Software Bill of Materials

ONAP Journey

Muddasar Ahmed, MITRE

2/15/2022

Supply Chain Attacks on the Rise

Solarwinds	KASEYA
MIMECAST	SITA
LEDGER	LOG4J

Open-Source Software Growth

- 73% Growth of Component Downloads
- 6 Million new Versions added in a year
- 37 million OSS Components Versions available
- 650% YoY increase in cyberattacks aimed at OSS suppliers

Regulatory and Consumer Demands

- US EO on America's Supply Chains(Feb)
- US EO on Improving the Nation's Cybersecurity (May) SBOM Called out
- UK Cyber resilience/NCSC efforts
- ENISA-Report on Supply Chain Security Attacks and recommendations

When is the Right Time for SBOM? NOW

- ✓Format Standard- **ISO/IEC 5962:2021**
  - ✓**SPDX® Specification V2.2.1**
- ✓Software- Many Commercial and OSS
- ✓User Demand- Enterprises and Governments
- ✓LFN IT

Software Bill of Material (SBOM)

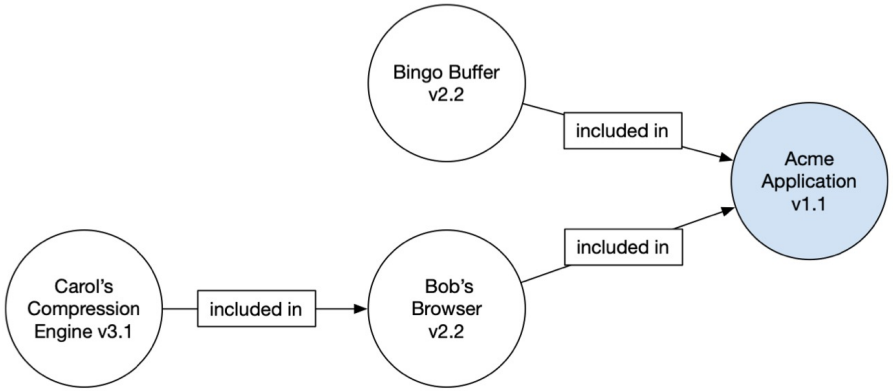
Software is made of bits of code and subroutines from numerous sources

SBOM is a list of all components, meta data and relationships

- Transparency (Software Supply Chain)
- Cyber Risk Management-
  - CTI to assets mapping
  - Assets to control mapping
- Source code & license management
- Early identification and mitigation of vulnerable systems
- Compliance and reporting (i.e., Gov. requirement for Software Composition Analysis-SCA, EO 14028)
- Slice and SLA Management (pricing and service)

Minimum Recommended Data Fields

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Componen	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

Source: www.ntia.gov, note minimum data field shown in the table, NTIA report also presents expanded data fields

NTIA Work and Options

SPDX 2.X is adopted as ISO standard

Three formats to implement SBOM

SPDX is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grass-roots effort includes representatives from more than 20 organizations—software, systems and tool vendors, foundations and systems integrators.

CycloneDX is a software bill of materials (SBOM) standard, purpose-built for software security contexts and supply chain component analysis. The specification is maintained by the CycloneDX Core working group, with origins in the OWASP community

OWASP Top 10

SWID tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.

<tag>

https://www.ntia.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf

SPDX - SBOM File Header

SPDXVersion: SPDX-2.2

DataLicense: CC0-1.0

SPDXID: SPDXRef-DOCUMENT

DocumentName: so-1.9.0-SNAPSHOT

DocumentNamespace: http://spdx.org/spdxpackages/so-1.9.0-SNAPSHOT-a132d8f5-e596-46e2-a600-bed5fc3abe2a

Creator: Tool: spdx-sbom-generator-v0.0.10

Created: 2021-10-13T03:08:25Z

SPDX - Package Information

Package representing the so

PackageName: so
SPDXID: SPDXRef-Package-so
PackageVersion: 1.9.0-SNAPSHOT
PackageSupplier: Organization: so
PackageDownloadLocation: https://mvnrepository.com/artifact/org.onap.so
FilesAnalyzed: false
PackageChecksum: SHA1: cd1b646ebd1f6844c60dd91951c6867e43857114
PackageHomePage: NOASSERTION
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageLicenseComments: NOASSERTION
PackageComment: NOASSERTION

SPDX - Relationship/Dependency

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-so

Relationship: SPDXRef-Package-so DEPENDS_ON SPDXRef-Package-jackson-annotations-

Relationship: SPDXRef-Package-so DEPENDS_ON SPDXRef-Package-javax.annotation-api-

Relationship: SPDXRef-Package-so DEPENDS_ON SPDXRef-Package-shazamcrest-0.11

Relationship: SPDXRef-Package-so DEPENDS_ON SPDXRef-Package-spring-boot-maven-plugin-2.3.7.RELEASE

Relationship: SPDXRef-Package-so DEPENDS_ON SPDXRef-Package-cxf-rt-rs-client-3.4.1

Relationship: SPDXRef-Package-so DEPENDS_ON SPDXRef-Package-jackson-databind-

SPDX - Included Packages

Package representing the logging-filter-base

PackageName: logging-filter-base
SPDXID: SPDXRef-Package-logging-filter-base-1.6.9
PackageVersion: 1.6.9
PackageSupplier: Organization: logging-filter-base
PackageDownloadLocation: https://mvnrepository.com/artifact/org.onap.logging-analytics/logging-filter-base/1.6.9
FilesAnalyzed: false
PackageChecksum: SHA1: 579ab04ada9450e0d9b481f8790434626e7a7574
PackageHomePage: NOASSERTION
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageLicenseComments: NOASSERTION
PackageComment: NOASSERTION

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Componen	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Follow Along

- ONAP Impelmentation
  - https://jira.linuxfoundation.org/browse/RELENG-4104
- LFN IT Gerrit SBOM generator conditional step
  - https://gerrit.linuxfoundation.org/infra/c/releng/global-jjb/+/69687
- Code
  - https://gerrit.linuxfoundation.org/infra/c/releng/global-jjb/+/69687/4/jjb/lf-maven-jobs.yaml#915

Useful References

- SPDX V2.2.1 Specification
- SPDX Online Tools
- NTIA SBOM Overview
- ONAP SBOM WIKI
- LFN-SCANs for ONAP

Useful References

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/**executive-order-on-americas-supply-chains/**
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/**executive-order-on-improving-the-nations-cybersecurity/**
https://www.gov.uk/government/collections/**cyber-resilience**
https://www.enisa.europa.eu/news/enisa-news/**understanding-the-increase-in-supply-chain-security-attacks**
https://www.ntia.gov/files/ntia/publications/**ntia_sbom_energy_jan2021overview**_0.pdf
https://www.ntia.doc.gov/**SBOM**

https://www.ntia.doc.gov/**SoftwareTransparency**
https://www.ntia.doc.gov/files/ntia/publications/**sbom_minimum_elements**_report.pdf
https://www.ntia.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf
https://www.devseccon.com/**security-fractals-and-the-open-source-supply-chain**-secadvent-day-4/
https://www.devseccon.com/a-**quick-introduction-to-software-bill-of-materials**-and-cyclonedx-secadvent-day-7/
Software Package Data eXchange (SPDX) https://spdx.dev/
https://**cyclonedx**.org/
http://dx.doi.org/10.6028/NIST.IR.8060