CISA PUBLIC LISTENING SESSIONS ON ADVANCING SBOM TECHNOLOGY, PROCESSES, AND PRACTICES

SHARING AND EXCHANGING SESSIONS SUMMARY

Recognizing the importance of SBOMs in transparency and security, and that SBOM evolution and refinement should come from the community to maximize efficacy, CISA hosted a series of "listening sessions" as a collaborative brainstorming exercise to elicit insights on specific aspects of SBOM.[1] One key area of focus was "sharing and exchanging SBOMs." Moving SBOMs and related metadata across the software supply chain will require understanding of how to enable discovery and access, and ensuring solutions are interoperable.

CISA hosted two 90-minute virtual sessions on sharing and exchanging SBOMs with several hundred experts from around the world to share insights and perspectives. Participants expressed strong support for CISA to continue to facilitate conversations and concrete, community-led efforts on this topic. Below is a short summary of the insights and potential activities that were suggested and emphasized over the course of the public conversation. These will be used to set up further conversations and collaboration.

Possible sub-topics

The following popular sub-topics for sharing and exchanging SBOMs were identified by participants: sharing multiple SBOMs together, sharing concerns with multiple technology domains, diverse supply chain considerations, identification for tracking purposes, SBOM trust (e.g., signing, validation, verification), issues with software/SBOM decoupling, SBOM visibility and access control policy considerations, sharing portal scalability, open interfaces/APIs, secure sharing, pain point tracking for current sharing methods, contract considerations (e.g., limited release), software differences may necessitate multiple retrieval methods, mapping different delivery mechanisms, and tool sharing transparency.

Existing solutions & related efforts

The following existing solutions and related efforts were identified by participants: Digital Bill of Materials (DBOM), STIX/TAXII, PURLs, OASIS Posture Attribute Collection and Evaluation (PACE), and the Internet Engineering Task Force Supply chain Integrity Transparency and Trust (IETF SCITT).

Desirable features

[1] https://www.federalregister.gov/documents/2022/06/01/2022-11733/public-listening-sessions-on-advancing-sbom-technology-processes-and-practices

Participants in the listening sessions identified the following desirable features for an SBOM distribution system including: third-party SBOM generation, discoverability, access control (building on DRM), integrity and validation features (e.g., signatures and assurances), legacy software accommodations, SBOM revocation/deprecation, mapping to other software delivery mechanisms, connection to coordinated vulnerability disclosure, packaging SBOMs alongside containers or blob, compatibility with other trust-related data, and methods to simultaneously update software and associated SBOMs. Participants also mentioned the importance of linking this data to other software metadata, as well as hardware metadata.

Use Cases

Popular responses by participants in the listening sessions for potential use cases are automation, leveraging existing tools, software distribution mechanisms (e.g., app store), vulnerability management/incident response, and considering SBOM revocation through versioning and/or deprecation.

Scoping

The listening sessions identified the following scoping considerations: building sharing solutions on other network engineering approaches, SBOM location (i.e., ship SBOM versus keeping it online), and understanding the unique features of OT and other embedded systems.

Other relevant issues

Additional relevant issues to sharing and exchanging SBOMs identified by the listening session participants are SBOM software identity, SBOM signing, SBOM completeness, backporting and rebasing, and SBOM process and lifecycle maturity.

Potential activities

Participants in the listening sessions identified the following potential outcomes for future community-led work on sharing and exchanging SBOMs: a sharing and exchanging pilot program, an SBOM sharing and exchanging playbook, and the creation of an SBOM OSS public repository.