

Language Subcommittee Meeting

Tuesday, May 8, 2018

Purpose: Weekly Language SC Meeting

Desired Outcomes:

Weekly Language SC Meeting

Agenda

- 1.0 Welcome
- 2.0 Material Changes - call for objections
- 3.0 Informative Changes - call for objections
- 4.0 Material Changes Triage
- 5.0 Informative Change Triage
- 6.0 Threads
- 7.0 Issue Discussion
- 8.0 Wrap up

Meeting Attendance

In Attendance

Danny Martinez (G2), David Lemire (G2), Duncan Sparrell (sFractal Consulting LLC), Jason Romano, Joe Brule (National Security Agency), Brian Berliner (Symantec Corp.), Charles White (Fornetix), David Hamilton (AT&T), David Kemp (National Security Agency), Efrain Ortiz (Symantec Corp.), Gerald Stueve (Fornetix), Jason Webb (LookingGlass)

Regrets

Allan Thomson (LookingGlass), Andrea Andrenacci (Moviri SPA), Andrea De Bernardi (Moviri SPA), Bret Jordan (Symantec Corp.), Chet Ensign (OASIS), David Waltermire (NIST), Dennis Young (FireEye, Inc.), Duane Skeen (Northrop Grumman), Glen Goffin (Lumeta Corporation), James Meck (FireEye, Inc.), Jason Keirstead (IBM), John-Mark Gurney (New Context Services, Inc.), Jyoti Verma (Cisco Systems), Lisa Mathews (National Security Agency), 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/187957>

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@gdms.com, jdroman@nsa.gov
 - Duncan Sparrell - DM on Slack (@sfractal), duncan@sfractal.com
 - Announcements
 - We are now working on Working Draft 06. Please make your additions and updates there.
<https://docs.google.com/document/d/1sHLopmRDhEofKh6OsK0dQzf31MzvIALeJ-IrbfvKIUQ/>
 - Schedule Review
<https://docs.google.com/presentation/d/14q1TvK5u6IaJD0Z882YGo3NCbRLZhrYL7XppBxqtGw/edi>
-

2.0 Material Changes - call for objections

Revis 3/27 proposed changes to validate what accepted/rejected/deferred - see <https://meet.lucidmeetings.com/meeting/186185>. Note these were ballot comments so if nothing else we should make sure documentation reflects outcome on issues 83,84,85,86

Notes and Action Items

The meeting reviewed again the ballot comments and the associated proposals made at the April 3 LSC meeting.

1. CSD03 Ballot Comment in Issue 86
 - Rationale <https://github.com/oasis-tcs/openc2-oc2ls/issues/86>
 - Proposed changes <https://github.com/sparrell/openc2-oc2ls/commit/899a75dbc32a65101f64c6d7f97>

- Resolution - The proposal to include Version in query was agreed to. It was also agreed to allow multiple versions to be returned if the OpenC2 consumer was backware compatible with one or more other versions
2. CSD03 Ballot Comment in Issue 85
 - Rationale <https://github.com/oasis-tcs/openc2-oc2ls/issues/85>
 - Proposed changes: <https://github.com/sparrell/openc2-oc2ls/commit/1544a6d6dd05c784be6777933> and <https://github.com/sparrell/openc2-oc2ls/commit/19644c73f5df2b084cc140fc8d49f21118a07b1a>
 - resolution - The LSC agreed with the proposed interpretation - that the Header information may or may not be in the JSON data of the command. It is required that the information be part of the message, but the Header information may be part of the transport and not necessarily carried as JSON. When the Header information is included in the JSON, it must be in the format per the LS. Note the above is more nuanced than proposed text in the ballot comment and appropriate text must be added to the LS
 3. CSD04 Ballot Comment in Issue 83
 - Rationale <https://github.com/oasis-tcs/openc2-oc2ls/issues/83>
 - Proposed changes: <https://github.com/sparrell/openc2-oc2ls/commit/90cfbb998dc68defec206e14ba>
 - resolution - The proposal to delete “*It may be documented in this Language Specification or within another standalone specification developed by the Implementation Considerations Subcommittee.*” when discussion Version in section 3.2.1.5 was initially objected to by Joe Brule but he withdrew the objection in subsequent discussion.
 4. CSD04 Ballot Comment in Issue 84
 - Rationale <https://github.com/oasis-tcs/openc2-oc2ls/issues/84>
 - Proposed changes:
 - A,B) [sparrell/openc2-oc2ls@2713017](https://github.com/sparrell/openc2-oc2ls@2713017)
 - C) [sparrell/openc2-oc2ls@0862089](https://github.com/sparrell/openc2-oc2ls@0862089)
 - D) [sparrell/openc2-oc2ls@c75f5b3](https://github.com/sparrell/openc2-oc2ls@c75f5b3)
 - E) [sparrell/openc2-oc2ls@3fb830f](https://github.com/sparrell/openc2-oc2ls@3fb830f)
 - resolution
 - Wrt proposal to have just one extension prefix (x-) to replace the 4 proposed prefixes (ap,ip,vp,fs) - the LSC agreed to let Joe (wants 4) and Duncan (wants 1) to resolve offline. Joe and Duncan met and agreed to 1 prefix “x-”, ie that extensions and customizations would not be categorized into ‘types’ of extensions.
 - * Sidenote. There was some confusion during the discussion on ‘types’ of extensions and someone thought there we were discussing forbidding custom extensions by vendors or users. This was never the intent in eihers proposal. To avoid this confusion in the future, we intend to use the term ‘custom’ profiles (similar to STIX custom properties) when discussing any Actuator Profiles other than those with OpenC2 draft specifications. The x- is for those profiles, regardless of whether they are made by a vendor, a user, an industry consortia, or

another recognized standards organization.

- Wrt proposal to avoid word ‘vendor’ when describing extensions (since users might make as well) - it was agreed and Duncan was tasked with working the details as editor. STIX uses ‘custom’ so where possible we will adopt wording similar to STIX
- Wrt proposal to include all the Arguments in the Language Specification (as opposed to some in Language Specification and some in the Acutator Profiles), Joe Brule objected. Duncan and Joe spoke offline after the meeting and Joe agreed to withdraw his objection (ie agree to put in the Language Specification the arguments in the existing Actuator Profile). It was agreed this could be revisited later if the list became unwieldy or churn was too great.

3.0 Informative Changes - call for objections

4.0 Material Changes Triage

5.0 Informative Change Triage

6.0 Threads

Discussion on “query>>openc2” examples:

https://docs.google.com/document/d/1vF7e9Mp_45u-RuPrbRiIoIUcOmoDCkKEAcJKCr6tvvgA/

7.0 Issue Discussion

Presentation on OpenC2 Message Generator: <http://openc2.ortizonline.com/>

8.0 Wrap up

Discussed: all action items; created in this meeting