BUILDING BLOCK

MOBILE DEVICE SECURITY FOR ENTERPRISES

Draft
February 21, 2014
mobile-nccoe@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest including vendors of cybersecurity solutions. The solution will become an NCCoE "building block": an approach that can be incorporated into multiple use cases. The solution proposed by this effort will not be the only one available in the fast-paced cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at mobile-nccoe@nist.gov.

1. DESCRIPTION

Goal

Traditionally, enterprises have established a boundary separating their trusted internal network(s) and untrusted external networks. The consumption and generation of corporate information on mobile devices erodes this traditional boundary. Faced with a rapidly changing array of mobile platforms, corporations must ensure that mobile devices connected to the enterprise can be trusted to protect sensitive corporate data as it is stored, accessed or processed on the device, without compromising the end user's experience.

This building block will demonstrate commercially available technologies that provide enterprise-class protection to both organization-issued and personally-owned mobile platforms. These technologies enable users to work inside and outside the corporate network with a securely configured mobile device, while allowing for granular control over the enterprise network boundary, and minimizing the impact on function. The architecture demonstrated by this building block will incorporate a layered technology stack that allows enterprises to tailor solutions to their business needs.

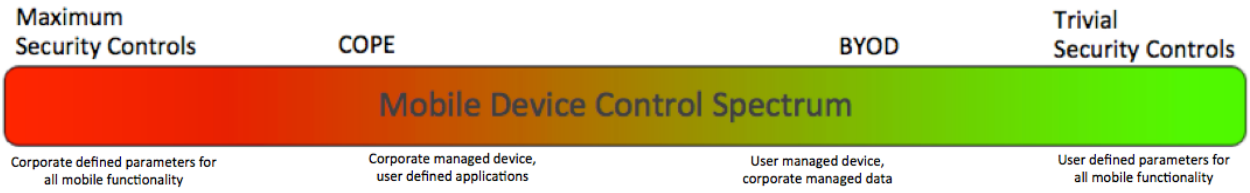
Background

In the past decade, mobile devices have significantly changed business capabilities, allowing employees access to information resources wherever they are, whenever they need to. These devices are both an opportunity and a challenge. While their unique capabilities—including their always-on, always-connected nature—can make business practices more efficient and effective, mobile devices create new challenges to ensure the confidentiality, integrity and availability of information they access.

As these technologies mature, employees increasingly want to use both corporate-issued and personally-owned mobile devices to access corporate enterprise services, data and resources to perform work-related activities. Enterprises are under pressure to accept the associated security risks inherent in today's mobile devices because of several factors, including anticipated cost savings and employees' desire for greater convenience.

2. SCENARIOS

This building block will demonstrate security capabilities that can provide greater assurance that a mobile device can be trusted to protect data stored, accessed or processed on the device. Understanding that every organization makes decisions regarding access to its resources based on an analysis of its enterprise risk posture, these solutions envision tools that support an array of security controls. This building block addresses two scenarios, bring your own device (BYOD) and corporate-owned, personally enabled (COPE), that provide fine-grain control over the resources available on the mobile device.



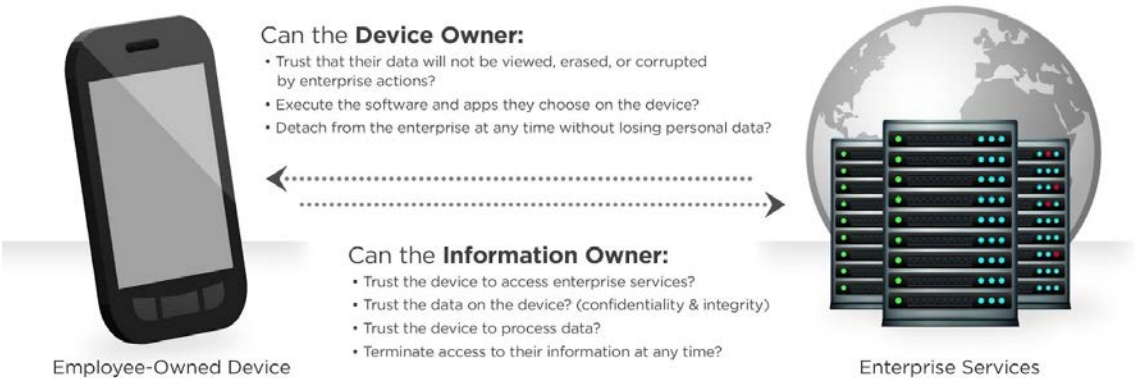
Example Scenario 1 - Bring Your Own Device (BYOD)

An employee wishes to use her personal mobile device (e.g., smart phone or tablet) to access corporate information resources, namely her e-mail, calendar, contacts and files. While she wants to retain control of the mobile device for her personal use, she also recognizes that her company needs assurance that her device will protect corporate information, and will likely have certain security requirements and policies that need to be employed and enforced by the device.

Before the employee can use her device to access corporate resources, it will need to be provisioned by the company. The provisioning step allows the company to verify the mobile device has not been tampered with in a way that would compromise the security of the device, establish user and/or device credentials, and configure its required security controls on the device. To minimize cost and maximize convenience, the provisioning step should be able to be performed remotely.

Before accessing corporate resources, users should be authenticated using a high assurance authentication method, such as those relying upon hardware-protected credentials. Sensitive information should be protected in transit, as well as encrypted at rest.

Corporate data and company-specific applications that are made available based on an enterprise risk analysis should be logically separated from the personal data and applications on the mobile device. Should the employee lose the device, the company should be capable of selectively wiping data from the device.



Example Scenario 2 – Corporate-Owned, Personally Enabled (COPE)

An enterprise has increased security needs due to the sensitive nature of information generated by its business activities and needs to acquire mobile devices for users for both corporate and personal data. In the past, the enterprise provided users with secured mobile devices; however, the consumerization of mobile technology has set user expectations for mobile devices to function past the feature set typically offered by the enterprise's corporately controlled devices. As a result, users are seeking out and using third party devices or applications with corporately owned data to obtain the additional functions that meet their personal and productivity needs.

Given the heightened security controls required to protect the company's sensitive data, the IT department decides to provide and maintain corporately owned devices. However, the corporation recognizes that a strict set of security controls may encourage users to take corporate data outside the organization's span of control. Therefore, the enterprise seeks a mobile management solution that will meet its enhanced security needs without encumbering the user experience.

Prior to deploying the mobile device, corporate IT staff provisions a security configuration. This allows the company to establish a security baseline and implement device and application layer policies. The device is updated with the latest software release and any applicable corporate applications.

The device is encrypted and secure containers are configured and ready for management. Application and/or device VPN credentials are issued and connectivity tested.

3. Security Characteristics

Specific methods for accomplishing the two scenarios focus on securing this technology solution stack:

- mobile device and application management
- mobile devices
- mobile applications

Each layer of the stack has multiple characteristics that are considered attributes of a secure solution. Each characteristic has one or more examples of security capabilities that would meet the intent of the characteristic. The below list of characteristics and corresponding capabilities is not exhaustive. Furthermore, capabilities are defined to provide context for the characteristics and are not meant to be prescriptive.

All characteristics should be implemented with a very high degree of assurance. To provide high assurance, there should be continued assertions that the integrity of the device has not been compromised (e.g., that key firmware or operating system files have not been tampered with, that the device has not been "rooted" or "jail broken," and that the device's security policies are verified as those being issued by the enterprise).

Mobile Device and Application Management

Mobile device and application management describes information systems and software used to enroll a mobile device into an organization's enterprise network, set policy, distribute applications and protect data within the mobile device. Desired security characteristics and example capabilities for mobile device and application management include:

Security characteristics	Example capabilities
data protection	• remote wipe: remotely render access to corporate data stored on the device infeasible • create and manage secure containers
device provisioning	• no-touch provisioning: enroll a user-owned device remotely • device identity verification: assure that the enrolling device is authorized for enrollment and belongs to a valid user
software update management	• application delivery and updates: push application and OS patches, as well as new applications, to the device • system updates: distribute the newest releases of corporate applications and security software

policy management	• define and deliver policies to mobile devices, for example: o remotely enable/disable device peripherals o password/PIN policy requirements o application black/white listing o geo-fencing: enforce policies based on the geographic location of the device o encrypted communications, e.g., encrypted and signed e-mail o file share restrictions, e.g., downloading e-mail attachments
asset management	• keep record of device make and model, device owner, current software versions, and installed corporate applications
monitoring and alerting	• canned reports and ad-hoc queries • compliance checks: provide information about whether a device has remained compliant with a mandated set of policies • auditing and logging: capture and store device and application information • root and jailbreak detection: ensure that the security architecture for a mobile device has not been compromised • anomalous behavior detection: observe activities of mobile users, devices and processes, and measure those activities against a baseline of known normal activity

107

108 ## Mobile Device Security

109 The mobile device consists of hardware, firmware and an operating system. Depending
110 on how the operating system is architected, certain capabilities such as policy
111 enforcement may reside at the application level. Desired security characteristics and
112 example capabilities for mobile device security include:

Security characteristics	Example capabilities
device integrity	• boot validation • application verification • verified application and OS updates: equipped with newest releases of corporate and OS and can verify the integrity of the updates before installation • baseband integrity • trusted device integrity reports • policy integrity verification
data, application, memory isolation	• virtualization • sandboxing • containers
data protection	• VPN (including per-app VPN): set up to require users to rely on a VPN connection to access parts of the corporate network that house sensitive functions and/or data • device encryption: equipped with encryption that protects corporate data when in transit (e.g., via cellular, WiFi, Bluetooth, or near field communication) • protected storage (key hierarchy) • hardware security modules
policy enforcement	• examples of desired enforceable policies include: o remotely enable/disable device peripherals o password/PIN policy requirements o application black/white listing o geo-fencing: enforce policies based on the geographic location of the device o encrypted communications, e.g., encrypted and signed e-mail o file share restrictions, e.g., downloading e-mail attachments

113

Mobile Application Security

Mobile applications run atop and leverage the capabilities provided by the mobile OS platform. Depending on an application's requirements, additional security capabilities may be needed to ensure the confidentiality, integrity and availability of information. Desired security characteristics and example capabilities for mobile application security include:

Security characteristics	Example capabilities
data protection	• protected storage: secure data stores are accessible only by the application • per app VPN: establish a secure tunnel between the application and the application server
policy enforcement	• application data tagging: as data is accessed by a mobile application, policies relevant to that data are transmitted simultaneously and enforced on that data by the application
device integrity	• validation of the device integrity during application launch
authorization and authentication	• local user authentication • remote authentication to the application server

4. Approach

This building block demonstrates a commercially available technology solution stack that addresses the security challenges that mobile devices present to an enterprise. This project will first address the implementation of the mobile device and application management layer to serve as the foundation for many of the desired security characteristics of this building block. Understanding that the implementation of the aforementioned security characteristics will span multiple layers of the technology stack, several layers may be worked in parallel, as dictated by requirements of the specific characteristic. In order to address a full array of mobile platforms and technologies, several initial builds may occur as part of this building block. Throughout the build process the implementation of all security characteristics shall be mapped to their corresponding security controls found in the standards in Section 6 of this document.

Note that this is an initial approach and that the building block process is intended to be iterative. As mobile technologies and capabilities evolve, the initial technology stack of this building block may be augmented with additional functionality.

Stage 0: Mobile Device and Application Management

- install and configure a mobile device management/mobile application management (MDM/MAM) solution
- verify, provision and enroll mobile devices
- develop and push policies to mobile devices
- remotely update/patch operating system and applications
- configure and manage a secure container
- demonstrate full and selective remote wipe capabilities
- pull and aggregate log and audit data from a mobile device

Stage 1: Mobile Device Security

- implement full disk encryption on device
- implement boot and policy integrity checks
- configure sandboxing, virtual containers or any other data separation mechanisms
- configure, implement and validate policy enforcement engine
- implement device VPN capability

Stage 2: Mobile Application Security

- configure per app VPNs
- demonstrate the functionality of application sandboxes
- implement per app authentication
- demonstrate the functionality of application data tagging

5. Business Value

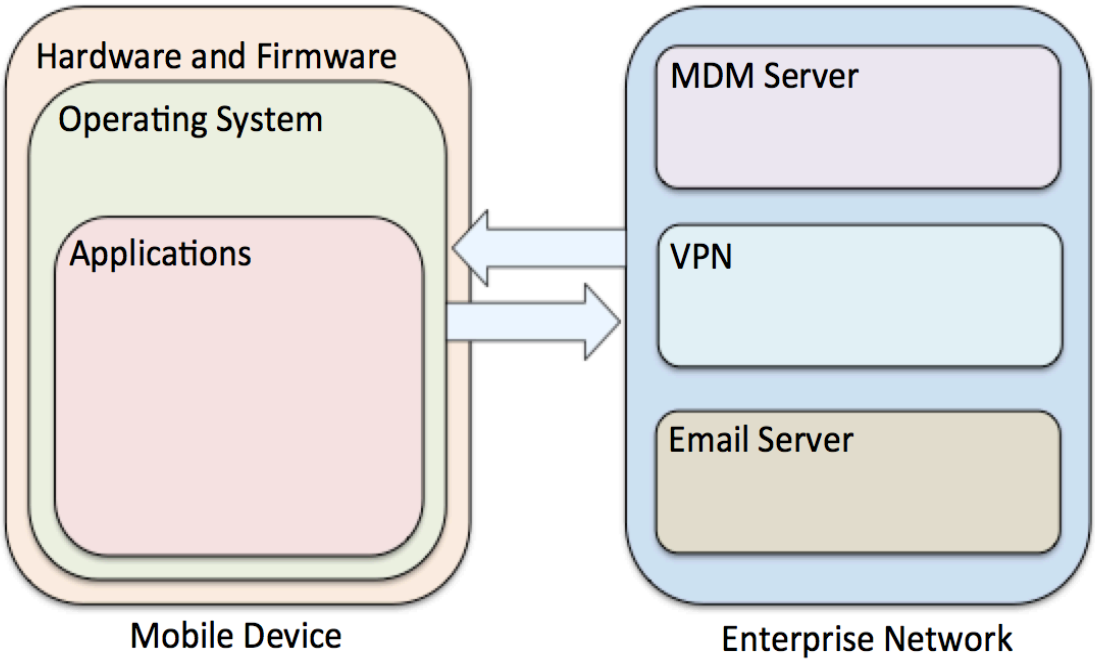
- provides enterprise-class protection to users who need to access untrustworthy cellular and WiFi networks, peripherals, apps, and web sites
- enables users to work inside and outside the corporate network with a hardened mobile device that is unlikely to adversely affect an enterprise
- reduces total outlays in redundant enterprise network security systems by improving security of mobile devices
- helps companies embrace BYOD model and reduce corresponding capital investment by increasing security on user mobile devices
- broadens visibility of users' behavior in accessing and working on corporate networks in order to bolster identity and access management capabilities

6. Relevant Standards

- NIST SP 800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-164, Guidelines on Hardware-Rooted Security for Mobile Devices
- Global Platform Secure Element and Trusted Execution Environment Specifications
- Trusted Computing Group Trusted Platform Module and Trusted Network Connect Specifications
- NIST SP800-147: BIOS Protection
- NIST SP800-155: BIOS Integrity Measurements
- NSA Mobility Capability Package 2.2
- DoD Mobility Implementation Plan
- NIAP Protection Profiles for Mobile Device Management Systems
- NIAP Protection Profiles for Mobile Devices
- Digital Government Strategy Mobile Security Baseline
- GSA Managed Mobility Program Request for Technical Capabilities

7. High-Level Architecture

Although there are two distinct scenarios within this building block, the general architecture for how a mobile device will access data and services on an enterprise network is depicted below.



8. Component List

- mobile device (e.g., smartphone, tablet) with hardware security features outlined in NIST SP 800-164
- MDM system
- MAM system
- mobile applications requiring security assurance
- enterprise infrastructure (e.g., directory server, VPN gateways, internal network)
- identity management system