BomBot: A LLM-based AI Agent Assistant for SBOM Visualization, Understanding and Vulnerability Identification

Xinyao Ma, Ankith Veldandi, Zitao Victor Zhang, Peter Caven, Ambarish Gurjar, L. Jean Camp
Luddy School of Informatic, Computing and Engineering, Indiana University

Introduction

- **Software Bill of Materials (SBOM):** a nested inventory for software, a list of ingredients that make up software components.
- **SBOM Visualizations** are designed to translate the data into actionable decisions. We evaluated two visualizations for usability, acceptability, and accuracy
- **BomBot:** LLM-based AI assistant for developers of all levels to leverage SBOMs

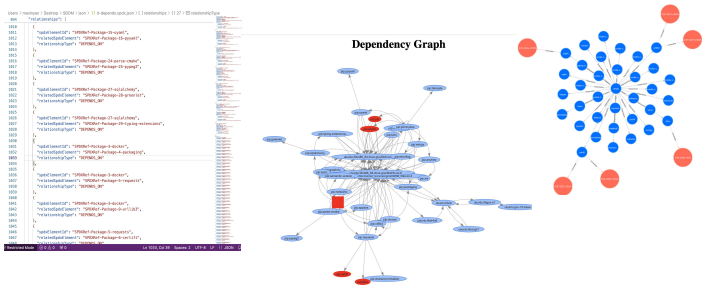


Fig.1 Comparison of a SBOM file in text (JSON), ItDepends, and and DeepBits formats

Motivation: SBOM Visualization Efficacy

- **Visualization Tools**:
  - **It-Depends** and **DeepBits** make it feasible to use SBOM data to identify vulnerabilities and the corresponding mitigations.
  - SBOM data maps dependencies, highlights vulnerabilities, and provides real-time CVE updates.

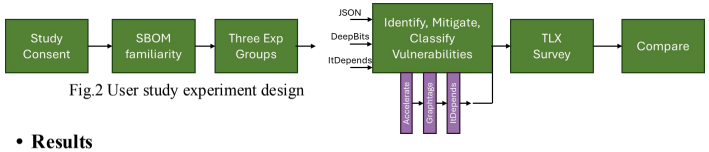


Fig.2 User study experiment design

- **Results**
  - Visualizations were useful in assisting developers in identifying vulnerabilities and mitigations.
  - The task was still perceived as burdensome, even for small packages
  - Likely infeasible when graphs contain thousands of nodes
  - Risk were underestimated even when SBOM data are visualized

Item	Options	n
Gender	Male	51
	Female	16
	Prefer not to answer	45
Age	18-24	34
	25-34	16
	35-44	9
	45-54	5
	55-64	5
	Prefer not to answer	43
SBOM Familiarity	Never heard of it	27
	Have heard of it	34
	Familiar	20
	Knowledgeable	15
	Very knowledgeable	16

Fig.3 Participant Summary

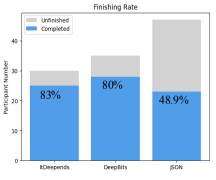


Fig.4 Acceptability Results

Fig.5 Accuracy Results

BomBot Conversation Example

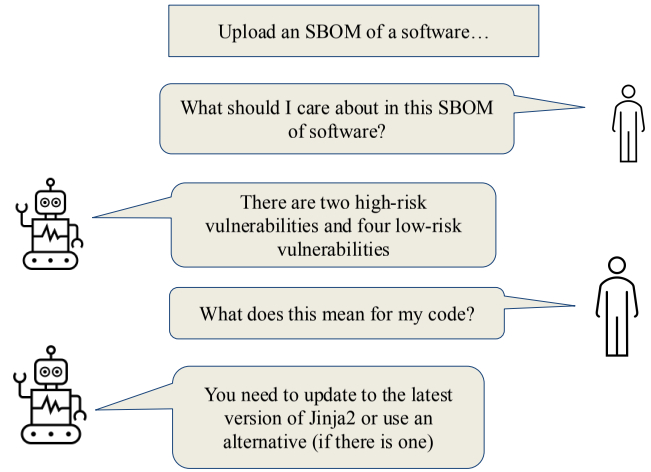


Fig.6 All steps are automated except mitigation information. Mitigation information is verified by researchers. Prompts are automated and invisible to users.

Motivation: SBOM Visualization Usability

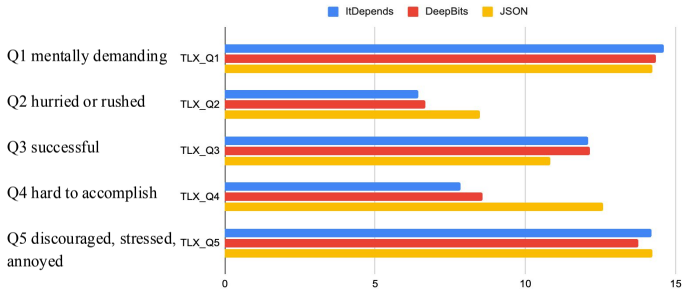


Fig. 7. Usability as Measured by the NASA Task Load Index

Implications

Visualizations are significantly helpful. However, they had limited efficacy even with relatively small graphs.

This motivated us to develop BomBot, a interactive chat system to process accurate SBOM data

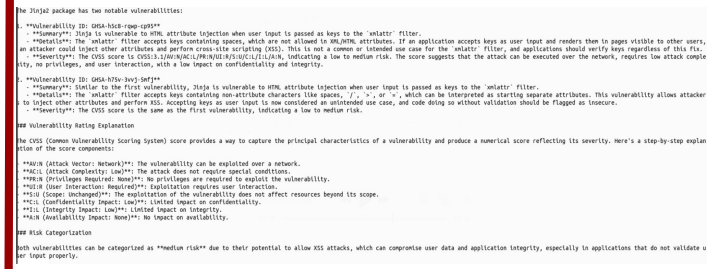
Current Functions

A RAG Bot to answer question about SBOMs of known software:

- generate visual graph via .json
- connect with OSV database
- identify known vulnerabilities and risk level

Output for question:

In this SBOM, what are the vulnerabilities in the Jinja2 package? Also, categorise it in between low, medium and high risk level.



Conclusions & Limitations

Conclusions

- Visualizations help but are not adequate. Visualizations can differ significantly in efficacy even when they are equally usable. One risk of both SBOM and the associated visualizations is that people may be unduly confident that they have a full understanding of their attack space, when in fact they are underestimating the risks.
- A chatbot offers an interactive method that can address concerns and answer questions regardless of scale. A chatbot can rank and integrate information.

Limitations

- There are multiple visualizations for the SBOM. Our work tested only two options. Innovative or next iteration of visualization will improve.
- Text requires more attention and may interrupt programming while a visualization can provide continuous if passive feedback.
- Our sample was recruited primarily from University computer science students and using Prolific for people with computing backgrounds. There were fewer than 20 industry participants, these were not significantly different. Repeating the experiment with a private sector software engineering team may yield different results.

Future Work

- Allow users to upload new, updated SBOMs after making changes and bot will compare the new with the original, analyze the changes, and provide feedback.
- Evaluate expansions to improve acceptability, e.g. automate compliance verification
- Collaborate with GUAC team from Google for future visualization evaluation and API for chatbot.
- We are just beginning to understand how to merge risk communication with SBOMs.

Acknowledgment: *This work was funded by the U.S. Department of Homeland Security under Grant (Award # 17STQAC00001-07-00), US Department of Defense (Contract W52P1J2093009) and funding from CTIA. The views and conclusions contained in this poster are those of the authors and should not be interpreted as representing the official policy or opinions expressed or implied by any funder.*