IRTF UFMRG
Sample Problem Idea – IMAP SEARCH

May 2023

stephen.farrell@cs.tcd.ie

Idea of a Sample Problem

- (I think) we’d like an IETF-oriented, relatively simple, non-cryptographic specification
- To use as a sample so that people proposing use of some formal method can apply their method(s) to that specification
- Should help IETFers understand HOWTO apply methods
- Should help IETFers understand HOWTO describe their problems in a way that’s friendly to formal methods folks
- Might help formal methods folks improve usability when applying their methods to IETF problems
- Who knows, we might find out something about the problem itself as well?

One possible sample problem

- (A subset of) IMAP SEARCH?
- Used by IMAP clients (e.g. mail user agents) to search messages stored on an IMAP server (e.g. message store)
  - Apparently, some clients (on mobiles) make extensive use of IMAP SEARCH so as to use less battery and limit use of local storage
- RFC9051 section 6.4.4
  - ...and related bits of ABNF
  - https://datatracker.ietf.org/doc/html/rfc9051#name-search-command

Example

- Client can use the result of a SEARCH command to FETCH headers of interesting messages
  - https://datatracker.ietf.org/doc/html/rfc9051#section-6.4.4.4

```
C: A282 SEARCH RETURN (SAVE) FLAGGED SINCE 1-Feb-1994
    NOT FROM "Smith"
S: A282 OK SEARCH completed, result saved
C: A283 FETCH $ (UID INTERNALDATE FLAGS BODY.PEEK[HEADER])
S: * 2 FETCH (UID 14 ...
S: * 84 FETCH (UID 100 ...
S: * 882 FETCH (UID 1115 ...
S: A283 OK completed
```

Why IMAP SEARCH?

- It’s not a cryptographic protocol
- Widely implemented and used so if we did find something that might even be useful
- Relatively rich syntax that could hide problems and/or provide ways for formalisms to “shine”
  - You can search based on lots of combinations of attributes
- Stateful responses e.g. via UIDs
  - But UIDs can (I believe, but don’t know:-) be invalidated e.g. if a second UA (for the same account) moves a message while search state in use
- I suspect (but don’t know) implementers might be able to point formal methods folks in good directions with war stories

If that, then...

- Would want to get help from someone familar with IMAP and someone familiar with some formalism
- Document the subset of IMAP SEARCH we want in an I-D
- Check that’s sensible but don’t (yet) publish as an RFC
  - So an RG last-call type thing
- Try get formal methods folks to attack the sample problem with their favourite method, show us how they did that and what (if anything) they found
- Publish the collection of those artefacts somehow
  - ANRW papers or one or more RFCs or some mixture

So...

- Independent of IMAP, what do people think of the general plan?
- Anyone want to work on this particular one?
- Anyone want to work on a different one?
- >1 sample problem would be just fine
  - At least, starting on >1 is fine, some attempt(s) might founder
- Let’s discuss!