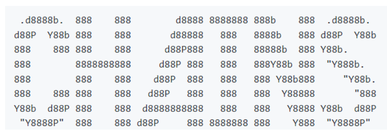
KTH Royal Institute of Technology
School of Electrical Engineering and Computer Science (EECS)



Implementing SBOM Attestations in an Enterprise Context: An Exploration of the Benefits and Challenges

Christofer Vikström
chrvik@kth.se

Abstract

In the wake of the SolarWinds incident, enterprises are increasingly recognizing the critical need for robust security measures, particularly in software supply chain management. Software Bill of Materials (SBOM) has emerged as a pivotal tool for enhancing supply chain transparency and security. SBOM offers a comprehensive inventory of software components, dependencies, and their origins, enabling organizations to effectively track and manage their software supply chain. By providing transparency into software assets, SBOM empowers enterprises to assess potential vulnerabilities, mitigate risks, and ensure compliance with regulatory requirements. The SolarWinds incident exemplifies the urgent need for SBOM attestations. Attackers exploited the software supply chain, infiltrating networks through a compromised update mechanism. Robust SBOM policies could have enabled organizations to detect unauthorized modifications, trace the affected components, and swiftly respond to the breach. Consequently, the incident underscores SBOM's pivotal role in bolstering supply chain resilience and incident response capabilities.

One way to approach SBOM utilization is by implementing SBOM attestations into the software supply chain. Attestations are formal statements or declarations made by trusted entities regarding the security, integrity, or compliance of a piece of software or system. These statements can confirm various aspects, such as adherence to security standards, absence of known vulnerabilities, and more. One presented framework for software attestations is in-toto, which is designed to be supported by automated policy engines but can be integrated into any system that can create and consume verifiable claims. This project aims to explore the challenges and benefits of implementing such a framework into existing CI/CD workflows. How policy changes and additional tool integration affect specific metrics, such as build times and failures, is useful data for enterprises looking to bolster their supply chain security, while also understanding in what way the supply chain in question gets more secure.

The research questions are the following:
1. What are the challenges when implementing in-toto attestations in an enterprise context, and what corresponding benefits does this provide?
2. What relevant enterprise requirements exist and how well can in-toto's attestation framework meet those requirements?

These questions will be explored by generating SBOMs from container images, attesting the SBOMs with in-toto's attestation framework using Syft, cosigned with SigStore's Cosign and Keyfactor's SignServer community edition, and finally attached to the container image in the registry. To understand how this implementation can meet enterprise requirements, a devops kubernetes cluster will be created, allowing for policy changes to occur and CI/CD workload differences to be measured.

(a) in-toto (b) SignServer by Keyfactor (c) Cosign by SigStore (d) Kubernetes

Figure 1: The key components in the project