

Source-Code-basierte Generierung einer Software Bill of Materials

Andreas Halbritter

Institut für innovative Sicherheit, Technische Hochschule Augsburg
Projekt DS2CCP

Motivation

In der Vergangenheit wurden Schwachstellen in der Software Supply Chain ausgenutzt, wie z.B. durch den xz-Angriff [1]. Um die Behebung dieser Schwachstellen zu unterstützen ist eine **Software Bill of Materials (SBOM)** geeignet. Eine **SBOM** bezeichnet eine Stückliste [2], welche die Komponenten einer Software aufzeigt. Verbreitete Standards sind: **CycloneDX** [3] und **SPDX** [4]. Die Generierung erfolgt im Regelfall mit SBOM Tools aus Dateien, welche der Paketmanager zur Verfügung stellt [5], aber unter Programmiersprachen wie C ist die SBOM Tool Unterstützung gering [6] und der Paketmanager Conan nicht verbreitet [7].

Problemstellung

Auch C-Programme arbeiten mit externen Abhängigkeiten, aber oft ohne Paketmanager. Diese Abhängigkeiten können Schwachstellen besitzen, welche durch eine SBOM schneller behoben werden können. Die SBOM Erstellung für C-Programme ohne Paketmanager ist daher essentiell und derzeit nicht gelöst.

Lösung durch mehrstufigen Ansatz

Zuerst wurde der statische build-Prozess analysiert. Files, wie z.B. .cmake oder .map-Files enthalten Informationen, z.B. über die Libraries der entsprechenden Software, welche dann im Nachgang extrahiert wurden. Diese wurden dann mittels öffentlichen Informationen, wie z.B. aus Package-Repositories ergänzt. Dieser unformatierte Datensatz wurde dann genutzt, um die gesammelten Daten zu CycloneDX und SPDX zu parsen. Anschließend erfolgte eine syntaktische Validierung nach CycloneDX und SPDX und eine inhaltliche Validierung nach BSI TR-03183.

[1] CVE-2024-3094, <https://www.cve.org/CVERecord?id=CVE-2024-3094>, 24.08.2026

[2] BSI TR-03183, Technical Guideline BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.1.0, 24.08.2026

[3] CycloneDX, <https://cyclonedx.org/>, 24.08.2026

[4] SPDX, <https://spdx.dev/>, 24.08.2026

[5] CycloneDX Guide to SBOM, https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-SBOM-en.pdf, 24.08.2026

[6] Menghan Wu, Yukai Zhao, Xing Hu, Xian Zhan, Shanping Li, and Xin Xia. 2026. More than Meets the Eye: On Evaluating SBOM Tools in Java. ACM Trans. Softw. Eng. Methodol. 35, 7, Article 180 (July 2026), 30 pages. <https://doi.org/10.1145/3766073>

[7] JetBrains, The state of C, <https://lp.jetbrains.com/the-state-of-c-2025/>, 24.08.2026

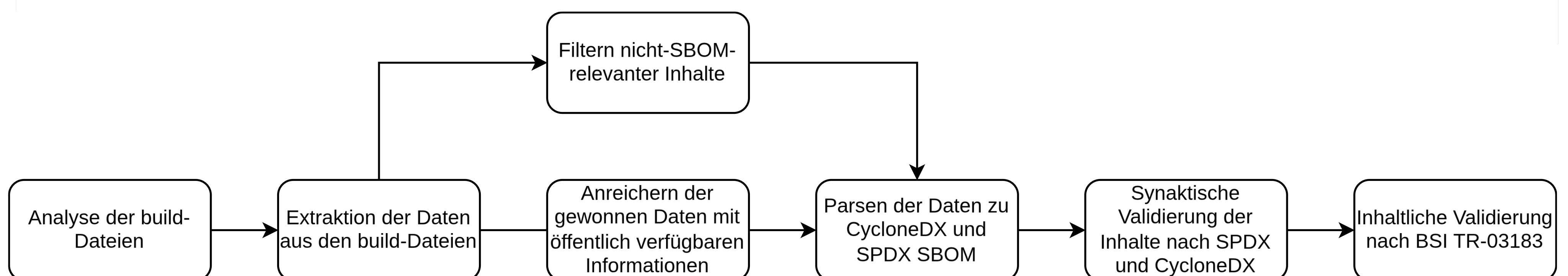


Abbildung 1: SBOM Generationsprozess ohne Paketmanager Dateien

Mehrwert für die Bundeswehr

- Überblick über die Software Supply Chain
- SBOM Generierung ohne Paketmanager für Sprachen wie C
- Enabler für robustes und teilautomatisiertes Schwachstellenmanagement



unibw.de



hsu-hh.de



dtecbw.de

gefördert durch



Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr



Finanziert von der Europäischen Union
NextGenerationEU