T2TRG: Thing-to-Thing Research Group

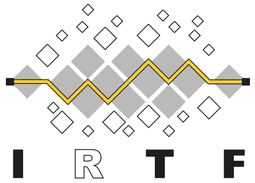
T2TRG Work Meeting, May 24, 2023

Chairs: Carsten Bormann & Ari Keränen

Note Well

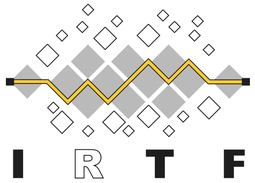
- You may be recorded
- Be nice
- The IPR guidelines of the IETF apply:
  see **http://irtf.org/ipr** for details.

Note Well – Privacy & Code of Conduct



- As a participant in, or attendee to, any IRTF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public
- Personal information that you provide to IRTF will be handled in accordance with the Privacy Policy at https://www.ietf.org/privacy-policy/
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this
- See RFC 7154 (Code of Conduct) and RFC 7776 (Anti-Harassment Procedures), which also apply to IRTF

Note Well – Intellectual Property



- **The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules**
- By participating in the IRTF, you agree to follow IRTF processes and policies:
  - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion
  - The IRTF expects that you file such IPR disclosures in a timely manner – in a period measured in days or weeks, not months
  - The IRTF prefers that the most liberal licensing terms possible are made available for IRTF Stream documents – see RFC 5743
  - Definitive information is in RFC 5378 (Copyright) and RFC 8179 (Patents, Participation), substituting IRTF for IETF, and at https://irtf.org/policies/ipr

Goals of the IRTF

- The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organisation, the IETF, focuses on shorter term issues of engineering and standards making

- **The IRTF conducts research; it is not a standards development organisation**

- While the IRTF can publish informational or experimental documents in the RFC series, its primary goal is to promote development of research collaboration and teamwork in exploring research issues related to Internet protocols, applications, architecture, and technology
- See “An IRTF Primer for IETF Participants” – RFC 7418

Administrivia

- (Blue sheets maintained by meetecho)
- Note-takers: **https://notes.ietf.org/notes-ietf-interim-2023-t2trg-01-t2trg**
- Meetecho chat: also via Zulip: **https://zulip.ietf.org/#narrow/stream/t2trg**
- Mailing List: **t2trg@irtf.org** — subscribe at: **https://www.ietf.org/mailman/listinfo/t2trg**
- Repo: **https://github.com/t2trg/2023-05-security**

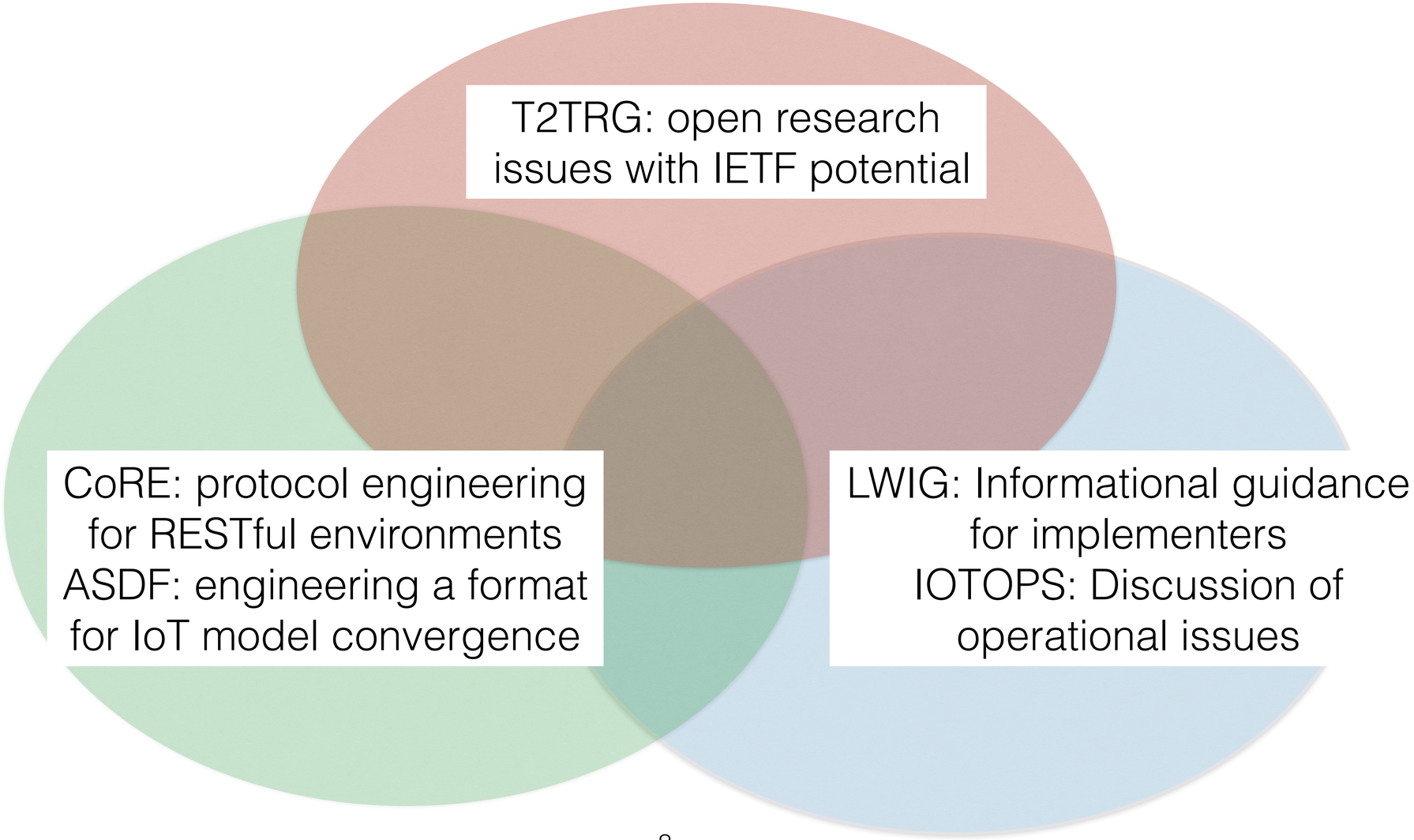
T2TRG scope & goals

- Open research issues in turning a true "Internet of Things" into reality
  - Internet where low-resource nodes ("things", "constrained nodes") can communicate among themselves and with the wider Internet
- Focus on issues with opportunities for IETF standardization
  - Start at the IP adaptation layer
  - End at the application layer with architectures and APIs for communicating and making data and management functions, including security

IRTF and IETF

IRTF
(Research)

IETF
(Engineering)



This meeting

Short (1h) “work meeting” on security:

- 3 active RG drafts on security issues:
  - Amplification **attacks** using CoAP
  - Terminology and processes for **initial security setup** of IoT devices
  - A Taxonomy of operational security considerations for manufacturer installed **keys** and Trust Anchors
- 1 potential field of new work:
  - discovery: access control, security, privacy

Agenda

Time (UTC)	Who	Subject	Docs
13:00	Chairs	Intro	
13:05	John Mattsson	Amplification attacks using CoAP	irtf-t2trg-amplification-attacks
13:20	Mohit Sethi, Dan Garcia	Terminology and processes for initial security setup of IoT devices	irtf-t2trg-security-setup-iot-devices
13:35	Michael Richardson	A Taxonomy of operational security cons. for manuf. installed keys and Trust Anchors	irtf-t2trg-taxonomy-manufacturer-anchors
13:40ish	Chairs, all	Discussion on discovery access control, secure discovery, privacy-preserving discovery	
13:55ish	Chairs	Wrap-up	
14:00	Chairs	end of meeting	

discovery access control, secure **discovery**, privacy-preserving **discovery**

Carsten Bormann

T2TRG work meeting 2023-05-24

Discovery: important for IoT

- Need to **automate** setup processes as much as possible
  - Limited user interfaces in devices
  - Large number of devices (pet ➔ cattle)
  - Large number of **kinds** of devices

- Network Discovery
- Resource Discovery (for Service Discovery)

Discovery: Objectives

- Roughly: Device can find infrastructure; infrastructure can find device
- “Find”: Learn enough to do something useful then

- Objectives: CIA
  - Confidentiality: Adversary does not learn what it shouldn’t
  - Integrity: Adversary cannot inject/spoof information
    (for DoS or to gain further access)
  - Availability: Adversary cannot disrupt functioning

Discovery: Confidentiality

- Confidentiality: Adversary does not learn what it shouldn’t
  - Privacy requirements
    (Is there an insulin pump in this room? Any expensive gadgets worth to steal?)
    - Even stable identifiers create linkability issues (see MADINAS)
  - Do not disclose what would increase attack surface

- Realization:
  - Often falling back to (sub-)network security
  - Resource discovery: “View” approach (authorized users see more)
    Issue: Who is authorized to what? How did the authentication work?

Discovery: Integrity

- Integrity: Adversary cannot inject/spoof information
  - Abuse cases: DoS on actual discovery, confusion to gain further access

- Realization:
  - Often falling back to (sub-)network security
  - Integrity requires authentication —
    Issue: Who is authorized to what? How did the authentication work?

Discovery: Availability

- Availability: Adversary cannot disrupt functioning
  - “Finding”: Hard to ensure completeness of enumeration
  - Abuse of discovery capability for DoS (e.g., battery draining)

- Resource use should require authorization —
  Issue: Who is authorized to what? How did the authentication work?

Discovery Security as an Authorization Problem

- What authentication methods and authorization models are available for use in a discovery phase?
  - e.g., choose the right network
    melds into setup phase, e.g., accept “purpose in life”
- What partial authentication/authorization states can be used to authorize disclosure?
  - “Secret handshakes”: Mutual authentication **before** anything is disclosed to non-authorized parties

Discovery: next steps

- Are these important (and interesting) problems to solve, and/or to document the state of the art?
- Who is interested?
- Should we aim to write (some of) this up?
- Should we find time for a first meeting of interested people?