Terms

2019-04-11

The Framing WG proposes the following terminology. Progress will be difficult without shared agreement on terms and their meanings. The scope of this terminology is at least initially limited to this NTIA multistakeholder process. These terms have not yet been thoroughly discussed in the Framing WG, consider them a rougher draft than the Problem Statement.

Supplier

Entity (individual or organization?) that identifies (builds, assembles, creates, provides, defines?) components and creates associated SBOMs

A supplier may also be known as a manufacturer, vendor, developer, maintainer, or provider.

(Look up “supplier” from ISO 2700x?)

Suppliers are responsible for creating SBOMs for components that the suppliers produce first hand. Suppliers are also responsible for collecting SBOMs for components they use and providing both types of SBOMs to their customers/users.

We decided on “supplier” instead of “vendor” or “owner.”

Component

Unit of software defined by a supplier at the time the component is built, packaged, or distributed for distribution to others.

Unit of software defined by a supplier, somewhat generic, level of granularity not specified, at the time that the SBOM dependencies are reasonably well known.

For now, what is packaged/distributed, noting that this isn’t quite good enough for e.g. containers and node.

Boundary of delivering component from one supplier to another, in MDM world unit under test, what the customer would see.

Packaging includes build time, but packaging is preferred because the supplier has better knowledge of the inventory and build activity at that point in time. Packaging is more aware of other components included and how the component will be installed, and packaging can be aware of build instructions.

A product is a component. So is a library. So is a single file. So is a collection of other components, like an operating system, office suite, database system, car, an ECU in a car, or medical imaging device. An installation package like a .rpm.

From the Practices WG: Parts, compound parts, and final goods assembled are generically all components. The relationships between them matter.

SPDX terms package, file, and snippet map to “component.”

SWID term?

SBOM

Software Bill of Materials

A SBOM is the list of components (inventory) and associated metadata that make up a component.

In the most strict case, a SBOM for a single component with no dependencies is just the list of that one component.

“Software” can be interpreted as “software system,” thus hardware (true hardware, not firmware) and very low-level software (like CPU microcode) can be included. Hardware is not excluded, but not the primary focus.

Inventory of one or more components plus other necessary information

Inventory

List of components using required identity information.

A subset of the larger, more comprehensive set of information that makes up SBOM.

We need to decide what to call the overall collection of data (recommendation: SBOM) that includes core component identity plus associated metadata (that is often necessary to enable use cases and applications).

Suggestion: “Inventory” is core component identity, “SBOM” is the larger/parent collection of data that includes Inventory, other metadata, sharing/exchange processes, and supplier requirements.

Core component identity.

Inventory is a subset of SBOM, inventory is required or there is no SBOM. Other useful SBOM (meta)information is allowed and optional and is something other than inventory. This meta information is likely required for any realistic application or use case, but it is separate from and tied to components listed in inventories.

Hardware is not excluded.