NTIA Software Component Transparency

Standards and Formats WG

Agenda

- Review of Charter, Goals and Objectives
- Definition of Success
- Alignment with Framing: MVP for Formats
- Current Formats: Mapping and Relationships
- Use Cases
- Workflows and Tooling
- Next Steps: How-To Guide

Charter of the Standards and Formats WG

Investigate existing standards and initiatives as they apply to identifying the external components and shared libraries, commercial or open source,
used in the construction of software products.
The group will analyze efforts underway in the community and industry related to assuring this transparency is readily available in a machine-readable manner.

Review Goals of This Group

- Investigate the options available today
- Determine how the solutions can work in harmony
- Document a workable and actionable machine-readable format(s)
- There is NOT a requirement to find a single solution/format
- Consider International aspects of proposed solutions as this is not a US problem. EU is already talking about this.

- ***There is a Win-Win for all – our job is to find it***

Tasks and Objectives: Crystallizing the "What"

- Scope requirements to drive a successful effort, to include the actual intent of this effort - DONE
- Create a common understanding of role of SWID, SPDX and other formats while examining their overlapping capabilities - DONE
- White Paper: output and summarization of standards and formats work to date - DONE
- Work with Use Case group to map needs and capabilities to formats - PENDING
  - Taxonomy of simple and complex use cases is still coalescing
  - Build-out of use cases is a necessary element of How-To Guide (next objective)
- Develop guidance on how to implement and consume Software Bill of Materials - IN PROGRESS
  - How-To Guide: Next deliverable, concrete and technical
  - Documentation and Reference Implementations for Tooling
  - Recipes for Common Use Cases
  - Moving beyond that What to How (based on other groups articulation of Why and Who)
- This working group should not reinvent the wheel but leverage what is on-going today globally while assuring we properly address best practices we encounter during our research. -- DONE

What Does Success Look Like?

- Machine Readable Format that:
  - Provides direct linkage to software publisher and components
  - Signed by the publisher
  - Automatable by potential products including vulnerability management tools
    - Provides data that can be used to automate enforcement of policies and processes
  - Verifiable to the package it represents
- Documented capabilities and ways to interpret it
- Useful in both the Open Source and to Commercial Product Vendor communities
- Actionable in that software publishers can implement in a lightweight fashion (published reference implementation)
- Should be a integrated part of a software publisher's development process to there is extremely low maintenance involved in keeping it current

Aligning with Framing: Minimum Viable

Framing Field	Represented in SPDX by:	Represented in SWID
Supplier	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/publisher), @name
Component	(3.1) PackageName: **	<softwareIdentity> @name
Unique Identifier	(3.2) SPDXID	<softwareIdentity> @tagID

Under Discussion	Represented in SPDX by:	Represented in SWID
version	(3.3) PackageVersion:	<softwareIdentity> @version
checksum/hash	(3.10) PackageChecksum: **	<Payload>/../<File> @[hash-algorithm]:hash
Relationship	(7.1) Relationship:	<Link>@rel, @href

** File, Snippet supported as well

Field Categories and Distribution

Category	**# SPDX fields**	**# SWID fields**
Component Identity - MVP	3	3
Component Identity - Post-MVP	3+	2+
Component Info	15	16
Description	13	17
Discovery	0	20
Entitlement & Procurements	0	6
IP Related	22	0
Mappings	6	5
SBOM Metadata	5	4
SBOM Provenance	4	3

Mappings & Relationships

Mapping Types	SPDX	SWID
between components in document	29	13
to external documents	1	1
to external sources (NVD, etc.)	2	1

Use Cases

There is some overlap but different fit for purpose

Software life cycle

Origination vs. consumption (deployment) and procurement

Developer workflow vs. packaged software distribution and utilization

Software product vs. contractor deliverables (e.g. O&M of custom code)

Procurement: Commercial transactions vs. non-contracted assets

IP management and software assurance are two different workflows

It is probable that the same enterprise would use both formats

Workflows and Tooling

SPDX:

OSS & Proprietary Tooling exists, and needs to be documented.

How-To Guide needs to include examples and reference implementations

SWID:

Documentation of standard is not free to access, which is obstacle in the OSS world

- freely available documentation includes: NISTIR 8060, ISO XML schema.

How-To Guide needs tooling in addition to examples and reference implementations.

Questions and Discussion

ASKS:

Use Cases to document simple and complex use cases

Definition of Complete

Clarity on permissibility of free/open SWID documentation

- is https://doi.org/10.6028/NIST.IR.8060, https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/ sufficient

Clarity on roadmap for OSS tooling to support SWID

Logistics

Contacts:

- J. C. Herz (Ion Channel) jc.herz@ionchannel.io
- Kate Stewart (Linux Foundation) kstewart@linuxfoundation.org

Mailing List: ntia-sbom-formats@linuxfoundation.org

Subscribe at: https://lists.linuxfoundation.org/mailman/listinfo/ntia-sbom-formats

Shared Drive: https://drive.google.com/drive/folders/1KAQ7AWlWMKcSFnRc_S-7XB76xFRRWLmT

NTIA Director David Redl’s Blog

“It is important to note that many technical solutions developed by industry and standards experts are available, but they haven’t been widely adopted. Better coordination is needed among software vendors, purchasing organizations, and security solutions providers to increase awareness of solutions and new approaches. A key objective of this process is building consensus across stakeholders on the best tools for sharing information on component data between vendors and customers.”

“For the software component transparency initiatives, NTIA welcomes participation from across the digital ecosystem, including software vendors, IoT manufacturers, medical device manufacturers, enterprise customers such as the financial services community, health care delivery organizations and higher education institutions. We also encourage input from vulnerability management solution providers, information security experts, and civil society.”

It is also NTIA’s first step in implementing the actions put forward by government and industry stakeholders in the **Report to the President on Enhancing Resilience Against Botnets**.

https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Action 1.3 Software development tools and processes to significantly reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry. The federal government should collaborate with industry to encourage further enhancement and application of these practices and to improve market

- “As an example, modern products use many software components, libraries, and modules, some of which may be outdated or vulnerable and are not always closely tracked by manufacturers in the rapid development cycle. While the notion of transparency around components of software is not new, wide support and adoption has not been realized. NTIA should engage diverse stakeholders in examining the strategies and policies necessary to foster a marketplace for greater software component transparency, including identifying and exploring market and other barriers that may inhibit progress in this space. Knowing what software has been incorporated into a product is a fundamental step toward being able to keep it updated and to mitigate threats when they arise.

https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets