BlackBerry

May 26, 2021

National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899

Re: Standards and Guidelines to Enhance Software Supply Chain Security

Dear NIST,

BlackBerry supports NIST leadership to enhance the security and integrity of software supply chain to address the President Executive Order In Improving the Cybersecurity of the Federal Government (14028). We appreciate the opportunity to share views and ideas and participate in the Workshop on Software Supply Chain Security June 2-3.

Our position paper addresses the second area of NIST inquiry, initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government and the fourth area, initial minimum requirements for testing software source code.

We respectfully submit the attached position paper with the contact information of the proposed speaker.

Takashi Suzuki, Senior Director, Standards
tsuzuki@blackberry.com / + 1 647 440 7551

Respectfully submitted,

Takashi Suzuki

Takashi Suzuki,
Senior Director, Standards

BlackBerry Position Paper
Secure Software Development Environment and Testing Software Code

Securing software development environment

Protecting the software development environment from sophisticated malicious attacks is imperative because the software (data), the build environment and signing services are the most important assets or resources of the suppliers. The EO calls for 6 actions in Sec.4 (e)(i). BlackBerry recommends applying zero trust principles laid out in NIST SP 800-207 to address the requirements.

Define policies to identify and limit subjects who have access and apply logical segmentation to administratively separate the build environment (A), evaluate or audit trust in the requester of information before granting access per session basis, regardless of its network location (B), apply dynamic or risk based policies for multi-factor authentication, conditional access and authorization (C), setting polices to protect data and ensure integrity at rest, in transit and in use (E) and collect as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture, monitor operations, alert and respond to cyber incidents (F).

We emphasize the importance of continuous authentication based on user and entity behavior analytics and dynamic adaptation of the access policies. Anomaly of user behavior can be constantly monitored and evaluated. AI/ML technology enables authentication of users by their behaviors not only location and time of information access, but also characteristics of device usage including typing, touching and application utilization. When anomaly is detected, the access policy can be instantly adjusted to trigger multi factor authentication or disconnect the device from the network. Detecting anomalous user behavior early may help reduce the likelihood of compromise of build systems.

Concerning artifacts that demonstrate conformance to the secure development environment in the EO Sec.4 (e)(ii), BlackBerry recommends that conformance assessment should be conducted according to widely adopted and proven information security management system standards, for example, ISO 27001 or independent AICPA SOC2 validation of controls in the development and production environments. Such standards provide organizational and system level requirements and technology agnostic security controls which address the key requirements in (e)(i) and are easily tailored to zero trust architecture and protocols. The standard requires the organization to plan, establish, implement and maintain an audit program, and retain documented information as evidence of the audit program and the results. Upon request from a purchaser, a summary of the most recent audit results can be provided.

Testing software source code complemented by binary composition analysis

BlackBerry agrees that use of automated source code review tools, including both static and dynamic analysis, are necessary to enable developers to write secure codes efficiently without requiring security expert knowledge. As required in the EO Sec.4 (e)(iv), vulnerability detection and

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

remediation are essential requirements. One prerequisite for vulnerability detection is software composition analysis to provide insight into the software bill of materials. The composition analysis is key to identifying open-source code included in the software, its provenance, identification, version information and applicable open-source licenses.

The output from the composition analysis can be used to identify risk associated with software developed both in-house and the supply chain (e.g. public vulnerabilities, information leakage), testing and verification (actual components included vs. provided software bill of material) and alignment with security design (do delivered software components address the planned security design?).

BlackBerry would like to highlight the significant limitations in relying solely on source code review and testing. A source code review is unable to capture what source is actually compiled and bundled into the final product. Factors such as compiler and build system configurations, including optimizations and compiler defenses, and compiled libraries, to which you have no source code access and build scripts, source code reviews cannot have complete visibility into what the final solution will really become.

In this regard, we recommend that binary software composition analysis should be added to the minimum requirements. There are several advantages of this approach, with the most important being allowing the security team to review the actual binary that external attackers will have access to. This is critical as security issues can be introduced at the build stage and would not be caught by a source code review. Binary software analysis can also be performed by the consumer, decreasing the probability that a compromised build system will evade detection.

Finally, the software testing tool should evaluate or score findings of potential weakness or vulnerability e.g. using the Common Vulnerability Scoring System (CVSS). The score can provide curated information on a wide variety of issues ranging from insecure API and c-runtime use, recursive function calls, the inclusion of system networking tools to files containing debug information. Such metrics may form artifacts of the execution of the tools or a summary of the risk addressed and mitigated (Sec.4 (e)(v)). Monitoring changes in evaluated and remediated vulnerabilities can be used as an indicator of the supplier's security posture.

Summary

BlackBerry recommends applying Zero Trust principles to secure development environments along the entire software supply chain and utilizing proven information security management system or attestation standards to assess the conformity. For software code testing, we respectfully urge NIST to include binary software composition analysis as a minimum requirement. The binary code analysis tools address gaps or blind spots of source code review tools by revealing a full list to software components in the final products including third party binaries and issues introduced in build stage such as improper compiler defense options and build environment. As such will complete the visibility required for software code verification by suppliers or consumers.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661