Privacy and Security Program
IETF 91

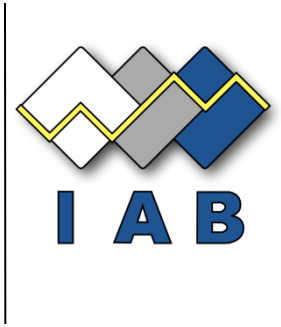
Landscape of work

- 3 challenges:
  - Internet protocols are developed as building blocks and thus security and privacy protections are piecemeal
  - security approaches presume that attackers have resources on par with those available to those secure the system.
  - many systems breach confidentialitr to simplify the delivery of services or meet other requirements.

3 streams of work

1. Internet scale resilience
    - ➔ Showrunner: Brian Trammel)
2. Confidentiality Area
    - ➔ Showrunner: Joe Hall
3. Trust Area
    - ➔ Showrunner: Karen O'Donoghue

Internet Scale Resilience



Areas of work: route hijacking, distributed denial of service, and related attacks; it will describe the available mitigations and work with related IETF programs to limit the development of protocols which offer amplification opportunities to the attackers.

Documents:

- Threat model document
- Mitigations document
- IAB statement on prevention of UDP amplification attacks
- Program slides and white paper for broad audience

Confidentiality

Areas of work: threat models related to surveillance, describe building blocks which may be used to mitigate that threat, and provide a systems engineering level of description of how to build a confidential application which flows across the open Internet.

Documents:

- Threat model document
- Mitigations document
- IAB statement on applicability of cleartext protocols
- Systems engineering document

Trust

Areas of work: PKI infrastructures, with a specific focus on how to manage protocol systems in which there are multiple sources of truth which may provide assurances related to identity, authorization, or repudiation.

Documents:

- Threats related to multiple sources of truth
- Mitigations document
- IAB statement on designing protocols with multiple sources of truth
- IRTF charter for work exploring block-chain models as sources of truth for community managed resources