SBOM at a Glance

Purpose

This document is an introduction to the practice of Software Bill of Materials (SBOM), supporting literature, and the pivotal role SBOMs play in providing much-needed transparency: enabling stakeholders to answer questions like “Am I affected?” and “Where am I affected?” when faced with a supply chain concern.

What is an SBOM?

An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be. SBOMs may include open source or proprietary software and can be widely available or access-restricted.[1]

SBOMs should also include baseline attributes with the ability to uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of a modern development process. For older software, less-automated methods exist.

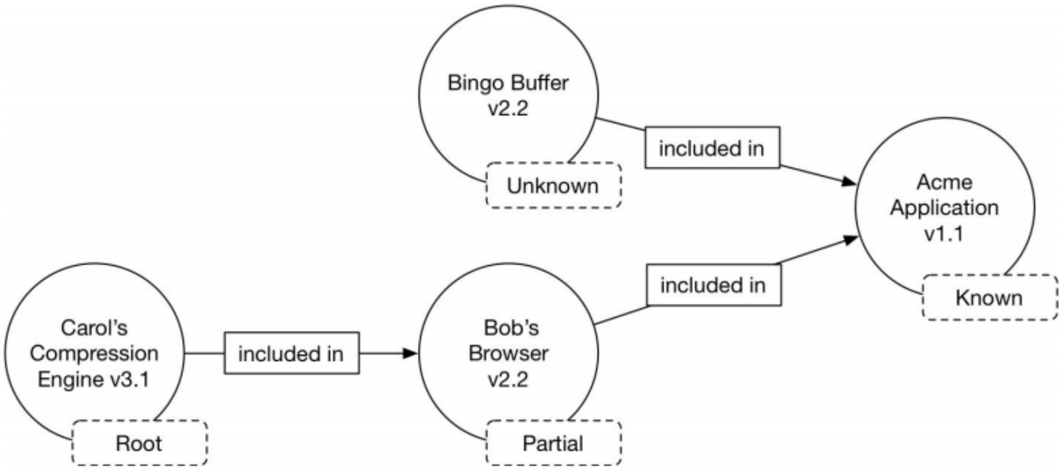

Figure: Conceptual SBOM tree with upstream relationship assertions

Benefits and Use Cases

The benefits and use cases for SBOMs[2] are numerous; vary across stakeholders who produce, choose, and operate software; and are amplified when combined. Benefits include reducing cost, security risk, license risk, and compliance risk. Use cases include improved software development, supply chain management, vulnerability management, asset management, procurement, and high assurance processes. An ongoing SBOM Healthcare Proof of Concept[3] has exercised many of these use cases and demonstrated the value of producing, sharing, and consuming SBOMs, prompting similar proofs of concept in the Automotive and Energy industries.

Baseline Component Information

The primary purpose of an SBOM is to uniquely and unambiguously identify components and their relationships to one another. In order to do so, some combination of baseline component information is required. Certain attributes provide greater uniqueness or unambiguity, as does having a greater number of the baseline attributes in an SBOM entry.

These baseline components support many use cases, but not all. Additional attributes may be required to support advanced use cases.

Baseline Component Information
Author Name
Supplier Name
Component Name
Version String
Component Hash
Unique Identifier
Relationship

Machine-Readable Formats and Tools

To fully realize the benefits of SBOMs and software component transparency, machine processing and automation are necessary. This requires widespread interoperability across the supply chain which, in turn, requires standardized data formats and identification schemes.

The following three formats[4] focus on the core problem of identifying software entities and conveying associated metadata – and have the requisite fields to cover the needs for the baseline SBOM. Tools are available to produce, consume, and transform these SBOMs.[5]

Format	Specification	Known Tools
SPDX	https://spdx.github.io/spdx-spec/	https://tiny.cc/SPDX
CycloneDX	https://cyclonedx.org	https://tiny.cc/CycloneDX
SWID	ISO/IEC 19770-2:2015	https://tiny.cc/SWID

Sharing and Exchanging

Sharing SBOM data across the supply chain will involve a combination of technical platforms, predictable data formats, and operational processes.[6] Due to the diverse needs of the software ecosystem, there is no one-size-fits-all solution; however, modeling SBOM processes on existing approaches and methods will enable interoperability between vendors, dampen variance, minimize the need for new tools, and thereby simplify processes required for better supply chain management.

Learn More

For more resources about SBOM, see www.ntia.gov/sbom. For additional introductory information on SBOM, see the two-page Overview,[7] FAQ,[8] and Explainer Videos.[9] For a concrete example of an SBOM in all supported formats – or to create, transform, or visualize one – see SwiftBOM.[10] For ongoing multistakeholder engagement information, see www.ntia.gov/SoftwareTransparency.

References

[1] Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)
https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

[2] Roles and Benefits for SBOM Across the Supply Chain
https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

[3] Software Component Transparency: Healthcare Proof of Concept Report
https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf

[4] Survey of Existing SBOM Formats and Standards
https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf

[5] SBOM Tool Classification Taxonomy
https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf

[6] Sharing and Exchanging SBOMs
https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf

[7] Two-Page SBOM Overview
https://www.ntia.gov/files/ntia/publications/sbom_overview_20200818.pdf

[8] SBOM FAQ
https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

[9] Explainer Videos
https://www.youtube.com/playlist?list=PLO2lqCK7WyTDpVmcHsy6R2HWftFkUp6zG

[10] SwiftBOM – SBOM Generator Tool
https://democert.org/sbom/