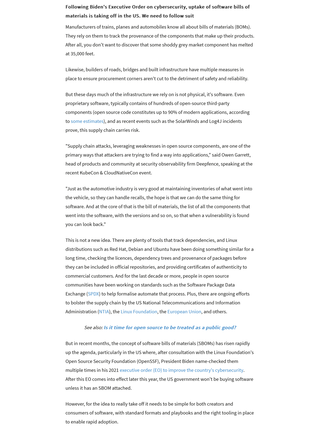


All about SBOMs: the latest moves to secure the software supply chain

John Leonard
29 July 2022 • 4 min read

Following Biden's Executive Order on cybersecurity, uptake of software bills of materials is taking off in the US. We need to follow suit

Manufacturers of trains, planes and automobiles know all about bills of materials (BOMs). They rely on them to track the provenance of the components that make up their products. After all, you don't want to discover that some shoddy grey market component has melted at 35,000 feet.

Likewise, builders of roads, bridges and built infrastructure have multiple measures in place to ensure procurement corners aren't cut to the detriment of safety and reliability.

But these days much of the infrastructure we rely on is not physical, it's software. Even proprietary software, typically contains of hundreds of open-source third-party components (open source code constitutes up to 90% of modern applications, according to some estimates), and as recent events such as the SolarWinds and Log4J incidents prove, this supply chain carries risk.

"Supply chain attacks, leveraging weaknesses in open source components, are one of the primary ways that attackers are trying to find a way into applications," said Owen Garrett, head of products and community at security observability firm Deepfence, speaking at the recent KubeCon & CloudNativeCon event.

"Just as the automotive industry is very good at maintaining inventories of what went into the vehicle, so they can handle recalls, the hope is that we can do the same thing for software. And at the core of that is the bill of materials, the list of all the components that went into the software, with the versions and so on, so that when a vulnerability is found you can look back."

This is not a new idea. There are plenty of tools that track dependencies, and Linux distributions such as Red Hat, Debian and Ubuntu have been doing something similar for a long time, checking the licences, dependency trees and provenance of packages before they can be included in official repositories, and providing certificates of authenticity to commercial customers. And for the last decade or more, people in open source communities have been working on standards such as the Software Package Data Exchange (SPDX) to help formalise automate that process. Plus, there are ongoing efforts to bolster the supply chain by the US National Telecommunications and Information Administration (NTIA), the Linux Foundation, the European Union, and others.

See also: Is it time for open source to be treated as a public good?

But in recent months, the concept of software bills of materials (SBOMs) has risen rapidly up the agenda, particularly in the US where, after consultation with the Linux Foundation's Open Source Security Foundation (OpenSSF), President Biden name-checked them multiple times in his 2021 executive order (EO) to improve the country's cybersecurity. After this EO comes into effect later this year, the US government won't be buying software unless it has an SBOM attached.

However, for the idea to really take off it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place to enable rapid adoption.

"We really need to be able to figure out how to get to scale efficiently and effectively," said Kate Stewart, VP dependable embedded systems at the Linux Foundation.

Focusing minds: Biden's EO

There are, of course, many differences between a software stack and a car. Unlike a tappet or a shim, which are largely fit-and-forget until they reach end of life, software libraries, modules, services and their subordinate dependencies - change often. To make things more complex, production versions of software may differ from those in development with the addition of agents and services. Moreover, different development toolchains may produce slightly different results.

But there are similarities too, not least that some components are more critical than others: you worry more about a database that has a vast header. Likewise, not everything in an SBOM needs to be to the same depth.

But what is an SBOM?

According to the NTIA, it's "a formal record containing the details and supply chain relationships of various components used in building software".

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier Name, Component Name, Version of Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

Source NTIA

To comply with Biden's EO, it should contain, as a minimum, information about the supplier of each component, the version, identifiers which may include hashes and checksums, the dependency relationship (for example, that it is built on it); that there are dynamic dependencies on third-party services), a timestamp and authorship. It should be machine-readable and contain information about the frequency of updates, the nature of dependencies (direct or transitive) - and 'known unknowns' which may need to be explored by other means.

SBOMs are extensible, designed to support requirements as needed, while remaining backwards-compatible. They may contain data about licences and copyright. They should not affect IP as they contain only metadata, a list of ingredients rather than code. They do not cover the workings of algorithms.

Ideally, a new SBOM should be created automatically every time the code changes. They should include links to embedded dependencies and be digitally signed at the build, although there is no standard way to do this as yet.

There is more than one type of SBOM: they may cover source code, build artefacts, binary analysis and deployed software - tracking how it is used. These types should fit together to cover the software development and usage lifecycle.

There are open source projects like *Zephyr* and *Yocto* that are aimed at automatically creating SBOMs at various points in the lifecycle, including for embedded systems and IoT.

As far as their consumption is concerned, this should be automated, with tools able to accept or reject software based on pre-chosen criteria, such as configuration, licensing, vulnerabilities, and supply chain risk.

SBOM awareness

Awareness of SBOMs varies depending very much where you are, geographically, culturally and in your maturity with open source. "The future is here, it's just unevenly distributed", notes the NTIA, quoting author William Gibson. If you are in a regulated industry in the US, you are likely to have a good understanding of SBOMs, to have been proactively securing your software supply chain for a few years now, and be preparing to formalise the process. If not, they are likely something of a mystery.

A survey of IT vendors, service providers and end users by the Linux Foundation found that 76% of respondents were considering changes in response to the US Executive Order on Cybersecurity, with 82% aware of the term SBOM.

"We're seeing a a fair amount of activity in the healthcare sector, the energy sector, the automotive sector, anything that's potentially interacting with safety certifications, and so forth, at least in the US," said Kate Stewart, VP dependable embedded systems at The Linux Foundation, saying that organisations in those sectors have been working on proofs of concepts.

Meanwhile, in the UK the picture is very different. A survey by OpenUK of organisations that use open source software found that just 23% of respondents were aware of and use SBOMs. An additional 22% were aware but do not use them, leaving 51% unaware of the term. That study is published in the not-for-profit's latest *State of Open* report.

It seems the US government's edicts have focused minds in a way that has yet to be replicated in Europe, where a clump of specialists are in the know, often those deeply involved in open source or security, while the broad landscape of the business and software communities is unaware. While open source adoption is gathering pace along with digital transformation in the UK, best practices are a bit behind, said Amanda Brock, CEO of OpenUK.

"It's getting a shift from doing open source, which is happening, and doing open source well, so that we know that we've got a well-maintained and secure open source software that people are going to want over the long term."

What's next?

SBOMs are not the only tool for securing the software supply chain. In fact, they make up just one element of the OpenSSF's 10 point plan to improve open source security. A well-known issue is that many widely used components are maintained by just one volunteer (or at least very few), probably unpaid. This is sometimes called the 'bus problem', as in 'what if the maintainer goes under a bus'?

Source. Randall Munroe, Licensed under CC BY-NC 2.5

The bus problem is a focus of another OpenSSF effort, Alpha Omega, a project kickstarted with funding from Microsoft and Google. Alpha seeks to support maintainers of the most critical open source projects (those that would have an especially large impact they have a significant vulnerability), while Omega is focused on finding security flaws in the top half of 10,000 projects.

The two funders are also moving ahead with code security ventures of their own. Microsoft has adopted SPDX (recently made an ISO standard (ISO/IEC 5962:2021)), for its own SBOM generator; Google recently announced its Assured OSS which is designed to enable users of open source software to incorporate the same OSS packages that Google uses into their own developer workflows; and there are other examples too of firms 'curating' components to de-risk them for users.

But it's no good all this activity happening in silos, said OpenUK's Brock. It needs to scale up, and it needs to scale up fast.

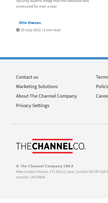
"There is a global community that contributes to open source. So we need to make sure that all governments are going on that journey, not just the US."

Related Topics
Security Technology Open Source SBOM open source Linux Foundation OpenSSF
openssh supply chain attack

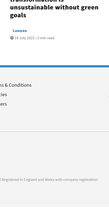
PREVIOUS ARTICLE
US Senators demand cryptominers disclose emissions and energy use

AUTHOR SPOTLIGHT
John Leonard
View profile
More from John Leonard
Learning lessons from Netflix's losses
How attack can reveal identities of anonymous users on any major browser

More on Hacking



HACKING
Alibaba executives questioned over Chinese data breach
Security experts allege that the database was unsecured for over a year
Otto Owens
13 July 2021 • 2 min read



STRATEGY
Partner content: Emerging technology - why digital transformation is unsustainable without green goals
Lenovo
18 July 2022 • 3 min read

STRATEGY
Partner Content: Keynote series - Smarter Technology for the Next Reality
Lenovo
18 July 2022 • 3 min read