The path from an Internet registry to an IoT registry based on DNS - Abstract

Sandoche Balakrichenan – Afnic

sandoche.balakrichenan@afnic.fr

My DINR 2016 abstract was titled - "*Why DNS should be the naming service for the Internet of Things (IoT)?*" This abstract is based on the fact that even though there are multiple naming conventions in IoT, most have certain standard features: hierarchical allocation, decentralized control, and allocation nature ensures no duplicity. These features are similar to the domain name allocation and management, and thus, naming conventions used in IoT could leverage the DNS infrastructure and software for ***allocation*** and ***resolution***. Two IoT standards [1] [2] where we had been active contributors had standardised our hypothesis, and there are other standards such as Object Resolution System standardised jointly by the ITU-T and ISO/IEC, and the Handle system standardised by the ISO that uses the DNS infrastructure to resolve the IoT identifiers to its related service on the Internet.

For DINR 2020, the hypothesis was that the DNS and its ***security*** extensions such as DNSSEC (Domain Name System Security Extensions), DANE (DNS Authentication of Named Entities) with TLS (Transport Layer Security) could be used as the PKI (Public Key Infrastructure), ensuring end-to-end security. End-to-End security between the IoT end-device communicating via a RF (Radio Frequency) signal to a RGW (Radio Gateway) and between the RGW and the cloud service on the Internet, wherein the communication is via IP (Internet Protocol). In order to validate this hypothesis, we are working with multiple Industrial and Academic partners on a French Government funded project - DiNS (DNS Naming and Services for Secure Seamless IoT) [3]. As a benchmark, we propose to validate our hypothesis on one of the most constrained IoT networks - Long Range Wide Area Network (LoRaWAN). If the DNS based PKI is validated with LoRaWAN having constraints such as the maximum frame size of 51 bytes (or 222 bytes for lower spreading factors) and latency requirements of two seconds for default uplink/downlink, we believe that it will be applicable for all IoT networks.

The missing segment in the two previous abstract submissions are – ***Privacy***. The DNS infrastructure, its security extensions, and other Open Internet Standards (e.g., TLS) could provide IoT provisioning, service resolution, and communication channel security. However, they do not protect the identities of the source, the end-points and the metadata, thus enabling the (monetarily valuable) option of reconstructing contexts of the IoT communication. To address this issue, we are working on a German/ French Government funded project – PIVOT (Privacy-Integrated design and Validation in the constrained IoT) [4]. The proposed architecture also will be validated with LoRaWAN.

In this long journey, we have evolved from idea to implementation to peer-reviewed articles to standards. The journey is successful only when the proposed architecture is applied in a real-world use case. To achieve this objective, we are working on a federated roaming infrastructure for IoT called ***IoTRoam*** [5] [6]. The objective with IoTRoam is to achieve the same service as that of cellular or Wi-Fi Roaming built on a DNS based global resolution, security and privacy infrastructure.

In this talk, I will provide a panoramic overview of the features of IoT registry using DNS – features implemented, issues still to be resolved and how it is applied for the IoTRoam use case?

References:

[1]. Object Naming Service. *https: / / www. gs1. org / sites / default/files/docs/epc/ons_2_0_1-standard-20130131. pdf.* 2013.

[2]. LoRaWAN® Backend Interfaces Technical Specification (TS002-1.1.0). https: / / lora - alliance . org / wp - content / uploads/2020/11/TS002-1.1.0_LoRaWAN_Backend_ Interfaces.pdf.

[3]. https://anr.fr/Project-ANR-19-CE25-0009 - DiNS (DNS Naming and Services for Secure Seamless IoT)

[4]. https://pivot-project.info/ - PIVOT (Privacy-Integrated design and Validation in the constrained IoT)

[5]. https://github.com/AFNIC/IoTRoam-Tutorial

[6]. "*IoTRoam: design and implementation of a federated IoT roaming infrastructure using LoRaWAN*" – Sandoche Balakrichenan, Antoine Bernard, Michel Marot, Benoît Ampeau, Globecom 2021