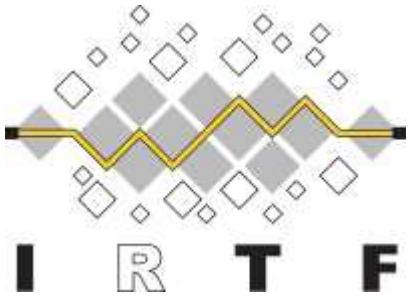


UFM RG @ IETF 114

March 29th 2023

Chairs: Jonathan Hoyland, Stephen Farrell

Charter: https://datatracker.ietf.org/rg/ufmrg
Mailing list: ufmrg@irtf.org
RG Wiki: https://wiki.ietf.org/en/group/ufm
Meetecho: https://meetings.conf.meetecho.com/ietf116/?group=ufmrg&short=ufmrg&item=1

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF 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.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

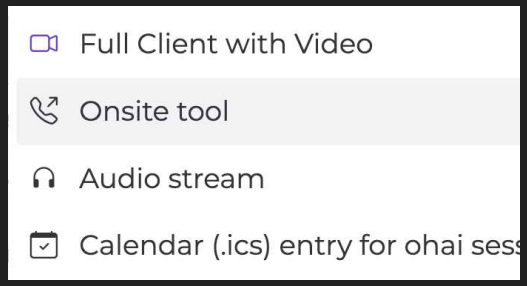
As a reminder:

- 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.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

IETF 116 Meeting Tips



In-person participants

- Make sure to sign into the session using the Meetecho (usually the “onsite tool” client) from the Datatracker agenda
- Use Meetecho to join the mic queue

Remote participants

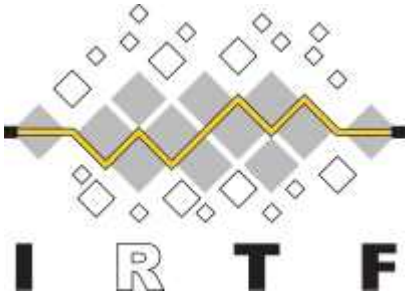
- Make sure your audio and video are off unless you are presenting or speaking during a session
- Use of a headset is strongly recommended

Mask Policy

- **Masks must be worn in meeting rooms**
- In meeting rooms, masks may briefly be removed for eating and drinking, but that cannot be an excuse to leave them off for long periods.
- In meeting rooms, active speakers, defined as those who are at the front of the room, presenting or speaking in the mic queue, can remove their mask while speaking.
- No exemptions for mask wearing, medical or otherwise, will be allowed.
- Masks must be equivalent to N95/FFP2 or better, and free masks will be provided.

Agenda

- Welcome and Agenda Bash (chairs, 10)
- Formal Methods background (Jonathan Hoyland, 15)
- Foundational End-to-End Verification of High-Speed Cryptography (Bas Spitters, 20, may shift to later in agenda)
- Current work-in-progress: VDAF analysis (Chris Patton, 15)
- Open discussion and review of (some) problem areas (all, 45)
- Delegated Credentials analysis (Jonathan Hoyland, 15, if time permits)
- Next steps/action (Chairs, 10)



Welcome!

- We’re a “proposed” IRTF Research Group
  - If we act like an effective RG, we’ll become an official RG
- IRTF != IETF (more in a bit)
  - Don’t say “working group” :-)
- We’ll prosper or flounder based on people doing or not doing work
  - We don’t get to make anyone do stuff
  - Don’t be shy about volunteering things
- Be tolerant if someone suggests something you think unlikely to succeed
  - Actually, just generally “be tolerant” :-)

Goals (summarised)

From https://datatracker.ietf.org/rg/ufmrg/about/

1. Bring together the IETFers and the researchers studying formal methods to share experience and ideas
2. Explore strengths and limitations of formal methods for systems specified in the IETF, and try improve things
3. Explore how formal methods can be usefully incorporated into IETF work
4. Educational material, examples, open source software that can be used by the IETFers
5. Experimentation with formal methods relevant to IETF

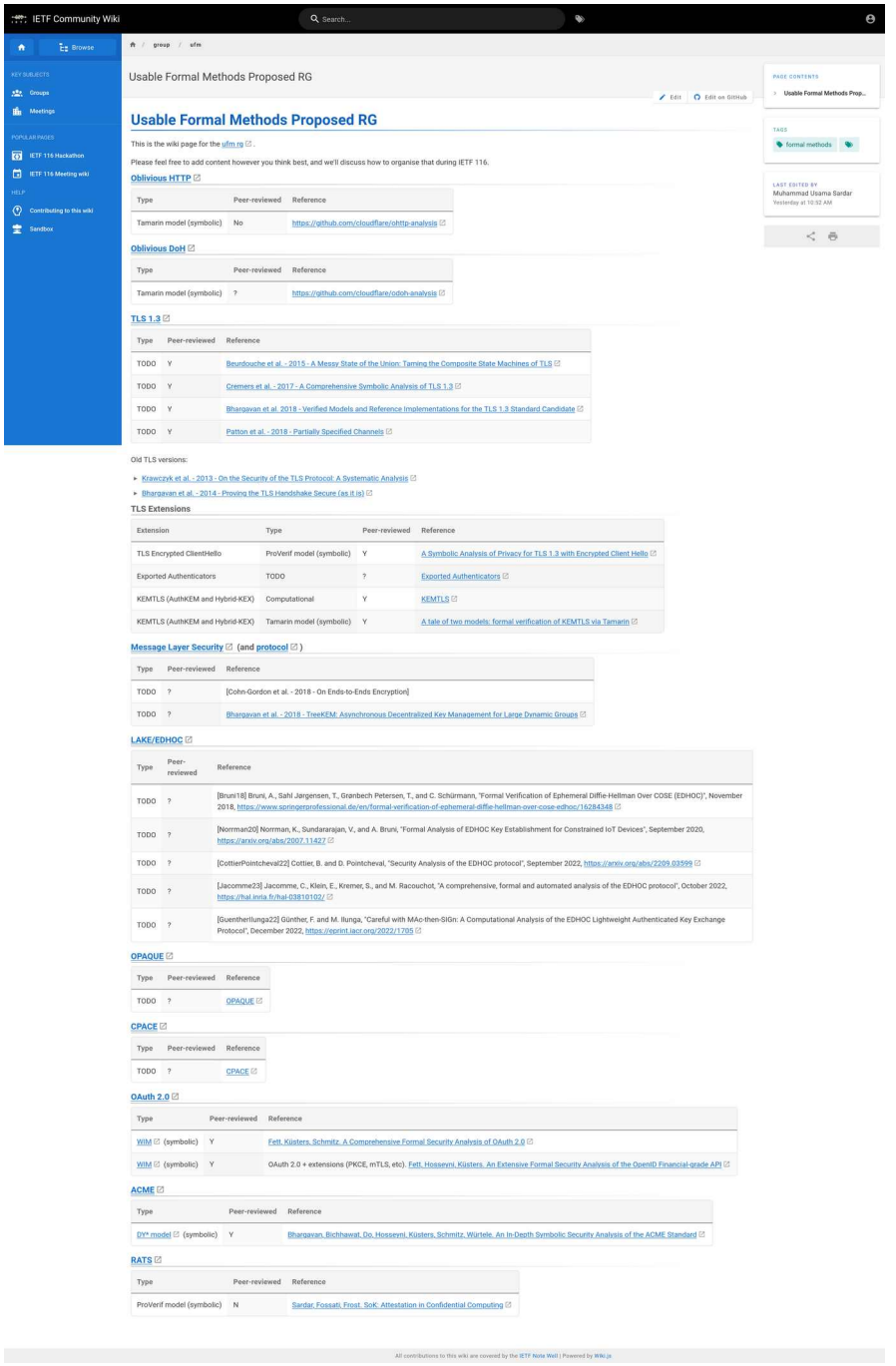
A word of caution

- No matter how smart we are, no matter how excellent our formalisms, we do not get to tell the IETF what to do
  - ‘Cause we’re an IRTF RG
  - We might help demonstrate that there’s some new better way to do things that gets voluntarily adopted in the IETF though
- Maybe consider formal methods work on IETF protocol foo as mostly an activity of the IETF foo-wg, but one that’s welcome to be discussed in UFMRG?
  - IOW: If you’re doing such work, consider yourself as participating in the IETF WG for the foo protocol, in addition to being someone doing work relevant to UFMRG
  - Why? ‘cause IETF WGs mightn’t welcome external protocol police parachuting in:-)

UFM RG Wiki

- Nice start: we have a bunch of references to formal analyses of IETF protocols (TLS, EDHOC etc)
  - https://wiki.ietf.org/en/group/ufm
  - Thanks to those who've already done edits!

- For later:
  - How'd we like to use that?
  - Who wants to volunteer to add what content (or structure)?



Open Discussion

- Sample problem?
- Scoping topics for the RG
- Why aren't these things already usable?
- You can't publish confirmatory results
- How do/should formal methods usefully fit in RFC development?
- How to model privacy?
- HOWTO structure wiki?

Sample Problem

- Wouldn’t it be nice if there were an IETF-relevant sample problem?
- Problem should be simple and generic enough to be widely understood by IETFers
- People developing formal methods (or tools) could show off their new stuff by showing how to approach the sample problem
- What to pick? Given crypto-heavy protocols are maybe not sufficiently-widely understood, maybe something related to email or BGP?
- Anyone want to volunteer to work on this?