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

Andrew Losty[1], Abhishek K. Mishra[2], Mathieu Cunche[2], Anna Maria Mandalari[1]
[1]University College London, [2]INSA-Lyon, Inria, Univ. of Lyon, CITI Lab

SYNOPSIS

The Domain Name System (DNS) is vital for Internet operation, but its lack of standards for Internet of Things (IoT) devices raises security and reliability concerns. This paper investigates inconsistencies in IoT DNS operations, revealing both security risks and irregular behaviors. We analyze DNS on a large IoT testbed through passive traffic inspection and active testing, uncovering serious anomalies. Our findings highlight vulnerabilities to cache poisoning, fingerprinting, and DoS attacks. We assess standardization gaps in IoT DNS security and move towards proposing guidelines to enhance resilience.

ACM Reference Format:
Andrew Losty[1], Abhishek K. Mishra[2], Mathieu Cunche[2], Anna Maria Mandalari[1], [1]University College London, [2]INSA-Lyon, Inria, Univ. of Lyon, CITI Lab, . 2025. Towards Operational and Security Best Practices for DNS in the Internet of Things. In *Applied Networking Research Workshop (ANRW '25), July 22,2025, Madrid, Spain.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3744200.3744764

1 INTRODUCTION

The Domain Name System (DNS) is crucial for Internet connectivity, translating domain names into IP addresses. However, the lack of standards that define DNS behavior for Internet of Things (IoT) devices raises concerns about their operational consistency, security, and efficiency.

Leveraging a large-scale IoT testbed and conducting hundreds of automated experiments, we systematically analyze the DNS behavior of IoT devices, revealing operational discrepancies such as frequent DNS queries, failure to adhere to Time-To-Live (TTL) values, reliance on hard-coded DNS resolvers, and inconsistent retry mechanisms. It also evaluates IoT adoption of secure DNS technologies such as DNS over HTTPS (DoH), DNS over TLS (DoT), DNSSEC, and IPv6 support on IoT devices.

Applied Networking Research Workshop (ANRW '25), July 22,2025, Madrid, Spain, 2025.

ACM ISBN 979-8-4007-2009-3/2025/07
https://doi.org/10.1145/3744200.3744764

Although RFC 5452 was published in 2009 [37], many devices exhibit serious security flaws, such as fixed source ports and predictable transaction IDs, that leave them vulnerable to DNS spoofing and cache poisoning. Additionally, predictable query behaviors expose devices to fingerprinting and traffic analysis attacks. With the growing prevalence of IoT devices, these inconsistencies pose risks to network security and stability.

This study emphasizes the need for standardized DNS handling practices to improve security, efficiency, and interoperability in IoT networks. We aim to compile all our findings/irregularities and turn them into specific guidelines/recommendations for IoT devices.

2 NEED FOR IOT DNS GUIDELINES

2.1 Limited IoT resources

IoT devices are subject to CPU and energy limitations that may restrict their ability to perform complex tasks, potentially hindering support for both encryption (DoH/DoT) and data integrity/authentication (DNSSEC) [20, 34]. Limited memory capacity constrains DNS caching, resulting in increased latency and higher network utilization [39].

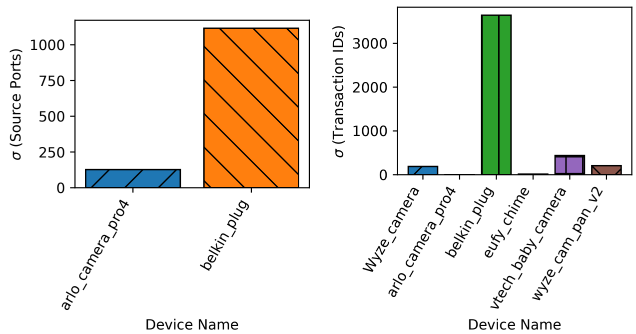
2.2 Absence in existing frameworks

DNS operations were initially defined in 1983 by RFCs 882 and 883 and later superseded by RFCs 1034 and 1035 [1–4]. Security standards were introduced through RFCs 8484 (`DNS over HTTPS`) [35], 7858 (`DNS over TLS`) [36], and `DNSSEC` (RFCs 4033–4035) [36, 40–42]. While standards define DNS operations, they lack explicit guidance for IoT devices.

European Telecommunications Standards Institute (`ETSI`): Seven standards are examined to identify operational recommendations for DNS security in IoT devices; none mandate IoT support for DNSSEC, DNS over HTTPS (DoH), or DNS over TLS (DoT). Although some reference DNS in general terms, none address IoT-specific DNS security or operations [23–29].

National Institute of Standards and Technology (`NIST`): This study reviews all relevant NIST standards to identify operational controls for DNS services on IoT platforms; however, it does not identify any specific controls [6, 9, 21, 30–33].

European Commission: Provides a comprehensive cybersecurity framework that is applicable to all products with



(a) Source ports. **(b) Transaction IDs.**

Figure 1: Poor randomness in DNS query fields.

digital elements. However, the `framework` lacks specific recommendations for `IoT DNS` [5].

ISO/IEC (International Organization for Standardization / International Electrotechnical Commission): Seven standards related to IoT security, interoperability, and cybersecurity are reviewed. However, no pertinent references to IoT DNS are identified [8, 10–18].

3 TOWARDS IOT DNS BEST PRACTICES

We perform a passive evaluation of IoT devices with respect to regular DNS traffic, and we also aim to actively evaluate devices in the presence of potential malicious actors.

3.1 Testbed and Dataset Collection

We analyze 30 consumer IoT devices from various categories, representing a typical smart home network: Appliance (4), Baby Monitor (2), Camera (5), Doorbell (4), Hub (2), Light (6), Pet (2), Plug (1), Medical (1), Sensor (2), and Speaker (5).

3.2 Uncovering DNS Anomalies Passively

Compliance to secure/privacy-preserving standards: We reveal *no support* for encrypted DNS (DoH/DoT), leaving devices vulnerable to interception and manipulation. Additionally, *no device implements* DNSSEC, increasing susceptibility to DNS spoofing and cache poisoning. Furthermore, five devices *use hard-coded DNS servers*, potentially bypassing security monitoring.

Irregularities in setting packet fields: We find considerable inconsistencies in DNS query behavior, such as *failure to follow* Time-To-Live (TTL) values, resulting in unpredictable intervals between queries. Some devices made an unexpectedly high number of domain queries, showing extreme fluctuations in query frequency and *increasing DNS queries tenfold when a resolver is unavailable*. We observe limited support for *EDNS(0)*, which causes devices to fragment frames for queries exceeding 512 bytes and thereby reduces their efficiency.

Poor source port randomization in requests: Several IoT devices *fail to properly randomize source port numbers* in DNS queries, increasing susceptibility to DNS cache poisoning attacks. Although most operating systems comply with RFC-6335 [22] using dynamic source ports in the 49152–65535 range, and some platforms support broader ranges [7], we observe that certain IoT devices operate within significantly narrower ranges, with a standard deviation (σ) of ≤ 1000. As shown in Figure 1a, devices such as (`arlo_camera_pro4`) and (`belkin_plug`) exhibit extremely poor randomization.

Non-randomized transaction IDs: Several IoT devices demonstrate insufficient DNS Transaction ID randomization, with some failing to implement effective randomization or employing predictably sequential values within the 16-bit range (0–65535). This deficiency in entropy increases susceptibility to DNS spoofing, man-in-the-middle (MITM), and amplification attacks. As illustrated in Figure 1b, the low standard deviation of transaction IDs in devices such as cameras (Wyze_camera), smart plugs (belkin_plug), and doorbells (eufy_chime) reflects inadequate randomization.

3.3 Active Evaluation – Advancing Inquiry

Mitigating Malformed RR Exploits: Malformed Resource Records (RRs) pose security risks by enabling manipulation of encodings, injection of invalid values, and abuse of optional fields [38, 43]. We test IoT devices to evaluate resilience by altering RR types, padding lengths, domain/IP values, answered RR content, encoding, etc.

TTL Management: TTL manipulation poses risks of cache poisoning and query inconsistency. [19]. We subject test devices to deliberate manipulation of TTL values in DNS responses to create conditions associated with an increased risk of poisoning. We also examine the handling of extreme TTL values by injecting abnormal values into DNS responses and analyzing the responses of IoT devices. '

Denial-of-Service Protection: To mitigate DoS attacks originating from compromised IoT devices, we focus on query anomaly detection, identifying deviations in DNS query patterns to detect botnet-driven DDoS and exfiltration attempts. We also stress-test the resolvers with queries.

4 CONCLUSION

As IoT devices continue to proliferate and integrate into critical infrastructure, ensuring their secure and efficient operation becomes increasingly vital. Our systematic analysis of DNS behavior across a range of IoT devices reveals alarming inconsistencies in their DNS practices.

Our findings underscore the urgent need for clear, standardized DNS handling practices tailored to the IoT ecosystem. In the absence of such standards, device manufacturers risk perpetuating insecure behaviors that threaten the stability and security of global networks. As a next step, we are consolidating our observations into actionable recommendations and best practices to guide the development of more robust and secure IoT DNS implementations.

REFERENCES

[1] 1983. *Domain names: Concepts and facilities*. Request for Comments RFC 882. Internet Engineering Task Force. https://doi.org/10.17487/RFC0882 Num Pages: 31.

[2] 1983. *Domain names: Implementation specification*. Request for Comments RFC 883. Internet Engineering Task Force. https://doi.org/10.17487/RFC0883 Num Pages: 74.

[3] 1987. *Domain names - concepts and facilities*. Request for Comments RFC 1034. Internet Engineering Task Force. https://doi.org/10.17487/RFC1034 Num Pages: 55.

[4] 1987. *Domain names - implementation and specification*. Request for Comments RFC 1035. Internet Engineering Task Force. https://doi.org/10.17487/RFC1035 Num Pages: 55.

[5] 2013. Cyber Resilience Act (CRA) | Updates, Compliance, Training. https://www.european-cyber-resilience-act.com/

[6] 2013. Cybersecurity Framework. *NIST* (Nov. 2013). https://www.nist.gov/cyberframework Last Modified: 2025-05-20T15:15-04:00.

[7] 2020. Configuring Kernel Parameters for Linux. https://docs.oracle.com/en/enterprise-manager/cloud-control/enterprise-manager-cloud-control/13.4/emrel/configuring-kernel-parameters-linux-1.html Publisher: June2020.

[8] 2020. ISO/IEC 21823-2:2020 - Internet of Things (IoT) – Interoperability for IoT systems – Part 2: Transport interoperability. https://www.iso.org/standard/80986.html

[9] 2021. NISTIR 8259 Series. *NIST* (Nov. 2021). https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series Last Modified: 2021-11-16T14:47-05:00.

[10] 2022. ISO/IEC 27002:2022 - Information technology – Security techniques – Code of practice for information security controls. https://www.iso.org/standard/75652.html

[11] 2022. ISO/IEC 29192-8:2022/CD Amd 1 - Information security – Lightweight cryptography – Part 8: Authenticated encryption. https://www.iso.org/standard/90708.html

[12] 2023. ISO/IEC 30161-2:2023 - Internet of Things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points. https://www.iso.org/standard/86671.html

[13] 2023. ISO/IEC TR 30164:2020 - Internet of Things (IoT) — Edge computing. https://www.iso.org/standard/53284.html

[14] 2024. ISO/IEC 27001:2022/Amd 1:2024 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/88435.html

[15] 2024. ISO/IEC 27403:2024 - Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics. https://www.iso.org/standard/78702.html

[16] 2024. ISO/IEC 30141:2024 - Internet of Things (IoT) – Reference Architecture. https://www.iso.org/standard/88800.html

[17] 2024. ISO/IEC FDIS 27404 - Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT. https://www.iso.org/standard/80138.html

[18] 2024. ISO/IEC TS 30149:2024 - Internet of Things (IoT) — Trustworthiness principles. https://www.iso.org/standard/53269.html

[19] Oscar Arana, Hector Benítez-Pérez, Javier Gomez, and Miguel Lopez-Guerrero. 2021. Never Query Alone: A distributed strategy to protect Internet users from DNS fingerprinting attacks. *Computer Networks* 199 (2021), 108445.

[20] Abdullah Aydeger, Sanzida Hoque, Engin Zeydan, and Kapal Dev. 2025. Analysis of Robust and Secure DNS Protocols for IoT Devices. https://doi.org/10.48550/arXiv.2502.09726 arXiv:2502.09726 [cs].

[21] Information Technology Laboratory Computer Security Division. 2020. Control Baselines: NIST Publishes SP 800-53B | CSRC. https://csrc.nist.gov/news/2020/control-baselines-nist-publishes-sp-800-53b

[22] Michelle Cotton, Lars Eggert, Joseph D. Touch, Magnus Westerlund, and Stuart Cheshire. [n. d.]. Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. https://doi.org/10.17487/RFC6335 Num Pages: 33.

[23] ETSI. 2016. ETSI TR 103 375 V1.1.1 (2016-10): SmartM2M; IoT Standards Landscape and Future Evolutions. https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf. European Telecommunications Standards Institute.

[24] ETSI. 2017. ETSI GR IP6 008 V1.1.1 (2017-06): Deployment of IPv6-based Internet of Things. https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_ip6008v010101p.pdf. European Telecommunications Standards Institute.

[25] ETSI. 2021. ETSI TS 103 701 V1.1.1 (2021-08): Cyber Security for Consumer Internet of Things – Conformance Assessment of Baseline Requirements. https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf. European Telecommunications Standards Institute.

[26] ETSI. 2022. ETSI TR 103 621 V1.1.1 (2022-03): Guide to Cyber Security for Consumer Internet of Things. https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.01.01_60/tr_103621v010101p.pdf. European Telecommunications Standards Institute.

[27] ETSI. 2023. ETSI TS 103 457 V1.2.1 (2023-03): Trusted Cross-Domain Interface – Interface to Offload Sensitive Functions to a Trusted Domain. https://www.etsi.org/deliver/etsi_ts/103400_103499/103457/01.02.01_60/ts_103457v010201p.pdf. European Telecommunications Standards Institute.

[28] ETSI. 2024. ETSI EN 303 645 V3.1.3 (2024-09): Cyber Security for Consumer Internet of Things – Baseline Requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf. European Telecommunications Standards Institute.

[29] ETSI. 2024. ETSI TS 103 645 V3.1.1 (2024-01): Cyber Security for Consumer Internet of Things – Baseline Requirements. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/03.01.01_60/ts_103645v030101p.pdf. European Telecommunications Standards Institute.

[30] Michael Fagan, Katerina Megas, Paul Watrobski, Jeffrey Marron, and Barbara Cuthill. 2022. *Profile of the IoT Core Baseline for Consumer IoT Products*. Technical Report NIST Internal or Interagency Report (NISTIR) 8425. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8425

[31] Michael Fagan, Katerina Megas, Paul Watrobski, Jeffrey Marron, Barbara Cuthill, David Lemire, Brad Hoehn, and Chris Evans. 2024. *Recommended Cybersecurity Requirements for Consumer-Grade Router Products*. Technical Report NIST Internal or Interagency Report (NISTIR) 8425A. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8425A

[32] Joint Task Force. 2020. *Security and Privacy Controls for Information Systems and Organizations*. Technical Report NIST Special Publication (SP) 800-53 Rev. 5. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

[33] Joint Task Force. 2022. *Assessing Security and Privacy Controls in Information Systems and Organizations*. Technical Report NIST Special Publication (SP) 800-53A Rev. 5. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53Ar5

[34] Hamed HaddadPajouh, Ali Dehghantanha, Reza M. Parizi, Mohammed Aledhari, and Hadis Karimipour. 2021. A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things* 14 (June 2021), 100129. https://doi.org/10.1016/j.iot.2019.100129

[35] Paul E. Hoffman and Patrick McManus. 2018. *DNS Queries over HTTPS (DoH)*. Request for Comments RFC 8484. Internet Engineering Task Force. https://doi.org/10.17487/RFC8484 Num Pages: 21.

[36] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessels, and Paul E. Hoffman. 2016. *Specification for DNS over Transport Layer Security (TLS)*. Request for Comments RFC 7858. Internet Engineering Task Force. https://doi.org/10.17487/RFC7858 Num Pages: 19.

[37] Bert Hubert and Remco Mook. 2009. *Measures for Making DNS More Resilient against Forged Answers*. Request for Comments RFC 5452. Internet Engineering Task Force. https://doi.org/10.17487/RFC5452 Num Pages: 18.

[38] Xiang Li, Wei Xu, Baojun Liu, Mingming Zhang, Zhou Li, Jia Zhang, Deliang Chang, Xiaofeng Zheng, Chuhan Wang, Jianjun Chen, et al. 2024. TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 181–181.

[39] Marta Moure-Garrido, Carlos Garcia-Rubio, and Celeste Campo. 2024. Reducing DNS Traffic to Enhance Home IoT Device Privacy. *Sensors* 24, 9 (Jan. 2024), 2690. https://doi.org/10.3390/s24092690 Number: 9 Publisher: Multidisciplinary Digital Publishing Institute.

[40] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. *DNS Security Introduction and Requirements*. Request for Comments RFC 4033. Internet Engineering Task Force. https://doi.org/10.17487/RFC4033 Num Pages: 21.

[41] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. *Protocol Modifications for the DNS Security Extensions*. Request for Comments RFC 4035. Internet Engineering Task Force. https://doi.org/10.17487/RFC4035 Num Pages: 53.

[42] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. *Resource Records for the DNS Security Extensions*. Request for Comments RFC 4034. Internet Engineering Task Force. https://doi.org/10.17487/RFC4034 Num Pages: 29.

[43] Giovanni Schmid. 2021. Thirty years of DNS insecurity: Current issues and perspectives. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2429–2459.