

5

Mobile, Embedded and Specialized Device Security

Up to this point we've mainly been looking at securing computers. While most of what you've learned also applies to devices like laptops, phones, and tablets, these devices present additional security challenges. In this section you'll learn about the special security problems faced by mobile devices, such as the loss of physical protection when they're taken out of the home or office, and network security challenges since many users connect their mobile devices to open public networks. Mobile devices also present new challenges if you want to allow individuals to connect their personal devices to an otherwise secure network. You will also learn about specialized small computers such as industrial controllers and IoT devices, and the challenges in securing them.

Objectives

At the end of this module, you will be able to:

1. Define the following terms and describe how they are related to security: SCADA, ANT, Bluetooth, BYOD, Arduino, Raspberry Pi, RFID, NFC, and BLE
2. List and compare the different types of mobile devices and how they are deployed
3. Explain the ways to secure a mobile device
4. Describe the vulnerabilities and protections of embedded and specialized devices
5. Explain the issues surrounding securing specialized devices
6. Secure their own mobile devices (check app permissions, install updates and patches, use strong passwords, perform backups, ensure anti-malware is enabled, ensure location service is enabled).

Section Content

Introduction

In this section you're going to learn about securing mobile, embedded, and specialized devices. This includes cell phones and tablets, as well as smart devices and something called embedded controllers which are used industry. In addition to learning about these devices you will also learn about the communication protocols used by these devices, and the extra security challenges presented by the devices in these categories.

The list of devices you'll be learning about in this chapter include:

1. Laptops, phones, tablets, etc. Any device that's meant to be portable
2. Smart devices such as smart TVs and smart cars, smart garage door openers, etc.
3. Embedded systems and industrial systems
4. Specialized devices such as drones, VoIP phones, IoT devices, etc.

In other words, this chapter covers pretty much everything that isn't a standard computer or network router, which is pretty much all the cool new stuff. And while the chapter has security in the title, it also discusses risks associated with these devices.

Once again, this chapter presents a lot of new terminology. While some of the terms in this chapter are super basic, like what is a smartphone, laptop or tablet or portable computer; there are a few terms that refer to things you may not have seen before, such as ANT, or SCADA or BYOD and MDM. Some of the book's explanations of these technologies won't make a lot of sense unless you already know something about the technology. I'm sure you know what laptops, cell phones, and tablets are so we won't spend any extra time explaining those. But I will explain what SCADA, Arduino and Raspberry Pi devices are, as they are aspects of computing and security you should know about. After that you'll learn about a few additional communication protocols used by mobile devices such as ANT or Bluetooth. Then we'll go a

little deeper into the new security challenges you'll face if you're tasked with protecting these devices in the workplace, plus ways for you to protect your own mobile devices.

As you go through the chapter try to keep in mind the main goal at this point is to simply introduce you to these technologies and terms. A secondary goal is to maybe pique your interest in things like Arduino or Raspberry Pi programming. Hopefully you will leave this chapter feeling like you want to learn more. If that's the case, remember that you will learn a lot more detail about the different risks and ways of mitigating the risks in later classes.

Terminology

In this section I'll provide explanations of a couple of the technologies that I think you should know about. I'm only going to do this slightly deeper dive for a couple of items, otherwise we'd be discussing this material for a year or two. These items are SCADA, Raspberry PI, and Arduino. The reason we're going deeper into these items is that I believe these are huge opportunities for you, and this might be the only time they're discussed in the classes in the CBC Cybersecurity degree program.

SCADA

SCADA stands for Supervisory Control And Data Acquisition. SCADA devices consist of devices that combine smart sensors and device controllers and they're typically used for industrial applications. One simple example of a SCADA like device is your home thermostat. This monitors the temperature in your home, and if the temperature moves past a certain limit the thermostat sends a signal to your homes Heating Ventilation and Air Conditioning (HVAC) unit instructing it to heat (or cool) your home. SCADA devices are similar to the smart devices you can buy for your home, but instead of controlling your garage door they do things like monitor water pressure in pipes and use the data they gather to decide things like whether to open or close valves; or monitor the flow of electricity through the nation's power grid. SCADA devices are critically important to our modern infrastructure and way of life, and learning how to protect them is another subject that should lead to an interesting and lucrative career.

Maybe you've done some Arduino programming or used the Lego Mindstorm system. These are pretty similar to SCADA, where you have a sensor that checks for something like a sound or physical pressure, and then runs a motor or triggers some other code to run. If you have experience with Arduinos or similar systems, then you have a good idea of what SCADA is. If not, and you want to know more about SCADA you can watch the videos in the list below. I would suggest watching the first two videos if you're still unsure what SCADA is. The second two videos are optional but go into much better detail on the security issues associated with SCADA devices. If these links are no longer valid, you can do your own search.

<https://www.youtube.com/watch?v=XbZE0Xd5RIs> What is SCADA. This video provides a quick intro and definition. (~3:00)

<https://www.youtube.com/watch?v=nIFM1q9QPJw> What is SCADA. This video provides a little deeper dive into SCADA, along with a good history of SCADA. (~8:00)

<https://www.youtube.com/watch?v=LyzlrE6DpOM> A Pentester's Intro to Attacking ICS/SCADA - Tripp Roybal (~33 minutes)

<https://www.youtube.com/watch?v=sCd--Tsj4sM> Industrial Control System (ICS) and SCADA: Risks and Solutions (~1 Hr)

Arduino and Raspberry Pi

The next two terms you'll learn about are Arduino and Raspberry Pi. These are great ways for you to make your own smart devices and controllers. Understanding the books descriptions of these devices probably doesn't help you understand what they are or what you can do with them. I could also add more text to try and explain, but these are systems that are much easier to define in a video. You can start with the following links or do your own search for Arduino or Raspberry Pi.

<https://www.youtube.com/watch?v=nL34zDTPkcs> You can learn Arduino in 15 minutes from AfroTechMods

<https://www.youtube.com/watch?v=p40OetppIDg> What's the difference? Arduino vs Raspberry Pi – From TinkerNut

<https://www.youtube.com/watch?v=rS9CbsohFGk> Top 10 Raspberry Pi Projects for 2022

The Arduino and Raspberry Pi systems are both extremely versatile systems designed for home use. They both have tremendous community support with the instructions for thousands of projects available. They are both also surprisingly inexpensive, both the main boards and the add on sensors. If you're even halfway interested, I suggest you buy an Arduino or a Pi, find a project on the Internet, and start tinkering yourself. The hands-on experience should not only be fun, but it's also a great way to gain insight into several subjects such as SCADA, smart devices, and Linux if you work with a Raspberry Pi. This isn't a class requirement, it's just something that I've found to be super educational and fun. If you want to check out what's possible do an Internet search for Arduino projects or Raspberry Pi projects and be prepared to be amazed.

The last thing I want to say about Arduino and Raspberry Pi is that I'm not sure why the book says that the Arduino is generally considered a better solution. Maybe because an Arduino consumes less power. But in reality, there are some projects that can only be done with a Raspberry Pi because it has a programmable CPU. In other words, if you have a project that doesn't require any "smarts" and can be done by either an Arduino or a Pi, the Arduino will be a better choice. But if your project requires the device to use programming code, you'll have to use a Pi.

I know I just said I had one last thing to tell you, but here's one more. This just a stupid piece of trivia, but the Arduino is named after a bar in Italy where the original designers used to meet while they were planning the project. Oh ... and here's one more, and this time I promise it's the last. I imagine that if this is all new to you it can feel a bit overwhelming. But from my perspective I'm a bit envious that there's so much interesting and fun stuff for you all to start your careers working on.

Security Challenges

The explosion of mobile and smart devices presents new challenges and opportunities for anyone in charge of protecting the devices or protecting a network that permits these devices to connect. In this section we'll look at the challenges with protecting these devices, then look at the challenges posed by allowing mobile devices to connect to a network.

The Challenge of Protecting Multiple Devices

One of the reasons that dealing with mobile devices and smart devices is such a challenge is the rapid rate of growth of the number and types of these devices. And one of the difficulties in being a security specialist is that you need to be intimate with the systems you're assigned to protect.

Use your own situation as an example. You may have years of experience as a Windows user, but it's also quite possible that before this class you never heard of things you will need to know about to be a security specialist. For example, before taking this class had you even heard of Local Group Policies, or Registry, or using the mmc or other tools? It takes some amount of time and effort to learn about these things, and how they can be configured or used to protect your computer. Or think about something that you are intimate with, like your phone, or a video game. Do you remember how foreign it seemed when you first started to use it, but after weeks or months of use you gradually learned all the little details about it. The point is, it takes some time to become truly intimate with any new hardware or software.

And the bigger point is, that there's been an explosion of new mobile and smart devices. If you're the person responsible for security, it can be a challenge to keep up with all the devices that your users or customers want to use and connect to the company network. It's hard enough just to keep up with the security issues for Windows computers. Now imagine if you also have to understand and keep up with security issues for all the different phones and tablets or other smart devices a user wants to connect to your network.

However, this new challenge also brings a new opportunity. If I were just starting on my career, I'd strongly consider setting up a company that specializes in helping configure and secure smart devices. That is, I would come to your home or business and help you integrate and secure all your smart devices and appliances. I'd help with your Alexa, Google Nest, or Siri or whatever home hub you use, with your wireless network, your smart devices, and your computing devices. I think the market for this type of business is only going to grow in the next 5 years. And I also believe that the people who pay top dollar for a smart fridge are probably not technically inclined enough to set it up themselves, but they will have enough money to pay someone who is technically competent and can do the setup and integration for them.

The Challenge of Protecting BYOD Networks

In the old days networks consisted of traditional desktop computers and networking equipment like switches and routers. These were relatively easy to protect as you, or the person in charge of cybersecurity, could control the security on each device and control what was connected to the network. Now people want to connect all kinds of devices to a network, either directly, like connecting a laptop or tablet through a wired or wireless connection, or indirectly by doing something like connecting their phone or other devices to their laptop via Bluetooth and then connecting the laptop to the network.

A good analogy would be to say you're going to have a party at your house. You'll probably feel ok about the security of the items in your house if you only invite family and friends that you know very well. You're intimate with this group and know that you can trust them. But you may

feel different about it if everyone you invite is also allowed to invite whomever they want. If you allow this, you end up in a situation where you no longer have direct control of the people in your house, and you end up placing control of your security on others. Plus, you know your uncle and a couple of your cousins hang out with some sketchy people. If you have to worry about security with the strangers your uncle or cousins invite in your home, it's going to be a much different situation.

The book introduces some of the ways that organizations deal with blessing devices that can be connected to the network, and ways that these models will theoretically protect a network. For example, say your company buys you a laptop or phone, but tells you it's only for business use and you're not allowed to install any other applications. This way, when the device is connected to the network there should be little risk of user introduced malware. But ... what if a user opens an email attachment that's infected with malware? My point is that the Enterprise Deployment Models are theoretical models, and when put into actual practice will still cause headaches for the person in charge of cybersecurity.

Communication Protocols

Another big concept that's introduced in this section is the additional set of networking and communication protocols developed mainly for mobile devices. This includes Bluetooth, which I'm sure you've used and are aware of, but also includes a couple of protocols that the book doesn't mention in this chapter such as RFID, NFC, ANT/ANT+, and BLE. The book discusses these protocols in the chapter on Wireless Security. We won't be covering that chapter in this class, but you'll have an entire class on wireless later in the degree program. In any case, I'm going to present a little more information on a few of these protocols as I think you're probably using a few of them whether you know it or not.

Radio Frequency ID (RFID) systems consist of “dumb” devices that only transmit when they receive power beamed in from an external source. You may be familiar with RFID tags from shopping. The RFID tags consist of a small chip that will broadcast a radio signal any time it has power. The chips don’t need much power to operate, and the tags don’t have any power source so the chip is usually lying dormant. Since there’s no power on the tag it has to be obtained from an external source. With RFID, the power is supplied via radio waves, which are broadcast by a set of pillars like those you see at store entrances. The RFID pillars broadcast energy at a specific frequency which is enough to supply power to the RFID chip in tag, essentially waking it up and telling it to broadcast its ID information. The information from the RFID chip is read by the pillars, which decide how to handle it.



Near Field Communication (NFC) systems are similar to RFID, and can be used like RFID, but they are also used for things like contactless payment, where you just tap your credit card or get your phone close enough to another device to exchange information. Since NFC is available in most modern phones, it can be a security concern. However, it has a very limited range. Theoretically it’s ~4 cm, which means you would almost assuredly know if someone were that close to your phone unless you’re in a crowd. But in practice the range has been extended, to ~20cm, which is still pretty close.

If you want to know more about RFID and NFC, and their possible security risks, I suggest you watch the following, or do your own research. I liked learning about both technologies as I always had questions about how the RFID tags work, and how contactless payment works.

<https://www.youtube.com/watch?v=mzPb9QLJu8k> RFID and NFC (~8:50)

Advanced and Adaptive Network Technology (ANT/ANT+) and Bluetooth Low Energy (BLE) are both communication protocols commonly used by exercise equipment. If you're not a cyclist or runner, the thing that makes them of interest is that they're used by a lot of wearable devices, and I personally believe that wearable technology is going to big. You don't need to know anything about them for this class, I just thought you might want to be aware of them. If you want to know more, you can check the following site or do your own search.

<https://gadgetsandwearables.com/2018/01/30/what-is-ant/>

Applying What You've Learned to Your Home System(s)

This brings us to looking at practical things you can do to protect your own devices. I'm going to assume that most of you own laptops and cell phones, and maybe tablets or other smart devices, so we'll look at ways you can apply security to those devices.

For laptops, the book does a decent job of listing some of the extra things you need to do with mobile devices, like not setting them down in public, but it doesn't really talk about applying some of the basic security steps that should be applied to all your devices. For laptop computers the basic steps are exactly the same as the basic steps for desktop computers. That is, you should:

- a. Install patches and updates.
- b. Use anti-malware.
- c. Backup important data on a regular basis.
- d. Use strong passwords.

These basic steps should also be performed on your phones and tablets, but as you'll see most of the major phone vendors do this automatically, so you might not have much to do.

mobile and smart devices. There are many things you can and should do, and hopefully you're doing them already. I'm not going to go into great detail on any of these items, as the specific steps will vary greatly depending on the type of phone or device you're trying to secure. I'm going to assume that you'll be able to search the Internet to find information on securing your specific devices if you decide to. But I have provided some links to some web sites that have excellent checklists for securing Android and Apple products.

Android

If you have an Android phone, I suggest you start by reading the following articles and following their suggestions. If these web sites aren't available, you can do an Internet search for something like "android security checkup".

<https://www.computerworld.com/article/3012630/android-security-checkup.html>

<https://www.computerworld.com/article/3268079/android-security-settings.html>

iPhone

If you own an iPhone ... well, I feel sorry for you. I'm just joking of course, but maybe not. 😊 In any case, you might run through the checks specified in the following articles. . If these web sites aren't available, you can do an Internet search for something like "iPhone security checkup".

<https://support.apple.com/guide/security/welcome/web>

<https://www.fastcompany.com/90254589/use-these-11-critical-iphone-privacy-and-security-settings-right-now>

OS Updates - Phones

If you're using an iPhone or an Android phone you don't have to worry about configuring

updates. Updates are forced onto both of these OS's using something called Over The Air (OTA) updates. These are pushed onto your phone, you don't have to search for them or download them, all you possibly need to do is restart your phone when prompted. You might have a setting that allows you to delay updates for a bit. Some Android phones allow you to delay update installation up to 30 days at the longest. You should be aware that most updates are rolled out over a 30 day period, which allows the update to be tested before it's forced on everyone.¹

Updates – Smart Devices

For smart devices, like nanny cams or smart outlets, installing updates is usually pretty critical for security. The smart devices typically only run a single program, which is loaded into the device's firmware. If any vulnerabilities are discovered in the device, the only way to patch them is to update the firmware. And in my limited experience, installing updates for smart devices is usually trickier than loading updates on a phone or tablet. In most cases I've had to run the device's configuration app on my phone, and find the selection for checking for updates. That is, the updates are distributed in different ways. Using technical terms phone and tablet updates are pushed out, while the updates for smart device updates have to be pulled down to the computer/phone/tablet you use to control your smart device, and then pushed out to the device.

Anti-Virus & Anti-Malware – Phones

Anti-malware on cell phones is another security feature that's built into both iOS and Android systems. Android devices use Google Mobile Services (GMS), and while the iOS protection doesn't have a name, Apple devices have pretty decent built-in anti-virus and anti-malware built in. The OS on both Android and iPhones has been built to provide some built-in protection by running apps in their own "sandbox" which prevents them from accessing your data or other

¹ <https://www.macworld.com/article/627670/automatic-ios-updates-delay.html>

parts of your phone. The prevailing thought is you don't need to run an anti-malware package on your phone like you do on your computer^{2 3 4}.

You might hear a different message regarding anti-malware on your phone or tablet, as the anti-malware vendors want you to purchase their products. There are other anti-virus applications available, many of them free. On a personal basis, I haven't added a 3rd party anti-virus to my Android phone as the GMS anti-virus seems to be pretty robust and I'd like to avoid running another battery draining app if it's not really adding to the GMS security. Plus, I never do anything even halfway sketchy with my phone.

Also, both Google and Apple screen the apps they make available for download. The thought is that this screening process will catch malware before it's made available for download. Their screening process isn't perfect though, and there have been many occurrences where an app containing malware has been found on Google Play or in the Apple app store.

Of course, your phone's safety requires you to be careful about the apps you load on your phone, that you get them from a reputable source, and that you haven't given away unnecessary permissions to applications that you've installed on your phone.

Your phone's built-in safety also assumes that you haven't rooted your phone or jailbroken it. (Is it jailbroken? Jailbroke?) If you don't know what jailbreaking means, here's a quick explanation. Your phone is really a small computer, and both the Android OS and iOS are versions of Linux. The Linux OS, like Windows, has an administrator account, named root, which can do anything on the computer, and user accounts which can be restricted and prevented from doing certain things or accessing certain files and folders. When you jailbreak a phone or

² <https://www.androidcentral.com/phones/you-dont-need-to-install-an-antivirus-app-on-your-phone>

³ <https://www.extremetech.com/computing/104827-android-antivirus-apps-are-useless-heres-what-to-do-instead>

⁴ <https://www.techadvisor.com/feature/apple/do-you-need-antivirus-on-ipad-or-iphone-3669234>

root a phone, it means running a process that will give you access to the root or administrator account, essentially giving you access to everything on the phone. If you run any apps on a rooted phone, it makes it possible for the app to break out of its sandbox and access data that it shouldn't, which increases your security risk.

Anti-Virus & Anti-Malware – Smart Devices

Adding security software is not really an option for most smart devices such as smart cameras or smart garage door openers, as they typically only perform a single function and you're not installing other applications. So, even if you wanted to add anti-virus to your smart fridge, it probably doesn't exist, and you wouldn't be able to load it even if it did exist.

Backups - Phones

You should also be backing up certain files your phone. For most people the most valuable data is typically their pictures, movies, music, and text messages. Many cell providers provide an automatic cloud backup of your data, but if this does occur there may be limits on the amount of data. And even if your data is being backed up, you need to be aware of how your image files are being stored. Pictures are usually one of the most valuable things that people keep on their phones and would regret losing the most. Many cloud backup services, such as google photos, will make backups of your images but they store the image files at a lower resolution to save space. This usually isn't a big deal, and most people are simply ecstatic if they lose or break a phone and discover their images have been backed up. The one time the lower resolution can be a problem is if you want to make a large print of an image. In any case, I suggest that you make regular backups of your phone, making sure to get copies of your photos and videos.

Text messages are another item that are typically backed up to the cloud, but backing up critical text messages to somewhere other than the cloud can be also done with an app. However, I'm going to suggest that if you're having a conversation that you need to record for legal purposes, that you do it via email instead of via text. In any case, make sure that you're backing up anything that you can't easily recreate and you may need or want in the future.

Use Strong Passwords – Phones

This is critical for phone and smart devices. Obviously, you want to protect access to your phone, and there are currently several ways to do this such as using passwords or pins, biometrics such as fingerprint detection, pattern detection, etc. While biometrics and patterns provide a quick way to unlock a phone, they are also less secure. But in any case, make sure you at least use something to lock your phone. The following site discusses the relative strengths of the various ways of locking your phone.

<https://www.androidauthority.com/fingerprints-insecure-phone-1043477/>

Use Strong Passwords – Smart Devices

Setting or changing the password on smart devices is also a basic step you need to take to protect your devices. Smart devices usually have default administrator password, so if you don't set a new password, it makes it very easy for an attacker to gain access to the device⁵. You may have seen all the news stories about hackers gaining access to someone's smart baby monitors or doorbell cams. They were able to do this because the users never changed the default password.

Physical protection for mobile devices

This refers to preventing theft of a device and it's an aspect of security that's different for mobile devices than it is for most home desktop computers and networking equipment. You need to think about physical protection for all your devices, your home computers, and your mobile devices. However, you can provide physical protection for your home computer and home router by locking your doors since these devices rarely leave home. But phones, laptops, tablets, wearables, etc. are meant to be mobile, and locking them up in your house really hinders their mobility. In addition to being mobile, devices like your phones and tablets are

⁵ <https://www.digitaltrends.com/home/default-password-flaw-ben-gurion-university/>

smaller, which makes them much easier to take with you, but also much easier to lose or steal. So, in the case of mobile devices, physical protection means doing the same types of things you would do to protect your wallet or purse. That is, don't leave your devices laying around, even for a second while you refill your coffee; and take special care when you travel.

Finding lost or stolen devices

Even with our best intentions and efforts, devices get lost or stolen. There are all kinds of situations that may be extra chaotic or where you're under more stress than normal or physically exhausted and not quite thinking straight. If you've ever travelled with small kids or a herd of teenagers, flown for hours, or experienced a severe illness or death in the family, you know how easy it is to misplace something, especially something small like a phone. So, what do you do if this happens? Is there any way to get your laptop or phone back once it's been lost or stolen?

You can probably guess that the answer is yes because I wouldn't have brought up the subject if the answer was no. Apparently this happens frequently enough that the major OS vendors have built-in ways to track or lock lost devices. Or you can download 3rd party apps that will also help you retrieve lost devices. You'll use one of these 3rd party apps in one of the exercises for this section.

If you want to use the built-in applications for using lost devices, you'll probably need to turn on the feature as it's not turned on by default. You may also need to create an account, either in the Microsoft environment for Windows, or a Google account for Android devices. The instructions for configuring and using these features can be found in the following sites. As usual, if these links no longer work you can do your own search. Oh, one last note on this. If you think or know your device has been stolen don't try to retrieve it on your own. You can locate the device but give this information to the police or other law enforcement and let them do the retrieval.

<https://support.microsoft.com/en-us/account-billing/find-and-lock-a-lost-windows-device-890bf25e-b8ba-d3fe-8253-e98a12f26316> Find and lock a lost Windows device

<https://support.apple.com/en-us/HT210515> Use the Find My app to locate a missing Apple device

<https://support.google.com/android/answer/6160491> - Find, lock, or erase a lost Android device

Practice safe computing

Practicing safe computing with mobile devices is similar to what you should do with your home computer but has some special twists. With mobile devices safe computing includes:

1. **Downloading and installing apps.** iPhones are fairly well protected by Apple, which tightly controls the apps that can be distributed through their official channel. In the past Android phones were easier targets for hackers and even innocent looking apps, like several of the flashlight apps, have been found to carry malware. So, just as you should be careful and do your due diligence before loading programs on your PC, you should take the same care when loading apps on your phone. If you have an Android phone and load apps from the Google Play store, there's some assurance that GMS will check the apps. But if you load apps from other sites, you shouldn't just assume it's safe. Do a little research on the Internet before loading any app, and make sure that it's considered safe.
2. **Giving apps privileges.** Take care with the privileges you grant to any applications you install. It's easy to say "yes" and allow an app access to everything it asks for during the install, but once again you should do your due diligence and take a close look at what you're giving away to each app.

3. **Being careful connecting to wireless networks.** We've talked about this before, but it can be tempting to connect to free wireless when you're travelling or shopping, or anywhere away from home or work. The problem is knowing whether the free wireless is a legitimate service, or something setup by an attacker to capture network traffic from unsuspecting users.
4. **Being careful with Bluetooth connections.** Much like wireless connections, you need to be careful when using Bluetooth (or any protocol) to connect to another device.
5. **Avoid using tiny URLs and QR codes.** These are items that make it quicker to connect to web sites, wireless networks, or other resources. They make connecting simpler, but they can also present a security risk. You've learned about the huge risk associated with visiting unknown web sites, and how simply opening a web page can allow an attacker to download and run malicious code on your device. However, URLs can be long and hard to type, so a few different systems have been developed to make them easier to use. One of these systems known as Tiny URLs⁶, provides a way to substitute short URLs for longer ones. Another system, known as QR codes, provides a way to scan an image which will then map to a URL. QR stands for Quick Response, and the system itself has been appropriately described as bar codes on steroids. QR codes are widely used with cell phones and other mobile devices equipped with a camera and make it possible to connect to a web site without typing anything. So, even though tiny URLs and QR codes can make life easier, they also hide the information you typically use to determine whether a resource is secure or not. You'll gain experience using QR codes, and see the potential risks associated with using them in one of the assignments for this section.

⁶ <https://tinyurl.com/app>

Ways to Check Your Comprehension

The test over this chapter won't be for a few weeks, so I suggest that you use the review questions at the end of the chapter to check your comprehension. I don't have the review questions loaded in Canvas, so you'll have to just read them and figure out your answers on your own. Or you could try and connect with some other students in the class and drill each other using these questions.

The material in this section will be included in Test 2, which isn't due for a few weeks. If you look in the Test 2 Canvas Module you'll see it contains a link to a Practice Test. You can take the Practice Test as few or as many times as you want. You're not required to take the practice test, but it's also a good way to check your comprehension and prepare for the "real" test.

The Activities for This Section

There are two sets of activities for this section, the required hands-on assignments, and a couple of optional assignments.

Required Hands-On Projects Homework

The required homework for this section consists of two hands-on projects from the book. You need to complete Hands-On Projects **5-1 Creating and Using QR Codes** and **5-2 Using Software to Locate a Missing Laptop**.

5-1 Provides you with experience using QR codes and demonstrates one of the security conundrums you face when using QR codes or tiny URLs. Note that the instructions in the book won't work as the web sites have changed. I've made a video that you can use to help you finish the project.

5-2 provides you with experience in locating missing devices. It requires that you install some software. Do this assignment on the CBC Cloud VM if you don't want to do this on your

personal computer. Also, be aware that when the alarm sounds it can be **VERY LOUD**. If you do this on your home computer you should probably take appropriate steps to ensure that it doesn't disturb anyone else and get you in trouble with other students, or your family members, or your pets. And once again, you won't be able to follow the exact steps in the book as the web site interface has changed. If you can't figure out where to click try watching the video I made to help you finish the project.

Read the following notes carefully, as they explain exactly what you need to submit to receive credit.

Before submitting your work, add all of the information for your submission into a single document. Make sure that this document has the proper header information (your name, project number, date) and well as the project and step number for each item in the document.

You will have to submit screenshots. If you need help creating a screen shot there are many videos on YouTube that will provide further instruction and details. Do NOT take a picture of your screen with your camera/phone.

What to submit for Project 5-1:

- Answer the questions in steps 6, 17 and 23.
- Make screenshots after steps 3, 9, and 20.

What to submit for Project 5-2:

- Answer the questions in steps 13, 14, 21 and 23.
- Make screenshots after steps 13, 17 and 23.

Optional Activities

There are two optional activities for this section. The first is to do a security check up on your phone, and the second is to find and check the security on your home smart devices. These activities are completely optional. There is nothing to turn in and you will not be graded on any of this work. However, I think these tasks are worth your time as they will help you check the security on your personal mobile and smart devices.

Optional Activity 1 - Mobile Phone Security Checkup

There's the obvious reasons why I think it's important that you check your phone's security, but if you have an Android that uses Google Mobile Services it's also important that you check to see what you're giving away through GMS. I don't own an iPhone, but I assume that the same type of thing happens in the Apple universe.

Android

If you have an Android phone I suggest you start by reading the following articles and following their suggestions. If these web sites aren't available, you can do an Internet search for something like "android security checkup".

<https://www.computerworld.com/article/3012630/android-security-checkup.html>

<https://www.computerworld.com/article/3268079/android-security-settings.html>

iPhone

If you own an iPhone ... well, I feel sorry for you LOL. But you might run through the checks specified in the following articles. . If these web sites aren't available, you can do an Internet search for something like "iPhone security checkup".

<https://support.apple.com/guide/security/welcome/web>

<https://www.fastcompany.com/90254589/use-these-11-critical-iphone-privacy-and-security-settings-right-now>

Optional Activity 2 - Find and Secure Smart Devices

Another task I think you should do is to find all your smart devices, and devices connected to your wireless network. Once you find all of the devices, you should verify that you have done the basic security steps of installing the latest updates and changing the administrative password from the factory default. Oh, and before we go any further, I need to provide a disclaimer. I'm definitely a novice when it comes to dealing with smart devices and dealing with Bluetooth. I can do the basic tasks like pairing devices with Bluetooth, but I've struggled to configure the few smart devices we own. So, if you have questions or need help with your devices, I most likely will be unable to provide any meaningful assistance. The only thing I'll be able to do is provide the age old wisdom I learned as a young Padawan, which is RTFM or "read the fine manual". :) All joking aside, this is actually decent advice as in most cases the setup procedures are typically well documented. If you don't have the device's documentation, check at the manufacturer's website. In addition to the official documentation, I always check online for videos, as I'm just like you when it comes to learning and keeping track of (by which I mean losing) all my device manuals. That is, I often understand better if someone shows me how to do something as opposed to just reading about it. Which might seem ironic at this point, as I give you instructions to read.

In any case, here are some general instructions for accomplishing this task. Here's a link to a decent article from Lifehacker on how to go about this.

<https://lifehacker.com/how-to-take-back-control-of-your-smart-home-devices-fro-1827974017>

The specific steps for doing these tasks will vary with each device, but the general steps are as follows:

1. Enumerate your smart devices and Bluetooth devices. This is basically building a list of the devices. There are basically two categories of devices, devices that you can (or must) connect to and control directly, and those you connect to and control through a smart home platform such as Google Nest, Amazon Alexa, or Apple's HomeKit.
 - a. To see a list of the devices that are part of the Google, Amazon, or Apple home ecosystem, open the app that you use to control your Alexa, or Siri or Google Nest, or whatever hub you're using. This will include many of the smaller devices such as smart wall plugs and smart light bulbs, but also may include larger devices such as TVs etc.
 - b. To build a list of devices that you control directly, you can either:
 - Check your phone (or tablet) for the applications that control your devices. For example, if you have an application that lets you control your smart garage door opener, it means there's a really good chance that you have a smart garage door opener.
 - Check your home router to find a list of connected devices. If you can control the device from anywhere on the Internet, it means that the device has to be accessible via your home network, which means it must be connected to your home router. There are a couple of ways to do this. You can login to your router, and then find the list of connected devices. Or you can run a program or application that checks all of the IP addresses for your home network and shows any IP address that is currently assigned to a device. The following links take you to sites with Android and iPhone apps, and a Windows

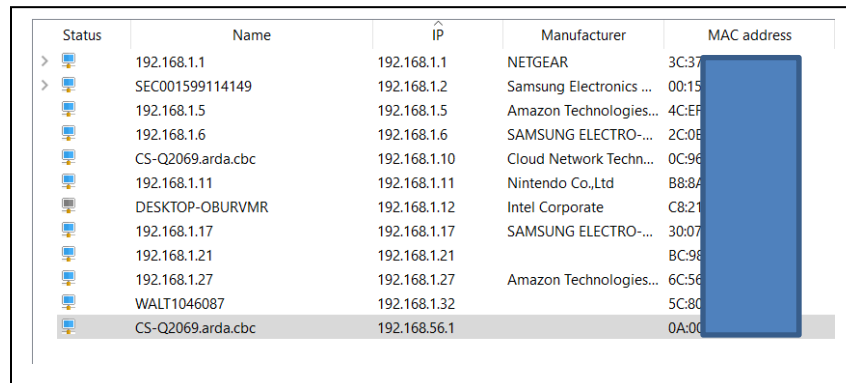
program for displaying all of the devices connected to your home network.

<https://www.groovypost.com/howto/find-ip-address-of-all-devices-home-network-fing/>

- article about apps and programs for listing all the IP addresses of devices connected to your home network.

<https://www.advanced-ip-scanner.com/> - download link for Advanced IP Scanner

In either case, you'll have a little detective work to do, as the Names assigned to each device probably won't directly identify the device. Hopefully you can look at the information in the Name and Manufacturer columns and figure out which devices are which. For example, here's a sample display from my home network. I know that some of the devices with names ending in arda.cbc are my work computers which are owned by the college, and devices from Samsung are the printer and phones, while those from Amazon and probably Echo and Echo Dots.



Status	Name	IP	Manufacturer	MAC address
>	192.168.1.1	192.168.1.1	NETGEAR	3C:37:58:...
>	SEC001599114149	192.168.1.2	Samsung Electronics ...	00:15:8D:...
	192.168.1.5	192.168.1.5	Amazon Technologies...	4C:EF:3C:...
	192.168.1.6	192.168.1.6	SAMSUNG ELECTRO-...	2C:08:90:...
	CS-Q2069.arda.cbc	192.168.1.10	Cloud Network Techn...	0C:96:00:...
	192.168.1.11	192.168.1.11	Nintendo Co.,Ltd	B8:87:98:...
	DESKTOP-OBURVMR	192.168.1.12	Intel Corporate	C8:21:8A:...
	192.168.1.17	192.168.1.17	SAMSUNG ELECTRO-...	30:07:98:...
	192.168.1.21	192.168.1.21		BC:98:4D:...
	192.168.1.27	192.168.1.27	Amazon Technologies...	6C:5E:00:...
	WALT1046087	192.168.1.32		5C:80:39:...
	CS-Q2069.arda.cbc	192.168.56.1		0A:00:27:...

-
2. For any devices that are password protected, ensure that you have changed it so that it no longer uses the default password, and that it now uses a strong password. Since each device will use its own setup program, you'll have a little work to do. You can refer to the Lifehacker article linked above for some tips and decent guidance.