Roughtime hackathon experience

Quick recap: roughtime

- CT for time
- Use signatures on responses, incorporating nonce from queries
  - Attests to reply generation within an interval
  - If response was generated outside that interval, tractable evidence that at least one server was lying
  - Can then lead to server impechment
- Applications: signature verification, IOT, time synchronization daemons
- Montonotic time representation based on MJD and microseconds since midnight

Hackathon

- Cloudflare client and server implementation: work on -03
  - Not done: update interfaces
- Interop with Johan Lindquist’s client
- Identified issues:
  - MJD: necessary information tracked in kernel, need portable interface.

Barriers to draft

- Impeachment remains a challenge: text needs to be written
- If deploying, need to hear input: even “this is fine”
- At that point think ready for WGLC

Particular areas of concern

- Is minimum radius 1 second and gettimeofday enough?
- MJD: arithmetic depends on leap second tables
  - Is 86399 or 86400 the last second of the day?
- MJD representation has invalid representations:
  - Invitation to do arithmetic on degenerate reps normalize afterwards
  - Introduces differences
- Ed25519 signature canonicalization
  - Not needed?
  - But if signatures are valid to some invalid to others can it break impeachment?

Barriers to deployment

- Currently small number of earlier versions deployed
- Not enough -03 servers
- Need to have places to report malfeasance
- Need clients
  - Clients: have to have policies about acceptable servers
  - Similar to CT

Any Questions?