Language Subcommittee Meeting

Tuesday, July 31, 2018

Purpose: Weekly Language SC Meeting

Desired Outcomes:

Weekly Language SC Meeting

Agenda

1.0 Welcome

2.0 Material Changes - call for objections

2.1 Issue 97 - one target type

2.2 Issue 104 - "core actuator profile"

2.3 Issue 93 - endangered actions

2.4 Issue 105 - JADN/Tables Normative

2.5 Issue 98 - numbers in json serialization

3.0 Informative Changes - call for objections

3.1 Issue 103

3.2 Issue 99

4.0 Material Changes Triage

5.0 Threads

6.0 Informative Change Triage

7.0 Issue Discussion

8.0 Wrap up

Meeting Attendance

In Attendance

Danny Martinez (G2), David Lemire (G2), Duncan Sparrell (sFractal Consulting LLC), Joe Brule (National Security Agency), Andy Gray (ForeScout), April Jackson (G2), Charles White (Fornetix), David Hamilton (AT&T), Efrain Ortiz (Symantec Corp.), Lisa Mathews (National Security Agency)

Regrets

Jason Romano, Allan Thomson (LookingGlass), Andrea Andrenacci (Moviri SPA), Andrea De Bernardi (Moviri SPA), Bret Jordan (Symantec Corp.), Brian Berliner (Symantec Corp.), Chet Ensign (OASIS), David Kemp (National Security Agency), David Waltermire (NIST), Dennis Young (FireEye, Inc.), Duane Skeen (Northrop Grumman), Gerald Stueve (Fornetix), Glen Goffin (Lumeta Corporation), James Meck (FireEye, Inc.), Jason Keirstead (IBM), Jason Webb (LookingGlass), John-Mark Gurney (New Context Services, Inc.), Jyoti Verma (Cisco Systems), Kent Landfield (McAfee), Michael Stair (AT&T), Natalie Suarez (NC4), Philip Royer (Phantom), Radu Marian (Bank of America), Robin Cover (OASIS), Sourabh Satish (Phantom), Trey Darley (New Context Services, Inc.), Sridhar Jayanthi (Individual)

Full Meeting Record

View this record online at https://meet.lucidmeetings.com/meeting/192778

1.0 Welcome

- register attendance on OASIS at https://www.oasis-open.org/apps/org/workgroup/openc2/event.php?ev
- LSC Contacts
  - Jason Romano - DM on Slack preferred (@romano), jason.romano@gd-ms.com, jdroman@nsa.gov
  - Duncan Sparrell - DM on Slack (@sfractal), duncan@sfractal.com
- Annoucements
  - Current Working Draft is WD08-wip. Please make your additions and updates there. See google docs https://docs.google.com/document/d/1hOv8NR-jo6JUVXcZaO8t-MzzPFURziTjIB1mXxptKQE or Github openc2-oc2ls/oc2ls-v1.0-wip.md. Issues are recorded on github
  - Progress was made at F2F and agreed to changes will be summarized again today to make sure we got them correctly
- Schedule Review
  - https://docs.google.com/presentation/d/1LouMl_K54yDRaQAYaZrQS_ZXJv5nNLkwYCDsPX

Notes and Action Items

https://www.oasis-open.org/apps/org/workgroup/openc2/event.php?event_id=47274 is the link to record attendance

---

2.0 Material Changes - call for objections

One slide on each of the following

1. Issue 97 - one target type
2. Issue 104 Replace “core actuator profile” with text requiring all consumers to response to query openc2
3. Issue 93 - endangered actions - reserved vs under consideration
4. Issue 105 Tables are normative if conflict with JADN
5. Issue98 - JSON Serialization of Numbers

2.1 Issue 97 - one target type

Issue:

To resolve ambiguity and to be more precise in section 2.2.1 in that only one type of target is allowed

Current wording:

“The TARGET of an OpenC2 Command may include a set of targets of the same type, a range of targets, or a particular target. Specifiers provide additional precision for the target.”

New wording:

“The TARGET field in an OpenC2 Command MUST only contain one type of target (e.g. ip_addr). The TARGET SPECIFIERS provide additional precision to specify the specific target (eg 10.1.2.3) and MAY specify a range of the same type (e.g. 10.1.0.0/16).”

A separate issue (#102) was raised on whether specifiers should be a list.

Notes and Action Items

agreed to

2.2 Issue 104 - “core actuator profile”

- remove section 4 - core actuator profile
- add text requiring all openc2 consumers to respond to the query openc2 command
- Section 4 read:

“4 Core Actuator Profile

Editor’s Note - TBSL - This section be included in a future iteration (probably iteration 5) prior to submitting for Committee Specification.

This section defines the core functions applicable to every OpenC2 actuator.

Command and resulting response:

- *One action: query*
- *One target: openc2*
- _Target specifiers: versions, profiles, schema“_

New proposed text is in section 3.3.2.13 Type Name ActionTargets:

“All OpenC2 Consumers SHALL respond to a command with the fields:

- ACTION=query,
- TARGET=openc2,
- Target Specifiers of the query_items in section 3.3.2.8 (ie versions, profiles, schema, pairs)”

Notes and Action Items

is 3.3.2.13 the right place to put it? Joe objected. Replace section 4 with new section ‘required commands’. No one disagreed.

2.3 Issue 93 - endangered actions

Issue:

We don’t allow extensions to actions per section 2.2.2 “Only the actions in Section 3.2.1.2 SHALL be used”. Should we preclude implementors from using the ‘endangered’ actions (which the current wording might re read as doing) or should we allow implementors to use the endangered actions in custom actuator profiles with the understanding they might be removed in furture versions unless they bring in use cases and the TC approves.

Current Wording:

- “The following actions are reserved for future use and are not valid actions in this version of the Language Specification.”

New Wording:

- **“The following actions are under consideration for use in future versions of the Language Specification. Implementors MAY use these actions with the understanding they may not be in future versions of the language unless use cases are presented and the TC accepts the action into the table. All commands MUST only use actions from this section (either the table or this list).”**

Notes and Action Items

No disagreements.

2.4 Issue 105 - JADN/Tables Normative

Somewhere add “In event of a conflict between JADN OpenC2 schema and the property tables, the property tables will be the normative definition.”

Notes and Action Items

No disagreements. In SLPF a sentence like this went in the conformance section, and in the begining of the annex containing the schema. No one disagreed.

2.5 Issue 98 - numbers in json serialization

Agreed at F2F to follow RFC 7493 for integers. Add “JSON serialization shall be in accordance with RFC 7493.” to integer row in section 3.1.1.

Notes and Action Items

No one disagreed

3.0 Informative Changes - call for objections

1. Issue 103 - rename appendices as annexex and order
   - Acronyms
   - Examples
   - Acknowledgements
   - Revision History
2. give editors permission to fix issue 99 (id missing in section 2.2.1)

Notes and Action Items

No one disagreed

3.1 Issue 103

Notes and Action Items

per 3.0 - no one disagreed with resolution proposed on previous slide

---

3.2 Issue 99

Notes and Action Items

per 3.0 - no one disagreed with resolution proposed on previous slide

---

4.0 Threads

1. Review Efrain's use cases that got deferred in previous meeting due to time constraints on preparing for F2F. See https://github.com/oasis-tcs/openc2-usecases/tree/master/Symantec
2. Review Examples Duncan suggested in a previous meeting (9.3.3 albeit that is a misnumbering). See https://docs.google.com/document/d/1hOv8NR-jo6JUVXcZaO8t-MzzPFURziTjIB1mXxptKQE/edit#bookmark=id.wu9cl96b6dbr
3. Review Duncan's use cases (25,26) that got deferred. See https://github.com/oasis-tcs/openc2-usecases/commit/2e425fd81f1813bd89de3d26057a950bc9bb3bf6#diff-68fa3451a903b8515c76e18ea17f634f
4. Review other new use cases
5. Review plan to update use cases to wd07/8

Notes and Action Items

We reviewed several of Efrain's use cases.

Issue came up on 'command_ref' of Symnatec allows for multiple consumers to respond and producer to tell them apart. Danny raised issue that might be useful for others - since openc2 doesn't currently cover.

a response contains an id reference, which helps correlate a response to a command. However in the case when multiple actuators are responding an actuator identifier would be needed in order to make that correlation.

5.0 Material Changes Triage

Notes and Action Items

covered in section 2

6.0 Informative Change Triage

Notes and Action Items

covered in section 3

7.0 Issue Discussion

1. Issue 102 - target specifiers to allow a list?
2. default response
   - to query openc2
   - to any command
   - in language spec or in actuator profile
   - if defaulted in language spec, can actuator profile ‘override’?

Notes and Action Items

We did not get this far in the agenda

8.0 Wrap up

Discussed: all action items; created in this meeting

Chat Transcript

- { “id”: “017b53ed-0a59-4026-b071-092083315645”, “action”: “allow”, “device”: {}, “actuator”: { “endpoint”: { “asset_id”: “string” } }, “args”: { “start_time”: “2018-06-25T14:01:03.952Z”, “stop_time”: “2018-06-25T14:01:03.952Z”, “duration”: 0, “response_requested”: “ack”, } }
  Efrain Ortiz
- https://github.com/oasis-tcs/openc2-usecases/tree/master/Symantec
  Efrain Ortiz