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

NowSecure Response #3 - *"Guidelines outlining security measures that shall be applied to the federal government's use of critical software, including but not limited to, least privilege, network segmentation and proper configuration."*

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 recommends the use of industry-standard configuration guidance for the development and configuration of secure mobile applications. Here is a sample list of configurable features to be provided by mobile app developers and documented for proper configuration for federal use:

- Ensure sufficient encryption levels
- Ensure multi-factor authentication configuration, including soft tokens
- Ensure ability to configure mobile apps to run over secure VPN
- Ensure configuration to limit data storage
- Ensure configuration to limit data sharing between mobile apps and services on device (block SMS, Block external memory card, Block contact address book, etc)

NowSecure recommends that Zero Trust Architecture include specific standards and requirements for mobile applications, not just devices and users.

- Zero Trust architecture is an effective way to apply security standards to least privilege, network segmentation, and proper configuration
- The massive and ever growing use of mobile devices and apps, including 3rd party apps from public app stores through BYOD programs, creates often unknown, unmanaged risk in federal organizations.
- Create standards for 3rd party mobile app vetting that identifies all mobile apps untrusted in Zero Trust architecture until properly vetted before deployment AND continuously monitors all apps in production for new weaknesses that could be introduced.
- The standards for certification for use in Zero Trust environments can incorporate the same standards as documented throughout our other responses.

NowSecure has a database of millions of security assessments for millions of apps in the public app stores of Apple AppStore and Google Play. Data includes results of binary SAST, DAST, and APIsec testing including vulnerabilities, privacy issues, leaked PII, SDKs and SBOM, crypto, data storage, network connections and APIs, geolocation, and data transmission to other countries with history of app versions for years. These applications are continuously monitored with each new release, and we can provide additional information on trends and statistics from that data to assist in the process of defining standards.