Production Multi-Party Computation via DAP

MPC that you can use today

Tim Geoghegan & J.C. Jones

ISRG Internet Security Research Group

Divvi Up

USENIX PEPR
June 2, 2026

The Measurement Dilemma

Traditional Telemetry

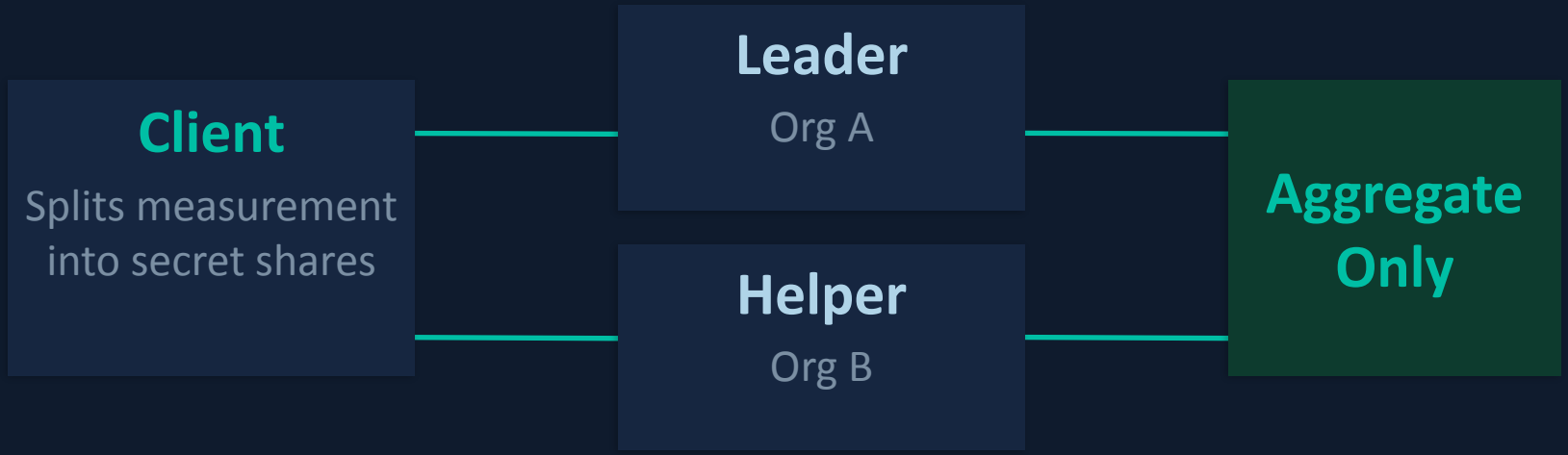
Raw data → central server

DAP

Aggregates only — no individual data

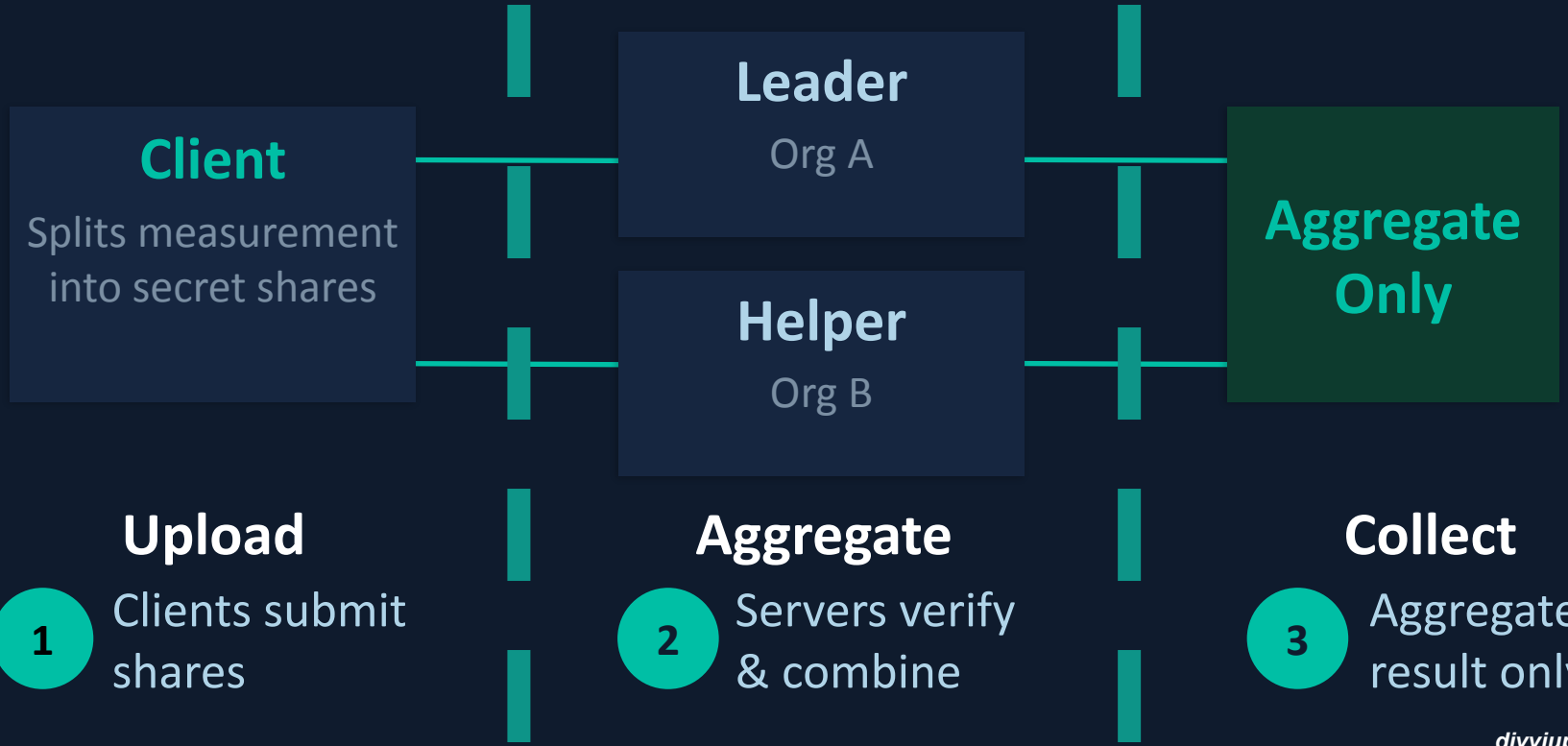
An IETF standard making MPC deployable at scale

The Two-Server Model



Two parties by design — not a limitation

Aggregation Flow



VDAFs bake zero-knowledge validity proofs into the shares — robustness against malicious clients without seeing inputs

Client

Splits measurement into secret shares

Leader

Org A

Helper

Org B

Aggregate Only

Upload

1 Clients submit shares

Aggregate

2 Servers verify & combine

Collect

3 Aggregate result only

divviup.org

Changes from prior MPC systems

General-purpose	→	Specialized aggregation protocols (VDAFs)
Bespoke design	→	Standard configurations
Finding independent operators	→	Hosted infrastructure

Running at Internet Scale

4.5 Billion
total reports processed

> 450 Million
reports per week, burst

Divvi Up

- 3+ years of continuous production operation
- Open source, running on commodity cloud infrastructure

Running at Internet Scale

- Previously impossible telemetry
- Publicly-verifiable privacy guarantees
- General-purpose measurements

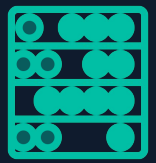
No individual browsing data is ever seen by any server

Cloud Costs Are Achievable

Storage

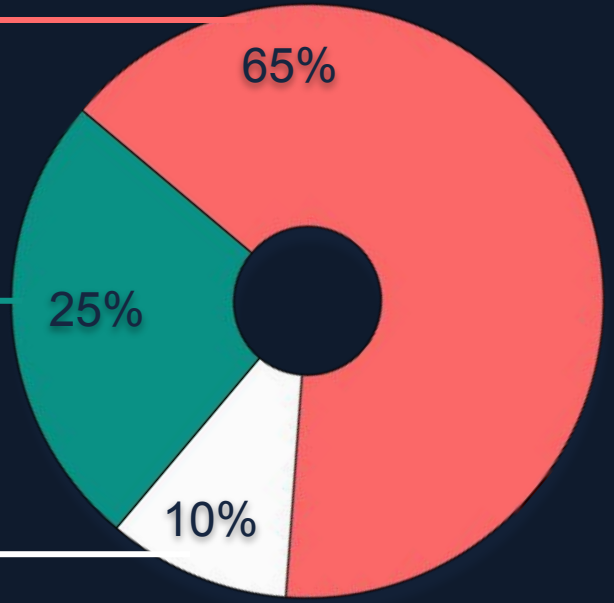
RDS PostgreSQL (db.m4.2xlarge)
RDS Storage (1 TB)

Data transfer and monitoring



Compute

EC2 virtual machines



Helper aggregator hosted in Amazon Web Services us-east-2
Processing 100M reports / week

Estimated monthly cost: ~$2,000 / month

Composing Privacy Layers

DAP / MPC

Input privacy

Differential Privacy

Output privacy

Oblivious HTTP

Metadata privacy

MPC protects inputs. DP bounds what can be inferred from outputs.

You Can Use This

Open Source – MPL 2.0

Janus aggregator in Rust
Clients in TypeScript, Rust, Java

IETF Standard

Not a research project

Hosted Service

Divvi Up as a Leader (or Helper)

Start Small

One counter metric ⟶ expand

You don't need to be a cryptography team

Practical MPC Aggregation is ready.

- divviup.org
- divviup.org/blog/command-line-intro
- datatracker.ietf.org/doc/draft-ietf-ppm-dap
- datatracker.ietf.org/doc/draft-irtf-cfrg-vdaf
- github.com/divviup/janus
- datatracker.ietf.org/wg/ppm/about

Questions?