7.12.3 Mobile Device Security Facts

Mobile devices can use various methods to connect to the internet, network and other devices.

- Cellular
- WiFi
- Bluetooth
- NFC
- ANT
- Infrared
- USB
- SATCOM (satellite)

Mobile device security considerations include:

- The management of content on the device
- The ability to wipe the device remotely
- Locking the device to a particular geographical area (geofencing)
- The ability to mange location information (geolocation)
- The ability to lock the screen with passwords
- The management of push notification services that can send messages and information to the device when the screen is locked and when the application is not active
- Storing and managing passwords to networks, web sites, etc.
- Biometrics
- Full device encryption

Security considerations regarding the management of applications on the mobile devices:

- Rooting/jailbreaking/sideloading to load apps from third-party app stores or other web sites
- Flashing with custom firmware
- Carrier unlocking or the ability to use different mobile carrier networks
- The ability to receive over-the-air (OTA) firmware updates and app updates
- Camera usage and adding a geolocation to a picture
- Text and multimedia message protocols (SMS/MMS)
- The ability to connect to external media
- The ability to connect using USB OTG (on-the-go)
- The use of a microphone for recording purposes
- The ability to share internet connectivity to other devices (tethering)

When working with mobile device apps, be aware of the following security issues:

Security Feature	Implementation

App Control	Application control is implemented in a similar manner for most mobile device operating systems:
	▪ For iOS devices, all apps come from Apple's App Store, which uses the following mechanisms to secure apps:
	  ▪ Running apps are sandboxed, which means they cannot access data stored by other running apps, nor can they access system files and resources.
	  ▪ All iOS apps must be digitally signed by either Apple or by a third party developer using an Apple-issued certificate. This ensures that apps from the App Store haven't been tampered with.
	  ▪ App developers can use encryption APIs to protect their app's data. Data can be symmetrically encrypted using AES, RC4, or 3DES.
	▪ For Windows RT devices, all apps come from Microsoft's Windows Store, which uses the following mechanisms to secure apps:
	  ▪ Windows RT refuses to load modules not digitally signed by Microsoft. This ensures that apps from the Windows Store haven't been tampered with.
	  ▪ All apps available through the Windows Store use the Windows RT API, which contains significant security enhancements, including:
	  ▪ Windows anti-buffer-overflow memory restrictions
	  ▪ Data Execution Prevention (DEP)
	  ▪ Address Space Layout Randomization (ASLR)
	  ▪ SafeSEH, sacrificial canary values
	
	Be aware, however, that iOS devices can be *jailbroken*, allowing apps to be installed from sources other than the App Store. Likewise, apps that aren't from theWindows Store can be installed on Windows RT devices using a process called *sideloading*. Either of these actions can seriously compromise the security of the device and should be avoided.
	
	Apps for the Android operating system are not as tightly controlled as those for iOS and Windows RT. Some Android app stores implement good security and tightly control apps much like the App Store and the Windows Store, but others do not. It is

	strongly recommended that you only use apps that come from a reputable source, such as the following: ▪ Google Play Store ▪ Amazon Appstore for Android ▪ Samsung Apps
Authentication and Credential Management	The average end user must remember a number of different passwords for different network resources and services, including Web-based services. To make life easier, the credential management functionality implemented in most mobile operating systems can store user names and passwords for the end user. A good example is Credential Manager in Windows RT. The iOS operating system performs a similar function using an encrypted keychain for storing digital identities, user names, and passwords. When the user accesses a password-protected network resource or website, the credential management software supplies the necessary username and password, effectively allowing the user to automatically log in. While using credential management software is convenient for the end user, it can also represent a security risk. For example, suppose a user has stored credentials to a sensitive network resource or website on a mobile device and then loses that device. If the user failed to secure the device with a password or PIN, a malicious individual could exploit the stored credentials to gain unauthorized access. As a consequence, it is recommended that you train users not to store credentials to sensitive network resources on their mobile devices.
App Whitelisting	App whitelisting is the process of defining specific apps that users are allowed to have on their mobile devices. For example, Windows RT provides a feature called *assigned access*, which allows you to define a whitelist of Windows Store applications. Assigned Access ensures that the device has only the apps required for its intended purpose installed, such as a point of sale system or an educational device. Apps that aren't on the whitelist are not allowed. For iOS and Android devices, app whitelists can be defined and enforced using a mobile device management (MDM) solution.
Geo-Tagging	Geo-tagging embeds GPS coordinates within mobile device files, such as image or video files created with the device's camera. While this feature can be useful in some circumstances, it can also create security concerns. For example, if a user regularly posts geotagged images to a social media site, cyber criminals could analyze the images and quickly discover where the user works--even where his cubicle is located. The attacker could possibly derive the user's work hours and many personal habits, such as restaurants the user visits for lunch. All of this information could be compiled and used for social engineering attacks on the organization. As a consequence, it is recommended that this functionality be disabled in the mobile devices you manage.