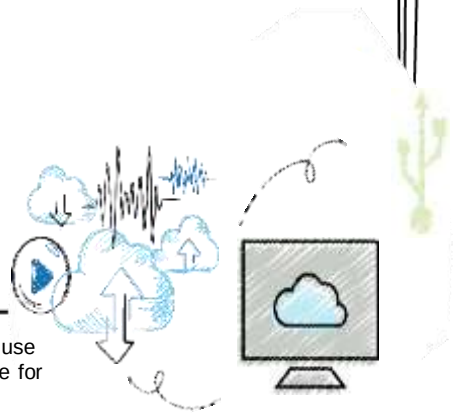
CompTIA Security+ Guide to Network Security Fundamentals, Sixth Edition

Chapter 10

Mobile and Embedded Device Security



Objectives

10.1 List and compare the different types of mobile devices

10.2 Explain the risks associated with mobile devices

10.3 List ways to secure a mobile device

10.4 Describe different types of embedded systems and IoT devices and how to secure them

Types of Mobile Devices

Core features	Additional features
Small form factor	Global Positioning System (GPS)
Mobile operating system	Microphone and/or digital camera
Wireless data network interface for accessing the Internet, such as Wi-Fi or cellular telephony	Wireless cellular connection for voice communications
Applications (apps) that can be acquired through different means	Wireless personal area network interfaces like Bluetooth or near field communication (NFC)
Local non removable data storage	Removable storage media
Data synchronization capabilities with a separate computer or remote servers	Support for using the device itself as removable storage for another computing device

Tablets (1 of 2)

- Tablets
  - Portable computing devices generally larger than smartphones and smaller than notebooks
  - Often classified by their screen size
  - Generally lack a built-in keyboard
  - Rely on a touch screen
  - Primarily a display device with limited user input
  - Most popular OSs for tablets are Apple iOS, Google Android, and Microsoft Windows

Tablets (2 of 2)

Figure 10-1 Tablet computer

Maximino/Shutterstock.com

Smartphones

- Smartphone
  - Has all the tools that a feature phone has but also includes an OS that allows it to run apps and access the Internet
- A **feature phone** is a traditional cellular phone with limited features, such as camera, MP3 music player, and the ability to send and receive **short message service (SMS)** text messages
- Considered handheld personal computers
  - Because of their ability to run apps

Wearable Technology (1 of 2)

- Wearable technology
  - Devices that can be worn by the user instead of carried
- Examples of wearable technology:
  - Fitness trackers
  - Smart watch
    - Can serve as an accessory to a smartphone to view messages

Wearable Technology (2 of 2)

Figure 10-2 Fitness tracker

Stephen VanHorn/Shutterstock.com

Portable Computers (1 of 4)

- Portable computers
  - Have similar hardware and run the same OS and application software found on a desktop computer
- Primary difference
  - Portable computers are smaller self-contained devices that can easily be transported from one location to another while operating on battery power
- Laptop
  - Regarded as the earliest portable computer
  - Have multiple hardware ports and may accommodate limited hardware upgrades

Portable Computers (2 of 4)

- Notebook computers
  - A smaller version of a laptop computer
  - Typically weigh less than laptops and are small enough to fit inside a briefcase
  - Designed to include only basic, frequently used features
- Subnotebook computer
  - Even smaller than standard notebooks
  - Use low-powered processors and solid state drives (SSDs)
  - Have both touch screen and a physical keyboard

Portable Computers (3 of 4)

Figure 10-3 2-in-1 computer with slate design

Chesky/Shutterstock.com

Portable Computers (4 of 4)

- Web-based computer
  - Contains a limited version of the Linux OS and a web browser
  - Has an integrated media player
  - Designed to be used while connected to the Internet
  - No traditional applications can be installed
  - No user files are stored locally
  - Accesses web apps and saves user files on the Internet

Mobile Device Connectivity Methods

- Many mobile devices use Wi-Fi as the standard connectivity method
- Many devices support other types of connectivity methods:
  - Cellular
  - Satellite
  - Infrared
  - ANT – a proprietary wireless network technology used primarily by sensors for communicating data
  - USB connections

Enterprise Deployment Models (1 of 2)

Model name	Description	Employee actions	Business actions
Bring your own device (BYOD)	Allows users to use their own personal mobile devices for business purposes	Employees have full responsibility for choosing and supporting the device	This model is popular with smaller companies or those with temporary staff
Corporate owned, personally enabled (COPE)	Employees choose from a selection of company approved devices	Employees are supplied the device chosen and paid for by the company	Company decides level of choice and freedom for employees
Choose your own device (CYOD)	Employees choose from a limited selection of approved devices but the employee pays the upfront cost of the device while business own contract	Employees are offered a suite of choices that the company has approved for security, reliability, and durability	Company often provides a stipend to pay monthly fees to wireless carrier
Virtual desktop infrastructure (VDI)	Stores sensitive applications and data on a remote server that is accessed through a smartphone	Users can customize the display of data as if the data were residing on their own device	Enterprise can centrally protect and manage apps and data on server instead of distributing to smartphones
Corporate-owned	Device is purchased and owned by the enterprise	Employees use the phone only for company-related business	Enterprise is responsible for all aspects of the device

Enterprise Deployment Models (2 of 2)

- Benefits of the BYOD, COPE, and CYOD models:
  - Management flexibility
  - Less oversight
  - Cost savings
  - Increased employee performance
  - Simplified IT infrastructure
- User benefits:
  - Choice of device
  - Choice of carrier
  - Convenience

Mobile Device Risks

- Security risks of mobile devices:
  - Mobile device vulnerabilities
  - Connection vulnerabilities
  - Accessing untrusted content
  - Deployment model risks

Physical Security

- About 68 percent of all healthcare security breaches were the result of the loss or theft of a mobile device
- One-quarter of all laptop thefts occurred from unattended cars
  - Or while traveling on airplanes and trains
  - 15 percent occurred in airports and hotels
  - 12 percent stolen from restaurants
- Users must guard against shoulder surfing
  - Strangers who want to view sensitive information

Limited Firmware Updates

- Apple iOS is a closed and proprietary architecture
  - Users update through iTunes or through the over-the-air (OTA) update (called firmware OTA updates)
- Google does not create the hardware that Android runs on
  - It is very difficult to distribute security updates to the devices through the wireless carriers
  - Many OEMs had modified Android and were reluctant to distribute updates that might conflict with their changes
  - Wireless carriers needed to perform extensive testing
  - OEMs and wireless carriers are hesitant to distribute Google updates
  - No financial incentive to update mobile devices

Location Tracking

- Mobile devices with global positioning system (GPS) capabilities support **geolocation**
  - The process of identifying the geographical location of the device
- Mobile devices using location services are at an increased risk of targeted physical attacks
  - Attackers can determine where users are and plan to steal the mobile device or inflict harm
- GPS tagging
  - Adding geographical identification data to media
  - Also called geo-tagging

Unauthorized Recording

- Basic precautions against unauthorized recording:
  - Do not use a webcam in any room where private activities take place
  - Place a piece of electrical tape over the lens of a webcam when not in use
  - Only allow permission to access the camera or microphone for apps that require that use
  - Periodically review app permissions on the device and turn off those permissions that are not necessary

Connection Vulnerabilities

Name	Description	Vulnerability
Tethering	A mobile device with an active Internet connection can be used to share that connection with other mobile devices through Bluetooth or Wi-Fi	An unsecured mobile device may infect other tethered mobile devices or the corporate network
USB On-the-Go (OTG)	A mobile device with a USB connection can act as either a host or a peripheral used for external media access	Connecting a mobile device as a peripheral to an infected computer could allow malware to be sent to the device
Connecting to public networks	Mobile devices must at time use public external networks for Internet access	Because these networks are beyond the control of the organization, attackers can eavesdrop on the data transmissions and view sensitive information

Accessing Untrusted Content (1 of 3)

- Quick Response (QR) codes
  - A matrix or two-dimensional barcode which can be read by an imaging device
  - Applications for these codes include:
    - Product tracking, item identification, time tracking, document management, and general marketing
  - An attacker can create an advertisement listing a reputable website but include a QR code that contains a malicious URL
    - Code directs a user's browser to the attacker's imposter website or to a site that downloads malware
- Users can circumvent built-in limitations on smartphones to download from an unofficial third-party app store (called **sideloading**)
  - Called **jailbreaking** on Apple iOS devices and **rooting** on Android devices

Accessing Untrusted Content (2 of 3)

Figure 10-5 QR code

Accessing Untrusted Content (3 of 3)

- **Short message service (SMS)**
  - Text messages of a maximum of 160 characters
- **Multimedia messaging service (MMS)**
  - Provides for pictures, video, or audio to be included in text messages
- Threat actors can send SMS messages that contain links to untrusted content
  - Or send a specially crafted MMS video that can introduce malware into the device

Deployment Model Risks

- Risks associated with enterprise deployment models:
  - Users may erase the installed built-in limitations on their mobile device, which disables the built-in security features
  - Personal mobile devices are often shared among family members and friends, subjecting sensitive corporate data installed on a user's device to outsiders
  - Different mobile devices have different hardware and OSs that technical support staff might have to support
  - It might be difficult securing the personal smartphone from an employee who left the company

Securing Mobile Devices

- Steps to securing mobile devices:
  - Configuring the device
  - Using mobile management tools
  - Configuring device app security

Device Configuration (1 of 3)

- Disable Unused Features
  - It is important to disable unused features and turn off those that do not support the business use of the phone
  - Should disable Bluetooth wireless data communication
    - In order to prevent bluejacking and bluesnarfing
- Use Strong Authentication
  - Restrict unauthorized users with a screen lock and require a strong passcode
- Screen Lock
  - Lock screen prevents device from being used until the user enters the correct passcode
    - Set screen to lock after a period of inactivity

Device Configuration (2 of 3)

- Screen Lock (continued)
  - After a specific number of failed attempts to enter a passcode, additional security protections will occur:
    - Extend lockout period
    - Reset to factory settings
  - Context-aware authentication
    - The device automatically unlocks and stays unlocked until a specific action occurs
- Passcode
  - Use a personal identification number (PIN)
  - Use a fingerprint “swipe” on a sensor to unlock the device
  - Draw or swipe a specific pattern connecting dots to unlock the device

Device Configuration (3 of 3)

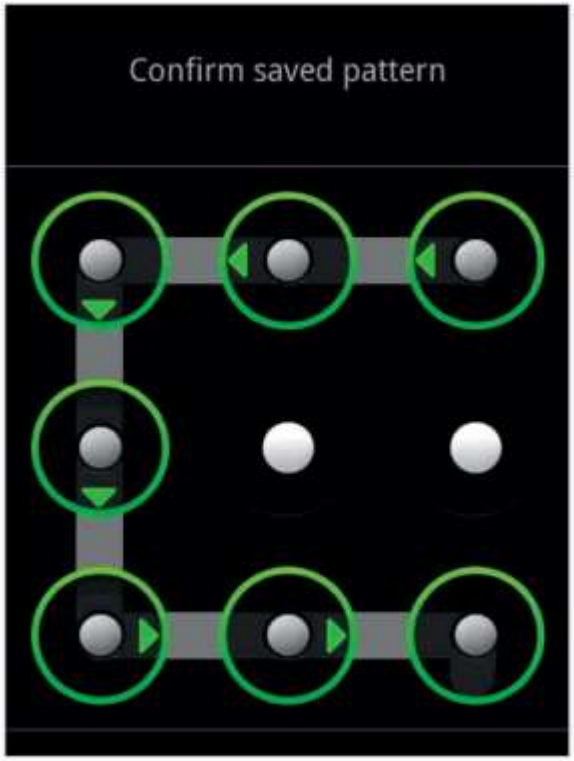


Figure 10-6 Swipe pattern

Source: OnlineAndroidTips.com

Manage Encryption

- Significant loopholes in which mobile device data can be accessed through data-in-transit and remote data-at-rest
- **Data-in-transit**
  - Carriers build surveillance capabilities into their networks
  - Allows law enforcement agencies to collect data-in-transit
  - New mobile apps deliver over-the-top (OTT) content
    - Delivery of content over the Internet without telecoms being directly involved
- **Remote Data-at-Rest**
  - Apple and Google possess decryption keys necessary to unlock data on their servers
  - Courts routinely server order to Apple and Google to provide data stored on their servers
  - Users can choose to turn off backups to iCloud or Google servers

Segment Storage

- Storage segmentation
  - Separating business data from personal data
- Containerization
  - Separating storage into separate business and personal “containers” and managing each appropriately
- Advantages to storage segmentation:
  - Helps companies avoid data ownership privacy issues and legal concerns regarding a user’s personal data
  - Allows companies to delete only business data when necessary without touching personal data

Enable Loss or Theft Services (1 of 2)

- To reduce the risk of theft or loss:
  - Keep the mobile device out of sight when traveling in a high-risk area
  - Always maintain awareness of your surroundings
  - When holding the device, use both hands to make it difficult for a thief to snatch
  - Do not use the device on escalators or near train doors
  - White or red headphone cords may indicate they are connected to an expensive device, so consider replacing cord
  - If theft does occur, do not resist or chase the thief
- If a device is lost or stolen, several security features can be enabled to locate the device or limit the damage (see Table on the next slide)
- If a device is lost or stolen and cannot be located, it may be necessary to perform a **remote wiping**, which erases sensitive data stored on the device

Enable Loss or Theft Services (2 of 2)

Security feature	Explanation
Alarm	The device can generate an alarm even if it is on mute
Last known location	If the battery is charged to less than a specific percentage, the device's last known location can be indicated on an online map
Locate	The current location of the device can be pinpointed on a map through the device's GPS
Remote lookout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen
Thief picture	A thief who enters an incorrect passcode three times will have her picture taken through the device's on-board camera and emailed to the owner

Mobile Management Tools

- Support tools:
  - Mobile device management
  - Mobile application management
  - Mobile content management

Mobile Device Management (MDM) (1 of 2)

- Mobile Device Management (MDM)
  - Tools that allow a device to be managed remotely by an organization
- Usually involve:
  - A server component that sends out management commands to mobile devices
  - A client component to receive and implement the management commands
- An administrator can perform over the air (OTA) updates or configuration changes to one device

Mobile Device Management (MDM) (2 of 2)

- Some features that MDM tools provide:
  - Rapidly enroll new mobile devices (on-boarding) and quickly remove devices (off-boarding)
  - Apply or modify default device settings
  - Enforce encryption settings, antivirus updates, and patch management
  - Display an acceptable use policy that requires consent before allowing access
  - Configure email, calendar, contacts, Wi-Fi, and VPN profiles OTA
  - Discover devices accessing enterprise systems
  - Approve or quarantine new mobile devices
  - Distribute and manage public and corporate apps
  - Securely share and update documents and corporate policies
  - Detect and restrict jailbroken and rooted devices
  - Selectively erase corporate data
  - Send SMS text messages to selected users or groups of users

Mobile Application Management (MAM)

- Mobile Application Management (MAM)
  - Tools and services responsible for distributing and controlling access to apps
- Initially controlled apps through **app wrapping**
  - Sets up a “dynamic” library of software routines and adds to an existing program to restrict parts of an app
- Using a MAM originally required the use of an MDM as well
- Newer versions of mobile OSs have MAM incorporated into the software itself

Mobile Content Management (MCM)

- Content management
  - Used to support the creation and editing/modification of digital content by multiple employees
- A **mobile content management (MCM)** system
  - Is tuned to provide content management to hundreds or even thousands of mobile devices used by employees in an enterprise

Mobile Device App Security

- Apps on the device should be secured also
- Apps can require that the user provide authentication (such as a passcode) before access is granted
- MDMs can support:
  - **Application whitelisting** - ensures that only preapproved apps can run on the device
  - **Geo-fencing** - uses the device's GPS to define geographical boundaries where the app can be used

Embedded Systems and the Internet of Things

- A growing trend is to add capabilities to devices that have never had computing power before
- These devices include:
  - Embedded systems and the Internet of Things

Embedded Systems (1 of 4)

- Embedded system
  - A computer hardware and software contained within a larger system designed for a specific function
- Examples of embedded systems:
  - Medical devices
  - Aircraft
  - Vehicles
  - Industrial machines
  - Heating, ventilation, and air conditioning (HVAC) environmental systems

Embedded Systems (2 of 4)

- Industrial control systems (ICS) - control locally or at remote locations by collecting, monitoring, and processing real-time data so that machines can directly control devices such as:
  - Valves
  - Pumps
  - Motors
- Multiple ICS are managed by a larger supervisory control and data acquisition (SCADA) system

Embedded Systems (3 of 4)

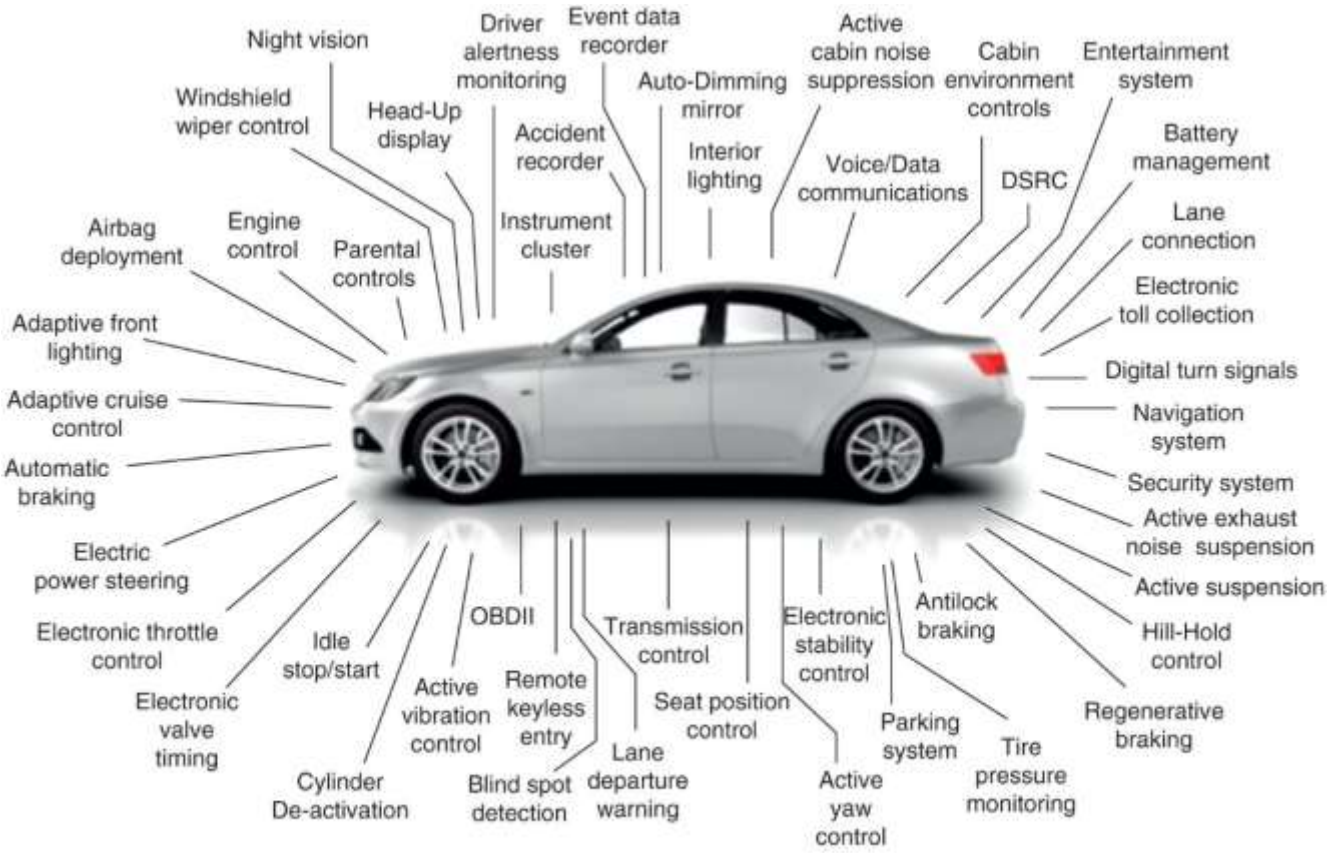


Figure 10-7 Embedded systems in cars

Embedded Systems (4 of 4)

- System on a chip (SoC)
  - All the necessary hardware components contained on a single microprocessor chip
- Real-time operating system (RTOS)
  - Software designed for an SoC in an embedded system
- Embedded system receive very large amounts of data quickly
- RTOS is tuned to accommodate very high volumes of data that must be immediately processed for critical decision making

Internet of Things (1 of 3)

- Internet of Things (IoT)
  - Connecting any device to the Internet for the purpose of sending and receiving data to be acted upon
- Includes:
  - Wearable technology and multifunctional devices
- Also includes everyday home automation items such as:
  - Thermostats, coffee makers, tire sensors, slow cookers, keyless entry systems, washing machines, electric toothbrushes, headphones, and light bulbs
- Body area networks (BAN)
  - A network system of IoT devices in close proximity to a person's body that cooperate for the benefit of the user

Internet of Things (2 of 3)

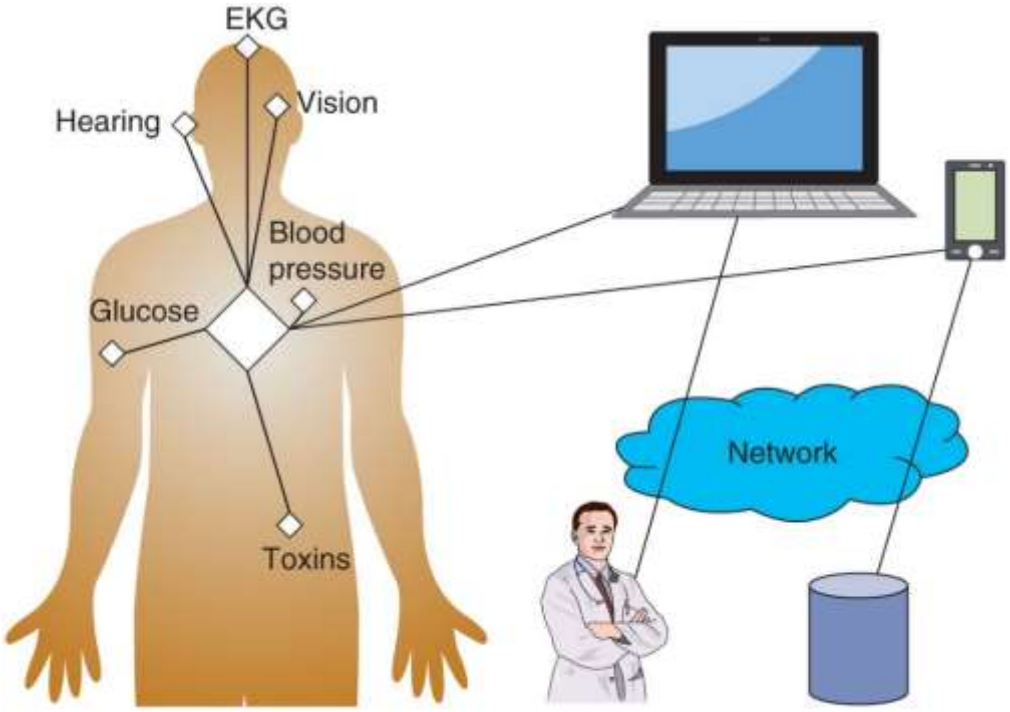


Figure 10-8 Managed body sensor network (MBSN)

Internet of Things (3 of 3)

- Autonomous body sensor network (ABSN)
  - Introduces actuators in addition to the sensors so immediate effects can be made on the human body
- ABSN can expand the use of functional electric stimulation to restore sensation, mobility, and function to those persons with paralyzed limbs and organs

Security Implications

- Reasons why IoT and embedded system devices are vulnerable:
  - Most IoT vendors are concerned with making products as inexpensive as possible, leaving out security protections
  - Devices that do have security capabilities implemented have notoriously weak security
  - Few, if any, IoT devices have been designed with the capacity for being updated to address exposed security vulnerabilities
  - IoT and embedded systems that can receive patches often see long gaps between the discovery of the vulnerability and a patch being applied
- There are several initiatives underway to address security vulnerabilities in IoT and embedded devices

Chapter Summary (1 of 3)

- Tablet computers are portable computing devices smaller than portable computers, larger than smartphones, and focused on ease of use
- Portable computers are devices that closely resemble standard desktop computer
  - A laptop is designed to replicate the abilities of a desktop computer with only slightly less processing power
- Many mobile devices use Wi-Fi as the standard connectivity method to connect to remote networks
- Many organizations have adopted an enterprise deployment model as it relates to mobile devices
- BYOD allows users to use their own personal mobile devices for business purposes

Chapter Summary (2 of 3)

- Mobile devices can be easily lost or stolen and usually use public external networks for their Internet access
  - Attackers can eavesdrop on data transmissions and view services to identify the location of a person carrying a mobile device
- Mobile devices have the ability to access untrusted content that other types of computing devices generally do not have
- It is important to disable features and turn off those that do not support the business use of the device or that are rarely used
- A lock screen prevents the mobile device from being used until the user enters the correct passcode

Chapter Summary (3 of 3)

- Mobile device management (MDM) tools allow a device to be managed remotely
- Mobile application management (MAM) consists of tools and services responsible for distributing and controlling access to apps
- MDMs can support application whitelisting, which ensures that only preapproved apps can be run on the device
- An embedded system is computer hardware and software contained within a larger system that is designed for a specific function
- The Internet of Things (IoT) is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon