2018-04-06 SAFE Meeting Notes

Working Group Proposal: Safe Access for Everyone (SAFE)

Attendance (PLEASE ADD YOURSELF):

- Dan Shaw, security expert, Node.js
- Mark Underwood Synchrony
- Rachel Myers, Security Rules and Events, Google
- Geri Jennings, CyberArk
- Prabath Siriwardena, WSO2
- Cheney Hester, Fifth Third Bank
- Sree Tummidi, Pivotal
- Sarah Allen, Security Rules and Events, Google

Agenda:

- Attendance/Check-in
- SAFE Personas WhitePaper continued
- Getting ready for CNCF TOC meeting 4/17, 8am Pacific
    - Apr 17, 2018: Telepresence + SAFE Working Group Proposal
    - Suggest to settle down the preference on general policy or security for CNCF SAFE to avoid any confusion or overlap (Howard)
    - CNCF WG process PR - https://github.com/cncf/toc/pull/106
- https://github.com/cn-security/safe

Notes (Please anyone feel free to join in shared note-taking):

- Scribes:
    - Geri Jennings
    - Cheney Hester
- Links:
- SAFE working group will be making a community presentation at the next CNCF TOC call on 4/17 at 8 AM PT (connection info here)
- Rachel: Is the Cross-cloud CI WG able to integrate additional clouds without the involvement of the cloud providers?
    - Dan: the CI working group has a lot of Linux Foundation / paid CNCF contractors involved, as opposed to this group which is more community driven - it gives them additional support for their time / involvement.

    - Expectation is cloud would allocate instances. Infra from node.js is primarily donated from each cloud providers giving instance/platform credits. Google is already well represented.
- To prepare for the 4/17 meeting, we will have a WG session on Monday and need volunteers for:
    - Preparing a pitch deck for SAFE (~10 slides, experienced members preferred):
        - Should be based on the draft working group proposal (which first needs to be finalized)
        - Rachel Myers
        - Cheney Hester
        - [insert names here]
- Geri: How was the name of SAFE decided on?
    - SAFE is a bit of a broader concept to encompass the policy as it exists with access control, etc
    - If you think it's a little too clever I agree, maybe needs rework to not need to explain
    - 'Security' or 'Security Policy' as name?
    - 'Security' is specifically a really big land to grab, addressing all of security is a bit too broad
    - Challenge with 'Security Policy' is that it's too narrow of a definition
    - Cloud Native Security is the idea used in the github
    - We may be better served if we go forward with a funky acronym and pivot to 'Security' once we have more buy in
    - Rachel Myers: Security is too broad we're not dealing with all aspects of security
    - Geri: There are a lot of things we could talk about outside of policy
    - Meeting on 17th we will go forward as 'SAFE' but are open to changing. 1-2 words.
- Mark Underwood: I'm here for the SAFE acronym :)
  Working on the big data security group, we eventually got to a safety framework. If others can live with this idiosyncratic name, there are similar naming conventions happening in other venues.
    - Dan: suggest creating a new issue in the cn-security/safe repo
- Kam & Geri why did you choose to come to this group?
    - Geri:
        - Works for CyberArk on the Conjur team
        - Managing security policies as code
        - Working on secrets management
        - Wanted to become more involved with cncf in general
        - Wanted a security working group to help contribute
    - Dan: SAFE vs Security will this affect your ability to influence your team?
    - Geri: Requires explanation
    - Kam
        - Works for iRhythm

        - Working on PADME, as an architect
        - Problems rolling out systems in past projects were due to lack of commonality
- Unnecessary system issues in the cloud because of permissions, IAM, etc.
- We need to figure out a way to make this work through standardization

- Does anyone here want to volunteer to join the document-building and presentation prep working group? Spend time reviewing, editing
    - Volunteers (**add notes about what you would want to help with**):
        - Rachel
        - Kam
        - Cheney
        - Geri - reading through the existing draft doc and adding comments
- Rachel: Should we edit in doc form at current or wait to edit in presentation form?
- Dan: Most content will come from the doc, and the other half will be laying out the governance plan on what we expect to do and who we'll be engaging with
- Rachel: Let's outline the governance plan in a doc as well to make it easier to track
- Dan: I'll pull from this doc info on anyone who wants to participate
- Mark: Good to have a deck that's simple for everyone to do an elevator pitch/socialize.
- We don't really have an elevator pitch right now for non-technical or people who aren't in the security space
- The initial deck could be considered as a seed deck that could be used for other purposes such as briefing out the group mission and needs to third parties for cross-fertilization (e.g, IEEE Product Safety Engr, IEEE P2675)
- Sarah, how did the working sessions go this week?
    - We edited the proposal
    - We got feedback that the prop+osal was very clear from Sara Navatny (sp?)
    - We crafted a vision statement based on her feedback
    - The sentence "They use cloud technologies with clear understanding of risks and the ability to validate that their security policy decisions are reflected in deployed software" seems to resonate the most with people as doable
    - This isn't just for the working group, it's to improve the language in the industry and make it easier for various orgs to have a baseline for solving the same kinds of problems
    - We should set timelines on our goals to ensure we continue making progress
    - The chief security officer at fast.ly said it's hard to hire a chief security architect, and the people in those roles are being asked to do things without the knowledge they need - our group can really contribute to setting a standard for this
    - We may have conflict within the group about how to address specific industry problems (eg RBAC vs ABAC), but this group provides an opportunity to have these discussions in the open and find common ground
    - Need to determine how SPIFFE, OPA fit into this working group

    - The audience is both dev and ops - communication between dev/sec/ops is not going well right now in the industry
    - We need a set of constraints that give freedom to allow devs to create business value but work parallel with ops and in the lines of security
- Mark: infra people don't have the same tools to ensure quality automatically, the way that developers do. Do we need to mature the requirements for IDEs on the ops side?
- Sarah: Maybe they just need better tooling - so however it's configured, you can automatically determine if it's configured as it's supposed to
- Kam: The documents feel like they're written by technical people for a technical audience
- Sarah: The attempt is to get it progressively more technical throughout the document with the vision at the top and flowing down into more technical 'in the weeds' talk
  In order to foster an ecosystem we need buy in from the technical people to provide feedback into our solutions.
  They understand the problem but might not be able to create a solution for the problem.
  It would be good if the charter was more accessible to non-technical people
- **Do we think the charter is good enough?**
    - Sree: Can we get time to review it then discuss next week?
    - Sarah: Give everyone a chance to review the charter
    - Dan: Is the charter in line with our expectations
        - If we can weave in more of that vision and high level terminology into the charter rather than getting too dense we'd be well served
- Sarah: Can we all think about different readers and provide feedback based on that, especially those of us coming from scientific communities or outlying communities. Really try to do suggestive edits and pull other colleagues into this. People who come from a different background vs our group.
    - **Ask "what do you think we're doing based on this?"**
- Sarah: What's the duration of each of these phases? Need to decide by next week
- JJ: There are some loose ends. The objective is to get value out of our combined brain power. What are the actionable things you want to see out of this? Can you map it to one of these phases to get it accomplished? If not, please raise that. If you can't find a tangible thing for you to get out of this working group, let's talk through how to incorporate it.
- Sarah: It would be good to have a list of working group members where each of us have stated why we're here
    - Add something to the GitHub repo (short, 1 page or less, responding to a set of key questions to answer the reason why we're here)?
- Dan: We talked about that a bit at the beginning of the meeting, but it's a great idea and a good opportunity to be clear about why we're all here
- Sarah: Does anyone have a suggested format?
- Rachel: How about the industry you are coming from, expertise that you have that would be valuable
- Sarah: A working-group specific bio. Can someone draft a set of prompts for this?

- Sree: I can do that.