CHAPTER

MANAGEMENT OF MOBILE APPLICATIONS

6

We all know the future is mobile, right? And the iPhone and iPad are Perfect Expressions of Beauty, Ideal Combinations of Form and Function. Except they're Not.
John Battelle

As we grow up in more technology-enriched environments filled with laptops and smart phones, technology is not just becoming a part of our daily lives—it's becoming a part of each and every one of us.
Adora Svitak

As with any relatively recent technological development, terminology is still in flux. While the use and meanings of terms may evolve even before the ink is dry on the first printing of this book, it is important to clarify some common terms that are relevant to this chapter. However, to avoid confusion and ambiguity, we will begin with a review of widely used terminology.

Enterprise mobility management (EMM) reflects the global **management** of the mobile environment. It typically involves the combination of **mobile device management (MDM)**, **mobile application management (MAM)**, and **mobile security management (MSM)**. Fig. 6.1 illustrates the interrelationships of these pieces.

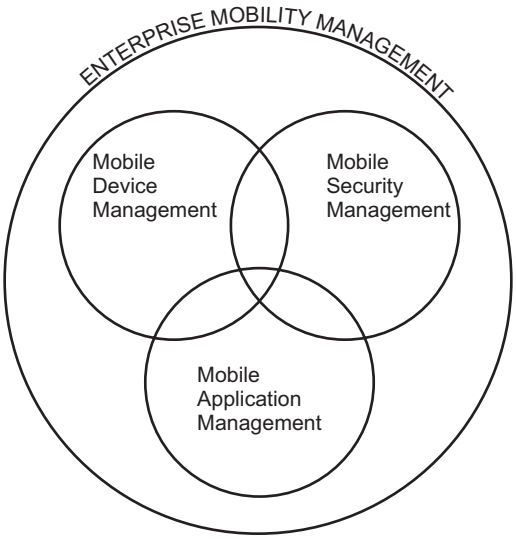

FIGURE 6.1

Enterprise mobility management.

Application Performance Management (APM) in the Digital Enterprise. http://dx.doi.org/10.1016/B978-0-12-804018-8.00006-1

The focus of MDM is the administration of the physical **mobile devices**. In particular, MDM is focused on making sure that the devices are configured and operating properly. MDM is also concerned with securing the devices and corporate data on those devices.

MAM is concerned with provisioning and controlling access to business **applications** running on mobile devices. It also provides controls at the application level that allow information technology (IT) to manage and secure application data.

The primary function of MSM is to control which applications and data users can access, download, or transmit and how those applications are permitted to be used. MSM profiles define privileges within the applications as well as access rights.

The security of MSM, MDM, and MAM will be addressed in Chapter 8.

MOBILE APPLICATIONS

The management of **mobile applications** is a complex and challenging issue. First, it is important to clarify exactly what is meant by "mobile applications." Applications themselves are not independently mobile. Applications reside and run on some type of computer. It does not matter if that computer is a **mainframe**, server, laptop, tablet, smartphone, or something else.

Without some kind of computer to run the program, an application is simply a set of coded instructions. Like a lightbulb without a source of electricity, its potential cannot be realized. If a computer is intended to be portable and is routinely moved from one location to another, then the applications that run on it are mobile. Of course, that begs the question of what is meant by "portable." Consider a rack-mounted server on an oil tanker that travels the globe. Does the movement of the ship mean that the server is portable? The answer is: "No!" This server may be administered locally or remotely and users may access applications running on it or elsewhere. However, the device itself is in a (relatively) fixed location. It is not designed to be carried to different locations on the ship or ashore.

> A mobile application (mobile app) is any application that runs on or is accessed from a device designed to be portable.

Mobile applications can be thought of as being characterized by the types of devices on which they run. There are three broad categories of mobile devices that will be considered in this chapter (Fig. 6.2):

- Laptop computers
- Tablets and smartphones
- Embedded devices

The embedded devices group includes a wide variety of devices ranging from handheld GPS units to smart cars, to portable gaming devices and many, many other devices. Each of those devices contains software that is more than some simple code burned permanently onto a chip.

FIGURE 6.2

The diverse world of mobile computing.

The primary focus of this chapter is applications that run on mobile devices—that is, laptops and handheld devices (tablets and smartphones). The applications may run entirely on the mobile device or be accessed from the mobile device, or it may be a combination of the two. The **Internet of Things (IoT)** includes a variety of applications running on a diverse assortment of devices, many of which are mobile. However, those applications will be addressed in Chapter 17.

For purposes of the discussion in this chapter, mobile applications must be manageable. That is, they must be:

- Addressable (i.e., can be communicated with)
- Configurable
- Updatable (e.g., a new version of the software installed)

BASIC MANAGEMENT OBJECTIVES

The objectives of **application management** were addressed in Chapter 3, but a quick review is in order. In simplest terms, the objective of application management is to ensure that the user can securely access the functionality and data provided by the applications whenever required at a level of **performance** that meet the user's needs. It is important to recognize that application management does not exist in isolation. System management is required to manage the performance and availability of the mobile device on which the application(s) run. Network management is necessary to allow the application to communicate with databases or applications located elsewhere. However, despite their importance, network management and system management are beyond the purview of this book.

Application management functions can be performed locally, on the mobile device, by the user. Consider one of your personal mobile devices. For the moment, we will use the example of a smartphone, although it could just as easily be a tablet or a laptop. You can go to the app store, purchase, download, install, and configure (i.e., adjust the settings) an incredible variety of applications. You can also configure the operating system (OS) or even download and install new versions of the **operating system** (it is important to remember that an OS is just another software element, albeit a special purpose one). You personally "monitor" the phone and any applications that you are using (or attempting to use). That is, you will be able to recognize if an app is available and working properly whenever you attempt to use it.

Alternatively, if the necessary management software is in place on the smartphone, and permissions granted, it is possible for an administrator to remotely perform some of the management tasks that can be done by a user. The smartphone managed by the administrator may be one issued by the company or a personal one authorized for business uses. Research has found that 78% of mobile devices (smartphones and tablets) and 46% of all laptops used to perform business tasks are employee owned.[1] In fact, depending on company policy, an administrator may have the authority to:

- Install (or update) applications
- Change the configurations of applications

[1]"Effective BYOD Management: Empowering a Mobile Workforce" Enterprise Management Associates, 2016.

FIGURE 6.3

Autonomous mobile computing.

- Grant or revoke access to applications or data
- Delete applications or data from the device
- Disable the device completely
- Monitor an application (i.e., availability and performance)
- Enforce security policies

LOCAL APPLICATIONS

In broad terms, there are three types of applications that may run on a mobile device. First, there are those that are strictly local applications (autonomous mobile computing), which means they do not require access to any resources other than those that may be found on that mobile device (or within a container on that device). For example, a spreadsheet on a laptop is a local application. Similarly, a notes application, an MP3 player, and a calculator on a smartphone or tablet are examples in those environments (Fig. 6.3).

REMOTE DATA

Second, there are applications that run on the mobile device but require access to data that is located somewhere else to provide the information or perform the function for which the applications were designed. In general, this means interfacing with an application on another computer to retrieve the required data. Once the data is retrieved, it may be stored and used later and analyzed in some manner. An eReader is a simple example of this type of application. The application user may use the local application to purchase and download a book. The book is stored on the device. The user can read the book later and even annotate it or bookmark it. A more sophisticated example is Microsoft Office 365. This application retrieves data required by the user from a server in the cloud. That data can then be reviewed or modified on the local device without maintaining the connection to the server. The next time the local application is able to connect to the host, the modified data will be uploaded.

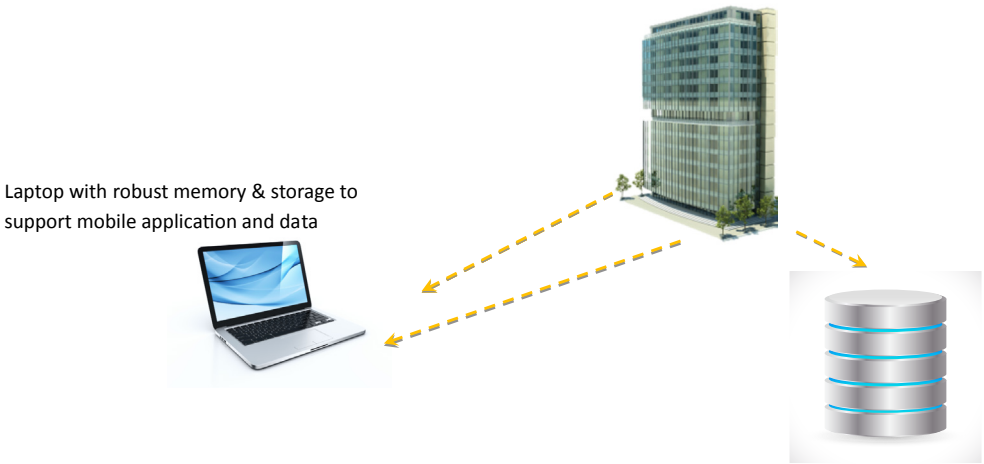

FIGURE 6.4

Dependent mobile computing.

The concept represented by Fig. 6.4 (dependent mobile computing) is that a robust version of the application resides on the mobile device. In fact, in this case, most or all of the application functionality will reside on the mobile device and the host is accessed only to download or upload data. While not exclusive to laptop computers, that is the platform that is best suited to this model since the laptop will normally have much greater memory and storage available. Alternatively, a mobile device may have only minimal data and application functionality on the device itself. It then acts more in the role of providing a user interface and enabling access to full functionality and data on a remote system.

REMOTE FUNCTIONALITY

Whenever data reside on a mobile device, **security** must be given serious consideration. However, the level of security will be dependent on the sensitivity of the data. If the only data being stored are publicly available (e.g., statistics for the user's favorite sports team), then the need for security is minimal. Alternatively, if the data include confidential products plans or pricing strategy, then close attention must be given to securing the application and its data. Security for applications will be discussed in greater detail in Chapter 8.

The third category of mobile applications includes those that rely almost entirely on remote applications to provide the information or functionality required by the user. In this case, the mobile device is essentially acting as a smart terminal. There is an application resident on the mobile device; however, its roles are to enable secure access to the primary application and data residing on a remote server and to display the information supplied by that remote application. There are countless mobile applications that fall in this category—news service applications, travel applications, social media, weather forecasts, stock reports, and sites for rating restaurants, hotels, etc.

To greater and lesser extents, each of these types of applications can be found running on laptops, tablets, and smartphones. Tablets and smartphones tend to make greater use of the remote data and remote functionality types of applications. Laptops are very much a mixed bag. The primary type is determined by the nature of the work being done and the company's IT strategy. For example, at Enterprise Management Associates (EMA), the analysts use Microsoft Office extensively. In EMA's case, the policy for Microsoft Office is that each user has a copy of the software installed on his/her laptop (local application). They also use some SaaS applications (remote functionality).

APPLICATIONS ON LAPTOPS

The objectives and challenges of application management are largely the same, regardless of the type of device on which the applications run. However, the technologies, tools, and processes vary significantly from one environment to another. The vast majority of laptops are **personal computers** running some version of Windows and a much smaller number run MacOS.[2] There are still other operating systems for laptops, including Chrome OS, Linux, and Unix.

When an application runs on a laptop computer, most of the issues and solutions are very similar (or even identical) to those for applications running on desktop personal computers (PCs). However, there are some important differences.

First, in general, there are periods when a laptop computer is not connected to a network and therefore does not meet the first requirement for manageability: it is not addressable. It may simply be turned off or may be in a location where a network connection is not available or is not permitted. Without connectivity, remote management tasks cannot be performed until it is possible to once again communicate with the laptop.

Second, mobile devices and the applications that run on them are inherently less secure than their counterparts. Because the devices are small and portable, they are easy to conceal and that makes them more likely to be stolen. In fact, research by EMA found that one of every 12 mobile device users reported they had a device lost or stolen within the past year.[3] It also makes it easier for them to be lost. This is more likely when the device is taken outside of the company's facilities. However, even within the confines of an enterprise's premises, mobile devices can be lost, stolen, or damaged beyond repair (it is really impressive to see how much damage can be done to a laptop when it is run over by a forklift). That mobility greatly increases the likelihood that the laptop will end up in a place where it should not be; a place where bad things happen to good devices. An example of this is illustrated in Fig. 6.5 (That example happened recently to an EMA analyst's laptop with the unfortunate, predictable results.) Unfortunately, there is no way that administrators or management tools can prevent this from happening. Administrators can try to teach users how to treat a laptop, but as many comedians are quick to point out, there is no cure for stupid. Therefore, some users will learn and adapt how they protect their laptops, while others will not. This makes backup and security even more important than they are for non-mobile devices.

[2]Research conducted by EMA found: 90% Windows, 6% Macs, 3% Chromebooks, 1% Linux on business-used laptops. Ibid.
[3]Ibid.

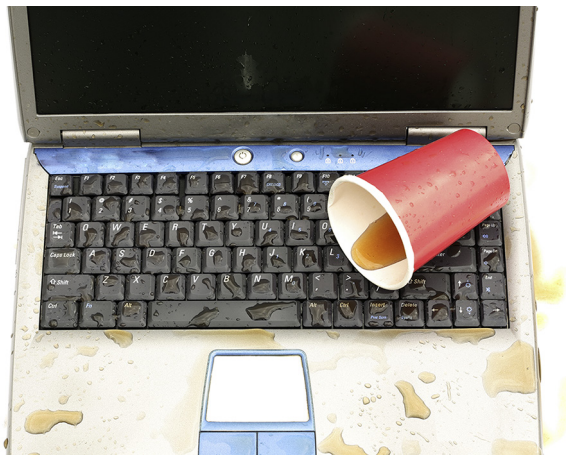

FIGURE 6.5

Bad things can happen to good devices.

Third, when a mobile device is taken outside of the enterprise, it is also taken outside of the enterprise's **firewall**. That makes it much more vulnerable to attacks. This also raises the importance of having good security in place for every mobile device.

As long as the mobile devices are owned by the enterprise, it is easier for the organization to require access to exercise control over the device. The key word is "require." It is much harder to actually enforce those policies. Users are inclined to view the devices as their personal property. Unless there is management software in place to prevent or at least limit the possibility of policies being violated then is likely that some individuals will violate them. Therefore management software needs to be coupled with the promise of serious consequences for the employee if violations do occur (e.g., "… will be subject to disciplinary action up to and including dismissal"). Eventually, most users will violate policies. The most common policy violations are:

- Loading unauthorized applications (frequently games)
- Loading personal data (photos, documents, email, etc.)
- Disabling of security features
- Connecting to unsecured networks or websites
- Using USB drives to load data from outside of the corporate domains (a common way for the introduction of malware)[4]

However, when the device is the property of the employee, the difficulty increases significantly—and that is the world of **bring your own device (BYOD)**.

[4]50 percent of users who find a USB drive will plug it into their computer. http://www.theregister.co.uk/2016/04/11/half_plug_in_found_drives/.

TABLETS, SMARTPHONES, AND BYOD

The use of company-issued laptops was getting along fairly well. Yes, there were occasional problems, but generally things worked reasonably well. Then came the smartphone, which began in a seemingly innocuous way. In 2007, Apple introduced the iPhone. Employees started to buy them for their personal use. It took the tech-savvy ones about 30 seconds to realize that they could access their personal email from their phones. It was only a small step from that to wanting to be able to access their company email. Next came the call for access to other business applications. The inflection point for **mobile computing** happened in 2009. It was in that same timeframe that BYOD entered the picture (strictly speaking, devices used for BYOD do not have to be mobile, but the term is generally used to refer to mobile devices).

The basic premise of BYOD is that employees are allowed to use devices that they own to do some or all of their work. The impetus for BYOD came from two directions—employees and enterprises. Many employees had strong preferences regarding the type of mobile device they used. However, letting each employee specify and select the mobile devices that he or she would use promised to create a support nightmare. BYOD became the compromise solution. Employees are given the freedom to choose the device that they prefer but are responsible for providing the technical support for their device(s).

Organizations began to take an alternative approach to providing employees with laptops, phones, and tablets. Instead, they gave employees a sum of money with which to buy the appropriate piece of equipment. For example, they might give an employee an allowance of up to $500 for the purchase of a smartphone. The employee could purchase whichever brand he or she preferred and have it configured however they wish, as long as it met a set of minimum specifications defined by the company. If the employee wanted a smartphone that cost more than $500, the employee had to pay the amount in excess of the allowance.

In each case, in the world of BYOD (regardless of whether it is a laptop, tablet, or smartphone), the mobile device is the property of the employee. That ownership brings with it a new set of problems and challenges. However, the business must protect its interests. Therefore, if the device is going to be used to run business applications, the organization must establish a set of reasonable policies that must be followed if access to business applications and/or data is to be permitted (this will be addressed in Chapter 8).

Another difference in a BYOD environment is that the employee is "technical support" for that device and the applications that run on it (while not true in every instance, this is the norm for BYOD). This means that the employee is responsible for the installation, configuration, and performance of each application on that device. It is the employee's responsibility to ensure that personal applications running on the device do not conflict with the business applications.

On the other hand, it is the responsibility of the organization to grant or restrict access to business applications and data. A key question that must be addressed is whether to permit data to be downloaded to the device. The simplest and most secure answer is to not permit any data to be downloaded to any device. However, this approach does limit when business applications can be accessed, since it requires that the device is connected in order to use any remote data. This is a thorny question that any organization allowing mobile applications must address.

Certainly, some mobile applications reside completely on a mobile device. Perhaps they exist in total isolation from other applications, systems, and data. The more common types of mobile

applications are ones that, at a minimum, access data that exists remotely. The entire application may reside on the mobile device and only the data is remote.

The other common scenario is one in which the mobile app is just a small fragment of software that runs on the mobile device and acts as an interface to the full application and data stores that exist elsewhere. In this scenario, while capable of much more, the mobile device is acting essentially as a thin client. The mobile app is simply acting as a means to provide access to the functionality of the remote application.

SECURITY IN BYOD[5]

The primary function of management solutions is to support BYOD and logically isolate business applications, data, and services (i.e., email, messaging, web browsing, etc.) from a user's nonbusiness resources (i.e., personal applications, email, games, and silly cat videos). In this way, the business IT operations can manage, secure, and restrict the enterprise resources without impacting or limiting any other device uses. Typically, profile-based policies are applied to a BYOD management solution allowing configuration and access rights for business resources to be customized for each individual user. While there are a number of resource isolation solutions on the market, they all principally fall into one of the following categories:

Desktop Virtualization

Arguably the first BYOD technology developed, desktop virtualization abstracts a user's workspace environment from the underlying device hardware and operating system. While there are many different types of desktop virtualization, the most commonly recognized is virtual desktop infrastructure (VDI), which remotely hosts a distinct workspace for each user on back office servers and displays them on any network-attached endpoint devices. The leading VDI technologies can be used on just about any endpoint device; however, since they are commonly implemented to be used on devices with larger screen sizes, they are most commonly used on desktop and laptop PCs.

Application Virtualization

Individual software components are hosted and run on enterprise servers but are displayed on user devices. To end users, a virtual application appears like any other local application on their device, but it is centrally maintained and restricted by the business. A particular advantage to this approach is that it allows application built on one platform to operate on any other. For instance, a Windows application can be accessed and used on an iPad or Android tablet.

Containerized Workspace

Containerization as a technology is an offshoot of virtualization with one principal difference, a container is completely self-contained and does not require the preinstallation of a hypervisor on the endpoint. While this simplifies the deployment process, it means any software must be designed for use specifically on the platform on which it will be run. For instance, a Windows application can only run on a Windows device and an iOS application can only run on an iOS device, etc. With this approach, an entire workspace environment—including all enterprise

[5]The BYOD Security section is taken from EMA Radar for Mobile Security Management (MSM), Enterprise Management Associates and is available at www.enterprisemanagement.com.

applications, data, and services—are available inside a single container. To access business resources, users simply open the container and use the isolated resources inside. Sometimes this method is referred to as a "duel persona" solution, although that term could reasonably also be applied to desktop virtualization.

Containerized Applications

Individual applications may be containerized rather than a whole desktop. Similar to application virtualization, end users are presented with business applications that appear on their devices just like any other local application, so there is no need to switch between a business environment and a personal environment.

App Wrapping

Rather than fully isolating an application, code can be added to an application that ensures it follows centrally-managed policies. There are two methods for accomplishing this. The most common method is for application developers to install hooks in their code that allow external management platforms to alter aspects of the application. Alternatively, a piece of software can be used that executes the application and effectively filters its use to limit its use or provide additional layers of authentication. While the latter approach can be effectively applied to any application (not just those supported by app developers), there are fewer application features than can be managed externally. For some time, app wrapping was generally preferred as the best approach to mobile app management; however, due to recent legal concerns over licensing altered software and a dwindling support from application developers who are not fond of maintaining hooks in their code for a variety of different management platforms, this approach has somewhat fallen out of favor.

Business-Dedicated Applications

Rather than relying on unsecure consumer applications, some organizations prefer to deploy business-dedicated applications that are designed to be inherently secure and may be managed from a centralized policy-based platform. For instance, a business-dedicated email package may be deployed that only allows messages to be sent from users to authorized personnel (limiting the distribution of sensitive information and files). Users would have a separate email solution for personal messages which has no access to business information. Similar software solution can be deployed for document editing, file sharing, web browsing, and remote access to business systems.

These approaches to BYOD management are not exclusive, and, in fact, most organizations that have adopted a BYOD platform employ more than one method. For instance, a virtual application can run on a virtual desktop or within a containerized workspace. Or another example might be using any business-dedicated applications that are available supplemented by app wrapping on any additionally required applications. Each organization is unique in its endpoint requirements, and care must be taken in deciding which approaches to use that will provide the best balance of accessibility with security in each particular use case.

SUMMARY

The first objective of mobile app management is to ensure that users are able to access the application functionality and the business data they require to do their jobs. Concurrent with providing that access, the other objective of application management is to protect corporate data and other assets.

KEY TAKEAWAYS

- Managing mobile applications consists of enabling users while protecting corporate assets.
- BYOD increases risk while shifting administrative responsibilities to the device's owners.
- Management of applications running on laptops can be very similar to managing applications on desktop PCs. However, the lack of persistent connectivity makes the management more difficult.
- Mobile computing has an inherently greater risk than computing done within the physical confines of the enterprise.