Activities of the Security Transparency Consortium to Enhance the Effective Use of Visualization Data

Yusuke Kumazaki, Akira Yamada, and Ryota Sato

Abstract

To promote responses to supply chain security risks using visualization data, it is crucial for the various businesses that form the supply chain to collaborate and advance the effective use of visualization data in the collaborative domain. This article introduces the activities of the Security Transparency Consortium, established in September 2023 to promote *co-creation of knowledge* among these diverse businesses and promote the use of visualization data. It also discusses the challenges associated with promoting the use of visualization data.

Keywords: Security Transparency Consortium, visualization data, SBOM

1. The importance of collaboration in expanding the use of visualization data

As the importance of addressing supply chain security risks becomes increasingly recognized, both domestically and internationally, the adoption of visualization data, including a software bill of materials (SBOM), is progressing rapidly. For the widespread use of visualization data, it is essential that not only the producers but also the users within the supply chain collaborate to effectively use these data, making activities within the collaborative domain crucial. Section 2 introduces the activity vision and initiatives of the Security Transparency Consortium as part of the effort within this collaborative domain. Section 3 discusses the challenges faced by the producers in promoting the use of visualization data.

2. Activities of the Security Transparency Consortium

2.1 Activity policy and organizational structure of the consortium

The Security Transparency Consortium was established in September 2023 with the aim of promoting *co-creation of knowledge* among the diverse businesses that form the supply chain, promoting the effective use of visualization data. The consortium operates under the following guiding principles:

- To explore utilization methods across various fields, it targets a diverse range of businesses, including product vendors, system integrators, security vendors, and businesses that use or operate products, systems, and services.
- To ensure activities are based on mutual trust among businesses, new members are reviewed by a steering committee selected by the participating members.
- To facilitate participation, membership fees are not required or are kept minimal.
- The consortium does not handle intellectual

Table 1. Challenges faced by users.

(1) Lack of social penetration and awareness Due to a lack of understanding of the concrete value of visualization data, users are unsure of how to effectively use them, among other issues.	(5) Continuous utilization It is necessary to continuously obtain accurate visualization data when updating software, among other issues.
(2) Lack of standardized formats and data To handle visualization data uniformly, it is necessary for the users to establish clear guidelines for their application, among other issues.	(6) Supply chain coordination A system for mutual sharing between the producers and users across the multi-tiered supply chain is needed, among other issues.
(3) Insufficient technology and tools Automation is required to manage the vast amount of visualization data, among other issues.	(7) Impact of visualization data As visualization data increase security transparency, there will be a need to address issues that were previously unseen and unaddressed, among other issues.
(4) Cost inflation Efficient training of personnel and familiarity with related tools are necessary to adapt to the operational changes brought about by the introduction of visualization data, among other issues.	(8) Additional considerations Since the utilization of visualization data is not part of traditional operations, a review of operational structures may be necessary, among other issues.

property and focuses on the collaborative domain of participating businesses.
- Activities do not rely on confidential information from participants but use only the information that can be disclosed by each business.

The consortium operates through a structure consisting of a general assembly, steering committee for operational discussions, and working groups (WGs) dedicated to the co-creation of knowledge. The general assembly, where all member businesses participate, decides on basic policies. For matters, such as the admission of new members, decisions are made by the steering committee to ensure efficient decision-making. The actual co-creation of knowledge activities are carried out by WGs. There is one WG, the "Visualization Data Utilization WG," which meets 1–2 times a month, combining in-person and online formats, fostering active exchanges among members. The outcomes of these activities are openly shared on the consortium's website [1].

Since its inception, the consortium has expanded from 8 to 18 member businesses by July 2024, leading to a broader sharing of knowledge and a strengthened cooperative framework.

2.2 Activity vision for expanding the use of visualization data

To broaden the use of visualization data, it is crucial to accelerate efforts not only by the producers of the data but also by the users. In line with this, the consortium has published an activity vision of the consortium in February 2024 [2]. This vision focuses on addressing the issues and challenges faced by the users of visualization data, in addition to outlining the consortium's activity policy and content.

Visualization data encompass a wide range of information related to the configuration of software and hardware, risks (e.g., vulnerabilities), and states (e.g., actual usage reflected in device settings). The activity vision begins with discussions on the utilization of an SBOM, a representative method of expressing configuration information related to software included in products and systems. The vision then introduces the challenges that the users of visualization data face in ensuring supply chain transparency, with a particular focus on SBOMs.

3. Challenges faced by users of visualization data

There are still many issues to be solved in the use of visualization data. The consortium has summarized the challenges encountered by users in **Table 1**, and we provide a brief overview of each challenge.

As a societal challenge, there is the issue of the social penetration and recognition of visualization data (Challenge 1). Ensuring supply chain security requires not only the efforts of individual companies but also the collaboration of society to expand the use of visualization data across all companies that form the supply chain.

From a technical perspective, Challenges 2 and 3 must be addressed. These include the standardization of data formats and the development of tools and technologies to handle the vast amounts of visualization data. These are essential for promoting the effective use of visualization data.

Challenges 4 through 8 highlight the need for tools

and internal training for the producers to use visualization data effectively as well as agreements and collaborations between the users and producers. There is also a need to review and adapt organizational structures and practices both within and between organizations to fully harness the benefits of visualization data. Each of these challenges is explained in more detail as follows.

Challenge 1: Lack of social penetration and awareness

While the efforts of the producers in creating and providing visualization data are expected to lead to the widespread collection of such data across society, there is still a significant gap in the understanding and recognition of its value, particularly among users. As data collection and sharing progress, the increased availability of visualization information is anticipated to promote its use across various fields. However, awareness of how to use visualization data and its benefits is not sufficiently widespread. Many users still lack a concrete understanding of its specific value and how to use it effectively.

The uneven adoption of visualization data, concentrated within a limited number of companies, undermines its potential effectiveness in ensuring supply chain security. Therefore, it is crucial that the use of visualization data is uniform across all companies within the global supply chain.

It is important to note, however, that the challenge of social penetration cannot be resolved in isolation. The value of visualization data must be enhanced by overcoming the various challenges discussed later. As users begin to experience the tangible benefits of using these data, social penetration and broader adoption are expected to accelerate.

Challenge 2: Lack of standardized formats and data

An SBOM is a standard specification used to represent software composition and is highly valuable as visualization data. However, the existence of various standard specifications for SBOM data formats can lead to inconsistencies in representation. Since an SBOM allows for flexible description of data, the content often depends on the discretion of the creator. This can result in variations in the items included and the methods of description across different products, making it challenging to handle the data uniformly.

Discrepancies can arise in the outputs from various SBOM-generation tools, such as differences in capitalization, text format, and the omission of certain details. These variations in SBOM content can also stem from differences in how users intend to use the data. If industries or client companies start defining and requesting specific information according to their unique needs, multiple SBOMs with differing content could be created for a single product.

These inconsistencies in SBOM content significantly impact the quality of visualization data. In vulnerability management, if the quality of the visualization data used to identify vulnerabilities is not accurately assessed, unnecessary actions may be taken, or critical vulnerabilities may go undetected, leading to significant issues.

Challenge 3: Insufficient technology and tools

To effectively use visualization data, it is essential to collect comprehensive and accurate information from a wide range of businesses. Although various technologies and tools for handling visualization data are already available, the information they provide may not fully meet the needs of users in their specific use cases. This highlights the need for further development of technologies and tools as well as the creation of knowledge to use them effectively.

For widespread adoption of visualization data, it is crucial that affordable and user-friendly technological options are available. This would enable a greater number of businesses to easily integrate and use visualization data in their operations.

Challenge 4: Cost inflation

The cost of generating the necessary visualization data on the producer side is often reflected in the overall cost of providing products or services. Therefore, it is crucial that the tools and systems required for this process be affordable. On the user side, in addition to the cost of tool implementation, there is a need for efficient training of staff to adapt to the changes in operations brought about by the introduction of visualization data. During the initial implementation phase, it is essential to train personnel who can accurately understand and communicate the value of visualization data within the organization, making education costs a significant consideration.

As discussed in the "Challenge 2: Lack of standardized formats and data" section, the possibility of creating multiple different SBOMs for a single product can lead to increased costs for the producers. These additional costs can also impact the users, highlighting the need for cross-industry and cross-company efforts to standardize the required information. This standardization can help reduce the overall

burden of implementation costs on both sides.

Challenge 5: Continuous utilization

After a product is deployed, software updates are frequently executed, which can result in discrepancies if the visualization data obtained at the time of procurement no longer align with the current state of the product, system, or service. Such inconsistencies can lead to security management issues. Therefore, users need to ensure the continuous accuracy and relevance of the visualization data.

For those who are already managing vulnerabilities, it may be necessary to establish a smooth transition from their current vulnerability management practices to one that fully integrates the use of visualization data.

When users customize the products, the visualization data might also need updates to reflect these changes. In such cases, it is crucial to establish clear guidelines on the responsibility for maintaining the accuracy of the visualization data, ensuring that the entire product remains consistent and secure.

Challenge 6: Supply chain coordination

Information about the components of a product, including the SBOM, is often confidential to the product vendor. Therefore, such information should be disclosed only to specific parties, with appropriate security measures in place. If data are inadvertently leaked, they can be exploited for cyber attacks, so strict control is required.

Users are required to clarify the range of visualization data they expect to use. On top of that, consensus building in the supply chain is necessary to obtain the necessary visualization data. The supply chain for products, systems, and services is generally multistage, requiring cross-organizational cooperation between the producers and users of visual data through the supply chain. When software is procured based on a contract, it is possible to include the items for consensus building regarding visualization data in the contract.

In the supply chain, as well as inquiries and responses regarding product defects, it is also necessary to have a method for confirming the accuracy of visualization data and request corrections.

Challenge 7: Impact of visualization data

As visualization data become more widespread and enhance security transparency, it may require organizations to address issues that were previously unnoticed or unaddressed. While cross-referencing visualization data with vulnerability databases allows for efficient and comprehensive automated checks for known vulnerabilities, it also raises the possibility of detecting a large number of vulnerabilities. This could overwhelm the existing vulnerability management capabilities, necessitating the development of strategies to handle this influx effectively. Given the numerous vulnerability databases available, it is crucial to understand the characteristics of each and carefully select the most relevant ones for cross-referencing before proceeding.

The integration of visualization data may lead to a reassessment of existing security practices. In managing product vulnerabilities using SBOMs and external vulnerability databases, for instance, the matching process may reveal vulnerabilities that pose no actual threat based on how the components are used within the product. In such cases, combining SBOM data with VEX (Vulnerability Exploitability eXchange) can help streamline vulnerability management by providing context about the impact of each vulnerability on the specific product, improving operational efficiency.

Challenge 8: Additional considerations

The utilization of visualization data requires a reevaluation of existing workflows, as it introduces tasks not traditionally included in standard operations, relies on automation through various tools, and necessitates ongoing data updates. While security measures are typically managed by the information technology department, it is crucial not to overly burden them. Instead, a company-wide reassessment of operations is necessary to effectively integrate visualization data into security practices.

For the producers, it is also important to ensure that visualization data align with industry-specific regulations and supply chain models. While it is theoretically possible to generate comprehensive visualization data for every aspect of a product, in practice, the complexity of multi-tiered supply chains may require decisions about how deep into the supply chain data should be generated for each product. For products where the entire configuration or parts of it are not publicly disclosed, special consideration must be given to how these data are handled.

4. Conclusion

We have introduced the collaborative efforts and challenges within the domain of addressing supply chain security risks. Participants of the consortium

are actively sharing their operational insights and engaging in vigorous discussions within WGs to tackle these challenges and publish relevant knowledge and use cases. Through these discussions, new issues, such as the limitations of the current SBOM formats, have begun to surface—issues that were previously unnoticed. These insights will be continuously shared on the consortium's website.

To enhance supply chain security risk management across the industry, the consortium will continue to widely disseminate knowledge from a variety of perspectives, contributed by diverse businesses. Through these ongoing activities, we aim to foster a more secure and resilient supply chain.

References

[1] Website of Security Transparency Consortium, https://www.st-consortium.org/?lang=en
[2] Press release issued by NTT, "Security Transparency Consortium Announces Activity Vision for Improving and Utilizing Security Transparency - Promoting comprehensive cybersecurity capabilities in the supply chain using SBOMs -," Feb. 16, 2024. https://group.ntt/en/newsrelease/2024/02/16/240216b.html

Yusuke Kumazaki
Director, Research and Development Planning Department, NTT Corporation*.
He joined NTT WEST in 1999. He was with NTT Corporation, where he was responsible for resource management and support for NTT's research and development, including security.
*He is currently with NTT WEST.

Akira Yamada
Director, Research and Development Planning Department, NTT Corporation.
He joined NTT DOCOMO in 2000, and engaged in the wireless LAN system development, 3G/LTE RAN development, standardization activities at the 3rd Generation Partnership Project (3GPP), Institute of Electrical and Electronics Engineers (IEEE) 802, and Association of Radio Industries and Businesses (ARIB), and service development with big data analysis. Since joining NTT Corporation in 2023, he has been responsible for resource management and support for NTT's research and development.
He received the Institute of Electronics, Information and Communication Engineers (IEICE) Young Researcher's Award in 2005 and the Information Processing Society of Japan (IPSJ) Industrial Achievement Award in 2023.

Ryota Sato
Senior Research Engineer, Supervisor, Social Innovation Research Project, NTT Social Informatics Laboratories.
He joined NTT in 2004. He has been involved in research and development of information and communication platforms, security platforms, and other areas. He received the FIT (Forum on Information Technology) Paper Award in 2011. He has Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP), and Registered Information Security Specialist (RISS) qualifications.