NIST Request: Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

NowSecure Response #4 - *"Initial minimum requirements for testing software source code including defining types of manual or automated testing, their recommended uses, best practices, and setting realistic expectations for security benefits."*

NowSecure, Inc. (parent company viaForensics, LLC)
1608 Spring Hill Rd, Ste 200, Vienna VA, 22182

NowSecure has 12 years in mobile app forensics, mobile app security testing, test automation, mobile pen testing and mobile security standards development.

Date Submitted: Wednesday, May 26, 2021 Submitted by: Jeff Miller, Director US Public Sector - jmiller@nowsecure.com Gentry Sims, Director Fed Bus Dev - gsims@nowsecure.com	Contributors: Alan Snyder, CEO - asnyder@nowsecure.com Andrew Hoog, Founder - ahoog@nowsecure.com Brian Reed, CMO - breed@nowsecure.com Brendan Hann, PMM - bhann@nowsecure.com

NowSecure is restating the objective to strike the specific use of of the term "source code" for clarity

- Effective security testing for mobile and web includes static and dynamic testing of app binary files, not just source code.
- Limiting to testing only "source code" means key parts of the app attack surface would remain untested and the software applications would remain at risk, and would prevent testing of commercial applications where testers may not have access to source code.

NowSecure suggests a multi-tool approach to security testing focused on test automation as each set of tools covers different parts of the mobile app attack surface. Creating a flexible set of guidelines will enable all software developers and purchasers to select the appropriate approach.

- Automated SCA and Static Source Code testing enables fast testing of 1st and 3rd party code as developed, identifying low hanging fruit and issues before they hit production
- Automated Dynamic Binary and APISec enables runtime testing for each build of each mobile app as developed, expanding coverage without the time and complexity of manual pen testing
- Automated Static Binary, Dynamic Binary and APISec enables runtime security testing of apps in production and can provide an SBOM with no access to source code.
- Expert manual Pen testing provides deepest coverage for high risk apps at additional cost and effort when required.
- Applying Automated SCA, Static Source, Static Binary, Dynamic Binary and APISec enables teams to develop and ship secure code faster at scale, with automation covering the majority of issues and Pen testing used where needed for highest risk items requiring human ingenuity.

NowSecure recommends leveraging the existing OWASP MASVS Standard as foundation for any new standards under this executive order.

- OWASP and the OWASP Mobile Project are well known, recognized, trusted and widely implemented across the industry, drafted and updated with the support of a global community. Note NowSecure believes strategically in community standards and has worked with OWASP on specification development, OWASP tools development and sponsorship since its inception.

- The OWASP Mobile Project combines the MASVS and MSTG, with recommendation to focus on MASVS which has levels of standard security requirements based on risk (L1, L2, R).
- Other standards such as the ioXt alliance certification standard for IoT-connected mobile apps and mobile VPNs have been built leveraging the OWASP MASVS with refinements as needed. The ioXt standard was created collaboratively by Google, Amazon, NowSecure, NCC Group, DEKRA, Onward Security and 7layers, and aligned with the initiatives set forth by VPN Trust Initiative. As recommended here, the initial work in the ioXt project started with OWASP MASVS as a proven baseline, then was refined for IoT.
- For standards to be adopted at a wide scale they must be easy to implement and cost effective, so automation, clarity and ease of use should be a core consideration.
- Given the need for speed and scalability, NowSecure suggests a 2 tiered standards approach
    - Automated testing designed to cover reasonable attack surface based on what can be deployed as fully automated testing for speed and scale in DevSecOps scenarios, like code scanners which run automatically in the background with no human intervention
    - Optional manual testing for additional high risk items that might be present in certain mobile apps that cannot be automated with current automation technology.
    - Provide the flexibility for the software developer and tester to select appropriate testing approach based on threat model and risk profile of the particular mobile app

Discussion of Automation requirements and impact

- Automation enables scale. The typical mobile application is updated 12-24 times a year, with the top 500 downloaded mobile apps updated as often as daily in the public app stores. Rapid release cycles and DevSecOps scenarios require speed and scale.
- A traditional mobile app pen test takes 2 weeks at a cost of $20k and cannot fit that cycle speed while becoming prohibitively expensive. Thousands of pen testing jobs remain open and unfulfilled, leaving organizations unable to perform manual testing with frequency they might wish. To be successful with security built in at scale, organizations leverage automated security testing built into their development pipelines.
- A lesson learned from NIAP compliance is that the requirement for manual attestation slows down the process and has reduced the speed of app releases and delayed ATO certifications for federal use.
- Benchmark analysis shows that automated software security testing drives the risk of breach down at least 30%.
- Automation will enable testing throughout the development process to ensure security is built in, and will also enable continuous monitoring of mobile app as they update in production for Continuous Diagnostics and Mitigation (CDM) that would be impossible without always-on automation

NowSecure proposes a straightforward path forward for mobile application security testing standards for mobile app category deemed as “critical software”:

1. Start with OWASP MASVS as the foundation of the new Security Testing Standards
2. Review the MASVS to ensure that all of the tests are relevant and can be Automated.
    a. Modify or remove tests that cannot be Automated.
3. Adopt the Automatable OWASP MASVS as the final primary Security Testing Standard
4. Optionally consider additional tier of non-automated testing for high risk scenarios as a follow-up phase 2 in the standards process after initial standards are released and proven success in marketplace.