Decentralized Internet Infrastructure
Proposed Research Group

Meeting at IETF-102

Dirk Kutscher Melinda Shore

IRTF IPR Policy

The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules. This is a summary of these rules as they relate to IRTF research group discussions, mailing lists and Internet Drafts:

- If you include your own or your employer's IPR in a contribution to an IRTF research group, then you must file an IPR disclosure with the IETF.
- If you recognize your own or your employer's IPR in someone else's contribution and you are participating in the discussions in the research group relating to that contribution, then you must file an IPR disclosure with the IETF. Even if you are not participating in the discussion, the IRTF still requests that you file an IPR disclosure with the IETF.
- Finally, the IRTF requests that you file an IPR disclosure with the IETF if you recognize IPR owned by others in any IRTF contribution.

The IRTF expects that you file IPR disclosures in a timely manner, i.e., in a period measured in days or weeks, not months. The IRTF prefers that the most liberal licensing terms possible are available for IRTF Stream documents, see RFC 5743. You may file an IPR disclosure here: http://www.ietf.org/ipr/file-disclosure

See RFC 3979 (BCP 79) for definitions of "IPR" and "contribution" and for the detailed rules (substituting "IRTF" for "IETF").

Administrivia

- Mailing List
  - din@irtf.org
  - https://www.irtf.org/mailman/listinfo/din
- Wiki
  - https://trac.ietf.org/trac/dinrg/wiki
- Datatracker
  - https://datatracker.ietf.org/rg/dinrg/about/
- Chairs
  - Melinda Shore -- Fastly
  - Dirk Kutscher -- Huawei
- Meeting Notes
  - https://etherpad.tools.ietf.org/p/notes-ietf-102-dinrg
  - Note taker:

Agenda

09:30	Welcome, Agenda Bashing	Chairs
09:40	SCP Update https://datatracker.ietf.org/doc/draft-mazieres-dinrg-scp/	David Mazieres
09:55	SCP Formal Verification	Giuliano Losa
10:10	Distributed Authenticated Mapping	Colin Man
10:25	Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers	Shehar Bano (remote)
10:45	DIN & ANIMA	Toerless Eckert
11:00	Decentralized Trustworthy Internet Infrastructure	Bingyang Liu
11:15	Scope & Agenda Discussion	Chairs, All
11:30	End of Meeting	

Presentations

Decentralized Internet Infrastructure

- Investigate open research issues in decentralizing infrastructure services such as
  - trust management
  - identity management
  - name resolution
  - resource/asset ownership management
  - resource discovery
- Focus on infrastructure services that can benefit from decentralization

Research Challenges

- Scalability - what are the problems that prevent decentralized infrastructure services from achieving global scale?
- Trust management and delegation in decentralized communication settings
- Privacy and targeted, verifiable disclosure
- Applicability of distributed ledger and related technologies to different use cases and environments
- Consensus algorithms for specific scenarios with a focus on Internet infrastructure services
- The ability of constrained nodes to benefit from elements of a consensus item that they cannot process or store as a complete set
- Economic drivers and roadblocks for decentralizing network infrastructure
- Disambiguation in decentralized naming and trust systems

Objectives

- Building a community of researchers working on decentralized infrastructure
- Identification of common requirements and properties of selected building block technologies
- Design and implementation of one or more general-purpose infrastructure systems
- Deployment and operation of one or more actual implementations

Recent Feedback, Discussions

- Establishing trust without relying on centralized systems seems most important theme
  - Also: overcoming centralized ID management and data collection
- Understand goals of different consensus protocols: agree on one solution vs. “embracing chaos” (uncertain knowledge)
  - Reputation systems, notion of relative information -- IoT use cases
- Might consider developing (experimenting with) common infrastructure (group communication, gossip protocols etc.)
- Experimental specifications (like SCP, Chainspace potentially)

Decentralized & Distributed

- Prefer not define extended taxonomy at this point -- need a basic handle for getting started as a community
  - Decentralized as in *establishing trust without relying on centralized systems/entities*
  - Distributed as in *distributed system implementation*

DISCUSS

- Charter sufficiently well defined (modulo comments that have been made so far)?
- Topic important and interesting enough?
- Viable community?

Future Plans

- Would like to have more meeting time -- Interim meetings seems useful
  - Probably in Bangkok -- difficult to squeeze something in before
  - Ideas for conferences or other non-IETF events to co-locate with in the future? (Went to NDSS in 2018)