draft-ietf-opsawg-mud-05

Eliot Lear

IETF98

Status

- Document in last call
- Normatively depends on draft-ietf-netmod-acl-model
  (it’s completed LC and there might be one or two changes)
- We have some implementation experience and more plans

Comments received thus far

- A MUD file attribute indicating the expected MUD URL emission method is of security value. (Max Pritikin)
  - Issue: it's possible to identify a downgrade attack within a deployment if we know how the file can be delivered.
  - Proposed approach: include an enumerated type that indicates this, and a list of accepted methods.
  - Whatever the approach it must be AUGMENTable
- A list of extension names to be used (Pritikin)
  - Issue: without the list, you don't know if someone is just shoveling garbage at you
  - Proposal: add a container that contains such a list

More issues

- Recommended time for updates should be clearer (anonymous)
  - Issue: too short an update time means that a virus can take hold before MUD servers do an update
  - Proposal: provide specific guidance on the value; stating a lower maximum (say 72 hours)
- More internationalization (lear)
  - Issue: the description in metadata is not internationalized
  - Proposal: change it to a URL that points to a description (can handle language and other things appropriate to the deployment)

Should the MUD URL be used for more than just MUD? (Pritikin, Fluffy, Maybe Henk)

- Issue: devices may want to point to multiple services. Having an extension for just MUD means that each of these other services requires an additional extension (and more cert space)
- Proposal: Use a fragment to indicate the specific service (MUD, ANIMA, other things) that gets added by the controller in the right context
- Eliot’s take: this causes implementation minor complications
  - All services need to hang off of the same base URL
  - MUD file servers would have to parse fragments and route accordingly
  - MUD controllers would have to do a modest bit of additional processing

Examples

OLD:

https://foo.example.com/.well-known/mud/FrobMaster3000v1

NEW:

https://foo.example.com/.well-known/mfgr/FrobMaster3000v1?service=mud

Other issues?

- (Here’s your chance)

Next Steps

- Resolve these issues
- Expecting a few more reviews (may request a bit more time in WGLC)
- Put out new draft to address acl-model changes and review edits
- Off we go…