ASBBS Conference Submission

Pipeline Bill of Materials (PBOM): A Zero-Trust Framework for Software Supply Chain Risk Visibility

Author: Amina Emenena

Affiliation: George Washington University, School of Engineering & Applied Science

Contact: amina@buildflowlabs.com

Submission Category: Abstract (Full paper to follow upon acceptance)

---

1. Abstract

Software supply chain attacks have surged by over 700% since 2019, with the average breach now costing organizations $4.45 million. While the industry has adopted Software Bills of Materials (SBOMs) to track component dependencies, a critical blind spot remains: the "digital kitchen" where the software is built. SBOMs document the ingredients, but they fail to capture the security of the build environments, tool versions, and secret access patterns, the exact vectors exploited in the SolarWinds and Codecov attacks.

This research introduces the Pipeline Bill of Materials (PBOM), a zero-trust framework for continuous visibility into software build lineage. PBOM applies zero-trust principles to the build pipeline itself: no build environment, tool version, or secret access pattern is implicitly trusted, and every component must be continuously verified. Implemented as a core capability of BuildGuard, a compliance CLI available in both open-source and enterprise tiers, PBOM utilizes a zero-touch architecture that scales across enterprise portfolios of 1,000+ repositories without requiring developer action. We present a four-axis health scoring model (tool currency, secret hygiene, build provenance, and vulnerability posture) that transforms raw metadata into actionable risk grades. Preliminary deployment across a 30-repository test organization demonstrates 100% coverage with zero developer friction. By establishing a zero-trust standard for build pipelines, PBOM sets a precedent for how organizations should govern software supply chain integrity.

Keywords: *software supply chain, zero trust, risk management, DevSecOps, build provenance, pipeline security, incident remediation*

2. Practical Significance

This research bridges the gap between theoretical cybersecurity frameworks and the operational realities of high-stakes incident response. The PBOM framework is informed by the author’s direct experience leading remediation strategies for major infrastructure breaches, where compromised build

pipelines resulted in the exposure of tens of thousands of internal accounts.

Unlike purely academic models, PBOM is designed to solve the "friction vs. security" paradox. It applies zero-trust principles to the build pipeline: every tool version, secret scope, and build artifact must be continuously verified rather than implicitly trusted. BuildGuard's open-source tier provides foundational pipeline scanning capabilities, while the PBOM zero-trust health scoring model is available as a premium capability for enterprise environments requiring continuous compliance verification. By leveraging organization-level event capture, this framework provides security practitioners with the "ground truth" of their build environment without requiring manual audits or workflow changes. This ensures that security remains a background utility rather than a development bottleneck, making it viable for organizations managing massive scale. PBOM establishes an informed zero-trust standard for CI/CD pipelines, setting a precedent for how the industry approaches build environment governance.

3. Managerial Implications

From a business and behavioral perspective, the PBOM shifts security from a reactive cost center to a proactive risk management tool. It allows leadership to:

- **Quantify Exposure:** Translate technical pipeline drift into a standardized "Health Score" for board-level reporting.
- **Scale Governance:** Implement automated guardrails that cover 1,000+ repositories without increasing headcount.
- **Ensure Compliance:** Provide immutable evidence of build provenance for regulatory audits and cybersecurity insurance requirements.

4. Author Biography

Amina Emenena is an Engineering Manager and a Doctoral Researcher at George Washington University, specializing in Cybersecurity and Software Supply Chain Security. With extensive leadership experience in infrastructure remediation, including directing recovery strategies for high-profile security incidents, Amina's work focuses on creating scalable, "zero-touch" compliance tools for enterprise environments. She currently leads the development of the PBOM framework and BuildGuard, a compliance CLI tool designed to automate security governance in CI/CD pipelines (buildflowlabs.com).

References

Sonatype. (2022). *8th Annual State of the Software Supply Chain Report*. Retrieved from https://www.sonatype.com/state-of-the-software-supply-chain/introduction

IBM Security. (2023). *Cost of a Data Breach Report 2023*. Retrieved from https://www.ibm.com/reports/data-breach