ITL BULLETIN FOR JULY 2013

ITL ISSUES GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently published revised guidelines for managing the security of mobile devices. Written by Murugiah Souppaya of NIST and Karen Scarfone of Scarfone Cybersecurity, NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, will assist organizations in centrally managing the security of mobile devices such as smart phones and tablets. The document describes the security issues inherent in mobile device use and gives recommendations for selecting, implementing, and using centralized management technologies to secure mobile devices throughout their life cycles. While the publication primarily covers the security of organizational devices, the information can also apply to personally owned mobile devices.

To improve the security of mobile devices, organizations should:

- Develop a mobile device security policy. The policy should define what types of organizational resources can be accessed via mobile devices, what types of mobile devices are permitted, degrees of access, and how provisioning should be handled;
- Develop system threat models for mobile devices and the resources accessed through such devices. Threat modeling helps organizations to identify security requirements and to design effective solutions;
- Consider the merits of each provided security service, determine the needed services, and design and acquire solutions which provide the services. Categories of services to be considered include general policy, data communication and storage, user and device authentication, and applications;
- Implement and test a pilot of the mobile device solution before putting the solution into production. Consider connectivity, protection, authentication, application functionality, solution management, logging, and performance of the mobile device solution;
- Fully secure each organization-issued mobile device before allowing access. This ensures a basic level of trust in the device before it is exposed to threats; and
- Maintain mobile device security on a regular basis. Organizations should periodically assess mobile device policies and procedures to ensure that users are properly following them.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.