SBOM Sharing Roles and Considerations

Introduction

As Software Bill of Materials (SBOMs) become a more important part of the software supply chain world, a gap has been identified: how will SBOM data be shared across organizations along modern supply chains?[1] Building on the SBOM Sharing Lifecycle Report,[2] this document defines the three roles (SBOM Author, SBOM Consumer, and SBOM Distributor) of the SBOM sharing lifecycle and the factors they should keep in mind or be aware of when engaging in the three phases of the sharing lifecycle (discovery, access, and transport).

When SBOM was initially being considered for adoption by the software community as a means of furthering software transparency and supporting risk management, work to mature SBOM focused on generating SBOMs. The National Telecommunications and Information Administration (NTIA) multistakeholder process published cornerstone documents that clarified the role and benefits of SBOM in an organization's software security and risk management practices and furthered the understanding, practicality, and usability of SBOM.[3] The Cybersecurity and Infrastructure Security Agency (CISA)'s community-driven SBOM working groups have continued this work. This document establishes a foundation for discussion of another aspect of SBOMs, SBOM sharing mechanisms.

This document describes the three SBOM sharing lifecycle phases from the perspectives of the three roles, outlining the considerations, shared or unique, of each role as they engage across the SBOM sharing lifecycle document. The scope of this document is limited to SBOM sharing and therefore assumes that an SBOM has been created, without commenting on whether it was created by the software producer or by another party. Furthermore, this document, importantly, does not discuss the creation of an SBOM or the quality, quantity, accuracy, pedigree, or type of SBOM.[4]

---

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

[2] CISA and U.S. Department of Energy. Software Sharing Lifecycle Report. April 17, 2023.

[3] NTIA. Software Bill of Materials.

[4] For information on these topics see: CISA Open Working Group on SBOM Tooling & Implementation Types of Software Bills of Materials (SBOM); NTIA Software Transparency Healthcare POC. How-To Guide for SBOM Generation. 2021.

Definitions

This document borrows the following SBOM sharing role definitions from the SBOM Sharing Lifecycle Report:

SBOM Author: Creates an SBOM.

This document assumes that each SBOM created is available for sharing.

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

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.

SBOM Distributor: Receives SBOMs for the purpose of sharing them with SBOM Consumers or other Distributors.

The SBOM sharing lifecycle phases are borrowed from the SBOM Sharing Lifecycle Report.

- **Discovery**: Mechanism used by the consumer to know the SBOM exists and how to access it.
- **Access:** Access control mechanisms used by the author or provider to regulate who can view or use an SBOM.
- **Transport**: Mechanism provided by the author or [distributor][5] to transfer an SBOM. Also, the action of the consumer receiving an SBOM.

On Roles in the SBOM Sharing Lifecycle

Stakeholders take on one or more of these roles (i.e., Author, Consumer, Distributor) as they engage in SBOM sharing. The delineation of these roles serves to simplify the SBOM sharing process for the purposes of discussion. Critically, organizations engaging in the SBOM sharing lifecycle can operate multi-hatted, i.e., an organization can simultaneously act as any combination of SBOM Author, SBOM Distributor, and SBOM Consumer.

It is important to note that SBOM Author, SBOM Consumer, and SBOM Distributor do not directly align with the software producer, software consumer, and software distributor. These roles are intentionally different from SBOM roles used in documents that discuss other SBOM processes, such as generating an SBOM or ingesting SBOM data.[6]

[5] This document uses Distributor in place of Provider.
[6] See NTIA Open Working Group on SBOM Use Cases and State of Practice. Roles and Benefits for SBOM Across the Supply Chain. November 8, 2019.

For example, while some software producers may also generate SBOMs, other software producers may outsource SBOM generation to a third party, making the third party the SBOM Author.

This document does not use the role of SBOM Provider. The SBOM Sharing Lifecycle Report defines the Provider as “possess[ing] an SBOM.” In this document, the role of Provider is encapsulated in both the SBOM Author and SBOM Distributor. The SBOM Author creates an SBOM and in doing so, makes it available for sharing. The SBOM Distributor obtains and possesses SBOMs for the purpose of sharing them with other actors.

SBOM Sharing Lifecycle Phases and Considerations

This paper discusses the three phases of the SBOM sharing lifecycle (Discovery, Access, Transport) from the perspectives of the three SBOM sharing roles (SBOM Author, SBOM Consumer, SBOM Distributor). The considerations outlined below are not intended to be an exhaustive list, nor are they requirements for every organization to take into account as they engage in SBOM sharing. Rather, the considerations are offered as factors that contribute to an actor’s decision-making process as they progress through the SBOM sharing lifecycle and make decisions about SBOM sharing methods.

Discovery

In the Discovery phase, the SBOM Consumer learns that an SBOM exists and identifies how to access it. The SBOM Author or Distributor can support SBOM discovery by placing the SBOM in a known location. The discovery may be automated or may require the SBOM Consumer to initiate a request for an SBOM from the SBOM Author or Distributor.

The **SBOM Author** has, prior to the Discovery phase, generated an SBOM. In making the SBOM discoverable, the SBOM Author considers the following:

(1) Legal concerns such as licensing, non-disclosure agreements, and who is entitled to the discovery data[7]
(2) Associating the SBOM with the appropriate software component and version
(3) Identifying their role as SBOM Author is clearly identifiable from the SBOM
(4) Placing a tagging mechanism to make the SBOM searchable and discoverable among other artifacts
(5) Who has control over and who is able to discover their SBOM

[7] Discovery information is **not** typically the SBOM itself, and thus may require looser confidentiality and authorization requirements.

The **SBOM Distributor** supports the SBOM Consumer in discovering an SBOM and the SBOM Author in making their SBOMs discoverable. In the discovery phase, the SBOM Distributor considers the following:

(1) The SBOM Author's guidelines for the discoverability of their SBOM(s)
(2) Requests from SBOM Consumers
(3) Identifying multiple SBOMs and SBOM Authors for the same software component or package
(4) Relevant legal concerns e.g., industry-specific requirements, consumer-specific legal concerns
(5) Self-identification as SBOM Distributor in the SBOM sharing process (rather than SBOM Author)
(6) Communication of expectations for distribution services to SBOM Authors and Consumers
(7) Security of SBOM storage
(8) Searchability of SBOMs within SBOM Distributor's system

The **SBOM Consumer** is looking for the SBOM for the software component they are operating or interested in acquiring. As they are searching for the SBOM they are interested in, the SBOM Consumer considers the following:

(1) Any applicable legal concerns, including those relevant to sensitive software source or destination and controlled components
(2) Requirements imposed by SBOM Authors or Distributors for receiving SBOMs
(3) Verification of SBOM Author identity
(4) Validation of SBOM integrity
(5) Matching the SBOM to the software component and version (via metadata or naming convention)
(6) Ability for changes or updates to SBOMs
(7) Notification of new SBOM release or updates (not due to software changes)

Access

In the Access phase, an SBOM Consumer gains authorization to continue to the transport phase. Access controls may be placed on the SBOM to limit access to the SBOM, depending on the SBOM Author's preferences. SBOMs may also require specific access control granularity to restrict an SBOM Consumer or Distributor's access to a specific version of the SBOM associated with a product or to specific information.

In the Access phase, the **SBOM Author** is making the SBOM available to SBOM Distributors and Consumers. The identification of data protection objectives is paramount. In determining desired access levels and establishing access controls, the SBOM Author considers:

(1) Legal concerns including relevant regulations and guidance, regarding the disclosure and sharing of information
(2) Verification of SBOM Consumer or Distributor's adherence to Author's preferences and requirements for access, e.g., organization level access, personnel level access
(3) Extension of access permissions based on SBOM "family," including updates, versions, or modifications
(4) Protection objectives regarding SBOM data, e.g., whether the SBOM Distributor or Consumer may further share the SBOM

The **SBOM Distributor** both accesses SBOMs from the SBOM Author or Distributor and determines desired access controls for SBOM Distributors or Consumers accessing SBOMs they possess. In determining the controls in the Access phase, the SBOM Distributor accounts for two sets of considerations: those from whom the SBOM is obtained (SBOM Author or Distributor) *and* those to whom access is granted (SBOM Consumers and Distributors). Because of this dual role, the SBOM Distributor considers:

(1) SBOM Author preferences and requirements for access
(2) Legal concerns, including relevant regulations and guidance, regarding the disclosure and sharing of information
(3) Validating SBOM Consumer and Author identity
(4) Documenting SBOM Consumer and Distributor access to the SBOM data for auditing purposes

The **SBOM Consumer,** after discovering the SBOM they are interested in, is now looking to access the SBOM data. As they seek to access the SBOM data, the SBOM Consumer considers:

(1) Conditions regarding viewing and distributing an SBOM
(2) Compatibility with SBOM format and sharing platforms is essential
(3) Any applicable legal concerns, including those relevant to sensitive software source or destination and controlled components

Transport

In the Transport phase, the SBOM Author or Distributor conveys the SBOM to the SBOM Consumer or Distributor. The transport phase initiates once the SBOM Consumer or Distributor has received access to the SBOM and concludes once the SBOM Consumer or Distributor has received the SBOM and is able to ingest the data. Transport methods vary and can be single point to single point, or a single point to multiple points.

Prior to the transport phase, the **SBOM Author** has internally generated an SBOM, and the SBOM has been discovered and accessed by an SBOM Consumer or Distributor. In transporting the SBOM to the SBOM Consumer or Distributor, the SBOM Author considers the following:

(1) Whether the transportation of the SBOM should be private or public
(2) Chain of custody[8] and integrity documentation
(4) Preservation of the SBOM's integrity throughout the transport process
(5) Maintaining agreed upon level of access (view only, download only)
(6) Verification that the SBOM reaches the correct recipient
(7) Whether the SBOM may be shared beyond the intended SBOM Consumer or Distributor
(8) Ensuring the SBOM arrives in a form usable for the SBOM Consumer or Distributor
(9) Identifying level of desired transparency for transaction history of the SBOM

The SBOM **Distributor** supports the SBOM Consumer in transporting an SBOM and the SBOM Author in making their SBOMs discoverable. In the transport phase, the SBOM Distributor considers the following:

(1) Verification of transport to or from SBOM Consumer or Author
(2) Chain of custody and integrity documentation
(3) Supporting the SBOM Author's requirements
(4) Supporting the SBOM Consumer's requests
(5) Scalability of the SBOM sharing mechanism

The **SBOM Consumer** is looking for the SBOM for the software component it is operating or interested in acquiring. As the Consumer is transporting the SBOM they are interested in, the SBOM Consumer considers the following:

(1) The SBOM data validation
(2) Chain of custody and integrity documentation
(2) Request time frame constraints
(3) File size constraints

Conclusion

The sharing of SBOM data is important today and will be even more important in the future. This document builds on previous work on the SBOM sharing lifecycle by recognizing the roles of SBOM Author and Consumer but also introduces the role of SBOM Distributor. Recognizing the role that an SBOM Distributor has of facilitating and amplifying the sharing of SBOMs broadens and enriches the document's discussion on the different roles' considerations that may affect their decision-making process as they engage in sharing SBOMs. Future work should use this document as a foundation for developing use cases and documenting current practices.

[8] A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. NIST. Glossary: Chain of Custody.

While some sharing solutions exist, more automation and scale are needed to deliver on the vision of efficiency and efficacy found in this document. Innovators, builders, and standardizers are invited to join these efforts to create infrastructure and tools that all stakeholders can use. Data is only good if it is in the hands of the right people.

Contributors

Adrian Diglio, Microsoft
Albert Ingram, GSA
Allan Friedman, CISA
Aruneesh Salhotra, SNM Consulting Inc.
Ayesha Kirk, GSA
Bruce Lowenthal, Oracle
Bunny Banowsky, SHE BASH
Charles Hart, Hitachi America, Ltd.
Charles Kelly, SAP
Charles Long, Arthrex
Chris Blask, Cybeats
Chris Gregoire, Boston Scientific
Curtis Yanko, Codesecure
Dale Gardner, Gartner
Daniel John Audette, HPE
Deanna Medina, Honeywell
Ian Dunbar-Hall, Lockheed Martin
Jeremiah Stoddard, INL
John Cavanaugh, Internet Infrastructure Services Corp.
John Nuckles, ODNI
Joyabrata Ghosh, CARIAD SE
Lynn Westfall, The Modem Lisa
Mehdi Entezari, Unisys Corp
Nicholas Vidovich, Finite State
Nick Mistry, Lineaje
Przemysław Roguski, Red Hat
Ricardo Reyes, Tidelift
Scott Heimann, CWD
Scott Van Eps, Danaher
Stephen Magill, Sonatype
Victoria Ontiveros, CISA
Yotam Perkal, Rezilion

Appendix

Glossary

SBOM Author	Creates an SBOM.
SBOM Consumer	Receives the transferred SBOM. This could include roles such as third parties, authors, integrators, and end users.
SBOM Distributor	Receives SBOMs for the purpose of sharing them with SBOM Consumers or other Distributors
Discovery	Mechanism used by the consumer to know the SBOM exists and how to access it.
Access	Access control mechanisms used by the author or [distributor] to regulate who can view or use an SBOM.
Transport	Mechanism provided by the author or provider to transfer an SBOM. Also, the action of the consumer receiving an SBOM.