Security Compass

Enhancing Software Supply Chain Security

National Institute of Standards & Technology Workshop
June 2-3, 2021

Position Paper Submitted by Security Compass
Altaz Valani, Director of Insights Research
Email: avalani@securitycompass.com

Introduction

Section 4(e) of the recent Executive Order requires the management of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government. The goal is to manage the cyber security posture of rationalized applications across their lifecycle within the supply chain.

The current backdrop of cyber security discussions within the supply chain center around:

1. A need to efficiently generate and implement mitigations based on a common set of well known threats. This implies the integration of security with the DevOps lifecycle, including feedback loops that continually add new mitigations to rapidly enhance application security.
2. Managing the complexity of our application portfolios and infrastructure through the injection of thought diversity. Expanding the pool of such advisors increases the likelihood of catching exploitable weaknesses and generating appropriate mitigations through a common platform.
3. Security as an ongoing activity, rather than a single event. Breaking apart silo thought patterns focused on generating discrete artifacts implies a different perspective. That perspective includes managing the entire application lifecycle from planning and procurement, to building and maintenance, and finally retirement.
4. Alignment with ongoing work with other standards and industry groups. For example, CMMI has a lot of similarities with work being done by NIST and ISO. Many of these types of standards and frameworks propose a baseline set of security controls that account for well known weaknesses. Leveraging them allows scarce security resources to focus on novel or edge security cases.

5. A focus on business value. When speaking in the language of business stakeholders, the discussion turns toward risk and resiliency. Such coarse grained concepts must be refined to permit practitioners with a clear understanding of intent and scope.
6. Extending security from a perimeter based model to an asset centric approach. This implies the use of models like Zero Trust where application and data centric requirements are treated as first class citizens.

Ongoing Application Rationalization in the Secure Supply Chain

Whether we acquire off the shelf software or build custom software, eventually we need to configure our systems across the portfolio. This manifests itself through some form of product configuration, custom software development, or integration. From an individual application perspective, that means making key security decisions around the posture to upgrade, patch, replace, integrate, or install new software.

Any decision around which rationalization posture to assume rests on the fundamentals of security risk and cost. We conduct this analysis by balancing business priorities and security threats. In the past, we could more fully understand all threats and vulnerabilities for a given system. However, today's highly distributed and integrated nature of our federal systems makes this practically impossible and requires a different, cross functional approach. The cross functional competencies needed to be successful are:

1. **Knowledge Management**: sharing of information across the supply chain as well as the injection of other knowledge bases from groups like MITRE.
2. **Requirements Management**: easily propagating the right requirements into DevOps and attesting its completion without bias.
3. **Audit and Compliance**: mapping audit requirements to security requirements provides the essential elements of traceability across the supply chain.
4. **Asset Management**: inclusion of security attributes not just on business priority or patch deltas, but also specific security standards and frameworks that apply to the system.
5. **Risk Management**: a repeatable process of aggregating impact and likelihood of a security breach and proposing mitigations to strengthen the broader portfolio.

Next Steps

To ensure the integrity of our supply chain, we need to democratize security across the supply chain. Such a platform based approach will help us better focus on requirements, provide in-situ guidance to implementation teams, provide defensible security attestation, integrate with current DevOps initiatives already in play within the federal space, and bring risk into the discussion. Only with a platform that elicits advice from multiple stakeholders on an ongoing basis, can we hope to respond quickly enough across the supply chain when vulnerabilities are discovered.