Risk Explorer for Software Supply Chains

Understanding the Attack Surface of Open-Source based Software Development

Piergiorgio Ladisa
SAP Security Research
Mougins, France
University of Rennes 1/INRIA/IRISA
Rennes, France
piergiorgio.ladisa@sap.com
piergiorgio.ladisa@irisa.fr

Henrik Plate
SAP Security Research
Mougins, France
henrik.plate@sap.com

Matias Martinez
Université Polytechnique
Hauts-de-France
Valenciennes, France
matias.martinez@uphf.fr

Olivier Barais
University of Rennes 1/INRIA/IRISA
Rennes, France
olivier.barais@irisa.fr

Serena Elisa Ponta
SAP Security Research
Mougins, France
serena.ponta@sap.com

ABSTRACT

Supply chain attacks on open-source projects aim at injecting and spreading malicious code such that it is executed by direct and indirect downstream users. Recent work systematized the knowledge about such attacks and proposed a taxonomy in the form of an attack tree.

We propose a visualization tool called *Risk Explorer for Software Supply Chains*, which allows inspecting the taxonomy of attack vectors, their descriptions, references to real-world incidents and other literature, as well as information about associated safeguards.

Being open-source itself, the community can easily reference new attacks, accommodate for entirely new attack vectors or reflect the development of new safeguards.

CCS CONCEPTS

• **Security and privacy → Software security engineering**.

KEYWORDS

Open-Source Security, Supply Chain Attacks, Malware Detection

ACM Reference Format:
Piergiorgio Ladisa, Henrik Plate, Matias Martinez, Olivier Barais, and Serena Elisa Ponta. 2022. Risk Explorer for Software Supply Chains: Understanding the Attack Surface of Open-Source based Software Development. In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED '22), November 11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3560835.3564546

1 INTRODUCTION

Open-Source Software (OSS) is extensively used across the whole technology stack. At the same time, more and more incidents shows that attackers discovered open-source projects as a means for spreading malware to downstream users.

Ladisa et al. [2] propose a taxonomy in the form of an attack tree to systematically describe attack vectors at the disposal of attackers, independent of technologies or ecosystems. Each attack vector is supported by scientific works and real-world examples, and linked to existing safeguards (if any).

To facilitate its use, adoption, and extension by the open-source and security communities, we developed and open-sourced an online tool supporting the visualization and exploration of the taxonomy and all the related information[1].

In the remainder of the paper, Section 2 describes the tool implementation and how to contribute, Section 3 outlines possible use-cases, and Section 5 concludes with closing remarks and an outlook.

2 RISK EXPLORER

Our work proposes a companion tool to the taxonomy of OSS supply chain attacks [2]. Being open-source, it facilitates keeping the said taxonomy relevant and up to date, similarly to other community-driven efforts, e.g., Common Weakness Enumeration (CWE)[2].

The tool has been developed using React.js[3], a front-end framework for single-page applications, and is hosted by a Node.js server. As such, it can be served via GitHub Pages, and the iterative exploration of the attack tree happens in the browser.

The interactive visualization of the attack tree is the tool's main functionality and has been implemented using the *collapsible tree* from the d3.js library[4]. Users can collapse and expand the different nodes of the attack tree to explore the attack surface of open-source-based software development. The description of the respective attack vector, references, as well as associated safeguards are shown below the tree (cf. Figure 1). This exploratory mode of visualization offers to the user the benefit of managing visual complexity and accessing information in more consumable portions on-demand [1].

SCORED '22, November 11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9885-5/22/11.
https://doi.org/10.1145/3560835.3564546

[1] https://sap.github.io/risk-explorer-for-software-supply-chains/
[2] https://cwe.mitre.org
[3] https://reactjs.org/
[4] https://d3js.org/

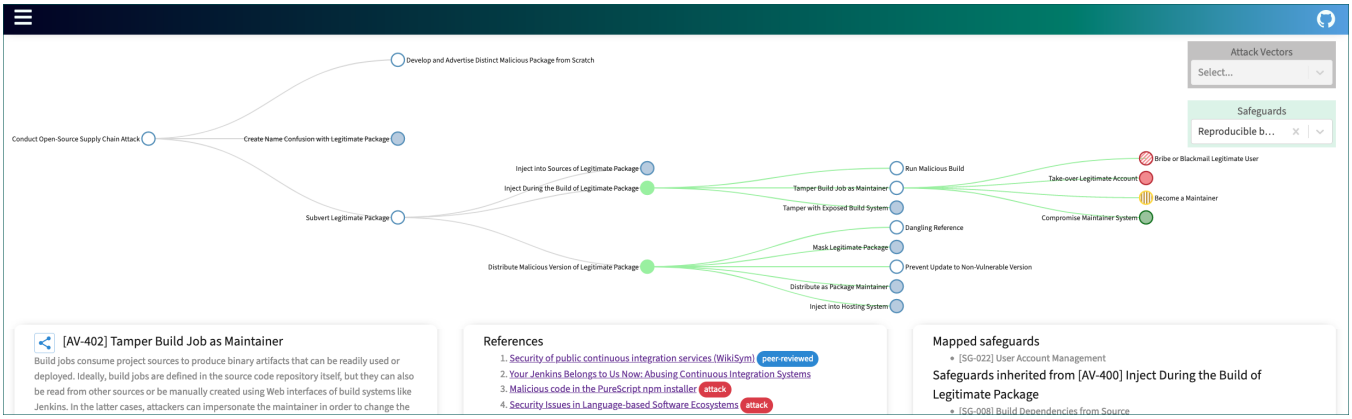

Figure 1: Screenshot of the attack tree visualization (in green attack vectors covered by safeguard *Reproducible builds*).

A share button generates a deep link to individual attack vectors, which can be referenced from 3rd party websites, e.g., in training material or security advisories. A search field in the top-right corner allows searching for attack vectors by name. Upon selection, the respective path from the root node to the selected attack vector is expanded and highlighted in red. The second search field right below is for safeguards. Upon selection, all the nodes mitigated by the respective safeguard are colored in green (cf. Figure 1).

Additionally, all attack vectors, safeguards, and bibliographical references can also be displayed in tabular form on dedicated pages. References can be sorted after title, publication year and affected ecosystem. The tabular display of attack vectors also allows showing information about associated safeguards in a modal window.

3 USE CASES

The tool can be used to raise awareness among developers and for training purposes. Security advisories could use deep links to reference the attack vector(s) used in a given attack. Another use-case is to support threat modeling activities for development and build environments, both for open-source and proprietary development projects. Similarly to the ATT&CK Navigator[5] , the tool can also be used for red/blue team planning and security assessments. Finally, the visual highlight of attack vectors covered by given safeguards can help in the selection and design of security controls.

The tool is used by a security expert providing guidance on supply chain security across the entire organization. She uses it *"to learn about specific software supply chain attacks, [...] its relation in the chain and suggested safeguards"*. She reported that, through the suggested safeguards and linked references, the tool *"helped learning more about preventive and detective measures"*. Content, but especially the combination of features offered by the tool, e.g. *"the visualization and mapping, [and the] ability to see cross-references"*, was reported as a strength. On the other hand, she pointed out some UI bugs and the need to have *"deep knowledge of the topic to understand how to use the safeguards"*. The expert concluded that she *"will continue to reference to this research while improving security practices for development"*.

[5]https://mitre-attack.github.io/attack-navigator/

4 HOW TO CONTRIBUTE

The tool and its underlying data are hosted on GitHub[6]. The flat data structures in separate files facilitate the addition and update of information. To this end, the repository also contains a template for references, which is supposedly the most frequent addition, e.g., to reflect new attacks or scientific publications. When Pull Requests are merged, a new version of the page is automatically deployed.

5 CONCLUSION AND FUTURE WORKS

This paper proposes a visualization tool for the taxonomy in [2]. With new attacks occuring, the evolution of the taxonomy is facilitated by the tool and data being open-source.

In future work, the tool can be extended to hold a more comprehensive database of OSS supply chain incidents. So far, only a subset of affected packages is referenced.

Another possible extension is to reflect the results of automated or manual assessments done for a given development project, to highlight open and covered attack vectors, similar to what the Atomic Red Team tool[7] does for the ATT&CK framework.

Acknowledgements. We thank all the reviewers and the security practitioner for their feedback. This work is partly funded by EU grants No. 830892 (SPARTA) and No. 952647 (AssureMOSS)

REFERENCES

[1] Ana Figueiras. 2015. Towards the Understanding of Interaction in Information Visualization. In *2015 19th International Conference on Information Visualisation*. 140–147. https://doi.org/10.1109/iV.2015.34

[2] Piergiorgio Ladisa, Henrik Plate, Matias Martinez, and Olivier Barais. forthcoming 2023. SoK: Taxonomy of Attacks on Open-Source Software Supply Chains. *IEEE Symposium on Security and Privacy (SP)* (forthcoming 2023).

[6]https://github.com/SAP/risk-explorer-for-software-supply-chains

[7]https://github.com/redcanaryco/atomic-red-team