SSAC Work Session (3 of 3)

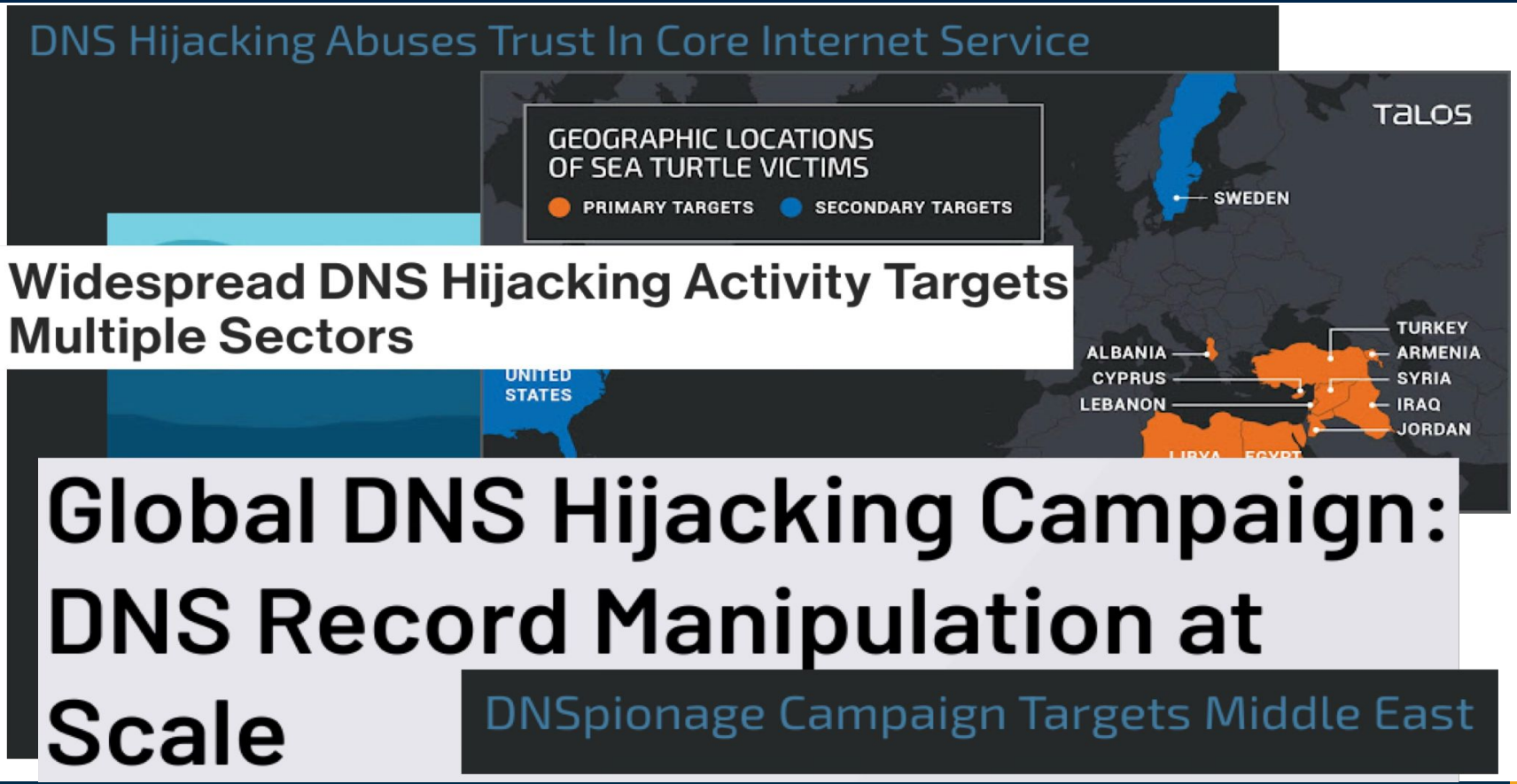
DNS Transparency WP

10 June 2026

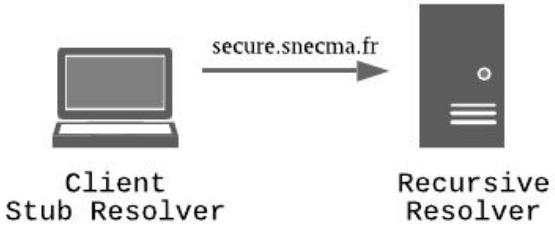
Agenda

1. Background
2. Discuss Access Models

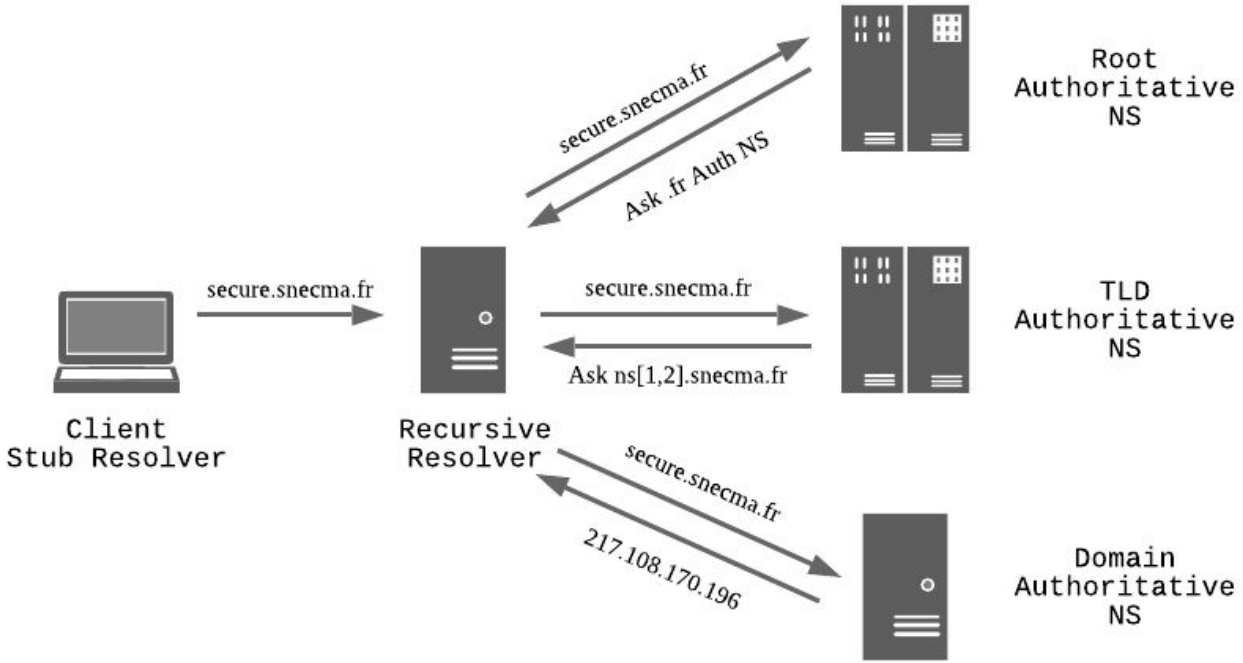
Motivation


DNS Hijacking Abuses Trust In Core Internet Service
GEOGRAPHIC LOCATIONS OF SEA TURTLE VICTIMS
PRIMARY TARGETS
SECONDARY TARGETS
Talos
SWEDEN
Widespread DNS Hijacking Activity Targets Multiple Sectors
UNITED STATES
ALBANIA
CYPRUS
LEBANON
TURKEY
ARMENIA
SYRIA
IRAQ
JORDAN
Global DNS Hijacking Campaign: DNS Record Manipulation at Scale
DNSpionage Campaign Targets Middle East

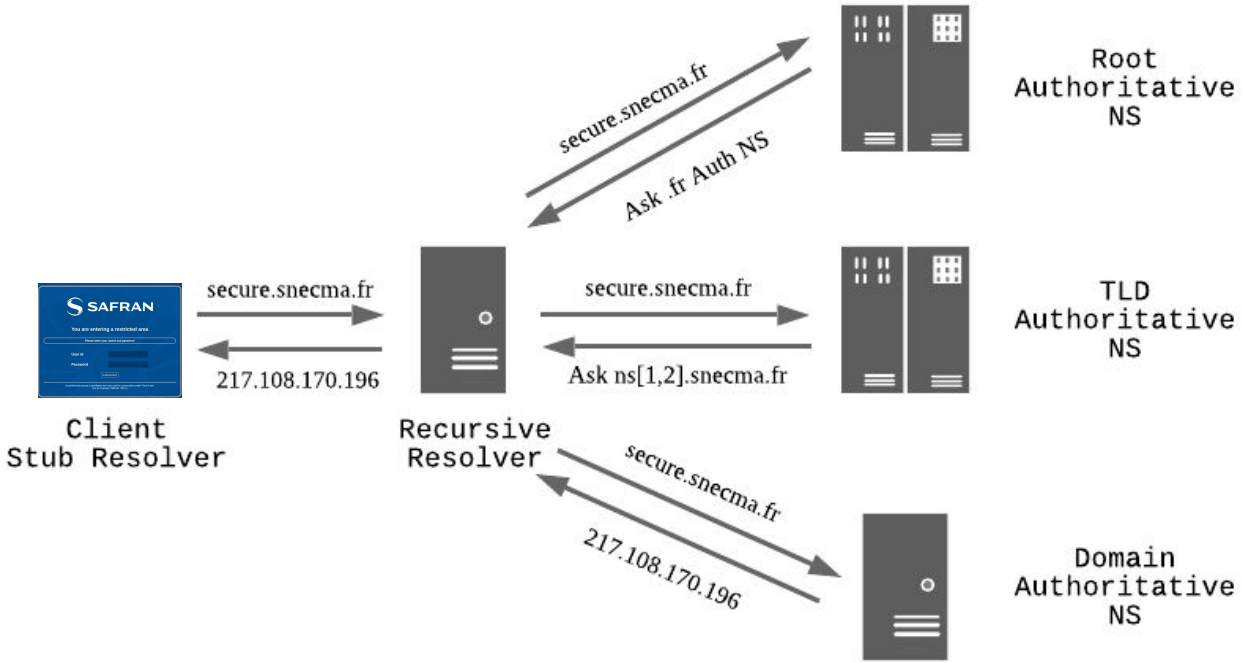
Introduction



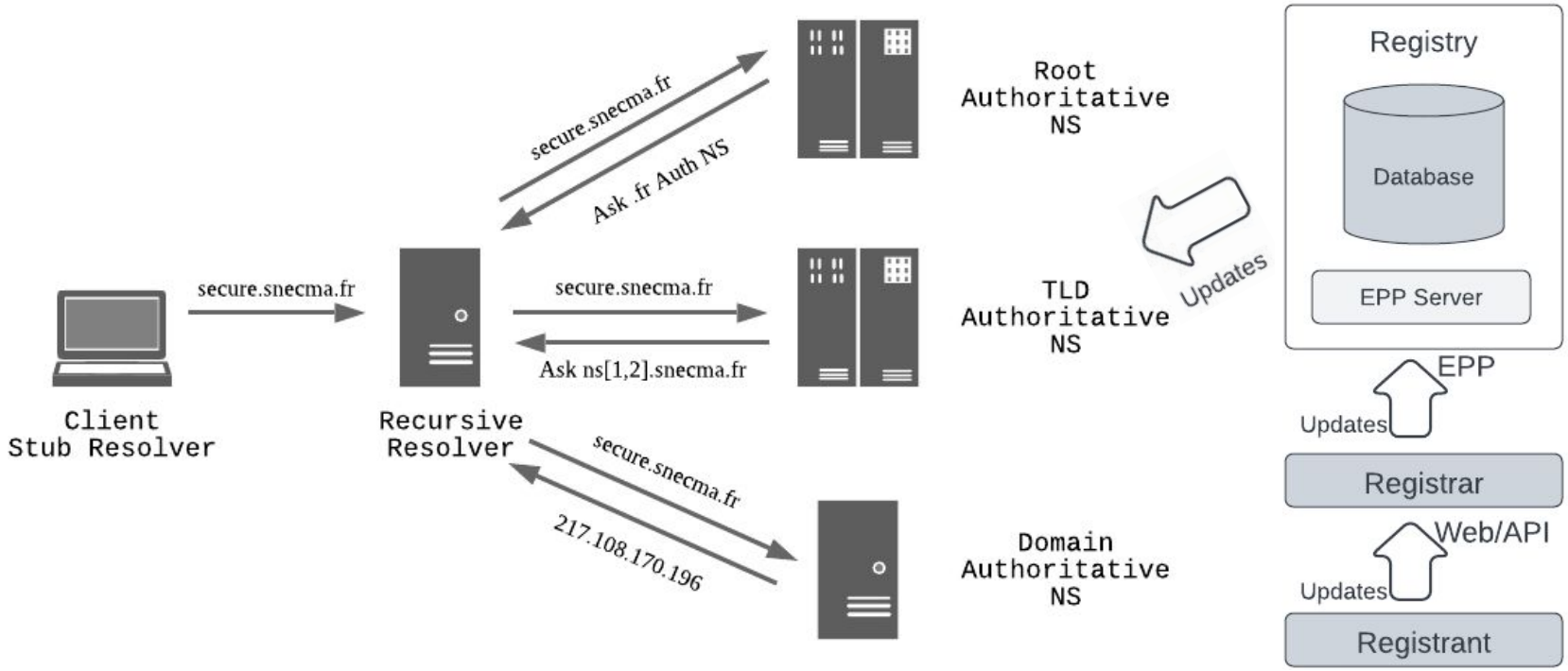
Recursive Resolution



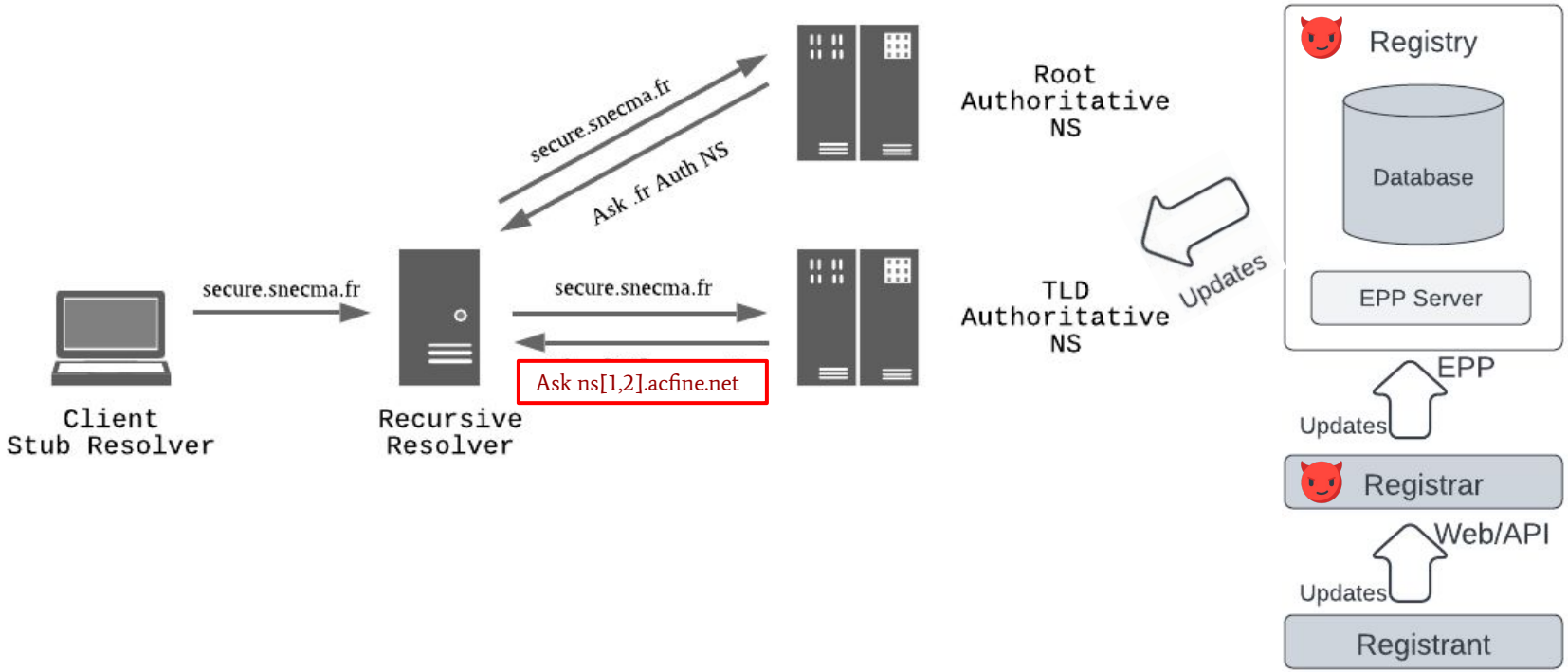
Recursive Resolution



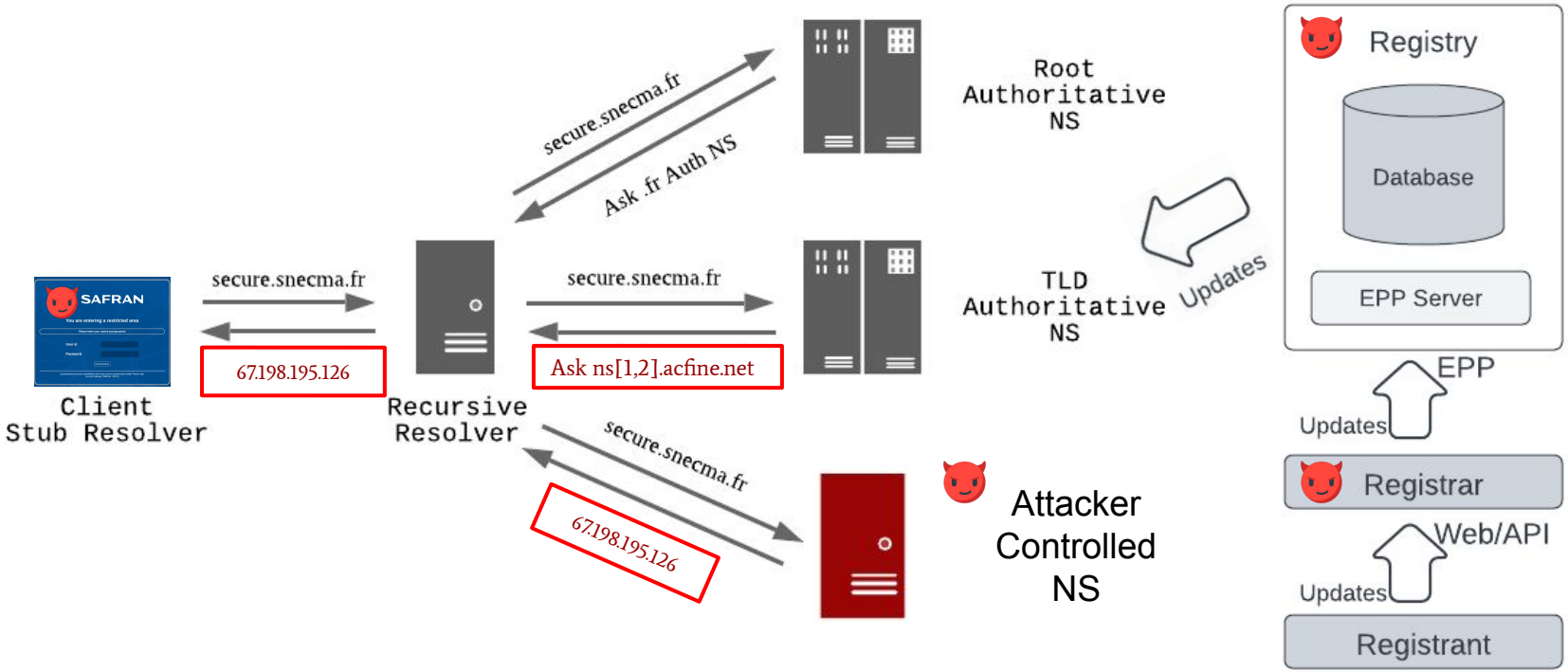
Setting and Updating Nameservers



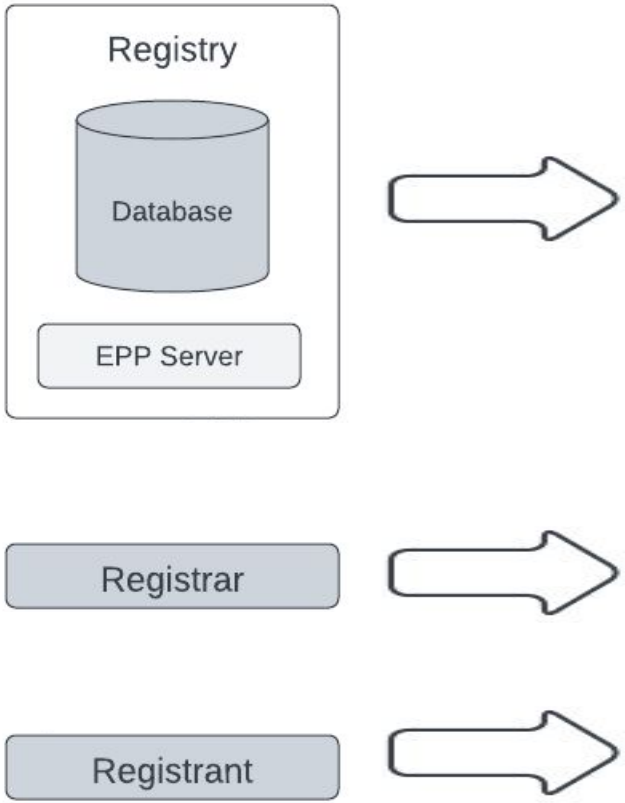
Attacks on Registry and Registrars



Bypasses Traditional Defenses



Key Idea Behind DNS Transparency



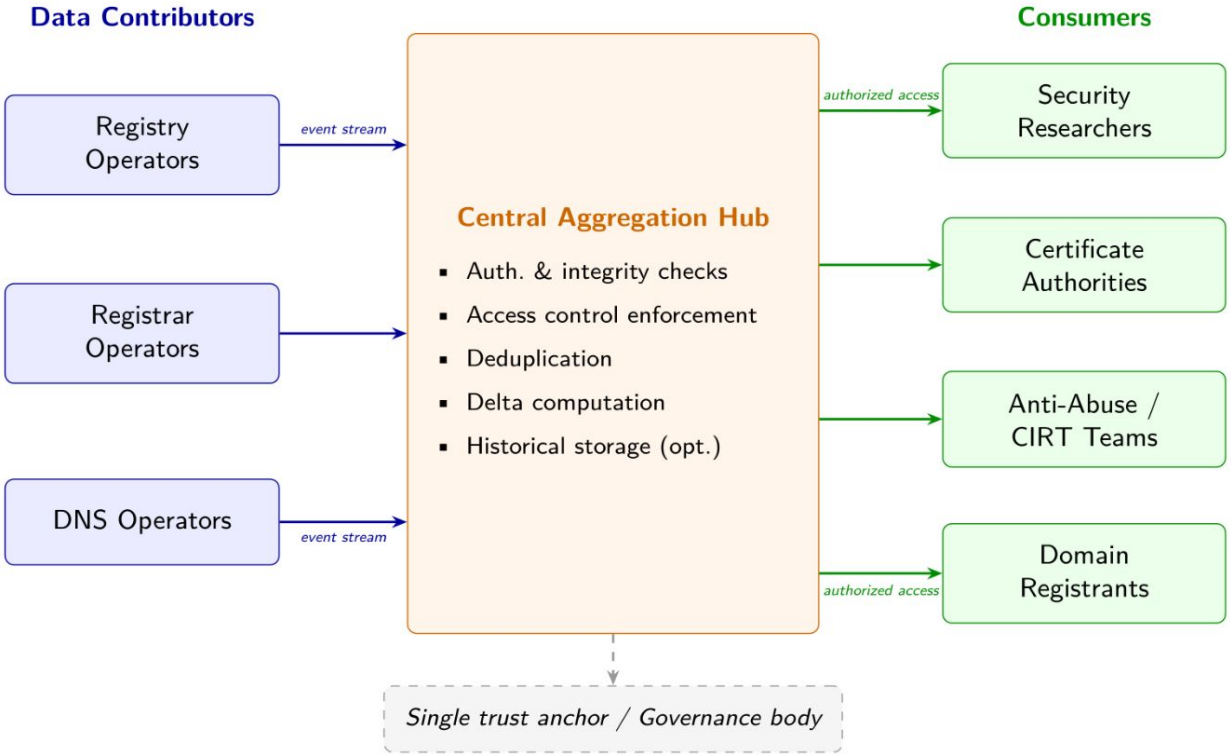
All
DNS
Configuration
Changes
are *Logged*

Data Types

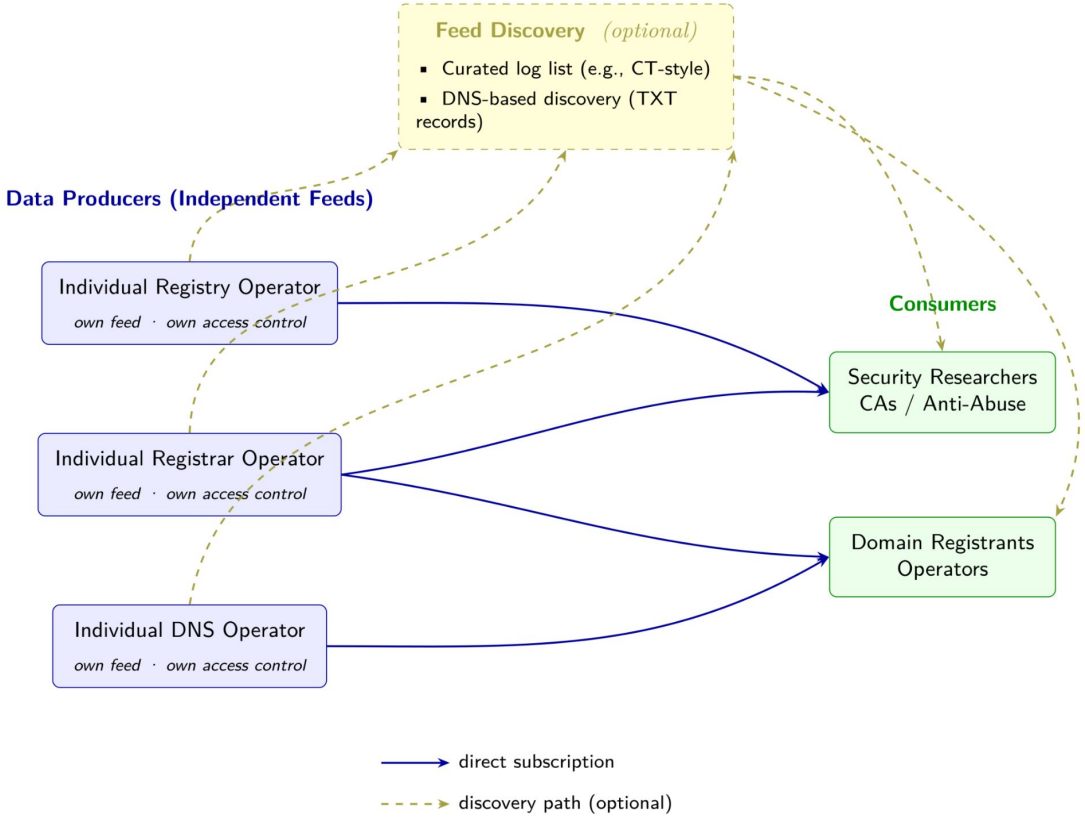
Discussion

1. DNS Transparency Data Collection Models
    a. Centralized Aggregation vs Independent Publication

Centralized Model



Independent Publication Model



Discussion

1. DNS Transparency Data Collection Models
    a. Centralized Aggregation vs Independent Publication
    b. Streaming data vs historical data
    c. Filtering data
2. Document needs to cover both potential models.
3. Does the model of publication/access affect the actionability of the data?

Centralized vs Independent Publication Model

Advantages:

- Single integration endpoint for contributors
- Lower risk of missing contributor data from the consumers
- Deduplication can reduce the amount of data exchanged/stored.
- Centralized policy enforcement reduces operator burden

Disadvantages:

- Concentration of data at a single point amplifies risks when operators have heterogeneous standards.
- The central actor bears significant operational cost and becomes a de facto trust anchor.
- The central actor becomes a structural bottleneck and a single point of failure for the entire system.

Advantages:

- Operators retain direct control over their own data and access policies
- The architecture can more readily evolve to accommodate new record types or new classes of contributors.

Disadvantages:

- Consumers bear the burden of discovering and maintaining connections to all relevant feeds and handle data heterogeneity.
- Each operator must independently scale their feed infrastructure to serve all authorized consumers.