Fledge: On-premise Trusted servers

PATCG June 2023

Contact: Vincent Minet (v.minet@criteo.com)

On-premise Trusted servers

Objective

Discuss how running trusted servers on premise could be made possible

Problem

Fledge: Trusted servers must be run on a cloud platform

- Large cost increase for Adtech. Cloud is more expensive than on-prem
- Need to run a dual infrastructure (Fledge vs other API)

On-premise Trusted servers

By design, TEE's operators do not have to be trusted

- Strong security guarantees
  (isolation, memory encryption, remote attestation, etc)
- Cloud and on-prem offer the same guarantees

Side channel attacks are the concern

- Are large scale exploitations scenario realistic ?
- Does the cloud offer more protection ?
- There are mitigations. Is-it enough ?
- Threat model

On-premise Trusted servers

Threat model for TEE operator

- What level of guarantee ?
- Physical attacks ? Software only ?
- What about dual actors (cloud provider being an adtech) ?
- Security vs other concerns ?

Operator approval process

- The path to become an approved TEE operator should be clear
- Security requirements ?
- Who approves ?