NTIA Multistakeholder Process on Software Component Transparency
September 5, 2019
Stakeholder Discussion of Potential Next Steps

NOTE: These notes are an edited version of the notes that were recorded live in front of participants during the September 5 meeting. NTIA edited them slightly for comprehensibility and topical organization, but they remain a rough documentation of the ideas raised during the conversation.

Extending and Refining the Model

- How to share SBOM data – what does transparency look like?
- High Assurance SBOMs
    - Integrity is discussed in the existing document w hashes, signing
    - What other elements to focus on
    - Start with risk-based approach
- Using SBOMs for cloud / SaaS / Containers
- Communicating non-exploitability of vulnerable components downstream
    - "exploitability" too specific – context, disposition, exposure could be terms.
- Further work on the naming challenge
    - Alias databases – who might maintain that database?
        - Unlikely to be a vendor
        - FIRST not necessarily the best fit
    - Focus on linking to other databases that we care about: vulns, licenses, etc
    - Focus on federation: encourage projects to own their own "domain" with unique names inside
    - Promulgate best practices – but whose?
- Version vs. patch clarification
- How to document that subcomponents have been removed in the compile/build process
- Potential starting point: reshuffle things in the Framing group, but could be a good home to avoid a brand new group
    - Framing WG can begin discussion, catalog potential next steps, prioritize, identify path forward (a new charter)
    - Clarification on expertise: each issue will need their own approach to expertise (e.g., in high assurance, a real understanding of real-time threat). Require many different perspectives.
    - No firm commitment, but general thought group should continue.
    -

Tooling, processes, and services

- What tools exist today for the *generation* and *consumption* of SBOM data?
- What further tools are needed?
- What operational lessons have been learned by organizations who have already tackled this?

- Maybe GitHub to host tools
    - However: could be a real barrier for non-tech folks to participate
    - Pick the best tool for the job
- A quickstart guide with pointers to tools, real code examples, etc
- Potential starting point: reshuffle things in the Formats group, but could be a good home to avoid a brand new group
    - Each format can have its own subgroup for more targeted focus
    - Want to identify optimal points to put efforts
-

Awareness and Adoption

- High level strategy for broader ecosystem outreach
- Sector-specific and technology-specific outreach and potential venues and champions
    - Want to have a clear strategy for outreach
    - Determine the best use of available resources
- Model contract language
- FAQs
- Joint messaging
    - A shared deck for to allow common messaging for presentations
        - Would need some community approval
    - Collecting presentations and other documents that stakeholders have used
- Translate documents into other languages
- Use multimedia formats to help convey the message – videos, etc
- A potential maturity model for transparency
- Each group itself could use more outreach on its own tasks – e.g. tooling
- Outreach as a separate focus
    -

Demonstrations

- A follow-on to the Healthcare Proof of Concept
- Other sector-focused proofs-of-concept
    - Are there other models beyond the Healthcare POC approach?
- Documenting existing successes in generating and using SBOM data
- Specific attention to the end-of-life or end-of-support issue

Potential outreach targets

- Developer conferences
    - Language
    - Tool
- Legal community
    - Export control
    - Licensing

    - Legal hackers
- Supply chain community
    - Need more information on this front – e.g., on import/export boundaries.
    - Groups w/in Commerce – supply chain assurance industry day.
    - Other government efforts point to SBOM work?
- Security community
- Safety / critical infrastructure
- Auto sector
    - AF speaking at Auto ISAC summit in October.
    - ITU consortium on automotive industry.
- Industrial IoT
- Auditors
- Insurance – way to assess relative risk.
- Healthcare/medical device
    - Already have visibility on ISACs, but other parts, too. ISACs can give more information on strategic watering holes.