University of Glasgow

Side Meeting on Usable Formal Methods

Colin Perkins

With help from Chris Wood

Discussion: irtf-discuss@irtf.org for now

Remote:
https://uofglasgow.zoom.us/j/82051131120?pwd=QlNqVU91cmpEYytnWjVLbldKMkI3QT09

Note Well

- This is an unofficial side meeting – not an official IETF or IRTF event
- But note that **the note well applies**

Agenda

- Goals and Motivation
- Motivating presentations
- Discussion of proposed charter
- Next steps

Goals and Motivation

- How should we describe and specify protocols?
- How can we ensure that network protocol specifications are consistent and correct, and verify that implementations match the specification?
- The IETF community has long used natural language to describe and specify protocols, with occasional use of formal languages and a some limited amounts of formal verification – is this the right approach? Are there benefits to more systematic use of formal methods? What are the factors limiting their adoption?

- Does it make sense to create an IRTF research group to explore such topics?

Short Presentations

- “A Bird’s Eye View of Formal Methods? And Why We Should Care”, Jonathan Hoyland
- “Formal Specification and Specification-Based Testing of QUIC”, Ken McMillan
- “Formal Security Analysis: OAuth and OpenID Connect”, Daniel Fett

RG Chartering Process

- The process for forming an IRTF research group is described in RFC 2014 – the IETF BoF process **does not apply**
- Draft charter and list of proposed founding members for a new research group are reviewed by the IRTF Chair and IRSG, then forwarded to the IAB for approval. The review considers:
  - Is the research area that the Research Group plans to address clear and relevant for the Internet community?
  - Will the formation of the Research Group foster work that would not be done otherwise?
  - Do the Research Group's activities overlap with those of another Research Group?
  - Is there sufficient interest and expertise in the Research Group's topic, with at least several people willing to expend the effort that is likely to produce significant results over time?

Discussion

- What are the obstacles to using formal methods in the IETF community?
- What are the research challenges where IRTF can provide useful support?

Proposed Charter – Context (1/2)

The process by which the IETF develops protocol standards is centred around production of documents written primarily in English prose. This facilitates discussion and consensus building, which are essential for the community to function, but the resulting documents suffer from the ambiguity of natural language and the inability to use automated tools to reason about, and validate, the specifications. The use of computer-aided verification, formal specification languages, and other formal methods can make specifications easier to validate against desired goals such as correctness and security and to define these goals. These technologies also support or enable automated tooling and reference code generation, but such approaches are not yet widely used in the IETF community.

Proposed Charter – Context (2/2)

There are technical and non-technical reasons for the slow adoption of formal methods by the Internet standards community. Technical limitations include performance of the verification tools which don't always allow to model or verify complex systems, the lack of support for specific kinds of proofs, and formalisms that may not be able to fully describe the complexity of modern protocols or the network environment. And, on the non-technical side, use of formal methods may require the use of unfamiliar protocol description languages and modelling tools, or assume familiarity with concepts that are not widely known by those writing RFCs. Further, there are questions around how such a shift in protocol design methodology would affect the collaborative social process by which consensus is built around the design of protocols.

Proposed Charter – Objectives

The objectives of the Usable Formal Methods Research Group are to:

- Bring together the Internet protocol standards community and the academic research community studying formal methods of protocol specifications to share experience and ideas;
- Explore and understand the strengths and limitations of computer-aided tools, verification languages, and other formal methods for specification and implementation of algorithms, protocols, and systems specified in the IETF, and to understand how those techniques can be improved to better support such specifications;
- Understand how formal methods can be incorporated into the development of technical standards, and to explore how this may affect the development of technical specifications and the consensus building process; and
- Produce resources such as educational material, for example formal analyses for existing IETF protocols, or open source software that can be used by the IETF to apply formal methods for improving technical specifications. Encourage and support experimentation with formal methods in the context of IETF, to gain insight into the feasibility, applicability, and limitations of such methods when applied to protocol development in IETF.

Proposed Charter – Examples

Examples of the types of formal protocol specification techniques to be considered include, but are not limited to, languages for specifying algorithms, modelling tools for specifying and validating protocols and systems, and tools and techniques to help derive formal models from natural language and semi-structured specifications. The group will consider the application of formal methods to several targets, including algorithms, network protocols at all layers of the protocol stack (low-level internetworking, routing, and transport protocols; security protocols; and applications and APIs), and distributed systems that compose these protocols.

Proposed Charter – Cooperation

The group will work closely with other IRTF research groups, with the IETF standards development community, and with researchers developing formal methods for protocol specification. It will meet regularly co-located with both IETF meetings and with related academic conferences and workshops (e.g., Security Standardization Research (SSR), Computer-Aided Verification (CAV), etc.).

An explicit non-goal is to propose changes to the IETF standards process, the RFC format, or the Internet-draft authoring process. The research group may explore ideas that require such changes, and is uniquely placed to discuss their implications with the IETF community, but the potential incorporation of such ideas into the standards process is a matter for the IETF and is out of scope for this group.

Next Steps

- Does this seem appropriate for an RG?
- What, if anything, have we missed?
- Are there volunteers to work on this topic?
- What would be the initial research directions?