DNS Threat and Privacy Internet Research

Introducing the DNS TAPIR project

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?

- The 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

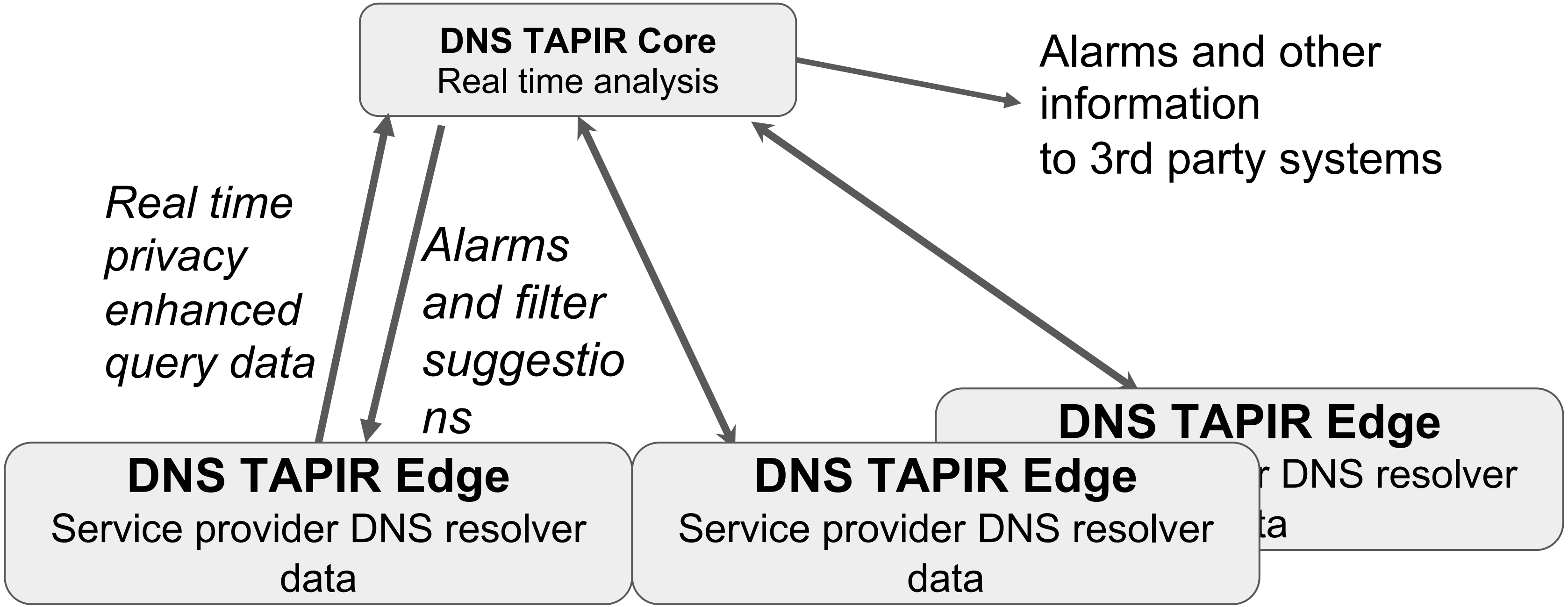
Goal:

- 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.

The DNS TAPIR software

- **DNStapir Edge** – A service that runs close to a DNS resolver and aggregates logs and forwards data to the cloud service. Thought to be installed in service providers' networks and similar places.
- **DNStapir Core** – The cloud 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



DNS TAPIR Core
Real time analysis

Alarms and other information
to 3rd party systems

Real time privacy enhanced query data

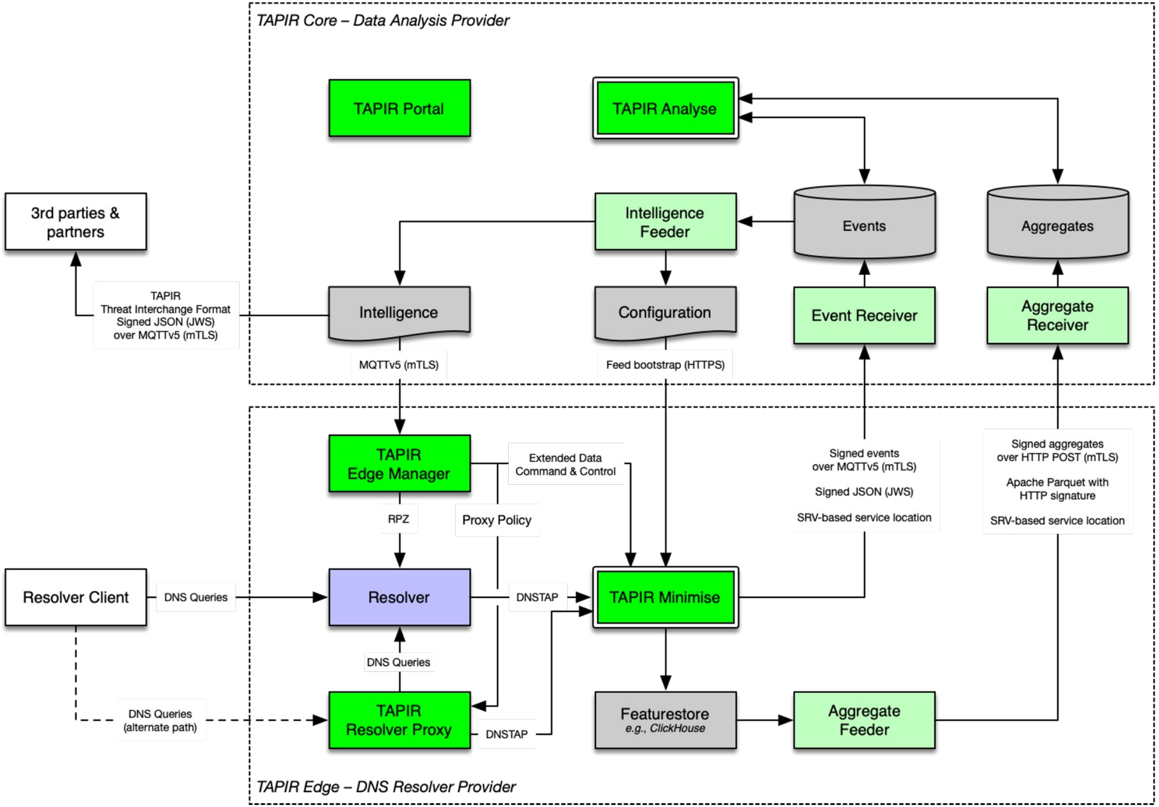
Alarms and filter suggestio ns

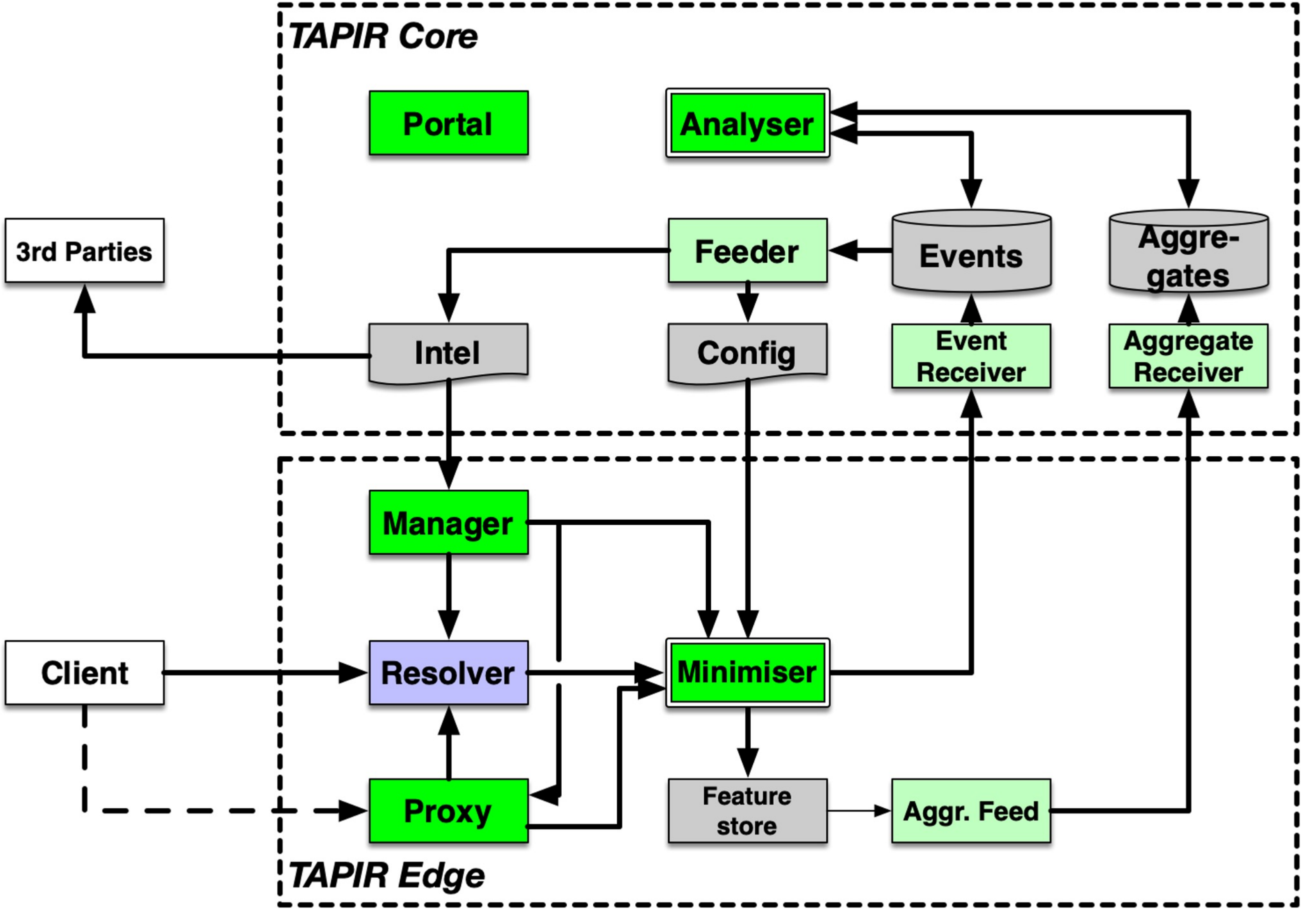
DNS TAPIR Edge
Service provider DNS resolver data

DNS TAPIR Edge
Service provider DNS resolver data

DNS TAPIR Edge
r DNS resolver
ta

Detailed System Overview




TAPIR Core
Portal
Analyser
3rd Parties
Feeder
Events
Aggre-
gates
Intel
Config
Event
Receiver
Aggregate
Receiver
Manager
Client
Resolver
Minimiser
Proxy
Feature
store
Aggr. Feed
TAPIR Edge

Next steps for DNS TAPIR

- Finalise the design and implementation of a proof-of-concept model.
- Set up cloud services for development and testing.
- Set up a cloud service for early adopters.
- Discuss with service providers, public sector and enterprises on how to cooperate to strengthen the cyber security for everyone.
- Find a long-term funding solution for the open-source project as well as for operations of the core analysis service.

DNS TAPIR Project Phases

Phase 1
(2023)

- Establish project
- Develop PoC
- Plan coming phases

Phase 2
(2024…)

- Build production platform
- Integrate with partners
- Build organisation for maintenance of code and platform

Phase 3
(...)

- Normal operations
- Algorithm maintenance
- Data analyses
- Code & container maintenance

Partners in Phase 1
Architecture and Proof of Concept

- Main funding by Post & Telestyrelsen (PTS), the Swedish telecommunications regulator, for the “Robust DNS” project.
- Resources provided by Sunet, Internetstiftelsen, and Netnod.
- Select partners – mainly technical experts, project administration, and a reference group.

www.dnstapir.se