DiffBOM: Does SBOMs Accurately Reflects File System Status?

Anonymous Author(s)

ABSTRACT

Modern IoT devices running embedded Linux often include various software packages providing key functionalities. However, it has been repeatedly shown that by compromising these software packages, attackers can take control of the whole device. A powerful tool against such software supply chain attack is a software bill of material, or SBOM. An accurate SBOM can help users quickly identify and mitigate potentially compromised software package in an IoT device. But whether SBOMs accurately reflects the content of file systems of IoT devices is largely unknown. The goal of this paper is to determine SBOM coverage, defined as the percentage of files in a file system claimed by an SBOM, in common IoT devices running embedded Linux. We develop DiffBOM, a tool that automatically collects package manager information as the SBOM for the device, compares the information against the file system, and outputs metrics about the coverage.

Using this tool, we discover…

CCS CONCEPTS

• **Security and privacy** → ;

KEYWORDS

template; formatting; pickling

1 INTRODUCTION

2 BACKGROUND

3 DIFFBOM

3.1 Desired Behavior

3.2 Implementation

4 EVALUATION

5 DATASET

6 ANALYSIS

7 LIMITATIONS

8 CONCLUSIONS

A APPENDIX

REFERENCES

In this section, we will introduce the desired behavior of a DiffBOM tool, as well as introducing our implementation of DiffBOM.

3.1 Desired Behavior

To evaluate if an SBOM accurately reflects the status of a file system, a DiffBOM tool should generally follow this three steps: SBOM Parsing, File System Parsing, and Comparison.

In SBOM Parsing, the tool should be able to accept major SBOM formats, like SPDX, as well as popular proxies of SBOM, such as opkg metadata. With the standardization of SPDX, the adoption of SBOMs is going to increase [**?**]. Meanwhile, available proxies such as package manager metadata typically varies across embedded Linux distributions [**?**]. So supporting multiple SBOM formats and proxies ensures the tool's ability to analyze file systems of a wide range of IoT devices. The tool should correctly read and digest information from different SBOM sources for the Comparison step.