CC in the Cloud (CCitC) Technical Working Group – CCUF Workshop Meeting Minutes – Day 1

9:04 AM EST 2023-10-26

Call to Order: 0907
Meeting Lead: Joshua BRICKMAN

Highlights:

- Matt Downey announced at the CCDB Joint Session that the CC in the Cloud Technical Working Group is now recognized as an official Technical Community (TC).

Old Business:

~

New Business:

- Jade S started by announcing some NIAP developments.
    - Monday October 30th NIAP will be issuing a policy that all evals using app software will need to produce a SBOM.
        - Assurance maintenance will also require a SBOM (according to federal mandate)
    - Microsoft Intune now listed in-eval against the MDM PP and MDM Agent PP-Module as of Wednesday October 25th.
    - Draft EUCC Implementing Act is open for comment, deadline for comments is October 31st.
- Josh B did a brief presentation to officially kickoff the workshop.
    - Our target for publication of the Guidance Doc is EOY (2023).
    - Progress
        - 43 pages & counting
        - Trusted Platform Mapping
        - Assumption Analysis
        - Equivalence rationale
    - Still working on
        - Scheme advice
        - Lab instructions/advice
        - PP update guidance
    - The hard stuff
        - Crypto
            - Will we be able to make assumptions for the crypto?
            - Will CMVP partner with CC on this?
        - Schemes
            - Will they align on what a trusted platform is or isn't?
        - Labs
            - Are they ready to make the investment?

        - Could labs change their models?
    - Challenges
        - CC in the cloud is hard but not impossible
            - US & Canada participating actively; it would be very helpful to have more international involvement especially to map other cloud schemes
        - Resources
            - 72 members but really only about 25 are showing up to meetings
            - We would like iTCs to add to their cPPs
            - More country participation/position statements
        - Industry Led
            - NIAP took an active role in late 2021
            - Industry led TWGs are harder for schemes to buy into
    - Reviewed Workshop agenda for today and tomorrow.
    - Reviewed management team roles
    - Reviewed Code of Conduct and Principles
    - Reviewed Decision-making process for editorial and technical changes
        - Decision process, consensus is the default
        - Voting processes. (eg to form working groups, changes to governing documents, etc.)
    - Reviewed inappropriate topics
        - Don't discuss anything that could be interpreted as collusion or business-related matters such as products, licensing, etc.
    - Reviewed the roles of participants.
    - Reviewed process for main document updates
        - Review open issues in GitHub
            - Brandon H to drive this process
            - GitHub issues to be prioritized over ad hoc /out of band comments
        - Virtual participants
            - Use 'raise hand' feature to comment or ask questions.
        - Reading
            - May stop to read/study certain sections, etc.
- Jade S added some additional comments
    - Justin F's work was done for NIAP which is why NIAP needs to review all work products prior to broader release
    - US Federal government has mandated that FedRAMP is the standard for cloud security authorization, however NIAP has not made this conclusion YET.
- Started walkthrough of open issues, led by Brandon H
    - Reviewed Issue #37 "Minor Feedback/Suggestions"
        - "On-Premises" section confirmed to be in guidance document and all items have been resolved/addressed.
        - This issue now closed
    - Reviewed Issue #47 "Steps for adding "CC in the cloud" to a PP"
        - Issue closed, will implement derivation guidance (Justin F's doc)
    - Reviewed Issue #50 "Labeling in Example Topology Diagrams"

- Renamed the diagrams to 'SaaS Composition Examples' instead of 'Topology'.
- Issue to remain open pending work to be done by Brandon H

- Reviewed Issue #51 "Title Page, Footnotes, Headers, Footers, References"
  - Discussion on revamping the title page with a new logo/graphic
  - Discussion on adding a 'contributors' page to acknowledge participants of this group.
  - "Contributors" placeholder section added to Guidance document.
  - Issue to remain open pending final list of participants/contributors, schemes, etc.
- Reviewed Issue #63 "CMVP certifications for CSPs"
  - This topic will be rolled into PP specific contexts,
  - This issue now closed.
- Reviewed Issue #66 "Guidance doc section 3.1 – Useful Terms"
  - Discussion on defining data sovereignty or addressing it in the guidance doc. Cory C talked about schemes like Canada being concerned about Canadian laws applying to Canadian data.
  - Brandon H advised that the data center must be identified, therefore the geographical area is known.
  - Valid definition of Data Sovereignty definition to be created and tagged as scheme advice and could be captured as an assumption.
  - Justin F advised that in the derivation document, a flag for follow up was that some SFRs may need to be added to PP's to address cloud related threats.
  - Date sovereignty claims merged with Issue #106 'Guidance for Schemes'.
  - This issue now closed
- Reviewed Issue #70 "Reuse of FedRAMP evidence for CC"
  - Discussion around standards for the collection of evidence in methodologies like FedRAMP and whether those standards could be applicable to CC
  - Justin F commented that the CC evaluation standards and evidence collection is more stringent than that of FedRAMP, so reuse of FedRAMP evidence is unlikely, however the other way around may be possible depending on what FedRAMP thinks. Evaluation activities in CC are more detailed than that of FedRAMP.

Break @ 10:35

Reconvene @ 10:52

- Continued review of Issue #70 "Reuse of FedRAMP evidence for CC"
  - Overall, reuse of FedRAMP evidence is implemented in the general Derivation Guidance document.
  - This issue now closed.
- Reviewed Issue #71 "Consistency of Comma Usage"
  - A thorough review was conducted on the use of commas where several incorrect occurrences were identified and rectified.
  - Correct usage has thus been enforced diligently and will be applied consistently to avoid similar gross errors in the future

        - This issue now closed.
    - Reviewed Issue #72 "Audience Clarification – Main Guidance and Guidelines for Optimizing existing Protection Profiles"
        - Main guidance document has included all audience types and end users without need to spin off other targeted docs.
        - This issue now Closed.
    - Reviewed Issue #73 "Scope of cloud operating environment claims"
        - Existing section (Cloud Equivalence Considerations) addresses this issue.
        - This issue now closed
    - Reviewed Issue #74 "Lab/Evaluator Instructions"
        - Discussion around integrating into "Guidance for Establishing Test Environments on Cloud Infrastructure" section.
        - Issue to remain open, pending discussion in lab instructions break-out session.
    - Reviewed Issue #96 "AGD for Cloud"
        - Discussion on integrating this into the Lab Instructions section.
        - Issue tagged as "Lab Instructions"
        - Issue to remain open, pending discussion in Lab Instructions breakout session
    - Reviewed Issue #100 "Guidance Doc Status and Ownership if Applicable"
        - Issue to remain open for tracking purposes.
    - Reviewed Issue #106 "Guidance for Schemes"
        - This issue to include the tracking of suggestions for implementing guidance on Data Sovereignty
        - Issue to remain open, for further discussion in breakout session
    - Reviewed Issue #108 "Log your issues questions and clarifications for the MDM mapping spreadsheet here"
        - Sufficient time has elapsed for comments to be entered.
        - This issue now closed.
    - Reviewed Issue #110 "guidance doc organization note - PP cloud adaptation process needs material on what may be added by cloud evals"
        - Issue to remain open
    - Reviewed Issue #111 "CSO is noted as CSP"
        - Issue to remain open as it is editorial
    - Reviewed Issue #112 "CCiTC Guidance for Cloud Evals Minor feedback/suggestions"
        - Discussion on the representation of TOE Identifiers and the level of granularity In which it should be documented. Depending on varying levels of hardware dependencies and scheme policies, the level of reporting required for things such as CPU models/microarchitectures may vary, and also may vary depending on the portability of the TOE as a result. This information should be defined at the PP level.
        - Discussion on the inclusion of an example for how SFRs must be modified in the SFR challenges section to distinguish between SFR challenges and SFR testing challenges.
        - Issue to remain open pending inclusion of Sample configurations/ TOE ID's to be added to the guidance document.

CC in the Cloud (CCitC) Technical Working Group – CCUF Workshop Meeting Minutes – Day 1

- Josh B led a section-by-section walkthrough of the Guidance document and provided an opportunity for issues to be raised by Members.
    - Issue #113 “Include ISO in Preface” created
        - Discussion on adding additional language to the Preface section that includes a roadmap for ISO inclusion.
        - Pending further discussion in tomorrow’s session.
- Discussion on Products vs Services and the delineation between the two

Break for Lunch @ 12:32pm

Reconvene @ 1:15pm

- Continued with section by section walk through of Guidance document
    - “Cloud Topology” Section
        - Discussion on the term “Lift and Shift” and what it means in the CCitC context
        - IaaS is the most translatable example of the concept of “moving to the cloud”, it’s the exact same product but being deployed in the cloud, (easiest migration method)
    - “Shared Security Model” Section
        - Discussion on developing clearer descriptions of Cloud Service Provider (CDP) vs Cloud Service Offerings (CSO)
        - This section is not to be construed as “Guidance” for PP authors to incorporate into PP’s it is more of a background description of the concept of SSM for the purposes of understanding this concept
        - Issue #115 “Shared Security Model” created for editorial tracking
            - Update all references of “TOE Vendor” to “TOE Developer”
            - Update all references of “TSS” to “ST” where appropriate.
        - Discussion on paragraph 4 of the Shared Security Model section to further discuss the responsibilities of the customer.

Break @ 2:24pm

Reconvene @ 2:40pm

- Continued with section-by-section walkthrough of Guidance doc
    - "Relationships Between the Trusted Platform / TOE Platform, and TOE" Section
        - Discussion around the potential convergence of the TOE platform and Trusted platform
        - Issue #116 “Trusted Platform and TOE Platform” created
            - Currently, the Guidance doc does not allow for any overlap between the Trusted Platform and the TOE Platform. Further discussion needed on whether or not this is a necessary distinction.

CC in the Cloud (CCitC) Technical Working Group – CCUF Workshop Meeting Minutes – Day 1

Adjourned @ 3:00pm to walk over to Marriott Metro Centre for CCUF/CCDB Joint Session

Questions/Follow-ups:

- **Minutes to be posted to GitHub**
    - Confirm if additional folder requiring log in to access is needed.

End of Meeting – Adjourned 3:00pm EST