dtec.bw

JAHRESTAGUNG 2025

ScienceForum – JT25

Die Lieferkette als kritischer Faktor für Software Sicherheit

A. Halbritter, D. Merli
Institut für innovative Sicherheit, Technische Hochschule Augsburg, Augsburg

Motivation

Die Sicherheit der Software Lieferkette als ist ein kritischer Faktor [1]. Sowohl der Cyber Resilience Act [2] als auch die Presidential Order [1] aus dem Jahr 2021 fordern eine sogenannte Software Bill of Materials (SBOM), welche die Komponenten und Abhängigkeiten einer Software aufweist. Verschiedene Stakeholder profitieren davon [3], wie Anwender, Käufer, oder Entwickler. Anwender profitieren von einer schnellen Behebung von Schwachstellen in Software, wenn ist ihre SBOM aktuell ist. Käufern ist es möglich durch eine SBOM bereits vor dem Kauf sich einen Überblick über die Software zu verschaffen. Komponenten, welche unerwünscht sind, können daher bereits präventiv ausgeschlossen werden. Entwickler können sich bereits während des Entstehungsprozesses einen Überblick über die Software verschaffen, um ungenutzte Abhängigkeiten zu vermeiden und sicherheitskritische Fehler in der Software zu beheben.

Hintergrund

SBOM sind derzeit in zwei Formaten verbreitet. CycloneDX [4] wird durch die Open Worldwide Application Security Project (OWASP) Foundation gepflegt. Das System Package Data Exchange [5] (SPDX) wird von der Linux Foundation gepflegt.

Problemstellungen

Zu den Faktoren, welche eine SBOM beeinflussen gehören die Programmiersprachen [6], welche durch verschiedene Tools unterstützt werden unterschiedliche Ergebnisse liefern. Unabhängig ob die Programmiersprachen eher industrienah oder webbasiert sind, sind erhebliche Defizite bei der SBOM Generation zu erwarten.
Angriff auf die Supply Chain der Software sind Realität [7], wie das Beispiel von XZ veranschaulicht. Auch haben Staaten, wie die USA bereits erkannt [8], dass auch Opensource Software nicht sicher ist, da immer eine gewisse Unsicherheit besteht, dass andere Staaten Hintertüren in die Software eingebaut haben. Umgekehrt ist es möglich gezielt Software-Abhängigkeiten zu vermeiden [9], welche unerwünscht sind, in etwa Software, welche Exportbeschränkungen unterliegt.

Forschungsansätze

Folgende Forschungsansätze sind zu untersuchen:

▪ Vergleich verschiedener Tools für Web und System Level Software

Die Untersuchung zur Genauigkeit der SBOM in verschiedenen Programmiersprachen bereits untersucht. Sie zeigt, dass die Generation von SBOM derzeit mit Schwächen verbunden ist.

▪ Vergleich der beiden verbreiteten SBOM Standards

Derzeit sind die beiden SBOM Standards CycloneDX und SPDX verbreitet. Es ist zu untersuchen, welcher Standard sich für welchen Anwendungsfall besser eignet und ob Stärken, oder Schwächen bestehen.

▪ Untersuchung der externen Einflussnahme bei Software

Es ist zu untersuchen, ob und wie oft externe Organisationen bereits versucht haben, Einfluss auf die Software Supply Chain zu nehmen. Es ist eine strukturierte Recherche nötig, um eine Übersicht zu erstellen, welche das Gefahrenbild verdeutlicht.

▪ Erstellung eines SBOM Addons

Erstellung eines SBOM Addons für Entwickler und Käufer, welches rekursiv die Abhängigkeiten durchläuft und basierend auf einem Datensatz Abhängigkeiten von externen Organisationen und Ländern ausgibt.

Mehrwert für die Bundeswehr

- Erhöhte Softwaresicherheit, bietet schnellere Mitigationzeiten

- Geeigneter SBOM Standard stärkt die SBOM

- Überblick über externe Einflussnahme in Software Lieferkette ermöglicht das gezielte Vermeiden von unerwünschten Bibliotheken

[1] Improving the Nation's Cybersecurity, Joseph Biden, 2021
[2] Cyber Resilience Act, European Union, 2024
[3] Building resilient medical technology supply chains with a software bill of materials, Carmody et al., 2021
[4] The System Package Data Exchange, https://spdx.dev, 06.08.2025
[5] CycloneDX, https://cyclonedx.org, 06.08.2025
[6] Accuracy Evaluation of SBOM Tools for Web Applications and System-Level Software, Halbritter & Merli, 2024
[7] The XZ-factor: social vulnerabilities in open source projects, https://english.ncsc.nl/latest/weblog/weblog/2024/the-xz-factor-social-vulnerabilities-in-open-source-projects, 06.08.2025
[8] Army diving ‘headfirst’ into SBOMs to secure software supply chain, https://federalnewsnetwork.com/army/2022/10/army-diving-headfirst-into-sboms-to-secure-software-supply-chain/, 06.08.2025
[9] What technologies are subject to the Commerce Department controls?, https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs/faq/48-what-technologies-are-subject-to-the-commerce-department-controls, 06.08.2025

unibw.de hsu-hh.de dtecbw.de

gefördert durch

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU