Cross Device Attribution

PATCG June 2023

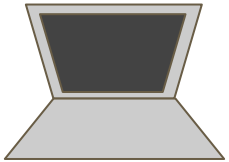
Agenda

- **Overview**
- Should cross-device support be a goal for the private measurement work?
- Device graph management
- Attacks, mitigations, and trust assumptions

Cross device

Measurements which span multiple user devices

Alice taps on an ad on her mobile phone



But purchases the item on desktop some time later

Alice views an ad on her connected TV

Possible improvements to utility and privacy

Utility

Including journey's across devices paints a better picture of the effectiveness of ad campaigns for advertisers

Privacy

If the private measurement system has a deep understanding of all of the user's contributions to a measurement, we can potentially protect *all* of their contributions

Measurement without cross-device can only make per-device privacy guarantees

Win win?

Agenda

- Overview
- **Should cross-device support be a goal for the private measurement work?**
- Device graph management
- Attacks, mitigations, and trust assumptions

Should cross-device support be a goal for the private measurement work?

The private measurement effort should aim to support cross-device measurement, while protecting privacy and security

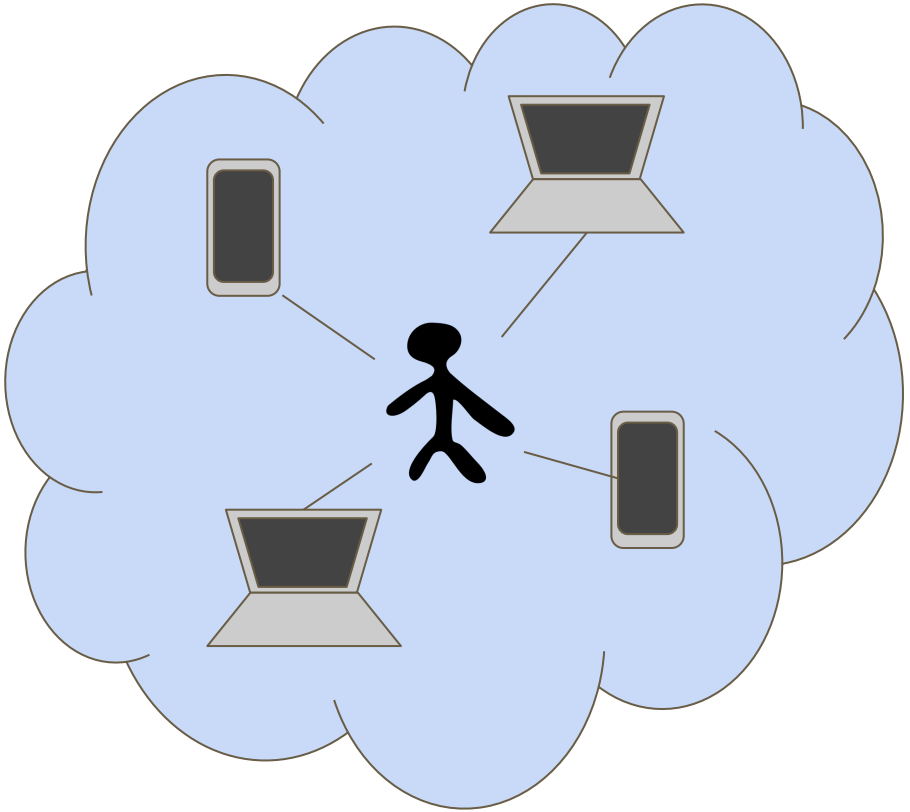
- There are challenges with supporting cross-device
- But does anyone fundamentally oppose the attempt to try?

Agenda

- Overview
- Should cross-device support be a goal for the private measurement work?
- **Device graph management**
- Attacks, mitigations, and trust assumptions

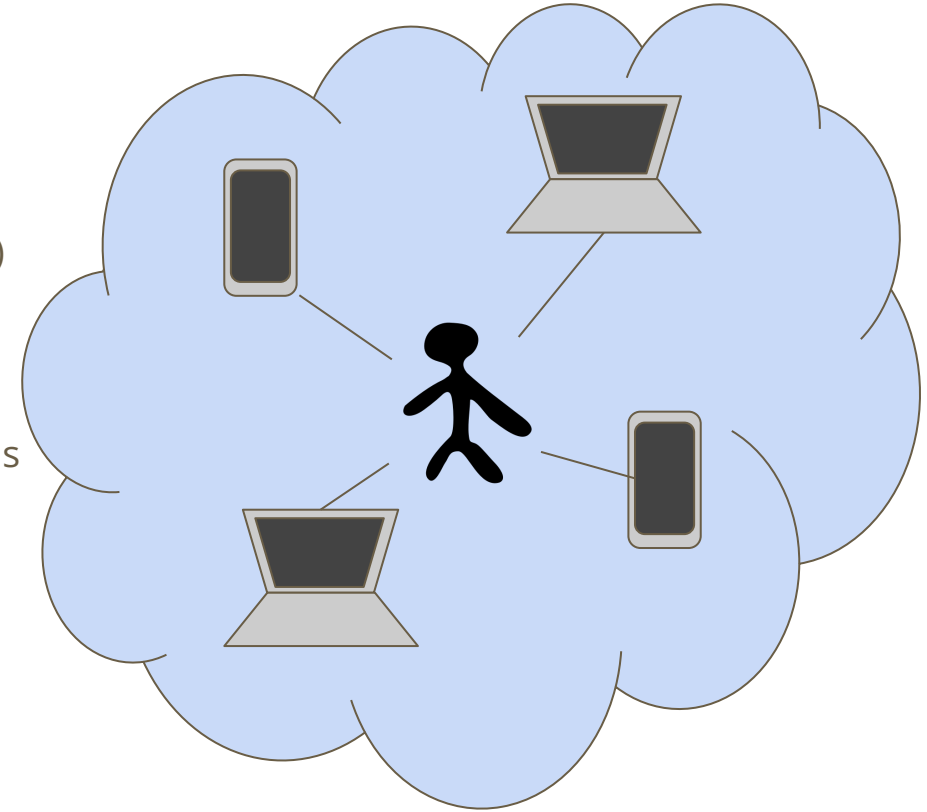
Device graphs

- How do we know whether it is the same user across devices?
- Match keys
- Match key providers



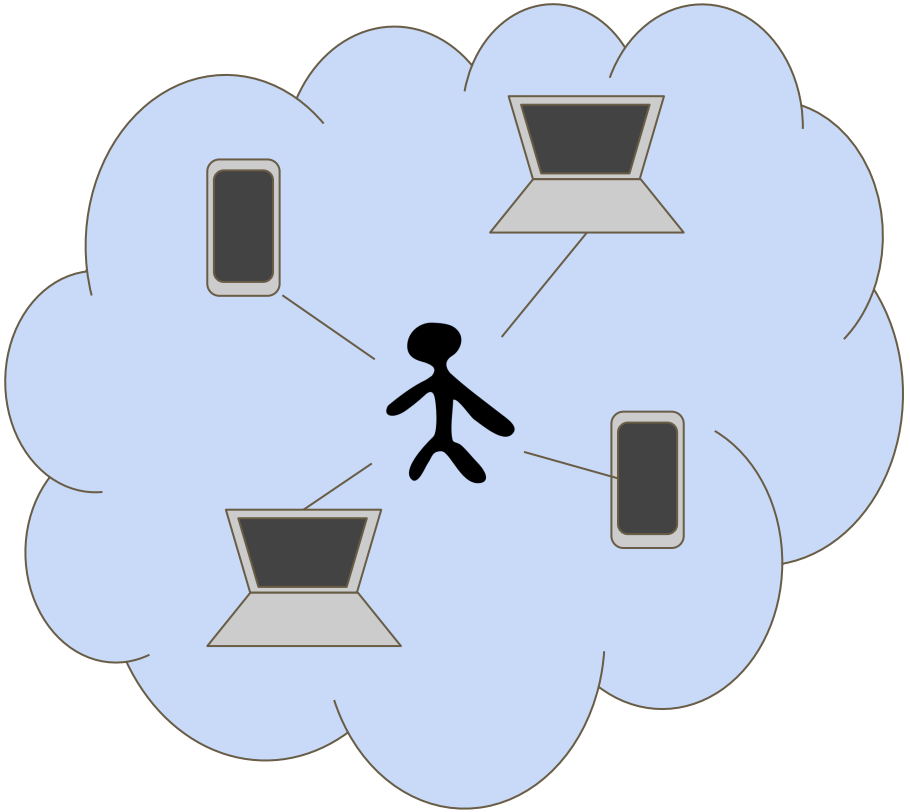
Match key providers

- **The ecosystem**
  - Low to no restrictions on who can be a match key provider
  - Allows for interoperability (the “I” in IPA)
  - IPA’s original design
  - E2E encryption design from Ben Savage
- **The platform**
  - Limited interoperability across platforms → more limited coverage
  - Archived ARA proposal
- **Something in between?**
  - “Platform trusted” ecosystem participants



Sharing device graphs

- Device graphs are proprietary and confidential, even in aggregate
- Device graphs contain sensitive user information
- MKPs may not be willing to share these arbitrarily / in full
  - ipa/39 has a proposed mitigation
- Privacy / security / utility trade-offs
- Open research questions!

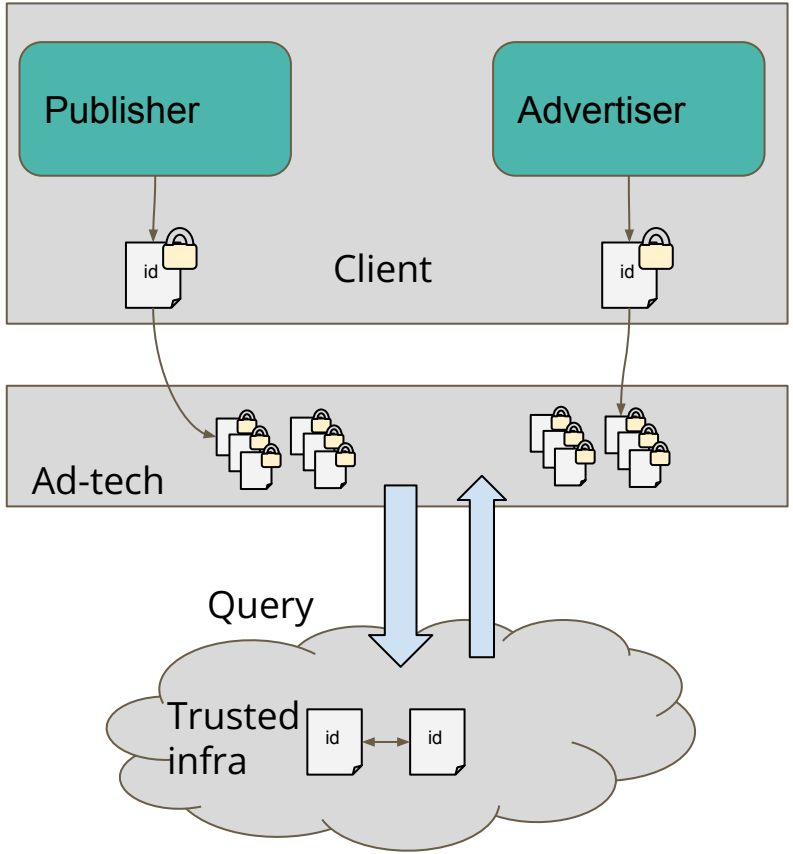


Agenda

- Overview
- Should cross-device support be a goal for the private measurement work?
- Device graph management
- **Attacks, mitigations, and trust assumptions**

Off-device attribution

- MKP provides access to a match key
- Events coming from the client encrypt the match key
- Trusted infrastructure privately joins based on the match key
- **Attacks**
  - MKP has the capability to “replay” events where it knows the match key a priori
  - *May* break privacy guarantees (depends on many factors)
  - MKP has the capability to inject offline data joinable with a match key (discussion)



On-device attribution

End to end encryption

- Match key provider(s) mediate a key exchange protocol
- Once all devices have each other's public keys, they communicate across untrusted channels
- **Attacks**
  - How trusted is the key exchange? Malicious MKPs might inject false "devices" and synchronize all events to a "device" they control
  - Communication channel can measure encrypted message patterns

Server Sync

- Vendors maintain per-user keys
- All relevant events are stored in the vendor's server, encrypted at rest
- Signed-in devices synchronize with the server to read/write events
- **Attacks**
  - Vendor access to decryption keys

Note: some attacks (across most designs) might be mitigated if the user must type a secret the MKP does not know on all of their devices before XD works properly

How much can we “trust” the MKP?

- Can anybody be an MKP, or should that role be restricted to the platform, or entities the platform trusts?
  - Accreditation, attestation, etc.
- What about if the user trusts them?
  - e.g. mediated with a permission prompt?
- See ipa/42
- To what extent can added trust on MKPs mitigate attacks?