

CycloneDX

Software Bill of Materials Standard



Steve Springett



@stevespringett



steve.springett@owasp.org

- Leader of OWASP Dependency-track
- Chair, OWASP CycloneDX Core Working Group
- Leader and co-author of OWASP SCVS
- Contributor to Package URL standard
- Multiple software transparency working groups
- Software security leadership at ServiceNow



Patrick Dwyer



@coderpatros



patrick.dwyer@owasp.org

- Co-Leader of OWASP CycloneDX
- Multiple software transparency working groups
- Software Development Lead (Government)
- OSS Maintainer

Got SBOM?

Analogy

INGREDIENTS: Peanuts Roasted Salted (Peanuts, Sunflower Oil, Salt), Chocolate Peanuts Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Peanuts Blanched Roasted (Peanuts, Sunflower Oil)), Almonds, Chocolate Coffee Beans Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Coffee Beans Espresso Roasted), Pecans, Organic Dark Chocolate Drops (Organic Evaporated Cane Syrup, Organic Chocolate Liquor, Organic Cocoa Butter, Organic Soy Lecithin), Chocolate Almonds Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Almonds), Yogurt Almonds Natural (Yogurt Coating Natural (Evaporated Cane Syrup, Palm Kernel Oil, Yogurt Powder, Soy Lecithin (an Emulsifier), Lactic Acid, Natural Vanilla, Salt), Almonds)

CONTAINS PEANUTS, SOY, NUTS, MILK

Analogy

INGREDIENTS: Peanuts Roasted Salted (Peanuts, Sunflower Oil, Salt), Chocolate Peanuts Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Peanuts Blanched Roasted (Peanuts, Sunflower Oil)), Almonds, Chocolate Coffee Beans Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Coffee Beans Espresso Roasted), Pecans, Organic Dark Chocolate Drops (Organic Evaporated Cane Syrup, Organic Chocolate Liquor, Organic Cocoa Butter, Organic Soy Lecithin), Chocolate Almonds Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Almonds), Yogurt Almonds Natural (Yogurt Coating Natural (Evaporated Cane Syrup, Palm Kernel Oil, Yogurt Powder, Soy Lecithin (an Emulsifier), Lactic Acid, Natural Vanilla, Salt), Almonds)

CONTAINS PEANUTS, SOY, NUTS, MILK

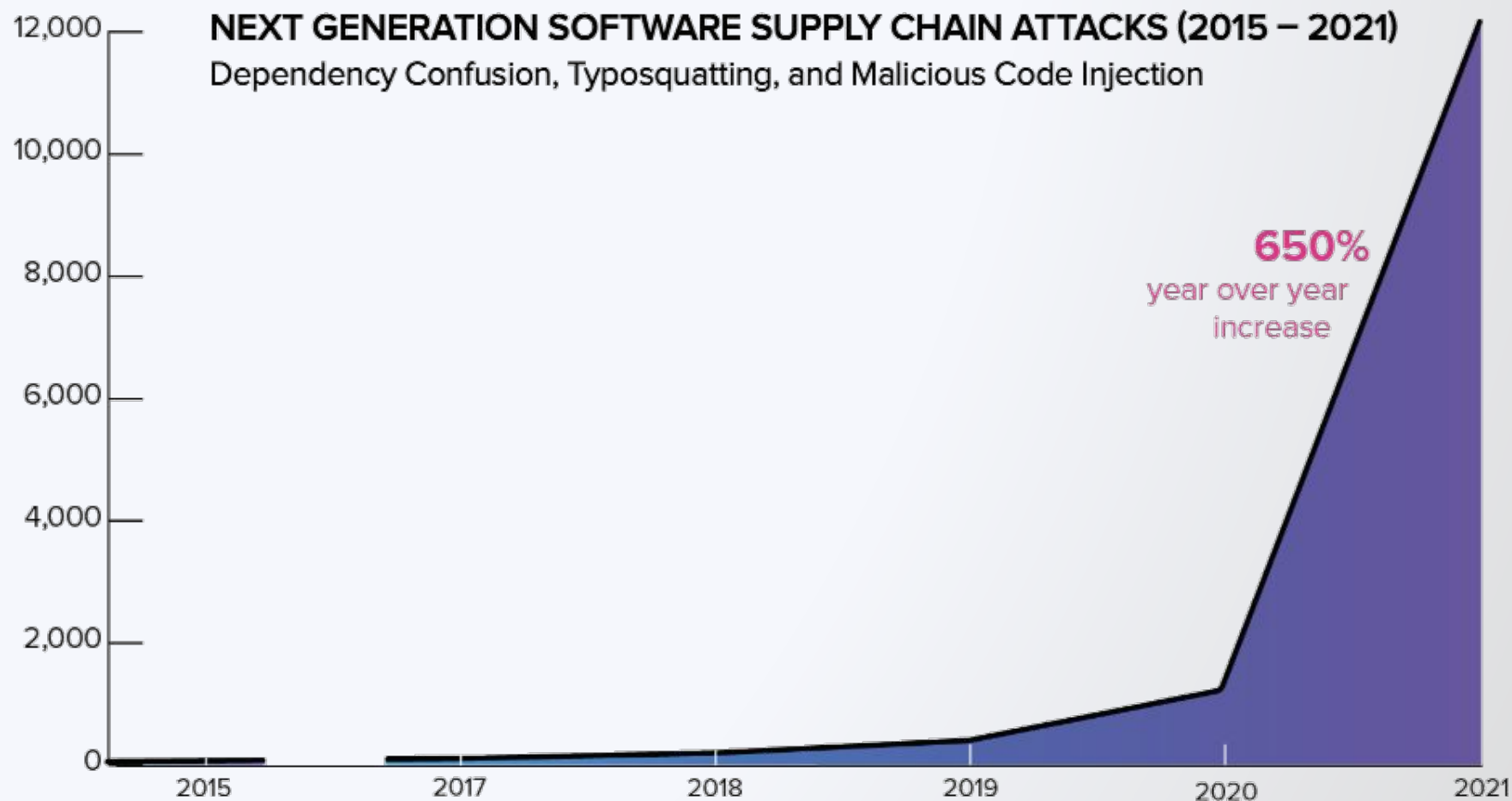
Contributing Factors

73%

YoY growth
of component downloads

Open source demand is exploding.

In 2021 developers around the world will request more than 2.2 trillion open source packages from these same four ecosystems, representing a 73% YoY growth in developer downloads of open source components. Despite the growing volume of downloads, the percentage of available components utilized in production applications is shockingly low.



Source: Sonatype 2021 State of the Software Supply Chain

Contributing Factors

Supply Chain Management

Fewer & better suppliers

Use highest quality parts
from those suppliers

Track throughout lifecycle

Market Forces

Maturity of software
development organization

Procurement and M&A

Operational costs

Impact analysis

Regulation

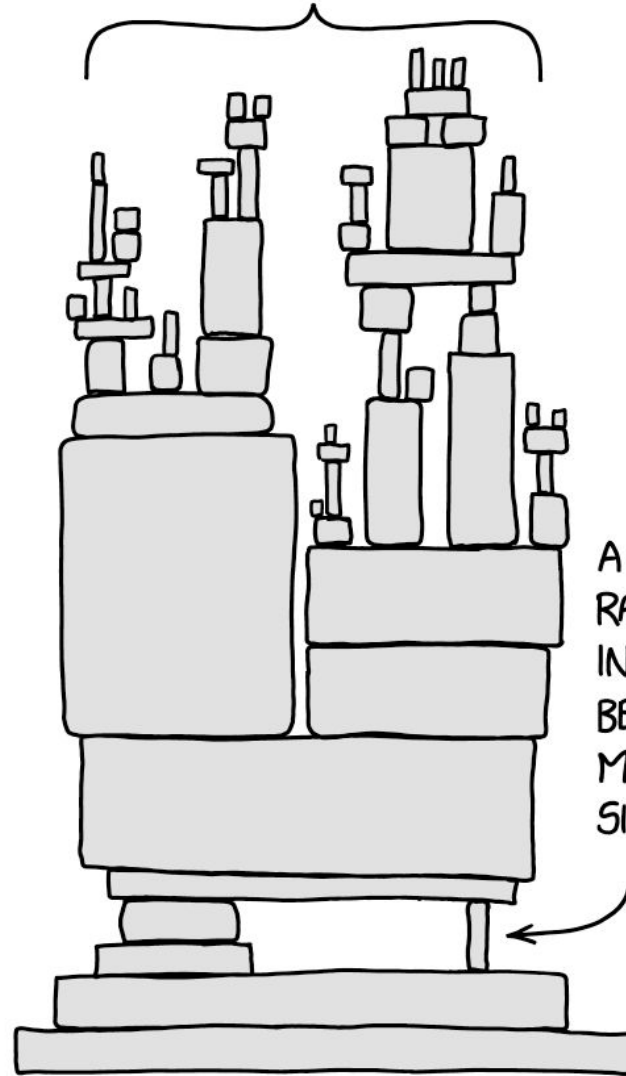
U.S. Executive Order 14028
requiring SBOMs

FDA pre-market
requirements

Critical infrastructure
(e.g. Energy)

... and many more

ALL MODERN DIGITAL
INFRASTRUCTURE



A PROJECT SOME
RANDOM PERSON
IN NEBRASKA HAS
BEEN THANKLESSLY
MAINTAINING
SINCE 2003

Source: xkcd Dependencies

Introducing CycloneDX

- Flagship OWASP standards project
- Lightweight SBOM standard purpose built for cybersecurity use cases
- Designed in May 2017
- Initial release March 2018
- Yearly releases since
- Formal governance and standards process
- Recommended by multiple world governments
- Large and growing industry and vendor support
 - <https://cyclonedx.org/about/supporters/>

Describe complete and accurate inventory

Security vulnerability analysis

Integrity verification

Software package evaluation

License identification and compliance

Describe complex component assemblies

Describe component pedigree

Describe component provenance

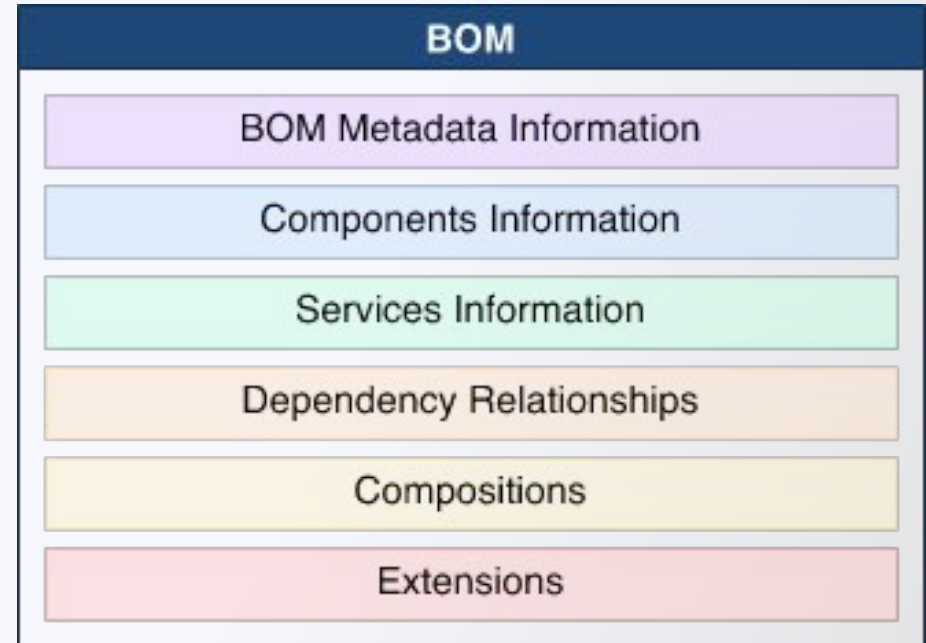
Describe reliance on services

Capture dependency relationships


and many, many more...

The CycloneDX Object Model

- Lightweight - focus on simplicity
- Optimized for highly automated processes
- Easy to implement and adopt
- Supports:
 - Applications
 - Libraries
 - Frameworks
 - Containers
 - Operating systems
 - Firmware
 - Devices
 - Files
 - Services



Use Case Examples

GETTING STARTEDSPECIFICATIONABOUTTwitterGitHubEmailDiscordYouTube

Use Cases

The following examples provide guidance as to the minimal fields required to achieve specific use cases. Ideally, all optional fields would be populated in order to achieve all use cases. Many of the cases highlighted are directly or closely related to security.

Inventory

A complete and accurate inventory of all first-party and third-party components is essential for risk identification. BOMs should ideally contain all direct and transitive components and the dependency relationships between them.

CycloneDX is capable of describing the following types of components:

COMPONENT TYPE	CLASS
Application	Component
Container	Component
Device	Component
Library	Component
File	Component
Hardware	Component

Inventory

Known vulnerabilities

Integrity verification

Authenticity

Package evaluation

License compliance

Assembly

Dependency graph

Provenance

Pedigree

Service definition

Properties / name-value store

Packaging and distribution

Composition completeness

OpenChain conformance

Vulnerability remediation

Vulnerability disclosure

Security advisories

External references

A collection of common use cases achievable with CycloneDX along with concrete examples in XML and JSON.

<https://cyclonedx.org/use-cases/>

Tool Center

The screenshot shows the CycloneDX Tool Center interface. At the top is a dark navigation bar with the CycloneDX logo and links for GETTING STARTED, SPECIFICATION, ABOUT, and social media icons. Below the navigation bar is the 'Tool Center' title. A filter bar allows users to show all tools (79) or filter by license (Open source: 65, Proprietary: 14), integration type (Build integration: 34, Analysis: 21), author (Author: 1), GitHub action (7), or transform (5). Further filters include Library (8), Signing / Notary (2), and Distribute (1). The main area displays six tool cards:

- Auditjs** (Sonatype): Audits an NPM package.json file to identify known vulnerabilities. 39 Forks, 158 Stars. Tags: opensource, build-integration.
- BOM Repository Server** (CycloneDX): A lightweight repository server used to publish, manage, and distribute CycloneDX SBOMs. 0 Forks, 8 Stars. Tags: opensource, distribute.
- Chelsea** (Sonatype): Dependency vulnerability auditor for Ruby. 3 Forks, 7 Stars. Tags: opensource, build-integration.
- CodeNotary vcn** (CodeNotary): Protects an organizations software development pipeline from supply chain attacks. CodeNotary natively supports CycloneDX SBOMs. 20 Forks, 115 Stars. Tags: opensource, signing-notary.
- CodeSentry** (GammaTech): Software Composition Analysis (SCA) platform that leverages binary analysis to identify components, inherited risk, and communicates inventory through CycloneDX SBOMs. Tags: proprietary, analysis.
- Contrast Security** (Contrast Security): Automatically generates component inventory from runtime analysis (IAST or RASP) and generates CycloneDX SBOMs. Tags: proprietary, analysis.

Community effort to establish a marketplace of free, open source, and proprietary tools and solutions that support CycloneDX.

<https://cyclonedx.org/tool-center/>

Community Participation

- Website (introduction, use cases, tool center, and specification)
 - <https://cyclonedx.org/>
- GitHub
 - <https://github.com/CycloneDX>
- Slack
 - <https://cyclonedx.org/slack>
 - <https://cyclonedx.org/slack/invite>
- Mailing List
 - <https://cyclonedx.org/discussion>

Thank You

