COMP210 Assignment 1
Cameron McLennan
8168187

Mobile phones in 2017 are everywhere, with most people having at least one mobile phone. They have become an item that one would bring anywhere with them, just as they would their keys or wallet. Some even feel lost without their cellphone as it is essentially an extension of some peoples arms and is how they communicate with the world.

Mobile phone technology has come a long way over the past few years, with phones becoming more powerful and being able to do more as manufacturers cram more and more into them as technology shrinks. There are two main forms of how a phone is able to communicate with the outside world that people use daily. These being through a cellular connection, and through the use of Wi-Fi connection. With more and more cellular network providers fighting it out for majority control of users on their network, prices for data to use on cellular networks have been coming down, and there is even offers for students in New Zealand to get free data if they use Spark as their cellular provider (Spark, 2017). As a student, I pay Spark $29 per month and have got the student deal, and I also acquired a 1GB bundle to use on Facebook, Twitter and Spotify. All told, I have 2GB of data to use on anything, and 3GB of data total. Along with the data, I also have unlimited calls to spark mobile phones and landlines through the student offer, unlimited SMS messages and 200 calling minutes to anyone from the $29 bundle. Also included in the bundle is Spotify Premium, which now costs $15 NZD. So for being a student and a loyal customer to Spark, my $29 has gone quite far. No other Telecommunications provider can offer quite this much at this price. Now, more than ever, people are more and more connected up, meaning if you are wanting to access someone or some information, there will be an easy way to get at it. I could keep my mobile data on all day and not worry that I will run out of it, it's my battery that I would worry about running out of.

Portable communication was the goal of the cellphone or "mobile phone", and given that this was the whole idea behind the original design, it only makes sense that cellular commination is kept. If there is no cellular connection in the device, it is not a cellphone, as cellphone is merely a contraction of cellular combined with phone. A cellphone will use a radio waves to communicate, using the radio wave to send data to the nearest cell tower, and from there through a network of towers to the receiving device (Wang, 2014). The goal of the cellphone is to send the weakest signal it can whist maintaining decent connection in order to preserve battery life as if it has poor connection, it has to work harder and send a stronger signal, thus reducing battery life faster than if the device were to have a strong connection (Wang, 2014). Modern smart phones have internal antenna for sending and receiving these radio waves, where-as older phones usually have an external antenna, and on some phones you could extend it out to provide better reception. Problems occur with modern smartphones and these antenna as a circuit board inside the phone, or even the materials that the phone is built out of can impact reception. There was an issue with the iPhone 4 which was coined "iPhone death grip" by the media ("iPhone 4 Death Grip", 2010). This issue was the result of grasping the phone during a phone call in such a way that reception could drop from a maximum strength five bars to a one bar signal in a matter of seconds. When a user is on a phone call with the phone up to their head, their phone absorbs a good amount of the radio waves, meaning the signal has to be propagated from other points about the phone, such as the back or edges. If one were to cover up the phone with their hand and place it against their head, there is a very limited amount of ways that the antenna can emit radio

waves to cell towers, leading to a potential drop in signal if the antenna is not placed correctly in the phone.

Given that it is harder to completely cover phones these days as they are becoming larger and larger and materials are moving towards the likes of glass which allow easy sending and receiving of radio waves, instances of the “death grip” should be a thing of the past. The SMS portion of the cellular network can be either utilized or exploited by people who wish to track a mobile phone user, all those who wish to track someone have to do is send what is known as a “silent SMS”. This sends an SMS to a desired number, and as a result they will receive notification as to whether or not the device is on. Wireless carriers or the likes of the police can use the silent SMS to get a rough idea of the user’s device location based on data received by a cell tower. The end user has no idea that they have received a text message, but if they did get a message it would show up blank ("Did you know that "silent" text messages can be used to track your whereabouts?", 2014)(Wolfe, 2017).

Wi-Fi has become an accepted fact of life as it is the most common form of connection to the outside world for a lot of people in this modern day and age, and some people will choose to not use SMS messaging or calling and will opt to do everything through the internet. Internet has gotten faster and cheaper over the years, and it is now easier than ever to get connected online. All smart devices these days have some form of internet connectivity, whether it be through the device itself or a companion device. An example of this could be smart watches using mobile phones to connect back to and communicate through. Wi-Fi has easily become the most popular feature on a cell phone, with it providing quick access to people’s music, social feeds, weather, news, and many more resources now available on the internet. The device connects to the modem or router, then any data that is sent through to the ISP is then redirected to where it needs to go. The highest tier of smartphones these days are offering the best in Wi-Fi technology, which is currently the 802.11ac wireless standard. This standard is designed to utilize both the 2.4ghz band and the 5ghz bands of Wi-Fi. If the device has the ac standard, it has backwards compatibility with previous standards. 802.11ac allows better data throughput due to the dual band setup but costs more to produce due to requiring the two bands, and is still prone to interference on the 2.4ghz band as many things operate on that band ("Wi-Fi Standards 802.11a/b/g/n vs. 802.11ac: Which is Best?", 2014).

Wi-Fi would have to be one of the biggest weakness in the current crop of phones as a majority of smartphones will have Wi-Fi and many people use Wi-Fi each day, and it wouldn’t be hard to access a phone via the Wi-Fi connection should one want to, and getting data off of the phone would be easy via the Wi-Fi connection as Wi-Fi is fast and no one would notice if their phone was being harvested of data or having data loaded if done correctly. Even intercepting data and gathering it when it is in transit wouldn’t be hard for people who know what they are doing, and this would be easier as they wouldn’t need to load anything onto the device or get access to the device The weakness with Wi-Fi on phones is unlike desktop computers and laptop computers, phones do not come with many systems to warn about viruses or malicious data. If someone were to accidentally download an app that wasn’t from the respective operating system application store and get it to run, it could execute malicious code which could harvest all data on the phone, such as contacts, SMS conversations, stored passwords, and even take control of sensors on the device with the proper know how.

Bluetooth has been around since the mid 1990s, and is a form of wireless data exchange using UHF radio waves in between the 2.4-2.5ghz spectrum. Bluetooth in the modern day is used mostly to pair with peripheral devices, such as speakers, headphones or game controllers to enhance interaction with the cell phone (Bourque, 2014). Class 3 Bluetooth radios have a range of around 1m, class 2 radios have a range of around 10m, and class 1 has a range of around 100m. The Bluetooth chips in phones is usually a class 2 chip, but certain eternal USB Bluetooth adapters can have ranges up to 1km, but this is usually only under the right conditions. Currently the latest Bluetooth version is 5, with a max data transfer of up to around 50 Megabits per second and a range of around 240 meters ("How it works | Bluetooth Technology Website", n.d.). Bluetooth range fades when trying to go through walls or even the human body, so the 10m range on mobile devices is usually a best case scenario, with real world ranges being less than this, sometimes maybe sub 2m under poor conditions.

Bluetooth back in the late 2000s and up until around 2013 was the most common way to transfer data between cell phones. There was not overlord application hub like Apple and Google have with their app stores, people downloaded games and music and the likes off of the internet from sketchy file sharing sites, and then could easily give them to their friends via Bluetooth. These files could have contained malicious code that could have messed with the phone that it was going on to, or end up costing the user a lot of money if it could somehow start purchasing things like ringtones off the internet. Phones were a lot harder to navigate when there was a number pad, small screens and what would now be looked at as a sub-par, yet functional, GUI. Trying to fix a rogue application would have been a nightmare and because people would trust their friends, Bluetooth would have been the best way to get a malicious application or code onto many devices.

NFC, or Near Field Communication, is designed for a similar purpose to Bluetooth, file sharing. It works by two NFC enabled devices touching together, or at least getting close together. NFC was actually an offshoot of RFID, or Radio Frequency Identification. It works off of the idea of electromagnetic induction to transmit data over a short distance. This feature allows data to be transferred between NFC enabled devices or NFC readers. There are three main modes that people will use. These are peer to peer data swap mode for data transfer between devices, and a read/write mode to read passive NFC enabled tags, and a card emulation mode (Egan, 2015). Just like with cards that can utilize things like PayWave that can be exploited, this could happen to phones as well. Usually there is a two-step verification that requires a user to input a password or use a fingerprint or other security feature to authorize payment, but if there isn't and people have the knowhow to make a reader, the phone users card details could be at risk. This also means that a user's credit card details are stored on their phone, making their phone a much larger target for thieves (Faulkner, 2015).

Modern day cellphone contains many sensors, with manufacturers trying to fit as many sensors and features into the phone as possible ("Sensors - Mobile terms glossary - GSMArena.com", n.d.). The only problem with more sensors is that there is more weakness in the device security, with ways to exploit these sensors for malicious use (Wolfe, 2017). The original main sensor on a mobile device would have been the microphone, as the main idea of the cell phone was for audio communication. As the cell phone evolved into the smart phone, the features that people on a daily basis has increased. People are using their phone

to tell them where to go, how many steps they use, their heart rate and recently smartphone users have had more options of security for their devices ("Sensors and Cellphones", n.d.).

The image sensor, or camera, is the part of a phone which takes still images and records video ("Sensors - Mobile terms glossary - GSMArena.com", n.d.). This is the most noticeable sensor on the phone as it is usually on both sides of a device and is now days a part of the phone that will stop it lying flat on its back as there has been a trend towards the "camera hump" in order to get the device as small as possible for the consumer. All modern smartphones will include at least one camera which will be located on the back of the phone. A lot of smart phones these days are including a second camera, located on the front of the phone. The camera on the rear of the phone is designed for taking pictures or videos of items behind the phone, such as landscapes, events, or even notes. The front camera is designed mainly to see the device user, and can be used to unlock the device, take pictures of one's self which is now known as a "selfie", and can be used to take pictures of people who try to get into your phone. The camera on a phone can be used for both good and bad. The good use would be as mentioned previously, the phone could take pictures of people who try to get into your phone and if the phone was stolen, the photos could get sent back to you in order to help solve who has your phone. The malicious exploit for the camera feature of the phone would be that someone could have your phone taking pictures of its surroundings to get a visual representation the device's position, and if geo tagging is enabled on the pictures then the location of each picture will be able to be found as well, thereby enabling them to track someone using the camera.

The microphone is an essential part of a cell phone as it is how audio is captured to be sent via Wi-Fi or cellular networks to someone else ("Sensors - Mobile terms glossary - GSMArena.com", n.d.). There will not be a cell phone around without a microphone of some form as the original idea of a cellular phone is to utilize cell towers to transmit voice to someone on the other end. The microphone can be a very powerful, if not one of the most powerful sensors on a mobile device to get a hold of. There are ways of being able to turn a cellphone into a listening device. If a call comes in to the phone that is to be the listening device, the phone can silently answer the call and start transmitting any audio that happens to be in the room at the time. This is a powerful tool in situations such as negotiations, because if you know what the other side of the negotiation are wanting and going to offer, you have a lot of bargaining power when it comes time to discuss terms of said negotiation (Wolfe, 2017).

The accelerometer is designed to determine the current orientation of the cellphone in three axes in space, the X, Y, and Z axes ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). While measuring tilt or orientation, it also measures motion. The most common use for this is for screen rotation, so that if one rotates their device from portrait to landscape, the applications (assuming compatible) will rotate accordingly. Another way the accelerometer can be used is flipping the device over to mute incoming calls or music. One potential exploit that someone could do with accelerometer data is being able to know if the user is actively on their mobile device or not. Depending on what data the accelerometer collects and is able to send, the receiver of the data could see if the phone is in the pocket of a user or in their hands due to the different orientation that a device will be in if the user is

actively on it, compared to if it is sitting in their pocket or lying face down on a surface, but not much more.

The gyroscope does a similar job to the accelerometer, but tracks rotation or twisting motions ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). This adds to motion depth when playing mobile games. The data from this sensor wouldn't have much malicious use as not much can be done with it, all that this sensor does is detect the rotation or twisting action of the device.

The Hall sensor has a more specialized role, and it is to detect magnetic fields close to the phone. This doesn't have many uses besides turning the screen on and off when a flip case is on the phone that is designed with the intent of turning on and off the screen when the case is opened and closed respectively ("What is the use of Hall effect sensors in smartphones?", 2015) ("how many different sensors are available inside a smartphone?", 2015). This sensor is harder to exploit as all it really does is sense if the cover of a phone is open or closed, and turns the screen on or off respectively. All it would be able to tell the exploiter would be whether or not the device has a flip case covering the phone and that it is waiting for the magnetic field to be changed to open to turn the phones screen on.

The magnetometer is a sensor that is designed to provide the cell phone with its orientation in relation to the magnetic field of earth ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). It is the basis of compass and navigation applications as the device knows which way is north, and can adjust the view to your current physical direction. This is a sensor that contains data which could be useful for locating someone's current direction, as with a bit of a GUI on top of this sensor data, you will have a compass. So this sensor could be used to locate someone's direction, and paired with the GPS, it could be able to be used to track someone's movement.

The proximity sensor is designed to detect if something is in front of the device and react accordingly ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). Most of the time it won't be doing much, but this sensor is important when talking on the phone. When someone is talking on their phone, with the phone up to their ear, the proximity sensor will turn off the screen in order to both preserve battery life and to disable touch on the screen, so that the person with the phone to their wont accidentally hit any buttons. This sensor really doesn't have much of a weakness that can be exploited as the only thing that it is used for is to turn the screen on and off depending on if the conditions are met, these being something blocking the sensor AND being in an application that has access and utilizes the sensor.

The light sensor is designed to measure ambient light levels and try to adjust the screen brightness in order to give the user a better experience with their device usability in the real world ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). This could be utilized to see if the user is surrounded by darkness or light, and if this data was used with the data from the GPS and the accelerometer then it could be used to locate where in a building someone is if they were using their phone. The worst thing that someone could do would if they got access to

this sensor is trick it into either turning the screen brightness all the way up, draining the battery and potentially damaging the screen if left on long enough, or always having the screen as dark as it can go. This can be mitigated as all a user has to do is disable automatic brightness in their device and the sensor no longer has to control the screen brightness.

The barometer sensor is designed to gauge the height that the phone is above sea level via measuring atmospheric pressures ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). This sensor could be exploited in a way to determine roughly what floor in a building someone is on, or if they are onboard an aircraft. This would be useful to use with the GPS to find where someone is, and how high up they are, relative to sea level. It is a more useful sensor to exploit in comparison to other sensors, such as the heart rate sensor on some devices as not a lot can be done with the heart rate, and it isn't always used, but the barometer sensor is always used for telemetry and when a user would be wanting to use a GPS application.

The thermometer is a sensor designed to measure the temperature of an area, and in the case of a smartphone, the temperature sensor is able to measure either the ambient temperature or the temperature of a part in the phone, usually the battery ("Sensors - Mobile terms glossary - GSMArena.com", n.d.) ("how many different sensors are available inside a smartphone?", 2015). The primary reason to have a thermometer sensor in a cell phone these days will be to protect the device and the user from an overheating battery, as batteries can be dangerous if they get too hot. Some phones have thermometer sensors that are designed to measure ambient temperatures, but these temperature sensors could be skewed somewhat due to heat soak from the users hands or body, and heat from the device itself. If someone got access to the sensor and wished to annoy people, they could have the battery temperature sensor always say that the battery is too hot, and will constantly turn the device off when the user attempts to turn it on. IF they wished to put people in potential danger, could also give it a false reading so that the sensor read the same temperature, regardless of actual battery temperature. This could potentially result in damage to the phone and the user if there was a battery temperature issue.

The pedometer sensor is a health orientated sensor designed to count how many steps you take in one day (Woodford, 2016) ("how many different sensors are available inside a smartphone?", 2015). These sensors aren't the most accurate as it can interpret certain movements as footsteps, which can then in turn result in an incorrect reading. In modern phones they are starting to be found to use an accelerometer to measure the change in angles when the user takes a step, as humans tend to have a predictable step pattern. There is usually two or three accelerometers which are tasked with measuring this (Woodford, 2016). This sensor is another sensor which wouldn't have much of a malicious use, but being able to see roughly how far someone has walked in a day could be good for some to know. This data could also be sold to companies who are marketing sporting or fitness goods, thus allowing targeted marketing towards the user of this device. Pairing this sensor with the GPS is what builds the underlying foundation for tracking walking or running paths taken.

The heart rate sensor is another form of a health monitoring sensor which monitors a user's heart rate when their finger covers the sensor ("how many different sensors are

available inside a smartphone?", 2015). It utilizes pulses of light to measure the users pulse when the sensor is covered. The data is usually sent back to an application that interprets and potentially tracks your heart rate if you do it regularly enough. There isn't really a way that one could exploit the heart rate monitor for malicious gains, as it would be one of the least used sensors, and even then there is not much, if anything, that could be done with the heartrate of someone.

The fingerprint scanner sensor is held in the home button of a phone or on the back, roughly where one's index finger would naturally sit ("how many different sensors are available inside a smartphone?", 2015). Popular way to protect one's mobile device as no one can see what your password is and replicate it – isn't fool proof though although effort is required to get access to someone's phone via this method. The method of actually getting the fingerprint as a form of security is rather simple now days. The fingerprint is scanned, the grooves in the print are analysed and converted into a unique numerical code, and then the code is either stored as a reference code or the newly scanned code is compared to a current reference code. If they match, the area in which the fingerprint was protecting is now unlocked to the user (Wolfe, 2017). Fingerprint scanners can be beaten though, but it is a somewhat laborious task. It requires getting their fingerprint that they use to unlock the device, casting it in some sort of conductive material and then still having access to their device to unlock it (Wolfe, 2017). If one was to exploit this sensor, they could get access to purchase items off of the phone if the user has cards linked to the phone that require some form of authentication, which could be the finger print. If people had hidden files on the device, protected via fingerprint, then they would also be vulnerable.

The iris scanner is a newer sensor on the current crop of smartphones, and is a new method to protect one's device or contents on said device ("How the Galaxy Note 7 iris scanner works", 2016). The scanner sends an infrared light beam at the users eye to capture the iris. Once this image is within the phone, the software turns this iris pattern into code. This code is then stored as the reference for a user. Each subsequent time that it is used, the code for the unique iris is generated based off the map of the iris, and is compared to the reference key. If the keys match, it unlocks the device ("How the Galaxy Note 7 iris scanner works", 2016)(Wolfe, 2017). This could be thwarted if it has no liveness test, as iris scanners in the past have been thwarted through the use of a high resolution photograph, as if the photo is good enough the iris's topography can be seen well enough by the scanner.

The evolution of the cellphone into the smartphone due to consumers wanting more and more from their portable devices has left the user with something in their pocket worth a lot to the right people. There is so much that can be taken off a smartphone that people load onto them. People are now easier than ever to find as they will more often than not have a device on them packed with sensors that can be utilized to locate them, whether it be an emergency or not. Their viewing habits and application use could be valuable to advertising companies, giving people incentive to want to harvest as much data off of mobile phones as possible. This is similar to what companies bury in their terms of service agreements and why people may get targeted ads on their social media feeds as companies know that they can get money by selling user data, so why not try tap into the goldmine that is inside of a majority of people's pockets. The best thing that users can do is to be careful what sites they visit, what applications they download and what they store on their device.

References

Bourque, B. (2014). *This is how Bluetooth works, and no, it's not by magic*. *Digital Trends*. Retrieved 13 April 2017, from http://www.digitaltrends.com/mobile/how-does-bluetooth-work/

Did you know that "silent" text messages can be used to track your whereabouts?. (2014). *Phone Arena*. Retrieved 8 April 2017, from http://www.phonearena.com/news/Did-you-know-that-silent-text-messages-can-be-used-to-track-your-whereabouts_id53557

Egan,. (2015). *How to use NFC on your smartphone to do useful things*. *PC Advisor*. Retrieved 10 April 2017, from http://www.pcadvisor.co.uk/how-to/mobile-phone/what-is-nfc-how-nfc-works-what-it-does-3472879/

Faulkner, C. (2015). *What is NFC? Everything you need to know*. *TechRadar*. Retrieved 13 April 2017, from http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410

How do fingerprint scanners work. (2017). *Explain that Stuff*. Retrieved 5 April 2017, from http://www.explainthatstuff.com/fingerprintscanners.html

How it works | Bluetooth Technology Website. *Bluetooth.com*. Retrieved 13 April 2017, from https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works

how many different sensors are available inside a smartphone?. (2015). *Quora*. Retrieved 5 April 2017, from https://www.quora.com/how-many-different-sensors-are-available-inside-a-smartphone

How the Galaxy Note 7 iris scanner works. (2016). *Phone Arena*. Retrieved 6 April 2017, from http://www.phonearena.com/news/Here-is-how-the-Galaxy-Note-7-iris-scanner-works_id82854

iPhone 4 Death Grip. (2010). *Know Your Meme*. Retrieved 5 April 2017, from http://knowyourmeme.com/memes/events/iphone-4-death-grip

Khandelwal, S. (2015). *Hacker Finds a Simple Way to Fool IRIS Biometric Security Systems*. *The Hacker News*. Retrieved 7 April 2017, from http://thehackernews.com/2015/03/iris-biometric-security-bypass.html

Miles, S. (2017). *Samsung Galaxy S5 heart rate monitor vs iPhone 5S heart rate monitor: What's the difference? - Pocket-lint*. *Pocket-lint.com*. Retrieved 8 April 2017, from http://www.pocket-lint.com/news/127656-samsung-galaxy-s5-heart-rate-monitor-vs-iphone-5s-heart-rate-monitor-what-s-the-difference

Prepaid Mobile Plans & Sim Cards - Mobile Plans | Spark NZ. (2017). *Spark.co.nz*. Retrieved 4 April 2017, from https://www.spark.co.nz/shop/mobile/prepaid.html

Sensors - Mobile terms glossary - GSMArena.com. *Gsmarena.com*. Retrieved 5 April 2017, from http://www.gsmarena.com/glossary.php3?term=sensors

Sensors and Cellphones. *Stanford.edu*. Retrieved 6 April 2017, from https://web.stanford.edu/class/cs75n/Sensors.pdf

Specials, S. (2017). *Student specials | Spark NZ. Spark.co.nz*. Retrieved 4 April 2017, from https://www.spark.co.nz/shop/student-special/#student-application-form

Wang, R. (2014). *How Do Cell Phones Work?*. *Pong: Making the Case for Cell Phone Radiation Protection*. Retrieved 3 April 2017, from http://www.pongcase.com/blog/cell-phones-work/#sthash.58plMQRa.dpbs

What is the use of Hall effect sensors in smartphones?. (2015). *Quora*. Retrieved 6 April 2017, from https://www.quora.com/What-is-the-use-of-Hall-effect-sensors-in-smartphones

WiFi Standards 802.11a/b/g/n vs. 802.11ac: Which is Best?. (2014). *Semiconductorstore.com*. Retrieved 5 April 2017, from http://www.semiconductorstore.com/blog/2014/WiFi-standards-802-11a-b-g-n-vs-802-11ac-Which-is-Best/806

Wolfe, H. (2017). *COMP210 Course*. Lecture, University of Otago.

Woodford, C. (2016). *How do pedometers work?*. *Explain that Stuff*. Retrieved 7 April 2017, from http://www.explainthatstuff.com/how-pedometers-work.html