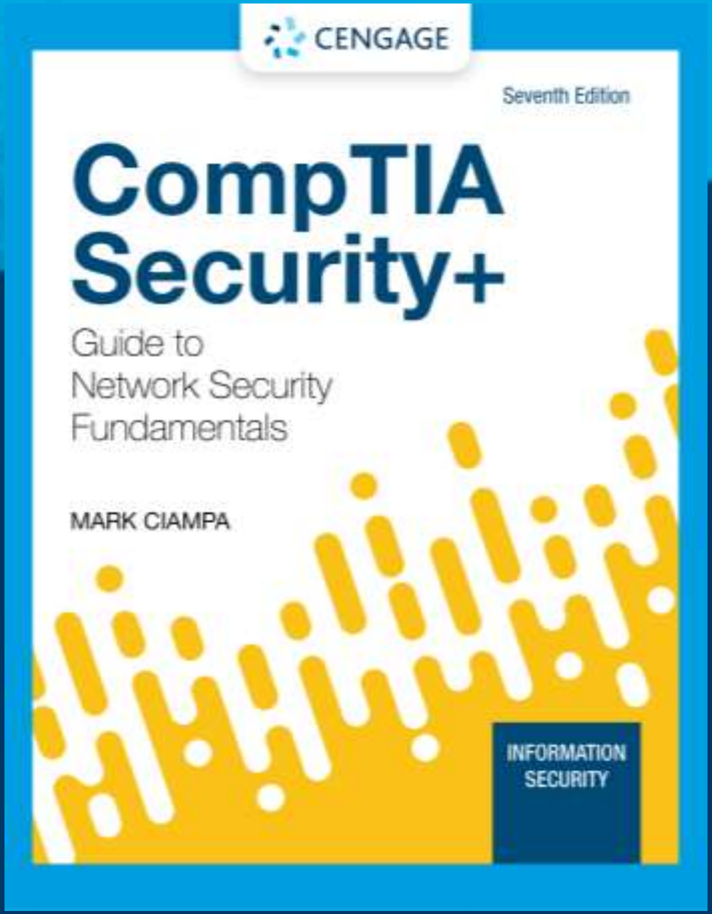


CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 5: Mobile, Embedded, and Specialized Device Security

Module Objectives

By the end of this module, you should be able to:

1. List and compare the different types of mobile devices and how they are deployed

2. Explain the ways to secure a mobile device

3. Describe the vulnerabilities and protections of embedded and specialized devices

4. Explain the issues surrounding securing specialized devices

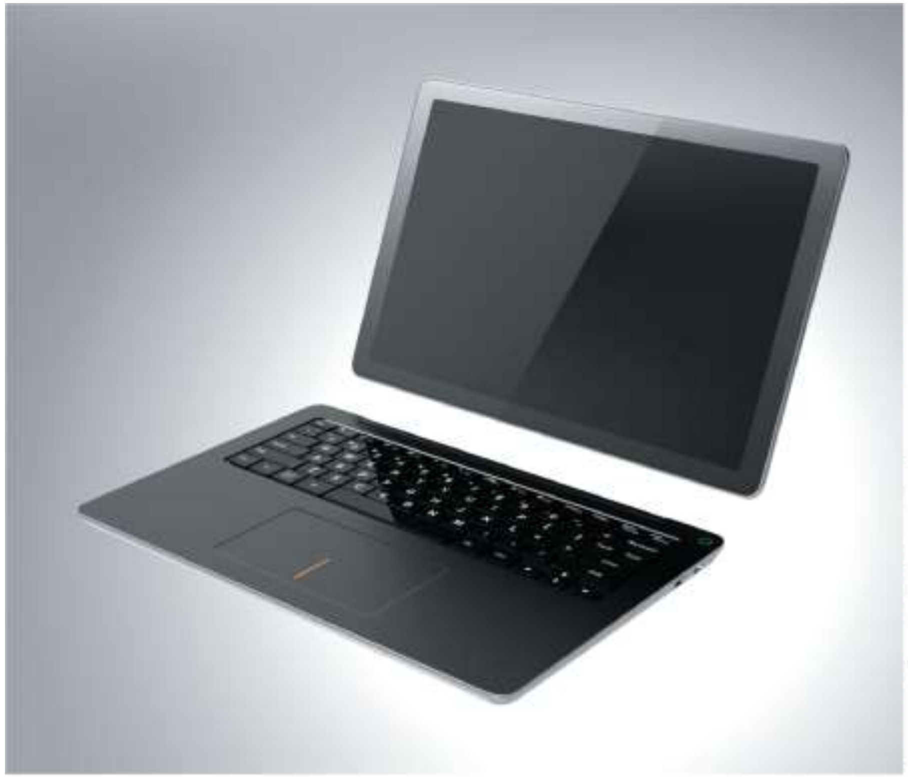
Securing Mobile Devices

- Each type of mobile device faces cybersecurity risks
- Security professionals can use a variety of techniques and technologies for securing mobile devices

Introduction to Mobile Devices (1 of 7)

- Types of Mobile Devices
  - *Tablets* are portable computing devices that generally lack a built-in keyboard or mouse
  - *Smartphones* have all of the tools of a feature phone plus an OS that allows it to run apps and access the Internet
  - *Wearables* are devices that can be worn by the user instead of carried
    - The most common of these devices is the smart watch
  - *Portable computers* are devices that closely resemble standard desktop computers
    - They are smaller, self-contained devices that can easily be transported from one location to another while running on battery power
    - A *web-based computer* contains a limited version of an OS and a web browser with an integrated media player

Introduction to Mobile Devices (2 of 7)



Source: Chesky/Shutterstock.com

Figure 5-3 2-in-1 computer with slate design

Figure 5-3 2-in-1 computer with slate design

Introduction to Mobile Devices (3 of 7)

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
Stores or other means of acquiring applications (apps)	Wireless personal area network interfaces such as Bluetooth or near field communications (NFC)
Local nonremovable 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

Introduction to Mobile Devices (4 of 7)

- Mobile Device Connectivity Methods
  - *Cellular* – coverage area for a cellular telephony network is divided into cells
    - Transmitters are connected through a mobile telecommunications switching office (MTSO) that controls all of the transmitters in the cellular network
  - *Wi-Fi* – a wireless local area network (WLAN) designed to replace or supplement a wired local area network (LAN)
  - *Infrared* – uses light instead of radio frequency (RF) as the communication media
    - Due to slow speed and other limitations, infrared capabilities are rarely found today
  - *USB connections* – these include standard-size connectors, mini connectors, and micro connectors

Introduction to Mobile Devices (5 of 7)

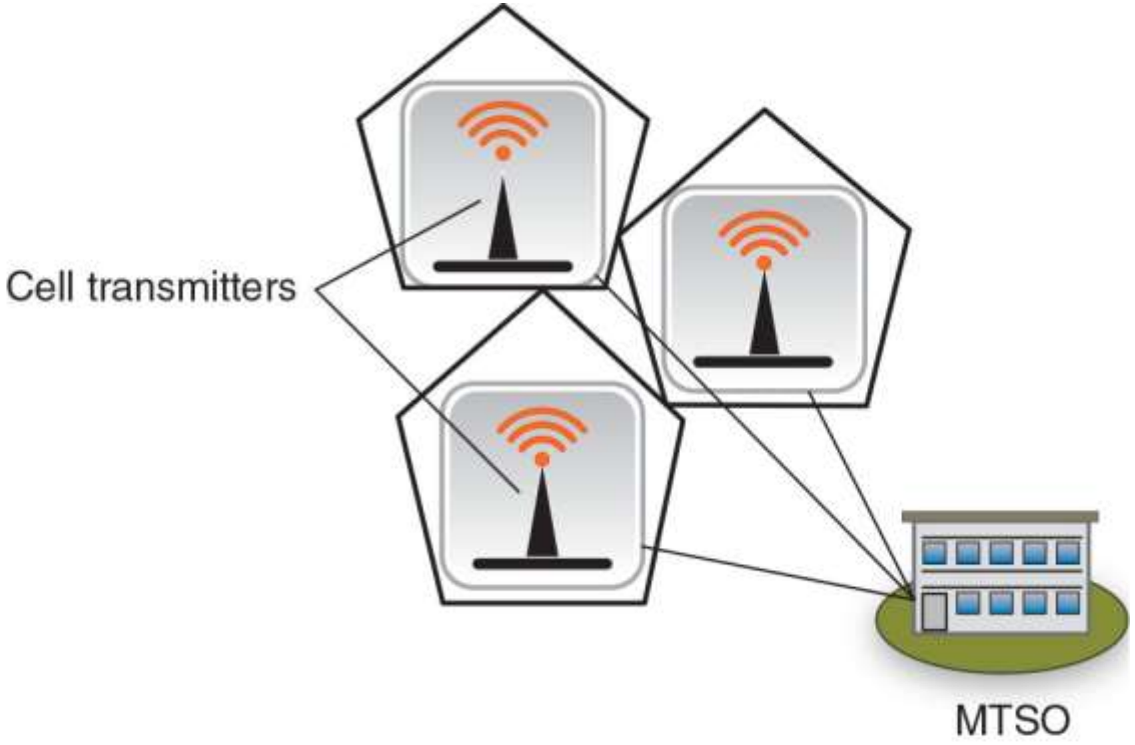


Figure 5-4 Cellular telephony network

Figure 5-4 Cellular telephony network

Introduction to Mobile Devices (6 of 7)

Model Name	Description	Employee actions	Business actions
Bring your own device (BYOD)	Employees 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 a 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, but they can also use it for personal activities.	Company decides the level of choice and freedom for employees.
Choose your own device (CYOD)	Employees choose from a limited selection of approved devices but pay the upfront cost of the device while the business owns the 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 accessed through a smartphone	Users can customize the display of data as if the data were residing on their own mobile device.	Enterprise can centrally protect and manage apps and data on server instead of distributing to smartphones.
Corporate owned	The 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.

CENGAGE

Introduction to Mobile Devices (7 of 7)

- Enterprise Deployment Models
  - Benefits of BYOD, COPE, and CYOD models include:
    - *Management flexibility*
    - *Cost savings*
    - *Increased employee performance*
    - *Simplified IT infrastructure*
    - *Reduced internal service*
  - User benefits include:
    - *Choice of device*
    - *Choice of carrier*
    - *Convenience*

Mobile Device Risks (1 of 3)

- Security risks associated with using mobile devices include mobile device vulnerabilities, connection vulnerabilities, and accessing untrusted content
- Mobile Device Vulnerabilities
  - **Physical security** – mobile devices are frequently lost or stolen
  - **Limited updates** – security patches and updates for mobile OSs are distributed through **firmware over-the-air (OTA) updates**
  - **Location tracking** – mobile devices with GPS capabilities typically support geolocation
    - Mobile devices using geolocation are at increased risk of targeted physical attacks
    - A related risk is GSP tagging which is adding geographical identification data to media
  - **Unauthorized recording** – by infecting a device with malware, a threat actor can spy on an unsuspecting victim and record conversations or videos

CENGAGE

Mobile Device Risks (2 of 3)

- Connection Vulnerabilities
  - See Table 5-4 on the following slide
- Accessing Untrusted Content
  - Users can circumvent the built-in installation limitation on their smartphone (called **jailbreaking** on Apple iOS or **rooting** on Android devices) to download from an unofficial third-party app store (called **sideloading**)
  - Untrusted content can invade mobile devices through SMS, MMS, and RCS text messaging
  - Mobile devices can access untrusted content using *QR* codes
  - An attacker can create an advertisement listing a reputable website but include a QR code that contains a malicious URL

Mobile Device Risks (3 of 3)

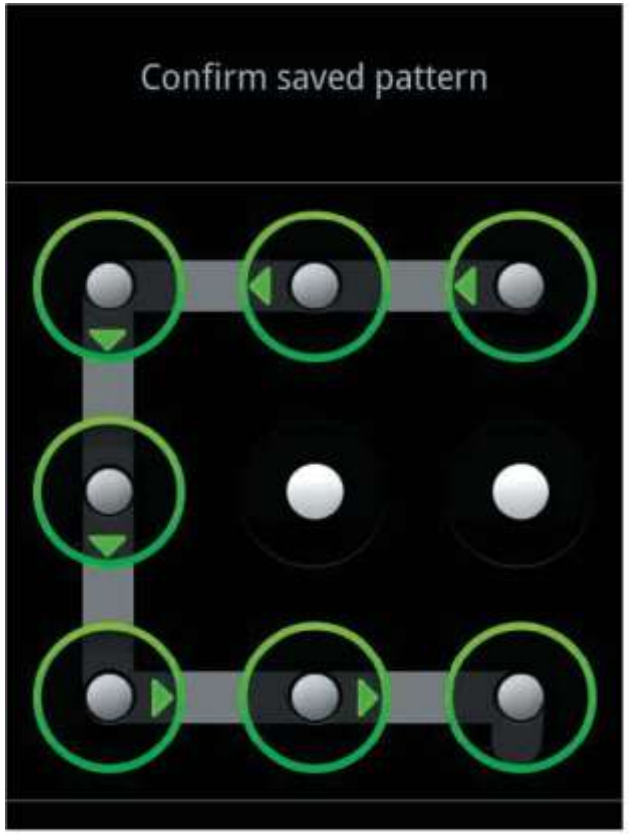
Name	Description	Vulnerability
Tethering	A mobile device with an active Internet connection can be used to share that connection with other mobile devices through Bluetooth or Wi-Fi.	An unsecured mobile device may infect other tethered mobile devices or the corporate network.
USB On-the-Go (OTG)	An OTG mobile device with a USB connection can function as either a host (to which other devices may be connected such as a USB flash drive) for **external media access** or as a peripheral (such as a mass storage device) to another host.	Connecting a **malicious flash drive** infected with malware to a mobile device could result in an infection, just as using a device as a peripheral while connected to an infected computer could allow malware to be sent to the device.
Malicious USB cable	A USB cable could be embedded with a Wi-Fi controller that can receive commands from a nearby device to send malicious commands to the connected mobile device.	The device will recognize the cable as a Human Interface Device (similar to a mouse or keyboard), giving the attacker enough permissions to exploit the system.
Hotspots	A hotspot is a location where users can access the Internet with a wireless signal.	Because public hotspots are beyond the control of the organization, attackers can eavesdrop on the data transmissions and view sensitive information.

CENGAGE

Protecting Mobile Devices (1 of 6)

- Device Configuration
  - Several configurations should be considered when setting up a mobile device for use
  - Use Strong Authentication
    - Verifying that the authentic user of a device involves requiring a strong passcode and restricting unauthorized users with a screen lock
    - Options include using:
      - A passcode
      - A PIN
      - A fingerprint
      - A pattern connecting dots to unlock the device
    - A *screen lock* prevents the mobile device from being accessed until the user enters the correct passcode

Protecting Mobile Devices (2 of 6)



Confirm saved pattern

Source: OnlineAndroidTips.com

Figure 5-6 Swipe pattern

Figure 5-6 Swipe pattern

Protecting Mobile Devices (3 of 6)

- Device Configuration (continued)
  - Manage Encryption
    - Early versions of both mobile OSs encrypt all user data on their mobile devices (**full disk encryption**) by default when the device is locked
    - Mobile device data can still be accessed through remote data-at-rest
  - Segment Storage
    - **Storage segmentation** separates business data from personal data on mobile devices
    - Users can apply **containerization**, or separating storage into business and personal “containers”
    - It helps companies avoid data ownership privacy issues and legal concerns regarding a user’s personal data stored on the device

CENGAGE

Protecting Mobile Devices (4 of 6)

- Device Configuration (continued)
  - Enable Loss or Theft Services
    - If a lost or stolen device cannot be located, it may be necessary to perform a remote wipe, which will erase sensitive data stored on the mobile device
    - To reduce the risk of theft or loss, users should:
      - Keep the mobile device out of sight when traveling in a high-risk area
      - Avoid becoming distracted by what is on the device
      - When holding a device, use both hands to make it more difficult for a thief to snatch
      - Do not use the device on escalators or near transit train doors
      - Use a less conspicuous color for headphone cords
      - Do not resist or chase a thief if they steal your device

Protecting Mobile Devices (5 of 6)

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 lockout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen.
Thief picture	Thieves who enter an incorrect passcode three times will have their picture taken through the device’s on-board camera and emailed to the owner.

Protecting Mobile Devices (6 of 6)

- Mobile Management Tools
  - **Mobile Device Management** (**MDM**) tools allow a device to be managed remotely by an organization
  - **Mobile Application Management** (**MAM**) covers application management, which comprises the tools and services responsible for distributing and controlling access to apps
  - **Mobile Content Management** (**MCM**) supports the creation and subsequent editing and modification of digital content by multiple employees
  - **Unified Endpoint Management** (**UEM**) is a group or class of software tools with a single management interface for mobile devices as well as computer devices
    - It provides capabilities for managing and securing mobile devices, applications, and content

Knowledge Check Activity 1

Which enterprise deployment model of mobile devices stores sensitive applications and data on a remote server that you can access through a smartphone?

a. VDI

b. CYOD

c. BYOD

d. COPE

Knowledge Check Activity 1: Answer

Which enterprise deployment model of mobile devices stores sensitive applications and data on a remote server that you can access through a smartphone?

- **Answer: a. VDI**
- **A virtual desktop infrastructure (VDI) uses servers at the employer's site or at a cloud provider to deliver applications, data, and entire OSs, to a mobile device app or Web browser.**

Knowledge Check Activity 2

Which mobile management tool provides capabilities for managing and securing mobile devices, applications, and content?

a. MDM

b. MCM

c. UEM

d. MAM

Knowledge Check Activity 2: Answer

Which mobile management tool provides capabilities for managing and securing mobile devices, applications, and content?

Answer: c. UEM

Unified Endpoint Management (UEM) supports all of the capabilities of MDM, MAM, and MCM. It provides a single management interface for mobile devices.

Embedded Systems and Specialized Devices

- Computing capabilities can be integrated into appliances and other devices
- An embedded system is computer hardware and software contained within a larger system designed for a specific function
- These devices can pose security risks

Types of Devices (1 of 7)

- Categories of embedded and specialized devices include the hardware and software that can be used to create these devices, specialized systems, industrial systems, other devices, and IoT devices
- Hardware and Software
  - One of the most common hardware components is the **Raspberry Pi**, which is a low-cost, credit-card-sized computer motherboard
    - It can perform almost any task that a standard computer can and can be used to control a specialized device
  - A **field-programmable gate array (FPGA)** is a hardware “chip” that can be programmed by the user to carry out one or more logical operations
  - A **system on a chip (SoC)** combines all the required electronic circuits of the various computer components on a single chip
    - SoCs often use a **real-time operating system (RTOS)**

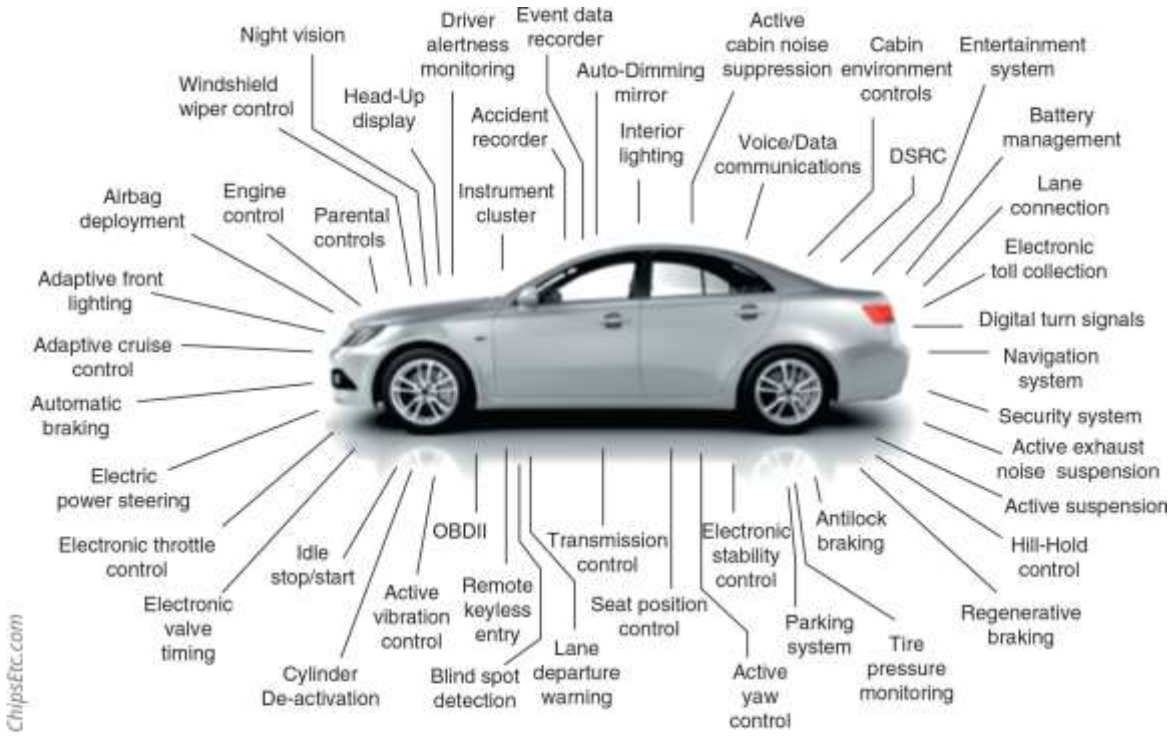
Types of Devices (2 of 7)

- Specialized Systems
  - Digital smart meters are used to measure the amount of utilities consumed
    - Smart meters have several advantages over analog meters (see Table 5-8 on the following slide)
  - Other specialized systems include medical systems, aircraft, and vehicles
    - Embedded systems in cars use sonar, radar, and laser emitters to control brakes, steering, and the throttle
- Industrial Systems
  - **Industrial control systems (ICSs)** in local or at remote locations collect, monitor, and process real-time data so that machines can directly control devices such as valves, pumps, and motors without human intervention
  - ICSs are managed by **supervisory control and data acquisition (SCADA)** systems

Types of Devices (3 of 7)

Action	Analog meter	Smart meter
Meter readings	Employee must visit the dwelling each month to read the meter.	Meter readings are transmitted daily, hourly, or even by the minute to the utility company.
Servicing	Annual servicing is required in order to maintain accuracy.	Battery replacement every 20 years.
Tamper protection	Data must be analyzed over long periods to identify anomalies.	Can alert utility in the event of tampering or theft.
Emergency communication	None available	Transmits “last gasp” notification of a problem to utility company.

Types of Devices (4 of 7)



ChipsEtc.com

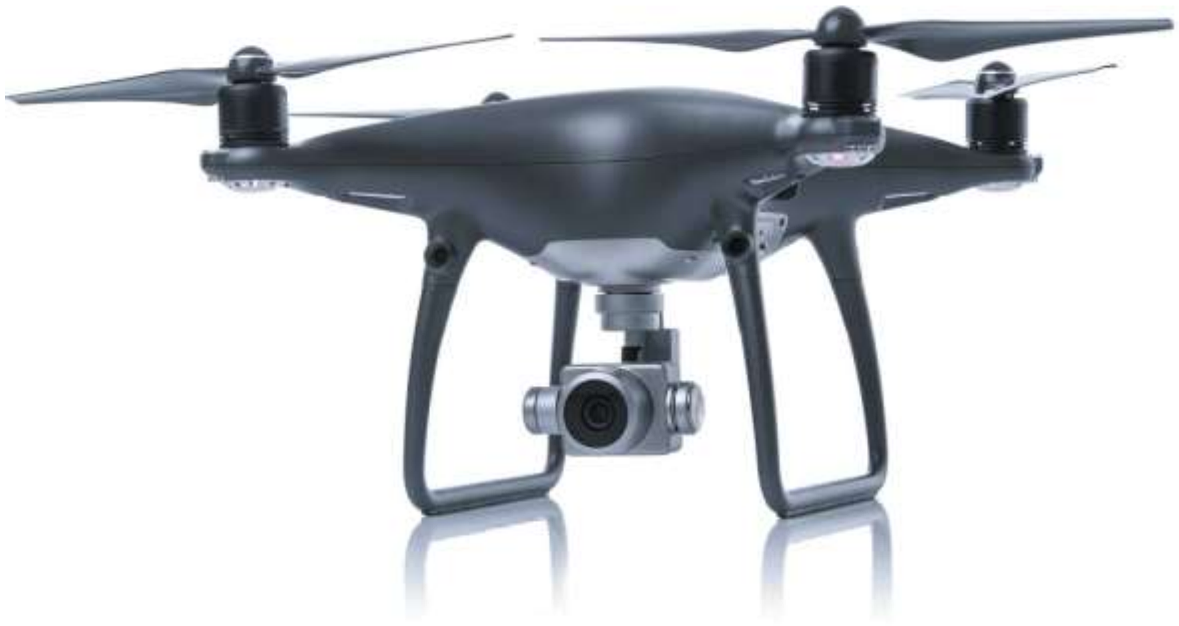
Figure 5-9 Embedded systems in cars

Figure 5-9 Embedded systems in cars

Types of Devices (5 of 7)

- Other Specialized Systems
  - Other examples of specialized systems include **heating, ventilation, and air conditioning (HVAC)** environmental systems
  - A **multifunctional printer (MFP)** combines the functions of a printer, copier, scanner, and fax machine
  - An **unmanned aerial vehicle (UAV)** commonly known as a drone, is an aircraft without a human pilot on board to control its flight
    - They are commonly used for policing and surveillance, product deliveries, aerial photography, infrastructure inspections, and drone racing

Types of Devices (6 of 7)



Source: Den Rozhnovsky/Shutterstock.com

Figure 5-10 Drone

Figure 5-10 Drone

Types of Devices (7 of 7)

- Internet of Things
  - **Internet of Things** (**IoT**) is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon
  - IoT devices include wearable technology as well as every 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*) is a network system of IoT devices in close proximity to a person’s body that cooperate for the benefit of the user
  - *Autonomous body sensor network* (*ABSN*) introduces actuators in addition to the sensors so that immediate effects can be made on the human body

Security Issues Table (1 of 2)

Constraint	Explanation
Power	To prolong battery life, devices and systems are optimized to draw very low levels of power and thus lack the ability to perform strong security measures.
Compute	Due to their size, small devices typically possess low processing capabilities, which restricts complex and comprehensive security measures.
Network	To simplify connecting a device to a network, many device designers support network protocols that lack advanced security features.
Cryptography	Encryption and decryption are resource-intensive tasks that require significant processing and storage capacities that these devices lack.
Inability to patch	Few, if any, devices have been designed with the capacity for being updated to address exposed security vulnerabilities.
Authentication	To keep costs at a minimum, most devices lack authentication features.
Range	Not all devices have long-range capabilities to access remote security updates.
Cost	Most developers are concerned primarily with making products as inexpensive as possible, which means leaving out all security protections.
Implied trust	Many devices are designed without any security features but operate on an “implied trust” basis that assumes all other devices or users can be trusted.
Weak defaults	User names (such as “root,” “admin,” and “support”) and passwords (“admin,” “888888,” “default,” “123456,” “54321,” and even “password”) for accessing devices are often simple and well known.

Security Issues (2 of 2)

- Over several years, many industry-led initiatives have attempted to address security vulnerabilities in IoT and embedded devices
  - The initiatives were scattered and did not represent a comprehensive solution to the problem
- Governments have begun to propose or enact legislation to require stronger security on embedded systems and specialized devices
- *The Internet of Things* (*IoT*) *Cybersecurity Improvement Act of 2019* was legislation introduced in the U.S. Senate in May 2019
- California and Oregon passed state laws addressing IoT security that went into effect in January 2020
  - Requires that connected devices be equipped with “reasonable security features” appropriate for the nature and function of the device and the information the device collects, contains, or transmits

Knowledge Check Activity 3

Which of the following is used to manage industrial control systems (ICSs)?

a. SoC

b. SCADA

c. Real-time OS

d. Embedded system

Knowledge Check Activity 3: Answer

Which of the following is used to manage industrial control systems (ICSs)?

Answer: b. SCADA

Supervisory control and data acquisition (SCADA) systems are used to manage ICSs and are crucial in maintaining efficiency and reducing downtime.

Self-Assessment

Rate your competence of the following module objectives on a scale of 1 to 5 where 5 indicates you have full confidence in your competence of that objective and 1 indicates you have very little to no confidence in your competence of that objective. If you self-score less than 4 you should consider reviewing the module and related exercises:

1. List and compare the different types of mobile devices and how they are deployed

2. Explain the ways to secure a mobile device

3. Describe the vulnerabilities and protections of embedded and specialized devices

4. Explain the issues surrounding securing specialized devices

Summary (1 of 2)

- There are several types of mobile devices: tablet computers, smartphones, and wearable technology devices are a few
- Portable computers are devices that closely resemble standard desktop computers
- Connectivity methods used to connect mobile devices to networks include cellular telephony, which divides the coverage area into cells
- It is not always feasible to require an employee to carry a company-owned smartphone along with a personal cell phone
  - Bring your own device (BYOD) allows users to use their own personal mobile devices for business purposes
  - Choose your own device (CYOD) gives employees a limited selection of approved devices, though the employee pays the upfront cost of the device while the business owns the contract

Summary (2 of 2)

- Several risks are associated with using mobile devices
- Mobile devices have the ability to access untrusted content that other types of computing devices generally do not have
- Users should consider security when initially setting up a mobile device
- Several support tools can facilitate the management of mobile devices in the enterprise
  - Mobile device management (MDM) tools allow a device to be managed remotely by an organization
  - Mobile application management (MAM) covers application management
  - A mobile content management (MCM) system provides content management to mobile devices used by employees in an enterprise
- Embedded and specialized devices can be classified into several categories
- Security in embedded systems is lacking and can result in a wide range of attacks