Draft NIST Special Publication 800-124
Revision 2

Guidelines for Managing the Security of Mobile Devices in the Enterprise

Joshua M Franklin
Gema Howell
Vincent Sritapan
Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-124r2-draft

C O M P U T E R   S E C U R I T Y

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

Draft NIST Special Publication 800-124 Revision 2

Guidelines for Managing the Security of Mobile Devices in the Enterprise

*Joshua M Franklin
Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Vincent Sritapan
Science and Technology Directorate
Department of Homeland Security

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-124r2-draft

March 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by non-governmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-124 Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-124 Rev. 2, 59 pages (March 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-124r2-draft

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: ***March 24, 2020 through June 26, 2020***

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000), Gaithersburg, MD 20899-2000
Email: 800-124comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Mobile devices were initially personal consumer communication devices but they are now permanent fixtures in enterprises and are used to access modern networks and systems to process sensitive data. This publication assists organizations in managing and securing these devices by describing available technologies and strategies. Security concerns inherent to the usage of mobile devices are explored alongside mitigations and countermeasures. Recommendations are provided for deployment, use and disposal of devices throughout the mobile-device lifecycle. The scope of this publication includes mobile devices, centralized device management and endpoint protection technologies, while including both organization-provided and personally owned deployment scenarios.

Keywords

enterprise mobility management (EMM); mobile; mobile device management (MDM); mobile security; smartphones; tablets.

Acknowledgments

The authors wish to thank the Federal CIO Council's Mobile Technology Tiger Team and the Advanced Technology Academic Research Center (ATARC) Mobile Working Groups. The authors especially appreciate the contributions of Wayne Jansen, who coauthored the original version of this publication. The authors also thank all the individuals and organizations that provided comments on the publication, including Andrew Regenscheid and Nelson Hastings of NIST; Jeffrey A. Myers of the Department of Homeland Security (DHS); Deborah Shands and Kareem Eldefrawy of SRI International; and Michael Peck and Terri Phillips of MITRE.

Trademarks

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: 800-124comments@nist.gov

Executive Summary

Modern mobile devices, which are essentially general-purpose computing platforms capable of performing tasks far beyond the voice and text capabilities of legacy mobile devices, are widespread within modern enterprise networks. Mobility has transformed how enterprises deliver information technology (IT) services and ensure mission impact. Targeted toward consumers for on-demand personal access to communications, information, and services, these devices are not configured by default for business use. As mobile devices perform everyday enterprise tasks, they regularly process, modify, and store sensitive data. While organizations understand that using mobile devices and mobile applications for anytime, anywhere access can increase employee productivity, enhance decision making and situational awareness, they may also consider that these devices bring unique threats to the enterprise.

While consumers and enterprise organizations have increased their adoption and use of mobile technologies, the mobile threat landscape has also shifted. This includes an increase in mobile malware and vulnerabilities that span the device (e.g., operating system, firmware, the baseband processor used to access cellular networks), mobile apps, networks, and management infrastructure. The diversity and complexity of the mobile ecosystem and the rapid pace of change offers challenges to selection, integration, and management of mobile technologies into an enterprise IT environment. To reduce risk to sensitive data and systems, federal enterprises need to institute the appropriate policies and infrastructure to manage and secure mobile devices, applications, content, and access.

Mobile devices often need additional protections as a result of their portability, small size, and common use outside of an organization’s network, which generally places them at higher exposure to threats than other endpoint devices. Laptops are excluded from the scope of this publication. Although some laptop/desktop management technologies are converging with mobile device management technologies, the security capabilities currently available for laptops are different than those available for smartphones, tablets, and other mobile device types. Further, mobile devices contain features not generally available in laptops (e.g., multiple wireless network interfaces, Global Positioning System, numerous sensors, and built-in mobile apps). Devices with minimal computing capability, such as the most basic cell phones and general Internet of Things (IoT) devices are also out of scope because they typically do not have a full-fledged operating system (OS), and limited functionality and limited security options are available.

Organizations should implement the following guidelines to improve the security of their mobile devices.

Organizations should conduct a threat analysis for mobile devices and any information systems accessed from mobile devices.

Before designing and deploying mobile device solutions, organizations should conduct a threat assessment for managing and using mobile devices and mobile apps to access and process sensitive data. Threat modeling involves identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, quantifying the likelihood of successful attacks and their impacts, and then synthesizing this information to determine where security controls need to be improved or added to mitigate the threats. General security recommendations for any IT technology are provided in NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* [1]. Specific controls for securing mobile devices are presented in an appendix of this publication.

Threat models such as NIST's Mobile Threat Catalogue [5] and its associated NIST Interagency Report (NISTIR) 8144, *Assessing Threats to Mobile Devices & Infrastructure* [6] used in conjunction with a threat modeling process such as draft NIST SP 800-154, *Guide to Data-Centric System Threat Modeling* [48] can help organizations identify security requirements and design mobile device solutions to incorporate the necessary controls to meet the security requirements. See also the Department of Homeland Security's Congressional report, *Study on Mobile Device Security* [23], for additional threat information on mobile device security for federal agencies.

Organizations should employ Enterprise Mobility Management, Mobile Threat Defense, and other applicable enterprise mobile security technologies.

The reliance on mobile devices to access and process enterprise information requires a comprehensive solution for mitigating threats to the organization's information and systems from use of mobile devices. Enterprise Mobility Management (EMM) systems are a suite of products used to deploy, configure and actively manage mobile devices in an enterprise environment. They are central to an enterprise mobile security solution and can be used to control the use of both organization-issued and personally-owned mobile devices by enterprise users. In addition to managing the configuration of mobile devices, these technologies offer other features, such as controlling access to enterprise computing resources.

By integrating EMM with enterprise backend services such as authentication, an organization can enable more granular management of mobile device access to mission-critical enterprise resources. System administrators can set policy-based configurations for mobile devices to constrain access to sensitive resources, depending on mobile device conditions (e.g., device connecting from a public WiFi network, jailbroken or rooted device, user-managed device running a corporate application). EMM systems should be integrated with Mobile Threat Defense (MTD) systems to protect the mobile endpoint. MTD systems can detect the presence of malicious apps or operating system (OS) software, known vulnerabilities in software or configurations, and connections to blacklisted websites/servers or networks. The integration of MTD with EMM enables administrators or defense systems to remediate detected vulnerabilities or quarantine applications or devices.

EMM systems can also be extended to provide Mobile Application Vetting (MAV) capabilities using tools that perform enterprise-level security analysis of managed apps and their libraries prior to deployment and throughout the lifecycle of the apps. Vulnerabilities or malicious code discovered prior to deployment can be referred to the developer, or the app may be disallowed for use on the organization's devices or within the enterprise mobile appstore. If vulnerabilities or malicious code are discovered after an app has been deployed or updated, the administrator is informed and offered the option to deploy various EMM remediation actions.

Organizations should leverage the Enterprise Mobile Device Deployment Lifecycle where applicable.

Organizations may wish to consider a number of key steps in the deployment process of the Enterprise Mobile Device Deployment Lifecyle before putting mobile devices in the hands of users or allowing users to access enterprise resources via a mobile device. The lifecycle contains guidance on selecting a deployment model (e.g., enterprise use only, organization-managed with personal use allowed, or bring your own device), device and EMM selection, conducting a risk assessment, and device and EMM configurations. Each step of the lifecycle discusses numerous security considerations—such as ensuring an accurate inventory of devices, selecting devices supported by the vendor for OS and app updates and patches, securely configuring devices, selecting an EMM and applying security policies to the device, verifying configuration each time the user attempts to access the network, and integrating EMM into existing identification, authentication and remote access infrastructure.

Organizations should implement and test a pilot of their mobile device solution before putting the solution into production.

Any new mobile device solution should be tested before use. This includes in a laboratory or test environment and subsequently with a small group of users. Aspects of the solution that should be evaluated for each type of mobile device include connectivity, protection, authentication, application functionality, solution management, logging and performance. The enterprise should carefully consider whether the proposed solution meets the predetermined functional and technical requirements, alongside helping to meet stated policy and security objectives.

Organizations should fully secure each organization-issued mobile device before allowing a user to access the organization's systems or information.

For newly deployed mobile devices, organizations should enroll and configure the device in an EMM solution. Baseline profiles are available in industry, but the precise profile to be deployed should be tailored based on an organization's needs and risk assessment. Commercial programs are available to simplify device enrollment and enforce security and configuration policies prior to provisioning; in-house programs can be leveraged to accomplish this task as well. This ensures a basic level of trust in the device before first use. For already-deployed, organization-issued mobile devices with an unknown security profile (e.g., unmanaged device), organizations should fully secure them to a known good state (for example, through deployment and use of EMM technologies using the latest mobile OS). Supplemental security controls, such as MTD, MAV, and Data Loss Prevention (DLP) technologies, should be deployed per results of mobile device risk assessment.

Organizations should keep mobile operating systems and apps updated.

As with any technology, vulnerabilities in mobile devices or OSs are discovered quite often—particularly with broadly deployed devices or OSs. Attackers seeking to gain access to sensitive personal or business information will exploit vulnerabilities in the mobile OS, device firmware, or app. OS and firmware vendors produce security updates to fix the vulnerabilities, and app developers often produce mobile app patches and updates to fix known vulnerabilities. Organizations can use EMM and mobile app management solutions to maintain an inventory of their mobile devices, OSs, and deployed apps, enabling them to identify vulnerable mobile devices. Organizations may have a vulnerability management system in place that allows them to continuously check for these patches and updates and immediately apply them to the mobile devices within their enterprise.

Organizations should regularly maintain mobile device security.

Organizations should perform periodic assessments to confirm that their mobile device policies, processes and procedures are being followed. Assessment activities may be passive, such as reviewing device and management infrastructure (e.g., EMM) logs, or active, such as performing vulnerability scans or penetration testing of the mobile management infrastructure. Operational processes to maintain device security include checking for upgrades and patches and acquiring, testing and deploying them; ensuring each mobile device infrastructure component has its clock synced to a common time source; verifying that device and infrastructure audit logs are collected and sent to the enterprise's security logging system; reconfiguring access control features as needed; and detecting and documenting anomalies within the mobile device infrastructure, including unauthorized configuration or policy changes to mobile devices. Additional maintenance processes include keeping an active inventory of each mobile device, its user and its apps; revoking access to or deleting installed apps that have subsequently been assessed as too risky to use; and scrubbing sensitive data from mobile devices before reissuing them to new users.

Table of Contents

List of Figures and Tables

1. Introduction

Mobile devices are no longer new to the workplace. Modern mobile devices are essentially general-purpose computing platforms capable of performing tasks far beyond the voice and text capabilities of legacy mobile devices. Smartphones and tablets process enterprise information and are regularly included in the design phase of modern network architectures. Multiple mature mobile operating systems are available in the marketplace and have a variety of functionality to secure these devices in the workplace. New mobile technologies for the enterprise are still being introduced. Full parity does not yet exist when comparing the management technology available for traditional desktop environments and those afforded to security professionals to secure their mobile devices – although they are constantly evolving and maturing.

1.1 Purpose

The purpose of this publication is to assist organizations with managing and securing mobile devices. This publication provides recommendations for selecting, implementing, and managing devices throughout their lifecycle via centralized management technologies. Additionally, security concerns inherent to mobile devices are explored alongside mitigation strategies. This approach includes protecting enterprise information such as email, contacts and calendar, which are some of the most commonly used applications in the workplace. This can be expanded to include protection of enterprise-developed and third-party applications, and the sensitive enterprise data they store and process. Recommendations also are provided for deployment, use, and disposal of devices throughout the mobile device lifecycle. This publication can be used to inform risk assessments, build threat models, enumerate the attack surface of the mobile infrastructure, and identify mitigations for mobile deployments.

1.2 Scope

This publication is scoped to managing modern mobile devices in the enterprise. Mobile devices primarily include smartphones and tablets, but also include other devices running a modern mobile operating system (OS). Laptops are specifically excluded from the scope of this publication as the security controls available today for laptops are quite different than those available for smartphones, tablets and other mobile-device types. Mobile devices with minimal computing capability are excluded, including feature phones, wearables and other devices included under the Internet of Things (IoT) umbrella. This document does not discuss the mechanisms needed to evaluate the security of mobile applications [2] or those needed to securely deploy and maintain a cellular network [3]. Unique feature sets available in specialized areas (e.g., construction, public safety, medical) are not analyzed or discussed.

1.3 Audience

This document is intended for information security officers, information security engineers, security analysts, system administrators, chief information officers (CIOs), and chief information security officers (CISOs). Other organization personnel may find this document helpful, such as security managers, engineers, analysts, administrators and others who are responsible for planning, implementing and maintaining the security of mobile devices. It assumes that readers have a basic understanding of mobile device technologies, networking, and enterprise security principles.

1.4 Document Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 provides an overview of mobile devices, focused on what makes them different from other computing devices, particularly in terms of security.
- Section 3 discusses threats to enterprise use of mobile devices.
- Section 4 presents an overview of mobile security technologies and discusses mitigations and countermeasures to the threats listed in Section 3.
- Section 5 discusses security throughout the mobile device lifecycle. Examples of topics addressed in this section include mobile device security policy creation, design and implementation considerations, and operational processes that are particularly helpful for security.
- The References section contains a list of references cited in this document.

The document also contains the following appendices with supporting material:

- Appendix A defines selected acronyms and abbreviations used in this publication.
- Appendix B lists the major controls from NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* and the subcategories from the *NIST Cybersecurity Framework* that affect enterprise mobile device security.

1.5 Document Conventions

The following conventions are used throughout this document:

- Smartphone and appstore are both written as a single word,
- The term app is used in place of mobile application, and
- WiFi is written without the hyphen.

2. Overview of Mobile Devices

This section defines what a modern mobile device is, outlines characteristics of mobile devices, and discusses their underlying architecture. Understanding the full composition of a mobile device is useful in defining the threats facing these information systems. This section also provides an overview of the built-in security capabilities such as isolation, communication and authentication mechanisms.

2.1 Mobile Device Definition

Mobile devices are essentially general-purpose computing platforms. They are not restricted to performing one operation and can instead be used in many different domains—including medical, industrial and entertainment. NIST Special Publication (SP) 800-53 Revision 4 [1] defines a mobile device as:

A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations.

This definition emphasizes portability, wireless communication, local storage and long battery life—all of which exist in modern smartphones and tablets. It's common for these systems to have an always-on cellular connection, but this feature is not shared by all mobile devices. In fact, many tablets lack a cellular modem, yet still run a mobile OS. It also is not a requirement that mobile devices run applications or *apps*, although this capability is commonplace. Applications are used to expand a mobile device's basic functionality.

2.2 Mobile Device Characteristics

Commercially available mobile devices lack a unified set of features. Each feature and characteristic has the potential to introduce new threats to security and privacy, so it is important to establish a baseline understanding of the set of characteristics that are common to mobile devices. The following list explores the baseline characteristics of a mobile device for the purposes of this publication:

- Operating system: A mobile device comes with a rich OS that can be used in a variety of ways. This is the primary distinction between mobile devices and IoT devices, which typically do not have a full-fledged OS and have limited functionality.
- Small form factor: The size of a mobile device allows for easy portability.
- Self-contained power source: Mobile devices traditionally house a self-contained power source. Some mobile devices are capable of swapping out their battery power source for another.
- Physical port: A physical connection can be used to sync/transfer data or to charge the device. Some phones have wireless charging capabilities.
- Wireless network interface: Mobile devices have at least one wireless network interface for data communications, often offering connectivity to the internet or other data networks.
- Data storage: Mobile devices contain local, built-in and non-removable data storage.
- Apps: A mobile device ships with native apps to handle common operations. Beyond native apps, most mobile devices also support third-party apps, which usually add functionality and significantly expand a device's utility.

- Management capability: Mobile devices include a consistent way to manage the device via MDM Application Programming Interfaces (APIs) or proprietary mechanisms.

The following details other common characteristics of mobile devices. These features do not define the scope of devices included in the publication, but rather indicate features that are particularly important in terms of security. This is not intended to be an exhaustive list:

- Network services: A mobile device may come with additional networking capabilities such as Bluetooth, near-field communications (NFC), and cellular data and voice (e.g., 4G LTE or 5G).
- Camera: Mobile devices may use one or more digital cameras that are capable of capturing photos and video recordings. Cameras also accept biometric input to unlock a device or can interpret non-human readable data formats (e.g., Quick Response [QR] code).
- Sensors: Sensors within a mobile device capture data to perform an operation such as authentication or measurement. Examples are: gyroscope, accelerometer, magnetometer, fingerprint reader, pedometer, infrared, barometer, photometer, and thermometer.
- Speaker and/or microphone: A mobile device usually has a speaker that provides an audio output ability and/or a microphone that provides audio input ability.
- Removable media: Removable media allows for additional data and memory storage on a mobile device, normally provided through a secure digital (SD) card. Removable media also serves as a way to transport data from one mobile device to another device.
- Data synchronization: Mobile devices have built-in features for synchronizing local data with a different storage location (desktop or laptop computer, organization servers, telecommunications provider servers, other third-party servers, etc.)
- Hardware-backed security module: A mobile device uses a hardware module or some portion of a hardware chip to perform cryptographic functions and store sensitive cryptographic keys and secrets.

2.3 Mobile Device Components

Multiple organizations work in concert to provide the hardware, firmware, software, and other technology that make up a mobile device. For smartphones and tablets with cellular capabilities, a separation exists between the hardware and firmware used to access cellular networks, and the hardware and firmware used to operate the general-purpose mobile OS. Users and administrators generally interact with the general-purpose mobile OS that utilizes the *application processor*. The hardware and firmware used to access the cellular network, often referred to as the *telephony subsystem*, typically runs a completely separate real-time operating system (RTOS). This telephony subsystem utilizes a completely separate System on a Chip (SoC) called the *baseband processor*. This often means that a cellular-enabled smartphone is concurrently running multiple OSs.

Other features of the telephony subsystem include the universal integrated circuit card (UICC), international mobile equipment identifier (IMEI), and the international mobile subscriber identity (IMSI). The UICC, also known as the subscriber identity module (SIM) card, stores cryptographic information and personal data and is used to enable access to the cellular network. The IMEI is an identifier specific to a mobile device and is used to uniquely identify a device to the cellular network. The IMSI is used to uniquely identify a subscriber or user on the network. More information on these features can be found in NIST SP 800-187, *Guide to LTE Security* [3].

A set of lower-level systems exist in the form of firmware to initialize the device and load the mobile OS into memory, which includes the bootloader. This initialization firmware may also verify other device initialization code, including device drivers. All of this activity occurs before a user can interact with the device. If the initialization code is modified or tampered with, the device may not properly boot or may function in a simplified mode. Many modern mobile devices contain an isolated execution environment, which is used specifically for security-critical functions [6]. For example, these environments may be used for sensitive cryptographic operations—e.g., to verify integrity—or to support Digital Rights Management (DRM). These environments typically have access to some amount of secure storage that is only accessible within that environment.

The mobile OS enables a rich set of functionality by supporting the use of mobile apps written by third-party developers. Accordingly, it is common for mobile apps to be sandboxed (or securely separated) in some manner to prevent unexpected unwanted interaction between the system, its apps and those apps' respective data. This includes separating user data stored by different apps from interacting with each other. Mobile apps may be written in a native language running close to the hardware, in interpreted languages or in high-level web languages. The degree of functionality of mobile applications is highly dependent upon the application programming interfaces (APIs) exposed by the mobile OS and the frameworks used by the developer. Functionality is also dependent on the level of permissions granted to allow the mobile app to leverage mobile device features, such as the camera or microphone.

This section has described the various technologies which work together to make a mobile device function. Figure 1 illustrates a mental model of the previously discussed layers of a mobile device:

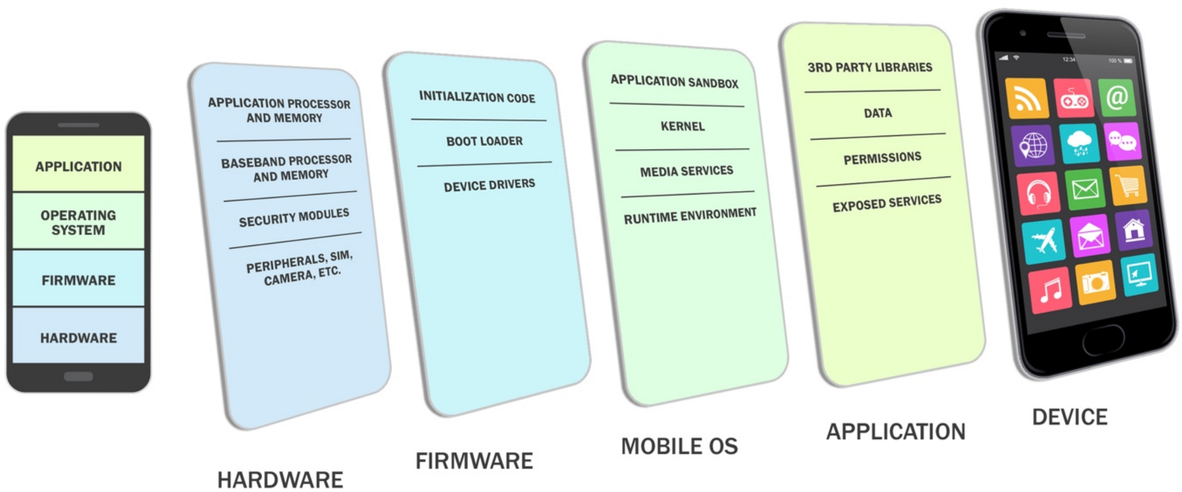

Figure 1 - Mobile Device Components

2.4 Mobile Communication Mechanisms

Mobile devices support a variety of wireless communication protocols such as cellular, WiFi, Bluetooth, global positioning system (GPS) and NFC. Wired physical connections also are commonplace via a power and synchronization cable using micro USB, USB-C and others. Figure 2 depicts some of the communication mechanisms offered by mobile devices.

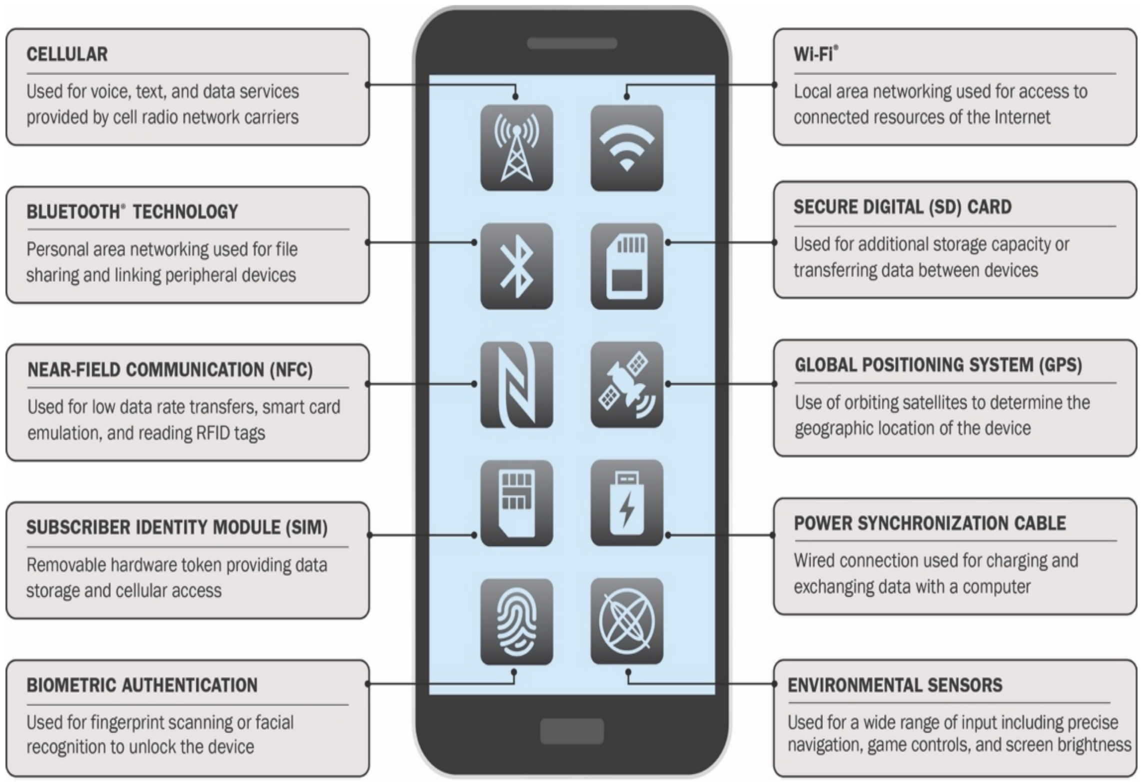

Figure 2 - Mobile Communications Technology

WiFi is a wireless local area network (WLAN) technology and is generally available on most mobile devices. WiFi devices often connect via centralized wireless access point (AP) but can also work in a device-to-device, *ad-hoc* mode. Bluetooth is a short-range wireless communication technology primarily used to establish wireless personal area networks (WPANs). Bluetooth technology is common in consumer mobile devices and can be used to communicate with headsets, wearables, keyboards, mice and other IoT devices. Another form of short-range wireless communication is NFC, which typically is optimized for distances of less than four inches but may be vulnerable at greater distances. NFC is based on the radio frequency identification (RFID) set of standards. Mobile payment technology commonly relies on NFC, which has led to a large increase of use in recent years.

A global navigational satellite system (GNSS) provides worldwide, geo-spatial positioning via GPS. GPS uses line of sight communication with a satellite constellation in orbit to help a handset determine its location. These systems run independently of cellular networks. The U.S. Federal Government operates a GPS constellation, although mobile devices may use other constellations (e.g., Global Navigation Satellite System [GLONASS], Galileo). The U.S. Federal Communications Commission (FCC) mandates that cellular devices must have GPS built-in for public safety and emergency medical reasons. It should be noted the GPS system is not the only way to identify a mobile device's location. Other techniques include cellular positioning, WiFi-assisted positioning, and geolocation of IP addresses.

3. Threats to the Mobile Enterprise

Mobile devices support a series of security objectives, but these can differ based on the organization. These mobile security objectives can be accomplished via a combination of security features built into, installed onto, or managed externally to mobile devices. Achieving an organization's security objectives often requires devices to be secured against a variety of threats. General security recommendations for any IT technology are provided in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [1]. Specific recommendations for securing mobile devices are presented in Section 4.3 of this publication and are intended to complement the controls specified in SP 800-53. See Appendix C of this document for a summary of SP 800-53 controls tailored to mobile enterprise security.

Before designing and deploying mobile device solutions, organizations should develop threat models for all facets of mobile device usage. Threat modeling involves identifying resources of interest and the feasible threats, vulnerabilities and security controls related to these resources; quantifying the likelihood and impacts of successful attacks; and analyzing this information to determine where security controls should be improved or added. Threat modeling helps organizations identify security requirements and design the mobile device solution that incorporates the controls needed to meet the security requirements. The NIST *Mobile Threat Catalogue* [5], a threat modeling process such as draft NIST SP 800-154, *Guide to Data-Centric System Threat Modeling* [48], and the *DHS Study on Mobile Device Security* [23] can be used as a foundation for beginning threat modeling activities. The threats listed in the following sections are mapped to the corresponding threats from the NIST Mobile Threat Catalogue document.

3.1 Threats to Enterprise Use of Mobile Devices

The following threats are related to the general use of mobile devices.

3.1.1 Exploitation of Underlying Vulnerabilities in Devices

Software development is a complex discipline that creates the instruction set that powers mobile devices and apps. In the case of typical software, errors and vulnerabilities exist at an estimated frequency of ~25 errors per 1000 lines of code [33]. There are many definitions for vulnerabilities, but this report leverages the following definition [1]: "*Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source*." Software vulnerabilities will exist at all levels of the mobile device stack. Due to the nature of how mobile devices are developed and manufactured, multiple distinct organizations will contribute software and firmware to the same device. The contributing organizations may or may not have robust software development practices and processes in place. A vulnerability in the code from any of these vendors could potentially compromise the device [25]. An example exploitation is using vulnerabilities in the voice assistance or quick access features to bypass the lockscreen and gain unauthorized access to a mobile device.

NIST *Mobile Threat Catalogue Reference:* STA-0 – STA-11

3.1.2 Device Loss and Theft

Mobile devices are used in a variety of locations outside an organization's control (e.g., building, office) such as employee dwellings, coffee shops, hotels and taxis. Some organizations have strict rules around mobile devices that state that they are only allowed to be used within an organization's perimeters. Yet many organizations have multiple sites, so mobile devices are transported from building to building. The portability of mobile devices makes them more likely to be lost or stolen than traditional desktop systems, and the sensitive data on these devices adds an increased risk of compromise to the organization.

NIST Mobile Threat Catalogue Reference: PHY-0

3.1.3 Accessing Enterprise Resources via a Misconfigured Device

Similar to most other information systems, mobile devices can be misconfigured. The mobile OS contains many security and privacy-relevant configuration options such as the use of a passcode, device encryption, user tracking, and VPN. Unfortunately, not all security- and privacy-relevant settings are located within the security options area of the mobile OS interface. Apps installed on the device also can be configured, sometimes within the administrative area of the device, but also within the app itself. Relevant configurations include authentication to the app, tracking users and the proper use of encryption. Connecting an improperly configured device to an enterprise resource such as a networked drive could lead to information exposure to entities monitoring the network or those improperly accessing the device directly.

NIST Mobile Threat Catalogue Reference: STA-8

3.1.4 Credential Theft via Phishing

Enterprise employees receive emails and text messages to their mobile devices on a daily basis. Sometimes the authenticity of emails and texts can be difficult to determine. Often attackers attempt to steal or request an employee's user credentials through an email or text message. An employee may be tricked into believing the message is from a trusted source and provide their credentials or allow an attacker unauthorized access to their mobile device by clicking a hyperlink within the email or text message. These are examples of phishing on mobile devices.

NIST Mobile Threat Catalogue Reference: AUT-9

3.1.5 Installation of Unauthorized Certificates

Digital certificates are software cryptographic tokens used for authentication and signing software, among other things. These certificates can be distributed to devices through a variety of channels, including web browsers, physical connections (e.g., USB cable) and profiles similar to EMM profiles. Once a certificate is provided to a mobile device's certificate store, it can be used for authentication, and it also can be used for making trust-based decisions about apps by showing warnings to users. The presence of a malicious certificate could trick a user's device into trusting a phishing site or installing a fake phishing or Trojan application such as a banking app.

NIST Mobile Threat Catalogue Reference: ECO-23

3.1.6 Use of Untrusted Mobile Devices

Many mobile devices—particularly those that are personally owned —are not inherently trustworthy. There also is the frequent jailbreaking and rooting of devices, which bypasses built-in restrictions on security, OS use, and other functions. Organizations should assume all mobile devices are untrusted unless the organization has properly secured them and continuously monitors their security while the devices are used to access enterprise apps or data. Untrusted devices are the riskiest mobile devices and oftentimes have access to sensitive enterprise information, and are also the easiest to compromise.

NIST Mobile Threat Catalogue Reference: STA-1

3.1.7 Wireless Eavesdropping

Because mobile devices primarily use non-enterprise networks for internet access, organizations typically will have no control over the security of the external communications networks the devices access. Communications media may include wireless systems such as Bluetooth, WiFi and cellular networks. Bluetooth devices often are used to transmit audio information (e.g., voice traffic, music) as well as notifications and health information from wearable devices [31]. WiFi and cellular can be used to transmit multiple types of traffic, including voice and data. All these network protocols and media are susceptible to eavesdropping and man-in-the-middle (MitM) attacks that can intercept and modify communications between a device and an enterprise system [26].

NIST Mobile Threat Catalogue Reference: CEL-0, CEL-6, CEL-18, LPN-2, LPN-16

3.1.8 Mobile Malware

Mobile devices are designed to make it easy for users to find, acquire, and install third-party apps offered by appstores. This accessibility poses significant security risks, especially for mobile device platforms and appstores that do not place security restrictions or other limitations on third-party app publishing. Organizations should base their mobile device security policy on the assumption that all unknown third-party apps downloaded by its employees to enterprise-accessible mobile devices are untrusted. Any application installed onto a mobile device can act as a portal for the developer to compromise the device and access sensitive enterprise information.

NIST Mobile Threat Catalogue Reference: APP-16, APP-26, APP-43, CEL-33, STA-15

3.1.9 Information Loss Due to Insecure Lockscreen Configuration

The lockscreen is the first barrier an unauthorized user must pass to gain access to information stored on a mobile device. The lockscreen can be configured with a numeric password or pattern to restrict access to the device. If poorly protected with a simple password, the lockscreen may be breached through a brute-force attack. An unauthorized user with access to a mobile device can access all sensitive information, modify the information and pretend to be the device's owner to gain further access to enterprise data.

The lockscreen can also be configured to display quick access to notifications related to missed calls or messages, app alerts, emails received, etc. Information shown on the lockscreen, such as emails, may display sensitive enterprise information. These lockscreen notifications may provide an unauthorized user with information without the need to unlock the mobile device.

NIST Mobile Threat Catalogue Reference: AUT-1

3.1.10 User Privacy Violations

The collection and monitoring of user or employee data can greatly undermine an individual's personal privacy. Many mobile devices and apps collect and monitor user data such as location, contacts, browsing history, and general system information. A common use of this information is for marketing purposes to direct specific advertisements to the user. Mobile applications are not the only systems that collect user information, as most of the business systems (e.g., EMM, MTD) used for mobility may also have this capability, meaning that an employer may collect sensitive information about an employee. Under the Privacy Act of 1974, this type of data collection is allowed as long as the business publicly notifies users of any data it has collected, including PII and other user information [38]. The collection of data without the user's consent hinders confidentiality and is a privacy violation because the collected data may be used in an unwanted manner without the user's knowledge.

One common privacy violation is user location tracking. Location services are commonly used by applications such as social media, navigation and weather apps, as well as web browsers. In terms of organization security and personal privacy, mobile devices with location services enabled are at increased risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are located and to correlate that information with other sources about who the user associates with and the kinds of activities he or she performs in a particular location. Although access to location services can have positive cybersecurity impacts by enabling location-based policies and device configurations, this should require user consent accompanied by a thorough understanding of what type of personal information an enterprise has access to.

NIST Mobile Threat Catalogue Reference: APP-24, APP-36, EMM-7

3.1.11 Data Loss via Synchronization

Mobile devices may interact with other systems to perform data exchange, synchronization, and storage. This can include both local or remote device syncing. Local synchronization generally involves connecting a mobile device to a desktop or laptop computer wirelessly or via a cable. It can also involve tethering such as using one mobile device to provide network access for another mobile device.[1]

Remote system synchronization often involves automatic backups of data to a cloud-based storage system. When all of these components are under the organization's control, risk is generally acceptable. But often one or more of these components are external to the enterprise. Examples include connecting a personally owned mobile device to an organization-issued laptop, connecting an organization-issued mobile device to a personally owned laptop, connecting an organization-issued mobile device to a remote photo backup service, and connecting a mobile device to an untrusted charging station. In all of these scenarios, the organization's data is at risk of being stored in an unsecured location outside the organization's control. In these scenarios, transmission of malware from one device to another also is a possibility.

NIST Mobile Threat Catalogue Reference: EMM-9, STA-6

3.1.12 Shadow IT Usage

Organizations that implement a fully managed mobile device policy should be cognizant of the risks associated with Shadow IT. The term "Shadow IT" typically denotes staff members' work-related use of IT-related hardware, software or cloud services without the knowledge of the IT organization. The canonical example of Shadow IT is a department that performs mission-critical work using an independently purchased server running software that is not approved, managed or even known by the larger IT organization. IT staff may not learn of the existence of this system until it fails or is breached, jeopardizing the critical mission.

Staff members often resort to use of Shadow IT systems when enterprise-provided systems and processes are seen as cumbersome or impeding work, or when the enterprise fails to provide necessary systems. In the mobile systems environment, staff members may be motivated to use personal devices to circumvent restrictive mobile device policies implemented by full enterprise management of enterprise-provided

[1] Organizations should have policies regarding the use of tethering. If an organization permits tethering, it should ensure the network connections involving tethering are strongly protected (e.g., communications encryption). If an organization prohibits tethering, it should configure mobile devices to prevent tethering.

mobile devices. Staff members may send work-related emails or documents to their personal email accounts to better enable access during travel, or they may take pictures of whiteboard drawings with the camera on their personal devices. Staff members may also be motivated to use Shadow IT when enterprise administration practices appear to invade their privacy (e.g., warnings that enterprise system administrators are permitted to monitor all communication from an enterprise-owned mobile phone).

Shadow IT systems do not comply with organizational requirements for enterprise control or documentation and may or may not violate security or reliability policies. In a few cases, a benefit arising from Shadow IT is that some of the technologies, software, or systems become part of the future enterprise due to their benefit in boosting productivity. Organizations should be aware of the potential threats from Shadow IT for which there is no single, complete solution (e.g., EMM technologies do not completely address it), and should treat Shadow IT seriously.

NIST Mobile Threat Catalogue Reference: N/A

3.2 Threats to Device Management Systems

The following threats are related to the use of EMM and other systems used to manage and secure mobile devices. More information describing EMMs can be found later in the document (Section 4.2.1).

3.2.1 Exploitation of Vulnerabilities within the Underlying EMM Platform

EMM infrastructure and subsequent components run on top of commodity hardware, firmware and software—all of which are susceptible to publicly known software and hardware flaws. Although extensive customization of systems occurs, commodity hardware and well-known OSs should be identified and understood. This guidance implies these systems be properly configured leveraging the security configuration guides found in the NIST Checklists repository and regularly patched to remediate known vulnerabilities such as those listed in the National Vulnerability Database [39].

NIST Mobile Threat Catalogue Reference: EMM-1, EMM-2

3.2.2 EMM Administrator Credential Theft

Credential theft is a primary issue for employees, but the credentials of system administrators working the EMM console can also be compromised. If attackers can log into the EMM as an administrator, there could be a loss of sensitive information. For instance, EMMs store a variety of sensitive information about employees at all levels of an organization. Examples include email addresses, phone numbers, user names, assigned resources, levels of access, and potential metadata from voice and text communication. Additionally, EMM administrator credentials allow an attacker to misconfigure and put mobile devices into an insecure state by modifying the policies enforced on the devices. Finally, an attacker may also be able to perform a denial of service (DoS) attack on an enterprise by removing enterprise access for all mobile devices by erasing their records from the EMM.

NIST Mobile Threat Catalogue Reference: EMM-2

3.2.3 Insider Threat

An insider threat originates from an individual—for example, a current or former employee—who uses authorized access to an organization's system to violate the organization's security policy. As an essential tool for secure mobile system administration, an EMM system may be a "double-edged sword." To wit, it may be used both as a mechanism for protecting an enterprise from insider threats (e.g., to implement practices focused on password and account management, access controls, system change controls and app usage policies) as well as an attack vector for a malicious insider. A malicious insider with access to an EMM system could weaken permissions to enable data leaks, enroll unauthorized devices or outsiders, or whitelist malicious apps, among other inappropriate actions. The use of EMM systems and other mobile device administration tools should be monitored carefully to detect possible malicious insider activities.

NIST Mobile Threat Catalogue Reference: EMM-2

3.2.4 Installation of Malicious Developer & EMM Profiles

Installation of EMM profiles enables an enterprise to control privileged operations provided by mobile OSs. There are multiple ways mobile device users can be enrolled into the EMM and profiles distributed. One of the most common is installing an EMM application—sometimes referred to as an MDM agent—directly onto the mobile device. When this setup is completed, end-users can enter information unique to their organization and authenticate to the EMM server. At this point, an EMM profile is presented to the user. This profile contains specific permissions and other resources approved by administrators.

EMM profiles can be conveyed to a user from a variety of avenues such as email, text and drive-by downloads. If a user accidentally accepts a malicious profile delivered via one of these methods, privileged access could be provided to an attacker. Using this access, an attacker can leverage all management APIs to access enterprise data on the device and possibly even information stored on backend infrastructure run by the organization.

NIST Mobile Threat Catalogue Reference: EMM-3, STA-7

4. Overview of Mobile Security Technologies

Mobile security technologies have evolved over the past decade to become full-featured security management suites. New capabilities and features are being added to increase the control administrators have for their enterprise devices. Some of these capabilities are built into the device, whereas others are services provided by external systems residing on more traditional webservers. Device-side security capabilities are introduced in Section 4.1, and are followed by a description of enterprise management technologies in Section 4.2. Recommendations on how to mitigate the threats described in Section 3 through policy, user education, use of security management technologies, and industry best practices are presented in Section 4.3.

4.1 Device-Side Management & Security Technologies

The following sections detail common on-device technologies used to enable management and enhance enterprise security. Note that not all mobile devices share the same functions and security capabilities.

4.1.1 Hardware-Backed Processing & Storage

Many mobile devices contain dedicated hardware components to protect cryptographic keys, passwords, digital certificates, biometric templates and other sensitive information. These hardware components are also frequently used to support the encryption of user data on the mobile devices. Some mobile devices offer dedicated components to perform sensitive operations such as making security decisions (e.g., granting access to a privileged API) or performing cryptographic operations on data. On some platforms, secure data storage and sensitive operations are combined into a single SoC. An example of this for Apple devices is the secure enclave [21], while an Android example is the Trusted Execution Environment (TEE) leveraging ARM TrustZone technology [22].

Although these components may exist on devices, they may not be used by default. Both the OS and/or apps must properly leverage the right APIs to fully utilize the security functions that are provided by the platform. On some platforms, APIs may not be exposed to all developers. Within other platforms, small applications can be developed to run specifically within these restricted security environments.

Finally, devices may use other security modules or elements dedicated to specific tasks. These modules/elements are often meant to provide a secure implementation of a specific task. One example is Apple Pay, which uses a *Secure Element*. The Secure Element is a chip specifically designed to handle certain transactions and encrypt payment information stored on the element.

4.1.2 Data Isolation Mechanisms

Some mobile devices provide data isolation mechanisms to prevent unauthorized access to user and device data. Examples of data isolation mechanisms include encryption and application sandboxing. Isolating data using encryption separates the data based on authorized access. This mechanism means only users possessing the appropriate cryptographic key can access the encrypted data on the device. Modern mobile devices generally encrypt user data, but data may be encrypted with a key that is managed by the OS, and *not* the user, developer or enterprise.

Sandboxing on a mobile device can be implemented in multiple ways. An app sandbox is implemented by the mobile OSs, which generally keeps apps from interacting with each other. Exceptions are made based on well-defined methods explicitly accepted by the user, done by sometimes asking a user if they grant a permission for an application to do a task. Additional sandboxes may exist at or below the user-level that provide an additional layer of data segmentation. While these may be built into the OS, some Original Equipment Manufacturers (OEMs) have decided to develop and ship their own (e.g., Samsung KNOX).

4.1.3 Platform Management APIs

The major mobile OS platforms offer a set of APIs and supporting protocols that can be used by third-party management tools [27][28]. Management APIs offer access to capabilities that are not offered to normal developers such as controlling app behavior, configuring device and security settings, and querying sensitive device information. Access to these APIs may be restricted to a subset of particular developers vetted by the platform owners. Additionally, access to these APIs must be agreed to by either a device's end-user or a member of an organization's IT staff.

The management capabilities offered by the platform owners also are supplemented by external infrastructure, which is discussed further in Section 4.2.1. In some management situations IT administrators are able to directly manage the devices, while in other settings IT administrators send commands to the platform owner's infrastructure, which is subsequently relayed onward to the device. Both of these scenarios can be accommodated within the same management panel and be made invisible to the user.

4.1.4 VPN Support

Mobile platforms natively support virtual private networks (VPNs) that can be leveraged by developers via APIs. VPNs primarily provide confidentiality protection by encrypting user data. There are three types of VPNs: OS-level VPNs, app level-VPNs, and web-based VPNs. OS-level VPNs can be configured via management platforms and sometimes can be put into an "always-on" state. OS-level VPNs may be more power-efficient and can encrypt a large amount of user traffic. Protocols that may be used include Internet Protocol Security (IPsec) and Layer 2 Tunneling Protocol (L2TP). Unlike OS-level VPNs, app-level VPNs can be configured in multiple ways. They can leverage system VPN APIs to protect user data or they may simply protect a single app's data. More complicated setups can deploy VPNs per mobile app, often known as a *per-app VPN*. Finally, web-based VPNs are easy for a user to take advantage of, often by simply agreeing to a web page's policy. Web-based VPNs use Transport Layer Security (TLS) and may not leverage the same additional protections used by other types of VPNs.

4.1.5 Authentication Mechanisms

Mobile devices offer a variety of sensors that can enable standard and biometric-based authentication. Use of biometric authentication on a mobile device may be used in combination with or in substitution of passwords or PINs. Mobile hardware typically does not contain or store raw biometric data. Instead the biometric data is transformed (e.g., tokenized) and may be stored securely, minimizing its susceptibility to reverse engineering. Biometric data typically is encrypted, stored on the device and protected with a key available only to a dedicated security environment. Sensors leveraged for biometric authentication include the following:

- Fingerprint sensor for fingerprint-based authentication,
- Dedicated cameras and other sensors to assist in facial recognition,
- Gyroscope, accelerometer, or pedometer for gait-based authentication, and
- Microphone for voice recognition.

Individual sensors of the same type can be of varying quality and ultimately more or less secure than a similar component. Some sensors are not directly exposed to developers and access decisions are made in proprietary security environments. Although these sensors are most often used for local user authentication, they also can be used for remote authentication. Another mechanism that can be used for remote authentication is a derived personal identity verification (PIV) credential. This is where a mobile device leverages certificate-based authentication through a token that is associated with a PIV credential. Additional information can be found in NIST SP 800-63-3, *Digital Identity Guidelines* [4] and NIST SP 800-157*, Guidelines for Derived Personal Identity Verification* [41].

4.2 Enterprise Mobile Security Technologies

Technology to manage smartphones and tablets can be used to control organization-issued and personally owned devices. This technology can take many forms such as a management tool for device configuration, an application management tool, or a mobile threat defense (MTD) tool. MTD is a category of technology that defends devices from a variety of threats posed to the devices themselves and any connected networks. Other products such as mobile identity management, mobile content management and mobile data management also exist, but are not covered in this publication. This section provides an overview of the current state and use of these technologies, focusing on their components and security capabilities. These technologies form the foundation for the recommended technical threat mitigations and countermeasures in Section 4.3.

4.2.1 Enterprise Mobility Management

EMM is a solution used to deploy, configure and actively manage mobile devices in an enterprise environment. An EMM suite may encompass mobile device management (MDM), mobile application management (MAM) and other management technologies. These management systems are developed by a variety of organizations, including mobile device manufacturers, mobile OS developers, and independent third-party development organizations. EMMs rely on the MDM APIs and protocols described in Section 4.1.3 and employ technologies to monitor mobile devices, track a device's location, deploy device policies, and configure device-side security technologies (e.g., secure containers).

The rest of this subsection contains a list of security capabilities that may be provided by EMMs or any of their supporting systems. Most organizations will not need all of the security capabilities listed in this subsection. Organizations deploying mobile devices should consider the merits of each security capability, determine which services are needed for their environment, and then design and acquire one or more solutions that collectively provide the necessary services for their needs. Additional guidance for implementing these technologies can be found in Section 5.

4.2.1.1 General Policy Enforcement

EMM technology can enforce enterprise security policies on a mobile device, which can configure or restrict the use of mobile functionality and security capabilities. EMM technology can automatically monitor, detect and report when policy violations occur and automatically take action when possible and appropriate. General policy restrictions or configuration options for mobile device security include the following:

- Manage wireless network interfaces (e.g., WiFi, Bluetooth, NFC),
- Restrict user and app access to hardware (e.g., digital camera and removable storage) and device features (e.g., copy and paste),
- Detect changes to the approved security configuration baseline, and

- Limit or prevent access to enterprise services based on the mobile device's OS version (including whether the device has been rooted/jailbroken), vendor/brand, model, or mobile device management software client version (if applicable).

4.2.1.2 User and Device Authentication

User and device authentication can be defined and enforced using EMM technology. Some basic options and considerations include the following:

- Require a password or other authenticator to unlock the device (e.g., passcode, fingerprint, face),
- Require a password/passcode and/or other authentication mechanism (e.g., token-based authentication, network-based device authentication, domain authentication, digital certificate) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device),
- Have the device automatically lock itself after it is idle for a period of time (e.g., 45 seconds, 5 minutes),
- Under the direction of an administrator, remotely lock the device if it is suspected the device is lost or was left in an unlocked state in an unsecured location, and
- Wipe the device after a certain number of incorrect authentication attempts or after a predetermined time interval without it checking into the EMM. Note that the ability to recover via an EMM after it has been wiped is limited.

4.2.1.3 Data Communication and Storage

Protections for data communications and on-device data storage can be defined and enforced using EMM technology. Considerations for these data protections include the following:

- Strongly encrypt data communications between the mobile device and the organization. This encryption is most often accomplished in the form of a VPN (see Section 4.1.4), although it can be established through other uses of secure protocols and encryption,
- Strongly encrypt stored data on both built-in storage and removable media storage. Removable media also can be "bound" to particular devices so encrypted information only can be decrypted when the removable media is attached to that specific device, thereby mitigating the risk of offline attacks on the media,
- Wipe the device before reissuing it to another user, retiring the device, etc., and
- Remotely wipe the device to scrub its stored data if it is suspected that the device has been lost, stolen or otherwise fallen into untrusted hands and is at risk of its data being recovered by an untrusted party.

4.2.2 Mobile Application Management

Some EMM systems include MAM functionality, enabling fine-grained control over different apps on a single managed device, although MAM also may be offered as a distinct third-party solution. MAM systems are designed to enable enterprise control over mobile apps that access enterprise services and/or data. These apps include privately developed apps and publicly available apps. Unlike MDMs, MAM systems do not require the device owner to enroll the entire device under enterprise management, nor must the owner accept installation of an enterprise profile on the device. This distinction is critical for apps designed, for example, to support business-to-business (B2B) transactions (e.g., an app provided to suppliers to enable access to an enterprise orders database). In such cases, the mobile user is not an employee of the enterprise that offers the app.

Apps used on mobile devices may be managed using EMM technology. Depending on how the device is managed and enrolled into an EMM solution, the following restrictions may be applied:

- Restrict which appstores may be used (e.g., limit access to official appstores),
- Restrict which apps may be installed through whitelisting allowed apps (preferable) or blacklisting prohibited apps. Whitelisting and blacklisting capabilities are highly platform-dependent and may not be available on all MAM systems,
- Restrict the permissions (e.g., camera access, location access) assigned to each app. App-wrapping technology (described further in Section 4.2.6) may be used and is highly platform dependent and may also limit app functionality,
- Safeguard mechanisms to install, update and remove apps on a mobile device. Keep a current inventory of all apps installed on each device. This capability is highly platform dependent and may not be available on all systems,
- Restrict the use of OS and app-synchronization and sharing services (e.g., local device synchronization, remote synchronization services and websites),
- Distribute apps from a dedicated enterprise mobile appstore provided through the EMM technology, and
- Distribute the organization's apps from a dedicated mobile appstore.

MAM solutions often enable an enterprise to integrate an in-house enterprise app catalog with a mobile device vendor's appstore (e.g., Apple's AppStore, Google Play) to allow mobile users to easily install an enterprise app. Enterprise system administrators may be able to deploy apps or push out over-the-air updates to mobile users; they may also be able to restrict app functionalities without affecting the entire device, an approach that is preferred by BYOD users. Capabilities for specification and enforcement of security and privacy policies is a key function of MAM systems, often including user- or role-based policies for access to specific apps and integration with remote wipe for employees departing the organization or changing roles. Encryption or containerization may be used to separate execution environments of apps or their communication with enterprise services. Finally, MAM systems may enable enterprise system administrators to monitor app behavior, configuration compliance or presence of unauthorized apps on a user device.

4.2.3 Mobile Threat Defense

MTD systems are designed to detect the presence of malicious apps, network-based attacks, improper configurations and known vulnerabilities in mobile apps or the mobile OS itself. Although MTD is becoming the preferred term, the terms mobile threat protection (MTP) and endpoint protection also are colloquially used. These systems often run an agent on the device—typically a mobile app—and may also initiate analysis and learning on external cloud-based platforms. MTD systems provide real-time, continuous monitoring, assessing apps after deployment to a mobile device as well as during runtime. In an enterprise context, an MTD system may be integrated with an EMM to enable user or administrator notification or automated response to remediate detected vulnerabilities or quarantine apps or devices.

An MTD can detect and protect the mobile device, apps and end-user against attacks via the wireless network. This defense covers MitM attacks that could intercept or eavesdrop on communications. MTD systems also may detect attacks against an app or OS software. For example, MTD systems may observe side-loaded apps—apps loaded from sources other than the standard mobile device vendor's appstore (e.g., Apple's Appstore, Google Play). Side-loaded apps may be special-purpose, enterprise-loaded, or whitelisted apps specified by the enterprise. MTD systems monitor the on-the-fly behavior of mobile apps within the current mobile environment, such as when the app navigates to known malicious URLs or phishing sites. For example, MTD systems may detect communication with a blacklisted service or an app's failure to encrypt communication with an enterprise's backend service. Unexpected interactions among apps or use of data on the user device (e.g., the app accesses a device owner's "contacts" or "location") also may alert an MTD system to potentially malicious or risky behavior.

4.2.4 Mobile App Vetting

The goal of app vetting is to detect software or configuration flaws that may create vulnerabilities or violate enterprise security or privacy policies. An app vetting system is used by enterprise system administrators before an app is deployed to a user's mobile device, unlike an MTD system. Mobile apps may be developed by mobile device manufacturers (e.g., Apple's apps for iOS), the mobile OS vendor (e.g., Google Maps for Android), third-party providers or in-house enterprise developers. App developers and OS developers, as well as enterprise administrators may make mistakes when designing or building an app. They may also intentionally insert malicious functionality that may impact the security or privacy of the mobile user or the enterprise.

App vetting involves a sequence of activities that typically are accomplished via automated test and analysis tools, which may interact with external vetting services. App vetting systems may analyze app source code, app binaries, or general app behavior. App vetting systems can expose several security-critical issues, such as problems with the use of cryptography, collection and handling of sensitive corporate or user data, or software dependencies on untrustworthy cloud services. Common problems with app use of cryptography include the use of weak or broken cryptographic algorithms, small key sizes or failure to cryptographically protect communications or stored data.

Vetting systems may also detect that an app will collect sensitive enterprise data or PII of the mobile user. Apps may be designed to use the device's camera or microphone or collect and share (or sell) sensitive information, including user location information, contact details, sensor data, photos and messages with backend services provided by untrustworthy third parties. Mobile app vetting systems may be able to expose such issues at several phases of the app lifecycle: during development by communicating issues and recommended mitigations to app developers; following development and prior to deployment by identifying vulnerabilities to app security analysts or enterprise system administrators; and post deployment through integration with an EMM by notifying enterprise system administrators of vulnerabilities in installed apps [2].

4.2.5 Virtual Mobile Infrastructure

Virtual mobile infrastructure (VMI) provides an alternative, or accompaniment, to EMM technology. Similar to Virtual Desktop Infrastructure (VDI), which hosts a virtual desktop image for applications and data, VMI uses backend infrastructure to host a virtual mobile device and mobile apps. A user then accesses their virtual device via an app (i.e., thin client) on their phone, and the thin client provides access to a virtual OS. This approach may be viewed as "sidestepping" data confidentiality concerns by storing sensitive information within external infrastructure versus on the mobile device itself. Since all enterprise information would only be available on the cloud-hosted infrastructure, enterprise data would likely be unavailable if there is no network connectivity. Depending upon how the VMI system is structured, VMI may or may not be deployed onto a device already provisioned into an EMM. VMI typically does not allow for device-wide controls and configurations. The deployment and use of this technology is not within the scope of this document.

4.2.6 Application Wrapping

App wrapping is a security mechanism that modifies a ready-to-run mobile executable to prevent functionality defined by a mobile administrator. This approach is often seen as an alternative to the usage of a secure container. Wrapping allows for policies to be enforced onto third-party applications that the enterprise does not own. App wrapping typically requires administrative access to the mobile device, and wrapped apps are installed onto the device without being uploaded to—or vetted by—a platform's native appstore. This process of nonstandard installation also is known as sideloading and if done incorrectly could make a mobile device extremely vulnerable to attack. To mitigate against these potential attacks, the sideloading functionality should be disabled when not used for installing the wrapped apps. The use of app wrapping can be seen as beneficial from a usability standpoint, as users simply use apps like normal. From an IT administrator standpoint, deploying updates can be problematic and error prone.

4.2.7 Secure Containers

Secure containers are mobile apps that provide software-based data isolation designed to segment enterprise applications and information from personal apps and data. Containers may present multiple user interfaces, one of the most common being a mobile application that acts as a portal to a suite of business productivity apps, such as email, contacts and calendar. IT administrators can manage policy sets on containers, but this process may require the use of a software development kit (SDK) integrated into an app. There are multiple secure container architectures, with the two major ones colloquially referred to as *app-based* and *OS-based*. App-based containers may not be wholly dissimilar from any other apps on a mobile device, with the exception of leveraging the management APIs provided by the OS developer. For instance, on most modern mobile platforms any information stored within an app's directory on a device will be encrypted by default. A more extensible implementation of an app-level container allows an enterprise to manage the cryptographic key protecting the container. OS-based containers provide additional segmentation and data isolation when compared to app-based containers. They also provide a consistent FIPS 140-validated environment across different platforms independent of the local cryptographic functions, and these containers are often preferable from a security standpoint.

4.3 Recommended Mitigations and Countermeasures

This section identifies mitigations to the threats identified in Section 3. Table 1 depicts the threats and associates them alongside potential mitigations and countermeasures. Not all threats have a corresponding mitigation listed. Unaddressed threats indicate open research areas and opportunities for new technologies and products. Each listed mitigation addresses at least one threat listed in Section 3. Applying the following mitigations to a personal device of an employee may not be easily accomplished if the user is required to configure their device without the assistance of an IT administrator. For example, it is commonplace for an EMM to create a profile that must be accepted by a user to put these mitigations in place, but an average user may be unable to acquire and properly configure the product.

Table 1 - Threat Mitigations and Countermeasures

Threats	Mitigations and Countermeasures
Exploitation of Underlying Vulnerabilities in Devices	• Security-Focused Device Selection • OS & Application Isolation • Rapid Adoption of Software Updates • Mobile Threat Defense
Device Loss and Theft	• EMM Technologies • Mobile Device Security Policies • Remote/Secure Wipe • Notification and Revocation of Enterprise Access for Policy Violations
Credential Theft via Phishing	• User Education • Mobile Threat Defense • Mobile Device Security Policies • Remote/Secure Wipe

Threats	Mitigations and Countermeasures
Installation of Malicious Developer & EMM Profiles	• User Education • Application Vetting
Accessing Enterprise Resources via a Misconfigured Device	• EMM Technologies • Mobile Device Security Policies • Notification and Revocation of Enterprise Access for Policy Violations
Installation of Unauthorized Certificates	• Mobile Threat Defense
Use of Untrusted Mobile Devices	• Security-Focused Device Selection • Notification and Revocation of Enterprise Access for Policy Violations
Wireless Eavesdropping	• Use of a VPN
Mobile Malware	• User Education • Security-Focused Device Selection • Rapid Adoption of Software Updates • Application Vetting • OS & Application Isolation
Information Loss Due to Insecure Lockscreen	• EMM Technologies • Mobile Device Security Policies • User Education
User Privacy Violations	• User Education • Application Vetting
Data Loss via Synchronization	• EMM Technologies • Mobile Device Security Policies • User Education
Shadow IT Usage	• Mobile Device Security Policies
Exploitation of Vulnerabilities within the Underlying EMM Platform	• Cybersecurity Recommended Practices • User Education
EMM Administrator Credential Theft	• Additional Authentication for System Administrators
Insider Threat	• EMM Technologies • Mobile Device Security Policies • User Education

4.3.1 EMM Technologies

EMM and its supporting technologies can mitigate several of the threats defined in Section 3 and prevalent in the mobile ecosystem. EMM can assist in preventing a misconfigured device from connecting to the enterprise by securely configuring device settings prior to granting access to enterprise resources. An EMM can also actively deny a device access to enterprise data if it is in an insecure state. If an employee loses his or her device or it is stolen, the EMM can wipe the enterprise data on the device. EMMs also can help manage what information is shared on a device lockscreen. Depending on the EMM's capabilities, the list of issues that can be mitigated may be much larger because some EMMs can be used to manage and configure other technologies like MTD and VPN applications.

Threats Addressed: Accessing Enterprise Resources via a Misconfigured Device, Device Loss and Theft, Information Loss Due to Insecure Lockscreen, Data Loss via Synchronization, Insider Threat

4.3.2 Cybersecurity Recommended Practices

EMM and other mobility management infrastructure rely on COTS systems to perform management functions. These core systems often run on top of general-purpose OSs and commodity hardware. It is important that computer security recommended practices, including network, physical and personnel security, be applied to these components in the same way they are applied to general information technology systems throughout industry. Protection mechanisms such as patch management [42], configuration management [43][40] (e.g., disabling serial ports on field network equipment), identity and access management, malware detection, plus intrusion detection and prevention systems can be carefully planned and implemented throughout the enterprise.

Threats Addressed: Exploitation of Vulnerabilities within the Underlying EMM Platform

4.3.3 Remote/Secure Wipe

Remote wipe enables enterprise system administrators to delete enterprise data and applications on enterprise-owned or employee-owned (BYOD) mobile devices. Remote wipe capability is widely available on mobile devices such as smartphones and tablets supporting Android or iOS. Variants of this feature also are natively available for OSs and third-party applications that can be installed on these devices.

To enable remote wipe, a system administrator installs and configures a profile/agent on a device before enterprise data or applications are available to be used. To later perform a remote wipe, an enterprise server issues an erase command that is sent over the network to instruct the EMM device agent to delete data and/or apps on the device. The EMM device agent responds to the server with an acknowledgement that the erasure has been performed or the wipe failed.

Remote wipe may be implemented at different levels of granularity, ranging from full-device wipe (e.g., deleting everything within the system's user partition; typically this level is used for an enterprise-owned device) to an enterprise wipe (e.g., deleting only those device settings, data and apps previously pushed out to the user for enterprise use [typically this level is used to delete work data residing on an employee's personal device]). Native remote wipe capabilities for iOS and Android devices require the device be powered on (with a sufficient charge) and connected to the network. Some third-party EMM systems can execute a remote wipe even when the device is not connected to the network.

Organizations should not rely on remote wipe as the sole security control for protecting sensitive data, but instead consider it to be one layer of a multi-layered approach to protection. By itself, remote wipe is a fundamentally unreliable security control. For example, an attacker could access information on a device before it is wiped or an attacker could power off a device to prevent it from receiving a remote wipe signal.

Threats Addressed: Device Loss and Theft, Credential Theft via Phishing

4.3.4 Security-Focused Device Selection

Out of the box, some devices may have embedded vulnerabilities or malicious software, firmware or hardware. Malicious actors who have access to the hardware, firmware or software supply chains may be able to modify device components, source code or executables during the design or manufacturing phases. For example, an attacker could manipulate software development or integration tools (e.g., compilers, software test systems, configuration management systems), software support tools (e.g., software update or upgrade systems), system administration tools (e.g., software installation and release management systems, patch management systems) or an MDM, MAM, or EMM system. NIST IR 8151, *Dramatically Reducing Software Vulnerabilities* [29] defines a framework and provides a broad catalog of supply chain attack patterns, which cover malicious insertion of hardware, software, firmware and system information.

While it is very difficult to avoid a targeted supply chain attack against a single organization or group of individuals, choosing validated devices and software and using a vetted system integrator can help to mitigate the risk of more broadly focused attacks. NIST's Cryptographic Algorithm Validation Program (CAVP) "provides validation testing of [Federal Information Processing Standards] FIPS-approved and NIST-recommended cryptographic algorithms and their individual components" [13], while the NIST Cryptographic Module Validation Program (CMVP) validates cryptographic module implementations against the Security Requirements for Cryptographic Modules (FIPS 140-2) [17].

The National Security Agency's (NSA) National Information Assurance Partnership (NIAP) [7] is responsible for federal government implementation of the internationally recognized Common Criteria. Products certified through the Common Criteria program are evaluated for conformance with specific security protection profiles. NIAP's product compliance list identifies evaluated products and may be searched by vendor, technology type, protection profiles and certifying country [8]. NSA's Commercial Solutions for Classified Program (CSfC) [9][10] also "requires specific, selectable requirements to be included in the Common Criteria evaluation" and provides a list of software or hardware systems [34], including MDM and mobile platforms, that meet these more stringent requirements. In addition, CSfC provides a Trusted Integrator List [11], which identifies companies that have met its criteria for trustworthy systems integration capabilities. Organizations are encouraged to use lists of validated products and vetted system integrators to reduce the risk of acquiring devices or software with embedded vulnerabilities. In addition to these practices, devices and software manufacturers can also follow their respective industry recommended practices for secure software development to demonstrate they are meeting a set of requirements and have integrated them within their software development lifecycle. More information about secure software development can be found in the NIST Cybersecurity White Paper (DRAFT), *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* [44].

Threats Addressed: Exploitation of Underlying Vulnerabilities in Devices, Use of Untrusted Mobile Devices, Mobile Malware

4.3.5 Use of a VPN

VPN providers compete to provide different security functions in their products. System administrators understand what data is encrypted, what algorithms are used and how both ends are authenticating each other (if at all) by their selected VPN. VPNs may not encrypt all data, and organizations need to take time to fully understand what information is actually being protected. Additionally, the systems and geographic region that enterprise information is sent to are important to understand. Additional information for secure VPN implementation can be found in NIST SP 800-77 rev. 1 (Draft), *Guide to IPsec VPNs* [45] and NIST SP 800-113, *Guide to SSL VPNs* [46].

An organization should base its mobile device security on the assumption that external networks between its mobile devices and its enterprise system, such as ISP and cellular networks, cannot be trusted. Risk from use of untrusted networks can be reduced by using strong encryption technologies such as a VPN to protect the confidentiality and integrity of communications as well as using mutual authentication mechanisms to verify the identities of both endpoints before transmitting data. Another possible mitigation is to prohibit use of unsecured WiFi networks, such as those running known vulnerable protocols.

Threats Addressed: Wireless Eavesdropping

4.3.6 Rapid Adoption of Software Updates

Developers are constantly improving their technology to provide better functionality, but also to fix software bugs and other errors. These technological improvements and security fixes are a key reason to upgrade a device's software or firmware. It is important that a mobile device receives these updates, otherwise it will remain in a vulnerable state. Typically, these updates are not performed automatically, unless a device is configured to do so. Software updates are often developed and provided for the user to manually download and install on their device. Updates should be rapidly deployed, as the longer a mobile device is vulnerable to exploits, the longer enterprise information and all other information is vulnerable to compromise.

EMMs can notify the user when OS and app updates are available. If the user does not make the appropriate updates, the administrator can enforce compliance actions. These actions include blocking or restricting access to enterprise information or the complete removal of enterprise information on the mobile device. If app management is enabled, EMMs can manually update apps and send them to mobile devices.

When patching or updating the OS or an app, enterprise administrators should consider many of the same issues that arise in standard IT environments: the urgency of the update, the likelihood that an update will "break" mission-critical functionality for users, and the ability of the user, the mobile device, and affected systems to roll back failed patches. The urgency of an update is affected by the severity of the potential impact of a vulnerability's exploitation (e.g., critical, important, moderate, low). For example, the Common Vulnerability Scoring System (CVSS) [19] [20] is a numerical scoring system used to communicate the severity of vulnerabilities. NIST uses the CVSS to score the vulnerabilities found in the NVD. Updates to mobile apps may interact poorly with existing enterprise infrastructure software or application software and cause a mobile app or even the entire device to become unusable.

When choosing to take corrective actions and how "strong" such actions should be, the enterprise administrator should consider special factors that affect software deployment in the mobile computing environment. If users are traveling, "offline" for extended periods of time or connected only via low-bandwidth networks (e.g., cellular), updating software may be almost infeasible. To address these cases, administrators should develop mitigations in advance for unpatched mobile systems. For example, reducing permissions to sensitive enterprise assets can allow the mobile devices of traveling users to reconnect to the enterprise network and download the new software without undue risk to the enterprise.

Best practices for mobile updates include pushing updates periodically (e.g., weekly) to acclimate users to regular patching and prevent apps from becoming excessively outdated. Administrators should identify a group of relatively tolerant users—for example, other system administrators—and push updates to these users before organization-wide patching of mobile devices. By using this approach, problems with updates may be discovered and addressed before they impact a larger number of users who are less tolerant of software problems.

Threats Addressed: Exploitation of Underlying Vulnerabilities in Devices, Mobile Malware

4.3.7 OS & Application Isolation

Using a secure container to isolate enterprise data is a commonplace strategy for preventing data compromise. As stated in Section 4.2.7, containers use a variety of underlying technology to separate enterprise and user data. Secure containers often act as an EMM's device-side agent to obtain information about a device's health, enforce enterprise policy and notify administrators of nonconformance. They also can be used to provide cryptographic confidentiality protection of data. Acting as the EMM agent, secure containers may work in conjunction with the management APIs to perform their security and management functions.

Administrators also can configure policy, receive notifications of policy violations, prevent data exfiltration and manage device health by embedding a security-focused SDK into an app residing on an employee device. Although this approach can be fruitful, it requires a certain level of expertise from the enterprise to develop the SDK. Another approach to isolation includes wrapping applications as mentioned in Section 4.2.6. All of these can work in concert to provide the desired degree of isolation.

Enterprises may need to employ multiple isolation mechanisms within their mobile deployment. The exact combination necessary for a particular enterprise is a function of an enterprise's unique security and operational requirements. Implementing all of the isolation mechanisms listed here may not be an appropriate response to the threats posed to an enterprise, and may also be too costly to implement. Yet enterprises should gain an understanding of what security benefits an isolation mechanism is actually providing, and what features are simply a byproduct of the underlying OS. In addition, organizations should ensure isolation mechanisms are activated and properly configured.

Threats Addressed: Exploitation of Underlying Vulnerabilities in Devices, Mobile Malware

4.3.8 Application Vetting

MAV tools can be employed to identify vulnerabilities and malicious code in mobile applications. They can also integrate with many EMM and MTD systems. When an issue is discovered, an administrator can be properly informed and automatically deploy various EMM-provided remediation actions. These include notifying administrators, affected users and departments; automatically removing affected apps; disallowing access to enterprise resources; or performing other remediation actions available via the EMM. To achieve this automated operation, the EMM is integrated with MAV tools via APIs that coordinate the submission of mobile apps—one-off or in bulk—to the MAV service via the EMM dashboard. These APIs often are implemented using web services. For MAV services, EMM integration can enable a flexible conduit through which results from multiple MAV vendors can be received and aggregated at the EMM dashboard or portal without requiring all app vetting reports to conform to a single format.

Threats Addressed: Installation of Malicious Developer MDM Profiles, Mobile Malware, User Privacy Violations

4.3.9 Mobile Threat Defense

MTD can operate as a standalone and isolated system that detects malicious applications and other threats. MTD systems can detect network-based attacks (e.g., MitM that could intercept and redirect or eavesdrop on communications), app-based attacks (e.g., information leakage or malicious, sideloaded apps), platform-based attacks (e.g., rootkits that undermine basic OS functions) and others. When coupled with an integrated EMM, these systems offer multiple remediation approaches following an attack attempt or data breach is detected or a device is compromised. Remediation for network-based attacks include disconnecting the device from the enterprise network, re-establishing a trustworthy connection or blocking attempts to connect to blacklisted networks.

For app-based attacks, an integrated EMM and MTD system can remove malicious apps or modify app permissions to limit access to sensitive enterprise resources. In cases where an integrated EMM and MTD system detects a potential attack against the mobile platform, it might notify the user to apply an OS patch or—in the extreme—remotely wipe (i.e., factory reset) the device. Integrated EMM and MTD systems typically are configured to alert the system administrator and potentially the mobile device user to the detected problem and the remediation approach initiated.

Threats Addressed: Credential Theft via Phishing, Installation of Unauthorized Certificates

4.3.10 User Education

Security is everyone's responsibility. The user cannot solely depend on the EMM and other third-party apps to secure their device and enterprise data. User awareness is important because the device user plays a vital role in securing the enterprise's information. Understanding the importance of securing the device and how to contribute is important for both the user and the enterprise.

Providing effective ways to teach users how to protect their mobile device is essential to understanding the importance of security mechanisms and how to apply them. Following are a few examples of mobile device security on which device users should be trained:

- How to identify phishing attacks,
- How to properly manage authentication credentials,
- The organization's privacy policy and the personal information collected,
- How to identify malicious EMM profiles or other malicious applications, and
- Why it is important to rapidly perform OS and application updates.

If the device users are not educated on how to properly secure their mobile device, this oversight could endanger enterprise and user information. That's why user education is essential for enabling users to do their part securing their mobile device—for themselves and the enterprise.

Mobile device and EMM administrators also require the proper security training in addition to the users. The enterprise may want to identify the Workforce Categories and Specialty Areas from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (SP 800-181) [47] that are of interest and applicable to the enterprise's needs. Through identifying the Workforce needs, the enterprise will be able to understand the necessary knowledge, skills, and abilities for a mobile device/EMM administrator.

Threats Addressed: Credential Theft via Phishing, Installation of Malicious Developer and EMM Profiles, Mobile Malware, Information Loss Due to Insecure Lockscreen, Data Loss via Synchronization, Exploitation of Vulnerabilities within the Underlying EMM Platform, Insider Threat

4.3.11 Mobile Device Security Policies

The development of security policies is vital to establishing a prominent security posture through well-defined procedures and governance. The purpose of security policies is to provide a clear course of action for organizations to follow when deploying new technologies and remediating issues or other occurrences. Mobile device security policies can be established by performing a threat modeling exercise or risk assessment to understand the attack landscape and plan according to an organization's specific security needs.

Mobile device security policies can define the device configurations required for each mobile device that accesses enterprise data. For example, a configuration policy may require user authentication before accessing the mobile device or the organization's resources. Further, that policy may define the strength of the authentication mechanism or require multi-factor authentication. These types of policies inform the system administrators of the policies to enforce on the mobile device and can in turn protect against an attacker gaining unauthorized access to enterprise resources.

In the case of remediation, an organization should define policies to guide the necessary actions to perform in the case of an error or attack. An organization may develop a policy that requires a mobile device to be erased/wiped if it is lost or stolen. This policy will prevent anyone from retrieving unauthorized access to sensitive enterprise information. Additionally, if it is found that there is a breach due to implementation of a weak or outdated policy, an organization should have procedures for reviewing and updating policies as needed. Additional information about recommended mobile device security policies can be found in Appendix D.

Threats Addressed: Device Loss and Theft, Credential Theft via Phishing, Accessing Enterprise Resources via a Misconfigured Device, Information Loss Due to Insecure Lockscreen, Shadow IT Usage, Insider Threat

4.3.12 Notification and Revocation of Enterprise Access

Every enterprise and organization should have security policies and rules that influence remediation actions when network attacks or breaches occur. These policies and rules also cover mobile devices. Remediation actions may span a spectrum of possibilities ranging from notifying affected individual users or groups of users, to revoking access to enterprise data and services, to wiping the data of the affected device(s) or restoring it/them to a default pristine state (e.g., factory reset).

Notifying users of an issue is often the most basic and least aggressive remediation option. This is typically done via a push notification to the phone's notification center or potentially an SMS to follow up. Temporary revocation of access to enterprise resources is often seen as the next step if the notification does not remediate the issue. This is most easily done via the EMM agent if one is installed on the employee device. The temporary revocation may last a predefined period of time—for example, 24 hours—and access may be automatically restored or only restored manually by the enterprise's systems administrators. Removing applications or wiping the mobile device are some of the more aggressive remediation options available to the enterprise. This more drastic action can be performed because an app on their mobile system was compromised or is malicious and is the source of attacks or leaks affecting the enterprise. But beware: wiping data not owned by the enterprise can cause legal issues.

Threats Addressed: Device Loss and Theft, Accessing Enterprise Resources via a Misconfigured Device, Use of Untrusted Mobile Devices

4.3.13 Additional Authentication for System Administrators

System administrators who use the EMM console have access to sensitive information about the enterprise's mobile devices. Individuals with EMM credentials can grant and revoke access to enterprise resources and collect private information about employees such as device location. Additionally, they may be able to wipe an entire device, not just the enterprise data. For this reason, EMM administrator credentials should conform to standard password strength and complexity rules listed in NIST SP 800-63-3 [4]. If supported by the EMM, multi-factor authentication also should be used. These additional layers of authentication for system administrators can help to thwart EMM credential theft.

Threats Addressed: EMM Administrator Credential Theft

5. Enterprise Mobile Device Deployment Lifecycle

There are many factors to consider when deploying mobile devices within an enterprise environment. These include selecting the correct management technologies and devices, alongside properly providing them to users. This section defines a process, as seen in Figure 3, for deploying devices and managing them throughout their operational lifecycle, known as the Enterprise Mobile Device Deployment Lifecycle. Each step of the process is described below along with necessary implementation details. Organizations may wish to document their decision-making process and implementation details into a mobile security policy.

Alternative process models and frameworks exist, and enterprises should adopt or combine the ones that suit their needs while satisfying their requirements. One example is the Mobile Computing Decision Making Framework (MCDF), a four-stage framework that is used to determine if a mobile solution is necessary to support an enterprise's overall mission. More information on the MCDF can be found in the CIO Council's Mobile Computing Decision Making Framework [12].

Figure 3 - Enterprise Mobile Device Deployment Lifecycle

5.1 Identify Mobile Requirements

In this first stage of this Lifecycle, the organization decision-makers define the mission needs and requirements for mobile devices, inventory the mobile devices already in use, and identify the mobile deployment model that fits your organization. This is all in an effort to gather requirements for managing current and future mobile devices to meet mission needs for functionality, security and privacy.

Participation of both IT-focused and business-focused decision-makers is necessary in this stage to ensure that the needs of the mission will drive the technology choices in later stages.

5.1.1 Explore Mobile Use Cases

Many organizations find that mobile devices are essential to enable their staff to meet evolving mission requirements. Tasks that once might have been accomplished in the office (at a much slower pace) are now handled "in the field," often while requiring access to enterprise data or apps and through interaction with colleagues from partner organizations. This need to meet challenging and fast-paced mission requirements should be weighed against the need to protect sensitive data, address privacy concerns, financial costs and other issues. Developing use cases specific to an organization's needs for mobile devices can help to identify and clearly describe requirements. Common elements of use cases include understanding who your users are, why they need mobile devices, and what apps or device features will be necessary for them to meet their organizational objectives.

For example, a disaster management organization may send staff members to sites affected by natural disasters, such as tornadoes, floods, and earthquakes, to provide assessments and assistance. Mobile devices are essential to reach back to enterprise data sources and to enable submission of information gathered on site. Staff also should share information with members of the public, local first responders, representatives of other local, state and federal organizations, as well as staff from various other non-governmental organizations (NGOs). In this use case example, the strong need for a mobile capability is clear, and backend systems may need to be restructured to enable appropriate security characteristics to support these interactions. The characteristics (e.g., durability will be important for rough worksites) and cost of the selected mobile devices should be considered carefully to ensure all staff have the necessary equipment and expensive devices are not too fragile for a rough worksite.

5.1.2 Survey Current Inventory

When modern mobile devices were first introduced to the enterprise, management platforms were less mature and likely had not been managed in a centralized manner. These sorts of practices may have continued over time. Therefore, an inventory of the mobile systems alongside other information systems within an organization's network can be valuable when deploying a new mobile infrastructure. This can be performed by directly asking employees for the mobile devices they are using and performing network scans to understand the devices on a network. These two sources of information combined provide a picture of the devices that are actually being used and need to be protected and/or upgraded.

Unidentified mobile devices may leave holes in the enterprise's infrastructure. These devices may not acquire the necessary security configuration, which leaves the mobile user and the enterprise unprotected from vulnerabilities and exploits. Malware or unauthorized access to the enterprise's network through the unidentified mobile device can leave the enterprise blind to attacks due to the lack of awareness of all mobile devices within their infrastructure. Identifying current inventory may be performed through an inventory management methodology. NIST and DHS produced NISTIR 8011, *Automation Support for Security Control Assessments Volume 2: Hardware Asset Management* [34], which provides operational guidance for automating and assessing the FISMA security controls with regards to hardware asset management.

5.1.3 Choose Deployment Model

Today, organizational leaders may choose from a variety of deployment models for the mobile devices to be used within the enterprise. A deployment model captures alternative options for device ownership, as well as policy and technological controls that manage device behavior. The spectrum of options ranges from devices issued by (i.e., purchased or leased by) and fully managed by the enterprise to devices owned by individuals with little or no enterprise management of device interaction with enterprise systems. The following sections describe three of the most commonly used categories of options in the spectrum. NIST SP 800-114 Rev. 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* identifies some similar categories in the context of devices used for teleworking [35].

5.1.3.1 Strict Enterprise Usage

Strictly enterprise-enabled mobile devices and the information on those devices are issued by the organization. Users should be made aware that all data on the device are owned by the organization. Within the federal government, this deployment model is sometimes known as Government Furnished Equipment (GFE). This section covers enterprise-enabled mobile devices that are provided to employees for (strictly) enterprise use only. GFE devices strictly limit personal use; employees typically own and carry a separate personal device.

Enterprise-enabled mobile devices provide significant security benefits. Organizational leaders may consider the supply chain of candidate devices before selecting devices for purchase, and IT system administrators may develop device hardening plans before the products arrive. At deployment time, the IT staff may configure restrictive policy settings to significantly alter the functionality of the device such as removing text messaging functionality, restricting WiFi and Bluetooth access, and ensuring that communication takes place over a VPN. In the enterprise-enabled model of device deployment, tradeoffs between security and functional usability can be made entirely at the discretion of organizational leaders.

An example for an only enterprise-enabled deployment includes a GFE that is provisioned to the end user as a fully managed or supervised device. Mobile security technologies include enrollment of the device into an MDM with the use of mobile threat defense for endpoint protection, and access to enterprise resources through web-based interfaces or mobile applications. A whitelisting approach is implemented for enterprise-enabled deployments; all mobile apps on the device will be examined through a mobile app vetting service before the apps are provisioned to the device or allowed to be downloaded from the managed enterprise appstore [2]. Access to the official public appstores or unofficial appstores is restricted in this deployment model.

Device ownership status: Organization

5.1.3.2 Corporate Owned Personally Enabled (COPE)

COPE devices are issued by the enterprise to employees. The COPE model is less restrictive on employee personal use. While the enterprise owns (or leases) the device and enforces usage restrictions, these restrictions are more lenient, allowing employees some personal use of the device. For example, an employee may be permitted to download certain apps or receive personal text messages on the COPE device. Although a COPE device is personally enabled, the device and information on the device belongs to the enterprise. Employees should be informed about enterprise restrictions and have appropriate expectations of software and device configurations that affect functionality and privacy.

An example of the COPE deployment model includes a managed GFE device. This may include a fully supervised device or a separate enrollment to manage the device by downloading an EMM application from the official appstore. A blacklisting approach is implemented for many COPE deployments. All mobile apps on the device should go through a mobile app vetting service; apps downloaded to the device are vetted during or after installation by the app vetting service and checked and maintained against an application blacklist. For COPE, personal applications are allowed on the GFE device and the end user is able to access the official public appstores.

Device ownership status: Organization

5.1.3.3 BYOD and Choose Your Own Device (CYOD)

The BYOD deployment model allows employees to use their personally owned mobile devices to access enterprise data and services. The employee may, for example, access both personal email and sensitive enterprise email via the same application. The BYOD model raises concerns regarding leakage of sensitive enterprise information via the device to untrustworthy third-party backend systems that communicate with various apps on the device. To protect the confidentiality and integrity of enterprise data and systems as well as the privacy of the device user/owner, IT staff may use a tool such as an EMM to enforce DLP by applying restrictions such as disabling the copy/paste feature when in enterprise applications. Also, an enterprise may use MTD technology to ensure the device is protected from mobile threats and attempts to compromise the device.

A Choose Your Own Device (CYOD) device is purchased by an employee for personal use. In the CYOD model, the enterprise provides employees a list of devices (e.g., the Commercial Solutions for Classified Component list) that are acceptable for interaction with enterprise networks and software. If the employee's personal device is on the approved list, and the employee installs software required by the enterprise, then the employee may use that device to access the enterprise's data and services. Employees with personal devices that are not on the approved list must often carry a second (enterprise-enabled) device for work-related activities, so choosing from the approved list allows a user to avoid carrying an additional device.

Another concern with BYOD and CYOD devices is lack of supply-chain management. The enterprise has little-to-no knowledge of the device's origination or if it has been modified. A BYOD/CYOD device may be rooted or jailbroken with installed untrusted apps. The device may be infected with malware without the user's knowledge. The lack of a baseline leaves the enterprise at a disadvantage when it allows a user to access enterprise data via their device.

For the organization, CYOD offers the opportunity to limit the hardware supply chain risk and to control access to enterprise data and backend systems through enterprise protection software (e.g., an EMM or MTD agent). The advantage of CYOD over BYOD is that employees are informed in advance of the devices which are capable of running the necessary enterprise protection software and, thus, will be permitted to access enterprise resources. When IT staff members decline to allow a BYOD device because it is unable to run an enterprise EMM agent, then BYOD equals CYOD, but with the appearance of IT management inconsistency and capricious application of unstated policies.

Device ownership status: Employee

5.1.4 Select Devices

Organizational mission and constraints such as cost and deployment models are considered in the selection of mobile devices [18]. That is why an approach for assessing an organization's mission needs for mobile solutions is needed. It recommends that "for each candidate mission, the organization must determine who needs mobile access, to what data, why and where." For example, many organizations find that providing access to email through mobile devices allows a majority of employees to work more efficiently by enabling communication on time-critical issues. However, mobile access to specialized data and apps may be essential to only a few key employees. Understanding the impact of mobile devices on mission needs can help an organization to focus its selection process by narrowing it to a small set of candidate devices that satisfy the organization's requirements.

Costs and security concerns related to mobile devices impact the purchasing decisions of many organizations. Costs can be minimized by limiting deployment of devices only to users who need them to support an organization's mission and by selecting devices with only the necessary capabilities (e.g., choosing a previous model rather than the "latest model"). For security, it is important to select device models that are current enough to be well supported by the manufacturer and can accommodate OS and application updates and patches.

5.1.5 Determine EMM Capabilities

Identifying the EMM capabilities required to work effectively within an enterprise is an important activity to perform before acquiring an EMM. This step requires organizational leaders to use the information gathered in the previous sections to define the capability requirements for their EMM solution. For example, the EMM must support the devices selected to meet the mission needs and, potentially, existing devices in the current inventory. Other commonly required EMM capabilities are options for integrating the EMM infrastructure into the enterprise's infrastructure. These options include "on prem" operations (i.e., running on servers hosted on premises, within the enterprise datacenter), support for a Software as a Service (SaaS) model, or product certifications/accreditations and third-party service integrations. Section 4.2 discusses many other important capabilities for EMMs and other enterprise technologies designed to support mobile computing for the enterprise. The list of required EMM capabilities will support the well-reasoned selection of an EMM for the enterprise, ensuring that it provides the necessary functional and security capabilities.

5.2 Perform Risk Assessment

Risk assessments are a foundational component of cybersecurity. The risk-assessment process can be used to identify, estimate and prioritize risk to organizational operations and assets, staff and other organizations that result from the operation and use of information systems. Risk assessments should be performed periodically, as the threat landscape is constantly changing and the systems to be protected are evolving. Section 5.6 addresses the topic of periodic security audits, which assess the effectiveness of controls for protecting the enterprise. Periodic risk assessments should inform security audits.

Risk assessments can be conducted at the organization level, mission level, and information-system level. This guidance recommends that mobile devices, mobile apps and any systems used to manage the mobile system be included as part of the risk-assessment process. The risk assessment may have mobile devices included under a larger risk assessment umbrella, or may be conducted against a specific mobile device deployment. A variety of risk assessment methodologies exist, such as mobile-agnostic guidance (NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*), and mobile-specific guidance (Mobile Computer Decision Framework) [14]. Another example of mobile-specific guidance also exists for performing risk assessments such as NISTIR 8144 (DRAFT), *Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue* [5][6] used in conjunction with a threat modeling process such as draft NIST SP 800-154, *Guide to Data-Centric System Threat Modeling* [48], and the MITRE Mobile ATT&CK Framework [15]. Organizations that fail to conduct risk assessments may inadvertently select and apply incorrect security controls or spend precious resources addressing risks that are unlikely to occur. Enterprises are encouraged to revisit their identified requirements once a risk assessment has been performed in order to update the list of requirements based on information identified within the risk assessment.

5.3 Implement Enterprise Mobility Strategy

Resource availability, mission needs, and various other organization constraints will guide decisions on mobile deployment options, devices, and EMM systems. Some organizations must have full control of all components in the enterprise environment, so all mobile equipment must be purchased by the organization and managed by enterprise system administrators through an EMM. Other organizations allow employees to bring their own devices (possibly from an approved list) and may manage a few enterprise applications through a MAM system. By focusing on the enterprise requirements, decision makers can narrow the range of appropriate deployment options.

5.3.1 Select & Install Mobile Technology

The list of mobile technology requirements previously identified should be compared against those of the EMMs under consideration. There may not be a perfect match with a complete overlap of requirements and capabilities, especially when EMM selection must be made from a predetermined list owned by an external organization. Once an EMM selection is made, the EMM should be appropriately implemented inside of the enterprise network boundary. This includes proper product configuration, which is another important step in securing enterprise mobile infrastructure. A misconfigured EMM can lead to data leaks of confidential and proprietary enterprise information which may include self-developed internal mobile apps, personnel employee data, and data that could include trade secrets.

EMM technology can be set up in different ways within the enterprise, and different architectures are possible. The two primary methods focus on the location of the EMM and associated technology. These methods are on-premise and cloud-based, sometimes referred to as the Software-as-a-Service (SaaS) model. These are described below.

5.3.1.1 On-Premise Architecture

On-premise (i.e., *on-prem*) instances of the EMM technology are less common. Organizations install and configure the EMM themselves, and also pay for any software licenses for any underlying platforms or components. Some EMM vendors offer images and containers that can help ease the burden of installation and configuration. Organizations are encouraged to double-check the images or containers for commonplace software vulnerabilities. The primary benefit of this model is that enterprise data resides within the organization, other than the allowed devices that can query and receive information they are authorized to obtain. Enterprises can monitor this traffic alongside all of the authentication from the EMM to other devices. Finally, physical security of the EMM can be ensured for this model.

Below is a sample architecture demonstrating an on-prem implementation of the mobile security technologies. MTD applications are sometimes cloud-based, even if the organization's management technology is on-prem. Figure 4 shows the MTD as part of the cloud, although real-world deployments may significantly differ. The EMM components are hosted via on-prem servers owned and managed by the enterprise. This architecture requires considerable installation and maintenance of the technologies by the enterprise, but also provides the enterprise with more control over how the enterprise data is transmitted and managed.

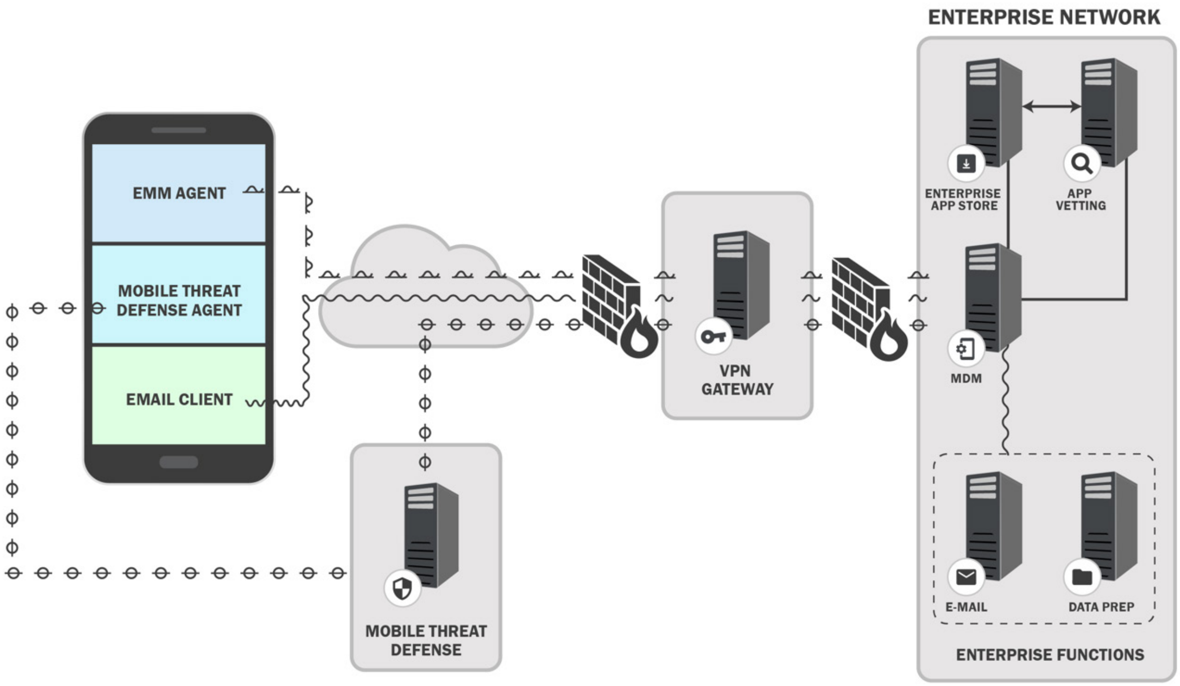

Figure 4 - On-Premise Mobile Architecture

5.3.1.2 Cloud Architecture

The cloud solution is an alternative to the on-prem architecture that allows mobile security technologies to be hosted external from the local enterprise network. When using the cloud solution, the mobile security technology provider gives the enterprise the ability to use its applications, which are run on a cloud infrastructure. This is also known as SaaS, and mobile security and management services are delivered via the internet to the enterprise [24].

Cloud-based EMM deployments are often easier to set up and begin using. They involve signing up for a web-based service, and users are quickly taken to the primary dashboard after payment is provided. The most difficult aspects of setup are joining the EMM to an Active Directory service and proving that the email domain being used actually belongs to the company. The EMM vendor often provides unique information that must be placed into DNS, and then can be externally checked. Another benefit of the SaaS model is that problems or issues can be more easily addressed by the vendor, since they have access to the EMM instance and underlying platform. Finally, with this model the enterprise data resides outside the traditional enterprise, much like the mobile devices the EMMs manage. This is oftentimes a key factor in organizations deciding not to use this model. Below is a sample architecture demonstrating a cloud-based mobile enterprise architecture (e.g., MDM server, app vetting server).

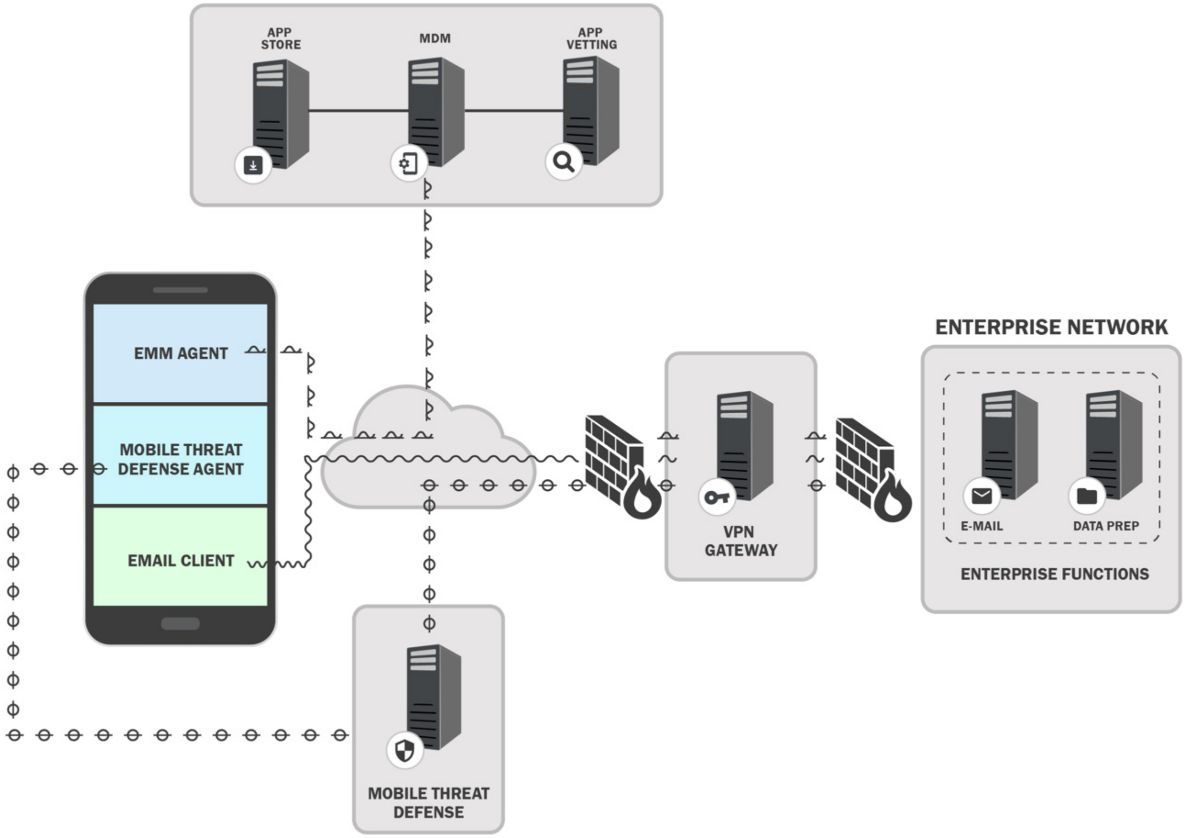

Figure 5 - Cloud-Based Mobile Architecture

5.3.2 Integration of EMM into the Enterprise Service Infrastructure

Both large and small enterprises may connect their EMM system to existing enterprise infrastructure services to improve security management of mobile devices. Such services support authentication, identification and access control to enterprise networks and resources. Remote Authentication Dial-In User Service (RADIUS) is a standard network authentication service protocol, providing authentication of access credentials followed by policy-based network resource assignments (e.g., Internet Protocol [IP] address, permitted network connection time). Directory services such as Microsoft's Active Directory map network resources (e.g., volumes, printers, users, devices) to network addresses. Enterprise systems use the Lightweight Directory Access Protocol (LDAP) to communicate with directory services. Another set of services enables remote connectivity via a VPN to enterprise systems.

By integrating an EMM with enterprise backend infrastructure services such as RADIUS or directory services, an organization can enable finer-grained management of mobile device access to mission-critical enterprise resources. System administrators can set policy-based configurations for mobile devices to constrain access to sensitive resources, depending on mobile device conditions (e.g., connection from a public WiFi network or user-managed device running a corporate application). When enterprises deploy an EMM without integrating it with their backend security infrastructure, mobile device connections to the enterprise network may be managed via global passphrases for connection to the enterprise WiFi network. Mobile devices with WiFi network access can then reach any of the services on the enterprise network, meaning that when a device is connected to the WiFi network, it can access everything on the typical enterprise network.

5.3.3 Set Policy, Device Configuration and Provision

In certain deployment models, mobile devices should be properly set up before they can be provided to enterprise users. IT-focused and business-focused decision-makers should work together to define a mobile device usage policy acceptable for these devices. The usage policy should address the standard security protections to be applied to all enterprise mobile devices, as well as specifying the permissions and special configurations that apply to users with different organizational roles. Devices can then be properly configured and provisioned to enforce the chosen policy. For organizations with a less stringent stance on device usage, such as BYOD, users should be made aware of the mobile device usage policy and signal their acknowledgement of the policy.

5.3.3.1 Define EMM Policy

An EMM policy is a set of rules that defines what a user is allowed (or not allowed) to do on their mobile device and the mobile device configuration requirements. EMM policies are put in place to assist in securing the enterprise data within the mobile device. To do so, the enterprise must understand the type of data the user handles (e.g., sensitive data), the risk factors and the proper way to protect that data from accidental or intentional threats. Upon understanding these key factors, the enterprise then documents the EMM policy and applies the policy configurations within the EMM.

These policies may vary per user or device since a particular user group or role within the enterprise may have different permissions to adequately perform its duties. If the EMM policy is not well defined, the user permissions may not accurately reflect the policy requirements and a user may be given too much or too little access to enterprise data. This could negatively impact an employee’s ability to accomplish their work or allow the employee unauthorized access to enterprise information. Some examples of elements to include within an EMM policy include password requirements, device encryption, VPN requirements and geo-fencing.

5.3.3.2 Consider Personal Account Usage

One of the primary means of communication within an enterprise is email. While most businesses provide work email accounts to their employees, others might allow an employee to use a personal email account to handle business communication. Email may be used for general communication between employees, account establishment, password initiation/reset, the sharing of sensitive information, and enterprise alerts/notifications.

Using personal email accounts leaves the enterprise without security control over the personal email accounts. Similar issues also arise with other cloud-based services, e.g., cloud-based storage and sharing of documents. Without this control, sensitive enterprise information could be transferred to unauthorized recipients, the enterprise cannot control or have knowledge of what servers its emails are transmitted through, and it cannot apply enterprise-level security protection of its emails. Another concern is litigation against the enterprise; the inability to backup or archive personal email accounts could make it difficult for an enterprise to respond to a demand for discovery or a Freedom of Information Act (FOIA) request. If an employee resigns or is terminated, the enterprise is unable to remove that person’s access to enterprise emails that were sent to their personal email address. This security gap could allow a former employee to retain access to sensitive enterprise data.

Enterprise email is the prime option for establishing account access for individuals because—as mentioned above—enterprise email addresses give an enterprise optimum control over its data. Access-control policies and privileges can be provisioned to a specified enterprise email account, which coincides with the employee who uses the email address. Personal email addresses can be used in a similar fashion, but enterprises are left with less control of information sent to them. Finally, shared emails—enterprise or personal—make it difficult to manage account access. Each employee on the shared account is given the same access privileges and has the ability to repudiate responsibility because there is no way of monitoring individual access. Multiple users having access to a single account eliminates the ability to apply least privilege and separation of duties.

5.3.3.3 Device Configuration

Device configuration is the system configuration of a mobile device before it is provisioned to the user. The system configuration may include updating the OS to the most recent release, establishing password length requirements and/or enabling device encryption. How devices are configured depends on the device deployment model used by the enterprise.

The device configuration process for enterprise-issued and BYOD devices is different because of how devices are ultimately provided to users. Enterprise-issued devices can be preconfigured in-house, or the enterprise can have a mobile device vendor preconfigure the devices prior to shipping them to the users, such as Apple's Device Enrollment Program (DEP). In the case of BYOD devices, it is required that the enterprise requests the device owner bring their device into the enterprise to be properly configured for enterprise access.

The requirements for device configuration may vary per enterprise. An enterprise may reference suggested secure mobile-device configuration guidance from established entities. The Defense Information Systems Agency (DISA) provides Security Technical Implementation Guides (STIGs) that dictate detailed configuration standards for the Department of Defense (DOD). The Center for Internet Security (CIS) offers the CIS benchmarks, which are "best-practice security configuration guides both developed and accepted by government, business, industry and academia" [36][37]. NIST hosts the National Checklist Program (NCP) [40], which supplies checklists for securely configuring specific types of technology. Device manufacturers may also provide suggested configurations for their mobile products.

5.3.3.4 Device Provisioning

Device provisioning enrolls a device into the EMM by installing an EMM certificate onto each device that provides privileged device access to enterprises alongside in-depth security features. Provisioning a mobile device requires your device to have the necessary certificate to be enrolled in an EMM service. This certificate is installed on a device and allows the EMM to verify the device can be provisioned. Once the device is provisioned to the EMM, the appropriate EMM policies are applied to the mobile device and, if the device configuration is not automatically updated, the device will need to be configured to meet the policy requirements. After the provisioning process is complete, the device user has access to enterprise data (e.g., email, calendar, contacts) and the enterprise is able to monitor the device and ensure it is compliant to their enterprise policies.

Devices may be provisioned in-person or remotely. In-person provisioning requires an administrator to physically have the device to install the EMM certificate and confirm the device is properly provisioned. Remote provisioning requires the device user to implement the provisioning process on their own. The user may not provision the device properly, which may render the device and enterprise data vulnerable because it may not be compliant to enterprise policies.

5.3.4 Verification Testing

To protect the operational enterprise environment, as well as enterprise and user data, it is important to verify the device configurations and software installed on mobile devices that connect with the enterprise. Before deploying an app, a software update, or a patch throughout the enterprise, enterprise administrators may run pre-deployment tests to provide insight into how the change may impact the security or functionality of existing enterprise systems. For significant software deployments or major updates, administrators may want to first deploy to a limited group of users to enable assessment of the impact to the production environment.

Allowing mobile devices to access enterprise resources can better enable staff members to execute the enterprise mission. However, mobile devices also carry security risks for enterprise systems, data and users. Verifying that mobile devices and their applications have acceptable configurations is essential to ensure that the benefits of mobile access outweigh the security risks that they present to the enterprise ecosystem.

Mobile device or app-level configurations can significantly impact the security posture of the enterprise, thus permissions for the device or individual apps may be granted depending on specific configuration settings. Network configurations may include an obligation to authenticate and use a VPN before permitting connection to an enterprise wireless network. A geofencing policy may specify that a device operating within a particular geographic region be granted different permissions than the same device used within a different region. Different users, devices or apps may be granted different permissions for accessing enterprise backend services (e.g., a database holding sensitive information), depending on the app or device configurations. In many cases, mobile device security features are configured to better protect the enterprise in addition to the mobile device itself: device data encryption, screen lock timeout, password and application firewall requirements are configurable and contribute to the security posture of the enterprise. Finally, enterprise policy may restrict the apps that may be installed on the device, require updates to apps or the mobile OS, or limit access to some of the device features in order to protect enterprise systems or data.

5.3.5 Deployment Testing

Enterprise networks and applications require software updates to improve functionality, patch vulnerabilities, fix bugs, or enable new hardware deployment. To make sound enterprise deployment decisions, systems and network administrators may first perform deployment testing before pushing new software into the production environment.

Administrators consider a broad spectrum of test scenarios to evaluate a software update, deciding what tests will be sufficient to indicate that the update is ready for the production environment. A phased approach to component level, feature, network, and enterprise-wide testing is typically recommended for deployment testing.

For example, when introducing a new enterprise capability such as managed mobile devices or mobile application vetting, the administrator should consider rolling out a limited trial with only a small set of carefully chosen users. After the trial deployment has been operating satisfactorily for a predetermined period of time, and if the user experience and satisfaction has met its target level, the organization may then be ready for an enterprise-wide deployment. Following this approach not only ensures minimal disruption to the enterprise operation and a satisfactory user experience, but also facilitates the discovery of security issues as early as possible in the deployment process.

5.4 Operate & Maintain

It is necessary to design and implement security controls to protect enterprise systems, as well as enterprise and user data. However, initial deployment of controls is not sufficient to protect an operational enterprise. In addition, IT audits should be used to periodically evaluate the effectiveness of security controls for protecting the evolving enterprise, identify security issues, and modify or add controls to better protect the system in the future. Auditors need data to perform those evaluations, and mobile device usage logs provide important data for assessing the effectiveness of controls on the mobile computing environment.

5.4.1 Auditing

In order to keep up with a rapidly changing attack surface and cybersecurity landscape, the enterprise security team may practice and conduct security assessments. An essential component of such assessments is the periodic audit of the enterprise IT and mobile networking infrastructure. A comprehensive audit should cover the following:

- Enumerating the enterprise audit objectives,
- Establishing a security baseline through periodic (e.g., annual) audits,
- Relying on auditors with well-established (and verified) security assessment experience,
- Developing an automated audit process to cover all of the enterprise IT infrastructure, including mobile devices,
- Analyzing the data generated by the audit process, rather than relying on compliance checklists, and
- Using a third-party auditor to report risks facing the enterprise.

Periodic audits should include the enterprise mobile infrastructure and device management systems, including components such as EMM/MDM, services for mobile app vetting, integration with backend services, and the employees' mobile devices and their applications. The audit should help the enterprise security team to assess whether the benefits of mobile access outweigh the security risks that they present to the enterprise ecosystem.

5.4.2 Device Usage

An organization should develop security and privacy policies for mobile device (and app) usage. A key element of that policy is enterprise monitoring of device/app usage. EMM, MAM and many mobile network monitoring systems enable enterprise administrators to track or monitor many mobile user activities, including identification of all device apps, app usage patterns (e.g., downloads, when/how often an app is launched), device features used by each app (e.g., microphone, camera), data used by an app (e.g., user location, contacts), device/user geographical location, and phone calls (e.g., phone number, name, time duration, date, location). An appropriate monitoring policy for devices/apps should consider many factors, including organization mission (and how the mobile device/app supports that mission), security/privacy characteristics of the enterprise data and systems accessed via the device, user relationship to the enterprise (e.g., employee, contractor, employee of a partner organization, members of the general public), deployment model (e.g., enterprise owned, BYOD), and user privacy. A monitoring policy that is appropriate for enterprise-owned devices carried by employees in a very high-sensitivity environment might include location tracking the device/user and geo-fencing the use of certain applications. Such a policy would be unacceptable (and likely infeasible to implement) for individually owned devices of employees of a partner organization who are visiting the enterprise site.

User privacy is an important consideration because most devices will contain some personal user information, and certain types of monitoring (e.g., geolocation) may bring enterprise interests into conflict with privacy regulations. Organizations that do business within the European Union (EU) also should consider how the EU's privacy and data protection regulation—the General Data Protection Regulation [30]—constrains mobile device/app usage monitoring.

5.5 Dispose of and/or Reuse Device

Mobile devices may hold sensitive information such as passwords, account numbers, emails, voicemails, text message logs or mission-specific data such as law enforcement sensitive information. When a mobile device must be disposed of, it is important to take the proper steps to ensure that sensitive information does not fall into the wrong hands.

While techniques such as degaussing, memory overwriting or even physical grinding can be used to sanitize magnetic media, these techniques are not effective for sanitizing the solid-state memory used in mobile devices. However, most mobile devices now store user data on Self-Encrypting Drives (SEDs), which provide "always-on" encryption. Mobile OSs leverage the encryption inherent in the SED to provide "hard reset" or "factory reset" functionality to clear nearly all information from the device's memory using a "cryptographic erase" technique [16]. Cryptographic erase is accomplished by sanitizing the encryption key for the drive, rendering the encrypted user data unreadable. Some devices offer a choice to encrypt all user data when the device is initialized. It is essential to activate whole-device encryption before a device is deployed and to perform a "factory reset" operation to cryptographically erase all user data before disposing of a device.

There are two additional considerations for secure device disposal: assured destruction of the drive encryption key and destruction of user data on removable memory cards (e.g., SIM or Secure Digital [SD] cards). If the device encryption key is backed up or escrowed outside the device, it is possible that the key could be used to recover user data on the device. The organization should address the existence and location of such backups when designing device sanitization procedures.

In addition to storing information such as photos and downloaded documents on the device's internal memory, many mobile devices store such information on an external SD card. Contacts, voicemails and text message logs may be stored on a SIM card as well as in the device's internal memory. A factory reset will not clear the information contained on SIM or SD cards used with the device. To remove all information from these cards they should be physically removed and destroyed. A thorough device disposal process includes both a factory reset and removal of any associated cards.

References

The lists below provide examples of resources that may be helpful in better understanding mobile device security.

[1] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[2] Ogata MA, Franklin JM, Voas JM, Sritapan V, Quirolgico S (2019) Vetting the Security of Mobile Applications. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-163, Rev. 1. https://doi.org/10.6028/NIST.SP.800-163r1

[3] Cichonski JA, Franklin JM, Bartock MJ (2016) Guide to LTE Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-187. https://doi.org/10.6028/NIST.SP.800-187

[4] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[5] National Institute of Standards and Technology (2019), *Mobile Threat Catalogue*, Available at https://pages.nist.gov/mobile-threat-catalogue/

[6] Franklin JM, Brown CJ, Dog SE, McNab N, Voss-Northrop S, Peck M, Stidham B (2016) Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8144. https://csrc.nist.gov/csrc/media/publications/nistir/8144/draft/documents/nistir8144_draft.pdf

[7] U.S. National Information Assurance Partnership (NIAP) (2019) Available at https://www.niap-ccevs.org

[8] U.S. National Information Assurance Partnership's (NIAP) (2019) *Product Compliant List*. Available at https://www.niap-ccevs.org/Product/

[9] U.S. National Security Agency's (NSA) (2019) *Commercial Solutions for Classified Program (CSfC).* Available at https://www.nsa.gov/resources/everyone/csfc/

[10] U.S. National Security Agency's (NSA) (2019) *Commercial Solutions for Classified Program (CSfC) Components List.* Available at https://www.nsa.gov/resources/everyone/csfc/components-list

[11] U.S. National Security Agency's (NSA) (2019) *Commercial Solutions for Classified Program (CSfC) Trusted Integrator List.* Available at https://www.nsa.gov/resources/everyone/csfc/trusted-integrator-list.shtml

[12] Federal CIO Council, *Mobile Computing Decision Framework*, May 23, 2013.

[13] U.S. National Institute of Standards and Technology (2019) *Cryptographic Algorithm Validation Program (CAVP).* Available at https://csrc.nist.gov/projects/cryptographic-module-validation-program

[14] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[15] The MITRE Corporation (2019) *Adversarial Tactics, Techniques & Common Knowledge Mobile Profile (ATT&CK).* Available at https://attack.mitre.org/mobile/index.php/Main_Page

[16] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[17] U.S. National Institute of Standards and Technology (2019) *Cryptographic Module Validation Program (CMVP).* Available at https://csrc.nist.gov/projects/cryptographic-module-validation-program

[18] Miller JF, (2013) *Supply Chain Attack Framework and Attack Patterns MITRE Technical Report MTR140021.* Available at https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

[19] First.Org, Inc. (2019) *Common Vulnerability Scoring System SIG*. Available at https://www.first.org/cvss/

[20] National Institute of Standards and Technology (2019) *National Vulnerability Database: Vulnerability Metrics, (National Institute of Standards and Technology* Gaithersburg, MD). Available at https://nvd.nist.gov/vuln-metrics/cvss

[21] Apple (2018) *iOS Security Guide*. Available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[22] Android 2016 *Android Security White Paper.* Available at https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf

[23] Department of Homeland Security (2017) *Study on Mobile Device Security*. (Washington, DC). Available at https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

[24] Franklin JM, Bowler K, Brown CJ, Dog SE, Edwards S, McNab N, Steele M (2019) Mobile Device Security: Cloud and Hybrid Builds. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-4. https://doi.org/10.6028/NIST.SP.1800-4

[25] Lookout (2015) *Stagefright Detector: Lookout's app tells you if your Android device is vulnerable*. Available at https://blog.lookout.com/stagefright-detector

[26] Armis (2017) *The Attack Vector "BlueBorne" Exposes Almost Every Connected Device*. Available at https://www.armis.com/blueborne/

[27] Google (2019) *The Android Management API.* Available at https://developers.google.com/android/management/introduction

[28] Apple (2019) *Mobile Device Management Protocol Reference.* Available at https://developer.apple.com/library/content/documentation/Miscellaneous/Reference/MobileDeviceManagementProtocolRef/1-Introduction/Introduction.html

[29] Black PE, Badger ML, Guttman B, Fong EN (2016) Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8151. https://doi.org/10.6028/NIST.IR.8151

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

[31] Health Insurance Portability and Accountability Act of 1996, H. Rept. 104-736, H.R. 3103. https://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CRPT-104hrpt736&packageId=CRPT-104hrpt736

[32] Lookout (2016) *Technical Analysis of Pegasus Spyware.* Available at https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

[33] McConnell, Steve, *Code Complete: A Practical Handbook of Software Construction*, Microsoft Press, 2nd edition, June, 2004.

[34] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 2. https://doi.org/10.6028/NIST.IR.8011-2

[35] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[36] Center for Internet Security (2019) *Apple iOS Benchmark.* Available at https://www.cisecurity.org/benchmark/apple_ios/

[37] Center for Internet Security (2019) *Google Android Benchmark.* Available at https://www.cisecurity.org/benchmark/google_android/

[38] The United States Department of Justice (2015) *The Privacy Act of 1974*. Available at https://www.justice.gov/opcl/privacy-act-1974

[39] National Institute of Standards and Technology (2019) *National Vulnerability Database.* Available at https://nvd.nist.gov/

[40] National Institute of Standards and Technology (2019) *National Checklist Program Repository.* Available at https://nvd.nist.gov/ncp/repository

[41] Ferraiolo H, Cooper DA, Francomacaro S, Regenscheid AR, Burr WE, Mohler J, Gupta S (2014) Guidelines for Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157. https://doi.org/10.6028/NIST.SP.800-157

[42] Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[43] Scarfone KA, Jansen W, Tracy MC (2008) Guide to General Server Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-123. https://doi.org/10.6028/NIST.SP.800-123

[44] Dodson D, Souppaya, MP, Scarfone K (2019) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology Gaithersburg, MD), Draft NIST Cybersecurity White Paper. Available at https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

[45] Frankel SE, Kent K, Lewkowski R, Orebaugh AD, Ritchey RW, Sharma SR (2005) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77. https://doi.org/10.6028/NIST.SP.800-77

[46] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[47] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[48] Souppaya MP, Scarfone KA (2016) Draft NIST SP 800-154, Guide to Data-Centric System Threat Modeling. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-154. Available at http://csrc.nist.gov/publications/drafts/800-154/sp800_154_draft.pdf

Appendix A. Acronyms and Abbreviations

Selected acronyms and abbreviations used in this publication are defined below.

AP	Access Point
API	Application Programming Interface
ATARC	Advanced Technology Academic Research Center
B2B	Business-to-Business
BYOD	Bring Your Own Device
CAVP	Cryptographic Algorithm Validation Program
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMVP	Cryptographic Module Validation Program
COPE	Corporately Owned, Personally Enabled
CYOD	Choose Your Own Device
DEP	Device Enrollment Program
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DRM	Digital Rights Management
EMM	Enterprise Mobility Management
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GFE	Government Furnished Equipment
GLONASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPsec	Internet Protocol Security
IR	Interagency/Internal Report
IT	Information Technology
ITL	Information Technology Laboratory
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAM	Mobile Application Management
MAV	Mobile Application Vetting
MCDF	Mobile Computing Decision Framework
MDM	Mobile Device Management
MitM	Man in the Middle
MTD	Mobile Threat Defense
MTP	Mobile Threat Protection
NFC	Near Field Communication
NGO	Non-Governmental Organization
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology

NSA	National Security Agency
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OS	Operating System
PAN	Personal Area Network
PID	Process Identifier
PII	Personally Identifiable Information
PIN	Personal Identification Number
P.L.	Public Law
QR	Quick Response
RADIUS	Remote Authentication Dial-In User Service
RFID	Radio Frequency Identification
RTOS	Real Time Operating System
SaaS	Software as a Service
SD	Secure Digital
SDK	Software Development Kit
SED	Self-Encrypting Drive
SIM	Subscriber Identity Module
SoC	System on a Chip
SP	Special Publication
SSID	Service Set Identifier
TEE	Trusted Execution Environment
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
UID	User Identifier
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VMI	Virtual Mobile Infrastructure
VPN	Virtual Private Networking
WiFi	Wireless Fidelity
WLAN	Wireless LAN
XML	Extensible Markup Language

Appendix B. Supporting NIST SP 800-53 Security Controls

The list below maps mobile security technologies to the appropriate NIST SP 800-53 security controls and to the Cybersecurity Framework version 1.1 functions, categories, and subcategories.

Mobile Technology	Capabilities	NIST SP 800-53 rev. 4 - Control Families	NIST SP 800-53 rev. 4-Security Controls	NIST Cybersecurity Framework (CSF) Functions, Categories, Subcategories		
				Function	CSF Category	CSF Subcategory
Enterprise Mobile Management (EMM) or Mobile Device Management (MDM)	Access Control	Access Control	AC-3, AC-4, AC-6, AC-7, AC-8, AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20	Protect	Identity Management, Authentication and Access Control	PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7
					Data Security	PR.DS-5
					Protective Technology	PR.PT-4
				Identify	Asset Management	ID.AM-3
		Identification & Authentication	IA-2, IA-3, IA-5, IA-6, IA-7, IA-10	Protect	Identity Management, Authentication and Access Control	PR.AC-1
		Security Assessment and Authorization	CA-1, CA-9	Identify	Asset Management	ID.AM-3
					Governance	ID.GV-1, ID.GV-3
	Data Protection	Media Protection	MP-5, MP-6, MP-7	Protect	Protective Technology	PR.PT-2
		System and Communications Protection	SC-3, SC-4, SC-7, SC-12, SC-13, SC-23, SC-24, SC-28, SC-39, SC-43	Protect	Protective Technology	PR.PT-4, PR.PT-4
					Identity Management, Authentication and Access Control	PR.AC-5
					Data Security	PR.DS-1, PR.DS-2, PR.DS-5
	System Integrity	System and Information Integrity	SI-2, SI-3, SI-4, SI-7	Identify	Risk Assessment	ID.RA-1
				Protect	Data Security	PR.DS-5, PR.DS-6
				Detect	Anomalies and Events	DE.AE-3
					Security Continuous Monitoring	DE.CM-1, DE.CM-4, DE.CM-7
				Respond	Analysis	RS.AN-1

Mobile Technology	Capabilities	NIST SP 800-53 rev. 4 - Control Families	NIST SP 800-53 rev. 4-Security Controls	NIST Cybersecurity Framework (CSF) Functions, Categories, Subcategories		
				Function	CSF Category	CSF Subcategory
		Configuration Management	CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, CM-11	Protect	Information Protection Processes and Procedures	PR.IP-1
				Detect	Security Continuous Monitoring	DE.CM-7, DE.CM-3
	Detection and Monitoring	Audit and Accountability	AU-2, AU-3, AU-5, AU-7, AU-8, AU-9, AU-10, AU-12, AU-14	Identify	Supply Chain Risk Management	ID.SC-4
				Protect	Protective Technology	PR.PT-1
				Respond	Analysis	RS.AN-3
		Incident Response	IR-5	Detect	Anomalies and Events	DE.AE-3, DE.AE-5
				Respond	Analysis	RS.AN-1, RS.AN-4
		Security Assessment and Authorization	CA-9	Identify	Asset Management	ID.AM-3
Virtual Private Network (VPN) Endpoint	Access Control	Access Control	AC-4, AC-17	Identify	Asset Management	ID.AM-3
				Protect	Identity Management, Authentication and Access Control	PR.AC-3, PR.AC-5
					Data Security	PR.DS-5
					Protective Technology	PR.PT-4
		Identification and Authentication	IA-3	Protect	Identity Management, Authentication and Access Control	PR.AC-1, PR.AC-7
	Data Protection	System and Communications Protection	SC-8, SC-11	Protect	Data Security	PR.DS-2, PR.DS-5
	System Integrity	System and Information Integrity	SI-4	Detect	Anomalies and Events	DE.AE-1, DE.AE-2
					Security Continuous Monitoring	DE.CM-7