PHYS.ORG

NIST updates guidelines for mobile device security

July 11 2012

The National Institute of Standards and Technology (NIST) has released a proposed update to its guidelines for securing mobile devices—such as smart phones and tablets—that are used by the federal government. NIST is asking for public comment on the draft document.

Mobile devices allow workers, including government employees, to work in multiple locations and to improve their efficiency. But the same features that make these devices desirable make them a security challenge. Mobile devices can easily be lost or stolen, and users may be tempted to download nonsecure apps that might conceal "malware" that could be used to steal confidential data. Since security is minimal for mobile devices, a thief can retrieve sensitive data directly from the device, or use the phone or tablet to access an organization's computer network remotely.

The revised guidelines recommend using a software technology that centralizes device management at the organization level to secure both agency-issued and personally owned devices that are used for government business. Centralized programs manage the configuration and security of mobile devices and provide secure access to an organization's computer network. They are typically used to manage the smart phones that many agencies issue to staff. The new NIST guidelines offer recommendations for selecting, implementing, and using centralized management technologies for securing mobile devices.

"Mobile devices need to support multiple security objectives:

confidentiality, integrity and availability, so they need to be secured against a variety of threats," explains co-author and NIST guest researcher Karen Scarfone. This publication provides specific recommendations for securing mobile devices and is intended to supplement federal government security controls specified in NIST's fundamental IT security document, Recommended Security Controls for Federal Information Systems and Organizations (Special Publication 800-53).

The draft guidelines also recommend developing system threat models for mobile devices and those resources accessed through them, instituting a mobile device security policy, implementing and testing a prototype of the mobile device solution before putting it into production, securing each organization-issued mobile device before allowing a user to access it, and maintaining mobile device security regularly.

Originally published as Guidelines on Cell Phone and PDA Security, the revision has been updated for today's technology. The guidelines do not cover laptops because the security controls available for laptops today are quite different than those available for smart phones and tablets. Basic cell phones are not covered because of the limited security options available and threats they face.

More information: NIST requests comments on Guidelines for Managing and Securing Mobile Devices in the Enterprise (SP 800-124 Revision 1). The document can be found at csrc.nist.gov/publications/dra … t_sp800-124-rev1.pdf. Comments should be sent to 800-124comments@nist.gov by Friday, Aug. 17, 2012, with the subject "SP 800-124 Comments."

Provided by National Institute of Standards and Technology

Citation: NIST updates guidelines for mobile device security (2012, July 11) retrieved 1 May 2024 from https://phys.org/news/2012-07-nist-guidelines-mobile-device.html