Architectural Reference Working Group

Meeting Minutes

23 Sept 2021

Attendees: **Russ Warren, Dennis Moreau, David Kemp, David Lemire, Mark Mastrangeli, Forrest Hare, Mike Rosa, Andrew Beard, Mudit Tyagi, Claudia Rauch, Dee Schur, Guy Martin**
Agenda:

Here is the agenda for our call Thursday.

(1) Review an initial pass at mapping the OCA architecture to OpenC2 and PACE

The document covered mapping the OCA architecture commands and response flows (Lines on our C4 diagram) with the OpenC2 commands defined in the current specification. The OCA ontology will align with this effort. The PACE project is also mapping to OpenC2. We discussed the table that mapped the OCA architecture actions to the OpenC2 commands. OpenC2 does support request and responses (99% OpenC2 uses this). We discuss the support for synchronous and asynchronous responses. OpenC2 is normally synchronous. Language supports notifications or events, but none yet defined. Pub/sub fabric and http protocol layers are supported by OpenC2. OpenC2 message has request, respond, notification. Query is an action that goes into a request. Request carries OpenC2 action. Need an action and a target for the table. Example Query for collect posture action (for PACE). Will need an evaluator and assess action yet and will probably have to add that to OpenC2. Target refers to IP address of a Deny, for example. Action and target are how we can best represent the mapping in the table. Dave Lemire will help with the draft table. Quarantine should map to contain. We will need to specify the target(s) for the OCA actions.

We then discuss the OCA architecture communications need. OpenC2 has the MQTT transfer specification out for public review. We discuss OpenDXL has a provider of a communications layer for OpenC2 and OCA. We discussed the Security Services (our OCA projects PACE, STIXShifter, Kestrel). These are aimed at facilitating collaboration across security capabilities.

We discussed authentication and authorization on the message bus. OpenDXL provides an authorization layer. OpenC2 is going to provide a signature-based approach. OpenDXL is widely used today and could provide value to OpenC2. Mark will investigate what can be shared and we can discuss this topic in our next workgroup meeting. OpenDXL broker, manager, and multiple clients (and API spec) have been open sourced by McAfee. Another valuable part is the Integration Pattern Engine (IPE) that can bridge between different fabrics (ie. MQTT to XMPP or MQTT to Kafka, MQTT to HTTP). This would be valuable to leverage this technology.

We discussed next steps. We need to work on Actuators so we can define what OCA needs in this area. OpenC2 actuator is a function. A packet filtering function is an actuator. It is device independent. An actuator is a cyber-defense function. An actuator profile maps the OpenC2 actions on to a specific actuator function. There are 5-10 actuator profiles under development in OpenC2. An OpenC2 producer generates and sends OpenC2 commands and accepts responses from actuators. OpenC2 commands are atomic things.