

Survey of SBOM Challenges Facing Cyber-Physical Systems

Survey Flow

Standard: Consent (2 Questions)
Block: General Cyber-Physical Questions (2 Questions)
Standard: SBOM Background (3 Questions)
Standard: HBOM Background (4 Questions)
Standard: Likert-scale Questions (7 Questions)
Standard: Open-ended Questions (5 Questions)
Standard: Demographic Questions (11 Questions)

Page Break

Start of Block: Consent

CF1 Investigating the state of practice in software supply chain management RESEARCH GOAL AND PROCEDURE

The purpose of this study is to investigate issues, needs, and opportunities related to software supply chain management. The software supply chain is the set of processes, components, and tools used to develop, build, and publish a software product (a system, library, tool, etc.).

Software supply chains can extend to and intersect with other kinds of supply chains, including **hardware supply chains**. As **cyber-physical systems** lie at the intersection of computation and other physical components, they represent a unique space to design techniques to improve supply chain management, ensure regulatory compliance, and safeguard supply chain security.

If you decide to participate, you will take a brief survey/questionnaire. The survey will last about 10 minutes during which time you will be asked questions regarding your familiarity and experience with several topics related to software supply chains, **including Bills of Materials for both software (SBOMs) and hardware (HBOMs), and supply-chain challenges for cyber-physical systems.**

We may contact you by email to invite you to participate in a follow-up interview.

RISKS AND BENEFITS There are no foreseeable risks for participating in this research. There are no benefits to you as a participant other than to further research in software engineering and the open source software supply chain. **PARTICIPATION** You must be at least 18 years old to participate. Your participation is voluntary, and you may withdraw from the study at any time and for any reason. If you decide not to participate or if you withdraw from the study, there is no penalty or loss of benefits to which you are otherwise entitled. There are no costs to you or any other party. Your decision whether or not to participate will not prejudice your future relations with [Organization]. If you decide to participate, you will be entered into a drawing for a \$50 USD Amazon gift card upon completion of this survey. We will randomly choose respondents and give out 10 gift cards. **CONFIDENTIALITY** The data collected by this study will be confidential, including your responses. Any information obtained in connection with this study that can be identified with you will remain confidential and disclosed only with your permission. You will be assigned a code number to protect your identity and all data will be kept secure. If you give us your permission by signing this document, we plan to disclose the results of the questionnaire in any publication resulting from this study. The disclosed results will not be personally identifiable (if needed, they will be anonymized). The de-identified data could be used for future research without additional consent from participants. The Institutional Review Board (IRB) and [committee] that monitor research on human subjects may inspect study records during internal auditing procedures and are required to keep all information confidential. **CONTACT** This research is being conducted by [Anonymous Author(s)] from [Organization].

Questions regarding the rights of research subjects may be directed to [redacted].

Such committee has reviewed and approved the present research

([protocol]) CONSENT You are welcome to print this page to keep a copy of this form.
Do you consent to participate in this survey?



CF2 YOU ARE MAKING A DECISION WHETHER OR NOT TO PARTICIPATE.

IF YOU WANT TO PARTICIPATE, PLEASE ENTER YOUR NAME IN THE TEXT FIELD BELOW, AND START THE SURVEY.

Please enter your name.

End of Block: Consent

Start of Block: General Cyber-Physical Questions

Q1 What are the challenges that people currently face in the supply chain of cyber-physical systems?

Q3 What is the role of open-source software in cyber-physical systems?

End of Block: General Cyber-Physical Questions

Start of Block: SBOM Background

Q10 Are you familiar with the concept of Software Bills of Material (SBOMs)?

☐ Yes (1)

☐ No (2)

Display This Question:

If Are you familiar with the concept of Software Bills of Material (SBOMs)? = No

Q11 The [NTIA](#) defines a **Software Bill of Materials** (SBOM) as follows:

An SBOM is a formal, machine-readable **inventory of software components and dependencies**, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be.

SBOMs may include **open source or proprietary software** and can be widely available or access-restricted. SBOMs should also include baseline attributes with the ability to uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of a modern development process. For older software, less-automated methods exist.

Q38 **Important note:** for the purposes of this survey, we consider SBOMs to potentially include information regarding software used in embedded systems, devices, and machines (in general, software required by any physical device or component to function). This includes firmware and other types of embedded software.

End of Block: SBOM Background

Start of Block: HBOM Background

Q32 Are you familiar with the concept of a Hardware Bill of Materials (HBOM)?

☐ Yes (1)

☐ No (2)

Display This Question:

If Are you familiar with the concept of a Hardware Bill of Materials (HBOM)? = No

Q40 A **Hardware Bill of Materials** (HBOM) is a formal document that tracks the various hardware components of a system. According to [CycloneDX](#), HBOMs "inventory hardware components for IoT, ICS, and other types of embedded and connected devices." This can include information regarding component suppliers, dependencies, vulnerabilities, and more.

Display This Question:

If Are you familiar with the concept of a Hardware Bill of Materials (HBOM)? = Yes

Q33 Have you ever used HBOMs in a project?

☐ Yes (1)

☐ No (2)

Display This Question:

If Have you ever used HBOMs in a project? = Yes

Q34 Which formats have you used for HBOMs?

☐

SPDX (1)

☐

CycloneDX (2)

☐

SWID (3)

☐

Others (Please specify) (4)

Q39 Indicate your agreement with the following statements.

Q12 SBOMs are a potential solution to problems that people face in the supply chain of cyber-physical systems

- ☐ Strongly disagree (1)
 - ☐ Disagree (2)
 - ☐ Neutral (3)
 - ☐ Agree (4)
 - ☐ Strongly agree (5)
-

Q13 SBOMs can be used to effectively manage open-source components in cyber-physical systems

- ☐ Strongly disagree (1)
 - ☐ Disagree (2)
 - ☐ Neutral (3)
 - ☐ Agree (4)
 - ☐ Strongly agree (5)
-

Q16 Current formats (e.g., SPDX or CycloneDX) convey all the information necessary to create inventories of physical components

- ☐ Strongly disagree (1)
 - ☐ Disagree (2)
 - ☐ Neutral (3)
 - ☐ Agree (4)
 - ☐ Strongly agree (5)
 - ☐ I don't know (6)
-

Q14 For a cyber-physical system, the software and hardware manifests (i.e., inventories) should be separated into an SBOM and a HBOM (Hardware Bill of Materials).

- ☐ Strongly disagree (1)
 - ☐ Disagree (2)
 - ☐ Neutral (3)
 - ☐ Agree (4)
 - ☐ Strongly agree (5)
-

Q17 SBOMs/HBOMs can be effectively used to demonstrate compliance with regulatory requirements and standards in cyber-physical systems.

- ☐ Strongly disagree (1)
 - ☐ Disagree (2)
 - ☐ Neutral (3)
 - ☐ Agree (4)
 - ☐ Strongly agree (5)
-

Q18 Tool support exists for creating and processing SBOMs/HBOMs for cyber-physical systems.

- ☐ Strongly disagree (1)
- ☐ Disagree (2)
- ☐ Neutral (3)
- ☐ Agree (4)
- ☐ Strongly agree (5)

End of Block: Likert-scale Questions

Start of Block: Open-ended Questions

Q35 What are the necessary data fields that an SBOM or HBOM must contain to accurately and sufficiently describe software/hardware components in cyber-physical systems?

Q5 What is the role of SBOMs/HBOMs in ensuring the traceability of components in cyber-physical systems?

Q6 How can the use of SBOMs/HBOMs impact risk assessment in cyber-physical systems?

Q8 How should SBOMs/HBOMs for cyber-physical systems be distributed? Rank by preference (by dragging the options).

- ☐ Stored with trusted third party (1)
 - ☐ Published in associated repositories (2)
 - ☐ Downloadable from project website (3)
 - ☐ Available upon request (4)
 - ☐ Packaged/included with the associated system (5)
 - ☐ Other(s) (6)
-

Q37 (Optional) Do you have anything else you would like to note regarding SBOMs and HBOMs for cyber-physical systems?

End of Block: Open-ended Questions

Start of Block: Demographic Questions



Q1 How many years of experience in software / hardware development do you have?


Q2 How would you describe your primary role in your organization(s)?

Q3 What is your highest level of education?

- ☐ Did not graduate from high school (1)
- ☐ High School (2)
- ☐ Some college (3)
- ☐ Bachelor's Degree (4)
- ☐ Master's Degree (5)
- ☐ Doctoral Degree (6)
- ☐ Other (7) _____



Q4 Which programming languages have you most used in past project(s)?

- ☐ Python (1)
- ☐ Java (2)
- ☐ C / C++ (3)
- ☐ Javascript (4)
- ☐ C# (5)
- ☐ Others (6) _____
- ☐  Not Applicable (7)

Q5 What types of systems have you most developed?

Q7 For which domains (e.g., banking or healthcare) have you developed applications / systems?

Q8 Do you have a background in computer security? Formal (college classes, degree, certification) or informal (self-learning or other training)?

- ☐ Yes, formal (1)
- ☐ Yes, informal (2)
- ☐ No (3)

Q9 Do you have a background in software licensing? Formal (college classes, degree, certification) or informal (self-learning or other training)?

- ☐ Yes, formal (1)
- ☐ Yes, informal (2)
- ☐ No (3)
-

Q10 How often did you release or help release a new major version of an application / software over the past two years?

Please give your best estimate; if you develop more than one software / application, please answer based on the most frequently updated software / application.

- ☐ Never (1)
 - ☐ Annually (2)
 - ☐ Quarterly (3)
 - ☐ Monthly (4)
 - ☐ More frequently (5)
-

Q11 Which country / countries are you and / or your organization based in?

Q41 Please enter your email address. This will be used to contact you for compensation. If we are interested in your responses, we may contact you for a follow-up interview, if you are willing.

End of Block: Demographic Questions
