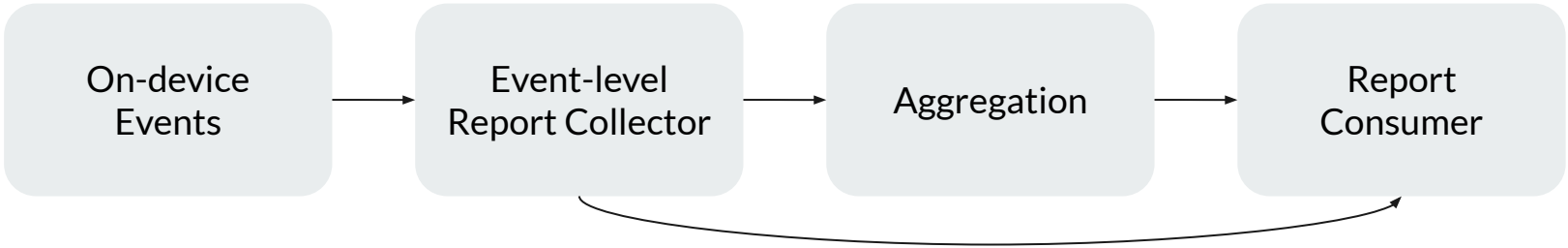
Goals (and antigoals) for the next 55 minutes

1. Antigoals
    a. Decide on the threat model
    b. Debate specific tradeoffs / implementations / parameters
2. Goals
    a. Get ~3 volunteers (editors) to work on a threat model draft
    b. Discuss high level sections, identify missing considerations
    c. For authors, outside this session (but hopefully before next session)
        i. Produce a draft document / outline
        ii. Highlights specific areas of open questions / lack of consensus to focus future conversation
3. Process Question
    a. Should this draft live in the CG or the WG?
        i. If WG, any concern advancing work on a draft before WG is formed?
    b. From meeting: No reason not to begin work.

Outline

1. Aggregate Measurement Scope
2. Actors
3. Actor Capabilities
4. Security Goals
5. Privacy Goals

Aggregate Measurement Scope



Actors

- User
  - Potentially malicious and/or bots
- User-agent / device / OS
  - Compromised software / malware likely partially out of scope
- First-party context (website / app)
  - Source and Trigger sites
- Third-party context (embedded site / SDK)
  - Ad-tech company / msmt partner
- Event-level report collector
  - Often an ad-tech company
- MPC Aggregation Service
  - Cloud operator
  - Aggregator / MPC participant
- TEE Aggregator Service
  - TEE server operator (physical)
  - TEE server tenant
  - TEE manufacturer / certificate authority
  - Coordinator service
- Aggregate report consumer
  - Source and Trigger sites
  - Possibly ad-tech company
- State actors / legal authorities
  - Subpoena power

Actor Considerations

- Assets
  - Secrets they can access which should remain private, or could enable an attack
- Capabilities
  - Attacks a malicious or compromised actors could mount
- Collusion capabilities
  - Attacks a set of coordinated malicious actors could mount
- Collusion risk
  - Which parties we assume can collude, and
  - explicitly which parties we assume (trust) not to collude
- Three C's
  - Curious (related to collision risks)
  - Compromised (e.g. hacked)
  - Compelled (e.g. subpoena)

Security Goals

1. Enable the report collector to learn the specific aggregation
2. Prevent any actor from learning anything beyond 1 or other specified leakage
3. Example specified leakage
    a. Aggregator learning number of event-level reports
4. Duplication of information already known within first-party context is not leakage
5. Correctness of result
    a. Should be resilient to poisoning, especially if poisoning reveals unintended leakage

References:

- Privacy Preserving Measurement (draft-ietf-ppm-dap-00) Threat model
- Mozilla Security / Anti tracking policy
- Webkit Tracking Prevention Policy

Privacy Goals

- TBD - Should come from the *Privacy Principles for Web Advertising Features* document
  - Question: Should measurement specific options (below) be in the threat model doc, or elsewhere?
- Specific to *measurement*, some possible options:
  - “Aggregated”
    - K-anonymity / approximate k-anonymity
  - “Anonymous”
    - Differential Privacy (epsilon or epsilon/delta)
  - “Aggregated and Anonymous”
    - K-anonymity + Differential Privacy
- Parameters to be determined
  - K and Epsilon (and delta)
  - Privacy Grain, e.g.
    - User / device
    - Site or Source/Trigger Site pair
    - Third Party / Ad Tech Company