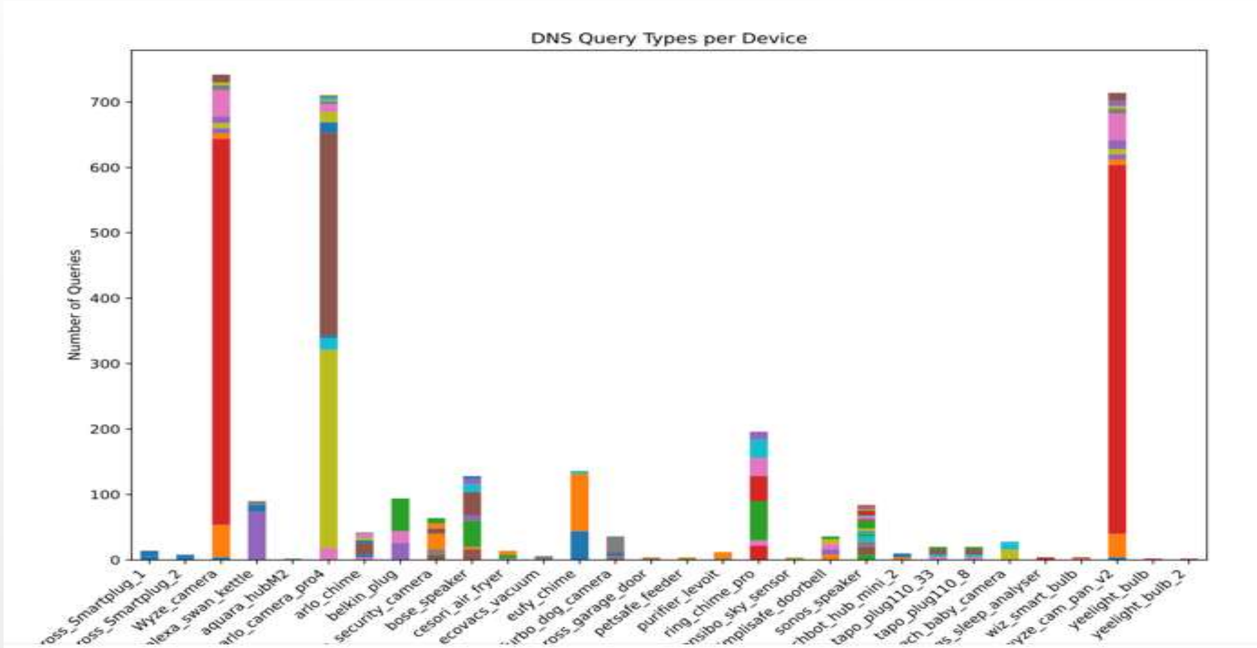
Lack of **exponential backoff mechanism** with **jitter/random delay**

DNS **retry storm**. (RFC 1035/1536)

DNS – High Number Sites contacted



Unique destinations

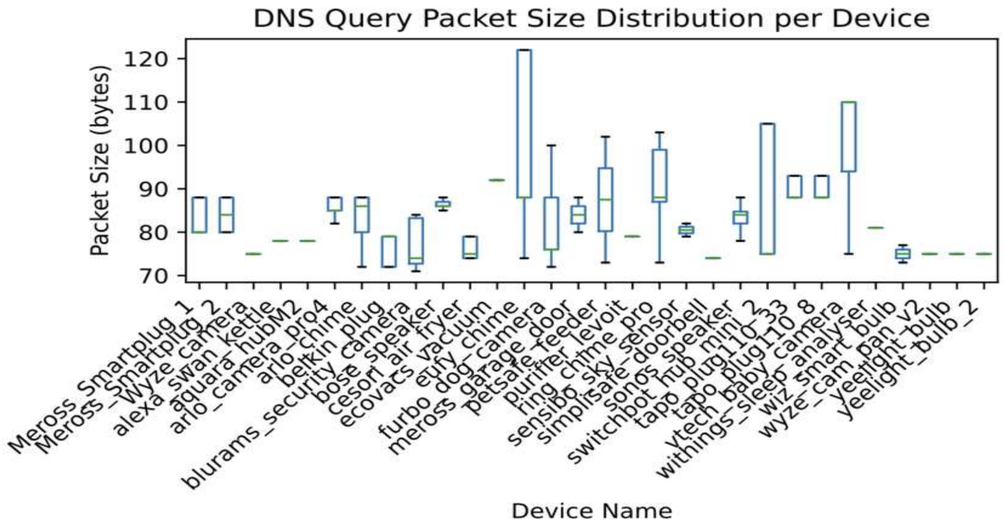


Unique destinations frequency

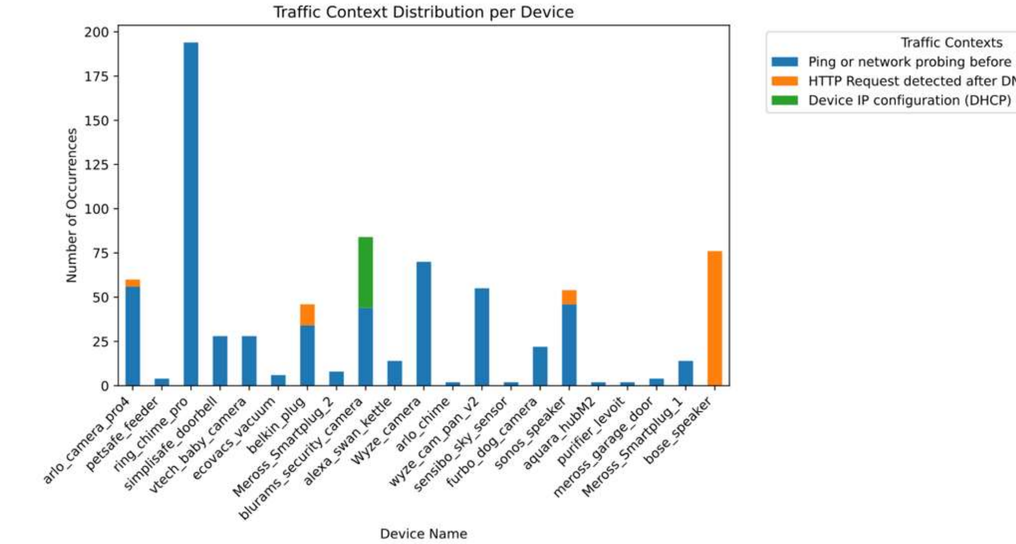
Observed Issue

High number of destinations for operational connections.
Difficult to monitor, **filter, control**, **more complex firewall rules**.

DNS – Device Identification



Query packet size



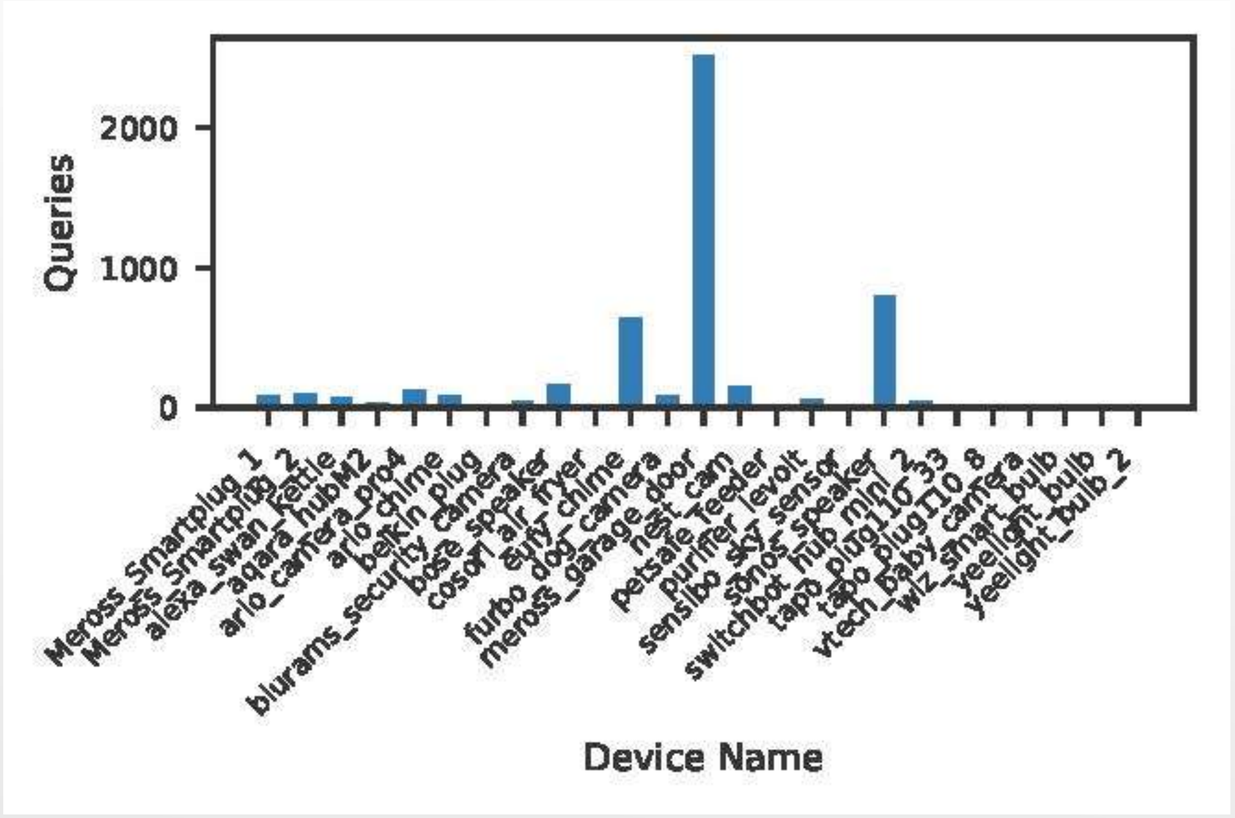
Precursor actions to query

Observed Issue

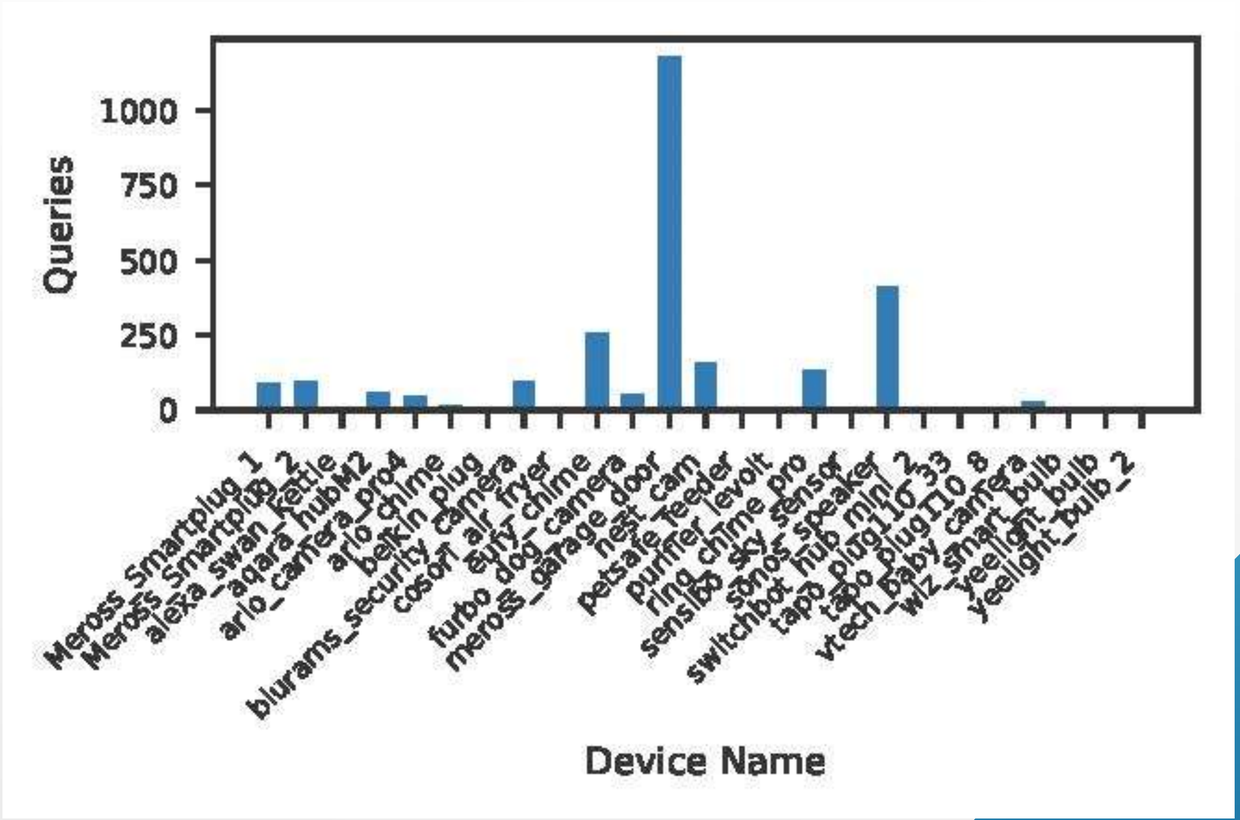
Highly “fingerprintable” DNS requests with precursor actions by device.

Device and model identification possible: smart locks, cameras, Correlate patterns , Track the device or user over time

DNS IoT – TTL



TTL = 0



TTL = 1000000000 (11574 days)

Observed Issue

Many devices disregard TTLs, relying on hardcoded query intervals.
While TTL manipulation has little effect, zero TTLs can induce query amplification in some cases.

DNS IoT – RR Injection

Active experiment to evaluate resilience to Inject RR values by altering domain/IP values

Response = A Record **IP 192.0.2.1** (non routable reserved IP address)

Response = AAAA Record **IP 2001:db8:1** (non routable reserved IP address)

Response = CNAME Record **example.com** (reserved domain name)

Observed Issue

Multiple **devices accept manipulated responses** – with **reserved non-routable content**.
No validation of IPs and domains - Devices vulnerable to **manipulation and redirection**.

DNS IoT – Amplification and Multi-RR Response

Active experiment to evaluate effect on IoT devices subject to DNS amplification attacks, amplification ratios of 10, 50, and 100 relative to their original queries.

Observed Issue

Good resilience with only 1 device (Qardiobase Scale) experienced a loss of wireless connectivity at highest amplification.

Active experiment to subject IoT devices subject to "oversize" payloads by increasing the number of A records in each DNS response. Replication ratios of 10, 50, and 100, exceed >512-byte limit.

Observed Issue

7 device (23%) suffered a loss of connectivity as they maintain UDP transport and fragment at the IP layer, rather than setting the TC (truncation) flag and transition to TCP.

Findings Overview

(Results to be used to develop IETF RFC - DNS best practices for IoT)

Device	Secure Standards	Source Port	Transaction ID	Query	Modified RR	Forged TTL	DoS
Arlo Camera Pro	✗	✗	✓	✗	✗	✓	✗
Blurams Security Camera	✗	✓	✓	✓	✓	✓	✗
Furbo 360 Dog Camera	✗	✓	✓	✓	✓	✓	✓
Google Nest Cam (Wired)	✗	✓	✓	✓	✓	✓	✓
Vtech baby camera	✗	✓	✓	✓	✓	✓	✓
Wyze Cam Pan v3	✗	✓	✗	✗	✓	✓	✓
Wyze camera	✗	✓	✗	✗	✓	✓	✓
Yi Home Camera	✗	✓	✓	✓	✓	✓	✓
Qardiobase scale	✗	✓	✓	✓	✓	✓	✗
Withings sleep analyser	✗	✓	✓	✓	✓	✓	✓
Aqara Hub M2	✗	✓	✓	✓	✓	✓	✓
Cosori Airfrier CS158	✗	✗	✓	✓	✗	✓	✗
Ecovacs vacuum Deepbot	✗	✓	✓	✓	✓	✓	✓
LeVoit Air Purifier Classic	✗	✓	✓	✓	✓	✓	✓
Meross Door Opener	✗	✓	✓	✓	✓	✗	✓
Petsafe Automatic Feeder	✗	✓	✓	✓	✓	✓	✗
Sensibo Sky	✗	✓	✓	✓	✓	✓	✓
Swan Alexa Kettle	✗	✓	✓	✓	✓	✓	✗
Switchbot hub mini 2	✗	✓	✓	✓	✓	✓	✓
Wiz Smart Bulb A.E27	✗	✓	✓	✓	✓	✓	✓
Yeelight smart led bulb 1+2	✗	✓	✓	✓	✗	✓	✗
Tapo Smartplug P110 (8+33)	✗	✓	✓	✓	✓	✓	✓
Belkin Plug	✗	✓	✓	✗	✓	✓	✗
Meross Smartplug 1 +2	✗	✓	✓	✓	✗	✓	✓
Sonos One Speaker	✗	✓	✓	✓	✗	✗	✓
Bose Home Speaker 500	✗	✓	✓	✓	✓	✓	✓
Arlo Chime Doorbell	✗	✓	✓	✓	✗	✓	✓
Eufy Chime	✗	✗	✗	✗	✓	✗	✓
Ring Chime Pro TV	✗	✓	✓	✗	✓	✓	✓
Ring Doorbell	✗	✓	✓	✓	✓	✓	✓
Simplisafe Doorbell	✗	✓	✓	✓	✓	✓	✓

Contact / Information

SafeNetIoT
SECURING THE IOT

Follow us:
https://safenetiot.github.io/
https://www.youtube.com/watch?v=0fg0acuRbUA

UCL-IoT DNS Experiments and Results
https://github.com/SafeNetIoT/DNS_priv_sec/tree/main/UCL-IoT

Contact:
andrew.losty.23@ucl.ac.uk