Roughtime Update

IETF 111: San^H^H^H Your Livingroom
Beyond the drafts
Roughtime is CT for time

- Many applications (X509 verification, Kerberos, etc) need a rough idea of the time
- Need high degree of confidence in server honesty
- Emphasis on rough: within a few seconds is fine
- Huge impact on security: nonmalicious certificate failures are often due to misset clocks
- Applications receive measurement of the time and uncertainty interval: decide if good enough
The drafts
draft-ietf-ntp-roughtime-05

- Defines communication between servers and clients
- Independently written, interoperable implementations from the spec
- We’d like to go to WGLC
More complicated
Defines what mississuance is, how to report it in a standardized format
Like CT have servers, auditors, and clients
Clients have their own policies in addition to what’s here
More attention, more info on needs wanted
Beyond writing spec need more standing up servers and auditors
Discussion
Discussion

- Who is interested?
- Who would want to implement?
- What applications should we be considering that we aren’t yet?
- Other questions/comments?