# Centralization

draft-mcfadden-pp-centralization-problem-00

Mark McFadden

PrivacyPass

IETF 110 Virtual - 12 March 2021

# Motivation

- Charter has a milestone on centralization:
  - “Risk assessment for centralization in Privacy Pass deployments for multiple design options”
- Significant discussion of this issue during the meetings prior to Working Group formation
- Independently: IAB open microphone discussions and IABOPEN

# What’s in the draft

- Potential privacy concerns
- Problem statement and potential mitigations

# From the Architecture draft

- Example
  - If there are 32 servers then verifiers learn 32 bits of information about the client
  - Having that much information about the client can lead to the client being uniquely identified
  - Contrary to the fundamental goal of Privacy Pass
- Mitigation
  - **“In cases where clients can hold tokens for all servers at any given time, a strict bound SHOULD be applied to the active number of servers in the ecosystem. [ID.davidson-pp-architecture-01].”**

# Is there an alternative?

- The architecture draft briefly considers limiting the number of redemption tokens at the client
- But . . . This implies establishing some control over the client
  - Very difficult in practice – far more difficult than restricting the number of servers

# Problem statement

- The architecture draft specifies and upper limit of four servers from which a client can acquire a token for later redemption.
- Proposed problem statement
  - An upper bound to available Privacy Pass servers creates architectural, engineering and practical problems for the deployment of the protocol
  - Any successful deployment of Privacy Pass must find mitigations for these problems.

# Problems to be discussed in the draft

- Architectural problems
- Engineering problems
- Practical deployment problems

# Are there mitigations?

- Inverse relationship between the number of servers and the amount of privacy seems difficult to fix
- Constraining the clients seems impractical
- Need to find a mitigation that is consistent with the aim of the underlying protocol but addresses the concern of centralization

# Next step

- -01 after IETF 110
- Discussion, comment on the list
- Thanks

Mark McFadden mark<at>internetpolicyadvisors.com