The need for regulation - DNS (Domain Name System) Security and Operations on Internet of Things (IoT) Platforms.

Andrew Losty, Dr. Anna Maria Mandalari
Department of Electronic and Electrical Engineering (EEE)

Research Questions.

What existing regulatory frameworks, governs DNS resolution behaviour in IoT devices.

Could new regulations help address IoT DNS security and operational conformance.

Passive analysis to assess IoT device support for Secure DNS (DoH[1], DoT[2], DNSSEC[3]) + assess operational behaviour.

Active analysis to evaluate IoT DNS deviations and their impact on security, performance, and privacy

([1] (DoH) DNS over HTTPS, [2] (DoT) DNS over TLS, [3] (DNSSEC) DNS Security Extensions)

Abstract

Internet of Things (IoT) devices are subject to unique limitations that influence the operation and security of DNS communications.

Our research aims to assess regulatory gaps in IoT DNS security and move towards proposing guidelines to enhance resilience. Standardised DNS practices are essential to securing IoT ecosystems and mitigating large-scale threats.

Assessment of IoT device DNS behaviour is made through both passive traffic inspection and active device probing. The results uncover serious operational anomalies and security vulnerabilities that can lead to cache poisoning, fingerprinting, and DoS attacks.

Limited IoT device resources

IoT devices face resource constraints that limit their ability to perform complex tasks. Cost, energy consumption, and size all constrain the processing capacity of the device.

Devices with limited CPU capacity may be unable to perform complex encryption as required by DoH and DoT, or the data integrity and authentication mechanisms in DNSSEC. Also, devices without secure storage may not be able to store the cryptographic keys or certificates as required by DNSSEC.
Limited memory hampers DNS caching, increasing latency and load.

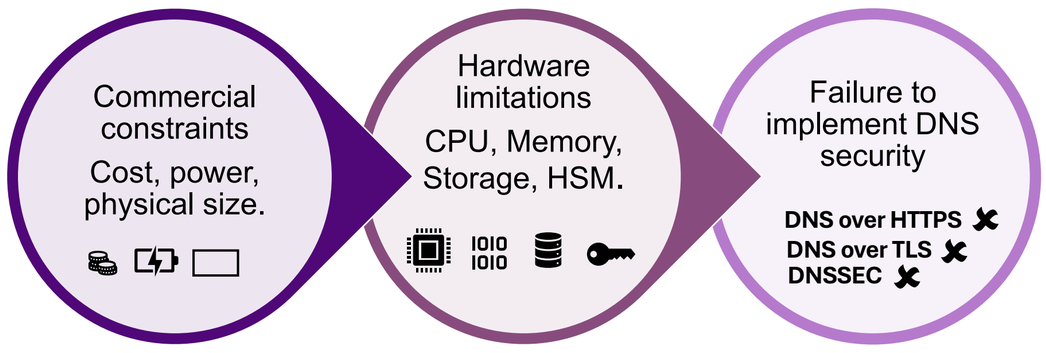

Figure 1: Limitation of DNS operations due to IoT platform restrictions

Methodology

Analysis of 30 consumer IoT devices that reflect a typical smart-home. Categories include: Appliance (4), Baby Monitor (2), Camera (5), Doorbell (4), Hub (2), Light (6), Pet (2), Plug (1), Medical (1), Sensor (2), and Speaker (5).

- Passive traffic analysis – determine security and operational behaviour.
- Active DNS analysis – determine behaviour when subject to malformed packet exploit, targeting buffer overflows or memory faults.

Existing regulation and standards

Regulations from major international bodies (e.g., ETSI, NIST, ENISA, ISO/IEC) are reviewed for DNS-specific controls on IoT devices. None mandate or recommend DNS-specific measures for IoT.

European Telecommunications Standards Institute (ETSI)			
ETSI EN 303 645	✗ DNS∩IoT ✓ DNS	ETSI TS 103 375	✗ DNS∩IoT ✗ DNS
ETSI EN 103 645 ETSI TR 103 621 ETSI GR IP6 008	✗ DNS∩IoT ✓ DNS	ETSI TS 103 701	✗ DNS∩IoT ✓ DNS
	✗ DNS∩IoT ✗ DNS	ETSI TS 103 457	✗ DNS∩IoT ✗ DNS
	✗ 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 NIST IR 8425A	✗ DNS∩IoT ✗ DNS	NIST IR 8425	✗ 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 30141:2018	✗ DNS∩IoT ✗ DNS	ISO/IEC 21823-2:2020 ISO/	✗ DNS∩IoT ✗ DNS
ISO/IEC 27001:2023+A1:2024 ISO/IEC	✗ DNS∩IoT ✗ DNS	IEC 27002:2022 ISO/IEC TS	✗ DNS∩IoT ✓ DNS
DIS 27404:2024 ISO/IEC 30161-2:2023	✗ DNS∩IoT ✗ DNS	30149:2024 ISO/IEC TR	✗ DNS∩IoT ✗ DNS
ISO/IEC 29192-8:2022	✗ DNS∩IoT ✗ DNS	30164:2020	✗ 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

Table 1. IoT DNS Regulations and Standards

Results

Analysis shows:

- All 30 devices fail to support encrypted DNS (DoH or DoT), which exposes them to interception and manipulation.
- All devices fail to implement DNSSEC, which increases their susceptibility to DNS spoofing and cache poisoning.
- Five devices use hard-coded DNS servers -, bypassing security monitoring and control mechanisms. Devices fail to adhere to received TTL.

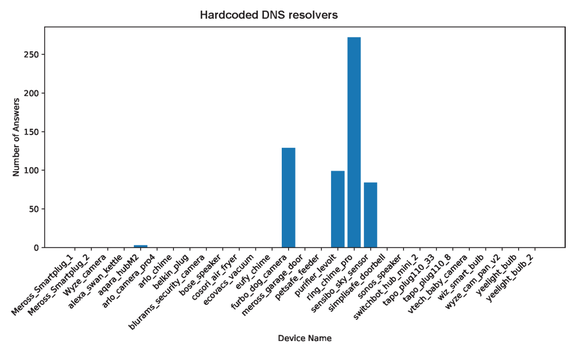

Figure 2. IoT Device "hardcoded" DNS addresses.

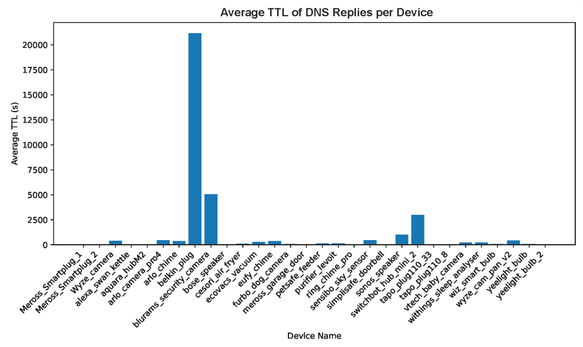

Figure 3. IoT Device Inconsistent TTL.

- Devices poorly randomize their Source-port numbers and Transaction-IDs in DNS queries. This creates a major DNS cache poisoning vulnerability.

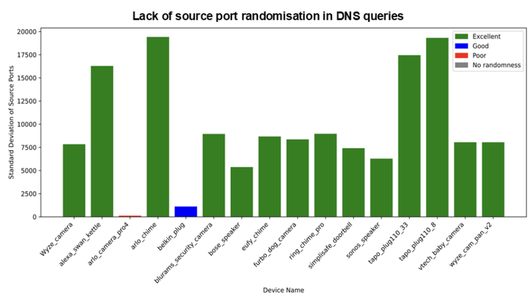

Figure 4. IoT Device poor Port randomisation.

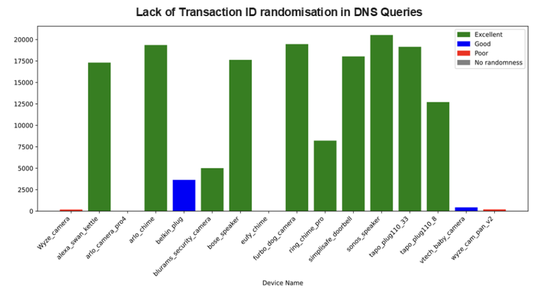

Figure 5. IoT Device poor Transaction ID randomisation.

Further Work

An IoT DNS regulation framework would provide a structured approach to mitigating inconsistencies in DNS operation and security. By implementing published guidelines that are adopted into global IoT governance, IoT stake-holders can enhance DNS security and prevent large-scale cyber threats.

E: andrew.losty.23@ucl.ac.uk
E: a.mandalari@ucl.ac.uk
T: +44 (0)771404 5924
T: +44 (0) 20 7679 7303 (int. 37303)
University College London, Roberts Building - Department of Electronic & Electrical Engineering, 1108 Torrington Place, London, WC1E 7JE, United Kingdom