Meeting Notes: 1st Plug Fest Planning Meeting

Meeting link:  [https://meet.lucidmeetings.com/meeting/235857](https://meet.lucidmeetings.com/meeting/235857)

- Agendas on Lucid / Issues on GitHub (GH)
- In agenda: Horizon = future (known work-in-progress)
- SaltStack uses a Zero MQ pub / sub for message transfer; not aware of anyone working with OpenC2 that are using Zero MQ
- Duncan:
  - Currently New Context has a GH repo with AWS controller code; creates and deletes instances of AWS compute elements (create, start, stop, delete, query);
    it's linked from the [Other OpenC2 Work](#) list
  - Horizon: They are working on equivalent capability for GCP
  - Duncan wants to demonstrate a vendor-agnostic cloud exchange using both (a planned use case he hasn't developed yet)
- Joe stated there's a range of participant complexity (one or two commands, vs. much more); he encourages everyone to bring anything they've got to the PF
  - First portion of PF will be exercise interoperability / "verify interoperability / interworking"
  - Second portion demonstrate use cases
- Duncan:
  - Agrees with that overall approach.
  - Favors preparation beforehand to maximize the value of time at DreamPort; minimize the setup difficulties
  - Suggests a "Table Top Exercise" (TTX) for reviewing messaging between nominally compatible participants, specifically review the JSON that would be exchanged
    - Find some problems ahead of time
    - Formulate a "test plan" of who is talking to whom
    - Uncover non-OC2 issues (e.g., IP version)
    - This is not a preliminary test, it's a coordination activity
  - Hackathon: TTX should uncover gaps where "someone can whip something up" in hackathon time
- Joe:
  - Reminder about [participant matrix](#) on GH, encourages review and corrections of that to disseminate information about capabilities
  - Encourages OOB communications, concerned don't have enough meeting time arranged for a TTX
- Duncan:
  - Thinks TTX requires more than what's in the matrix. Go beyond identifying the action to the actual JSON message content
- Not sure what Joe is talking about with "having JSON schemas", thinks command / responses still useful even with schema

- **DaveK:**
  - For schemas was not envisioning writing a complete AP
  - Would reverse engineer from JSON command / response messages
  - Ready to work with people who have example messages to share

- **DannyM:** re Duncan working on C2C use case
  - Is sFractal a Producer or Consumer? Duncan: Consumer only. Writing code for plug fest for Consumer side. (As system engineer / standards guy, working everything everywhere)
  - Assumptions re: Producer? Assuming someone else will create a Producer to be "quarterback" for C2C scenario
  - Creating schema for Consumer? Not planning on a schema, prefers sample JSONs; doing this to drive effort; will be all open source.
    - Another mention of OC2 + SBoM = "killer app"
    - Wants to flesh that out; get other opinions on approach
  - HTTPS or other? HTTPS is the plan; authentication, certificate supply are open issues.
  - Danny interested in orchestration piece but concerned about LOE; believes the OpenC2 Integration Framework (OIF) Orchestrator can be Producer to sFractal's Consumer
  - Duncan will be offline most of January; will be doing some coding "for relaxation"
  - Danny & Duncan will talk about the details after this meeting

- **Joe:**
  - Danny / Duncan dialog is "perfect", hope more of those happen ("full mesh" of communications)
  - C2C:
    - Since PF tech talk, McAfee is going to put "a similar scenario" out there
    - Duncan has noted that health care industry interested in a similar thing

- **Duncan, for C2C:**
  - Does OIF have capability to do the Producer portion? Joe: doesn't believe it's set up to execute full Courses of Action.
  - Duncan: can it handle command / response?
  - Danny: yes, based on a JSON schema (HII can make the schema).
    - OIF Orchestrator is a command generator similar to Efrain Ortiz's.
    - Assumes Consumer will know what to do with command.
    - Currently returning replies within the same session

- **Duncan thinks PF should focus on Command / Response interoperability, before COA / Playbook use cases**
  - Joe: agrees this make sense. Will need placeholders / pass-throughs / stand-ins for functional blocks to demonstrate robustness of OC2
  - "All orchestrators are welcome".
  - Also doesn't want to discourage people who are prepared to show off use cases
- Duncan concurs.

- Joe: need to start clustering participants with common interests; use email list to identify, encourage clustering

- Duncan: where are BAE (RF) and Denver Airport use case? Has heard discussion but hasn't seen it written down anywhere.
  - **ACTION (Joe):** add those to the matrix

- Danny:
  - Sees OC2 as different from other standards, interoperability is "paramount"
  - Wants PF to identify "small details" that obstruct interoperability; document what's needed to fix
    - Duncan concurs

- Joe:
  - Will forward BrianB email about commands that Symantec supports to the PF mail list
  - Uncertain where AT&T stands WRT OpenDXL

- Duncan: really wants to get DreamPort answers for FAQs documented on plug fest page?

- Danny:
  - Is it OK to move beyond the OASIS specs? e.g., using MQTT (not standardized) vs. HTTPS (standardized)
  - Joe: absolutely not taboo; the range of existing specs very limited (boring), need to explore beyond that
  - Duncan: agrees, *have to* extend beyond our specs (and then capture on the OASIS TC standards side)
  - Danny: have MQTT document started, but very rudimentary ([GH repo link](#); no meaningful content there yet)