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 done while at employer.*

September 2020

Final

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

The first draft of 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 vital workplace resources while giving employees the flexibility to perform their daily activities. There are several options for deploying mobile devices. One deployment model is Corporate-Owned Personally-Enabled (COPE). COPE devices are owned by the enterprise and issued to the employee. COPE architectures provide the flexibility of allowing both enterprises and employees to install applications onto the enterprise-owned mobile device.

Securing mobile devices is essential to continuity of business operations. While mobile devices can increase efficiency and productivity, they can also leave sensitive data vulnerable. Mobile device security tools can address such vulnerabilities by helping secure access to networks and resources.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore the challenges of securing mobile devices while managing risks and how various technologies could be integrated to help organizations secure their COPE devices.

This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-based, commercially available products to help meet their COPE mobile device security and privacy needs.

CHALLENGE

Mobile devices are a staple within modern workplaces. As employees use COPE devices to perform tasks, organizations are challenged with ensuring that these devices process, modify, and store sensitive data securely. COPE devices bring unique threats to the enterprise and therefore should be managed in a manner distinct from desktop platforms.

These challenges include securing them from different types of application- and network-based attacks on mobile devices that have an always-on connection to the internet. Mobile devices also introduce potential privacy implications for employees using the devices for personal activities.

Managing the security and privacy of workplace mobile devices and minimizing the risk posed can be challenging because there are many mobile device security tools available. Proper implementation can be difficult because the method of implementation varies considerably from tool to tool. In addition, unfamiliarity with the threats to mobile devices can increase implementation challenges.

SOLUTION

To address the challenge of securing COPE devices within an enterprise, NIST built an example solution in a lab environment at the NCCoE to demonstrate mobile device security 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 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, the National Information Assurance Partnership, U.S. Department of Homeland Security, and Federal

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

This guide provides:

- a detailed example solution and capabilities addressing risk and security control implementation
- a demonstration of the approach that uses commercially available products
- how-to instructions for implementers and security engineers, with instructions on integrating and configuring the example solution into their organization 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
- centralized management systems to deploy policies and configurations to devices
- evaluation of the security of mobile applications
- inhibited eavesdropping of mobile device data
- 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* can help your organization:

- reduce adverse effects if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- apply robust, standards-based technologies by using industry best practices
- reduce user privacy risks
- provide 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-owned networks, devices, and applications

- reduce risk so that employees can access necessary data from nearly any location by using a wide selection of enterprise-owned mobile devices and networks
- enhance visibility for system administrators into mobile security events, 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/corporate-owned-personally-enabled. 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.

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, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

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