From Lookup to Lockdown: DNS Guidelines for Securing IoT Ecosystems

Andrew Losty, Abhishek K. Mishra, Mathieu Cunche, and Anna Maria Mandalari

***Abstract*—The Domain Name System (DNS) serves as a fundamental component of Internet infrastructure; however, its frequently overlooked role in consumer Internet of Things (IoT) ecosystems exposes significant security vulnerabilities and operational challenges. This paper analyzes DNS behavior in consumer IoT devices and reveals widespread inconsistencies that undermine operational efficiency, resilience, and security. We construct a representative testbed spanning a heterogeneous set of IoT devices and employ both passive traffic monitoring and active experimentation to identify vulnerabilities, including cache poisoning, predictable transaction IDs, non-randomized source ports, and limited adoption of secure DNS protocols such as DNS-over-HTTPS (DoH), DNS-over-TLS (DoT), and Domain Name System Security Extensions (DNSSEC). We observe erratic operational patterns, such as excessive querying, poor adherence to TTL values, and overreliance on hard-coded resolvers, that amplify exposure to fingerprinting and denial-of-service attacks. Our findings demonstrate a concerning lack of standardized DNS practices across the IoT ecosystem. We conclude by proposing actionable guidelines to harden DNS handling in IoT devices and improve security, interoperability, and network stability as the consumer IoT landscape continues to expand.**

***Index Terms*—DNS, IoT, DoH, DoT, DNSSEC, security, privacy, vulnerability, attack.**

I. Introduction

The Domain Name System (DNS) [1], [2] is a foundational Internet protocol that translates human-readable domain names into IP addresses. Although DNS is mature and well-defined in general computing, its behavior in consumer Internet of Things (IoT) environments remains inconsistent and largely unregulated. This gap raises serious concerns regarding operational reliability [3], [4], security [5], [6] and privacy [7], [8] in IoT networks comprising billions of devices that often communicate autonomously.

DNS has long been recognized as a vector for attacks such as spoofing and cache poisoning [6], [9], where adversaries inject malicious records to redirect legitimate queries to attacker-controlled servers. In IoT, this threat can be exploited during firmware updates or configuration retrieval, potentially causing unauthorized code execution, botnet enrollment, or device bricking through redirection to non-existent IPs.

DNS also poses significant privacy risks. Queries often contain sensitive metadata, such as destination domains and timestamps, allowing passive observers to infer user behavior and device activity patterns, enabling fingerprinting and traffic analysis even with padded DNS encryption [7]. Although DNS-over-HTTPS (DoH) [10] and DNS-over-TLS (DoT) [11] provide encryption, they do not prevent side-channel leakage, as adversaries can infer sensitive information from traffic characteristics, timing, and destination metadata [12].

DNS Security Extensions (DNSSEC) [13] protect against cache poisoning via cryptographic authentication. However, no IoT devices in our study support DNSSEC, and only 30% of resolvers perform DNSSEC validation [14].

Limited adoption of DoH, DoT, and DNSSEC in IoT stems from multiple challenges. Constrained device resources, particularly limited processing power and memory, restrict support for encryption-based DNS mechanisms [15]. Lightweight OSes such as TinyOS [16] and RIOT OS [17] often lack native HTTPS or TLS libraries [18], and the higher energy cost of secure protocols further limits adoption for battery-powered devices [19]. DNS over Constrained Application Protocol (CoAP) [20] has been proposed to address these constraints; however, its use is not evaluated in this study, as it remains a draft standard [21]. Network visibility and deployment trade-offs further complicate protocol selection: DoH conceals DNS traffic within HTTPS flows on port 443, complicating detection and control, whereas DoT's use of port 853 makes it identifiable and blockable. Economic pressures and the absence of regulatory mandates also lead manufacturers to prioritize cost and functionality over security, resulting in widespread reliance on insecure DNS configurations.

Many IoT devices use hard-coded resolvers [22], ignore Time-To-Live (TTL) directives [23], and adopt retry mechanisms that do not conform to protocol specifications. These misconfigurations degrade performance and efficiency while increasing security and privacy risks. Moreover, the lack of regular and sustained firmware updates [24] often exacerbates these threats.

Motivated by these challenges, we conduct an empirical study analyzing IoT device DNS interactions. We focus exclusively on commercial consumer IoT devices such as smart plugs, cameras, and smart speakers. We do not consider medical or industrial IoT systems, which operate under different regulatory, security, and operational constraints.

Utilizing a controlled testbed and hundreds of automated experiments, we systematically characterize DNS behavior under realistic network conditions across 35 IoT devices, examining query frequency, TTL compliance, resolver configuration, and adoption of security features such as DoH, DoT, and DNSSEC. Our analysis reveals a range of vulnerabilities,

Andrew Losty and Anna Maria Mandalari are with University College London, United Kingdom (email: {andrew.losty.23, a.mandalari}@ucl.ac.uk).

Abhishek K. Mishra and Mathieu Cunche are with INSA-Lyon, Inria, Univ. of Lyon, CITI Lab, France (email: {abhishek.mishra, mathieu.cunche}@inria.fr).

including predictable transaction IDs, non-randomized source ports, and lack of support for Extension Mechanisms for DNS (EDNS(0)–based padding [25], [26], all of which expose devices to spoofing and traffic analysis attacks.

This study underscores the critical need for standardized DNS handling procedures to enhance the security, privacy, and operational consistency of IoT deployments. To this end, we synthesize our empirical findings into a set of targeted recommendations for IoT device behavior. To the best of our knowledge, this represents the first consolidated effort in the literature to formalize DNS-related best current practices for IoT, with the long-term goal of informing real-world adoption through regulatory and standardization bodies.

This paper makes the following contributions:

- We develop an automated and reproducible testbed that emulates realistic IoT environments and captures DNS behavior across a heterogeneous set of commercial IoT devices.
- We identify and categorize operational anomalies, including repeated queries, TTL violations, and hardcoded resolvers, that reflect non-compliance with DNS best practices.
- We assess the security posture of IoT DNS stacks and demonstrate common vulnerabilities such as non-randomized source ports, predictable transaction IDs, and minimal padding support.
- We evaluate the adoption of secure DNS mechanisms (DoH, DoT, DNSSEC) and analyze the technical and practical barriers to their deployment in constrained IoT environments.
- We provide targeted recommendations and design guidelines to improve the security, privacy, and robustness of DNS behavior in IoT systems.
- We release a curated dataset of DNS traffic and an open-source analysis toolkit to promote reproducibility and enable further research: https://github.com/SafeNetIoT/iot_dns.

This study has led to the development of an active Internet-Draft within the IETF [27], aiming to formalize DNS security and privacy guidelines for IoT deployments, highlighting the broader relevance of our findings.

The remainder of this paper is organized as follows. Section II introduces the threat model, including passive and active adversaries. Section III describes the experimental testbed and the methodology for dataset collection. Section IV outlines our approach for deriving DNS guidelines for IoT systems based on experimental findings. Section V presents the results, highlighting compliance issues, security weaknesses, and operational inefficiencies. Section VI discusses implementation considerations and long-term perspectives. Section VII reviews related work, and Section VIII concludes the paper with key findings and recommendations.

II. Threat Model

IoT ecosystems rely heavily on DNS for service discovery, connectivity, and cloud integration. However, DNS behavior in consumer devices remains highly heterogeneous and often deviates from protocol specifications, making DNS a significant vector for security and privacy compromise. In this section, we briefly outline the problem statement before defining the adversarial capabilities considered in the paper.

Problem Statement. Consumer IoT devices frequently implement DNS in insecure and non-compliant ways, creating a critical attack surface that undermines security, privacy, and availability. The absence of secure DNS mechanisms (DoH, DoT, DNSSEC), predictable protocol parameters, and weak adherence to caching and EDNS(0) semantics collectively enable cache poisoning, spoofing, traffic manipulation, and denial-of-service attacks. These weaknesses, exacerbated by IoT-specific resource constraints and inconsistent vendor practices, remain insufficiently addressed despite DNS's central role in IoT communication.

Threat Model. Our threat model focuses on how adversaries exploit DNS behavior across five domains: DNS manipulation, denial-of-service (DoS), IoT-specific design flaws, insecure communication channels, and metadata leakage through side channels.

DNS manipulation attacks target weaknesses in how devices generate, parse, or validate DNS messages. These include predictable identifiers, insufficient randomness in source ports, and inconsistent caching behavior. Such deficiencies enable spoofing or cache poisoning that redirects traffic to attacker-controlled endpoints. DoS attacks use amplification or malformed queries to deplete bandwidth, CPU, or memory resources on resolvers or IoT devices.

IoT-specific design flaws arise from constrained firmware architectures and limited protocol support. Devices may rely on fixed DNS resolvers, implement simplified DNS stacks, or follow non-standard retry and timeout behaviors, creating observable patterns that adversaries can exploit. Insecure communication channels, such as plaintext or unauthenticated DNS, allow on-path attackers to manipulate or inject responses. Metadata leakage through side-channel and timing attacks exploits observable DNS characteristics, including packet size, timing, and query frequency, enabling adversaries to infer sensitive information about device functionality or user activity [7].

Passive Adversary. The adversary operates on the same local network as the IoT devices (e.g., a compromised wireless network, gateway, or DNS resolver) and passively observes DNS traffic in transit. Although unable to modify or inject packets, the adversary leverages query timing, frequency, and structure to extract device-level intelligence. By correlating DNS patterns with known behaviors, the adversary infers device types, manufacturers, and operational routines [28]. Even when application-layer traffic is encrypted, DNS metadata remains a significant source of information leakage [7].

Active Adversary. A stronger adversary manipulates DNS traffic to influence resolution outcomes, including cache poisoning attacks that inject forged responses into resolver caches to redirect devices to malicious servers. Such an attacker may operate internally (via a compromised device) or externally by targeting vulnerable local resolvers, such as consumer-grade home routers. These attacks exploit predictable DNS

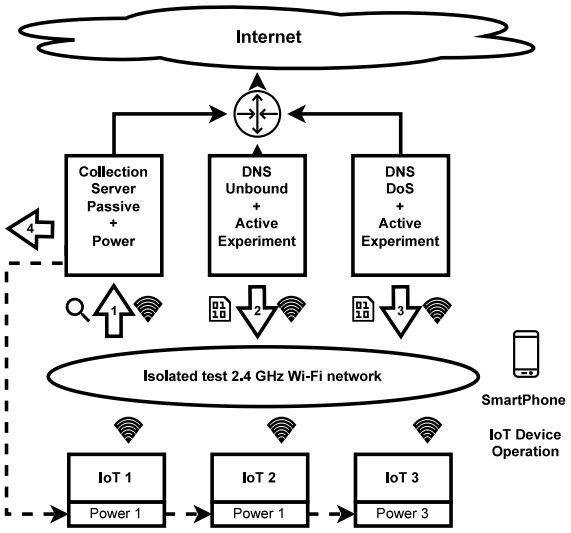


Fig. 1: Testbed and experimental framework

parameters, including transaction IDs and source ports, and prove particularly effective in the absence of secure DNS transports. Active adversaries may alter TTL values, inject bogus resource records, or replay prior responses. While our model does not assume compromise of the public DNS infrastructure, many consumer resolvers remain vulnerable due to weak configurations, outdated firmware, default credentials, and insufficient monitoring [29].

III. Testbed and Dataset

Prior datasets: Prior IoT datasets have substantially expanded real-device coverage and attack realism but have not explicitly targeted DNS as a security-critical protocol layer. Ren *et al.* measured traffic from 81 heterogeneous consumer IoT devices to characterize information exposure and communication behaviors, treating DNS only as part of aggregate network flows [30]. IoT Sentinel leveraged passive traces from diverse IoT devices for behavioral fingerprinting and network enforcement, without analyzing protocol-level weaknesses such as resolver dependence or transaction predictability [31]. Large-scale security benchmarks such as CICIoT2023 scaled realism to over 105 real IoT devices and numerous attack classes, yet focused primarily on volumetric and exploit-driven threats rather than DNS manipulation or secure DNS mechanisms [32]. Flow-based smart home datasets such as UNSW HomeNet further increased device diversity but abstracted away protocol semantics [33], while earlier intrusion datasets like UNSW-NB15 emphasized general network attacks in synthetic environments [34]. In contrast, our dataset aims to uniquely combine heterogeneous real consumer IoT devices with fine-grained passive DNS capture and active adversarial DNS experimentation, enabling systematic analysis of operational inconsistencies, protocol vulnerabilities, and security hardening opportunities in real IoT DNS ecosystems.

Testbed and dataset: We develop a dedicated testbed that employs two adversarial models and combines passive DNS traffic monitoring with active DNS manipulation experiments across a range of consumer IoT devices. As shown in Fig. 1, the testbed includes a dedicated secure IEEE 802.11b/g/n 2.4 GHz wireless network, dedicated external NAT router providing Internet connection, along with the following numbered components: (1) a collection server (passive) that performs continuous and per-experiment packet captures of local and IoT traffic, including source ports, DNS transaction identifiers, and TTL values; (2) a DNS Unbound resolver (active) [35], which conducts DNS manipulation experiments such as crafted response injection, resource record (RR) modification, TTL manipulation, and DNS-over-HTTPS (DoH) operation (see Section IV); (3) a dedicated denial-of-service (DoS) server (active) that generates amplified DNS responses via resource record (RR) duplication and high-rate query injection; and (4) an automated power control system that ensures consistent packet capture across experiments, while smartphones trigger specific IoT device activities in targeted scenarios, following the methodology in [36].

We select thirty-five consumer IoT devices to represent categories characteristic of a real-world smart home environment. The devices span a range of cost, complexity, functionality, and power sources, including both battery and mains-powered devices. The commercial IoT device categories include Home Automation and Appliances (16), Cameras (6), Health (1), Smart Plugs (3), Smart Speakers (5), and Hub/Doorbell with Chimes (4). Table I shows the selected devices.

In addition to device diversity, Table V (Appendix A) summarizes the collected passive and active DNS datasets per device, including firmware versions and traffic volumes, highlighting the scale and heterogeneity of the resulting measurements.

IV. Deriving DNS Guidelines for IoT

To guide the development of DNS guidelines for IoT devices, we design a dual measurement framework to identify existing and potential issues in DNS protocol robustness, security, and privacy. The framework combines passive observation of device traffic with active measurements, including the injection or modification of DNS responses. This approach enables detection of anomalies and non-compliance under both benign and adversarial conditions. By analyzing DNS interactions from both client- and network-side perspectives, we obtain comprehensive visibility into the semantics of DNS requests and responses.

A. Passive Measurements: Protocol Compliance and Traffic Characteristics

Goal: Characterize DNS behavior in IoT environments during standard operation in the absence of adversarial activity.

Methodology: We monitor IoT device DNS behavior while connected to conventional resolvers using port 53, as well as secure DNS resolvers employing protocols such as DNS-over-HTTPS (DoH). Our measurements focus on protocol

TABLE I: Overview of DNS vulnerabilities in IoT devices across multiple attack surfaces

Device	Secure DNS Support (Sec. V.A.1)	Random Source Port (Sec. V.A.2)	Random Transaction ID (Sec. V.A.3)	Query Consistency (Sec. V.A.4)	Modified RR Resilience (Sec. V.B.1)	Forged TTL Resilience (Sec. V.B.2)	DoS Resilience (Sec. V.B.3)
Severity	**Critical**	**High**	**High**	**Medium**	**High**	**Medium**	**Critical**
Camera							
Arlo Pro 4 Spotlight Camera	✗	✗	✗	✗	✗	✓	✗
Blurams Pan-Tilt Camera (a31)	✗	✓	✓	✓	✓	✓	✗
Furbo 360° Dog Camera	✗	✓	✓	✓	✓	✓	✓
Vtech Video Camera (VM5467)	✗	✓	✓	✓	✓	✓	✓
Google Nest Cam	✗	✓	✓	✓	✓	✓	✓
Yi 1080P Home Camera	✗	✓	✗	✓	✓	✓	✗
Health Devices							
Qardiobase scale	✗	✓	✓	✓	✓	✓	✗
Home-automation							
Aqara SmartHome Hub M2	✗	✓	✓	✓	✓	✓	✓
Cosori Airfrier CS158	✗	✗	✓	✓	✗	✓	✗
Ecovacs Deebot Vacuum (N8)	✗	✓	✓	✓	✓	✓	✓
Levoit Smart Humidifier (300S)	✗	✓	✓	✓	✓	✓	✓
Meross Smart Garage Door	✗	✓	✓	✓	✓	✗	✓
PetSafe Smart Feeder	✗	✗	✗	✓	✓	✓	✗
Sensibo Sky AC Controller	✗	✓	✓	✓	✓	✓	✓
SwitchBot Hub Mini	✗	✓	✓	✓	✓	✓	✓
Tapo SmartLight Bulb (L530e)	✗	✓	✓	✓	✓	✓	✗
Yeelight Smart LED Bulb W3	✗	✓	✓	✓	✗	✓	✗
Swan Alexa Smart Kettle	✗	✓	✓	✓	✓	✓	✗
WeeKett Smart Kettle	✗	✓	✓	✓	✓	✓	✓
Lavazza A Modo Mio Voicy	✗	✓	✓	✓	✓	✓	✗
OKP Smart Vacuum (K2P)	✗	✓	✓	✓	✓	✓	✓
LIFX Mini Light A19	✗	✓	✓	✓	✗	✗	✓
LG Television (32LQ630BLA)	✗	✗	✓	✗	✓	✗	✓
Smart-Plugs							
Tapo Mini SmartPlug P110	✗	✓	✓	✓	✓	✓	✓
Belkin WeMo SmartPlug	✗	✓	✓	✗	✓	✓	✗
Meross Matter SmartPlug Mini	✗	✓	✓	✓	✗	✓	✓
Smart speaker							
Sonos SmartSpeaker One	✗	✓	✓	✓	✗	✗	✓
Bose Home Speaker 500	✗	✓	✓	✓	✓	✓	✓
Amazon Echo Spot (BV84J9)	✗	✓	✓	✓	✓	✓	✓
Amazon Echo Dot 5	✗	✓	✓	✓	✓	✓	✓
Apple Homepod 1st Gen	✗	✓	✓	✓	✓	✓	✗
Doorbells + Chimes							
Arlo Chime 2	✗	✓	✓	✓	✗	✓	✓
Eufy Wi-Fi Doorbell Chime	✗	✗	✗	✗	✓	✗	✓
Ring Chime Pro Wi-Fi Extender	✗	✓	✓	✗	✓	✓	✓
Ring Doorbell Plus (5F77E9)	✗	✓	✓	✓	✓	✓	✓

Severity Legend: Critical: Directly compromises security or availability; high impact and exploitability. **High:** Enables significant attacks via reduced entropy or predictability; strong security implications. **Medium:** Impacts privacy, operational efficiency, or integrity; may facilitate indirect attacks. ✗ = Vulnerable / Failed, ✓ = Secure / Passed.

hygiene, randomness quality, and device-specific operational characteristics.

We capture IoT traffic during representative operational phases, including initial power-on (boot) and steady-state operation. Continuous monitoring enables the longitudinal behavioral analysis, while controlled experiments facilitate fixed-duration evaluation.

These captures show the number of contacted domains, DNS query frequency, use of caching or backoff mechanisms, support for optional DoH/DoT protocols, and EDNS(0) extensions, as well as susceptibility to metadata-based fingerprinting.

We further evaluate entropy in security-sensitive DNS packet fields, namely the source port and transaction ID. Their observed ranges over a device's lifetime ensure sufficient randomness to mitigate spoofing and cache poisoning attacks. We also monitor TTL behavior to detect caching violations, such as repeated queries despite valid records or excessively long-lived DNS entries.

Table II summarizes the passive metrics we use to assess DNS protocol compliance, implementation robustness, and information leakage in IoT devices. Together, these metrics capture both functional correctness (e.g., record handling, TTL behavior, EDNS(0) support) and security-relevant properties (e.g., entropy of source ports and transaction identifiers), enabling systematic identification of deviations from best practices under benign operating conditions.

B. Active Measurements: Robustness to Adversarial DNS Manipulation

Goal: Evaluate the resilience of IoT DNS implementations when exposed to malformed or adversarially crafted responses from compromised resolvers or malicious actors.

TABLE II: Passive DNS Measurement Metrics for IoT Devices

Metric	Description
DNS Query Rate	Rate of DNS queries generated per device over time (queries/s)
Inter-Query Interval	Distribution of time gaps between consecutive DNS queries
Queried Domain Set	Cardinality and diversity of fully qualified domain names (FQDNs) contacted
IP Version Usage	Relative use of DNS resolution over IPv4 (A) versus IPv6 (AAAA)
Secure DNS Support	Use of encrypted or authenticated DNS protocols (DoH, DoT, DNSSEC)
Resource Record Types	Distribution of queried and received DNS record types (e.g., A, AAAA, CNAME, TXT)
TTL Behavior	Observed TTL values and compliance with caching semantics
Message Size	Byte-level size of DNS queries and responses
EDNS(0) Capability	Support for EDNS(0), including advertised UDP payload size and fragmentation behavior
Query Name Length	Length distribution of queried domain names (labels and total length)
Temporal Query Patterns	Periodicity and burstiness of DNS activity over time
Source Port Entropy	Variability and randomness of UDP source port selection
Transaction ID Entropy	Variability and randomness of DNS transaction identifiers

Measurement period: August 2023–December 2025.

TABLE III: Active DNS Manipulation Experiments

Experiment Category	Adversarial Manipulation
Baseline Resolution	Unmodified DNS responses under standard resolver behavior
Zero TTL Injection	Resource records returned with TTL set to 0 seconds
Short TTL Injection	Resource records returned with TTL set to 1 second
Excessive TTL Injection	Resource records returned with extremely long TTL values (e.g., 10^9 seconds)
Forged IPv4 Address	Injection of non-routable IPv4 addresses (RFC 1918) in A records
Forged IPv6 Address	Injection of reserved IPv6 addresses (IANA special-purpose ranges) in AAAA records
Forged CNAME Redirection	Injection of CNAME records pointing to documentation/testing domains
Empty Response Injection	DNS responses with all legitimate resource records removed
Response Padding	Artificial inflation of DNS response size via payload padding
Resolver Unavailability	DNS resolution failure due to inactive or unreachable port 53
RR Amplification	Responses containing a large number of duplicated resource records
Response Flooding	Multiple duplicated DNS responses sent for a single query

Per-experiment capture duration: 1–4 hours .

Methodology: IoT devices are subjected to active controlled attacks by configuring the DNS resolver in an adversarial manner. To analyze cache manipulation and susceptibility to cache poisoning, we use Unbound (v1.19.3) as a recursive caching DNS resolver. Under default settings, Unbound does not alter DNS responses; however, in our configuration, it is modified to generate custom responses, enabling controlled manipulation, response validation, and security assessment.

We actively manipulate DNS responses by modifying resource records (RRs), including deleting all legitimate RRs and injecting non-legitimate IPv4 A, IPv6 AAAA, and CNAME records. All tests use non-routable IP address ranges reserved for documentation and testing. We analyze the resulting responses to assess device susceptibility to malformed or invalid DNS data.

We also manipulate TTL values by substituting extreme values, including zero seconds and excessively long durations, to evaluate device caching and retry behavior. Additionally, we increase DNS response sizes to simulate amplification attacks and assess device handling of large payloads, TCP fallback behavior, and packet fragmentation. Finally, we simulate replay attacks to measure vulnerability to spoofing and injection attacks.

Table III summarizes the active DNS manipulation experiments we use to evaluate device robustness against malformed, adversarial, and resource-exhaustion scenarios. These experiments target DNS response validation, caching behavior, payload handling, and failure recovery, enabling systematic assessment of resilience to cache poisoning, amplification, replay, and denial-of-service conditions. We further detail the individual experiment parameters in Section V.

All adversarial DNS experiments are conducted on a fully isolated and secure wireless network. Dedicated DNS and DNS-flooding servers remain disconnected from the Internet, ensuring that no external systems are affected. No traffic exits the testbed, and no cloud services or production networks are impacted.

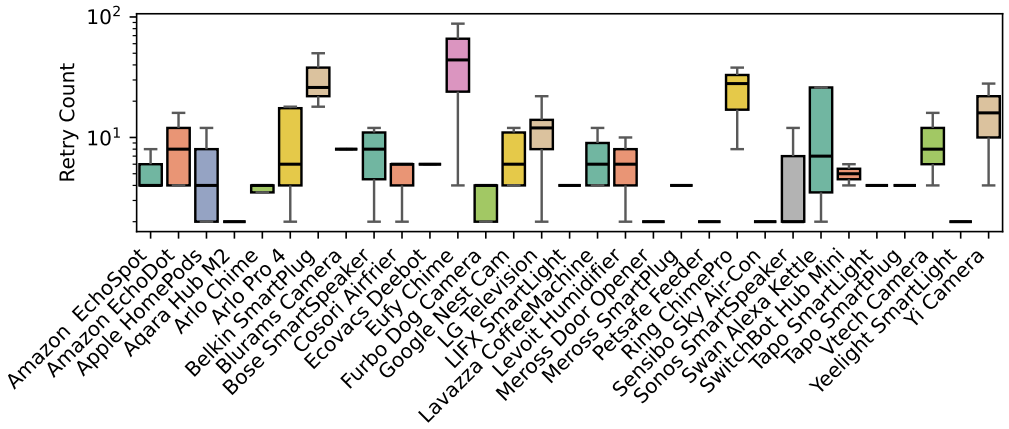
V. Results

Our passive and active measurement framework reveals several critical security and privacy shortcomings in the DNS behavior of consumer IoT devices. Table I summarizes the device-specific results presented in this section. The table classifies the severity of potential compromise using the MITRE ATTCK [37] and Common Attack Pattern Enumeration and Classification (CAPEC) [38] methodologies. We rate Support for Secure DNS (DoH/DoT/DNSSEC), which mitigates CAPEC-121 (DNS Cache Poisoning), and DoS Resilience, which mitigates CAPEC-191 (DNS Amplification), as Critical. We rate source port and Transaction ID randomization, along with RR injection resilience, as High, while all other entries are classified as Medium risk.

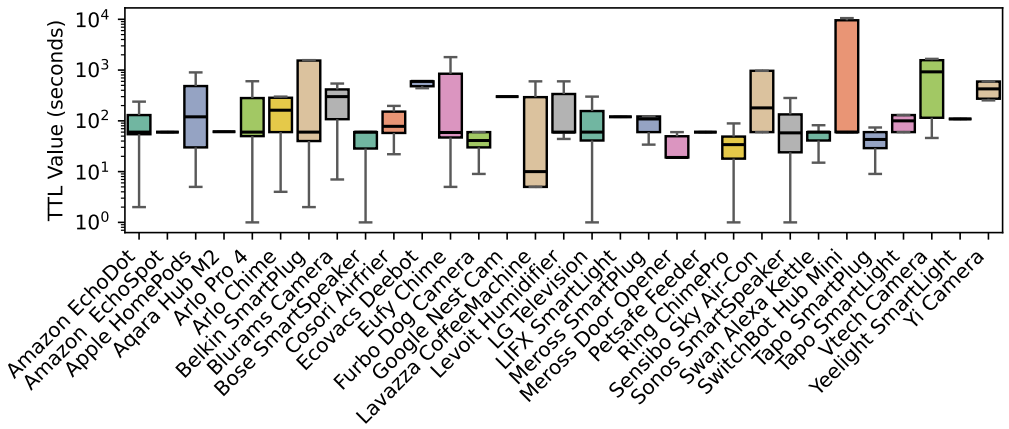
Based on these findings, we develop an Internet Engineering Task Force (IETF) Best Current Practice guideline entitled *IoT DNS Security and Privacy Guidelines*. The document has been adopted by the relevant working group and remains under development [27].

A. Passive Measurement Outcomes

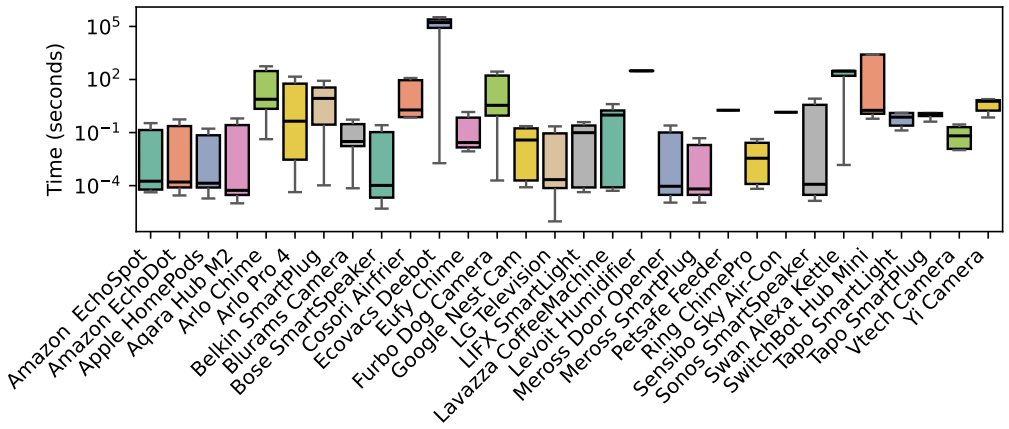
1) Compliance to Secure/Privacy-Preserving Standards: We examine the operational behavior of all IoT devices in the testbed using both a conventional DNS-over-port-53 resolver and a DoH-only resolver. We first present per-device metrics for the conventional DNS setup using box plots in Fig. 2, and then compare them with the DoH-only scenario shown in



(a) Number of retries



(b) TTL values

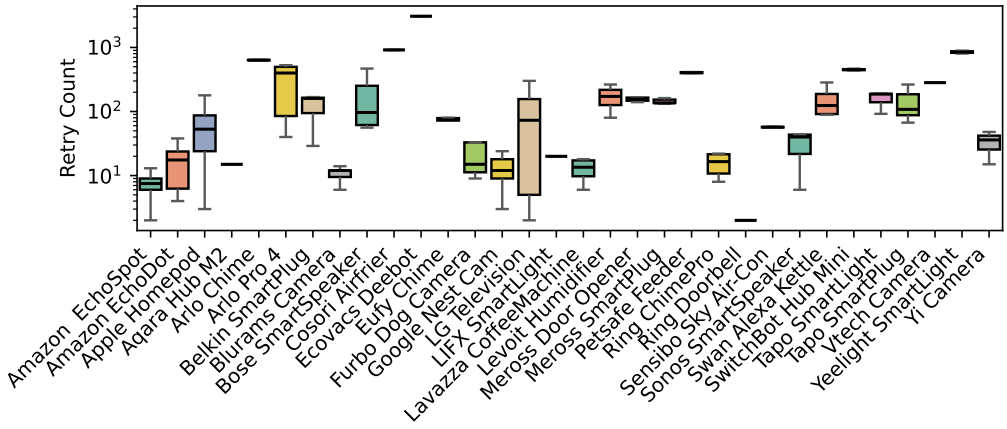


(c) Inter-query time

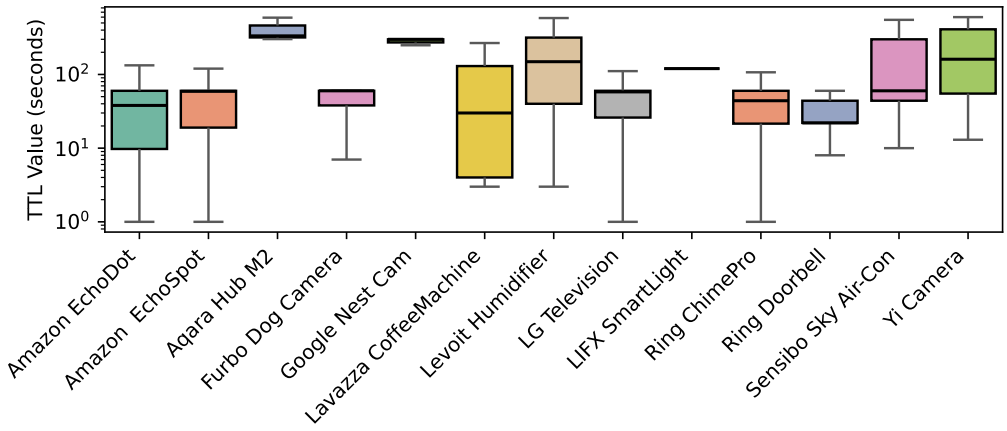
Fig. 2: DNS traffic characteristics for the traditional Do53. Each row showcases the metric: (a) number of retries, (b) TTL values, and (c) inter-query times.

Fig. 3, enabling a comparison of distributional information and levels of variability. The evaluated metrics include the average number of DNS query retries, average TTL values, and average inter-query intervals under both configurations. Differences are most pronounced in DoH-only scenarios, particularly with higher retry counts and lower inter-query timing. This behavior arises primarily from the lack of support for encrypted DNS protocols (e.g., DoH or DoT), which leaves devices vulnerable to interception, manipulation, and privacy threats.

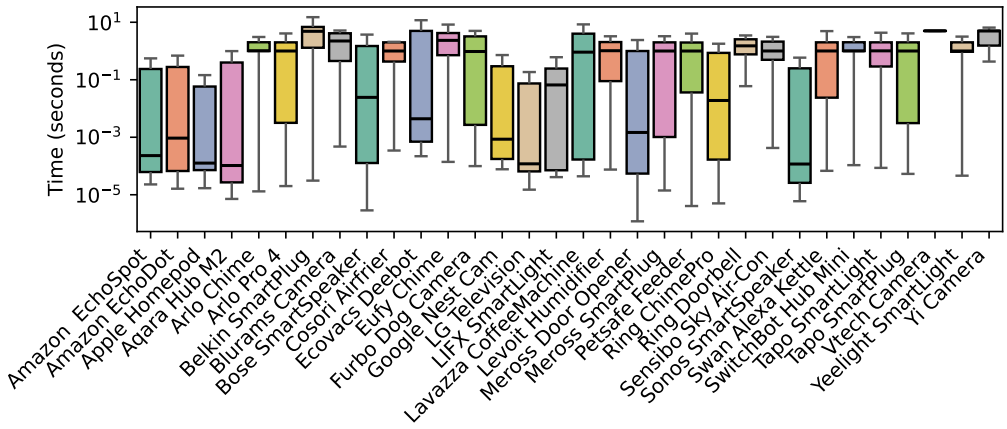
We observe that many IoT devices generate DNS queries of characteristic length. Query length alone constitutes a highly distinctive fingerprint due to significant variability across queries and responses. Even with DoH, query length remains fingerprintable if padding is not employed [7]. Furthermore,



(a) Number of retries



(b) TTL values

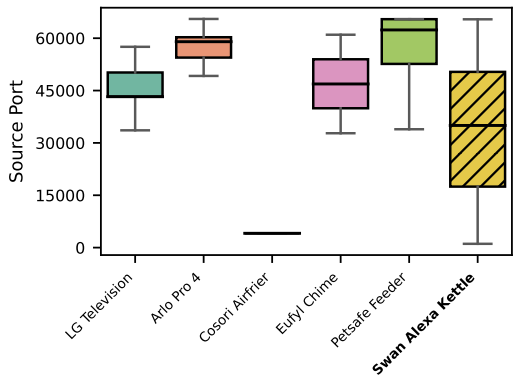


(c) Inter-query time

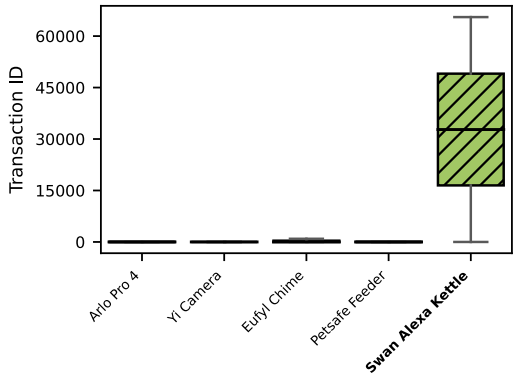
Fig. 3: DNS traffic characteristics for DoH-only resolvers. Each row showcases the metric: (a) number of retries, (b) TTL values, and (c) inter-query times.

despite being a mature technology [39], no device in our testbed implements DNSSEC [13], increasing susceptibility to DNS spoofing [40] and cache poisoning [41], which potentially results in redirection to malicious domains.

Among the 35 analyzed IoT devices, fourteen (40.0%), including the *Furbo Dog Camera*, *Levoit Humidifier*, *Ring Doorbell*, *Ring Chime Pro*, *Aqara Hub M2*, *Sensibo Sky*, *Echo Spot*, *Echo Dot*, *Google Nest Cam*, *Lavazza CoffeeMachine*, *LIFX SmartLight*, *LG Television*, *Amazon Echo Dot* and *Amazon Echo Spot* actively override DNS server addresses provided via DHCP. By using hard-coded DNS resolvers, these devices bypass network-level security controls and violate established security policies.



(a) Source ports



(b) Transaction IDs

Fig. 4: Variability of DNS source ports and transaction IDs in IoT devices. Limited dispersion indicates poor randomization, while the hatched rightmost device (Swan Alexa Kettle) exhibits correct operation and acts as a high-variability reference.

Recommendation #1

IoT devices should support DoH/DoT. In addition, padding should be utilized to reduce fingerprinting.

Recommendation #2

IoT devices should use the resolvers assigned through DHCP and not override to hard-coded fallback resolvers.

2) Poor Source Port Randomization in Requests: Effective DNS source-port randomization serves as a critical mechanism for mitigating spoofing, man-in-the-middle, and DNS cache poisoning attacks, as specified in RFC 5452 [42]. We illustrate the high randomization disparities (as reflected by the variation) in Fig. 4a, underscoring persistent DNS security weaknesses in consumer IoT implementations. Across 35 consumer IoT devices, 5 devices lack source port randomization or implement it at a very low level. Detailed packet capture analysis of six representative devices reveals substantial variation in compliance with these recommendations.

The *Cosori Airfryer* exhibits no randomization (standard deviation, $\sigma = 0$), with all DNS requests originating from a single fixed port (4096). The *LG Television* shows weak randomization ($\sigma = 4918.44$), with 42.75% of requests concentrated on one source port and the remainder confined to a small port set. The *PetSafe Automatic Feeder* similarly demonstrates poor randomness ($\sigma = 5586.66$), with over 99% of requests using only three ports. The *Arlo Pro 4* exhibits partial randomization ($\sigma = 4263.05$), distributing requests across multiple ephemeral ports but with strong bias toward a limited subset. The *Eufy Chime* shows moderate but constrained variability ($\sigma = 8132.58$). In contrast, the *Swan Alexa Kettle*, included as a reference, distributes DNS requests evenly across a wide ephemeral range, demonstrating effective source port randomization ($\sigma = 18{,}785.52$).

Recommendation #3

IoT devices should undergo adequate source port randomization in their DNS queries.

3) Non-Randomized Transaction IDs : Fig. 4b presents the variation of DNS transaction IDs across consumer IoT devices, highlighting substantial differences in randomization quality. Four of the 35 devices exhibit persistently low variance, indicating deterministic or weak ID generation and increased susceptibility to DNS cache poisoning within the 16-bit ID space (0–65535). The *Arlo Pro 4* and *Yi Camera* show extremely low variability, with standard deviations of 0.53 and 0.49, respectively, while the *Petsafe Feeder* exhibits slightly higher but still constrained variation ($\sigma = 115.96$). The *Eufy Chime* generates IDs with $\sigma = 725.59$, restricting traffic to a small portion of the valid space (0x00–0x4F, 0.12%). In contrast, the *Swan Alexa Kettle* demonstrates orders-of-magnitude higher variance ($\sigma = 18{,}857.74$), consistent with near-uniform randomization. These results underscore the substantial disparities in DNS resolver security across consumer IoT devices.

Recommendation #4

IoT devices should use adequate transaction ID randomization in their DNS traffic.

4) Query Inconsistencies: We identify significant inconsistencies in DNS query behavior across IoT devices when investigating and comparing Fig. 2 and 3. A common issue is the failure to respect DNS Time-To-Live (TTL) values, resulting in erratic and unnecessarily frequent re-queries. Several devices repeatedly query the same domain regardless of TTL validity, leading to inefficient caching behavior. In some cases, query rates increase by an order of magnitude when the DNS resolver becomes unavailable, indicating the absence of proper backoff or retry logic. As seen in Fig. 3b, only a handful of devices with hard-coded fallback DNS resolvers could get replies (hence reported TTL values), while the rest just continued regardless with aggressive querying.

Our analysis also reveals limited support for EDNS(0), a mechanism that allows DNS messages larger than 512 bytes and supports features such as optional padding. Only one of the evaluated devices implements this extension mechanism [25]. Without EDNS(0), devices either transition to TCP-based DNS queries for responses exceeding 512 bytes or fragment traffic at the IP layer, both of which increase latency and resource consumption.

Many IoT devices exhibit highly deterministic DNS behavior, with query rates that, while varying, remain strongly indicative of specific device models. The number of distinct queried domains is device-dependent, with some devices gen-

erating query rates up to two orders of magnitude higher than others. Such deterministic, repetitive behavior introduces multiple operational and security challenges:

1) **Device Fingerprinting:** Consistent query timing can be exploited to identify device models or firmware versions through metadata analysis.
2) **Resource Overhead:** Redundant queries generate unnecessary network traffic and increase power consumption, particularly in bandwidth- or energy-constrained environments.

To mitigate these risks, IoT devices should adopt random intervals that include jitter instead of fixed schedules, thereby reducing predictability and susceptibility to fingerprinting [43]. Devices should also respect TTL values by caching responses for their full validity period rather than issuing premature queries. For critical operations, such as periodic validation of control endpoints, manufacturers should implement configurable refresh intervals with user-defined bounds instead of static timers. Incorporating DNS TTL caching into an IoT device may require minimal configuration, as in FreeRTOS, where caching can be enabled via `ipconfigUSE_DNS_CACHE` parameter [44]. In contrast, platforms such as Contiki-NG [45] provide only a basic DNS client and require substantial modifications to support full TTL-based DNS caching.

Recommendation #5

IoT devices should have adaptive caching mechanisms and should comply with received TTLs before making repetitive queries.

B. Active Measurement Outcomes

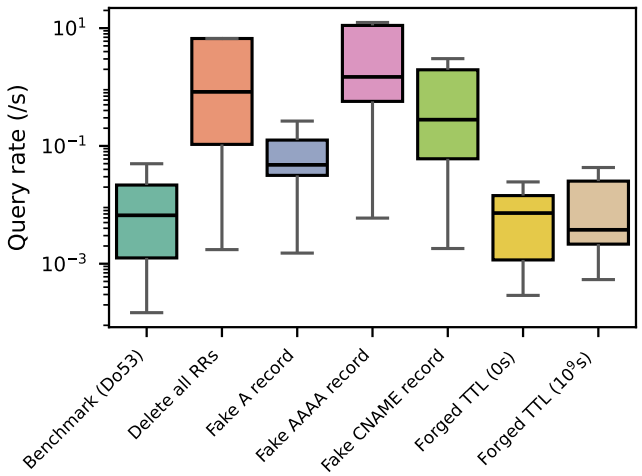
1) Effects of Modified RRs: We conduct an initial experiment to characterize IoT client behavior in response to unresolved DNS queries. We configure the Unbound server to omit all resource records (RRs) from DNS responses, effectively breaking name resolution for all devices. As shown in Fig. 5, we observe a surge in query and retry attempts, with some devices increasing the proportion of IPv6 queries during repeated resolution attempts. These results highlight the lack of robust handling of persistent DNS failures by IoT devices. Aggressive and uncontrolled retries not only risk network congestion and increased power consumption in resource-constrained devices but may also amplify adversarial attacks.

Recommendation #6

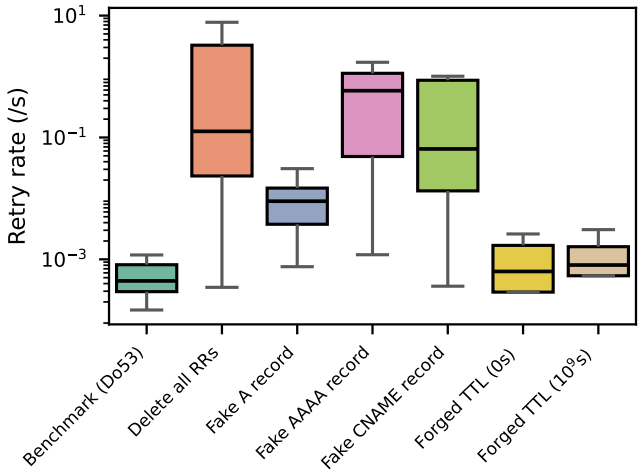
IoT devices should identify consistent DNS failures and implement exponential back-off strategies.

We next evaluate the robustness of IoT devices in handling forged DNS responses from the resolver to identify potential security and operational vulnerabilities. We replace the initial legitimate response with forged `A`, `AAAA`, and `CNAME` records. We present the resulting query and retry behavior in Fig. 5, including query rates (Fig. 5a) and retry rates (Fig. 5b), along with detailed per-device observations in Table I.

When dealing with a forged `A` record, most devices accept the fake IPv4 address (*192.0.2.1*) without validation, potentially causing them to contact adversary-controlled servers. In contrast, when we return the forged `AAAA` records (*2001:0db8::1*) in response to `A` queries, devices trigger a sharp increase in query and retry rates, as they fail to correctly interpret or utilize the IPv6 address. Finally, forged `CNAME` records (*alias.example.com*) produce mixed behavior, with some devices resolving the alias while others significantly amplify retry attempts.



(a) Queries during active measurements



(b) Retries during active measurements

Fig. 5: Query and retry behavior during active measurements.

The absence of validation mechanisms for forged resource records (RRs), combined with aggressive retry behavior, enables novel attack vectors that adversaries can exploit, including man-in-the-middle (MITM) and denial-of-service (DoS) attacks.

Recommendation #7

IoT devices should integrate robustness in their DNS stacks by including record-type validation, authenticity checks, potentially through actively utilizing DNSSEC.

2) Robustness against Forged TTLs: We further investigate scenarios in which the DNS resolver actively manipulates TTL values in DNS responses. We set TTLs to extreme values: (i) a

very low value (TTL = $0, \mathrm{s}$) and (ii) a very high value ($10^9, \mathrm{s}$). We compare these results against a benchmark representing normal IoT device operation, as shown in Fig. 5.

Our findings indicate that reducing TTLs to zero or near-zero values amplifies DNS query and retry rates in some IoT devices, demonstrating a failure to properly cache DNS records. In contrast, when exposed to a very high TTL of $10^9, \mathrm{s}$, some devices cease sending DNS queries altogether, while others continue querying at high rates, effectively ignoring the TTL. As a result, such devices may fail to detect updates to DNS records from target servers.

Overall, IoT devices exhibit high sensitivity to TTL manipulation by resolvers, which can introduce security vulnerabilities and lead to resource exhaustion.

Recommendation #8

IoT devices should detect abrupt/extreme changes in TTL values in DNS replies and follow up on their DNS activity, assuming a normal TTL value range.

Resilience Against DoS: We conduct experiments to evaluate IoT device resilience under anomalous DNS responses. In the initial DNS DoS experiment, we subject devices to DNS amplification attacks, receiving responses amplified by factors of 10, 50, and 100 relative to the original queries. While most devices remain stable, six (17.14%) become inoperable at the highest amplification level, including the *Tapo Light L530e*, *Apple HomePod*, and *Qardiobase Scale*, likely due to CPU, RAM, and buffer limitations.

We further stress devices by increasing the number of `A` records per DNS response, using replication factors of 10, 50, and 100. The resulting payloads often exceed the 512-byte UDP limit specified in RFC 1035 [2].

In our experiments, seven devices (20%) fail operationally when exposed to large DNS payloads that contain 100 resource records. During both DoS experiments, we measure sustained device operation under attack. While some devices may have partial defenses against flooding or oversized responses, our observations reflect real-world performance and guide the proposed IoT DNS security and privacy13. guidelines.

Overall, EDNS(0) support is limited, with only one device (Meross Garage Door Opener) utilizing the extension mechanism. Devices that support EDNS(0) should advertise larger payload sizes, while those without EDNS(0) support should fall back to TCP upon receiving truncated responses. Instead, we observe widespread IP-layer fragmentation, substantially increasing processing and memory overhead. Notably, one-fifth of the 35 evaluated devices fail to maintain network connectivity under maximum payload conditions, resulting in service disruption [46].

Recommendation #9

IoT devices should detect amplified responses and must implement validation of DNS response sizes along with supporting EDNS(0).

VI. Implementation and Long-term Views

We now outline broader guidelines for manufacturers and discuss their implementation through standardization.

Improving Trust and Privacy. We identify a significant privacy gap due to the lack of secure DNS protocols such as DoH and DoT. However, even when DoH or DoT is deployed, IoT devices remain identifiable through traffic-pattern fingerprinting. IoT manufacturers should integrate lightweight DoH/DoT stacks with support for padding, particularly for devices that process continuous and sensitive user data. Stronger policy enforcement mechanisms are also required, as many IoT devices currently lack effective controls.

Enforcing Compliance with Protocol Recommendations. Many observed vulnerabilities stem from partial or incorrect implementations of the DNS protocol stack. IoT devices must urgently comply with existing RFCs, particularly with respect to proper randomness in source ports and transaction IDs. These improvements remain protocol-agnostic and can be implemented via embedded DNS libraries. Manufacturers should validate implementations using test suites that cover both benign and adversarial resolver scenarios.

Towards DNS Standards for IoT. We emphasize the need for DNS security and privacy guidelines tailored specifically to IoT devices, given the prevalence of vulnerabilities and the absence of comprehensive regulatory frameworks.

We assess existing standards and recommendations in Table IV to determine whether regulatory and advisory bodies explicitly address DNS operational requirements for IoT devices. The table summarizes DNS coverage across standards: the first column (DNS∩IoT) indicates IoT-specific DNS guidance, while the second column captures generic DNS recommendations applicable beyond IoT contexts.

We observe a lack of DNS–IoT-specific guidance and regulation across current standardization and regulatory bodies. For example, ETSI EN 303 645 V3.1.3, Cyber Security for Consumer Internet of Things: Baseline Requirements [47], developed by the European Telecommunications Standards Institute (ETSI), defines baseline security requirements for consumer IoT devices. However, it does not address DNS security or operation in IoT contexts, except for a single provision (5.5-5) that permits devices to accept DNS responses from unauthenticated sources.

Both ETSI GR IP6 008 [48] and ISO/IEC 30161-2:2023 [49] have limited scope, addressing DNS primarily for device registration and higher-level name resolution. While the CIS Internet of Things Companion Guide [50] includes some DNS-related recommendations, it does not consider DNS from the perspective of IoT client devices.

IoT devices, particularly those with constrained hardware, should undergo verification to ensure DNS protocol compliance. Standardization bodies such as the IETF, ETSI, and ISO/IEC should incorporate DNS-specific compliance checks. In addition, regulatory frameworks should require manufacturers to disclose any DNS security measures or guidelines that they do not implement.

Accountability of Vendors. All proposed guidelines must remain enforced throughout the lifetime of IoT devices, with regular firmware updates to remediate emerging DNS vulnerabilities. Vendors should transparently inform users of any DNS-related failures.

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				
World Wide Web Consortium (W3C)						
Web of Things (WoT) Security Guidelines	✗ DNS∩IoT	✗ DNS				
Center for Internet Security (CIS)						
Internet of Things Companion Guide	✗ DNS∩IoT	✗ DNS				

TABLE IV: Absence of IoT-specific DNS References in Various Standards and Guidelines.

Scope Limitations. This paper examines the DNS behavior of commercial IoT smart-home devices in a simulated real-world environment. We treat devices as closed black boxes, without classification by OS, vendor (e.g., FreeRTOS, Zephyr), or platform (e.g., Tuya, HomeKit), and without analyzing SDK or library patterns. Direct access to commercial IoT internal systems is highly restricted. Analysis is therefore based on traffic measurements and active experiments, supporting DNS-for-IoT best-practice recommendations.

While we acknowledge the security benefits of encrypted DNS, we do not mandate DoH or DoT support in IoT devices, nor require DNSSEC for detecting malicious DNS redirects. Consistent with prior studies [19], many resource-constrained IoT devices remain limited by CPU, memory, and power, hindering support for secure DNS protocols.

VII. Related Work

The regulatory landscape for DNS security in IoT evolves, with increasing emphasis on enforcing cybersecurity standards and privacy protections. ICANN, as the global administrator of DNS, plays a pivotal role in governance, but its regulatory influence remains limited by the decentralized nature of the Internet [51]. To address security gaps, the European Union introduces measures such as the GDPR and the EU Cybersecurity Act, mandating stricter protocols for DNS-based services and IoT infrastructure [52].

Federated DNS architectures gain traction, decentralizing resolution processes and reducing reliance on a few major DNS providers [53]. These architectures allow IoT devices to use private resolvers, enhancing security while minimizing exposure to public attacks [54]. Industry initiatives such as DNS-based Authentication of Named Entities (DANE) and DNSSEC aim to improve authentication and integrity verification of DNS responses [55], [56].

Despite these advancements, challenges remain in enforcing compliance across diverse IoT ecosystems. Many manufacturers prioritize cost and efficiency over security [57], [58], resulting in widespread deployment of devices with minimal

or no DNS protections [56]. Legal scholars advocate a multi-stakeholder approach that balances regulatory intervention with industry self-regulation to ensure DNS security [59]. Standardization efforts led by the Internet Engineering Task Force (IETF) play an essential role in establishing universal security best practices and mitigating DNS vulnerabilities in IoT [60].

Automated approaches identify vulnerabilities and evaluate compliance. For DNS, fuzzing exposes protocol weaknesses [61], and RFC compliance has been studied for resolvers and nameservers [62], but client-side DNS behavior remains largely unexamined.

Our empirical investigation of DNS operations across 35 consumer-grade smart home IoT devices addresses this gap, providing a baseline for real-world adoption of security protocols, operational DNS behavior, and potential privacy exposures.

VIII. Conclusion

This study demonstrates that DNS implementations in consumer IoT devices frequently deviate from established standards and lack fundamental security protections, exposing users to significant security, privacy, and operational risks. Core defensive mechanisms, such as source port and transaction identifier randomization, are often absent, while none of the evaluated devices support secure DNS mechanisms. Limited adoption of EDNS(0) leads to IP fragmentation, increased overhead, and operational inefficiencies. Device-specific DNS behaviors enable reliable passive fingerprinting, widespread violations of caching semantics inflate query volumes, and the use of hard-coded DNS resolvers restricts administrative control. Active stress testing further confirms these weaknesses, with many devices exhibiting instability under DNS flooding and generating duplicated or malformed resource record responses. Collectively, these findings expose systemic weaknesses in DNS implementations across consumer IoT ecosystems and highlight gaps in existing standards. We therefore propose an IETF "DNS for IoT" guideline to establish a secure and efficient DNS baseline for IoT deployments [27].

Acknowledgments

The research in this paper was partially supported by the UK EPSRC grant EP/S022503/1 that supports the Centre for Doctoral Training in Cybersecurity delivered by UCL's Departments of Computer Science, Security and Crime Science, and Science, Technology, Engineering and Public Policy.

References

[1] P. V. Mockapetris, "Domain names-concepts and facilities," Internet Engineering Task Force, Tech. Rep. RFC 1034, Nov. 1987, accessed: Feb. 20, 2026. [Online]. Available: https://datatracker.ietf.org/doc/rfc1034

[2] P. V. Mockapetris, "Domain names-implementation and specification," Internet Engineering Task Force, Tech. Rep. RFC 1035, Nov. 1987, accessed: Feb. 20, 2026. [Online]. Available: https://datatracker.ietf.org/doc/rfc1035

[3] V. Pappas, D. Massey, and L. Zhang, "Enhancing DNS resilience against denial of service attacks," in *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2007)*, Jun. 2007, pp. 450–459, accessed: Feb. 20, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4272996

[4] M. Allman, "Comments on DNS robustness," in *Proceedings of the 2018 ACM Internet Measurement Conference (IMC '18)*, Oct. 2018, pp. 84–90.

[5] H. Shulman, "Pretty bad privacy: Pitfalls of DNS encryption," in *Proceedings of the 13th ACM Workshop on Privacy in the Electronic Society (WPES '14)*, Nov. 2014, pp. 191–200.

[6] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," in *Proc. 2nd International Conference on Availability, Reliability and Security (ARES '07)*, Apr. 2007, pp. 335–342. [Online]. Available: https://ieeexplore.ieee.org/document/4159821/

[7] S. Pélissier, G. Anselmi, A. K. Mishra, A. M. Mandalari, and M. Cunche, "Enhancing IoT privacy: Why DNS-over-HTTPS alone falls short?" in *Proc. 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2024, pp. 1353–1360.

[8] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on DNS encryption: Current development, malware misuse, and inference techniques," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 162:1–162:28, Dec. 2022.

[9] S. Lazzaro, V. De Angelis, A. M. Mandalari, and F. Buccafurri, "Is your kettle smarter than a hacker? a scalable tool for assessing replay attack vulnerabilities on consumer IoT devices," in *Proc. IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Mar. 2024, pp. 114–124.

[10] P. E. Hoffman and P. McManus, "DNS queries over https (doh)," Internet Engineering Task Force, Request for Comments RFC 8484, Oct. 2018. [Online]. Available: https://datatracker.ietf.org/doc/rfc8484

[11] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. E. Hoffman, "Specification for DNS over Transport Layer Security (TLS)," Internet Engineering Task Force, Tech. Rep. RFC 7858, May 2016. [Online]. Available: https://datatracker.ietf.org/doc/rfc7858

[12] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, "Encrypted DNS –> privacy? a traffic analysis perspective," Oct. 2019. [Online]. Available: http://arxiv.org/abs/1906.09682

[13] P. E. Hoffman, "Dns security extensions (DNSSEC)," IETF, Tech. Rep. RFC 9364, Feb. 2023, accessed: Feb. 20, 2026. [Online]. Available: https://www.rfc-editor.org/info/rfc9364

[14] Y. Afek, H. Berger, and A. Bremler-Barr, "POPS: From history to mitigation of DNS cache poisoning attacks," Jan. 2025, accessed: Feb. 20, 2026. [Online]. Available: http://arxiv.org/abs/2501.13540

[15] A. Aydeger, S. Hoque, E. Zeydan, and K. Dev, "Analysis of robust and secure DNS protocols for IoT devices," *arXiv*, vol. abs/2502.09726, Feb. 2025, accessed: Feb. 20, 2026. [Online]. Available: https://arxiv.org/pdf/2502.09726

[16] Daniel J. Bernstein, "Tinydns — DNS server software," [Online]. Available: https://tinydns.org/, accessed: Feb. 20, 2026.

[17] RIOT OS Project, "RIOT - The friendly Operating System for the Internet of Things," accessed: Feb. 20, 2026. [Online]. Available: https://www.riot-os.org/

[18] C. Sabri, L. Kriaa, and S. L. Azzouz, "Comparison of IoT constrained devices operating systems: A survey," in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, Oct 2017, pp. 369–375.

[19] I. Ayoub, S. Balakrichenan, K. Khawam, and B. Ampeau, "DNS for IoT: A Survey," *Sensors*, vol. 23, no. 9, p. 4473, May 2023. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10181686/

[20] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," Jun. 2014, accessed: Feb. 20, 2026. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7252

[21] M. S. Lenders, C. Amsüss, C. Gündogan, M. Nawrocki, T. C. Schmidt, and M. Wählisch, "Securing name resolution in the IoT: DNS over CoAP," *Proc. ACM Netw.*, vol. 1, no. CoNEXT2, pp. 6:1–6:25, Sep 2023.

[22] M. H. Mazhar and Z. Shafiq, "Characterizing smart home IoT traffic in the wild," in *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Apr. 2020, pp. 203–215. [Online]. Available: https://ieeexplore.ieee.org/document/9097598

[23] G. C. M. Moura, J. Heidemann, R. D. O. Schmidt, and W. Hardaker, "Cache me if you can: Effects of DNS time-to-live," in *Proc. Internet Measurement Conference*, Amsterdam, Netherlands, Oct. 2019, pp. 101–115. [Online]. Available: https://dl.acm.org/doi/10.1145/3355369.3355568

[24] J. L. Hernández-Ramos, G. Baldini, S. N. Matheu, and A. Skarmeta, "Updating IoT devices: Challenges and potential approaches," in *2020 Global Internet of Things Summit (GIoTS)*, Jun. 2020, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9119514

[25] J. L. S. Damas, M. Graff, and P. A. Vixie, "Extension mechanisms for DNS (edns(0))," Internet Engineering Task Force, Request for Comments RFC 6891, Apr. 2013. [Online]. Available: https://datatracker.ietf.org/doc/rfc6891

[26] A. Mayrhofer, "The EDNS(0) padding option," May 2016, accessed: Feb. 20, 2026. [Online]. Available: https://www.rfc-editor.org/info/rfc7830

[27] A. K. Mishra, A. Losty, A. M. Mandalari, J. Mozley, and M. Cunche, "IoT DNS security and privacy guidelines," Jul. 2025, internet Draft, work in progress. [Online]. Accessed: Dec. 22, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-mishra-iotops-iot-dns-guidelines/

[28] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis, "IoTFinder: Efficient large-scale identification of IoT devices via passive DNS traffic analysis," in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, Sep. 2020, pp. 474–489. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9230403

[29] J. Ye, X. D. C. De Carnavalet, L. Zhao, M. Zhang, L. Wu, and W. Zhang, "Exposed by default: A security analysis of home router default settings," in *Proc. 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24)*, Jul. 2024, pp. 63–79. [Online]. Available: https://dl.acm.org/doi/10.1145/3634737.3637671

[30] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer IoT devices: A multidimensional, network-informed measurement approach," in *Proceedings of the Internet Measurement Conference*, Oct. 2019, pp. 267–279.

[31] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "IoT Sentinel: Automated device-type identification for security enforcement in IoT," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, Jun. 2017, pp. 2177–2184.

[32] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, vol. 23, no. 13, p. 5941, Jun. 2023.

[33] M. M. Rahman, F. Bouhafs, S. A. Hoseini, and F. den Hartog, "Unsw homenet: A network traffic flow dataset for ai-based smart home device classification," *Computers & Industrial Engineering*, vol. 204, p. 111041, Jun. 2025.

[34] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*. IEEE, Nov. 2015, pp. 1–6.

[35] NLnet Labs, "Unbound — about," 2025, accessed: Feb. 20, 2026. [Online]. Available: https://nlnetlabs.nl/projects/unbound/about/

[36] A. M. Mandalari, D. J. Dubois, R. Kolcun, M. T. Paracha, H. Haddadi, and D. Choffnes, "Blocking without breaking: Identification and mitigation of non-essential IoT traffic," in *Proc. Privacy Enhancing Technologies*, vol. 2021, no. 4, Jul. 2021, pp. 1–30.

[37] MITRE Corporation, "Mitre att&ck: Adversarial tactics, techniques, and common knowledge," in *Online Framework*, Dec. 2025, accessed: Feb. 20, 2026. [Online]. Available: https://attack.mitre.org/

[38] MITRE Corporation, "Capec: Common attack pattern enumeration and classification," in *Online Framework*, Dec. 2025, accessed: Feb. 20, 2026. [Online]. Available: https://attack.mitre.org/

[39] A. Herzberg and H. Shulman, "DNSSEC: Security and availability challenges," in *Proc. 2013 IEEE Conf. on Communications and Network Security (CNS)*, Oct. 2013, pp. 365–366. [Online]. Available: https://ieeexplore.ieee.org/document/6682730/

[40] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks," in *Proc. 2017 Siberian Symposium on Data Science and Engineering (SSDSE)*, Apr. 2017, pp. 84–87. [Online]. Available: https://ieeexplore.ieee.org/document/8071970/

[41] K. Man, Z. Qian, Z. Wang, X. Zheng, Y. Huang, and H. Duan, "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels," in *Proc. 2020 ACM SIGSAC Conf. on Computer and Communications Security*. Virtual Event USA: ACM, Oct. 2020, pp. 1337–1350. [Online]. Available: https://dl.acm.org/doi/10.1145/3372297.3417280

[42] B. Hubert and R. van Mook, "Measures for making DNS more resilient against forged answers," Jan. 2009. [Online]. Available: https://www.rfc-editor.org/info/rfc5452

[43] J. Bushart and C. Rossow, "Padding ain't enough: Assessing the privacy guarantees of encrypted DNS," in *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2020)*. USENIX Association, Aug. 2020. [Online]. Available: https://www.usenix.org/conference/foci20/presentation/bushart

[44] FreeRTOS.org, "Freertos+TCP configuration: ipconfiguse_dns_cache," accessed: Feb. 20, 2026. [Online]. Available: https://www.freertos.org/Documentation/03-Libraries/02-FreeRTOS-plus/02-FreeRTOS-plus-TCP/06-Configuration#ipconfiguse_dns_cache

[45] Contiki-NG Documentation, "Contiki-ng documentation—develop," accessed: Feb. 20, 2026. [Online]. Available: https://docs.contiki-ng.org/en/develop/

[46] R. Pietrantuono, M. Ficco, and F. Palmieri, "Survivability analysis of IoT systems under resource exhausting attacks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3277–3288, Jun. 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10130289

[47] ETSI, "Welcome to the World of Standards!" accessed: Feb. 20, 2026. [Online]. Available: https://www.etsi.org/

[48] ETSI, "Ipv6-based internet of things: Introduction and functional requirements," European Telecommunications Standards Institute, Technical Report ETSI GR IP6 008 V1.1.1, Jan. 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_ip6008v010101p.pdf

[49] ISO/IEC, "Iso/iec 30161-2:2023," accessed: Feb. 20, 2026. [Online]. Available: https://www.iso.org/standard/86671.html

[50] "CIS controls v8 internet of things companion guide white paper," accessed: Feb. 20, 2026. [Online]. Available: https://www.cisecurity.org/white-papers/cis-controls-v8-internet-of-things-companion-guide/

[51] E. M. Weitzenboeck, "Hybrid net: The regulatory framework of ICANN and the DNS," *International Journal of Law and Information Technology*, vol. 22, no. 1, pp. 49–73, Jan. 2014.

[52] P. G. Chiara, "The IoT and the new EU cybersecurity regulatory landscape," *International Review of Law, Computers & Technology*, vol. 36, no. 2, pp. 118–137, May 2022.

[53] A. Lemogue, I. Martinez, L. Toutain, and A. Bouabdallah, "Federated IoT roaming using private DNS resolutions," in *Proc. IEEE/IFIP Network Operations and Management Symposium (NOMS)*, Apr. 2022, pp. 1–6.

[54] K. Kohler, "One, two, or two hundred internets?: The politics of future internet architectures," ETH Zurich, Report, Aug. 2022, accepted: 2022-08-25. Publication Title: CSS Cyberdefense Reports. [Online]. Available: https://www.research-collection.ethz.ch/handle/20.500.11850/563942

[55] C. Hesselman, M. Kaeo, L. Chapin, K. Claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour *et al.*, "The DNS in IoT: Opportunities, risks, and challenges," *IEEE Internet Computing*, vol. 24, no. 4, pp. 23–32, Jul. 2020.

[56] I. Ayoub, "Privacy-preserving communications for IoT based on DNS and its security extensions," Ph.D. dissertation, Université Paris-Saclay, Nov. 2024. [Online]. Available: https://theses.fr/2024UPASG074

[57] N. Nino, R. Lu, W. Zhou, K. H. Lee, Z. Zhao, and L. Guan, "Unveiling IoT security in reality: A Firmware-Centric journey," in *Proc. 33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 5609–5626. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/nino

[58] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, "Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms," in *Proc. 28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1133–1150. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/zhou

[59] R. H. Weber, "Internet of Things—need for a new legal environment?" *Computer Law & Security Review*, vol. 25, no. 6, pp. 522–527, Nov. 2009. [Online]. Available: https://doi.org/10.1016/j.clsr.2009.09.002

[60] G. Schmid, "Thirty years of DNS insecurity: Current issues and perspectives," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, Aug. 2021. [Online]. Available: https://doi.org/10.1109/COMST.2021.3105741

[61] Q. Zhang, X. Bai, X. Li, H. Duan, Q. Li, and Z. Li, "Resolverfuzz: Automated discovery of DNS resolver vulnerabilities with Query-Response fuzzing," in *Proc. 33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 4729–4746. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/zhang-qifan

[62] S. K. R. Kakarla, R. Beckett, T. Millstein, and G. Varghese, "Scale: Automatically finding RFC compliance bugs in DNS nameservers," in *Proc. 19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*. Renton, WA: USENIX Association, Apr. 2022, pp. 307–323. [Online]. Available: https://www.usenix.org/conference/nsdi22/presentation/kakarla

APPENDIX A
MODEL, FIRMWARE AND DATASET COLLECTION DETAILS

TABLE V: IoT Devices, Firmware Versions, and Collected Dataset Sizes for Passive and Active DNS Experiments

Device	Model	Firmware	Passive (5 months)	Active (1–4 h)
Cameras				
Arlo Pro 4 Spotlight Camera	Arlo Pro 4	1.080.33.1_38_0f7e1e1	81.6 GB	879 MB
Blurams Security Camera	A31	23.01418.*.*	55.8 GB	568 MB
Furbo 360° Dog Camera	Furbo 360°	108-003-005	23.2 GB	31.6 MB
VTech Baby Camera	VM901-1W	4.2.4.4	406 GB	537 MB
Google Nest Cam	Wired (3rd Gen)	Spencer-user 1.77 OPENMASTER 499686	20.6 GB	37.7 MB
Yi Camera 1080P	YYS2016	2.1.0.0E_201809191630	12.2 GB	194 MB
Health Devices				
Qardiobase Scale	Gen 1	2.55.1679594	7.17 MB	1.13 MB
Home Automation & Appliances				
Aqara Hub M2	HM2-G01	4.3.4_0012.0652	2.12 GB	9.28 MB
Cosori Airfryer	CS158	1.0.06	14.7 GB	1.11 GB
Ecovacs Vacuum (N8)	Deebot N8	1.2.0	1.00 GB	5.25 MB
Levoit Air Purifier	300S	1.3.02 (1.0.06)	7.06 GB	67.9 MB
Meross Garage Opener	MSG100	4.2.6	10.9 GB	24.8 MB
Petsafe Feeder	2nd Gen	2.0.9	1.32 GB	6.50 MB
Sensibo Sky	SEN-SKY-03	Latest	1.17 GB	3.42 MB
SwitchBot Hub Mini 2	Mini 2	6.2–5.1	5.44 GB	189 MB
Tapo Smart Bulb	L530e	1.1.9 (240524)	1.69 GB	227 MB
Yeelight LED Bulb 2	YLDP02YL	Firmware (β)	1.43 GB	45.9 MB
Alexa Swan Kettle	SK14650BLKN	308003520	3.15 GB	3.69 MB
WeeKett Kettle	KE4071TF-GS	Firmware (β)	10.8 GB	568 MB
Lavazza Coffee Maker	Voicy	1.0.56 (81)	4.04 GB	17.4 MB
OKP Smart Vacuum	K2P	21.3.21 (2.5.2)	4.48 GB	10.0 MB
LIFX Mini Light	A19	4.83.0	8.50 GB	2.97 MB
LG Television	32LQ630BLA	04.53.80	55.8 GB	527 MB
Smart Plugs				
Tapo Smart Plug	P110	1.4.0 (251020)	30.1 GB	3.43 MB
Belkin Plug	F7C027uk	5.03.21	1.12 GB	8.56 MB
Meross Plug	MSS315	9.3.26	2.52 GB	162 MB
Smart Speakers				
Sonos One	Gen 1	1.26.1.10-2.2	30.1 GB	21.9 MB
Bose Speaker 500	—	24.0.30	33.2 GB	70.7 MB
Amazon Echo Spot	BV84J9	690917620	10.0 GB	112 MB
Amazon Echo Dot 5	C2N6L4	12584504452	67.4 GB	89.0 MB
Apple HomePod	1st Gen	26.2	63.8 GB	103 MB
Doorbells and Chimes				
Arlo Chime Doorbell	AC2001	1.1.0.0_385_b0e4dcc	4.15 GB	83.9 MB
Eufy Chime	T8023	3.3.0.4m	8.60 GB	46.2 MB
Ring Chime Pro	2nd Gen	Latest (α)	161 GB	101 MB
Ring Doorbell	2nd Gen	Latest (α)	22.9 GB	673 MB

$^{\beta}$ Firmware version not exposed in vendor interface.
$^{\alpha}$ Firmware updated to latest available version but not explicitly displayed.
Passive dataset spans continuous operational traffic (Aug. 2023–Dec. 2025).
Active dataset corresponds to controlled DNS manipulation experiments.

Andrew Losty is currently a second-year Ph.D. candidate in Electronic and Electrical Engineering at University College London (UCL), U.K., where he is affiliated with the UCL Centre for Doctoral Training in Cybersecurity.

His research focuses on the privacy, security, and operational behaviour of Internet of Things (IoT) ecosystems. His current work examines the security and operation of DNS on IoT devices, including support for secure DNS and deviations from standards, as well as the Matter smart-home protocol, with a particular focus on regulatory alignment, firmware updates, robustness, and service discovery mechanisms such as mDNS.

Abhishek K. Mishra is currently a Postdoctoral Researcher with the PRIVATICS Team at Inria, France. He received his Ph.D. in Computer Science from Ecole Polytechnique, Paris, in 2023, where his research focused on inherent privacy risks in networked systems and wireless communications. Before that, he obtained his M.S. degree in Computer Engineering from KTH Royal Institute of Technology, Stockholm, and his B.Tech. degree in Electrical Engineering from the Indian Institute of Technology (IIT), Mandi.

His research interests lie at the intersection of security, privacy, and machine learning. In particular, his work focuses on privacy-preserving data publishing, anonymisation techniques, differential privacy, and privacy attacks and defenses in machine learning systems. He is also interested in wireless network security and privacy, device fingerprinting, and privacy-preserving network protocol design. His work has been published in top-tier venues including IEEE INFOCOM, ACM CCS, CCR, and EACL, and he serves on the Program Committee of ACM CCS 2026.

Mathieu Cunche is currently a Professor at INSA Lyon and a researcher with Inria, France, where he is a member of the PRIVATICS team hosted by the CITI Laboratory. Previously, he was an Associate Professor in the same environment from 2012 to 2023. Before joining INSA Lyon, he was a post-doctoral researcher with NICTA, Sydney, Australia, from 2010 to 2012.

He obtained the Habilitation à Diriger des Recherches (HDR) from the University of Lyon in 2021 and the Ph.D. degree in computer science from the University of Grenoble, France, in 2010. In 2006, he received an engineering degree from ENSIMAG (Grenoble INP) and a Master's degree in Cryptography, Coding, and Security from Grenoble University.

His research focuses on privacy and security issues in information and communication technologies, with a particular emphasis on wireless networks, mobile systems, and the Internet of Things. He teaches computer science, security, and privacy at INSA Lyon and is actively involved in standardization activities within international organizations, including the IETF and IEEE 802.

Anna Maria Mandalari (Member, IEEE) is a Lecturer in Communications and Networking with the Department of Electronic and Electrical Engineering, University College London, where she is also the Deputy Director of the UCL Institute of Communications and Connected Systems (ICCS), the Director of the SafeNetIoT Laboratory and the Programme Director of the M.Sc. in Internet Engineering and Telecommunications. She is an Honorary Research Fellow with Imperial College London and a Visiting Assistant Professor with Yokohama National University, Japan. Her research interests include cybersecurity and privacy of the Internet of Things, networking and communication systems, Internet measurement, and the security and resilience of connected and wearable systems.

Dr. Mandalari is a member of several professional, policy and standardization bodies, including being Chair of the IoT WG at RIPE, part of the executive board of the IoT Security Foundation, and Secretariat of ETSI CYBER EUSR WG.