Finite State - NIST Position Paper
Standards and Guidelines to Enhance Software Supply Chain Security

Focus: In this Position Paper, we address topic areas 1 and 4 directly (and areas 2 and 5 indirectly). We request the opportunity to present on these issues at the NIST Virtual Workshop.

Conclusion: Acquisition personnel have long been required to perform an effectively impossible task: manage supply chain risk without adequate information about the software products they purchase. Executive Order 14028 represents an opportunity to require vendors to provide essential information in a manner that is transparent, verifiable, and reproducible across a broad universe of products and thereby dramatically improve opportunities to manage supply security.

Introduction: Measures to enhance software supply chain security must enable federal acquisition personnel to make an informed decision about the underlying security of the software they are buying and whether the inherent risk that software represents is acceptable.

While this question of risk extends to any code or device (including any legacy code or device) that has access to a network, different federal agencies will weigh the degree of acceptable risk differently depending on the function of the network to which it is connecting along with the nature of access it has to that network. What is acceptable risk in one context may not be acceptable in another.

It is the responsibility of acquisition personnel to make this assessment, but they cannot do so if they lack transparent, verifiable, and reproducible information. In other words, if the risk is not known, it cannot be managed.

From our perspective, the key function of the guidance that NIST has been tasked with developing is to enumerate the minimum requirements (and standardized format) for the information necessary to enable acquisition personnel to carry out this risk assessment - not only before they purchase software, but also throughout the lifecycle of that software.

Minimum Requirements: Enabling acquisition personnel to assess whether software represents an acceptable risk requires, at a minimum, enabling acquisition personnel to:

- See a comprehensive inventory of all components included in the final build of software
- Identify what entity created each component (to include at least the name and geographic location of the entity)
- Verify that all code in the final build has been tested:
    - In an automated, machine readable, scalable fashion
    - Using a tool that provides traceable, third-party validation
    - Using capabilities such as Static Application Security Testing; system-level testing; and analysis of cryptographyy

- Identify publicly known vulnerabilities and exploits present in that inventory
- Follow an established plan for prioritization and remediation of discovered vulnerabilities
- Independently repeat the testing/validation process on an ongoing basis (and with respect to any updates/patches to the software)

Scope of "Critical Software": Precisely because context matters in the software risk assessments that the various departments and agencies conduct, the scope of software covered under the definition of "critical software" must be broad. What qualifies as a mission-critical software component in one deployment may be of little or no consequence in another. By requiring vendors to provide key information for a very wide range of software products, acquisition personnel will be empowered to apply it in context.

Accordingly, the question of scope should be driven not just by the characteristics of the software itself but also by the nature of its connection to agency networks that perform critical functions.

In this, however, it is important to avoid conflating "critical software" and "critical function" with the concept of "critical infrastructure."[1] Restricting the application of Executive Order 14028 to only those systems which, if disrupted, would have a "debilitating impact" on U.S. security and public health or safety would require only a small portion of software developers to address supply chain security and deprive the vast majority of federal networks of critical risk management information.

Instead, the guidelines should be applicable to any software (including software embedded in devices) that: (1) performs a critical function[2] - whether with respect to mission, operations, or data, or (2) that connects to such software. No matter how trivial the function of the software, a security flaw or vulnerability can enable an attacker to compromise the entire network.

To be sure, we anticipate that some commenters will express the view that it is too difficult, time consuming, or expensive to implement the guidelines with a wide array of software products (including, and perhaps especially, legacy software).

The reality is that there are already tools on the market that are capable of performing the testing described in Section III on an automated basis and at scale.

[1] The USA PATRIOT Act of 2001 defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[2] NIST 800-161 defines "critical functions" as "those functions, which if corrupted or disabled, are likely to result in mission degradation or failure."