Radios

This lesson is going to cover radios, and not the ones you think of when you hear the word radio. When I say radios, I'm referring to *Bluetooth, location services, NFC, cellular data, and anything else that gives off a signal.* This lesson will be broken up by each type of radio. Let's get into it!

Promotional Spot

Let's begin with *Bluetooth.* Bluetooth has allowed us to interact with devices wirelessly like never before. But it's one of the most inherently insecure technologies. *Security risks like Bluejacking, Bluesnarfing, and Bluebugging have affected every version of Bluetooth except 4.0 and onward. Even the newer versions are vulnerable to eavesdropping through the new Bluetooth Low Energy tech, and we even saw the BlueBorne vulnerability in 2017, not to mention the recent vulnerability discovered in July of this year.* These exploits can lead to tampering with sensitive data, theft of data, privacy invasion, and sometimes even more extreme issues.

As for privacy, Bluetooth is a major component of invasive technologies like contact tracing, as well as methods of tracking individuals in things like retail stores.

What can you do about this? *First, make sure you're up-to-date on your devices.* Second, utilize proper bluetooth passwords on devices requiring them, *so don't use the default 0s. Third, leave Bluetooth off as much as possible; it doesn't need to be on all day.* Lastly, don't use it at all if possible. **** show wire and phone **** If you have the option to go wired--go wired!

The next radio i*s GPS.* GPS is great for navigation and other situations that require your location, *but there are concerns, especially with recent location-based features from Google and Apple.*

Location data can be used in ways you may not intend, *like tracking travel patterns, targeting you for marketing, and location tracking itself is another data point used to build a comprehensive record on your life. We've seen how Uber handled this back in section 3, Apple got in trouble some time ago for storing GPS data in an unencrypted file, and if you've enabled Google location history--go look for yourself at how extensive this can be.* As of today, there have been no widespread security breaches involving location data, but that doesn't mean you shouldn't be concerned. A breach could happen any day, and we don't

know if companies like *Snapchat or Google* are using your location for ad targeting and other misuses.

Additionally, *certain apps and programs may publicly reveal your location without your knowledge, opening up the door for stalkers.* The last concern is surveillance. Law enforcement agencies can obtain location data through various methods, some as simple as a court order. *According to a report by the ACLU, law enforcement agents can track innocent people who happened to be in the vicinity of a crime, so this can impact people who do nothing wrong*--and they aren't alerted when their data is snagged. This doesn't even include the fact that when your data is snagged by law enforcement, it most likely reveals sensitive destinations: *like medical clinics, religious institutions, courts, political rallies, or union meetings;* all things intended to be private.

So...don't record the data in the first place! *First, only grant apps and programs the permission to view your location if it's required. Calculators don't need your location, and neither does Snapchat. If there's an app that requires a location to function, like Tinder, you can try to fake your location on Android using a location spoofer. Set the location to a random area near you and keep it there at all times.* iPhones don't allow location spoofing unless you jailbreak; *there are great tweaks if you do decide to go this route.* Second, opt out of any location-based tracking and/or personalization on your device, *Google and Apple both do this.* Third, install a *custom ROM like GrapheneOS on Android devices* to cut out Google tracking altogether. Fourth, make sure to *disable location sharing in apps like Snapchat and Find my Friends.* Fifth, completely disable location services, unless you explicitly need to use them. The last (and very extreme) thing you can do is *physically remove the GPS chip in your device.* This isn't always possible and every device is different, but the option is there for people willing to go those lengths. It is important to mention that according to a study by Berkeley, 99.6% of the times that Android accesses location data, the icon isn't visible to the user because the chip isn't used for location tracking, your location can be tracked from your IP address, MAC Address, nearby WiFi networks, and other clever ways of bypassing Android permissions, there's a great talk I'd recommend you watch covering this.

NFC is the next radio. NFC is used when you make a payment at a store with your phone; it's also used for things like data transfer between two devices . Apple devices also have NFC, *it was just rebranded as Apple Pay.* Let's start with the positives...

First, *NFC has a short range, requiring devices to be close together, limiting the chance of someone eavesdropping, corrupting, or manipulating the connection. You can read more about these attacks on this webpage.* Second, NFC allows you to use secure channels, where information is encrypted, and only authorized

devices can decode it. Third, NFC is arguably safer than using a credit card. If you lose your credit card, someone has access to some of your personal information. But, if you lose your phone and it's properly protected, your information is safe. BUT (there's always a but) NFC is not perfect.

Google, Sprint and other companies have stated they do NOT intend to generate revenue by taking cuts from NFC transactions. *Instead, they hope to use NFC to provide highly personalized ads and coupons. Likewise, retailers and digital signage companies are considering ways to leverage NFC to deliver marketing tailored to a user's location and preferences.* To top it all off, Google and Apple's involvement in payments means your shopping habits are now tied to your Google and Apple account.

What do we do? *First, disable NFC as often as possible, only enabling it when it's needed.* Second, ensure companies you're doing business with use NFC secure channels to properly secure your transactions. The final option is to leave NFC disabled at all times, never using it for anything--this isn't terribly extreme as of today.

Now before I reveal the most intrusive and undisclosed form of radio tracking, let's cover some other quick little things to watch for...

- *Google Nearby is creepy, and it should be clear why I recommend disabling this.*

- *Lastly, don't forget to lock your SIM card. This will ensure anyone who gets your SIM will need a password in order to start using your cell service, just a tip :)*

Alright, what's the final radio you need to watch out for? You may be surprised to hear this, but it's *wifi and cellular radios.* First, *firms like Google and Apple use customer data to compile large databases of cell towers and wifi access points, but this is the least of our worries.*

Simply leaving wifi enabled on your laptop or phone can be detrimental to your privacy. *Snowden revealed that the CSEC can identify travelers passing through Canadian airports by capturing their MAC address.* This type of technology can be used anywhere at any time without your knowledge.

To dive deeper, your mobile device connects to a series of cellular towers. *The closest one handles calls, texts, and internet sessions. As you move, your phone pings other towers to make sure you're still using the best tower. Here's the problem, the data logged from pinging multiple cell towers can geographically*

pinpoint a user using triangulation techniques from 3 or more cell towers--with extreme accuracy; this was actually the technique used to catch Pat Barbaro in an australian mafia investigation. Not only are you trusting your cellular provider to properly manage this data, but law enforcement can, and do request this information.

If this wasn't alarming enough, *law enforcement is known to create devices that pretend to be cellular base stations that intercept voice and text messages when your phone mistakenly connects to it. These are typically used at large rallies, allowing law enforcement to later identify who was attending the rally.*

What can we do? *First, disable wifi as much as possible to avoid any tracking done when you're searching for networks.* Once you're inside a location with wifi, then turn it on. Second, and I know it's extreme, *try to keep your phone on airplane mode as much as possible, or utilize a faraday bag.* It'll decrease the amount of tracking done by cell towers, improve your security and privacy, make you less reliant on technology, and it'll improve your battery life. What I like to do is keep my phone on airplane mode and re-enable data every 30 minutes or so to check for messages or notifications. If this isn't enough for you, *a step up is to leave your phone at home, it can't track where you're going if it's not with you--although this is getting into the extreme realm.* The last thing you can implement is a burner phone, which is legal in the US, but not in every country. Burner phones are a very private option since they don't require a name, address, social security number, or a revealing payment method. Keep in mind that walking into a store means there will likely be cameras, and most forms of transportation are tracked as well. The inconvenience of getting through these problems is astronomical, but you will have close to an anonymous phone if you purchase it properly. This is definitely not for everybody, but the option is there for people who need the absolute highest privacy.

Queue Outro Promos

To summarize the lesson, every radio you use creates a new potential security exploit, or a potential leak of information about your personal data. I hope this lesson has taught you to think differently about radios, and I'll see you in the next lesson *discussing Device Separation.* Thank you for watching.