2018-05-25 SAFE Meeting Notes

Working Group Proposal: Safe Access for Everyone (SAFE)

Join: https://zoom.us/j/629934721

Attendance (PLEASE ADD YOURSELF):

- Dan Shaw, security expert, Node.js
- Sarah Allen, Google, Serverless Events & Policy
- Mark Underwood Synchrony (rep self)
- Jason Melo, nearForm
- Rachel Myers, Google, Firebase & Serverless Events & Policy
- Christian Kemper, Google Cloud Security
- Doug Davis, IBM
- Rae Wang, Google

Agenda:

- Attendance/Check-in
- (As needed) Check-in from partner SIGs and WGs
    - Kubernetes SIG-Auth
    - Kubernetes Policy WG
    - NIST Big Data WG
- PR yourself as a member on https://github.com/cn-security/safe
- SAFE WG Scheduling Use Cases

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

- Scribes:
    - Sarah
    - Mark U
- Links:
    -

Marc Underwood - ethical trace-ability, GDPR, agile particularly challenging with scrum process
Dan Shaw - how does this relate to safety and the work of this group? Operator ethics?
Marc: use cases in diff domains

- Cross-domain: managing firewalls, on-boarding, training, ISO-9000 for quality
- Domain requirements: as we move to cloud, needs to be articulated
- 1454-99 IEEE IoT Harmonization
    - Use case: smart device, TP-link smart-switch, need to rely on two cloud platforms
    - Cloud-to-cloud connection, then back into on-prem at home

        - How do you make that a secure thing?
            - How do you deal with children?
        - Do they deal with authentication and risk management?
            - Lights probably innocuous, but garage door has other implications
            - Who owns cloud-cloud connectivity?
            - Hands-free when it usually does work, but when it doesn't — SLA for that? The better it works the higher the expectation
- For some domains, like social media, maybe ok if not all the messages get thru,

Question about Agile?

- Sarah: Doesn't really have to do with agile?
- Mark: If you defer what the feature set is supposed to be and fail fast in small chunks
- Sarah: that's doesn't really sound like agile
- Mark: could happen with any process
- Mark: Ethics folks think that it's all design up-front, like to require engagement throughout the process
- Sarah: hard to make compliance a story with points
- Christian: is it that we don't understand the requirements, hard to plan

With well-understood design patterns, it is easier to make security work, but green-field scenario. We have designated communities-of-interest that do more innovative stuff and work in isolated networks and can discover new design patterns and operate with a bit more risk
If they are using very standard eng practices, then they can use standard patterns, but with the new stuff, that is sometimes not available.

Domain-specific is more worrisome, like with child-access

JJ Are there specific issues associated with scalability? He says yup. Ecosystem-specific considerations are rife.

Sarah - What is specific to cloud native - But what is the design pattern? Reasoning is harder, must be reasoned bottom-up.

Micro-services? How do you bring in security, authentication, PCI compliance - That is what is attractive about this.

"Knobs and dials" - does this appeal to a subset? Goal here per Sarah to identify the patterns to aid with SAFE practices.

Interactions between roles in different sized firms have different ways to managing interactions w/ security.

There are things that are being designed for a certain magnitude of scale, then things are re-thought,

In cloud-native ecosystem, coming from an environment like Google, Twitter, Netflix — very specific environments that handle things, and safety nets

Rae: KubeCon/K8s audience isn't the same folks who use the public cloud. 20-30% are very sophisticated, 70% just want to know what to do, don't have in-house expertise, want to transform their culture, want to move away from an IT ticketing system, guardrails, trust but verify

Mark: Product owners ask for features that their engineers might not

Rae: The personas interact in specific ways
Sarah: and those personals may be interact in different ways in different companies

Rae: Compliance auditors struggle with public cloud — maybe we could get to a place where if you deploy on public cloud: 80% is already checked off for you

Mark (for notes) We (P2675) is working with the Office of the Currency on DevOps -- they are the regulators de jour for finance -- and the focus there is not cloud per se but the SDLC in the context of a software-defined data center.

Sarah: from KubeCon says we need an elevator pitch for CNCF SAFE.

Admin Things

JJ: Recap of Kubecon - small attendance, yet quite active. People reached out later.

- Security is not a feature — it is a system wide property
- We are not seeking to replace the SIGs, mostly about cross-pollinating and cross-training

KubeCon Shanghai — Dan will be attending, Rae W might

CFPs for KubeCon NA and KubeCon Shanghia are open

- Proposals? Maybe discuss as part of next meeting, do a PR or issue on Github

Gartner - IAM Conference

If we come up with a checklist or framework, maybe an adaptation of NIST, maybe something in the IDE, SDLC

We lack a great "elevator pitch" — everyone should think about how to articulate the problem we are solving. What is currently in the proposal isn't clear to newcomers:

cloud-aware access controls and safety concerns needed for interoperable cloud-native systems that serve operators, administrators, developers, and end-users.

Publications? Could think about publishing use cases / personas as an interim thing to publish that could be useful.

Consider relationship with Oasis OMG

- JJ has talked to …. Who is on the board for Oasis

Next week: <no meeting>

June 8: Geri will share about what they are building at Cyberark for K8s
Jason (June 15 or June 1) — will get back to us