

DNS Threat and Privacy Internet Research

Introducing the DNS TAPIR project

Lars-Johan Liman, Netnod
2024-06-10 ICANN 80 Tech Day



The Problem

- **Privacy leaks** – By querying DNS, you create data about what you do, which servers you communicate with, and much more. This data is often used without respect to the user's privacy.
 - Unique DNS queries are used as a "replacement" for HTTP Cookies, circumventing cookie regulations.
- **Cyber Security** – Malicious software uses DNS for communication and pinging home. These cyber operations need to be monitored, and reactions need to be formed.



What can be done?

- DNS resolvers, the servers that handle queries from and responses to clients, produce logs that include privacy data.
- This data can be aggregated, gathered and analysed almost in real time.
- By collecting only select data, and aggregating it sensibly, a reasonable level of anonymity – a.k.a. "pseudonymity" – can be achieved in the data processed.
- One result of such analyses is threat warnings, which can be used to configure filters to help protect users and networks.

Aggregated, pseudonymised DNS resolver logs can be analysed and used for cyber security monitoring without privacy issues.



The Robust DNS Project

Goal:

- To produce an open-source software design for robust DNS resolver service that can be deployed by anyone who wishes to participate.
- To design software for a central analysis function, which receives pseudonymised data from these resolvers and which feeds threat information back to the resolvers.
- We want to develop tools that anyone may operate.

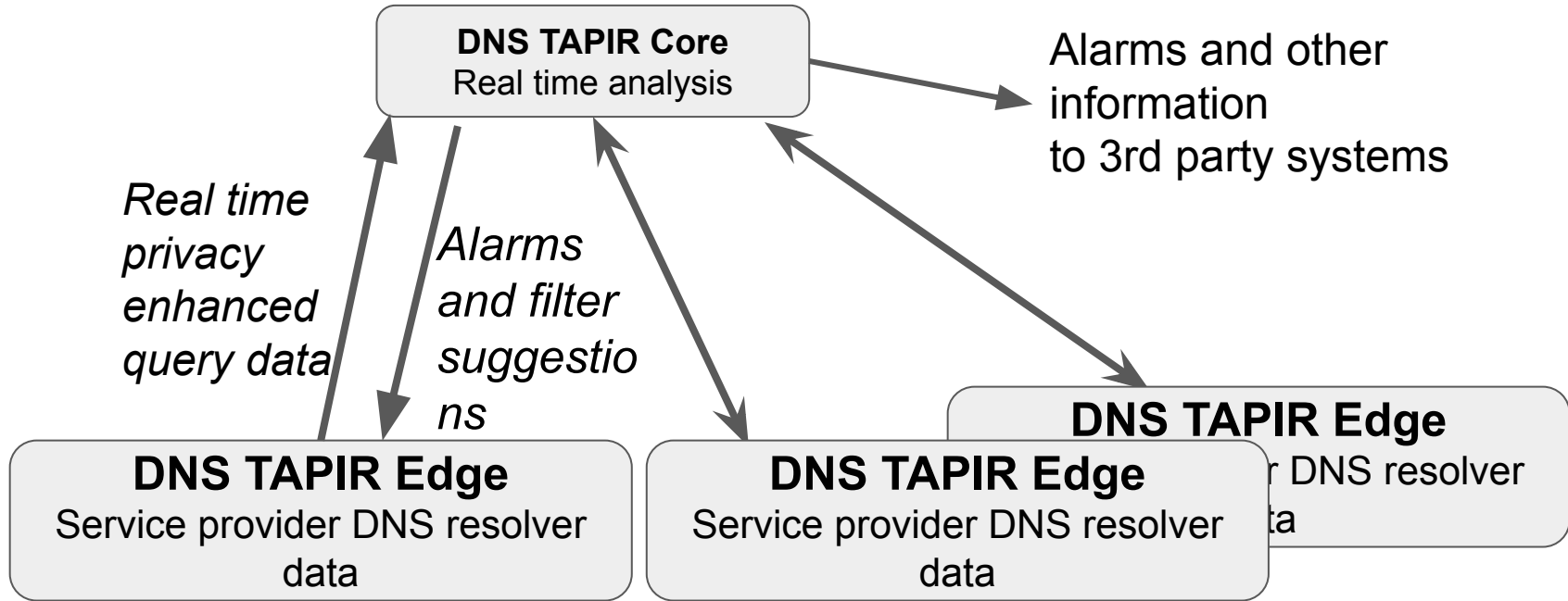


The DNS TAPIR software

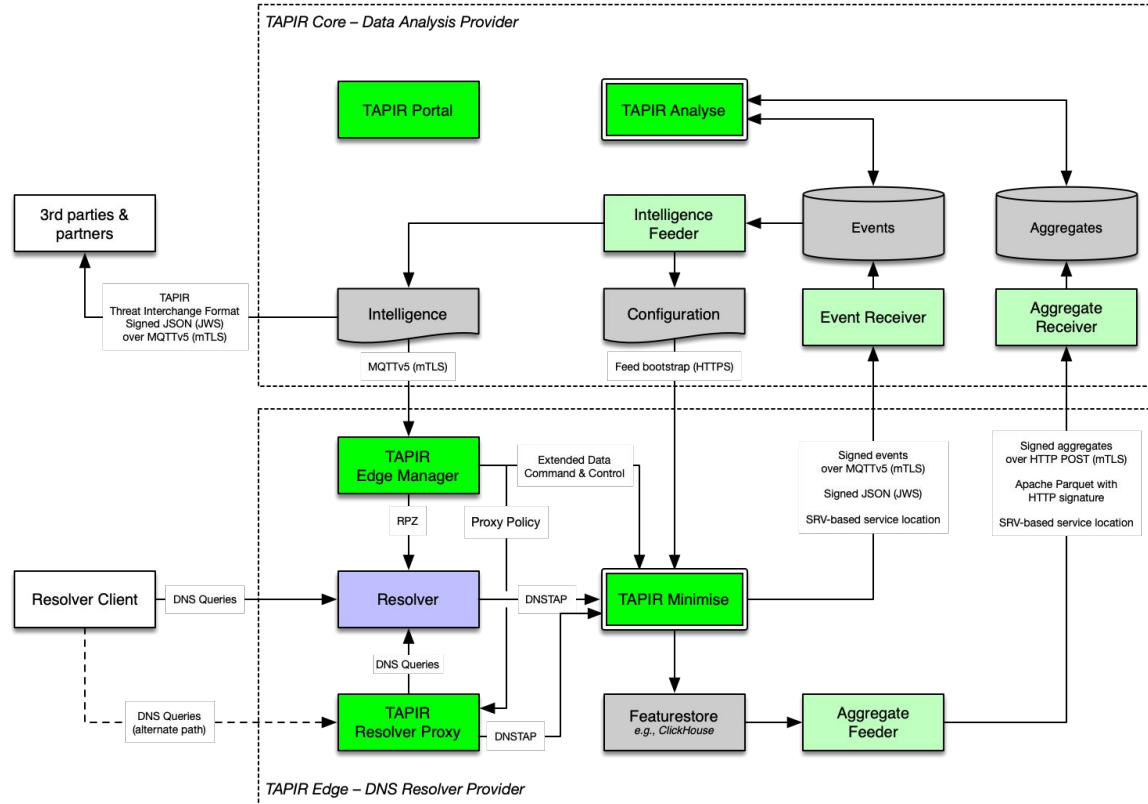
- **DNStapir Edge** – A service that runs close to a DNS resolver and aggregates logs and forwards data to the central service. Intended to be installed in service providers' networks and similar places.
- **DNStapir Core** – The core service that aggregates, analyses, and annotates data, in order to produce different alerts. The cloud service can be divided into a federated network of instances without affecting the user's privacy.

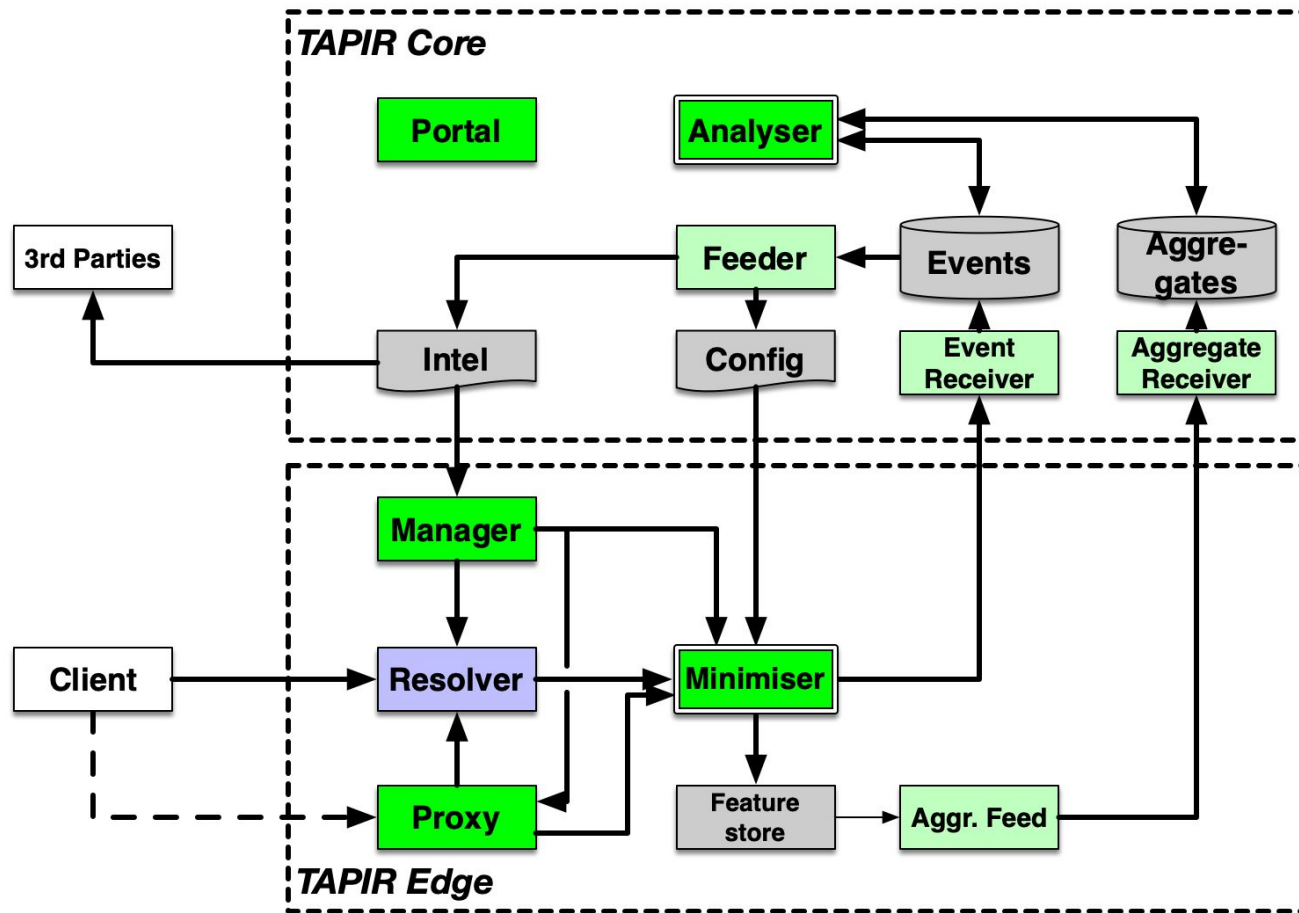


The DNS tapir service overview



Detailed System Overview



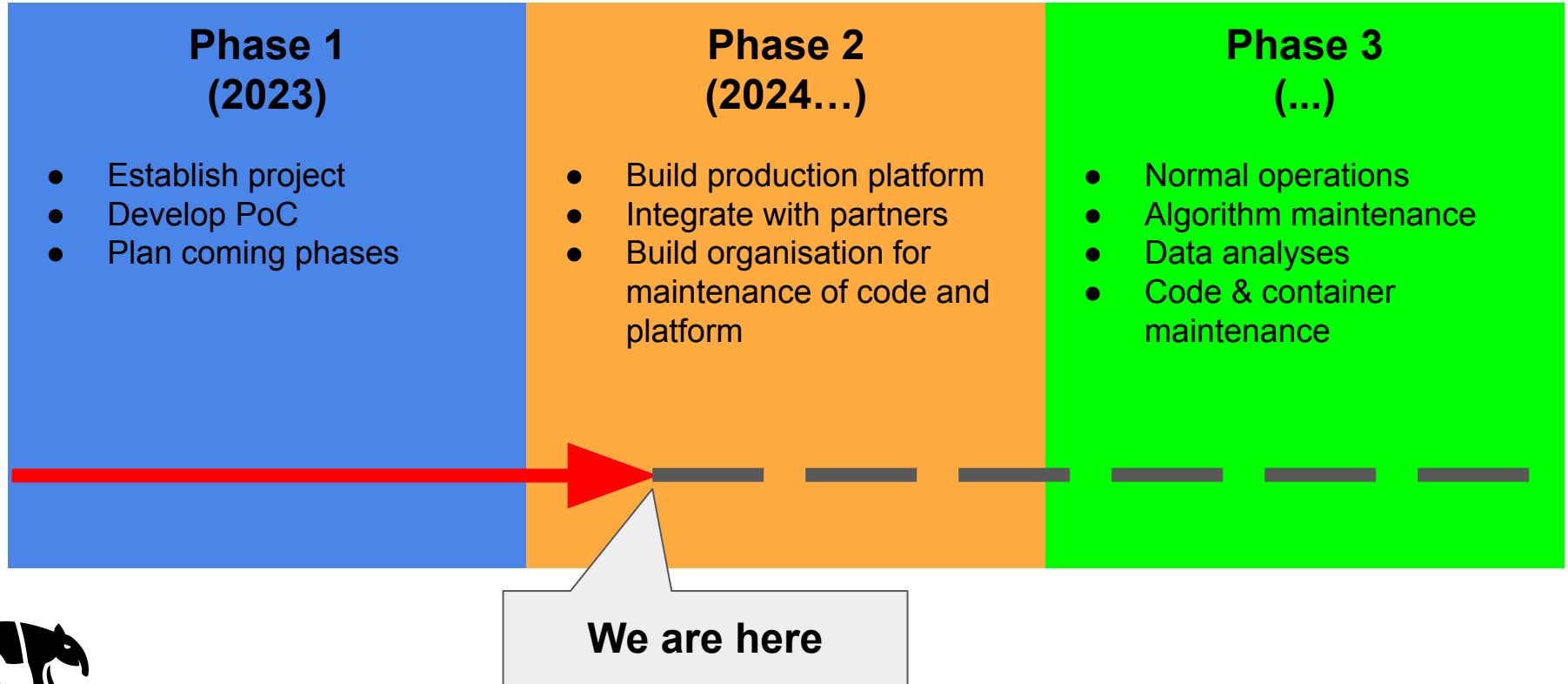


Next steps for DNS TAPIR and **[Current Status]**

- Finalise the implementation of a proof-of-concept model. **[Real Soon Now™]**
- Set up core services for development and testing. **[Done]**
- Set up a core service for early adopters. **[Being developed]**
- Discuss with service providers, public sector and enterprises on how to cooperate to strengthen the cyber security for everyone. **[Ongoing]**
- Find a long-term funding solution for the open-source project as well as for operations of the core analysis service. **[Not started]**



DNS TAPIR Project Phases



Partners in Phase 1 & 2

Architecture and Proof of Concept

- Main funding by Swedish Post and Telecom Authority (PTS).
- Resources provided by Sunet, the Swedish Internet Foundation (.SE), and Netnod.
- Select partners – mainly technical experts, project administration, and a reference group.



www.dnstapir.se

