Position Paper: NIST Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

(5) Guidelines for software integrity chains and provenance. See EO Sections 4(e)(ii, vi, and viii).

CyTRICS™ is The Department of Energy’s program for cybersecurity vulnerability testing and digital subcomponent enumeration, to include software and firmware evaluation. CyTRICS partners across stakeholders to identify high priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing. CyTRICS leverages best-in-class testing facilities and analytic capabilities at four DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

Based on experience developed in designing and implementing software cyber supply chain security functions under the CyTRICS program, we offer the following observations.

1. Technical enumeration of the digital ingredients in software, in the form of software bills of materials (SBOMs), is superior to the currently ad-hoc self-attestation processes. Given agreed upon standard formats, automated generation of SBOMs is technically feasible, and is the desired end state to support commercial use cases.

2. SBOM standard formats should identify code sourced from common libraries and differentiate it from uniquely developed code. This differentiation will enable analysis of vulnerabilities carried through code reuse.

3. SBOMs should be developed in different levels of detail, depending upon the use case being supported. The community of interest should define 3-5 levels of detail and correlated use cases that different levels of transparency could support. The highest level of detail should be reserved for an internal-to-the-enterprise use case, recognizing the importance of sharing awareness of the digital ingredients included in products, to promote illumination of dependencies among different development units, and ideally, implementation of security-be-design principles.

4. Provenance of software is important, but the role of digital hardware should not be minimized. SBOM standard formats should be developed to allow for interaction of analyses with relevant hardware in hardware bill of materials (HBOM) format; while software-only analysis is valuable, it becomes significantly more actionable when paired with operational hardware.

5. Public disclosure of SBOMs on a public website is not advisable for a majority of use cases. The principle use case for SBOM generation and exchange is to support supply chain illumination for commercial transactions. In that case, the relevant parties to the transaction may exchange standard formatted SBOMs directly, or through a trusted third party. Public disclosure of SBOM data generates risk unnecessarily, as it provides a level of detail that could be used for malicious cyber purposes.

6. Although a primary use case for SBOM generation is to support risk-informed commercial transactions, a critical second use case is to support broader vulnerability-focused (and national security-focused) analyses of dependencies across software products. Such analyses are only possible with aggregation of SBOM data across a wide variety of products.

7. While a single centralized national repository would be challenging, the federal government (or a third-party agent of the federal government, such as the DOE National Labs) could create a centralized repository of SBOMs obtained from federal procurement actions. A federally held repository would be the best positioned to conduct national security-focused (to include application of classified threat intelligence) vulnerability analyses.

8. A distributed data storage method such as blockchain has been proposed as an underlying structure for the sharing of this information between various actors. However, this would not be as effective or accessible as it increases challenges for end users when attempting ensure security across multiple vendors. A distributed data storage method also reduces the ability to streamline and standardize data input. However, a distributed ledger may be a viable alternative to a centralized data repository for ensuring historical accountability and enabling data sharing.

9. Trusted third parties are a critical component of the end state for software integrity chains and provenance. Requirements for trusted third parties should be developed to create a strong secure ecosystem for retaining and managing SBOM data repositories, to include secure data ingest, handling, and storage processes. Additional functions could include requirements for periodic updates (refresh) of SBOM holdings.

10. Trusted third party repositories could also be developed around critical infrastructure sectors, to support regulatory requirements in a more efficient manner, and perform analyses of vulnerabilities across an entire sector. Additionally, trusted third party repositories could perform vulnerability analyses among trusted repositories across multiple critical infrastructure sectors to develop a national view; or trusted repositories in other countries to support a global view of the cybersecurity of the software ecosystem.

Please direct any questions to jess.smith@pnnl.gov; virginia.wright@inl.gov; or Cherylene.caddy@hq.doe.gov.

If requested, we would be happy to present this position and supplementary information related to our experience in the CyTRICS program. The coordinating author will be:

Jess Smith, PhD

Jess.Smith@PNNL.gov

509 372 4213