NTIA SBOM Framing WG

2020-04-15

Michelle Jump
Art Manion

Administration

- Weekly meetings remain Friday 14:00 EDT
- Sending Monday reminders
- Ask participants to dedicate 30 minutes during the week
- Liaisons
  - Brief updates from other WGs at each meeting
  - Collaboration with Health Care PoC
  - HSCC vulnerability communication effort

The ~~Naming~~ Identification Problem

Name is part of identity

- Framing and Health Care PoC collaboration
  - Test the Framing model, formats, tooling
  - How much identification
- Supplier identification, possible supplier registry, need, feasibility
- Framing supplier use cases
- Ad-hoc discussion on identification, exploring other large-scale solutions
- Questions:
  - To what extent does solving identification block SBOM progress?
  - How fast/far can SBOM scale without significant solution to identification?

Identification Use Cases

- To help explore identification: Use cases
  - Supplier creates SBOM for supplier's component
  - Someone creates SBOM for someone else's component
  - Supplier determines and populates baseline elements
  - Supplier distributes SBOM
  - Consumer consumes SBOM
- See "NTIA Framing - Naming-Focused Use Cases" document
  - Thanks Ed H.

SBOM Exchange

- SBOM exchange and sharing is still important
  - Tightly connected with identification
  - Part of PoC-Framing collaboration
- MUDMaker
  - MUD Manufacturer Usage Description, RFC 8520 https://www.rfc-editor.org/info/rfc8520
  - "…provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function."
  - https://www.mudmaker.org/
  - Thanks Eliot L.
- Other (existing) options, maybe STIX?

Asks and Next Steps

- Help discuss and try to answer
  - To what extent does solving identification block SBOM progress?
    - What does partial progress look like?
    - What aspects of identification are blockers?
    - Do we need a supplier registry, and is it feasible?
    - How fast/far can SBOM scale without a significant/global solution to identification?
- Next steps
  - Continue multiple threads on identification and exchange
  - Transient vulnerability/exploitability (VEX) is important but on hold
    - Consider a generic SBOM annotation feature
  - Health Care PoC collaboration