NIST SPECIAL PUBLICATION 1800-4A

Mobile Device Security

Cloud and Hybrid Builds

Volume A:
Executive Summary

Joshua Franklin
National Institute of Standards and Technology
Information Technology Laboratory

Kevin Bowler
Christopher Brown
Spike E. Dog
Sallie Edwards
Neil McNab
Matthew Steele
The MITRE Corporation
McLean, VA

February 2019

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-4

The original draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Executive Summary

- Adopting mobile devices without the necessary policies and management infrastructure in place increases the opportunities for attackers to breach sensitive enterprise data.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed example mobile device and enterprise mobility management solutions that organizations can use to reduce the likelihood of a data breach.
- The security characteristics in this guide are informed by guidance and best practices from standards organizations.
- The NCCoE's approach uses commercially available products that can be included alongside your current products in your existing infrastructure.
- The example solutions are packaged as a "how to" guide that demonstrates implementation of standards-based, commercially available cybersecurity technologies in the real world. The guide helps organizations utilize technologies to reduce the risk of intrusion via mobile devices while saving them research and proof of concept costs.

CHALLENGE

Information technology (IT) environments have changed drastically because of the increasing popularity of smartphones, tablets, and other highly capable, rapidly maturing mobile devices. These devices have many functional similarities to traditional IT systems — including access to a wide range of enterprise applications and data, as well as additional functionality particular to mobile computing. This has greatly expanded the utility and value of mobile devices, enabling employees to do their jobs more effectively and efficiently. Unfortunately, security controls have not kept pace with the security risks that mobile devices can pose, not only in bring your own device (BYOD) scenarios but also in corporately owned and personally enabled (COPE) mobile device deployments, where mobile devices are adopted on an ad hoc basis. This gap in protection mechanisms means that data stored on or accessed from mobile devices is at increased risk of being breached.

For example, suppose that an organization has enabled mobile access to its email, calendaring, and contact management services regardless of the origin of the employees' mobile devices (organization-owned and employee-owned, organization-provisioned and employee-provisioned, etc.). If sensitive data is stored on a poorly secured mobile device that is lost or stolen, an attacker may be able to readily gain unauthorized access to that data. Even worse, a mobile device with remote access to sensitive organizational data could be leveraged by an attacker to gain unauthorized access to not only that data but also any other data that the user can access from a mobile device.

SOLUTION

The NIST cybersecurity practice guide *Mobile Device Security: Cloud and Hybrid Builds* demonstrates how commercially available technologies can meet your organization's needs to secure sensitive enterprise data accessed by and/or stored on employees' mobile devices.

In our lab at the NCCoE, part of the National Institute of Standards and Technology (NIST), we built an environment based on typical mobile devices and an enterprise email, calendaring, and contact management solution.

We demonstrate how security can be supported throughout the mobile device life cycle. This includes how to configure a device to be trusted by the organization, how to maintain adequate separation between the organization's data and the employee's personal data stored on or accessed from the mobile device, and how to handle de-provisioning a mobile device that should no longer have enterprise access (e.g., device lost or stolen, employee leaves the company).

This guide…

- identifies the security characteristics needed to sufficiently reduce the risks from mobile devices storing or accessing sensitive enterprise data
- maps security characteristics to standards and best practices from NIST and other organizations
- describes two detailed example solutions, along with instructions for implementers and security engineers on installing, configuring, and integrating the solutions into existing information technology (IT) infrastructures
- selects mobile devices and enterprise mobility management systems that meet the identified security characteristics
- provides example solutions that are suitable for organizations of all sizes, and evaluates those solutions3

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 to *Mobile Device Security: Cloud and Hybrid Builds* can help your organization…

- reduce risk so that employees can access the necessary enterprise data from nearly any location, over any network, by using a wide variety of mobile devices
- enable the use of BYOD, COPE, and other mobile device deployment models, which may provide cost savings and increased flexibility for organizations
- leverage cloud services to secure sensitive corporate data that uses the latest industry best practices and defense-in-depth security strategies, which may reduce infrastructure costs for organizations
- enable identity federation between an on-premise identity store and associated cloud services, which may improve user experience and enhance enterprise security
- enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implement industry standard mobile security controls, reducing long-term costs and decreasing the risk of vendor lock-in

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-4.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid. 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 implementation.

intel Lookout Microsoft Symantec.

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://nccoe.nist.gov
nccoe@nist.gov
301-975-0200