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)

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)

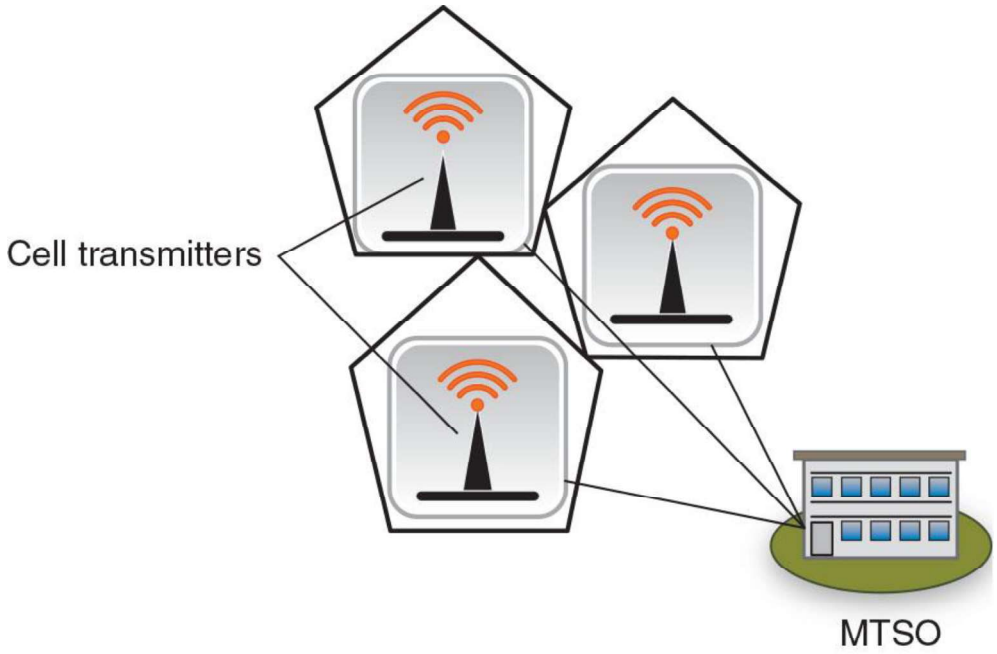

Figure 5-4 Cellular telephony network

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.

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

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.

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)

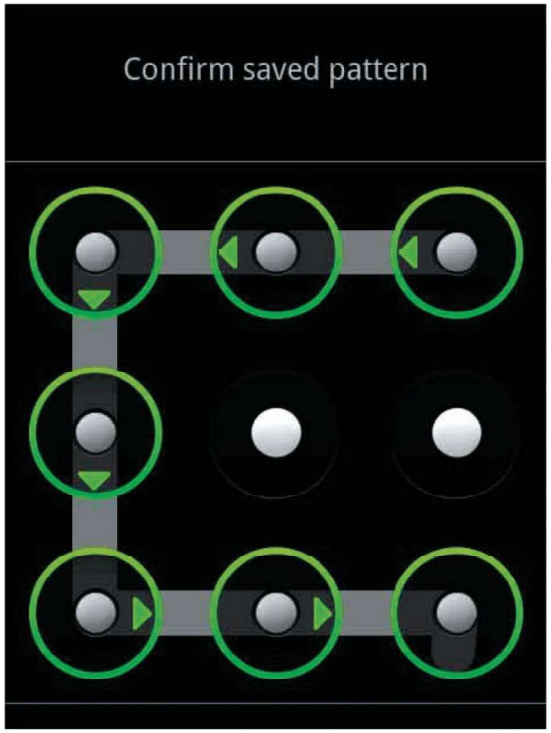

Figure 5-6 Swipe pattern

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

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.