DAP Updates

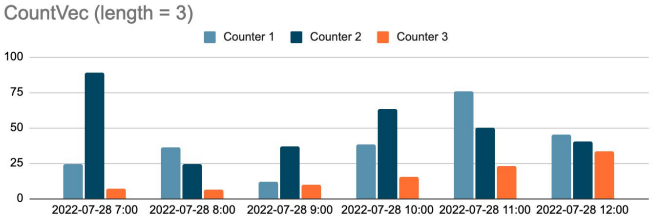
Christopher Patton

PPM - IETF 115 - London

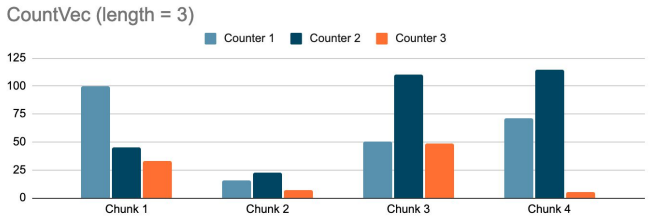
DAP-02 Change Log: Notion of "query types"

- New task parameter: **query type**
  - Used by aggregators to partition reports into **buckets**
  - Collector specifies a **query** that determines a sequence of buckets (i.e., the **batch**) to be aggregated.
- Two query types are specified:
  - **time_interval**: "all reports generated in a given time window"
  - **fixed_size**: "the next N reports"
- Need a new query type? **Let us know!**

time_interval queries



fixed_size queries



DAP-02 Change Log: Task expiration

- New task parameter: **expiration**
  - Primary consideration is operational
  - Aggregators MAY reject reports with timestamps past the expiration date

DAP-02 Change Log: Mutual authentication

- Need mutual authentication for Leader-Helper and Collector-Leader channels
- DAP-01 used a simple bearer token scheme
- In DAP-02 we specify **requirements** for mutual auth rather than a concrete scheme.

Next steps

- DAP-03: Resolve a few "bug" issues [1]:
  - ~~Issue 342: fixed_size: Unspecified batch ID discovery~~
  - Issue 362: Anti-replay requirements
  - Issue 369: Extension processing model is unspecified
  - Issue 373: Ambiguous encoding of AAD
  - …
- Beyond DAP-03:
  - API semantics (see Tim G.'s slides)
  - Integration of Poplar [2]
  - Editorial (improve readability)
  - Experimentation, security analysis

[1] https://github.com/ietf-wg-ppm/draft-ietf-ppm-dap/issues
[2] https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-vdaf#section-8

Implementation status

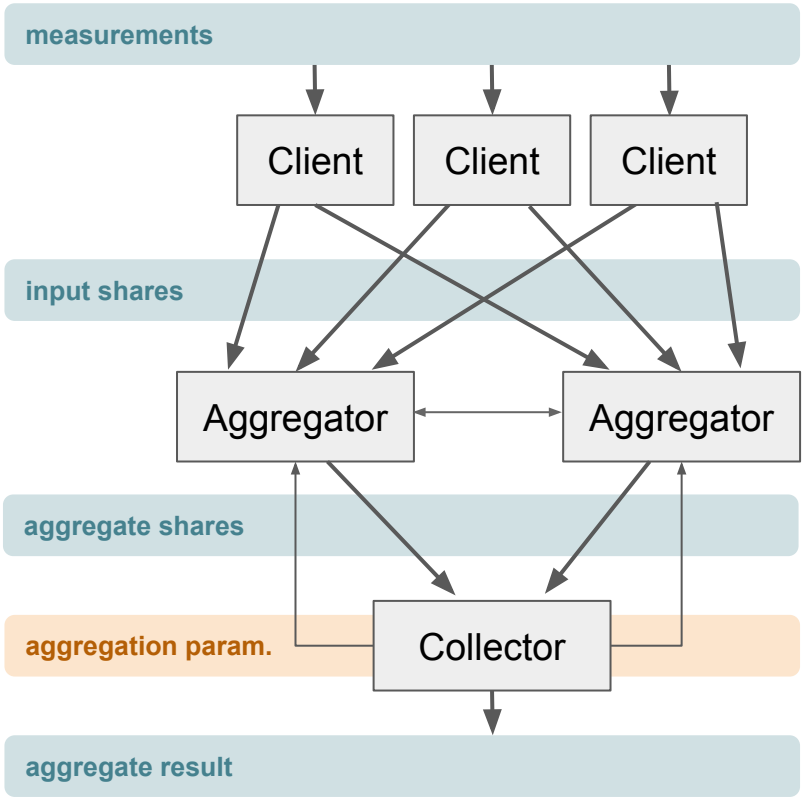
- DAP-02 is implemented by Daphne [3] and Janus [4]
  - We're ready to deploy experiments (ISRG as Leader, Cloudflare as Helper)
    - **Ping ppm@ietf.org or #ppm if interested.**
- David Cook (Janus co-developer) is working on a draft specifying endpoints for automated cross-implementation tests [5].

[3] https://github.com/cloudflare/daphne
[4] https://github.com/divviup/janus
[5] https://github.com/divergentdave/draft-dcook-ppm-dap-interop-test-design

Backup Slides

DAP overview

- Specifies **execution of a VDAF over HTTP**
  - Each VDAF defines the distributed computation of some **aggregation function**
    - Prio, Poplar, …
  - Work-in-progress in CFRG: draft-irtf-cfrg-vdaf-02

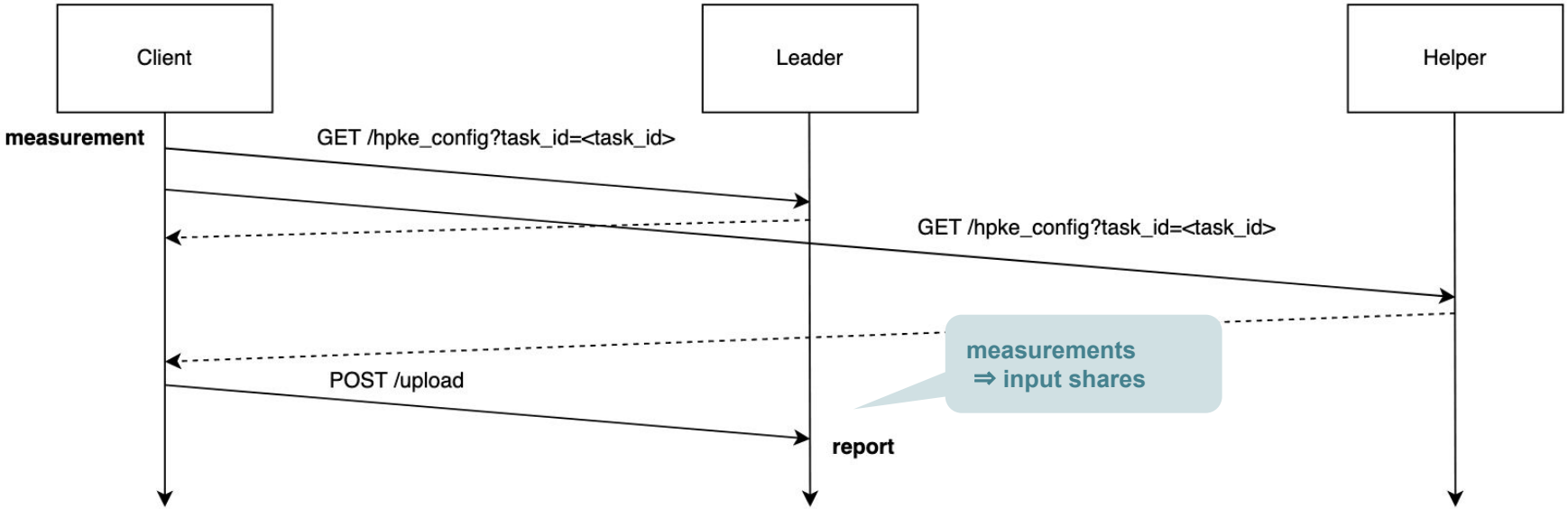


DAP = *"Distributed Aggregation Protocol"*

VDAF = *"Verifiable Distributed Aggregation Function"*

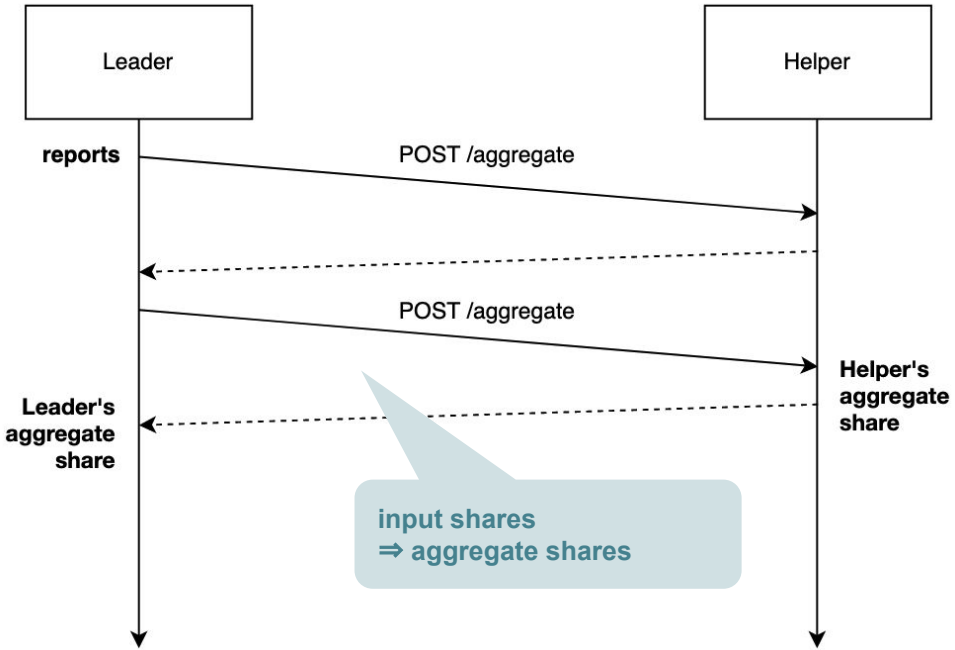
DAP is three protocols in one

Upload sub-protocol: Client generates **report** (i.e., encrypted input shares) for its **measurement** and sends report to Leader.



DAP is three protocols in one

Aggregate sub-protocol: Leader picks a set of reports and interacts with the Helper to verify them and compute **aggregate shares**.



DAP is three protocols in one

Collect sub-protocol: Collector issues **collect request** to Leader. Leader and Helper send encrypted aggregate shares for the corresponding **batch of reports** to the Collector.