SBOM Sharing Primer

Executive Summary

This document provides examples of how software bill of materials (SBOM) can be shared between different actors across the software supply chain. It focuses on the processes and mechanisms for sharing SBOMs, assuming one party has created an SBOM and another party wants to access it. The examples demonstrate SBOM sharing methods currently in use, ranging from proprietary software vendors sharing SBOMs via email to open source projects publishing SBOMs in centralized repositories.

Additionally, this document builds upon the “SBOM Sharing Lifecycle Report,” a joint publication from the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Energy (DOE) Cybersecurity, Energy Security, and Emergency Response’s (CESER) “SBOM Sharing Lifecycle Report,” and the “SBOM Sharing Roles and Considerations” document drafted by the CISA facilitated Sharing and Exchanging SBOM community-driven workstream. The three SBOM sharing lifecycle phases (Discovery, Access, Transport) described in the Lifecycle Report are represented and accompanied by definitions for SBOM Author and Consumer. This document does however deviate from the SBOM Sharing Lifecycle Report’s use of SBOM Provider by adopting the “SBOM Sharing Roles and Considerations” document’s use of SBOM Distributor.

The SBOM sharing concept of sophistication that originates in the Lifecycle Report is adopted in this document through the inclusion of a table from the Lifecycle Report that gives sharing examples at each lifecycle phase by order of low, medium, and high sophistication. All the sharing examples include benefits and cautions of using the different Discovery, Access, and Transport methods. The document then provides each example’s lifecycle phase, a sophistication rating, and a justification for that rating.

The document concludes that choosing an appropriate sharing mechanism depends on factors like software licensing, industry practices, and organizational priorities. As SBOM adoption grows, new sharing models will likely emerge, especially those leveraging automation and standards. Mature SBOM sharing practices will be key to realizing the full benefits of software transparency.

Introduction

This document, [1] building on the work of the "SBOM Sharing Lifecycle Report"[2] and the "SBOM Sharing Roles and Considerations",[3] offers examples of how SBOMs can be shared between actors across the SBOM sharing lifecycle. It may be helpful for the reader to begin with the "SBOM Sharing Roles and Considerations" and "SBOM Sharing Lifecycle Report" before delving into the practical applications of the SBOM sharing discussions in this Primer. The basis of the SBOM sharing discussion can be found in those preceding documents and is not explored here. This document records methods for SBOM sharing currently being implemented by practitioners in the software community. This is only the first iteration of this document. Examples were gathered from members of CISA's community-driven working groups. The authors intend that this document be regularly updated with new methods of SBOM sharing.

The examples are listed in order of sophistication[4] of the overall SBOM sharing method based on the evaluation of the Discovery, Access, and Transport phases. Organizations can use the examples offered here to understand where their SBOM sharing process is on the sophistication scale, compare other methods of sharing SBOM, and consider other methods for SBOM sharing.

It is important to note that sophistication does not imply maturity or preferability. For example, publishing a publicly available SBOM for anyone to download may be a low-sophistication discovery method, and that could be the appropriate choice for an open source project. Furthermore, sophistication may be dependent on industry standards and regulations. In short, the sophistication level likely reflects priorities in the sharing context rather than a judgment of security maturity.

Scope

This document focuses on processes and mechanisms for sharing SBOMs. Critically, the document assumes that one party has created an SBOM and another party is interested in that SBOM data. Any topics regarding the quality of the SBOM, how to generate an SBOM, or how to utilize an SBOM after receiving it are outside the scope of this paper. For guidance on what goes into an SBOM or best practices for generating SBOMs, see "Framing Software Component Transparency: Establishing a Common Software Bill of

[1] This document was drafted by the SBOM Sharing and Exchanging Working Group, a community-driven workstream. For more information see About this document.

[2] The authors borrow the "Discovery; Access; Transport" framework from the SBOM Sharing Lifecycle Report to break down the SBOM sharing process. CISA and U.S. Department of Energy. Software Sharing Lifecycle Report. April 17, 2023.

[3] The authors borrow the SBOM Author; SBOM Distributor; SBOM Consumer definitions from the SBOM Sharing Lifecycle Report and the definitions can also be found in this document in the Definitions section. CISA and U.S. Department of Energy. Software Sharing Lifecycle Report. April 17, 2023.

[4] The term sophistication is borrowed from the SBOM Sharing Lifecycle Report and the definition can also be found in this document in the Definitions section.

Materials (SBOM)”[5] and the Software Transparency Healthcare POC’s “How-To Guide for SBOM Generation.”[6]

This paper is not intended to be an exhaustive list of methods for sharing SBOMs but rather to offer existing options for sharing SBOMs and to outline the considerations in each model that may determine whether a model is a good fit for an organization. Similarly, this paper documents existing SBOM sharing methods without comment on SBOM quality, accuracy, format, or requirements for self-attestation.

Definitions

The following SBOM sharing actors' definitions are borrowed from the “SBOM Sharing Lifecycle Report”, “SBOM Sharing Roles and Considerations” document, and the NTIA’s “Sharing and Exchanging SBOMs” document:

SBOM Author: Creates an SBOM.

SBOM Consumer: Receives the transferred SBOM. This could include roles such as third parties, authors, integrators, distributors, and end users.

SBOM Distributor: Receives SBOMs to share them with SBOM Consumers or other SBOM Distributors.

The role of the SBOM Distributor is a new addition to the SBOM sharing discussion. The role is introduced to capture the role of organizations that neither produce SBOMs nor make use of SBOM data.

Sophistication: The relative amount of time, resources, subject-matter expertise, effort, and access to tooling needed to implement a phase of the SBOM sharing lifecycle. Sophistication can be either Low, Medium, or High.

The definition of “sophistication” is borrowed from the “SBOM Sharing Lifecycle Report.” The term sophistication does not imply judgment regarding the SBOM sharing mechanism selected by an organization. As stated in the “SBOM Sharing Lifecycle Report,” sophistication levels for the three phases (Discover, Access, and Transport) do not imply low or high maturity for the SBOM sharing method. Organizations select the discovery, access, and transport mechanism based on their priorities, potential industry constraints, and best practices.

[5] NTIA Open Working Group on Software Component Transparency Framing. Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM). October 21, 2021.

[6] NTIA Open Working Group on Software Transparency Healthcare Proof-of-Concept. How-To Guide for SBOM Generation. 2021.

This document practically applies the SBOM sharing discussions in the “SBOM Sharing Lifecycle Report” and “SBOM Sharing Roles and Considerations” documents. The report divides the SBOM sharing lifecycle into three phases.

Discovery: Mechanism used by the Consumer to know the SBOM exists and how to access it.

Access: Access control mechanisms the Author or Distributor uses to regulate who can view or use an SBOM.

Transport: Mechanism provided by the Author or Distributor to transfer an SBOM. Also, the action of the Consumer receiving an SBOM.

SBOM Sharing Lifecycle Phases and Sophistications

The purpose of Table 1 (see below) is to highlight possible examples of sophistication for each SBOM lifecycle phase. Table 1 is borrowed from the “SBOM Sharing Lifecycle Report” but with one modification: “Provider” has been changed to “Distributor.”

The table is included here due to its central role in evaluating the sophistication of the Discovery, Access, and Transport phases in the SBOM sharing examples discussed in this document. The authors of this document are grateful to Department of Energy (DOE) Cybersecurity, Energy Security, and Emergency Response (CESER) and the Cybersecurity and Infrastructure Security Agency (CISA), the co-sponsors of the “SBOM Sharing Lifecycle Report” for granting permission to use the table in this document. For a more in-depth discussion on the SBOM sharing lifecycle sophistication examples shown in Table 1, see the discussion section of the “SBOM Sharing Lifecycle Report” and the “Sharing and Exchanging SBOMs”[7] document.

[7] NTIA Open Working Group on Software Component Transparency Framing. Sharing and Exchanging SBOMs. February, 10, 2021.

Figure 1: SBOM Sharing Lifecycle Phases and Sophistications

Lifecycle Phase	**Sophistication Low**	**Sophistication Medium**	**Sophistication High**
Discovery	● Consumer initiated ● Limited or non-existent guidance given by Author or Distributor	● SBOM placed in software source code - Point in time (Singular Version) - Manufacturer Usage Description (MUD) ● Known central repository ● Website	● Automated propagation of available SBOMs ● Continuous updates to relevant parties ● Publish/Subscribe pattern ● Distributed ledger
Access	● No controls in place ● Manual controls ● Case-by-case	● Authentication required ● Limited access control granularity ● Private/broadcast/public channels, roles ● Private chains/consensus algorithm	● Delegated authentication and access controls ● Full access control granularity
Transport	● Human initiated process ● Point-to-point ● Verbal transmission	● Inconsistent, varied method or documentation ● Ad-hoc automation	● Documented ● Repeatability ● Automated access ● Well-known protocols (e.g., REST/RESTful/SOAP API) ● Distributed ledger synchronization

Examples of SBOM Sharing in Use Today

SBOM sharing is happening today among different parties that could be classified as SBOM Authors, Distributors, or Consumers. This paper documents use cases of SBOM sharing among these actors.[8] These examples assume that the SBOM Author or Distributor has an SBOM available for sharing and that the SBOM Consumer or Distributor knows what SBOM they are looking for and is able to communicate that to the appropriate parties. The sharing use cases are then evaluated in terms of benefits and cautions to help the reader understand the trade-offs of using a particular discovery, access, or transport method.

Furthermore, the sophistication levels of the Discovery, Access, and Transport phases of each example are indicated to anchor the paper in the larger SBOM sharing discussion and analysis conducted in the "SBOM Sharing Lifecycle Report" and the "SBOM Sharing Roles and Considerations" documents. The six examples are organized in this paper by aggregate levels of sophistication as determined in the "SBOM Sharing Lifecycle Report," with average lower levels of sophistication for Discovery, Access, and Transport at the top of the paper and higher average levels of sophistication at the bottom. Arranging the paper by levels of sophistication does not imply an organization needs to continuously increase its level of sophistication for its chosen SBOM sharing mechanism. Instead, the examples are ordered by sophistication to allow readers to identify similar SBOM-sharing mechanisms and consider additional methods. The paper also provides justifications for why each mechanism has been designated as sophistication Low, Medium, or High. As a note for the reader, it is possible for Discover, Access, and Transport mechanisms to lie between the sophistication Low, Medium, and High categories.

Example 1: SBOMs for Proprietary Software Shared via Email

An organization, here acting as an SBOM Consumer, would like an SBOM for software it already operates. To obtain an SBOM, the organization reaches out to its software vendor via email. The software vendor has an internally generated SBOM, making it the SBOM Author.

Upon receiving the email request, the SBOM Author's legal and production teams verify that the organization making the request is (1) an existing customer or party with a pre-

[8] This paper is not intending to be an exhaustive list of SBOM sharing methods currently being used.

sales agreement in place and (2) not barred from technology transfers by export controls or other regulations, such as Office of Foreign Asset Control Sanctions.[9]

Once all policy and compliance requirements are met, the SBOM Author responds to the SBOM Consumer with an encrypted email containing a non-disclosure agreement (NDA). The SBOM Consumer then digitally signs and returns the NDA to the SBOM Author, and the SBOM Author replies with an encrypted email containing an SBOM.

Benefits	Cautions
● High degree of control over Discovery, Access, and Transport processes ● Opportunity to customize process and data transmitted on a per-request basis	● Not automatable or scalable ● Legal challenges and requirements ● Longer time to delivery

Discovery Sophistication: Low

Justification: The SBOM Consumer initiated contact with the SBOM Author using email, which is a non-resource-intensive communication method that required no subject-matter expertise.

Access Sophistication: Medium

Justification: The SBOM Author has manual access control processes in place with its internal vetting process. The encrypted email requires identity authentication.

Transport Sophistication: Low

Justification: The SBOM Author is sending the SBOM as an email attachment.

Example 2: SBOMs for Proprietary Software Shared via Vendor Portal

An organization, acting as an SBOM Consumer, logs into its vendor's support portal and requests an SBOM for a software component supplied by the vendor. The vendor has an internally generated SBOM, making them the SBOM Author. The SBOM Author receives the request through the portal and initiates internal compliance procedures, including vetting against legal requirements and internal policy. An NDA is already in place in this case. Upon receiving the request in the portal, the SBOM Author sends the SBOM

[9] For more information, see the U.S. Department of the Treasury's Office of Foreign Assets Control website.

Consumer a secure link to a private file-sharing platform that allows them to download the SBOM.

Benefits	Cautions
● High degree of control over Discovery, Access, and Transport processes	● Not automatable or scalable ● Legal challenges and requirements ● Long time to delivery

Discovery Sophistication: Medium

Justification: The SBOM Consumer initiated contact with the SBOM Author through a known website (i.e., vendor support portal).

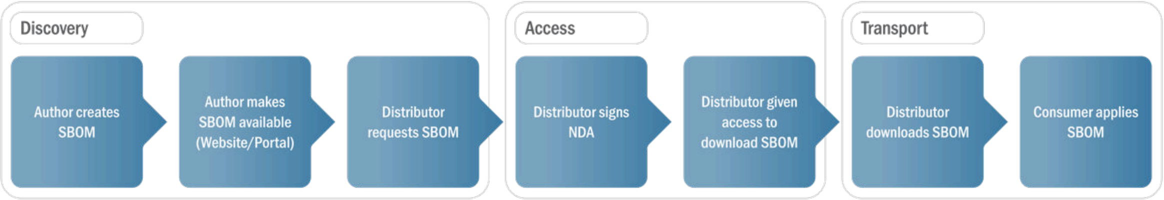
Access Sophistication: Medium

Justification: Authentication is required by the SBOM Consumer logging in to the vendor portal to request and download the SBOM.

Transport Sophistication: Low

Justification: The transport process is human-initiated by the vendor sending the file-sharing link to the SBOM Consumer. The private file-sharing platform is a form of point-to-point transport.

Example 3: SBOMs for Proprietary Software Shared via Vendor Portal with Pre-Vetting


Discovery
Author creates SBOM
Author makes SBOM available (Website/Portal)
Distributor requests SBOM
Access
Distributor signs NDA
Distributor given access to download SBOM
Transport
Distributor downloads SBOM
Consumer applies SBOM

A device vendor, (e.g., a medical device manufacturer), generates an SBOM internally and uploads the SBOM to a portal, without request from an SBOM Consumer.

The device vendor’s customers have been previously vetted for access to any data provided through the portal, including SBOM data. An organization, one of the device vendor’s customers, is acting as an SBOM Consumer and looking for an SBOM from the device vendor.

The SBOM Consumer logs into the portal and requests the SBOM. The SBOM Consumer is automatically presented with an NDA within the portal. After completing and signing electronically, the SBOM Consumer is automatically granted access to download the SBOM from within the portal. All SBOM sharing-related activity occurs within the vendor's portal.

Benefits	Cautions
● More streamlined than e-mail ● Legal agreement is done inline	● Not automatable and scalable due to reliance on Consumer initiating the SBOM sharing process for each SBOM ● Requires digital authentication of the SBOM Consumer and automatic policy checks

Discovery Sophistication: Medium

Justification: The SBOM is placed in a portal, the functional equivalent to a known central repository.

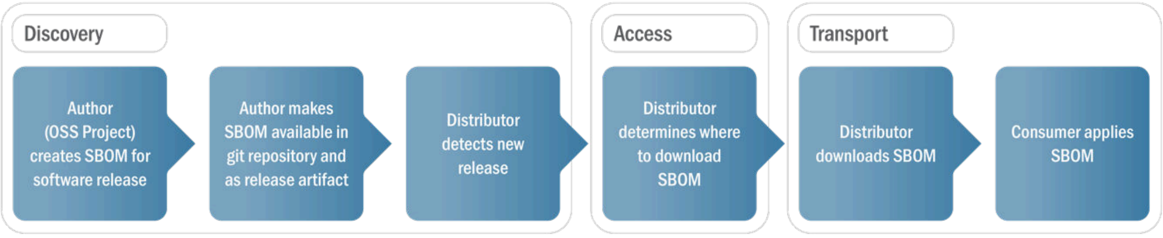
Access Sophistication: Medium

Justification: The initial vetting of the device SBOM Consumer to receive portal access is a prerequisite of authentication. Authentication is required to log into the device vendor portal, and requiring an NDA to be electronically signed before the device user has access to an SBOM is an access control measure.

Transport Sophistication: Medium

Justification: Transport is accomplished through an HTTPS download, a well-known transport method.

Example 4: SBOM for Open Source Software (OSS) Shared via Tooling


Discovery
Author (OSS Project) creates SBOM for software release
Author makes SBOM available in git repository and as release artifact
Distributor detects new release
Access
Distributor determines where to download SBOM
Transport
Distributor downloads SBOM
Consumer applies SBOM

The Open Source Security Foundation (OpenSSF) SBOM Everywhere Special Interest Group[10] is establishing guidance on open source software SBOM naming conventions.[11] These naming conventions provide consistent naming and storage locations for SBOM Authors of open source software to place Source and Build SBOMs.[12] Consistency in naming and storage allows for easier discovery by SBOM Distributors and Consumers.

OSS project maintainers, acting as SBOM Authors, automatically create Source and Build SBOMs[13] and publish SBOMs to the locations outlined in open source software SBOM naming conventions[14] or Security Insights Specification[15] for application releases. The SBOM Author is effectively publishing the SBOM on a website either as a release artifact or within the version control management system. SBOM Distributors and Consumers are then able to anonymously access and download the SBOM. Consistency in naming conventions allows SBOM Distributors and Consumers to manually or automatically download SBOMs if mapping is available from the package to an open source repository. This will be easier in some open source ecosystems than others.

There are burgeoning SBOM repositories for open source projects. For example, OpenSSF's Sigstore Cosign Specification[16] allows container image SBOMs to be stored in an Open Container Initiative (OCI) compatible registry as an artifact. The operator of the container registry acts as an SBOM Distributor.

SBOM Consumers can use automated dependency update tooling to detect new application releases and discover the correct SBOM for the release needed. Since SBOMs in this ecosystem are publicly accessible and have consistent naming, SBOM Consumers can collect SBOMs "at scale" to better automate license management and vulnerability analysis.

Benefits	**Cautions**
● SBOM was created by the OSS project instead of a third party	● It requires mapping from the application to the OSS project

[10] GitHub. OSSF SBOM Everywhere SIG. February 16, 2024.

[11] GitHub. OSSF SBOM Everywhere SIG: Best Practices for Naming and Directory Conventions for SBOMs (Software Bill of Materials) in Open Source Projects. February 6, 2024.

[12] CISA SBOM Tooling and Implementation Community Working Group. Types of Software Bill of Materials (SBOM). April 21, 2023.

[13] This can be done using continuous integration: Wikipedia. Continuous Integration. February 11, 2024.

[14] GitHub. OSSF SBOM Everywhere SIG: Best Practices for Naming and Directory Conventions for SBOMs (Software Bill of Materials) in Open Source Projects. February 6, 2024.

[15] GitHub. OSSF Security Insights: Specification. October 2, 2023.

[16] GitHub. OSSF Security Insights: Specification. October 2, 2023.

● Consistent naming and storage location allows automated discoverability for the Distributor and Consumer ● SBOMs are machine discoverable because of consistent naming and storage location	version configuration management tool ● Some open-source ecosystems have established their own SBOM naming and storage location standards

Examples of tools to help detect new open source software releases are:

- Renovate[17]
- Dependabot[18]

Discovery Sophistication: Medium

Justification: The naming conventions and known storing locations allow for automated propagation of available SBOMs. SBOM Consumers may also receive continuous updates if they choose to use automated dependency update tooling. Since mapping from an open source package to source repository is available for a portion of open source packages, the discovery sophistication is Medium. If an SBOM could be determined for all open source packages this would be elevated to High sophistication.

Access Sophistication: Low

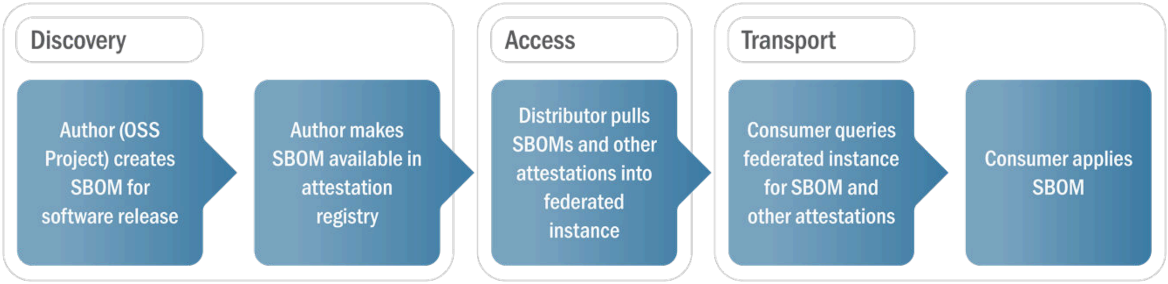
Justification: There are no access controls in place; anyone who discovers an SBOM is able to access it.

Transport Sophistication: Medium

Justification: SBOM Consumers may manually or automatically download SBOMs that have been published on a website or registry by SBOM Authors. While the basic transport process is human initiated, the process, established in the guidance, will be documented and repeatable. Additionally, SBOM Consumers can use the automated dependency update tooling which may allow the Consumers to collect SBOMs “at scale.” Medium sophistication was chosen because the transport mechanism is pull based instead of push based. A pull based transport mechanism introduces a delay in receiving updated SBOMs and requires more infrastructure to implement periodic pulling from upstream sources of information. A selection of High sophistication may be appropriate when using a push based transport mechanism as seen in the “SBOMs for OSS Share via Platform” example.

[17] Renovate Bot. Renovate Docs.
[18] GitHub. Code Security: Keeping Your Supply Chain Secure with Dependabot.

Example 5: SBOMs for OSS Shared via Platform


Discovery
Author (OSS Project) creates SBOM for software release
Author makes SBOM available in attestation registry
Access
Distributor pulls SBOMs and other attestations into federated instance
Transport
Consumer queries federated instance for SBOM and other attestations
Consumer applies SBOM

Several open source projects[19] are working on services to allow federated sharing of SBOMs and other attestation types which permit querying and searching multiple data sources for analysis of the SBOM components. While these attestation registries show great promise, they are not widely adopted and are relatively immature.

In this example, an SBOM Author creates an SBOM and uploads it to an attestation registry. The SBOM has unique identifiers like package URLs[20] and Secure Hash Algorithms (SHAs).

SBOM Distributors manage the federated services, which allow connections between centralized and organization-specific deployments of attestation registries. Federation allows organization-specific deployments to pull data from centralized or supplier instances while partitioning sensitive data.

The biggest advantage of attestation registries is not needing to know “where” to look for SBOMs. SBOM Consumers are able to use unique identifiers to query the attestation registry to find an SBOM and any other attestations like Supply-chain Levels for Software Artifacts (SLSA) Provenance.[21] The attestation registry can also hold data for risk management like Vulnerability Exploitability eXchange (VEX) documents. Both package URLs and SHAs can be computed and do not require mapping to a source code repository or website. These identifiers also correlate to data sources and other components in other SBOMs, which allows for complex analysis like listing all applications with components of a Common Vulnerability Scoring System (CVSS) score above 5.

Benefits	Cautions
● No mappings between product and source code or website are required	● Immature and not widely adopted ● Requires deep technical

[19] Examples include Archivista; DBOM; GUAC
[20] GitHub. package-url: purl spec.
[21] SLSA

- Complex querying across multiple data sources	knowledge

Discovery Sophistication: High

Justification: The federated service is easily searchable if a software identifier is known. Standards like package URL or SHA can be determined from a software package. This is determined to be a High sophistication since it is universal across all open source ecosystems.

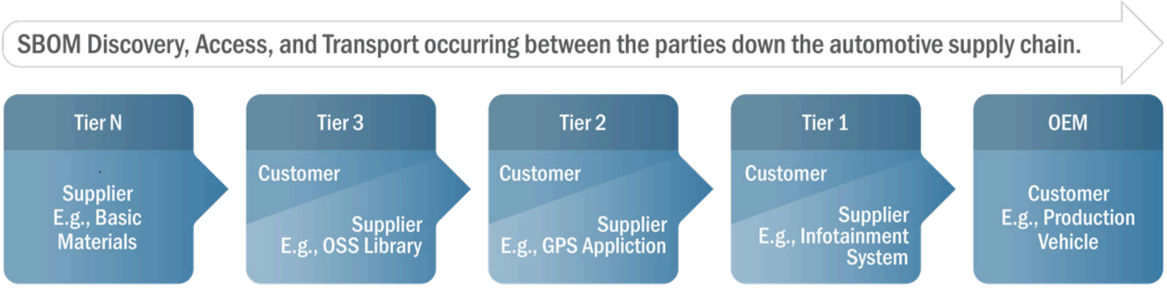
Access Sophistication: Medium

Justification: Federated sharing gives the Author or Distributor access controls once the data has been placed in the attestation registry. This access can be built into the attestation registry or through network segregation. This sophistication is Medium since access control is not consistently implemented across all platforms.

Transport Sophistication: High

Justification: The SBOM Consumer in this example normally receives up to date SBOMs through federated sharing. Unlike the “SBOM for Open Source Software Sharing via Tooling” example which assumes a pull transport mechanism, this example assumes federated services can operate on a push mechanism to share updates resulting in a High sophistication.

Example 6: SBOMs for Proprietary Software Shared Along Supply Chain



A traditional automotive industry manufacturing supply chain is a useful example to demonstrate the role of an SBOM Distributor in the context of proprietary software. Automotive supply chains are broadly similar to those of many industries but have some specific terminology and practices.

As in many industries, the automotive supply chain consists of layers of suppliers that provide a range of products from basic raw materials (e.g., steel, copper, and plastics) all the way up to sophisticated sub-assemblies (e.g., transmissions, suspension, infotainment systems) that may incorporate software components. Almost all suppliers are also consumers in the supply chain.

Tier N suppliers provide raw or basic materials and components, and represent the beginning of the supply chain.[22] Tier 3 suppliers process Tier N materials into more specific but still elemental components.[23] Tier 2 suppliers take those components and materials to manufacture more complex parts or systems, and thus require a combination of componentry from upstream suppliers. Tier 1 suppliers sell ready-for-installation products[24] directly to the automaker, commonly known as the Original Equipment Manufacturer (OEM). As the ultimate downstream supply chain participant, OEMs assemble the complete and final production vehicle, and are the final step in the supply chain.

While SBOM operations in the automotive industry are still in early stages of adoption, many automotive companies are moving toward a consensus that SBOMs will become one of the many security and design documents that are routinely exchanged by supply chain participants. Under this scenario, a request by an automaker for an SBOM from its suppliers may augment existing contractual obligations for documentation and would be included in standard information exchange agreements (e.g., non-disclosure agreement, cybersecurity interface agreement, development interface agreement).

In the example, as demonstrated by the graphic above, a Tier 3 supplier has produced an OSS library which the Tier 2 supplier has consumed, in part, to create its GPS application product. The Tier 2 automotive parts supplier has, according to contract, generated an SBOM internally, and then provided the SBOM to its downstream customer, the Tier 1 supplier, along with the GPS application product. At this stage of the supply chain, the Tier 2 supplier has acted as an SBOM Author. The Tier 1 supplier uses components, including those from the Tier 2 GPS application supplier, to produce the ready-for-installation infotainment system that it sells to the OEM. The Tier 1 supplier generates its own SBOMs for software it has produced and then bundles the upstream Tier 2 suppliers' SBOMs and its own together to make them available to OEM automakers, thereby acting as both SBOM Distributor and Author[25]. Ultimately, the OEM also acts as an SBOM Consumer.

[22] Tier N suppliers may serve various industries. The variable N could be any number representing the furthest upstream suppliers.

[23] Tier 3 suppliers operate relatively upstream in the supply chain, yet are more specialized than Tier N suppliers.

[24] Tier 1 suppliers assemble final components from Tier 2 suppliers into complete systems and parts, e.g., Dashboards or Infotainment Systems.

[25] While the compounding of SBOMs raises the question of verifying SBOM data along the supply chain, SBOM quality is outside the scope of this document.

In typical automotive industry information exchanges between suppliers and customers, the upstream supplier uploads the SBOMs to the downstream Tier 1 supplier or OEM's portal or secure document exchange. Each SBOM portal or secure document exchange is unique to the supplied part. Ultimately, the OEM automaker would be able to access SBOMs for its parts without requesting access from the upstream Tier 1 or 2 parts suppliers by using the documents the Tier 1 supplier has uploaded.

Benefits	Cautions
● Leverages existing supply chain documentation channels ● High degree of control over access ● SBOM Consumer does not have to request SBOM as it may be provided automatically by the upstream supplier(s) as part of development and post-production agreements	● Duplication of effort due to differing requirements for each OEM ● Due to confidentiality, legal, or compliance concerns, software documents including SBOMs for proprietary components are unlikely to be made publicly available

Discovery Sophistication: Medium

Justification: There is no automated discovery in the auto industry approach described above. Discovery of SBOM documents could be completed upon receipt of the deliverables included as part of the downstream suppliers/OEM's contractual requirements. A supplier typically updates the document inventory by using the downstream Tier 1 supplier/OEM portal or secure document exchange, and SBOM exchange will likely fit into that existing workflow.

Access Sophistication: High

Justification: As the upstream supplier shares the SBOM to the portal or secure document exchange, it has effectively delegated authentication and full access controls to the OEM. However, contracts govern confidentiality and access for all automotive intellectual property, including SBOMs.

Transport Sophistication: Medium

Justification: The methods of automotive industry document exchange are well known. Adding SBOMs to this practice will leverage this existing process. Suppliers will likely use a portal or secure document exchange to transport its SBOMs but may vary based on the relationship between parties. While transport in this instance is not automated, it is a highly repeatable, human-initiated process.

Conclusion

This paper has provided an overview of current methods for sharing SBOMs between different actors in the software supply chain. The examples demonstrate that SBOM sharing is already occurring today using a variety of mechanisms that range in sophistication. As the paper indicates, there are trade-offs associated with different sharing approaches. More manual methods allow for greater control over access but lack scalability. Automated sharing supports discoverability and transport at scale but may require more sophisticated access controls. Ultimately, choosing the appropriate SBOM sharing mechanism will depend on factors like software licensing, industry practices, organizational priorities, target consumers, and risk tolerance.

As SBOM adoption expands, new sharing models will emerge, especially those that leverage automation and standards. For example, discussion has emerged around moving toward including SBOMs in end user licensing agreements for SBOM management and sharing. Key areas for continued community collaboration include consistency in SBOM formats, identifiers, and storage locations as well as transport protocols and federated services. Maturation of SBOM sharing practices will be crucial to realizing the full benefits of software transparency across the entire software supply chain. As previously stated, this is only the first iteration of the paper. The authors intend for this paper to be regularly updated with new methods of SBOM sharing as they begin to be used by stakeholders. Maintaining a list of SBOM sharing methods being used will serve, over time, to chronicle the progress of SBOM sharing as the practice becomes more commonplace and mature.

Contributors

Allan Friedman, CISA
Aruneesh Salhotra, SNM Consulting Inc
Ayesha Kirk, GSA
Bunny Hernández Banowsky, SHE BASH
Charles Hart, Hitachi America, Ltd.
Chris Blask, Cybeats
Chris Gregoire, Boston Scientific
Curtis Yanko, CodeSecure Inc
Daniel John Audette, Hewlett Packard Enterprise
Deanna Medina, Honeywell
Ian Dunbar-Hall, Lockheed Martin Corporation
Isaac Hepworth, Google
Jeremiah Stoddard, INL
John Cavanaugh, Internet Infrastructure Services Corp
Joyabrata Ghosh, CARIAD SE
Nicholas Vidovich, Finite State
Przemysław Roguski, Red Hat
Ricardo Reyes, Tidelift
Scott Van Eps, Danaher
Victoria Ontiveros, CISA

References

SBOM Sharing Lifecycle Report
SBOM Sharing Roles and Considerations
OpenSSF's Best Practices for Naming and Directory

Additional documents offering analysis and guidance on additional SBOM-related topics including SBOM generation, quality, and general questions, can be found at cisa.gov/sbom.