NIST SPECIAL PUBLICATION 1800-21A

Mobile Device Security

Corporate-Owned Personally-Enabled (COPE)

Volume A:
Executive Summary

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

**Former employee; all work for this publication was done while at employer.*

July 2019

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise

Executive Summary

- Mobile devices provide access to workplace data and resources that are vital for organizations to accomplish their mission while providing employees the flexibility to perform their daily activities. Securing these devices is essential to the continuity of business operations.
- While mobile devices can increase organizations' efficiency and employee productivity, they can also leave sensitive data vulnerable. Addressing such vulnerabilities requires mobile device management tools to help secure access to the network and resources. These tools are different from those required to secure the typical computer workstation.
- To address the challenge of securing mobile devices while managing risks, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore how various mobile security technologies can be integrated within an enterprise's network.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-based, commercially available products to help meet their mobile device security and privacy needs.

CHALLENGE

Mobile devices are a staple within modern workplaces. As employees use these devices to perform everyday enterprise tasks, organizations are challenged with ensuring that devices regularly process, modify, and store sensitive data securely. These devices bring unique threats to the enterprise and should be managed in a manner distinct from traditional desktop platforms. This includes securing against different types of network-based attacks on mobile devices that have an always-on connection to the internet.

Managing the security of workplace mobile devices and minimizing the risk posed can be challenging because there are many mobile device security tools available. Proper implementation is difficult to achieve for an end user because the method of implementation varies considerably from tool to tool. In addition, unfamiliarity with the threats to mobile devices can further compound these implementation difficulties.

SOLUTION

To address the challenge of securing mobile devices within an enterprise, NIST built an example solution in a lab environment at the NCCoE to demonstrate mobile management tools that enterprises can use to secure their networks. These technologies are configured to protect organizational assets and end-user privacy, providing methodologies to enhance the security and privacy posture of the adopting organization.

Both Apple iOS and Android devices are used in the example solution, which includes detailed device configurations and enterprise mobility management policies provisioned to the devices. The foundation of this architecture is based on federal U.S. guidance, including that from NIST 800 series publications, National Information Assurance Partnership, U.S. Department of Homeland Security, and the Federal

Chief Information Officers Council. These standards, best practices, and certification programs help ensure the confidentiality and integrity of enterprise data on mobile systems.

This guide provides:

- a detailed example solution and capabilities that address risk and implementation of security controls
- a demonstration of the approach using commercially available products
- how-to instructions for implementers and security engineers, with instructions on integrating and configuring the example solution into their organization's enterprise in a manner that can achieve security goals with minimum impact on operational processes

The NCCoE sought existing technologies that provided the following capabilities:

- enhanced protection of data that resides on the mobile device
- centralization of management systems to deploy policies and configurations to devices
- ability to evaluate the security of mobile applications
- inhibition of the eavesdropping of mobile device data when traversing a network
- privacy settings that protect end-user data
- protection from phishing attempts

Commercial, standards-based products such as the ones we used are readily available and interoperable with existing information technology (IT) infrastructure and investments.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* can help your organization:

- reduce adverse effects on the organization if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- apply robust, standards-based technologies using industry best practices
- reduce privacy risks to users through privacy protections
- provide users with enhanced protection against loss of personal and business data when a device is stolen or misplaced
- deploy enterprise management technologies to improve the security of enterprise networks, devices, and applications

- reduce risk so that employees can access the necessary data from nearly any location, using a wide selection of mobile devices and networks
- enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implement government standards for mobile security

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at mobile-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

appthority kryptowire Lookout MobileIron paloalto Qualcomm

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit http://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200