System & Software Security
Software Bills of Materials

Davide Baggio - s4426428
João Pereira - s4443322
Nuno Pereira - s4443330

October 2024

Contents

We confirm that this report was fully produced by the team members **Davide Baggio, João Pereira and Nuno Pereira** and we are jointly responsible for all content presented in this work. All used sources were attributed properly.

1 Introduction

Software systems, now more than ever, outsource parts of application logic to first- or third-party *dependencies* — pieces of code that are used in conjunction or as a part of the application's business logic but that are not part of the application itself.

Keeping track of dependencies can be an arduous task, which can be more easily managed using software tools and components such as *package managers* that keep track of an application's dependencies and their versions [1], like *npm* or *cargo* [11, 12].

SBOMs (Software Bills of Materials) [2], proposed by the U.S. National Telecommunications and Information Administration (NTIA), are a formal way of describing the software dependencies of an application and the relations between these dependencies. Other metadata can be attached to SBOM entries for a more comprehensive outline of the software components being dependended upon.

Currently, there are 3 SBOM standards used in practice: OWASP CycloneDX [9], Software Product Data eXchange (SPDX) [10] and Software Identification Tagging (SWID) [8]. However, little consensus exists between these 3 standards, making for one of the many challenges against general SBOM adoption [3].

To ensure widespread practice of SBOM, potential challenges and their solutions must be known and categorized beforehand in order to mitigate issues during development that might arise from a lack of understanding of the software components that make up a product. However, since the topic of SBOMs is still relatively new, there is not much research made into the topic that provide for a standardized view of the common practices in place, and thus further work is required.

2 Overview of reviewed papers

To assess the state-of-the-art with respect to SBOMs and their industry-wide use, we conducted a critical review of some examples from the literature, which are enumerated and described below:

Software Bills of Materials Are Required. Are We There Yet? [4] In this paper, written by Zahan et al. and published in the *IEEE Security & Privacy (Volume: 21, Issue: 2, March-April 2023)*, the authors conducted a Grey Literature (GL) review of 200 internet articles, 100 for "challenges to adopt SBOM" and 100 for "benefits to adopt SBOM" in order to assess the biggest upsides and downsides experienced in practice regarding SBOM adoption. Grey literature was chosen as the majority of content regarding SBOMs in practice cannot be found in literature but rather in online articles and blog posts. The authors came up with 5 reported benefits from SBOM adoption and 5 challenges preventing SBOM adoption.

BOMs Away! Inside the Minds of Stakeholders: A Comprehensive Study of Bills of Materials for Software Systems [7] The paper, written by Stalnaker et al. and published in *ICSE '24: Proceedings of the 46th IEEE/ACM International Conference on Software Engineering*, investigates the current state of Software Bills of Materials (SBOMs), which are recognized as vital tools especially after important incidents like the two mentioned ones: SolarWinds breach and Log4J vulnerabilities. The

study identifies 12 major challenges related to SBOM creation and use, such as: insufficient tool support, SBOM maintenance difficulties and standard incompatibilities across different industries (as highlighted by the 138 interviews with stakeholders). The study identifies key SBOM standards (SPDX, CycloneDX, SWID) and emphasizes the need for better tools to facilitate SBOM creation, verification, and maintenance. Furthermore, it proposes 4 actionable solutions to overcome these critical problems and outlines future research directions aimed at maintaining SBOM accuracy over time and dealing with legacy systems.

An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead [3] In this paper, written by Xia et al. and published in the *ICSE '23: Proceedings of the 45th International Conference on Software Engineering*, the authors aimed to understand the state of SBOM usage and adoption in practice, conducting 17 interviews and performing a survey based on the interviews. The authors gathered information about current SBOM practicioners and what these might feel is lacking in the industry regarding SBOM practices. The study is recent, provides a systematic methodology and provides perspectives from the Software Engineering standpoint.

On the Way to SBOMs: Investigating Design Issues and Solutions in Practice [5] This paper, written by Bi et al. and published in the *ACM Transactions on Software Engineering and Methodology, Volume 33, Issue 6*, explores current practical uses and concerns/problems of SBOM in "the wild". The authors gathered data by mining several GitHub repositories and, out of those, discussions pertaining to the topic of SBOM. It was found that, generally, there are 4 phases to the SBOM lifecycle: planning, development, publication and maintenance.

Charting the Path to SBOM Adoption: A Business Stakeholder-Centric Approach [6] The paper, written by Kloeg et al. and published in the *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, analyzes the slow adoption of SBOM in improving transparency and security within software supply chains. The research identifies four key stakeholder groups—system integrators, software vendors, B2B customers, and individual developers, and also examines how their roles affect SBOM adoption. Through interviews with 16 representatives from these groups, the authors analyze the incentives, concerns, and barriers related to SBOM. System integrators and software vendors are more likely to adopt SBOMs, driven by compliance requirements and the potential to improve their reputation and the quality of supplied software. On the other hand, B2B customers and individual developers show less interest because they struggle to see its immediate value and face challenges in resources and complexity. The study reveals that the main obstacles to adoption include a lack of expertise, concerns over the time and effort required to maintain SBOMs, vulnerability misclassification, and financial costs. The research concludes that while SBOMs have significant potential to enhance software security, widespread adoption will require external pressures and better tools to support stakeholders.

3 Metrics defined

To effectively compare the reviewed papers, objective metrics should be used to rank them based on those specific criteria.

Since SBOM is a relatively novel concept, comparing literature on this topic should focus on identifying and highlighting the most common challenges related to its widespread adoption and how those can be mitigated. Another interesting aspect relevant for SBOM adoption is how generalized these problems are, since problems that are too specific to a certain domain only provide value for that domain and cannot be reused in other contexts.

As such, the metrics we have devised for the critical comparison of the papers we reviewed are:

Metrics of Quality

1. **Aims**: are the aims/research questions of the paper clearly defined? This can help guide future work/development on the topic of SBOMs.

2. **Conclusions**: are the conclusions drawn from the study findings valid and do they align with the aims of the paper? Same reasoning as stated above.

Metrics of Quantity

3. **Number of SBOM adoption challenges**: the number of challenges an organization or system integrator must address before realizing value out of the use of SBOMs directly correlates to how eager they might be to adopting SBOMs in their processes. If the benefits don't outweigh the challenges, it is not valuable, and thus not desirable, to put in the effort required to correctly adopt and practice SBOM development.

4. **Number of solutions to standardize SBOM use**: the number of solutions proposed by the paper to standardize SBOM use is a strong indicator of the thought and research the authors have invested in the topic.

Metrics of methodological soundness

5. **Sampling**: is the sampling of participants clearly defined and does it provide a representative sample of the population the paper is studying? This can help generalize the findings to multiple domains and contexts, allowing findings to be reused across the industry and practitioners.

6. **Analysis of study findings**: are the analytic methods clear, systematic and reproducible? This can help guide future research work based on the papers mentioned.

With the exception of quantitative metrics, scores will be given based on a five-point scale, where 1 means the metric is not met at all and 5 means the metric is met perfectly. The quantitative metrics are used to numerically compare the papers.

3.1 Considerations on the defined metrics

Although we believe these metrics to be valid comparison points between the papers discussed, there are some potential issues which could hinder the validity of the comparisons made with them:

- For the **Number of SBOM adoption challenges** metric, one shortcoming of simply counting the challenges presented by each paper is that different authors might group their findings in different ways, so what would be, for example, 1 challenge for one author could become 2 for a different author. The same reasoning applies to the **Number of solutions to standardize SBOM use** metric. We did our best to analyze the papers with as much scrutiny regarding these issues as possible.
- Quantitative metrics might suffer from our bias/misunderstanding of the reviewed papers in the sense that different people might consider different results as a valid unit of measurement, leading to different results of the quantitative metrics. This can be mitigated by having all papers examined thoroughly by everyone and handling any disagreements that might appear.

4 Analysis and Discussion of reviewed papers

With a set of relevant metrics defined for the topic of SBOMs, we analyzed and compared the papers based on these criteria. Our findings are summarized in Table 1.

A value of *N/A* means that the relevant metric is not applicable to the paper in question or that there isn't enough data/evidence that can sustain a scoring on that metric.

4.1 Analysis

Zahan et al. [4]

1. The goals of the study are explained but could be more precise. (4/5)
2. The conclusions mention some of the points brought up throughout the article but there is no single conclusion that is logically drawn from the findings and discussed (2/5)
3. The study authors explicitly report finding 5 challenges against SBOM adoption (5)
4. Even though the paper talks about benefits of adopting SBOM practices, those cannot be considered solutions for common SBOM problems, so this metric is non-applicable to this paper (N/A)
5. The data collection process was clearly stated. However, the data points were gathered from online articles, and not actual participants, so this metric is non-applicable to this paper. (N/A)
6. Even though the analysis method was clearly stated, the fact remains that it is highly subjective to who is collecting and analyzing the data, meaning that the methodology employed is not entirely reproducible. (3/5)

Stalnaker et al. [7]

1. This study's aims are clearly defined through well-articulated research questions, focusing on identifying the current challenges practitioners face in SBOM adoption and usage, as well as exploring solutions to enhance the practicality and reliability of SBOMs. (5/5)

2. The authors provide a clear link between the research questions and the conclusions, making the study's findings valid. However, the range of insights tailored to specific stakeholders is occasionally generalized, resulting in some conclusions being somewhat superficial. (4/5)

3. Complexity of SBOM specifications, determining data fields to include in SBOMs, incompatibility between SBOM standards and keeping SBOMs up to date are some of the challenges presented by the authors. In total, the study's authors outlined 12 challenges against SBOM adoption. (12)

4. Multi-dimensional SBOM specifications, enhanced SBOM tooling and build system support, strategies for SBOM verification and increasing incentives for SBOM adoption are the main solutions found by the authors of this study. However, these don't account for challenges A, J and K, as they require additional research to be addressed effectively, as mentioned in the paper. (4)

5. The authors clearly describe their sampling process, targeting five key groups: SBOM Community and Adopters, Critical Open Source Developers, CPS Developers and Researchers, AI/ML Developers and Researchers, and Legal Practitioners. Of the 4,400 surveys sent, 229 responses were received, with 150 remaining after filtering. Additionally, they conducted eight in-depth interviews, where respondents provided valuable insights into use cases, challenges, and potential solutions, and represented a range of roles. While the sampling approach is robust, the sample size is too limited to generalize findings across the entire industry (4/5).

6. The researchers conducted their studies and designed the questionnaires considering previous literature on SBOMs and guidelines for survey design. Hence, the methodology is well-founded and reproducible. (5/5)

Xia et al. [3]

1. The aims of this study are clearly defined when defining the research questions, and the potential (and effective) contributions of the study reflect this. (5/5)

2. Since the survey data was compared against interview results and conclusions were drawn from analyzing both, we are confident in their validity. The link between research questions and conclusions is logically sound, so this paper scores a 5 on this metric. (5/5)

3. Lack of standard format extensibility, potential for attackers to use SBOMs as an attack "guide" or lack of SBOM education by industry professionals are identified as the 3 main concerns analyzed. (3)

4. The defined 3-goal model outlines steps that the authors believe are crucial to practice if SBOMs are to see more widespread adoption. (3)

5. The study included 82 participants from diverse backgrounds and countries. Most expertise categories have over 10 participants, with some exceptions, such as Researchers. However, each Researcher has at least 10 years of experience in software engineering, making their assessments highly representative (4/5).

6. The data analysis methods used for both the interviews' and online surveys' responses are backed by literature articles, so they are easily reproducible. (5/5)

Bi et al. [5]

1. The aims/research questions of this study are extensively discussed and clarified (5/5)

2. Since conclusions are drawn from the authors' analysis of the collected data and they help answer the defined research questions we can confidently say they are valid and thus this paper scores a 5 on this metric. (5/5).

3. The paper identifies three categories of SBOM issues, with the second and third categories further divided into subcategories, resulting in a total of eight distinct SBOM issues. Notably, issues are reported as percentages, while solutions are presented as measurable counts. Despite these differing metrics, we believe the reviewed papers can still be compared effectively as is. (8)

4. The authors explicitly state that they found "33 high-level solutions for the SBOM-relevant issues and their main design problem". It can be argued whether these are actual solutions or steps towards solutions but we will respect the author's own assessment. (33)

5. Even though the data collection method is clearly outlined, it comes from repository mining, not participant interactions. (N/A)

6. The data collection process is thoroughly explained and the analysis method is backed by literature references based on *Grounded Theory*. (5/5)

Kloeg et al. [6]

1. The aims of this study are very well defined, however the research questions are not explicitly stated in the paper. The researchers only hint at them, mentioning they were based on literature studies. (3/5)

2. The conclusions are sound and logically follow from the data analysis obtained from the interviews. The representation of the results using SWOM matrices is a good way to make the conclusions even more clear. (5/5)

3. The paper identifies the following challenges: lack of knowledge and expertise, limited usefulness, time or effort overheads, vulnerability misclassification, financial costs, imperfect tooling/formats/vulnerability databases, threat to intellectual property. (7)

4. Although the paper discusses some advantages of implementing SBOM practices, it doesn't provide actual solutions to overcome the challenges presented. (N/A)

5. Participants were selected to represent key SBOM stakeholder groups: B2B representatives, system integrators, software vendors, and developers. Recruitment was supported by an international security software provider's network to reach customers, while SBOM developers were contacted via publicly available GitHub emails. Sampling considered SBOM expertise and experience levels, ensuring a balanced range from beginner to expert to gather diverse perspectives on challenges and incentives. Sixteen interviews were conducted (without prior surveys), though the authors noted that a larger sample would enhance result validity (3/5).

6. The methodology is well explained and the data analysis uses the SWOT method, which is a well-known and reliable method to analyze qualitative data. They also provided a concise figure to summarize the methodologies used in the study. (5/5)

Paper	**Quality**		**Quantity**		**Methodology**	
	1	**2**	**3**	**4**	**5**	**6**
Zahan et al. [4]	4	2	5	N/A	N/A	3
Stalnaker et al. [7]	5	4	12	4	4	5
Xia et al. [3]	5	5	3	3	4	5
Bi et al. [5]	5	5	8	33	N/A	5
Kloeg et al. [6]	3	5	7	N/A	3	5

Table 1: Comparison of reviewed papers

4.2 Discussion

Regarding the qualitative metrics, nearly all papers received high scores in terms of quality. The one with the lower score is the paper by Zahan et al. [4] which involved the least "methodological" approach to data collection and analysis, as expressed by this paper's rating on metric 6. Regarding methodology metrics, the story is similar. It is worth noting that 2 papers ([4, 5]) couldn't be evaluated using metric 5 due to the nature of the studies themselves. This is a result of our choice of metrics to evaluate the papers by, which does not consider methodologies that do not depend on actual participants for data collection.

When discussing quantitative metrics, one can see that for metric 3 (*Number of SBOM adoption challenges*) the article by Stalnaker et al. [7] trumps the other 4. The same is achieved for the paper by Bi et al. [5] regarding metric 4 (*Number of solutions to standardize SBOM use*). However, as discussed in Section 4.1, this metric is highly subjective in the sense that different authors group their findings differently: even though Bi et al. described them as "high-level solutions", in our opinion these are more like steps towards solutions which could be likened to the solution sub-groups in that paper; this would greatly reduce the number of solutions into a value more similar to the others. It is worth noting that papers [4] and [6] don't have a meaningful value for this metric because, instead of solutions, they present benefits of SBOM adoption and incentives towards SBOM adoption, respectively.

5 Conclusion

Supply Chain Security is an increasingly important factor of modern Software Development. Ensuring that companies adopt good practices in regards to the code they outsource is a pivotal step in ensuring the security requirements of software products. SBOMs [2] are an example of such a technology that promotes good secure software engineering practices.

In this paper, we analyzed 5 examples of the state-of-the-art with regards to SBOMs and conducted a critical review of these papers according to our own metrics.

Our review indicates that the work done by Zahan et al. in [4] is a good starting point towards higher SBOM expertise, despite being arguably the least-quality article among the five based on our metrics and subjective evaluation. Stalnaker et al. provide in [7] the greatest level of detail regarding common challenges practitioners and organizations might face when attempting to adopt SBOM best practices. When it comes to employing solutions to mitigate those challenges, the work done by Bi et al. in [5] can be a good reference point for the steps needed to solve any problems encountered.

Future work can expand on the methodology and results of this paper by analyzing more articles to provide a broader and more comprehensive look on the state of SBOM-related literature and by coming up with more detailed and precise metrics that expand on or replace the metrics we have devised.

References

[1] Diomidis Spinellis. "Package Management Systems". In: *IEEE Software* 29.2 (2012). [Accessed 21-10-2024], pp. 84–86. DOI: 10.1109/MS.2012.38.

[2] Éamonn Ó Muirí. "Framing software component transparency: Establishing a common software bill of material (SBOM)". In: *NTIA, Nov* 12 (2019). [Accessed 15-10-2024].

[3] Boming Xia et al. "An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead". In: *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*. [Accessed 15-10-2024]. 2023, pp. 2630–2642. DOI: 10.1109/ICSE48619.2023.00219.

[4] Nusrat Zahan et al. "Software Bills of Materials Are Required. Are We There Yet?" In: *IEEE Security & Privacy* 21.2 (2023). [Accessed 15-10-2024], pp. 82–88. DOI: 10.1109/MSEC.2023.3237100.

[5] Tingting Bi et al. "On the Way to SBOMs: Investigating Design Issues and Solutions in Practice". In: *ACM Trans. Softw. Eng. Methodol.* 33.6 (June 2024). [Accessed 15-10-2024]. ISSN: 1049-331X. DOI: 10.1145/3654442. URL: https://doi.org/10.1145/3654442.

[6] Berend Kloeg et al. "Charting the Path to SBOM Adoption: A Business Stakeholder-Centric Approach". In: *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '24. [Accessed 15-10-2024]. Singapore, Singapore: Association for Computing Machinery, 2024, pp. 1770–1783. ISBN: 9798400704826. DOI: 10.1145/3634737.3637659. URL: https://doi.org/10.1145/3634737.3637659.

[7] Trevor Stalnaker et al. "BOMs Away! Inside the Minds of Stakeholders: A Comprehensive Study of Bills of Materials for Software Systems". In: *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. ICSE '24. [Accessed 15-10-2024]. Lisbon, Portugal: Association for Computing Machinery, 2024. ISBN: 9798400702174. DOI: 10.1145/3597503.3623347. URL: https://doi.org/10.1145/3597503.3623347.

[8] National Institute of Standards and Technology (NIST). *Software Identification (SWID) Tagging — CSRC — CSRC — csrc.nist.gov*. https://csrc.nist.gov/projects/Software-Identification-SWID. [Accessed 15-10-2024].

[9] Open Worldwide Application Security Project (OWASP). *OWASP CycloneDX Software Bill of Materials (SBOM) Standard — cyclonedx.org*. https://cyclonedx.org/. [Accessed 15-10-2024].

[10] Linux Foundation. *SPDX Linux Foundation Projects Site — spdx.dev*. https://spdx.dev/. [Accessed 15-10-2024].

[11] NodeJS Team. *NPM: Node Package Manager*. [Accessed 15-10-2024]. URL: https://www.npmjs.com/.

[12] Rust Team. *Cargo*. [Accessed 15-10-2024]. URL: https://doc.rust-lang.org/cargo/.