Security Management Considerations for Mobile Devices

Brian Davis

Mobile devices have been in existence for many years now. This class of computers began with the invention of laptops and, within the past few years, smartphones have been introduced and has quickly gained popularity. Data, ranging from personal information, to sales data, to industry secrets can now be accessed from or taken anywhere in the world. This brings about security concerns for all organizations, whether nonprofit and for-profit. Just like stationary computers, desktops and servers, these devices can be compromised by an attacker. What are some steps organizations can take to mitigate the threat and utilize the productivity increase that mobile devices provide?

The term "mobile device" can include a range of different devices. Most are small and easy to carry and transport, with some fitting into pockets. To narrow things down, NIST Special Publication 800-124 defines the term with the following baseline hardware and software characteristics:

- A small form factor
- At least one wireless network interface for Internet access (data communications)
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through multiple methods (provided with the operating system, accessed through web browser, acquired and installed from third parties)
- Built-in features for synchronizing local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.)

Optional characteristics include (but this list is not all inclusive):

- Network services:
    - One or more wireless personal area network interfaces, such as Bluetooth or near-field communications
    - One or more wireless network interfaces for voice communications, such as cellular
    - Global Positioning System (GPS), which enables location services
- One or more digital cameras
- Microphone
- Storage:
    - Support for removable media
    - Support for using the device itself as removable storage for another computing device (Souppaya & Scarfone, 2013)

For the scope of this article, laptops and tablet laptop computers, even though they are mobile in nature, will not be included since they typically have a full-featured operating system, even if most of the security threats mentioned later in this article apply to them. Full-featured operating systems allow for security policies to be created and applied to each system. So, with all of that stated, what is left to qualify? Devices that fit into the definition are smartphones, tablets, and others such as iPods, which include more functionality than a MP3 player. These

devices typically come installed with Android, iOS or Windows Phone and can be manufactured by various vendors such as Apple, Motorola, Samsung, Nokia, LG, and others.

Over the past several years, the number of mobile devices in use has increased every year since 2005. According to comScore, in just 4 years (December 2010 to December 2014), smartphone usage increased 394%, compared to a 34% increase in desktop usage. 75% of all people who own a mobile phone have a smartphone. The majority of users, regardless of age, now identify as using both mobile devices and desktop computers. (Comscore Inc., 2015) This has led to a greater possibility that organizational data is being accessed on mobile devices.

One of the main security concerns regarding mobile devices is malware. Malware is not present just on desktop computers, but can manifest on mobile devices as well. According to Gartner, "for attackers to get hold of files, they need to attack mobile apps…" (Zumerle & Hill, 2015) Just like on desktop computers, this type of software attempts to do malicious things like intercept banking information, passwords, and scan for personal information such as Social Security numbers. Specifically on mobile devices, malware can lead to a faster battery depletion rate. (He, 2013) Most malware gains access to mobile devices through third party application stores. In 2012, malware detected on Android devices increased 365%. Also, 99 percent of all malware detected in 2012 was written for Android, with less than 1 percent from the other platforms. (Harris & Patten, 2013) Apple devices have resisted the trend due to the fact that their "application distribution is limited to a centralized marketplace, the Apple Store, that signs all applications, subject to conformance to Apple application publishing criteria." (Asokan, Davi, Dmitrienko, Heuser, Kostiainen, Reshetova, Sadeghi, 2013) Google is not alone in the battle to prevent malware in their store and on Android devices. A threat vector exists that allows for apps to be "side loaded" onto iOS devices abuses enterprise provisioning profiles. This can be accomplished through third party app stores, email attachments, or webpages. (Lookout Inc., 2015)

Another concern on the application side is jailbreaking and rooting of mobile devices. Either option allows for users to bypass certain restrictions placed by manufacturers. This, in turn, allows for apps to be installed from unverified sources. It is much easier for malware to be installed and operate on these devices. Estimates place the number of jailbroken iOS devices at 8% and 27% of Android devices are rooted. (Lookout Inc., 2015) There are a number of different indications that a device has been rooted. On Android devices, when the device is rooted, the build tags are typically changed from "release-keys" to "test-keys", the Over the Air (OTA) certs are not present, packages such as Superuser (enables the su command) and Chainfire are present, and the /data directory is readable (which normally isn't in a non-rooted device.) (Gruber, 2013) Jailbroken Apple devices do share a similarity with Android devices in that there will likely be folder permission changes. There are two ways to jailbreak an iOS device: through a bootrom exploit which runs at bootup, or through an exploit of the application layer. Some jailbreaking methods leave the device with a well-known SSH password. Other reliable ways of detecting a jailbreak is whether a process can "fork" (in a normal iOS setup, processes are not allowed to fork), what number is returned when system() is called, what functions are currently loaded in dylibs, and whether a program called Cydia is installed. (Zmysłowski, 2014) (Asokan, Davi, Dmitrienko, Heuser, Kostiainen, Reshetova, Sadeghi, 2013)

Another significant security concern is that Wi-Fi and cellular networks are not completely secure. The popular Wi-Fi encryption techniques WEP, WPA and WPA2 are all vulnerable. WEP is vulnerable in a number of ways due to static encryption keys that are available and identical on every system connected, a vulnerable RC4 encryption algorithm, and an easily intercepted IV key. WPA, introduced in 2004 through the IEEE 802.11i security standard, sought to improve upon WEP by introducing a Temporary Key Integrity Protocol and a Message Integrity Check (MIC). But, just like WEP, its security remained temporarily before a flaw was found. These attacks focus on the fact that WPA reuses the same encryption algorithm, RC4, as WEP. It also uses the 4-way handshake protocol, which is vulnerable to dictionary attacks. Another type of attack can concentrate on the MAC layer and disconnect clients that were properly connected. Afterwards, the users would be denied access to the network. WPA2 was introduced in mid-2004 after WPA, but unlike WPA, WPA2 fully integrated the technical details of the 802.11i security standard, which made it much more secure. In WPA2, TKIP is replaced by Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) and RC4 is replaced by Advanced Encryption Standard (AES). Even with those improvements, WPA2 has its vulnerabilities too. Over 10 years after being introduced, a number of different attacks have been created to compromise WPA2 networks. Encryption is only applied to the data frames, leaving the management frames open to copying and reuse. These frames perform important tasks such as authentication and de-authentication, to name a few. WPA2 comes with two different modes, Personal and Enterprise. Even these two modes are vulnerable to a dictionary or brute-force attack. (Waliullah & Gan, 2014)

In most travel locations, whether it is an airport, train station, or hotel, Wi-Fi networks are typically unencrypted. They are extremely convenient, but the very nature of unencrypted networks is that they are unsecure. Any data that is transmitted is available exactly how it was encoded originally. The data may not be immediately accessible, but if any encryption were exchanged while being actively sniffed, then that data can be decrypted. Organizations have to be aware that their data could be transmitted over a network like this on a mobile device.

Vulnerabilities in modern cellular networks do not appear to be as prevalent as in Wi-Fi networks, but some still exist. Most of the vulnerabilities are associated with older protocols such as 2G and GSM. Even the widespread cellular data protocol 3G has a few vulnerabilities. 3G uses a cryptography technique, KASUMI, which has been shown to have several weaknesses. Also, cellular range extending devices called femtocells have been exploited in the past using an evil twin attack. (Harris & Patten, 2014) These devices which connect to the carrier's network via the internet can extend the cell network into areas not reached by signals from regular network towers. Theoretically, these devices can be placed anywhere to intercept cell traffic.

Location based services allow for mobile devices to utilize GPS to determine the current location. Typically the device uses that information to determine what businesses and restaurants are nearby. If this location information is intercepted by a hacker, it can be used to target their victim with attacks that could only succeed through close proximity. The attacker could also correlate more location information to see who the targeted victim associates with

and then also target them. This can be mitigated easily by turning off location services. (Souppaya & Scarfone, 2013)

Most mobile devices interact with other computers such as laptops and desktops through a syncing process using a cable. In 2015, Apple and Microsoft announced that their mobile operating systems will become interoperable with their desktop operating systems and have shared features. This feature will not require the use of a cable. Apple introduced this functionality with OS X 10.10 (Yosemite) and, in the second half of 2015, Microsoft will introduce Windows 10. With this level communication between desktop and mobile, there is a high likelihood that malicious software will be programmed to take advantage of this interconnection. Organizations will have to define policies for what is allowed in their environments, but must be careful not to stem the productivity increase that could come from this interoperability.

So, with all of the possible vulnerabilities that can be associated with mobile devices, how can they be managed to mitigate those vulnerabilities? NIST has developed a guideline, Special Publication 800-124 Revision 1: Guidelines for Managing and Securing Mobile Devices in the Enterprise, for organizations and lists steps designed to protect these devices. Even though it is still in draft form, it will be referenced for the following paragraphs.

The first step in securing data on mobile devices is to start the process off by determining the needs of the organization. This process plays into the next crucial step, the development of the mobile device security policy. By this point in an organization, a main security policy should be in place, and the mobile device security policy should be complimentary and should not counter the strategy set in the parent security policy. The elements included in the mobile device security policy should be: what device types are allowed (including device ownership), what those devices can access, the process of screening and configuring each device, administration of the mobile device management servers, and how policies in those servers are updated and distributed. Another part of this policy will likely be what access levels are given, which varies and depends greatly on the needs of the organization. (Souppaya & Scarfone, 2013) Factors that play a role in determining access levels are:

- “Sensitivity of work. Some work involves access to sensitive information or resources, while other work does not. Organizations may have more restrictive requirements for work involving sensitive information, such as permitting only organization-issued devices to be used. Organizations should also be concerned about the legal issues involved in remotely scrubbing sensitive information from BYOD [Bring Your Own Device] mobile devices.
- The level of confidence in security policy compliance. Meeting many of an organization’s security requirements can typically be ensured only if the organization controls the configuration of the mobile devices. For devices not running the organization’s mobile device management client software, some requirements can possibly be verified by automated security health checks conducted by the mobile device management server when mobile devices attempt to connect, but other requirements cannot be verified.

- Cost. Costs associated with mobile devices will vary based on policy decisions. The primary direct cost is issuing mobile devices and client software. There are also indirect costs in maintaining mobile devices and in providing technical support for users.
- Work location. Risks will generally be lower for devices used only in the enterprise environment than for devices used in a variety of locations.
- Technical limitations. Certain types of mobile devices may be needed, such as for running a particular application. Also, an organization's mobile device management client software may only support certain types of mobile devices.
- Compliance with mandates and other policies. Organizations may need to comply with mobile device-related requirements from mandates and other sources, such as a Federal department issuing policy requirements to its member agencies. An example of a possible requirement is restrictions on using mobile devices in foreign countries that have strong known threats against Federal agency systems; in such cases, it may be appropriate to issue 'loaner' mobile devices or to prohibit mobile device use altogether." (Souppaya & Scarfone, 2013)

The next step in the process, after developing a mobile device security policy, is to determine what mobile device management (MDM) solutions are available and create a framework that accomplishes the goals of the security policy. The following factors that should be considered when selecting an MDM is how the software is designed logically, what protocols are used to authenticate and keep data secure, the level to which a device can be secured, and whether the software can provide proof that a device has implemented the policy correctly. There are software packages available from companies such as Apple, Cisco, Citrix, and others which include third parties. There are essentially two different approaches centralized MDM platforms utilize: through a messaging system or through a third party vendor that supports various mobile device manufacturers. Both options are similar to the typical client/server architecture. But, either way, each option has some commonalities in how it communicates with the devices. If the mobile devices are purchased by the organization, the management software typically manages all features of the device. If the mobile device was purchased by and is property of the employee, then the management software typically manages the security and integrity of the organization's data through the use of VPNs or other enterprise services. The application seeks to keep the data separate from the rest of the applications that might be on the device. This also maintains the privacy of the device owner as well. (Souppaya & Scarfone, 2013)

Otherwise, if an organization cannot afford or is unwilling to purchase a mobile device management application, then the individual bears the responsibility of keeping the data secure. NIST authors Murugiah Souppaya and Karen Scarfone note the following security issues:

- "The security controls provided by a mobile device often lack the rigor of those provided by a centralized mobile device management client application. For example, a mobile device often supports only a short passcode for authentication and may not support strong storage encryption. This will necessitate acquiring, installing, configuring, and maintaining a variety of third-party security controls that provide the missing functionality.

- It may not be possible to manage the security of the device when it is not physically present within the enterprise. It is possible to install utilities that manage devices remotely, but it will require significantly more effort to use such utilities to manually apply updates and perform other maintenance and management tasks with out-of-office mobile devices." (Souppaya & Scarfone, 2013)

After developing the MDM software, the next step is to put that software into service and test it before deploying it to all of the mobile devices. Devices should be evaluated to ensure that they can maintain a connection to the resources it has been granted access to, whether they are maintaining confidentiality of the organization's data, whether it is permitting the right person to access the data, whether the applications allowed by the security policy and needed by the user operate properly, whether the technical staff can manage all aspects of the device, how the management software logs events, performance, whether vulnerabilities exist for the MDM software, and how the software is configured to change in the event of a "fall back" situation. (Souppaya & Scarfone, 2013)

Following deployment of the MDM software, it is important to maintain it. The NIST authors recommend the following in order to properly maintain the system:

- "Checking for upgrades and patches to the mobile device software components, and acquiring, testing, and deploying the updates
- Ensuring that each mobile device infrastructure component (mobile device management servers, authentication servers, etc.) has its clock synced to a common time source so that its timestamps will match those generated by other systems
- Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs
- Detecting and documenting anomalies within the mobile device infrastructure. Such anomalies might indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
- Providing training and awareness activities for mobile device users on threats and recommended security practices

Organizations should also periodically perform assessments to confirm that the organization's mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing. More information on technical assessments is available from NIST SP 800-115, Technical Guide to Information Security Testing and Assessment [SP800-115]." (Souppaya & Scarfone, 2013)

Inevitably, devices have to be discarded. This can be due to a number of reasons including obsolescence or damage. Just as is the case with other technology that stores information, it needs to be wiped clean of any data that may still be present on the device. The nuances of flash memory sometimes make the wiping process problematic. NIST publication SP 800-88, Guidelines for Media Sanitization gives further guidelines on how to wipe various storage devices.

Even though mobile devices are exposed to more security threats than desktops and laptops, they can still be managed by an organization. A reasonable degree of security can be attained for any organization. Productivity can be increased and employee satisfaction can improve as well when they are allowed to bring their own device.

References

Souppaya, M. & Scarfone, K. (2013). *Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)*. [Special Publication] Gaithersburg, MD: Author.

Comscore Inc. (2015). *U.S. Digital Future in Focus 2015*. Retrieved July 13, 2015.

Zumerle, D. & Hill, N. (2015). *How Digital Business Reshapes Mobile Security*. Retrieved July 13, 2015. *

He, W. (2013). *A survey of security risks of mobile social media through blog mining and an extensive literature search.* Information Management & Computer Security, Vol. 21 No. 5, 2013 pp. 381-400. *

Harris, M. & Patten K. (2013). *Mobile device security considerations for small- and medium-sized enterprise business mobility*. Information Management & Computer Security, Vol. 22 Iss 1 pp. 97 – 114. *

Asokan, N., Davi, L., Dmitrienko, A., Heuser, S., Kostiainen, K., Reshetova, E., Sadeghi, A. (2013). *Mobile Platform Security: Synthesis Lectures on Information Security, Privacy, and Trust.* Morgan and Claypool Publishers. *

Lookout, Inc. (2015). *Mobile Security: The 5 Questions Modern Organizations Are Asking*. Retrieved July 12, 2015.

Gruber, E. (2013). *Android Root Detection Techniques*. Retrieved from NetSPI Inc. website: https://blog.netspi.com/android-root-detection-techniques/

Zmysłowski, M. (2014). *Jailbreak Detection Methods*. Retrieved from Trustwave Holdings Inc. website: https://www.trustwave.com/Resources/SpiderLabs-Blog/Jailbreak-Detection-Methods/

Waliullah, M. & Gan, D. (2014). *Wireless LAN Security Threats & Vulnerabilities: A Literature Review*. International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014. *