Mobile Device Security: Cloud and Hybrid Builds

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) developed an example mobile device and enterprise mobility management solution 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 solution is 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.

THE CHALLENGE

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 information technology (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 is allowed to access from a mobile device.

THE 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 the deprovisioning of a mobile device that should no longer have enterprise access (e.g., device lost or stolen, employee leaves the company.)

The 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 a detailed example solution, along with instructions for implementers and security engineers on installing, configuring, and integrating the solution into existing IT infrastructures
- selects mobile devices and enterprise mobility management (EMM) systems that meet the identified security characteristics
- provides an example solution that is suitable for organizations of all sizes and evaluates the solution

While we have 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

Our example solution has several benefits, including the following:

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

SHARE YOUR FEEDBACK

You can get the guide at http://nccoe.nist.gov and help improve it by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email mobile-nccoe@nist.gov
- participate in our forums at https://nccoe.nist.gov/forums/mobile-device-security

Or learn more by arranging a demonstration of this example solution by contacting us at mobile-nccoe@nist.gov.

TECHNOLOGY PARTNERS

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partnership (NCEP) partners.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. As the U.S. national lab for cybersecurity, the NCCoE seeks problems that are applicable to whole sectors, or across sectors. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE
http://nccoe.nist.gov

ARRANGE A DEMONSTRATION
nccoe@nist.gov
240-314-6800