CACAO Technical Committee

Meeting Minutes

Date: 15 October 2019  Time: 15:00 UTC

Link to Meeting Agenda/Slides

Attendees
Allan Thomson  Jason Webb
Allen Hadden   John Morris
Andrew Storms  Jorge Aviles
Anup Ghosh     JP Bourget
Arnaud Taddei  Jyoti Verma
Bret Jordan    Karin Marr
Chris Dahlheimer Lior Kolnik
Chris O’Brien  Mahbod Tavallaee
Emily Ratliff  Paul Patrick
Frank Rodgers  Ryan Hohimer
Frans Schippers Shawn Riley
Gerald Stueve  Tim Zhan
Henry Peltokangas

Quorum was achieved during this meeting.

Action Items
- [TC members] Review requirements and make comments/suggestions
- [TC members] Add example playbooks to Use Case document to flesh out requirements

Notes
The TC reviewed the draft specification document
https://docs.google.com/document/d/1uQCWIItomFvQ466MdGhx_01HfJ4HOfboIRftmomVvrgYe
edit#

Talk at the National Press Club at Borderless Cyber went well, some attendees have joined the
TC. The goal was to drive participation in the working group since we need to ensure that the
model that we create is implementable.

Three documents that we have so far(if you have more please suggest them)
- Requirements document
- Use cases
- Specification

Requirements - capture the basic requirements, look through the list and make comments and
suggestions.
Use cases - capture high level use cases and key elements about the use case (i.e.
human-human). Bret added example playbook in text based format. Ideal get 1-3 fleshed out
playbooks in this document to have something concrete to work with.
Specification - start capturing things that we know are going to be part of the specification

Bret might add diagram because people are used to working in pictures for playbooks
Allan has some playbooks that need to be scrubbed and could be contributed. Where do you
want them? In use cases document.

Jyoti: question about Target - are we combining sensors or who the action will apply to?
Bret: Target is maybe the wrong term since it is overloaded.
An example target for a desktop support quarantine operation is to move a system to VLAN
500. In that case, the target is a router or switch.
Allen: need UUID and an argument identifying system that you are moving.
Also need an argument for VLAN and maybe additional arguments.
Define a mechanism with which to pass arguments to other playbooks.
Allen suggests a Type, value mechanism, so no ordering and easy to add additional arguments.
Bret updated Network Support section to reflect Allan’s comment
Bret: any suggestions to replace term Targets?
Jyoti: need to separate sensors from actuators
Bret: please write a proposal for what you would like to see

Control Logic
Probably the hardest section
Metadata is easy and we have a lot of previous work to leverage
BPMN, BPMN-lite? Programming language?
Actions need to be automated and not just the process
JSON based solution desired to help drive adoption - Web 2.0 most commonly used format
XML delayed the adoption of STIX and TAXII, switched to JSON and adoption is rapidly advancing
Allan: want to consider mappings to other languages

Question for this group - what we we want to start with?

Karin: are we considering using OpenC2
Allan: we are focused on the playbooks, action is connected with the playbook; playbook able to make openc2 commands, netconf and proprietary . Not intended to mandate action language.
We want to focus on the workflow and playbook and how it connects to the others. OpenC2 does not do everything that a member company needs and that is probably the case for other companies.
Karin: experimenting with OpenC2, using OpenC2 in playbooks
Translation between BPMN and JSON is doable. Is selection of JSON a set decision and voted on?
Bret: no it isn’t voted on; we started with it because it is most used. Vast majority of solutions that would be implementing this at scale would use JSON. If we build it at scale, then the data model can be changed as needed.
Allen: as long as model can be translated into whatever vendors are using then that is success. XML, JSON doesn’t matter as much.
Allan: having worked with xml, cordobas, and a variety of schema modelling tools, the ease of which you can convey a model as well as the ease with which you can prototype something is also important. Impacts the ability to express ideas.
Allen: object model is quite important, the form in which we are talking about it is important, it is important to have one language to express this. BPMN is a mature specification and have done everything that we are likely to want to do from a process model. As long as we are aware of BPMN and are learning from it, then we are fine. It should be a conscious model to diverge from BPMN. Consistency in the model is important.
Bret: we want to leverage your expertise in BPMN in this space
Need to be able to encapsulate a lot of atomic actions - OpenC2 etc.

JP: what is usability for this spec
2 users: developers and security engineers
Need to address this as part of core requirement
Champion for the most usability
Need more clarity around what we are modelling before we can start writing a specification for the objects/actions

Allan: High Level Structure
Borrowing from BPMN with this separation between Action and Control Flow

JP: How are we separating functional requirements from specification requirements? Want to be able use import playbooks into CI and test them

Bret: add these comments as prose text into document. We want to capture these ideas in the document.

Arnaud: think about hyperscale, example 1 billion containers. This may highlight some issues here.

Bret: agreed, this is something that CIOs desperately need, but we need to crawl, walk, jog, etc. to identify a minimum viable product

Allan: what do TC Members want to do between now and the next meeting. We haven’t started addressing control logic yet. Do we want to work on examples first?
Arnaud: focus on examples collected over the next month

Allan: we need to start somewhere, where do we start?
Rough consensus for starting with use cases.

End of meeting