NIST provides draft guidelines to secure mobile devices

November 1 2012

The National Institute of Standards and Technology (NIST) has published draft guidelines that outline the baseline security technologies mobile devices should include to protect the information they handle. Smart phones, tablets and other mobile devices, whether personal or "organization-issued," are increasingly used in business and government. NIST's goal in issuing the new guidelines is to accelerate industry efforts to implement these technologies for more cyber-secure mobile devices.

Securing these tools, especially employee-owned products, is becoming increasingly important for companies and government agencies with the growing popularity—and capability—of the devices. Many organizations allow employees to use their own smart phones and tablets, even though their use increases cybersecurity risks to the organization's networks, data and resources.

"Guidelines on Hardware-Rooted Security in Mobile Devices" defines the fundamental security components and capabilities needed to enable more secure use of products.

"Many current mobile devices lack a firm foundation from which to build security and trust," explains NIST lead for Hardware-Rooted Security Andrew Regenscheid, one of the publication's authors. "These guidelines are intended to help designers of next-generation mobile phones and tablets improve security through the use of highly trustworthy components, called roots of trust, that perform vital security functions." On laptop and desktop systems, these roots of trust are often

implemented in a separate security computer chip that cannot be tampered with, but the power and space constraints in mobile devices could lead manufacturers to pursue other approaches such as leveraging security features built into the processors these products use, he says.

The NIST guidelines are centered on three security capabilities to address known mobile device security challenges. They are device integrity, isolation and protected storage. A tablet or phone supporting device integrity can provide information about its configuration, health and operating status that can be verified by the organization whose information is being accessed. Isolation capabilities are intended to keep personal and organization data components and processes separate. That way, personal applications should not be able to interfere with the organization's secure operations on the device. Protected storage keeps data safe using cryptography and restricting access to information.

To attain the security capabilities, the guidelines recommend that every mobile device implement three security components. These are foundational security elements that can be used by the device's operating system and its applications. They are:

- Roots of trust, which are combinations of hardware, firmware and software components that are designed to provide critical security functions with a very high degree of assurance that they will behave correctly;
- An application programming interface that allows operating systems and applications to use the security functions provided by the roots of trust; and
- A policy enforcement engine to enable the processing, maintenance and policy management of the mobile device.

The authors of "Guidelines on Hardware-Rooted Security in Mobile

Devices," Special Publication 800-164 (Draft) request comments to improve the draft. The publication may be downloaded from csrc.nist.gov/publications/Pub … afts.html#SP-800-164. Please submit comments by December 14, 2012, to 800-164comments@nist.gov.

Provided by National Institute of Standards and Technology