Roughtime @ IETF 121 Hackathon

- **Updated roughtimed and pyroughtime client to draft-11**
- **Plummet interoperability framework**
  - https://github.com/ietf-wg-ntp/Roughtime-interop-code
- **New Rust server implementation**
- **Discussions**

Roughtime interoperability (all)

Server/client	cloudflare	craggy	node-roughtime	pyroughtime	roughenough	vroughtime
cloudflare	✅	✅	✅	✅	✅	?
roughenough	❌	❌	❌	❌	✅	✅
roughtimed	✅	❌	?	✅	✅	?

Roughtime interoperability (draft-11)

Server/client	cloudflare	pyroughtime	roughenough
cloudflare	✅	✅	✅
roughenough	❌	❌	✅
roughtimed	✅	✅	✅

Results

- **3 servers & 3 clients up-to-date with draft-11**
- **Found bugs**
  - Cloudflare: Missing NONC and VER tags in server responses
  - Many clients do not check NONC/VER tags or verify signatures
- **Roughenough follows RFC8032 when generating keys**
- **Version downgrade attacks**
- **Other issues with current draft**