IRTF Distributed Internet Infrastructure

Side Meeting at IETF-99

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").

Agenda

1. **Background & Purpose** (Dirk & Melinda)

2. **An analysis of the applicability of blockchain to secure IP addresses allocation, delegation and bindings (**Jordi Paillissé Vilanova):
   https://datatracker.ietf.org/doc/draft-paillisse-sidrops-blockchain/

3. **Lightest Project Overview** (Benno Overeinder): http://lightest.eu/

4. **Cloudless IoT** -- Lixia Zhang

5. **Discussion of Next Steps** (Dirk & Melinda)

"Distributed/Decentralized Internet Infrastructure"

- Exploring potential to **decentralize Internet Infrastructure with distributed ledger technology**

- Identifying use cases and their commonalities
- Understanding available/emerging technologies and their features and constraints
- Analyzing impact on Internet technologies and IETF work

Background (IRTF)

- Had two side meetings at previous IETF meetings
- "Distributed Internet Infrastructure"
  - https://trac.ietf.org/trac/irtf/wiki/blockchain-federation
  - https://www.irtf.org/mailman/listinfo/din
- Topics
  - Applying distributed ledger (blockchain et al.) to Internet technologies
  - Distributed protocol id/name registry
  - Infrastructure services for IoT -- avoiding centralized services etc.
  - Data and service federation in future telco networks
- Summary so far
  - There is interest -- need to find a good angle for IRTF
  - Most interesting: Internet infrastructure services based on distributed ledger tech

Selected IETF Activities

- Thomas Hardjono: Decentralized Service Architecture for OAuth2.0
  - https://tools.ietf.org/html/draft-hardjono-oauth-decentralized-00
  - From "single-sign-on" to user-centric, decentralized control of resource sharing
  - Discusses possible support by blockchain and other ledger systems

- IETF Ledger BOF at IETF-96
  - https://datatracker.ietf.org/wg/ledger/meetings/
  - Non-WG Forming BOF introducing some work on Interledger (payment across payment networks)
  - Not conclusive regarding future IETF work

- Internet-Level Consenus (ILC)
  - https://www.ietf.org/mail-archive/web/ilc/current/maillist.html
  - Foundational technology for certificate transparency, pseudonymous reputation systems

Activities outside IRTF

- (Obviously many projects, forums on blockchain, fintech etc.)

- Internet Governance Forum (IGF)
  - Dynamic Coalition on Blockchain Technologies: "common platform involving a large variety of stakeholders in a joint analysis of the blockchain debate"
  - Public web platform: http://coala.global -- multidisciplinary forum
  - Also ties to W3C
  - Approached IRTF people for potential Blockchain RG
  -
- Distributed web platforms
  - IPFS, Maidnet, decentralized cloud storage etc.
  - https://www.w3.org/2016/04/blockchain-workshop/
  - Wealth of community/grassroot efforts as e.g. described on http://nethood.org/links.php

Other Ideas of Interest

- Decentralized name registries (Namecoin, Ethereum Name Service etc.)
  - Alternative name resolution services…

- Smart contracts between/within network service providers
  - Augmenting/replacing routing / policy information exchange

- Also see https://trac.ietf.org/trac/irtf/wiki/blockchain-federation

Thoughts for Next Steps

- Intuitively there is an interesting networking angle to ledger technologies
  - Redesigning previously centralized infrastructure systems
  - Solving problems that were hard to address in the past
  - Addressing new use cases
- IoT
  - Identity management
  - Distributed protocol registries
  - Data sharing -- finding data and paying for it
  - Also see Carsten's presentation at previous DIN meeting
- Distributed Web
  - Thomas's OAuth work
  - Data sharing
- ICN
  - Name, identity, PK resolution systems (just a thought…)

Goals for Today

- Understand the research space that IRTF could operate in

- Get an understanding of potentially interesting use cases

- Identify areas that people would like to work on

- Come up with an initial list of activities/deliverables for an IRTF effort

An analysis of the applicability of blockchain to secure IP addresses allocation, delegation and bindings (Jordi Paillissé Vilanova): https://datatracker.ietf.org/doc/draft-paillisse-sidrops-blockchain/

Lightest Project Overview (Benno Overeinder):

http://lightest.eu/

Cloudless Internet of Things (Lixia Zhang)

Scope of a Potential IRTF Activity

- Forum for researchers concerned with Decentralized Network Applications and Operations
- Framing document
- Investigating and documenting use cases
  - And their requirements regarding ledger infrastructure etc.
  - With a focus on Internet technologies (not necessarily global Internet)
  - Security/privacy (cryptography expertise)
- Creating frameworks for most important use cases
  - Selecting applicable ledger technologies
  - Specifying transaction models, smart contract, operational requirements
  - Opportunity to avoid silo approach (specific ledger systems for individual use cases)
- Creating and operating testbeds
  - Operational infrastructure that can be used by others

Topics

- Applicability of cryptographic data structures to internet infrastructure
  - Scalability
  - Security properties
- Economics, "fairness," and property models
  - incentives
- Infrastructure elements
  - Naming
  - Identity
  - IoT
  - Routing (BGP)
- Data sharing
  - Authorization
  - Delegation

Discussion Questions

- "Distributed Infrastructure" -- interesting (and understandable) topic?

- Interesting topics/activities/deliverables?

- (Additional) use cases?

- What contributions can we expect?

- Other communities to reach out to?