IoT DNS Security and Privacy Guidelines

draft-mishra-iotops-iot-dns-guidelines-latest

Abhishek Mishra
Inria
abhishek.mishra@inria.fr

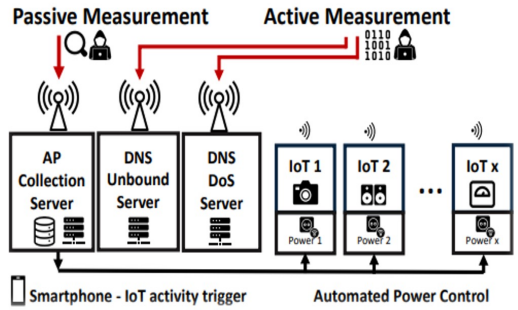
Jim Mozley
Infoblox
jmozley@Infoblox.com

IoT DNS Security and Privacy Guidelines

Why IoT-specific guidelines:

- Focuses on IoT-specific DNS threats, not seen in general OS behavior
- Resource constraints amplify DNS mis-implementation impact
- IoT devices typically lack local security agents
- Predictable DNS queries enable fingerprinting and attack profiling
- Maps multiple DNS RFCs to observed IoT vulnerabilities
- Aids mitigation by network security teams in large-scale IoT deployments
- Guides manufacturers about the evaluation of software's IoT DNS handling

Sample of 30 IoT devices reflecting Smart Home environment



Active experiments: crafted DNS responses, DNS amplification, RR duplication.

Passive experiments: capture operational and triggered DNS activity

Security:

- No support of DoH, DoT, DoQ
- Observed security vulnerabilities
- Vulnerable to response manipulation
- identifiable via traffic patterns

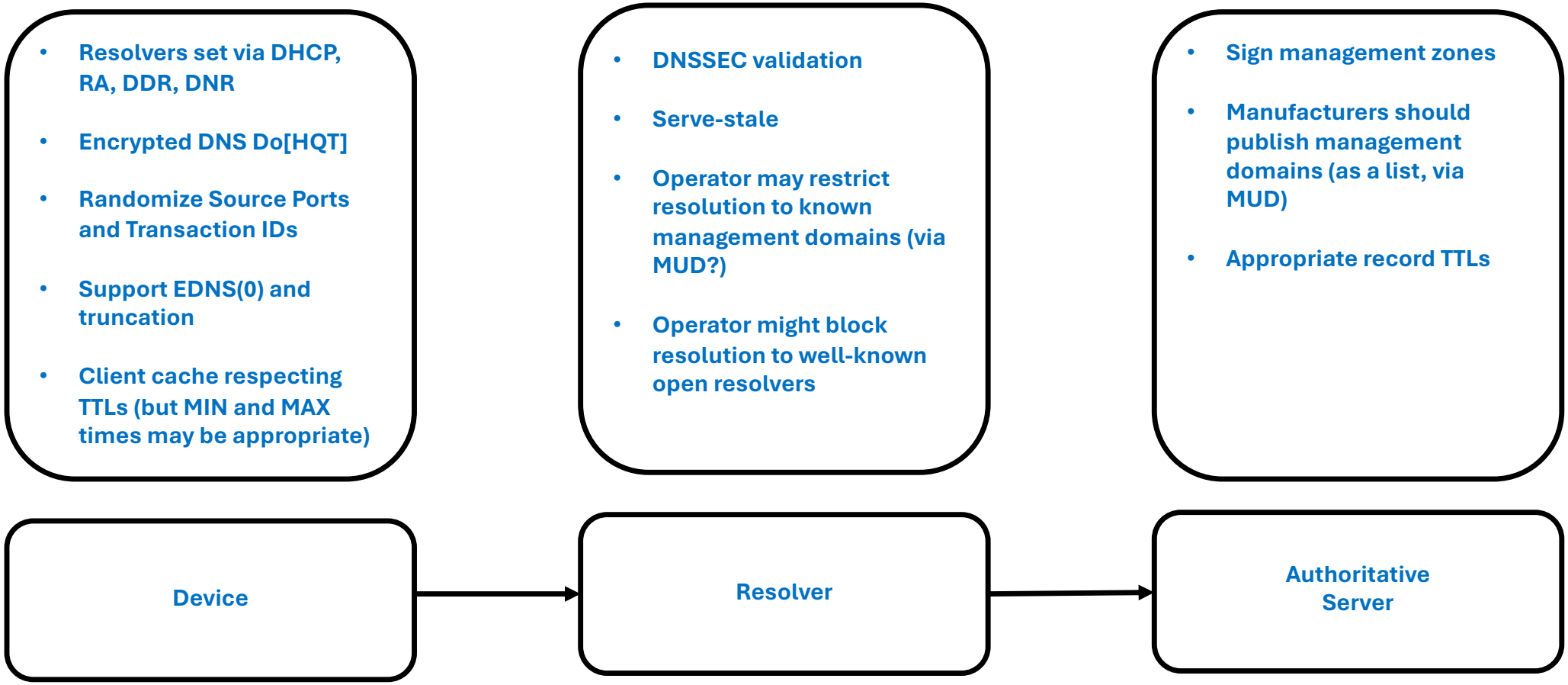
Behavior:

- Lack of TTL adherence and caching
- Hardcoded DNS servers
- High and repetitive query rates
- No support for EDNS(0)
- Limited IPv6 support

Regulatory Framework:

- Lack of existing DNS for IoT guidance from major international bodies (ETSI, NIST, ENISA, ISO/IEC)

Draft BCP


Resolvers set via DHCP, RA, DDR, DNR
Encrypted DNS Do[HQT]
Randomize Source Ports and Transaction IDs
Support EDNS(0) and truncation
Client cache respecting TTLs (but MIN and MAX times may be appropriate)
DNSSEC validation
Serve-stale
Operator may restrict resolution to known management domains (via MUD?)
Operator might block resolution to well-known open resolvers
Sign management zones
Manufacturers should publish management domains (as a list, via MUD)
Appropriate record TTLs
Device
Resolver
Authoritative Server

Progressing the BCP

- Feedback appreciated ☺
- Do we need more “**why?**”
- Is it realistic to put more “DNS intelligence” into the IoT device stub resolver e.g. use dnsmask?
- OR
- Is mitigate in the network resolver better?