SACM Architecture

Bill Munyan & Adam Montville

IETF 111 - Online

Updates to the draft, part 0

- March 2021 (-08)
- April 2021 (-09)
- May 2021 (-10)
- June 2021 (-11 and -12)
- July 2021 (lucky number 13)

- 2 new issues were opened
- 7 issues were closed

Updates to the draft, part 1

- March 2021 (-08)
  - Kept the draft alive and unexpired

Updates to the draft, part 2

- April 2021 (-09)
  - Enhanced “Architectural Overview” section
    - Producers/Consumers
    - Defined interactions, topics, payloads, capabilities
  - Added Manager component
  - Revised all diagrams to include Manager

Updates to the draft, part 3

- May 2021 (-10)
  - Further enhanced role of the Manager and its interactions
  - Defined generic status notification operation
  - Component Onboarding -> Component Registration
  - Payloads and Payload Categorization
    - Topic centric
    - Payload centric
  - “Health” operations over the Administrative interface
    - Health check: Manager queries components for liveness
    - Heartbeat: Component publishes liveness to Manager

Updates to the draft, part 4

- June 2021 (-11 and -12)
  - Added Terminology section, updated a couple of times
  - Russ Warren from OCA reviewed, provided comments
    - Clarified repository interface role
    - A couple of terminology items
  - Initial ideas for capability URNs in IANA section
    - Shot in the dark, really

Updates to the draft, part 5

- July 2021 (lucky number 13)
  - Added operational section for Ad-Hoc Collection
    - SACM Producer (e.g. Manager) to Orchestrator
    - Orchestrator to Posture Collection Service
    - Posture Collection Service to Repository Interface(s)
    - Status Notifications

Keeping up the PACE

- PACE == Posture Attribute Collection & Evaluation
- CIS in cahoots with OCA, DoD (Mike Rosa shout-out!)
- Working towards a prototype implementation
  - OpenDXL
  - OpenC2

Proposed Direction

- PACE Prototype development
  - https://github.com/opencybersecurityalliance/PACE
  - There's not much there yet, but we're moving.
- Continue evangelizing SACM architecture within OCA

- Draft work continuing
  - Other "flavors" of collection (periodic, event-based, observational)
  - All evaluation "flavors" (ad-hoc, periodic, etc)
  - Info and Data Models
  - IANA and Security Considerations (volunteers?)