Security WG Meeting, 3/27/19

Attendees: Janko, Michael Hall, Bryon, Greg, Ian Johnson, Jim Wang, Lenny Goodell, Toby, Tony, Rakesh, Trevor, Vlado, Tingyu. Others may have joined after the meeting started and attendance was captured.

Agenda

Old Business

- Securing service secrets doc
    - Discussion
        - Pass phrase is still not secure, so is it any better than an unsecure token file?
        - Phrase passed in at entry point – at user's discretion is could be kept more securely or not kept at all (presenting problems for restarting services)
        - Need some more research on what access levels would be need (categories, at rest, in motion)
            - Inventory of current secret protection needs & potential authorization concerns
            - What's the scope for this release?
    - Jim and Tingyu to take all the incoming feedback (more sought and gratefully accepted) by email/Slack and incorporate into the next version of the document.
- Addressing incoming security doc
    - Discussion
        - Need for private reporting
            - Email is public, but the report is kept private until triage and ready for publishing
        - Need a triage before publishing
        - All this depends on severity (case by case)
        - Are there other systems/orgs/tools that provide CVE handling (like Github)
            - A private repo of issues of sorts
            - Send any possible options to Jim &/or Tingyu
        - Look into Github CVE tooling for code scan
            - From Ian: https://help.github.com/en/articles/about-security-alerts-for-vulnerable-dependencies. It doesn't look like the github scanning works for go projects, only Python, Java, JS, .NET, and Ruby
    - Jim and Tingyu to take all the incoming feedback (more sought and gratefully accepted) by email/Slack and incorporate into the next version of the document. Additionally, if there are known tools that help provide for some of the suggested infrastructure we might need for this, please send the input our way.

New Business

- Intel roadmap/proposals – Bryon and Jim (Wang) to present Intel high level roadmap next week.
- Issue #185 – addressing Kong on ARM (unofficial support we need to take a look at). Tingyu and Jim to work the issue with Andy and team and get back to the group next week.