CACAO Technical Committee
Meeting Minutes

Date: 18 February 2020

Attendees

Allan Thomson  
Bret Jordan  
Andrew Storms  
Anup Ghosh  
Chris Dahlheimer  
Emily Ratliff  
Frans Schippers  
Gerald Stueve  
Jason Keirstead  
Jason Webb  
Jim Meck  
John Morris  
Jorge Aviles  
Jyoti Verma  
Lior Kolnik  
Marco Caselli  
Karin Marr  
Paul Patrick  
Shawn Riley  
Stephanie Hazlewood  
Tim Zhan  
Ryan Hohimer  
Vasileios Mavroeidis

Action Items

- AI for TC (all) - review use case document
- AI for TC (all) - review common specification document and other TC documents (see TC Cover Page at https://docs.google.com/document/d/1ycBm_H5TRY5d09fnjCdIBKrSOiJax2OzJHsqAW0ROHU/edit )

Meeting Notes

Bret asked if the TC reviewed the docs

Jason Keirstead (IBM) asked if we should include any IPR statement in the doc.
Better to do that in the spec, not the committee note draft.

We want to have a ballot as soon as possible- Bret, Allan
John Morris: Licenses for the playbooks, freely share-able vs marketable version. How can we protect access to open playbooks? Following versions may step on the initial versions (transition from open to marketable versions).

Jason K: This is also to protect the open playbooks, avoiding complications in the case that there is not a specific license key specified (legal ambiguous situations if we don't specify in the playbook that is for open use / sharing)

Allan: Agrees that it should be clear in the playbook. If there is no explicit license in the playbook then it can be considered open-source. Security Concern - it needs to be always digitally signed otherwise can somebody remove the license. This should be added in the requirements doc. So Allan’s opinion is that both cases should be able to be characterized in a playbook.

Bret: Tagging a playbook (e.g., TLP), we need a common way of doing it. Mark.3 in the Marking section can include the way of licensing playbooks. Allan agrees adding them in that section.

**Motion for ballot:**

Bret Jordan asked for a motion to open a ballot for approval to publish the requirements document as a committee note draft after a new version has been uploaded with the licensing update.

Allan Thomson from Looking Glass motioned
Andrew Storms from New Context seconded

Bret: 2nd Committee Note Draft the updated doc (working draft). In the following weeks make your comments into the working draft to move on issuing a 2nd Committee Note Draft.

Anup: Use case 1 made sense, didn’t understand what was trying to be accomplished by the graph above
2, 3, 4, 6, 7 wasn’t sure what was trying to be accomplished, looked like primitives
Likes the roles
What do we mean when we say use cases?

Allan: The graphic is intended to convey the lifecycle of a playbook, where things occur and how they interact with each other. There has to be something to create a playbook. Then there has to be something that exists and validates that the playbooks are correct. The graphic is trying to highlight that there is some process that has to take place.

John: scoping, full specific representation from some of these communities may be missing. We need to differentiate between IR and forensic communities, John will comment in the document

Allan: Please comment directly in the document before the next call.

Bret: if you don’t have comment access, you can request it in the document or via Slack or email to Allan and/or Bret. We are pushing hard to get design logic done - when we get this done, then we can get close to the first Committee Draft for the specification

Jyoti: made comments in the common specification document and recommends using a Data Table with an arbitrary number of properties.
Bret: Need a name or UUID so that you can reference a specific data table.
Allan: To allow multiple data tables
Jyoti: Yes, that’s right, there should be a name
Jyoti: We should introduce the concept of code carrying variables, local, input, output, or global
Bret: Will you do an example of that in the document?
Jyoti agreed to do so.

Allan: The ability of playbooks to share state and variables are important. Call a playbook and get a return value of yes, no, or information. Very much like a programming task, not reinventing the wheel.

AI for TC (all) - review use case document
AI for TC (all) - review common specification document and other documents

Want to get a CSD out in the next month to start writing code and fail fast. If it works great, if not, let’s come back and make changes.

Tentatively planning a plug fest in 3Q.

Thanks to Jason Webb in the variables section
Thanks to Jyoti to your contributions
Thanks to Anup and Jim

Next working call March 3rd