CIT 270: SYSTEMS SECURITY I

CHAPTER 10: MOBILE AND EMBEDDED DEVICE SECURITY

BYU IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

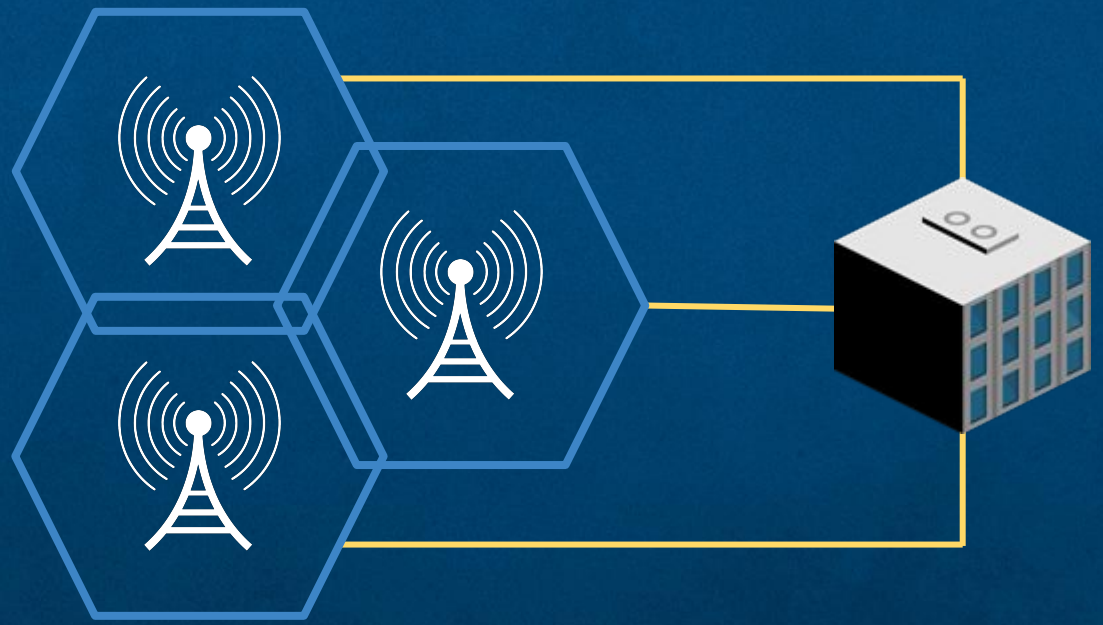
MOBILE DEVICE TYPES AND DEVELOPMENT

Laptops, tablets, fitness trackers, smartphones, smartwatches, and so on are common mobile devices with common features that many be possible to exploit:

Core Features	**Additional Features**
Small form factor	Global Positioning System (GPS)
Mobile OS	Microphone and/or digital camera
Wireless data network interface; Wi-Fi or cellular	Wireless cellular for voice communications
Applications (Apps)	Wireless PAN interfaces: bluetooth, NFC
Local non-removable storage	Removable storage
Data synchronization capabilities	Using the device as removable storage for another

MOBILE DEVICE TYPES AND DEVELOPMENT: CONNECTIVITY METHODS

When not using Wi-Fi mobile devices rely on Cellular Telephony to stay connected to the internet and other devices. Cell towers on average are placed 10 square miles (26 square kilometers) apart in an overlapping hexagon-shaped cell pattern. Mobile telecommunications switching offices (MTSO) send and receive tower signals with the wired telephone network.



MOBILE DEVICE TYPES AND DEVELOPMENT: CONNECTIVITY METHODS

Satellite Communications (SATCOM): repeaters located in satellites receive transmissions from ground stations and regenerates (repeats) this transmission to another station on earth; 250 milliseconds.

Infrared: one type of light invisible to the human eye but close to the visible spectrum. Can be used for small slow data transfers; gameboy, TV remotes.

ANT: similar to low energy bluetooth, ANT is a proprietary wireless network technology used primarily by sensors for communicating data; slave and master setup used in devices like fitness trackers, heart monitors, watches, and power meters.

MOBILE DEVICE TYPES AND DEVELOPMENT: DEPLOYMENT MODELS

Enterprise Deployment Models:

Model Name	Description	Employee Actions	Business Actions
Bring your own device (BYOD)	Use your own device for business purposes.	Employees have full responsibility of device.	Popular with small companies or temp staff.
Corporate owned personally enabled (COPE)	Employees choose from a selection of company approved devices.	Business supplies device but employee can still use it for personal use.	Company decides level of choice and freedom with the device.
Choose your own device (CYOD)	Similar to COPE but employee pays cost.	Uses company approved apps and settings.	Provides a stipend to pay phone fees.
Corporate owned	Device is purchased and owned by the company.	Only use phone for business purposes.	Company has full responsibility of device.

MOBILE DEVICE RISKS

When a mobile operating system requires updates it usually requires an over-the-air (OTA) update also known as the firmware OTA update. Many OEMs are reluctant to do OTA updates which in turn affects your security if you use one of their devices; Apple iOS versus Google Android.

Geolocation: the process of using the devices global positioning system (GPS) to identify the geographical location of a users device.

GPS Tagging: aka. geo-tagging is when geographical identification data is added into media such as pictures or video taken on your device.

MOBILE DEVICE RISKS

Normally users cannot download and install unapproved apps on their devices. Circumventing the installed built-in limitations of your smartphone to install these apps is known as jailbreaking on iOS devices and rooting on Android devices.

Third-party app stores provide users a way to download these unapproved apps which can be sideloaded (not added by the approved method) which can even allow users to run their own custom firmware.

NOTE: carrier unlocking is not the same as jailbreaking/ rooting. This refers to unlocking a phone so it can be used on another providers cellular network.

MOBILE DEVICE RISKS

Short Message Service (SMS): short text messages with a max length of 160 characters; links.

Multimedia Messaging Service (MMS): provides a way to send pictures, video, and audio along with text in a fashion similar to SMS; links or infected media.

Rich Communication Services (RCS): communication protocol between mobile telephone carriers aiming at replacing SMS messages with a text-message system that is richer, provides phonebook polling (for service discovery), and can transmit in-call multimedia (Wikipedia).

Securing Mobile Devices

Screen Lock: prevents the mobile device from being accessed until the user enters the correct passcode; biometrics, patterns, or personal identification number (PIN).

Context-aware Authentication: uses contextual settings to validate the user such as connected to a particular WiFi network or Bluetooth network; face lock.

Securing Mobile Devices

Storage Segmentation: an option on mobile devices that contain both personal and corporate data that separates business data from personal data.

Containerization: seperate storage “containers” for personal and corporate data that is managed separately and appropriately.

Remote Wipe: if a device is lost and can not be found this allows you to erase sensitive data stored on the device.

Mobile Management Tools

Read pages 446 – 454.

NOTE: References are not correct in this copy of the powerpoint.

REFERENCES

Book [PNG]. Flat Icon. https://www.flaticon.com/free-icon/book-opened-outline-from-top-view_30169

“DMZ (Computing).” Wikipedia, Wikimedia Foundation, 13 May 2019, en.wikipedia.org/wiki/DMZ_(computing).

Link Icon [PNG]. Share Icon. No license found, public domain inferred.

“Malware Protection Techniques (Part 3): Heuristics” Sourcefire, YouTube, 12 December 2012, https://youtu.be/d7boMCLmnaA

OSI model vs. TCP/IP model [Figure 7-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 284. Boston, MA: Cengage.

REFERENCES

Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.

“Question: What is Heuristic Analysis?” The Thing of the Name, YouTube, 4 February 2015, https://youtu.be/hLdYx1od-0o

Secure network protocol recommendations [Table 7-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 291. Boston, MA: Cengage.

Type I and Type II Hypervisors [Figure 7-8]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 301. Boston, MA: Cengage.

https://svgsilh.com/ffffff/image/28883.html || https://www.shareicon.net/building-skyscraper-880296