The Mobile Phone as a Surveillance Device

by
Dr. Henry B. Wolfe

***Abstract*— Mobile phone design makes possible a number of surveillance techniques that are concentrated in the single device. More than 8 billion mobile phones are currently in use and most people who use them keep the phone with them and turned on or active at all times. This means that the phone could be used as a tracking device or as a bug or listening device with various capabilities. It can be used for email and Internet activity surveillance. It can be used to communicate with RFID devices. It can be used to take photos and to record sound and video. Access to information held on a mobile phone has the potential to reveal personal and private data. In concert, these functions provide surveillance opportunities unavailable in any other single device. This paper will survey surveillance techniques and tools, compromise vulnerabilities, and propose protective measures to mitigate the various threats to mobile phone users.**

Keywords— Malware, Triggerfish, Bluetooth slurping, IMSI Catcher, roving bug, GPS, RFID, NFC, QR codes, cryptography, surveillance

I. Introduction

Mobile phones are ubiquitous. If you do not have one you may be considered to be either unusual or a Luddite. The mobile phone is simply a small computer connected to a radio transmitter/receiver with other additional communications channels. Because of the pervasive nature of mobile phone use, this platform becomes a very attractive potential surveillance opportunity. Newer phones have additional functionality in the form of Global Position System (GPS), Radio Frequency Identification (RFID) in the form of Near Field Communication (NFC), WiFi, Bluetooth, and various sensors.

These added features open possible tracking and a variety of surveillance, harassment, and other abuse. The potential for this kind of activity is based on the prize at stake. This prize is usually proscribed by attributes such as wealth, fame, politics, criminality, etc. Attributes of the target must satisfy the attacker that the expenditure of resources and effort will provide a satisfactory outcome. The author does not advocate abolishment or abandonment of mobile phones but rather promulgates the idea of safe informed use. This paper will discuss some of the surveillance possibilities that modern mobile phones can be put to and the risks to the user.

II. Objectives

The questions addressed in this paper are:

- How can the mobile phone be used for surveillance purposes?
- How can the mobile phone user protect themselves from these risks?

Explanation of terms used within the paper

Surveillance in the context of this paper is the monitoring of communications, physical location, sensory activity, WiFi, or Internet activity of any targeted mobile phone user.

In the context of this paper, a bug (normally a covert listening device) is a technique of covertly listening to a target's communications.

Various attack models would be in play for any given issue discussed in this paper. This paper does not deal with specific reasons or justifications or legal issues surrounding the use of the mobile phone as a surveillance or attack device. It is only focused on the methods that are currently available to be used.

III. Surveillance by Governments

Governments (law enforcement, intelligence and/or other agencies) use various methods to perform surveillance on targeted individuals or organizations. The discussion does not address the lawful authority of such entities to carry out surveillance.

This paper considers several methods of surveillance based on information researched from and about western nations.

3.1 What is "Triggerfish"?

Triggerfish is a keyword used to designate technology developed by law enforcement. The FBI and other governments make use of Harris Corporation's Stingray 2 [1] to locate a mobile phone even when it is not being used to make a call. This is a sophisticated and expensive piece of equipment (US$188,452) and unless other attackers are well resourced will be unlikely to be used by them. Triggerfish enables tracking and monitoring of a specific mobile phone, can activate the mobile phone's microphone (also known as a "roving bug"), is portable (a laptop hooked up to a Harris Stingray II with an AmberJack phased array direction finding antenna), poses as a base station within a given cell, and operates in the 800 – 1900 MHz bands (GSM, DCS, CDMA - mobile systems). However, the principles of simulating a cell base station are well known and the application of these principles enables non-government attackers to intercept mobile phone conversations as well.

3.2 Tracking

Mobile phone service providers manage a communications network. Part of that administration is network traffic analysis. This allows a service provider to upgrade bandwidth and other elements of their network before a cell's communication saturation threshold is reached. These providers use cell tower triangulation for this purpose and record every phone's location

when polled. The information is recorded for use in traffic analysis and is a necessary management tool.

Newer phones have GPS functionality and that makes tracking much easier and more accurate as well. Both offer the potential for a perpetrator to track the current, and potentially historical, location of any targeted mobile phone. That information may be vital for locating someone in an emergency and the requirement for this capability has been legislated in some jurisdictions – such as in the USA.

On the other hand, this information could be used to prove where the holder of the phone was at any given time. Normally this information is not available to the public. It must be obtained by providing the service provider with a warrant issued by an official judicial authority after the presentation of evidence of probable cause that justifies the issuance of the warrant by that judicial authority. Triggerfish [2, 3] allows for real time location tracking which does not require any contact with the service provider.

3.3 Bugging

Mobile phones can be configured to become a bug (listening device). Triggerfish technology has the ability to activate the mobile phone's microphone and to be able to listen to whatever it picks up – from wherever the mobile phone is located. This is not the only way that a mobile phone can be turned into a bug. The Internet provides many applications that can provide the same functionality and do so from wherever the perpetrator is located – virtually anywhere in the world. These will be addressed in more detail later in the paper. Mobile phones can also be configured by their owner to act as a bug and left to listen to whatever sound may be heard in the immediate vicinity. That requires no special devices or software.

3.4 Governmental IT Intrusion and Remote Monitoring Activities

FinFisher [44] is a suite of surveillance tools produced by Gamma International (a German company) which is a part of the UK-based Gamma Group. These are in use, currently in 36 countries around the world, primarily to collect Internet traffic. However, one specific non-Internet tool in the Gamma suite is called FinSpy Mobile. From the Gamma promotional material it claims that FinSpy Mobile is able to:

- Provide covert communications with Headquarters (the master)
- Record common communications like voice calls, SMS/MMS, and emails
- Live surveillance through silent calls
- File downloads (contacts, calendar, pictures, and files)
- Country tracing of target (GPS and cell ID)
- Full recording of all Blackberry Messenger communications
- Support most common Operating Systems: Windows Mobile, iOS (iPhone), Blackberry and Android.

According to a report produced by a group at the University of Toronto [4], FinSpy can be installed on a target phone via FinUSB, an associated tool produced by Gamma or by some form of socially engineered email or Internet Trojan software. Michael Kelley states, "None of the top 40 antivirus systems can even recognize it, much less block it." [5]

IV. ISP/Telco Considerations

This section will address surveillance issues specific to cell phone operation. Some jurisdictions may require by law that ISPs have certain facilities within their systems to allow for real time capture and surveillance.

4.1 Cell Phone Encryption

Mobile phone service providers have added protection of communications into their systems through the use of cryptography. However, research within the cryptographic community has shown these cryptosystems to be either deliberately weak (as proven to be the case within the GSM system) or poorly conceived as shown by Biham and Dunkelman in 2000 [6]. In any case, the cryptographic functionality often can be thwarted through various technical means – and in some cases without the application of cryptanalysis.

Examples of flawed or weak cryptographic protection provided within various cell phone systems follow:

In March 1997 the Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) systems were compromised by Counterpane Systems [7]. The Collision Eliminating Multiple Access (CEMA) cipher, a 64-bit algorithm, used in some early cell phones was shown to be weakened to an effective length of 24 or 32 bits (trivial to crack).

The Global System for Mobile Communications system (GSM - formerly known as Groupe Spécial Mobile - a common and popular cell phone system) has a long history of successful attacks. Two researchers (Biham & Dunkelman) discovered that the A5/1 (a block cipher) algorithm's GSM 64 bit key was deliberately designed to be less secure – "In practice, A5/1 was always used with only 54 bits of key, with the remaining 10 bits set to zero." [8].

Making a brute force attack (also known as an exhaustive key search) against a strong algorithm means testing every possible key until the correct one is found. A comparison of key spaces follows:

A5/1 - 2^{64} = the total possible key space is:

18,446,744,073,709,600,000 unique keys

Weakened A5/1 - 2^{54} = the total possible key space is:

18,014,398,509,482,000 unique keys

The difference between the two:

18,428,729,675,200,100,000 unique keys

The remaining key space represents 1/10th of 1 percent of the original 64-bit key space. Anyone could reasonably conclude that this constitutes a significant reduction in the security provided by the GSM A5/1 crypto algorithm.

NOTE: To put this into perspective, in 1998 Cracking DES [9] was able to solve a DES (the American Data Encryption Standard – a 2^{56} bit key space: 72,057,594,037,927,900 unique keys) encryption in a few hours. Processing power has improved in the past fifteen years since that occurred.

This flaw has since been corrected, however, it is evident that the original intention was to weaken the voice encryption capability of GSM. This issue is really academic; illustrating the fact that strong encryption could have been used but instead it was not. In December of 2000 the A5/1 crypto algorithm of GSM was defeated (shown to be solvable in a trivial amount of time) by Biryukov, Shamir & Wagner [10] and separately by Biham & Dunkelman. [8]

4.2 Cell Phone Encryption – Notification

In the GSM specification there is a provision for notifying each cell phone user when their conversation is not being encrypted. The GSM Technical Specification [11], on page 15 states: "The ciphering indicator feature allows the ME (Mobile Station) to detect that ciphering is not switched on and to indicate this to the user, as defined in GSM 02.09" [12]. However, GSM Technical Specification, on page 8 states: "This ciphering indicator feature may be disabled by the SIM)." [13].

Paget states the corresponding tag on the SIM is usually disabled and that means the user's phone will not inform them when communication is not being encrypted [14]. The rationale for service providers disabling this feature is not known. However, if an interception is in place that disables the phone's encryption, that fact will not be detected by the GSM notification feature and the user will not be informed.

4.3 SIM Card Exploit

There are more than 7 billion SIM cards currently in use. Of those around 500 million [15], use the Data Encryption Standard (DES) crypto algorithm to secure SMS over the air (OTA) update commands. The DES can be solved using a rainbow table (a pre-computed table for reversing cryptographic hash function, usually for cracking password hashes) with a standard computer in about two minutes.

SIM cards that use the DES can be exploited to take control of the device. Control means that the intruder can install software on the compromised mobile phone, spy on the user, and clone the user's SIM card. Cloning the SIM would allow the intruder to send text messages to premium rate numbers as well as facilitating several other malicious activities. This exploit affects a significant number of cards. The exploit was discovered by Karsten Nohl, founder of Security Research Labs in Berlin [15].

4.4 Carrier IQ a Case Study

CarrierIQ [16] is an application installed as a matter of routine on mobile phones (GSM) that subscribe to various service providers. This has been done without the express consent or knowledge of the individual subscriber. Depending on the model of mobile phone, disabling CarrierIQ will cause the phone to cease to work. CarrierIQ has been installed on over 140 million mobile phones. Analysis shows that it:

- Can record and report targeted text messages
- Can record and report keystrokes
- Can record and report applications used
- Can collect and record numbers dialed and received
- Can capture and report the contents of on-line searches
- Can record and report location information

Service providers claim that CarrierIQ is used by them to "collect diagnostic information about their network to improve the customer experience." The following is a timeline of events surrounding the CarrierIQ case:

- 12 Nov 2011 - Trevor Eckhart publishes a report indicating that CarrierIQ software was reporting private information without user knowledge or opt-out – potentially violating US Federal law [17].
- 16 Nov - Eckhart is sued by CarrierIQ – citing "false allegations" and for copyright violations [18].
- 16 Nov - Eckhart seeks and receives support from Electronic Frontier Foundation [19]
- 23 Nov - CarrierIQ drops their suit and apologizes
- Dec - Several civil suits filed against CarrierIQ and Congress takes aim

There are many who would like to be able to capture mobile phone activity for a myriad of reasons. Some of these reasons have to do with money, some have to do with advertising, some have to do with surveillance in its purest form, and some have to do with managing the mobile phone network. Most of this kind of surveillance, with the exception of network performance management, no matter what the excuse/justification is generally not in the users' interest.

4.5 Voice Mail

Voice Mail is recorded and held on the mobile phone service provider's (MPSP) servers and can be browsed by Law Enforcement (without a warrant in some jurisdictions) – without the user's knowledge. It can also be browsed by whoever the MPSP will allow – also without a user's knowledge.

V. Other Means of Surveillance

There are several means of surveillance that may be used by governments (law enforcement and intelligence) which can also be used by others. The following is a sample of these:

5.1 Targeted Acquisition - Bluetooth

Mobile phones can store all sorts of personal information as previously outlined above. Bluetooth is an open wireless technology for the exchange of data over short distances - it is just radio communication over a specific band width (2.40-2.48GHz). Its functionality is implemented in most mobile phones and enables actions such as hands free cable-less communication, backing up to the desktop, and other types of file transfers.

If the user's phone has Bluetooth and it is activated on the user's phone (that channel can be monitored by an Ubertooth One [20]), all of the information stored on the targeted phone may be downloaded by an intruder from more than a kilometer away. The user will not be aware of this action until the information downloaded is used to their detriment. John Hering, the builder, of Flexilis has published a "how to" set of plans [21]. The plans for building the device are freely available from the Internet. That means that other interested parties will use this technology to their advantage.

5.2 Sensor Exploitation

Most smart phones have a number of sensors built in such as accelerometer, gyroscope, GPS, compass, microphones, cameras, ambient light, and proximity. A group at the University of Pennsylvania [22] has created a program to analyze accelerometer readings. After a little training of the software, it can interpret movement into key strokes, and it may be possible to predict keystrokes on a mobile phone.

Soundcomber, a proof of concept Trojan, is another sensor exploit [23]. This one uses the audio sensor to capture credit card and PIN numbers from both tone and speech based interaction with the phone menu system.

5.3 Camera Exploitation

PlaceRaider [24] is a proof-of-concept Trojan, developed at the Indiana University in concert with the U.S. Naval Surface Warfare Center that demonstrates the invasive potential of visual malware. This application, once installed on a targeted mobile phone, captures an image using the phone's built in camera. These images are collected, analyzed and arranged into a 3D model of the environment. Anything in that environment can be further analyzed – such as documents that may be readable or other items or individuals of interest.

5.4 Interception

In the context of this paper, interception refers to communications that are compromised at some point on the communications channel. Often, but not in all circumstances, this facilitates a "man-in-the-middle" attack where the attacker controls both sides of the communication. An attacker can either listen in and gather information or take a proactive role and inject information into either or both sides of the communication. The targets would not be aware of this breach in their communications.

5.5 IMSI Catchers

The IMSI (International Mobile Subscriber Identity number) is the number used by the service provider to identify valid subscribed users and is stored on the SIM card. It forms a part of the initial handshake between the user and the cell tower. An IMSI catcher provides eavesdropping and surveillance capability by intercepting this number and using it in a man-in-the-middle attack. It is considerably less expensive than a Triggerfish setup. It also masquerades as a Base Station. For example: Vodafone Sure Signal Femtocell - NZ$249 including GST can be modified to be an IMSI catcher.

Every Mobile Station (MS) has the requirement to optimize reception. Therefore if more than one Base Station (BS) is accessible, the MS will choose to connect to the one with the strongest signal.

An intruder (Triggerfish, IMSI Catcher, Femtocell) merely has to place themselves between the cell tower and the target phone generating the strongest signal. During this handshake connection sequence (after the IMSI number has been verified), the BS instructs the MS to use a specific encryption algorithm: A5/0 or A5/1 or A5/2. In this case the man-in-the-middle instructs the MS to use A5/0 – meaning no encryption.

5.6 Private Mobile Phone Tracking

Shopping malls in some jurisdictions are tracking active (turned on) mobile phones using a system called FootPath [25] when they are within the mall. This information is collected, apparently in aggregate form, and used to analyze foot traffic within the mall with the idea of being able to identify key promotional areas. This facility could be developed further and used for other surveillance purposes. Another example requires that an application be active (with this malware incorporated into its functionality) → SonicNotify [26] makes use of ultra sonic sound. This system "embeds high frequency (inaudible) signals into music and audio played in the area which can be detected by a smart phone and delivers content to smart phones through "sound waves". The user is normally not informed that they are being tracked.

5.7 Spy Tools

The Internet is a source of specialized software that can accomplish capabilities found in Triggerfish and a lot more (and they cost a lot less and are not restricted to law enforcement). Some examples are: Interceptor SpyPhone [27] capabilities include roving bug, text interception, remote activation and all control; SpyPhone GSM [28] capabilities include roving bug, interception; FlexiSpy [29] capabilities include roving bug, GPS location if it's on the target phone, cell tracking, call interception; and MobiStealth [30] capabilities include for Blackberry, interception, roving bug, access to all logs. At this time there is no automated identification or detection of these surveillance tools being installed on a given phone. Installation may be accomplished through several vectors and does not require physical control of the target phone.

VI. Other Mobile Phone Security Issues

Mobile phones can be used by anyone to facilitate surveillance as well as posing other threats. A sample of those follow:

6.1 MALWARE

Spam, Viruses, and worms are all unsolicited, unwelcome and unnecessary to the normal operation of the mobile phone. Spam, phishing and the like are attempts to encourage the user to give up personal information which, in most cases, is not in their interest. Viruses, Worms and other attack software are designed to do damage or to take over the user's machine.

Mobile phone operating system APIs provide applications with large amounts of information about users. Applications, in addition to whatever service their primary purpose offers, may also provide a vector for installing malware or for reporting users' activities back to the application's master. Many applications take advantage of the permissions system and at installation time the user will be asked to allow access to various services that the application does not actually need to perform the stated/expected service. Most malware (73%) ask for permission to send SMS messages. Non-malicious applications rarely ask for that permission (4%). This attribute has been put forward as a potential identifier of malicious applications by a group at Berkeley [31].

6.2 LOSS, THEFT OR SEIZURE

Mobile phones that are lost or stolen (sometimes targeted) risk the potential of their contents being analyzed. The contents of any given mobile phone may be very sensitive. Passwords, account names, credit card account details, bank account details and much more may be stored on mobile phones. Obtaining someone's phone even if it is only for a short period provides the potential to produce a great deal of sensitive information and/or install spyware.

If the phone is lost or stolen, special tools can be used to extract all of this information. One tool used by the forensics community (not restricted to law enforcement only) is the Cellebrite UFED (Universal Forensics Extraction Device [32]). It comes in two versions. The first is able to capture the contents of any of more than 3,000 different models of mobile phone. It provides a reporting tool for investigative and analysis purposes that can see: Text Incoming, Text Outgoing, Video Clips, Audio Files, Ring Tones, Contact List, and Call Logs. Strictly speaking, this model does not conform to forensics acquisition rules in that it does not copy everything. The Cellebrite Physical model purportedly does copy everything. With that kind of access and analysis capability a perpetrator would be able to make use of any relevant data from a captured mobile phone to achieve their objectives – whatever they may be – assuming, of course, that the owner has kept sensitive, private or incriminating data stored on their phone. Typically mobile phones contain (a partial list):

- Phone Book
- Calendar
- To Do List
- Electronic Mail
- Instant Message
- Web Information
- Electronic Docs
- Photos
- Videos
- Audio
- Graphics

Subscriber ID
Equipment ID
Service Provider
Last Dialed #ail
Phone Number Logs
Short Text Msgs
Enhanced Msgs
Multimedia Msgs
Last Active Location
Voice & Data
Other Networks Encountered

6.3 SMART PHONES WITH GPS FUNCTIONALITY

Smart phones with GPS functionality and cameras provide the default of inserting physical longitude and latitude coordinates into the metadata which is a part of the JPG image files created by the phone's camera. Images captured in this way and shared with others can be probed to find out where and when the photo was taken.

Not all social networks clear this metadata before putting images up on their website. This information could be useful to a burglar or stalker. The GPS feature can be turned off for the camera.

6.4 NEAR FIELD COMMUNICATIONS (NFC)

NFC compliant mobile phones have the ability to communicate outside the mobile phone network using RFID technology. The exploitation of this technology is only just beginning and we have yet to see where it will go. However, it is worth mentioning that the NFC capability can be configured to read RFID credit cards and RFID passports capturing whatever information resides on the targeted RFID chip. The card/passport owner will not be aware of this data capture.

This capability is being promulgated to facilitate and simplify electronic wallet type transactions:

- This capability will enable merchants to collect previously unavailable information about customers - personally identifiable contact information as well as Level III information
- The payment network and banks involved will also have this contact and Level III information available to them
- Thus enabling far more in depth profiling and targeted marketing by the parties and whoever they sell the information to

At KiwiCon in November 2011 Nick von Dadeiszen demonstrated live capturing of an RFID credit card's data [45]. He also demonstrated live the capture of the contents, including the photo of the owner, of a New Zealand RFID compliant passport. The distance of the phone from the RFID document was only a couple of centimeters. That is merely a function of strength of the transmitter and sensitivity of the receiver used with this technology.

Note: At BlackHat 2010 –Paget demonstrated reading an RFID at a distance of 66.1 meters (using around 10W of power into a 9dBifo Yagi antenna) [33].

6.5 QR (QUICK RESPONSE) CODES

QR codes are a form of matrix barcode that is becoming more common. They are normally used for advertising purposes to facilitate quick connection to a website. These are scanned by an application on the mobile phone and used to push that phone to a website (which may or may not be malicious). When scanned by certain mobile phone applications the action is automatic. The user is not asked or notified – it just happens. If the site is malicious then various actions could be initiated by the site such as initiating a factory reset of the phone or killing the SIM or taking over and owning the phone. Software for the creation of QR codes is freely available from the Internet.

6.6 Over-The-Air Programming

Simple Messaging Service (SMS) is a method for sending short messages to the mobile phone. Normally these are used for texting. Not all SMS messages are used for texting. A service SMS is designed to enable service providers to update the client phone's operating firmware (aka Device Configuration). It may be possible, via SMS, to configure a mobile phone such that each entering and exiting phone call will be silently conferenced with the third party (the SMS originator). SMS has begun to be exploited as discussed previously with the exploitation of SIM cards through an SMS message. There will very likely be more developments in this space.

VII. Protective Measures

Some but not all compromises of mobile phone operation can be defended against. The following provides some example of these defensive measures:

7.1 Mobile Phone Blockers/Jammers

Mobile Phone Blockers/Jammers can be rechargeable, portable, and range variable (according to model). These devices can jam/block: 3G, GSM, CDMA, DCS communications. Blockers are illegal in some jurisdictions. However, where they are legal they can be useful for ensuring the confidentiality of a conference/negotiation/meeting by preventing participants from using a mobile phone as a bug. Costs vary from US$50 to US$500 or more.

7.2 Mobile Phone Firewall Protection

MobileScope [34] appears to be one of the first attempts to produce a working mobile phone firewall. This effort may provide another layer of mobile phone protection with similar capabilities to a standard PC's firewall. It purports to:

- "SEE what information their apps transmit"
- "BLOCK sensitive transmissions and unwanted traffic (ads)"
- "SECURE their communications (via HTTPs everywhere - SSL CERT pinning)"
- "SIGNAL that they don't wish to be tracked (Do Not-Track)"

As this technology becomes perfected, the necessity for mobile phone personal firewalls will become common as is the case for laptops and other computers.

7.3 Faking Application Requirements - Requests – MockDroid, TaintDroid, Paranoid Android

An approach to protecting the privacy of one's actions using their mobile phone has been created at Cambridge University. It is called MockDroid [35], and is a replacement version of the Android operating system. It fakes sensitive data to applications requesting it – thus protecting the user's privacy. The application gets valid data but that data is not reflective of the users' actions or personal data. It specifically provides the following:

Application Request	***MockDroid response***
• Location	→ no location fix
• Internet	→ connection timeout
• Calendar & Contacts	→ empty database – zero rows affected
• Device ID	→ fake constant value
• Broadcast intents	→ intents never sent/received

7.4 Mobile Phone Add-on Encryption

It is possible to implement third party encryption on mobile phones, thereby returning control of this important function to the user. Some examples from a plethora of products available on the Internet are; PhoneCrypt [36], SecureGSM PRO [37], GoldLock [38], Cellcrypt Mobile [39], and CryptoPhone [40]. These all use 256 bit AES for the algorithm. Any one of these is likely to provide adequate security for communicating using a mobile phone.

The average mobile phone user is unlikely to be aware of these products or even of their capabilities. It is incumbent on the user to assess their particular risk and make an informed decision as to whether such a product, as listed and described in these examples, is necessary for their purpose. Finally, the user needs to know that mobile phone communication is not secure and if the prize is significant enough, resources will be expended to make possible the covert interception of mobile phone communication traffic.

7.5 Protection Against Tracking

When a mobile phone is active, it will be tracked by the Telephone Service Providers (TSP) as explained in section 4.4. If the user does not wish to be tracked via their mobile phone, removing the battery will prevent this tracking. In most models of Mobile phone this is fairly easy to do but there are some models where this is either difficult or would void the warranty.

For those phones whose design makes it difficult to remove the battery i.e. iPhones, the phone can be put into a bag insulated with conductive material, usually metallic wire (which is a small Faraday cage). While the phone is inside the

bag [41], no radio transmissions in either direction can be received, processed or sent for that phone.

7.6 Protection Against IMSI Catchers

An Osmocom-based application called Catcher-Catcher uses a database of factors [43] to indicate to the user that their mobile phone is likely being monitored by an IMSI catcher. The wiki collates factors from users indicating that an IMSI catcher is in use. Catcher-Catcher also enables the user to determine whether security services have sent a silent SMS to their mobile [42].

VIII. A Summery of Protective Measures

So far only some of the surveillance methods that can be facilitated by the use of a mobile phone have been addressed. Mitigation techniques should now be considered. While not all of the surveillance techniques can be guarded against 100% of the time, the user can do a few things to minimize individual risk:

- Never store any sensitive or otherwise personal information on the mobile phone. For example: do not store credit card information or banking details on the mobile phone
- Use an anti-malware product to protect against Internet attackers.
- Disable Bluetooth when it is not needed to protect against the compromise of data on the mobile phone.
- Install a mobile phone firewall (MobileScope) and/or alternative operating system (MockDroid, TaintDroid, Paranoid Android).
- Be mindful of the mobile phone's location to minimize the opportunity of it being stolen or lost.
- Protect communications and personal data by using a third party strong encryption product.
- Insure that going to QR Code sites can only occur after user permission is granted.
- Remove the mobile phone battery when you do not want movements tracked and to protect against being bugged by "roving bug" technology. If you have an iPhone put it into a mobile Faraday cage [41] instead since removal of the battery is very difficult and voids the warrantee.

Conclusions

In most environments risk is rarely absolute and mobile phones are no different. In order for a specific user to be targeted for surveillance, there must be a potential prize. Some examples of potential targets are those who are rich or famous; those who's political, religious or other views are in conflict with the perpetrator; or those who the perpetrator has some sort of vendetta with. Targets may also be criminals of various description, terrorists, and other targets specified by law enforcement and/or the intelligence community.

If the potential payoff for an attack is worth the expenditure of resources – it will be mounted. Instituting various defensive measures should be an informed decision – knowing the cost of the real risk compared to the cost of the mitigating measure in time, effort and money.

The author is not advocating abandoning the use of this very important, useful, and powerful tool. For the user, the decision to accept any given risk is often a function of convenience. However, it should be an informed decision – knowing the cost of the real risk compared to the cost of the mitigating measure in time, effort and money.

This paper has discussed some of the current surveillance uses for mobile phones. There is no 100% security solution and one cannot protect oneself from every risk. Some risks are considered and then ignored as a matter of convenience. The ultimate protection from mobile phone surveillance would be to not have one. That is not an acceptable option for most users and so one must make some choices. The first is to do nothing at all and accept whatever risks there are. Perhaps no risk is apparent and the convenience outweighs any potential threat. For those who are more sensitive to security issues, then this paper has, in addition to revealing some of the potential threats, provided measures that can mitigate some of the risks.

Glossary

Faraday Cage according to Wikipedia "is an enclosure formed by conducting material or by a mesh of such material. Such an enclosure blocks external static and non-static electric fields." These shield the interior from external electromagnetic radiation and block such radiation from escape – in this paper that refers to radio waves.

Femtocell is a low power small cellular base station normally used by service providers to extend their service, however, with some modifications (less than NZ$1,000) this can become and IMSI Catcher.

IMEI (International Mobile Equipment Identity) – this is the unique number of the physical mobile device and can be found inside its case. Used by GSM to identify valid devices.

Note: Every phone has an International Mobile Equipment Identity – a unique 15 digit identification number. If the mobile phone is lost, this number can be given to cell phone service providers and the phone can be permanently disabled. Type *#06# to get this important serial number.

IMSI (International Mobile Subscriber Identity) – stored in a 64 bit field (15 digits or less) on the SIM and is used for various purposes by the service provider. It contains the country code, provider ID, and subscription ID.

IMSI Catcher is a false mobile base station used by Law Enforcement and others for eavesdropping on targeted cell phone communications traffic.

Luddite – the Oxford English Dictionary defines it as: "One who opposes the introduction of new technology, esp. into a place of work."

Man-in-the-middle according to Wikipedia is "a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each

other over a private connection, when in fact the entire conversation is controlled by the attacker."

SIM (Subscriber Identity Module) – normally purchased from the mobile service provider or his agent - It has a unique ID # (ICCID), an IMSI and other authenticating and ciphering information.

REFERENCES

[1] Stingray 2, Harris Corporation manufactured, Stingrays are designed to locate a mobile phone even when it's not being used to make a call. The Federal Bureau of Investigation considers the devices to be so critical that it has a policy of deleting the data gathered in their use, mainly to keep suspects in the dark about their capabilities, an FBI official told The Wall Street Journal in response to inquiries. http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html

[2] Triggerfish, Walls Street Journal, 22 September 2011.

[3] Electronic Surveillance Manual, Triggerfish, U.S. Justice Department, June 2005, http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf

[4] Marquis-Boire, Morgan et al, For Their Eyes Only: The Commercialization of Digital Spying, Munk School of Global Affairs, University of Toronto, 1 May 2013.

[5] Kelley, Michael, This Powerful Spy Software is Being Abused by Governments Around the World, Business Insider Australia, 3 May 2013.

[6] Biham, Eli & Dunkelman Orr, Cryptanalysis of the A5/1 GSM Stream Cipher, Progress in Cryptology – INDOCRYPT 2000, Bimel Roy & Eiji Okamoto – editors, Springer, India, December 2000, ISBN 3540414525.

[7] Counterpane Systems, 20 March 1997, Press release, www.schneier.com/cema-press.html

[8] Biham, Eli, Dunkelman, Orr, Cryptanalysis of the A5/1 GSM Stream Cipher, a research paper supported by the European Union fund IST-1999-12324 – NESSIE and by Technion- Israel Institute of Technology's Chais' Excellence Program, 1999.

[9] Gilmore, John, Electronic Frontier Foundation, Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design, Electronic Frontier Foundation, April 30, 1998, ISBN‑10 1565925203.

[10] Biryukov, Alex, Shamir, Adi, Wagner, David, Real Time Cryptanalysis of A5/1 on a PC, Cryptome, 27 April 2000, the Weizmann Institute, Israel.

[11] GSM 02.07 V7.1.0 (2000-03), Technical Specification, ETSI, Valbonne, France, 2000.

[12] GSM 02.09 V6.1.0 (2000-02), Technical Specification, ETSI, Valbonne, France, 2000.

[13] GSM 11.11 V5.0.0, Technical Specification, ETSI, Valbonne, France, 1995.

[14] Zetter, Kim, Hacker Spoofs Cell Phone Tower to Intercept Calls, Wired, July 2010. http://wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/

[15] Karsten Nohl, Encryption Flaw Makes Phones Possible Accomplices in Theft, The New York Times, 21 July 2013.

[16] Eckhart, Trevor, What is Carrier IQ? http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

[17] USC Title 18: Crimes and Criminal Procedure, Chapter 119: Wire and electronic Communications Interception and Interception of Oral Communications.

[18] CEASE AND DESIST DEMAND, Sent by Certified Mail and email, on November 16, 2011, to Trevor Eckhart. http://misc.branchable.com/posts/cease_and_desist_demand_sent_to_Trevor_Eckhart/

[19] Electronic Frontieer Foundation, Carrier IQ Tries to Censor Research With Baseless Legal Threat, 21 November 2011. www.eff.org

[20] Ubertooth - Bluetooth monitoring device, http://ubertooth,sourceforge.net

[21] Cheung, Humphrey, March 08, 2005, Bluesniper – a device designed to target and capture data from Bluetooth enabled mobile phones from a distance of a kilometre or more. Plans in two parts available from the internet:

Part 1
http://www.smallnetbuilder.com/content/view/24256/98/
Part 2
http://www.smallnetbuilder.com/content/view/24228/98/

[22] Aviv, Adam J., Sapp, Benjamin, Blaze, Matt, Smith, Jonathan M., Practicality of Accelerometer Side Channels on Smartphones, ACSAC '12, ACM 978-1-4503-1312-4, December 2012.

[23] Schlegel, Roman, Zhang, Kehuan, Zhou, Xiaoyong, Intwala, Mehool, Kapadia, Apu, Wang, XiaoFeng, Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones, City University, HongKong, and Indiana University at Bloomington.

[24] Templemany, Robert, Rahmany, Zahid, Crandally, David, Kapadiay, Apu, PlaceRaider: Virtual Theft in Physical Spaces with Smartphones, Indiana University and The US Naval Surface Warfare Center, September 27, 2012.

[25] FootPath Reporting Suite – from Path Intelligence, www.pathintelligence.com

[26] Sonic Notify, found at: http://sonicnotify.com

[27] Interceptor SpyPhone – http://www.fonefunshop.co.uk/spyphone/spy_interceptor.htm

[28] SpyPhone GSM → http://www.daddyseye.com/

[29] FlexiSpy → http://www.flexispy.com/

[30] MobiStealth → http://www.mobistealth.com/

[31] Felt, Adrienne Porter, Finifter, Matthew, Chin, Erika, Hanna, Steven, Wagner, David, A Survey of Mobile Malware in the Wild, SPSM'11, University of California at Berkley, 17 October 2011, ACM 978-1-4503-1000-0.

[32] Cellebrite, provider of mobile forensic solutions, www.cellebrite.com

[33] Paget, Chris, Extreme Range RFID Tracking, Black Hat 2010, Ceasar's Palace, Las Vegas, Nevada, 28-29 July 2010. http://blackhat.com/html/bh-us-10/bh-us-10-archive.html#Paget.

[34] MobileScope, Created by David Campbell, Aldo Cortesi, and Ashkan Soltani, Firewall for mobile phones: http://mobilescope.net/

[35] MockDroid, Digital Technology Group, University of Cambridge at: http//:www.cl.cam.ac.uk/research/dgt/android/mock

[36] PhoneCrypt http://www.phonecrypt.com/~phonecry/ge/index.php

[37] SecureGSM PRO http://www.securegsm.com/home.php

[38] GoldLock → https://www.gold-lock.com/app/en/Home

[39] Cellcrypt Mobile → http://www.cellcrypt.com/cellcrypt-mobile

[40] CryptoPhone → http://www.cryptophone.de/

[41] Identity Stonghold, RFID privacy protection, www.idstronghold.com

[42] 28th Chaos Communication Congress, New attacks on GSM mobiles and security measures shown, Berlin, 28 December 2011

[43] Open Source web site – last viewed 20/8/13 → opensource.srlabs.de.

[44] FinFisher™: Governmental IT Intrusion and Remote Monitoring Solutions - pp 18-20 → www.gammagroup.com

[45] Kiwicon V – 2011 – Nick von Dadeiszen Scans a credit card and separately a New Zealand passport with his mobile phone → www.lateralsecurity.com