Information Security (CP3404)

Chapter 10 – Mobile Device Security

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

- List and compare the different types of mobile devices
- Explain the risks associated with mobile devices
- List ways to secure a mobile device
- Explain how to apply mobile device app security
- Describe how to implement BYOD security

Outline

Preface

- Just as users have flocked to mobile devices, so too have attackers
- Because mobile devices have become primary or exclusive computing device for users now seen dramatic increase in malware and attacks directed at devices
- Mobile devices themselves must also be constantly protected from loss or theft

Types of Mobile Devices

Basic Characteristics

- Small form factor
- Wireless data network interface for accessing Internet (Wi-Fi or cellular data connection)
- Mobile operating system
- Applications (apps) can be acquired through different means (Web, included with the operating system, or provided by wireless data carrier)
- Data synchronization capabilities with separate computer or remote servers
- Local nonremovable data storage

Types of Mobile Devices

Optional Features

- Digital camera(s)
- Global Positioning System (GPS)
- Microphone
- Removable storage media
- Support for using device itself as removable storage for another computing device
- Wireless cellular connection for voice communications
- Wireless personal area network interfaces (Bluetooth, NFC)

Types of Mobile Devices

Types of Mobile Devices

- Several different types of mobile devices:
  - Portable Computers
  - Tablets
  - Smartphones
  - Wearable Technology
  - Legacy Devices
- Most devices also have removable storage capabilities

Types of Mobile Devices

Portable Computers

- Portable computers – Devices that closely resemble standard desktop computers
  - Similar hardware (keyboard, hard disk drive, RAM)
  - Run same operating systems (Windows, Apple Mac OS, or Linux)
  - Use same application software (Microsoft Office, web browsers)
- Primary difference is portable computers are smaller self-contained devices that can easily be transported from one location to another while operating on battery power

Types of Mobile Devices

Portable Computers — Laptops

- Laptop – Regarded as earliest portable computer
- Designed to replicate abilities of desktop computer with only slightly less processing power
- Small enough to be used on lap or small table
- Considered cumbersome to transport in carrying case for an extended period of time
- Have multiple hardware ports (USB, eSATA), wired network ports (RJ-45), optical drives (DVD or Blu-ray)
- May accommodate limited hardware upgrades

Types of Mobile Devices

Portable Computers — Notebooks

- Although often considered to be identical, laptop computer and a notebook computer are different (see Table 10-1)
- Notebook – Smaller version of laptop computer and considered as lightweight personal computer
- Typically weigh less than laptops
- Small enough to fit easily inside briefcase
- Designed to include only most basic frequently used features of computer in smaller portable size
- Have limited number hardware ports, do not include optical drives, and often cannot be upgraded

Types of Mobile Devices

Feature	Laptop	Notebook
Size	Larger devices with display screens ranging from 10 to 19 inches (25.4 to 48.3 cm)	Smaller devices designed to fit easily into a small bag or briefcase
Optical drives	Integrated into the device	Not included but can be attached externally
Processor	Slightly less powerful than desktops	Generally not as powerful as laptops
Cooling capacities	Includes fan similar to desktop	Does not require fan due to less powerful processor
Intended use	Replicates functionality of desktop system	Portable personal device for essential computing functions

Table 10-1 Laptop vs. notebook computers

Types of Mobile Devices

Portable Computers — Subnotebooks

- Subnotebook – Relatively new class of portable computers; sometimes called ultrabook (Intel/Windows) or air (Apple)
- Even smaller than standard notebooks and use low-power processors and solid state hard disk drives (SSDs)
- Have high-definition multimedia interface (HDMI) port along with limited number of Universal Serial Bus (USB) hardware ports (see Figure 10-1)

Types of Mobile Devices

Figure 10-1 Subnotebook computer
© Creativa/Shutterstock.com

Types of Mobile Devices

Portable Computers — Web-Based

- Web-based – New type of computing device that resembles laptop computer
- Contains limited version of Linux operating system and a web browser with integrated media player
- Designed be used primarily while connected to Internet
- No traditional software applications can be installed and no user files stored locally on device
- Device accesses online web apps and saves user files on Internet

Types of Mobile Devices

Tablets

- Tablets – Portable computing devices generally larger than smartphones and smaller than notebooks but focused on ease of use
- Generally lack built-in keyboard and instead rely on touch screen (see Figure 10-2)
- Tablets often classified by screen size
- Thinner, lighter, easier to carry, and more intuitive to use than portable computers
- Most popular operating systems for tablets are Apple iOS, Google Android, and Microsoft Windows

Types of Mobile Devices

Figure 10-2 Tablet computer

© maximino/Shutterstock.com

Types of Mobile Devices

Smartphones

- Feature phone – Traditional cellular telephone with limited number of features (camera, MP3 player, ability to send and receive *short message service* (SMS) text messages)
- Smartphone – All tools of feature phone and includes operating system to run apps and access Internet
- Because has an operating system smartphone offers a broader range of functionality (see Table 10-2 for market share)
- Ability to run apps makes smartphones essentially handheld personal computers

Types of Mobile Devices

Year	Smartphone market share (%)	Feature phone market share (%)
2011	35	46
2012	46	41
2013	54	38
2014	58	35
2015	62	33
2016	67	28

Table 10-2 Smartphone vs. feature phone worldwide market share[6]

Types of Mobile Devices

Wearable Technology

- Wearable technology – Mobile technology consists of devices that can be worn by user instead of carried for even greater flexibility and mobility
- One wearable technology device is optical head-mounted display (most common display is Google Glass —see Figure 10-3)
- Smart watch – Device serves as accessory to smartphone so users can easily glance to view messages
- May have own set of sensors and software features to function independently

Types of Mobile Devices

Figure 10-3 Google Glass

© Joe Seer/Shutterstock.com

Types of Mobile Devices

Legacy Devices

- Several different mobile devices are no longer widely in use and are considered legacy devices
- Personal digital assistant (PDA) – Handheld mobile device intended to replace paper systems
- Included appointment calendar, address book, *to-do* list, calculator, and ability to record limited notes
- Netbook – Small, inexpensive, and lightweight portable computer used low-powered processors, featured small screens and keyboards, omitted optical storage, and could not be upgraded

Types of Mobile Devices

Mobile Devices Removable Storage

- Mobile devices use flash memory for storage, which is nonvolatile that can be electrically erased and used
- All mobile devices have local nonremovable storage
- Most mobile devices also support removable data storage:
  - Large Form Factor Storage
  - Small Form Factor Storage

Types of Mobile Devices

Mobile Devices Removable Storage — Large Form Factor Storage

- PC Card – Credit cardsized peripheral slides into slot on laptop computer to add additional functionality
- PC Card standard defines three (3) form factors for three (3) types of PC Cards (see Table 10-3)
- CardBus – Enhanced type of PC Card
- ExpressCard – Replacing PC Card and CardBus devices

Types of Mobile Devices

PC Card type	Length (mm)	Width (mm)	Thickness (mm)	Typical uses
Type I	85.6	54	3.3	Memory
Type II	85.6	54	5.0	Input/output devices
Type III	85.6	54	10.5	Rotating mass storage devices

Table 10-3 PC Card form factors

Types of Mobile Devices

Mobile Devices Removable Storage — Small Form Factor Storage

- Compact Flash (CF) – Small form factor generally used as a mass storage device format for portable electronic devices
- Secure Digital (SD) – Format includes four card *families* available in three different form factors with different speed ratings
- Currently three (3) sizes of SD cards:
  1. Full SD
  2. MiniSD
  3. MicroSD (see Figure 10-4)

Types of Mobile Devices

Figure 10-4 microSD card

© *ExaMedia Photography/Shutterstock.com*

Types of Mobile Devices

Mobile Devices Removable Storage — Small Form Factor Storage

- Secure Digital (SD) speed classes were designed to support video recording
- There are two (2) types of speed classes (see Table 10-4):
  1. Standard Speed Class
  2. Ultra High Speed (UHS) class

Types of Mobile Devices

Class	Class ranking	Minimum speed (MB per second)	Application
Standard speed class	2	2	SD video recording
Standard speed class	4	4	High-definition (HD) video recording
Standard speed class	6	6	HD video recording
Standard speed class	10	10	Full HD video recording and still HD recording
UHS speed class	U1	10	Real-time broadcasts
UHS speed class	U3	30	4K resolution video files

Table 10-4 SD speed classes

Mobile Device Risks

Mobile Device Risks

- Risks associated with using mobile devices include
  - Limited Physical Security
  - Connecting to Public Networks
  - Location Tracking
  - Installing Unsecured Applications
  - Accessing Untrusted Content
  - Bring Your Own Device (BYOD) Risks

Mobile Device Risks

Limited Physical Security

- Greatest asset of a mobile device –portability– is greatest vulnerability
- Devices can easily be lost or stolen, and any unprotected data on the device could be retrieved by thief (see Table 10-5)
- Also using mobile device in public area can be considered a risk
- Users must guard against shoulder surfing by strangers who want to view sensitive information being displayed on phone

Mobile Device Risks

Area of airport	Percentage of laptops stolen
Luggage/storage area	29
Terminal/boarding area	22
Other	19
Airplane	18
Check-in/security	12

Table 10-5 Top five areas for airport laptop theft

Mobile Device Risks

Connecting to Public Networks

- Mobile devices must use public external networks for their Internet access
- Because these networks beyond control of organization, attackers may eavesdrop on data transmissions and view sensitive information
- Open networks may be susceptible to man-in-the-middle or replay attacks

Mobile Device Risks

Location Tracking

- Location services – Can identify location of a person carrying a mobile device
- Mobile devices using location services are at increased risk of targeted physical attacks:
  - Attacker can easily determine where user and mobile device are currently located to use information to follow user in order to steal mobile device or inflict harm upon person
  - Attackers can compile over time a list of people with whom the user associates and types of activities they perform in particular locations in order to craft attacks

Mobile Device Risks

Installing Unsecured Applications

- Software for traditional desktop computers is generally purchased from large and reputable vendors or is developed in-house
- Mobile devices are designed to easily locate, acquire, and install apps from variety of sources
- Sources range from large reputable vendors to single-person developers and even hobbyists.
- In many cases apps do not include security features

Mobile Device Risks

Installing Unsecured Applications — Apple iOS

- Apple iOS – Apple operating system that is closed and proprietary architecture
- Makes it more difficult for attackers to create app that could compromise it
- Many iOS app developers generate supplementary revenue by selling user data generated through app to advertising networks and analytics companies
- This user data sent back to developer for distribution is transmitted without encryption so that an attacker could access it (see Table 10-6)

Mobile Device Risks

Risky behavior	Free apps (%)	Paid apps (%)
Location tracking	62	49
Access address book	35	31
Access calendar	2	3
Identify user or device	24	27
Share data with ad networks	48	27

Table 10-6 Apple iOS apps risky behavior

Mobile Device Risks

Installing Unsecured Applications — Google Android

- Android – Google operating system for mobile devices
- Not proprietary but is entirely open for anyone to use or even modify
- Apps for Android devices can be downloaded from Google Play store (which does not screen apps like Apple does) or can from unofficial third-party website (sideloading).
- Generally makes Android apps highly risky

Mobile Device Risks

Accessing Untrusted Content

- Mobile devices have ability to access untrusted content
- Quick Response (QR) codes – Codes are a matrix or two-dimensional barcode that can be read by imaging device like mobile device's camera
- Attacker can create an advertisement listing a reputable website but include QR code that contains a malicious URL to redirect user's device to attacker's imposter website or site that immediately downloads malware

Mobile Device Risks

Figure 10-5 QR code

Mobile Device Risks

Bring Your Own Device (BYOD) Risks

- Bring your own device (BYOD) – Policy that allows users to use their own personal mobile devices for business or organizational purposes
- Several risks associated with BYOD:
  - Users may erase installed built-in limitations
  - Personal mobile devices often shared among family members and friends
  - Technical support staff support hundreds of different mobile devices
  - Mobile devices may be connected to user's personal desktop computer that is infected

Quick Quiz

1. **True or False:** Most portable devices have nonremovable data storage.
   Answer:

Quick Quiz

1. **True or False:** Most portable devices have nonremovable data storage.
   Answer: True

Quick Quiz

1. **True or False:** Most portable devices have nonremovable data storage.
   Answer: True

2. Google Glass is an example of _____ technology.
   Answer:

Quick Quiz

1. **True or False:** Most portable devices have nonremovable data storage.
   Answer: True

2. Google Glass is an example of _____ technology.
   Answer: wearable

Quick Quiz

1. **True or False:** Most portable devices have nonremovable data storage.
   Answer: True

2. Google Glass is an example of _____ technology.
   Answer: wearable

3. The most common locations for laptop theft are:
   (a) Hotels
   (b) Airports
   (c) Personal residences
   (d) Public Schools

   Answer:

Quick Quiz

1. **True or False:** Most portable devices have nonremovable data storage.
   Answer: True

2. Google Glass is an example of _____ technology.
   Answer: wearable

3. The most common locations for laptop theft are:
   (a) Hotels
   (b) Airports
   (c) Personal residences
   (d) Public Schools

   Answer: (d)

Securing Mobile Devices

Securing Mobile Devices

- Securing mobile devices requires several steps:
  - Device Setup
  - Device and App Management
  - Device Loss or Theft

Securing Mobile Devices

Device Setup

- Configurations should be considered when initially setting up a mobile device for use:
  - Disabling Unused Features
  - Enable Lock Screen
  - Use Encryption
  - Control Access

Securing Mobile Devices

Device Setup — Disabling Unused Features

- Mobile devices include a wide variety of features for the user's convenience
- Each of these can also serve as threat vector
- Important to disable unused features and turn off those that do not support the business use of phone or that are rarely used
- One feature should be disabled if not being regularly used is Bluetooth in order to prevent bluejacking and bluesnarfing

Securing Mobile Devices

Device Setup — Enable Lock Screen

- Lock screen – Prevents mobile device from being used until user enters correct passcode
- Lock screens should be configured so that whenever device turned on or left idle for a period of time passcode must be entered
- Many devices can be configured for additional security protections:
  - Extend lockout period
  - Reset to factory settings

Securing Mobile Devices

Device Setup — Enable Lock Screen (Passcode)

- Most mobile devices have different options for type of passcode that can be entered:
  - Strong passwords are seldom used on mobile devices but are most secure option
  - Draw or swipe a specific pattern connecting dots (see Figure 10-6)
  - Short four-digit PIN is least effective code (see Table 10-7)

Securing Mobile Devices

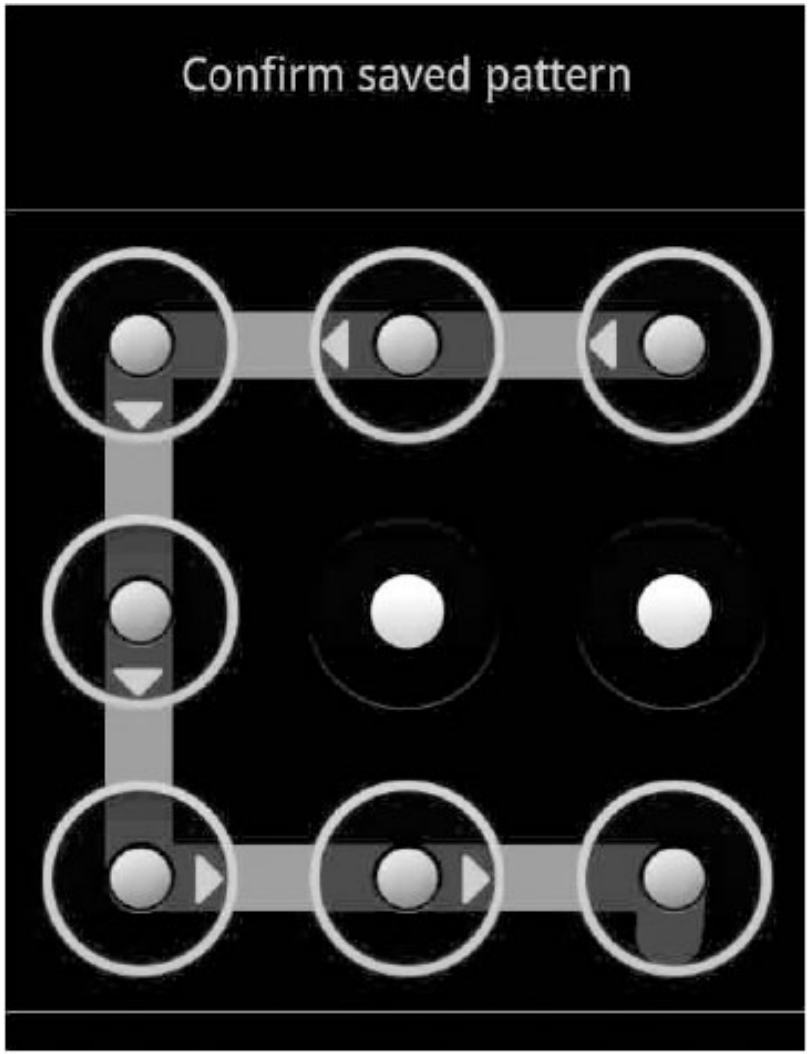

Figure 10-6 Swipe pattern
Source: OnlineAndroidTips.com

Securing Mobile Devices

PIN	Frequency of use (%)
1234	10.71
1111	6.01
0000	1.88
1212	1.19
7777	0.74

Table 10-7 Most common PINs

Securing Mobile Devices

Device Setup — Use Encryption

- Mobile devices that contain sensitive data should have data encrypted
- Currently neither Apple iOS nor Google Android provide native cryptography, so third-party encryption apps must be installed
- Two (2) encryption options:
  1. Full device encryption can be enabled to apply protection to all data stored on the device
  2. Separating data storage into containers and encrypting only sensitive data

Securing Mobile Devices

Device Setup — Control Access

- Key to securing mobile devices to control access to device and data by limiting who is authorized to use information
- At higher corporate level decisions must be made on who can access the data well before it is downloaded onto a mobile device
- Organizations are now beginning to focus their efforts on data instead of just device by extending data loss prevention to mobile devices

Securing Mobile Devices

Device and App Management

- Once the device is initially configured, both the device and its applications must be managed
- There are two (2) tools for facilitating this management:
  1. Mobile Device Management (MDM)
  2. Mobile Application Management (MAM)

Securing Mobile Devices

Device and App Management — MDM

- Mobile device management (MDM) – Tools allow device to be managed remotely by an organization; involves:
  - Server component that sends out management commands to mobile devices
  - Client component that runs on mobile device to receive and implement the management commands
- Administrator perform over the air (OTA) updates or configuration changes to one device, groups of devices, or all devices

Securing Mobile Devices

Device and App Management — MDM Features

- Rapidly enroll new mobile devices (on-boarding) and quickly remove devices (off-boarding) from the organization's network
- Apply or modify default device settings
- Enforce encryption settings, antivirus updates, and patch management
- Display acceptable use policy that requires consent before allowing access
- Configure email, calendar, contacts, Wi-Fi, and virtual private network (VPN) profiles OTA
- Discover devices accessing enterprise systems

Securing Mobile Devices

Device and App Management — MDM Device Control

- MDM also can facilitate device control:
  - Asset tracking – Maintaining accurate record of company-owned mobile devices
  - Inventory control – Operation of stockrooms where mobile devices are stored prior to their dispersal to employees

Securing Mobile Devices

Device and App Management — MAM

- Mobile application management (MAM) or Application control – Tools and services responsible for distributing and controlling access to apps
- Apps can be internally developed or commercially available
- MAM initially controlled apps through app wrapping, which sets up a dynamic library of software routines and adds to existing program (binary) restrict parts of app

Securing Mobile Devices

Device Loss or Theft

- To reduce risk of theft or loss:
  - Keep the mobile device out of sight when traveling in high-risk area.
  - Avoid becoming distracted by what is on the device
  - Use both hands on device to make more difficult for thief to snatch
  - Do not use device on escalators or near transit train doors
  - Change headset cord to less conspicuous color
  - If a theft does occur do not resist or chase thief

Securing Mobile Devices

Device Loss or Theft — Limit Damage

- If mobile device lost or stolen several different security features can be used locate device or limit the damage
- Can be used through (see Table 10-8):
  - MDM
  - Feature in operating system
  - Installed third-party app

Securing Mobile Devices

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	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.

Table 10-8 Security features for locating lost or stolen mobile devices

Mobile Device App Security

Mobile Device App Security

- Apps on device also should be secured:
  - App can be encrypted
  - Can require that user provide authentication such as a passcode before access is granted
  - MDMs can support application whitelisting, which ensures that only preapproved apps can run on device
  - Credential management – Serves as *vault* for storing valuable authentication information; MDMs allow users to store usernames and passwords within device itself

Mobile Device App Security

Mobile Device App Security — Geo's

- Geo-fencing – Uses device's GPS to define geographical boundaries where app can be used
- For example, tablet containing patient information that leaves hospital grounds can result in alert sent to administrator
- Geo-tagging – Adding geographical identification data

BYOD Security

BYOD Security — Company benefits

- Management flexibility
- Less oversight
- Cost savings
- Increased employee performance
- Simplified IT infrastructure
- Reduced internal service

BYOD Security

BYOD Security — User benefits

- Choice of device – Users like freedom of choosing type of mobile device they want
- Choice of carrier – Most users have identified specific wireless data carrier they want to use
- Convenience – Many users already have own device and want convenience of using only single device
- Attraction – BYOD can be appealing recruitment incentive for prospective employees

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer:

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

2. **True or False:** Disabling Bluetooth is a recommended security step?
   Answer:

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

2. **True or False:** Disabling Bluetooth is a recommended security step?
   Answer: True

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

2. **True or False:** Disabling Bluetooth is a recommended security step?
   Answer: True

3. A management feature that sends an alert when a device is carried into a restricted physical area is known as _____.
   Answer:

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

2. **True or False:** Disabling Bluetooth is a recommended security step?
   Answer: True

3. A management feature that sends an alert when a device is carried into a restricted physical area is known as _____.
   Answer: Geo-fencing

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

2. **True or False:** Disabling Bluetooth is a recommended security step?
   Answer: True

3. A management feature that sends an alert when a device is carried into a restricted physical area is known as _____.
   Answer: Geo-fencing

4. **True or False:** BYOD relies on management securing a common wireless data carrier for all employees.
   Answer:

Quick Quiz

1. Which is a more secure method of unlocking a screen: short PIN or swipe pattern?
   Answer: swipe pattern

2. **True or False:** Disabling Bluetooth is a recommended security step?
   Answer: True

3. A management feature that sends an alert when a device is carried into a restricted physical area is known as _____.
   Answer: Geo-fencing

4. **True or False:** BYOD relies on management securing a common wireless data carrier for all employees.
   Answer: False