Report authentication for PPM DAP

draft-cpribe-ppm-dap-reportauth

Christian Priebe
Linmao Song
Motivation

Sybil attacks

A malicious party may generate a large number of reports to skew aggregation results

- to reveal information about honest measurements (privacy violation)
- to influence results to their benefit ("stats poisoning")

But: Effective rate limiting requires strict authentication - cannot do on aggregators

ReportAuth extension

DAP extension to include Privacy Pass tokens to allow Aggregators to verify that reports have been authenticated (and rate-limited) without learning clients’ identities
Overview

Client → Attester → Issuer → Leader → Helper

Privacy Pass Issuance protocol
- per aggregator
  - Challenge
  - authenticate Client
  - Challenge
  - Blinded Token
  - [rate limit]
  - Blinded Token

PPM DAP
- per report upload
  - Report
    - Report metadata
    - Leader share
      - Token
    - Helper share
      - Token
  - validate Leader token
  - Challenge
  - validate Helper token
ReportAuth extension

Definition

```c
struct {
    ExtensionType extension_type;
    Token token;
    Challenge challenge;
} ReportAuth;
```

Extension identifier
Privacy Pass Token
Token Challenge, required to recompute challenge digest during token verification

Sent with report within each encrypted input share
Client behavior

Token acquisition

- Token Challenge is synthesized on client
- Fixed number of tokens acquired and cached per Aggregator per issuance window to mitigate timing attacks

Report creation

- Per Aggregator
  - Choose unused Token
  - Construct ReportAuth extension with Token and Token Challenge
Aggregator behavior

Token verification

- Extract the token and the challenge from the upload extension
- Validate the `origin_info` field of the challenge contains the Aggregator's hostname
- Validate the token, as per Privacy Pass Auth Scheme
  - Includes verifying the token has been signed with an active Issuer Token Key
- Keep track of token nonce and reject report if previously seen
Discussion: Recommendations & Optimisations

- Recommended: Use Rate-Limited Privacy Pass Issuance Protocol (draft-ietf-privacypass-rate-limit-tokens)
- Reusing token nonce as report ID
- Reusing tokens across tasks
References

v0 draft: http://github.com/cpriebe/draft-priebe-ppm-dap-reportauth

We welcome your feedback and contributions

Thank You