By Joseph Ooi

IMSI Catchers and Mobile Security

Advisor: Professor Nadia Heninger

EAS 499 Senior Capstone Thesis

School of Engineering and Applied Science
University of Pennsylvania

April 29, 2015

TABLE OF CONTENTS

1 INTRODUCTION

IMSI catchers are radio devices that pose as fake cellular base stations and exploit vulnerabilities in 2G telecommunications networks on the GSM standard in order to intercept mobile phone traffic. They are widely used by state and federal agencies across the United States and are also suspected of being deployed by private and criminal organizations in illegal ways. This paper sets out to understand how IMSI catchers work and what kind of contexts they are employed in, as well as to investigate the countermeasures currently available against IMSI catchers and their impact on mobile communications.

The next section provides a brief outline of cell phone networks, protocols, and standards, from the first generation of wireless communications to current 4G standards. Section 3 delves into IMSI catchers, how they work, and how they have been used. Section 4 explores the various countermeasures that are available against IMSI catchers. Finally, Section 5 summarizes the implications of IMSI catchers on cellular security.

2 CELL PHONE PROTOCOLS

2.1 Cellular Networks

A cellular network is a radio network distributed over land areas called "cells". Each cell is served by one fixed-location transceiver, which is called a "base station". When cells are joined together, they provide wireless coverage over a large geographic area, within which mobile stations or phones can communicate with base stations and each other. Overlapping coverage areas allows transmission to be maintained even when mobile stations are moving between cells. Assigning a different set of frequencies to neighboring cells avoids wireless signal interference.

2.2 1G (analog)

The first generation of mobile telecommunication standards was introduced in the 1980s. The radio signals used in these networks were analog and only allowed for the basic call functionality. In North America, Bell Labs developed the first cellular network standard, the Advanced Mobile Phone System (AMPS) system, in 1983 [1]. AMPS became the dominant 1G standard in North America and continued to be supported by major telecommunications companies like AT&T and Verizon until eventually discontinued in 2008. Other 1G standards worldwide include NMT, TACS, C-450, Radiocom 2000, RTMI, JTACS, TZ-801, TZ-802, and TZ-803.

The AMPS standard is based on Frequency-Division Multiple Access (FDMA), which assigns unique frequencies, or "channels", to each phone conversation. AMPS also enabled call centers to assign frequencies to mobile stations based on signal strength, allowing frequencies to be re-used in various locations without interference. This greatly increased the number of mobile phones which could be supported in any particular geographic region [2].

2.3 2G (digital)

Following the first generation of wireless communication networks, the GSM (General System for Mobile communications) standard[1], developed by ETSI (European Telecommunications Standards Institute), was the first 2G technology to replace the 1G analog standard. In 1991, GSM was first implemented in Finland by the operator Radiolinja. By 1998, GSM was being used all over the world with more than 100 million subscribers [3]. In 2015, GSM is the most widely-used technology for wireless networks worldwide, with over 90% market share and more than 6 billion subscribers across at least 219 countries [4].

[1] Originally *Groupe Spécial Mobile*, GSM was renamed following the worldwide adoption of the GSM standard.

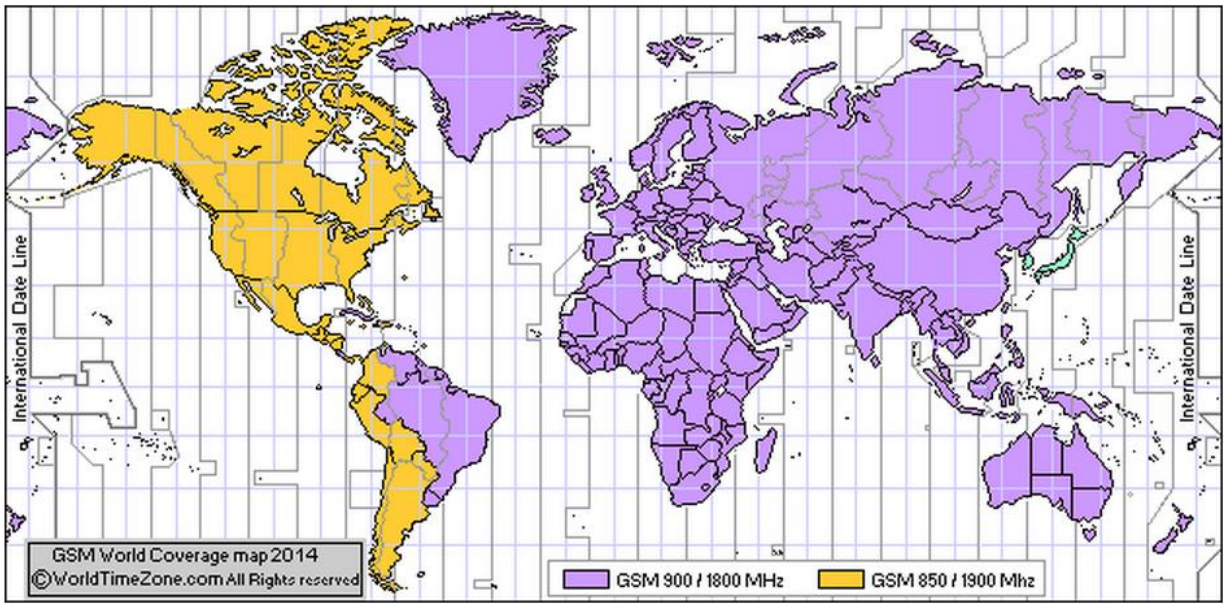

Figure 1: GSM World Coverage Map [5]

GSM significantly increased network capacity by using the assigned frequency bandwidth more efficiently. It also introduced mobile data services and enabled functionality such as SMS (Short Message System) texting, MMS (Multi Media Messages), voice mail, call forwarding, and other features. Estimates of 2G technologies data rates range from 9.6 to 28.8 KB/s [6]. Finally, 2G GSM enabled digital encryption of wireless communications, in contrast to 1G AMPS, which lacked encryption and was completely vulnerable to wireless eavesdropping.

Other major 2G standards include IS-95 (a.k.a. cdmaOne), PDC, iDEN and IS-136 (a.k.a. D-AMPS). Based on the way the technology shares the frequency bandwidth over multiple channels (multiplexing), these technologies can be divided into Time Division Multiple Access (TDMA)-based and Code Division Multiple Access (CDMA)-based standards [7].

Not all United States service providers use GSM technology. Sprint and Verizon, two of the largest service providers, use CDMA technology rather than GSM. This provides them with some immunity against IMSI catchers. During Def Con in 2010, where Chris Paget demonstrated a $1,500 homebuilt IMSI catcher, he explained that cell phones on the Sprint and Verizon networks would not connect to a fake cell tower [8]. This is likely due to the fact that SIM cards issued by Sprint and Verizon will not respond to GSM protocol requests and, thus, be immune to the IMSI catcher attack.

2.4 GSM Protocol

Since current models of IMSI catchers function almost exclusively by exploiting vulnerabilities in the GSM protocol, this section will delve into the details of how GSM networks function. The exact way IMSI catchers exploit these vulnerabilities is further discussed in Section 3.

2.4.1 Network Components

For simplicity, a GSM network can be understood as consisting of 4 main types of network components (see Figure 2), as described in [9]:

1) Mobile Stations (MS)

The Mobile Station is a cell phone or other mobile device equipped with a removable SIM (Subscriber Identification Module) smartcard. Each SIM card is uniquely identified by its IMSI (International Mobile Subscriber Identity) number [10], which is usually a 15 digit number consisting of:

- A 3-digit Mobile Country Code (MCC)
- A 2- or 3-digit Mobile Network Code (MNC), and
- The Mobile Subscriber Identification Number (MSIN)

The mobile device itself can also be uniquely identified by its IMEI (International Mobile Equipment Identity) number. This allows identification and rejection of stolen phones. Finally, the SIM card also stores 3 additional pieces of security-related data:

- The authentication algorithm A3
- The key generation algorithm A8
- A 128 bit long-term secret key K_i that is used in both algorithms and also shared with the GSM network

2) Base Stations (BS)

Also known as "cell towers" or "cell sites", Base Stations communicate directly with Mobile Stations and each Base Station essentially manages one "cell" in the cellular network. The size of each cell can range from a few hundred yards to several miles, depending on the geographic features in the area, which would expand or limit transmission capabilities accordingly, and the required call capacity. In densely-populated urban areas, more cells are required per unit area in order to serve more customers on the assigned frequency spectrum. Base Stations also manage encryption and decryption of communication data.

3) Base Station Controllers (BSC)

Each Base Station Controller manages several Base Stations. When a Mobile Station moves between cells during a call, the "handoff" is managed by either a Base Station Controller or Mobile Switching Center.

4) Mobile Switching Centers (MSC)

Mobile Switching Centers have the main role of mobility management in each GSM network. There are 4 databases that they draw on:

- Home Location Register (HLR): Each GSM network has only one HLR. The HLR stores the personal information of all subscribers in the GSM network, including their IMSI.
- Visitor Location Register (VLR): Each MSC has its own VLR, which stores the personal information of subscribers under the jurisdiction of the respective MSC.
- Authentication Center (AuC): The AuC stores the access data of every subscriber on the network, in particular, the long-term secret key K_i of each SIM card.

- Equipment Identity Register (EIR): This stores IMEI numbers of banned or stolen phones to prevent them from accessing the GSM network.

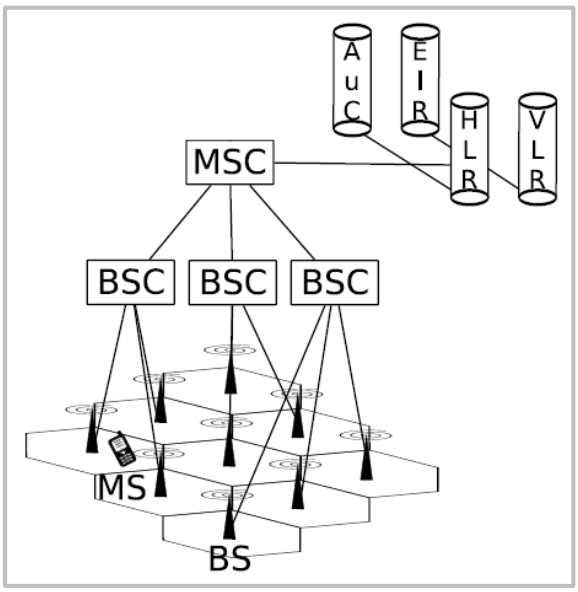

Figure 2: Simplified GSM network architecture [9]

2.4.2 Authentication and Encryption

When a Mobile Station tries to access the network, it must authenticate itself to the Base Station, although the reverse is not required. This procedure is outlined in Figure 3 below.

First, the Mobile Station sends its security capabilities to the VLR (through the Base Station). This tells the network what A5 encryption protocols it is capable of. The VLR then sends the Mobile Station an Identity Request command, which induces the Mobile Station to respond with its IMSI number. Now having the IMSI, the VLR then sends an authentication parameter request to the HLR which is forwarded to the AuC. The AuC first generates a 128 bit random number, RAND, and calculates a 32 bit signed response SRES based on RAND and the stored long-term secret key K_i that corresponds to the respective SIM:

$$SRES = A3(RAND, K_i) \quad [VLR]$$

The AuC also generates a 64 bit session key K_c using the algorithm A8:

$$K_c = A8(RAND) \quad [VLR]$$

The random number RAND, signed response SRES, and session key K_c are sent back to the VLR. However, only RAND is passed back to the Mobile Station. Using the secret key K_i stored in its SIM card, the Mobile Station can calculate:

$$SRES' = A3(RAND, K_i) \quad [SIM]$$

The Mobile Station then sends SRES' back to the VLR. If SRES and SRES' do not match, the authentication request is rejected. Otherwise, it is accepted and the VLR assigns the Mobile Station a Temporary Mobile Subscriber Identity (TMSI) and tells it what cipher mode A5 to use.

The possible cipher modes include:

- A5/0 – no encryption
- A5/1
- A5/2
- A5/3 – based on the KASUMI algorithm

The TMSI is intended to increase security by reducing the number of times the IMSI is broadcasted, and serves to identify the Mobile Station in future transactions with the VLR.[2]

If any option other than A5/0 is chosen, the Mobile Station calculates the session key K_c using the A8 algorithm on the input RAND, as shown above. The chosen A5 algorithm is then used to encrypt all subsequent communication between the Mobile Station and Base Station:

$$CIPHER = A5(K_c, MESSAGE)$$

The session key K_c continues to be used as long as no new authentication request is initiated. When this occurs is determined by the individual network operators. In practice, the same session key may stay in use for quite some time, extending to subsequent calls.

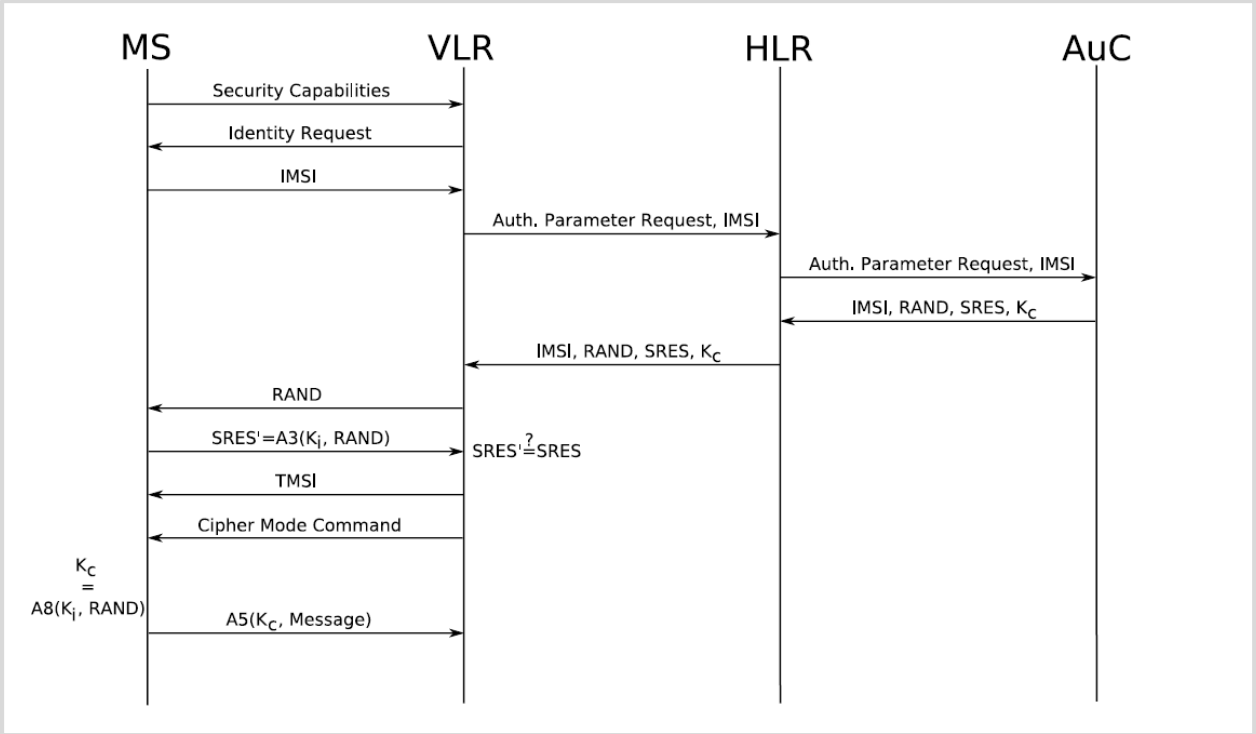

Figure 3: GSM Authentication Procedure [9]

[2] Note that when the Mobile Station is "roaming" (connected to a visiting network instead of its home network), since the visiting network does not recognize its TMSI, it must resend its IMSI to the visiting network, who will then communicate with its home network to authenticate its identity, before assigning the Mobile Station its own TMSI.

2.4.3 GSM vulnerabilities

At a glance, the GSM authentication procedure exposes a few vulnerabilities, which include the following:

- The one-way authentication process requires the Mobile Station to authenticate itself to the Base Station, but does not require a Base Station to verify its identity to the Mobile Station.
- From the advent of the GSM standard, the algorithms A3, A5 and A8 have been kept a secret instead of being subject to public scrutiny. They have only been discovered through reverse engineering and information leaks, allowing weaknesses to be discovered in the algorithms. Real-time cryptanalysis of A5/1 on a PC has been shown to be possible, and the successor algorithm A5/2 has been shown to be even more insecure [11].

The exact exploitation of these vulnerabilities by IMSI catchers will be more extensively discussed in Section 3.

2.5 2.5G (GPRS) and 2.75G (EDGE)

Since 2G networks were primarily built for voice services, data transmission capabilities were relatively slow. The first improvement on GSM networks came with the use of GPRS (General Packet Radio Service) networks that implemented a packet-switched domain in addition to the existing circuit-switched domain. GPRS allowed for a theoretical maximum transfer speed of 115 KB/s, but closer to 35 KB/s in reality [12].

The next improvement came in the form of EDGE (Enhanced Data Rates for GSM Evolution), with the introduction of 8PSK encoding. In 2003, this backward-compatible technology was first deployed on top of existing GSM networks by AT&T in the United States. EDGE allowed for a theoretical maximum transfer speed of 473 KB/s, but closer to 135 KB/s in reality [13]. Although EDGE meets the requirements for 3G technology, it is still considered 2.75G because most other 3G technologies still provide significantly faster data transmission rates.

2.6 3G (UMTS and CDMA2000)

Mobile networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications laid down by the International Telecommunication Union (ITU) may be branded as 3G technologies. In 2001, the first commercial launch of 3G took place in Japan by NTT DoCoMo [14]. As of 2013, estimates of the number of 3G and 4G subscriptions range from between 1.7 to 2.1 billion out of approximately 7.0 billion mobile subscriptions, suggesting that current global 3G market penetration is still under 30% [15].

The UMTS system, standardized by 3GPP, is most prevalent in regions dominated by 2G GSM infrastructure, including Europe, Japan, and China. It includes several available radio interfaces, including W-CDMA, TD-SCDMA (only in China), HSPA, and HSPA+, the last of which can provide data rates of up to 21-42 MB/s [16].

The other major 3G technology is the CDMA2000 system, standardized by 3GPP2, most prevalent in regions dominated by the 2G IS-95 standard, including North America and Sotuh Korea. The latest EVDO Rev B allows for peak data rates of 14.7 MB/s [17].

While ITU does not specify a minimum data rate for 3G technologies, it states an expectation that IMT-2000 technologies will provide transmission rates at a minimum speed of 2 MB/s for stationary or walking users and 348 KB/s for moving vehicles [6]. The increased bandwidth and location information on 3G networks also enable additional features, including GPS (Global Positioning System), location-based services, video on demand, and video conferencing.

Finally, 3G networks also offer additional security features. Most crucially, mobile stations are allowed to authenticate the network that they are connecting to in order prevent cell tower spoofing [18]. Additionally, 3G networks use the KASUMI block cipher (similar to the A5/3 cipher) as opposed to the A5/1 cipher [19].

Nevertheless, some vulnerabilities have also been reported in 3G security. In 2010, Dunkelman, Keller, and Shamir demonstrated a practical "sandwich attack" on A5/3 encryption using a single PC and in under two hours [19].[3] In addition, Meyer and Wetzel demonstrated in 2005 a man-in-the-middle attack that could exploit inter-operating GSM/UMTS networks [20].

2.7 4G (WiMAX and LTE)

4G technologies are specified by the International Telecommunications Union-Radio communications sector (ITU-R) in the International Mobile Telecommunications Advanced (IMT-Advanced) specifications. In contrast to earlier generations of wireless technologies, 4G systems require all communication to be Internet Protocol (IP)-based, such as Voice over IP (VoIP), and does not support traditional circuit-switched telephony. Requirements for peak speed data rates are 100 MB/s on trains and cars and 1 GB/s for stationary users and pedestrians [21].

The two main 4G technologies in the market are Mobile WiMAX, first deployed in South Korea in 2007, and Long Term Evolution (LTE), first deployed in Norway and Sweden in 2009. Currently, both technologies do not provide the expected data rates as specified by IMT-Advanced. LTE offers theoretical peak download and upload speeds of 300 and 75 MB/s respectively [22], whilst Mobile WiMAX offers theoretical peak rates of 70 MB/s [23]. Network operators nevertheless brand these technologies 4G as they represent a new generation of non-backward-compatible wireless technologies. In 2010, ITU-R recognized that these technologies could be considered 4G by acting as forerunners to the IMT-Advanced standard and a substantial level of improvement over current 3G systems [24]. In the United States, Verizon, AT&T, T-Mobile, and Sprint all employ LTE networks. Sprint still uses Mobile WiMAX, but plans to shut it off by the end of 2015 [25].

[3] Interestingly, the MISTY algorithm that KASUMI is based off remains unbroken.

3 IMSI CATCHERS

3.1 Introduction

Attacks on GSM include cracking GSM encryption, passive GSM interception, and active GSM interception. IMSI catchers fall into the last category, actively interfering in communications between mobile phones and base stations by acting as a transceiver (simultaneously transmitting and receiving). IMSI catchers use a "man-in-the-middle" attack, simultaneously posing as the fake mobile phone to the real base station and as the fake base station to the real mobile phone.

IMSI catchers are able to determine the IMSI numbers of mobile phones in its vicinity, which is the trademark capability from which their name is derived. Using the IMSI, they can then identify mobile traffic on the network and target traffic for interception and analysis.

The most famous IMSI catchers are StingRay devices sold by the Harris Corporation to various government agencies in the United States. Thus, IMSI catchers have also come to be generally known as "stingrays". They have also been called "cell site simulators" or "cell site emulators", especially among law enforcement agencies [26].

3.2 Functionality

Although the implementation of different IMSI catchers may vary, the section below attempts to highlight how most IMSI catchers function, as laid out in [9], [27], [28], and [29].

3.2.1 Obtaining the IMSI

Whenever there is more than one Base Station belonging to the home network in the vicinity, GSM mobile phones will always connect to the Base Station that is emitting the strongest signal. Thus, by transmitting a sufficiently strong signal, an IMSI catcher will cause every mobile phone within a small radius to connect to it.

The IMSI catcher then acts like a Base Station. First, the Mobile Station is induced to send its encryption capabilities to the Base Station, which can be ignored. Then, the IMSI catcher sends an Identity Request command to the Mobile Station, which is forced to respond with its IMSI.[4]

3.2.2 Initiating network connection

The IMSI catcher can now connect to the network by sending a Location Update Request.[5] When the network responds with an Identity Request, the IMSI catcher can respond with the stolen IMSI.

[4] There is a similar procedure that can be used for forcing transmission of the IMEI.

[5] This procedure allows the mobile station to inform the cellular network whenever it moves from one location to the next, so that the network can continue to keep it connected through the nearest base station.

The network then sends the IMSI catcher the challenge RAND. Since it does not have the secret key K_i, the IMSI catcher is initially unable to respond.

3.2.3 Completing Mobile Station connection

Instead, it forwards RAND to the Mobile Station as a challenge, following up the last communication in Section 3.2.1. The Mobile Station, having the relevant K_i, calculates the signed response SRES and sends this back to the IMSI catcher. At this point, since the IMSI catcher does not need to verify SRES, it can ignore the response, accept the authentication by the Mobile Station and complete the connection.[6]

Since the base station determines the encryption mode in the GSM protocol, the IMSI catcher can set the cipher mode to A5/0 (no encryption). It then allocates an arbitrary TMSI to the Mobile Station and accepts the Location Update. From here on, the IMSI catcher can communicate with the Mobile Station and easily gain access to outgoing calls.

3.2.4 Completing network connection

With the signed response from the Mobile Station, the IMSI catcher also forwards SRES' to the network, which completes the authentication procedure with the network.

If the network tries to set an encryption mode A5/1 to A5/3, the IMSI catcher can suppress encryption by declaring that it has no encryption capabilities, defaulting to A5/0 instead. The IMSI catcher can now communicate with the network.

Alternatively, given the vulnerabilities of the A5/1, A5/2 and A5/3 algorithms, newer IMSI catchers also have the option of breaking the encryption in practical time and communicating with the network with the assigned encryption algorithm. The A5/1 is vulnerable to precomputation attacks using rainbow tables, which are publicly available [30]. This allows for machines with 2 GB RAM and a 2 TB hard drive to obtain the secret key in approximately 2 minutes [29]. Due to serious vulnerabilities in the A5/2 algorithm, the GSM Association explicitly prohibited its use in 2006 and it is no longer implemented on GSM networks [31]. For the A5/3 algorithm, although practical attacks have been demonstrated, these are unlikely to be fast enough for IMSI catchers to use [19].

3.2.5 Cell Imprisonment

Once the IMSI catcher has completed the connection to a Mobile Station, it can try to prevent the Mobile Station from connecting to another base station. Base Stations usually make a list of other Base Stations nearby ("neighboring cell list") available to allow phones to easily and seamlessly switch between cells. The IMSI catcher can instead transmit an empty neighbor list or a list with neighboring base stations that are unavailable to the Mobile Station.

[6] If completing the connection with the Base Station is not required, the IMSI catcher can also choose to generate its own random challenge RAND and send RAND to the Mobile Station. After the MS responds with SRES, the IMSI catcher can simply ignore SRES and accept authentication, then continue to complete the connection with the Mobile Station.

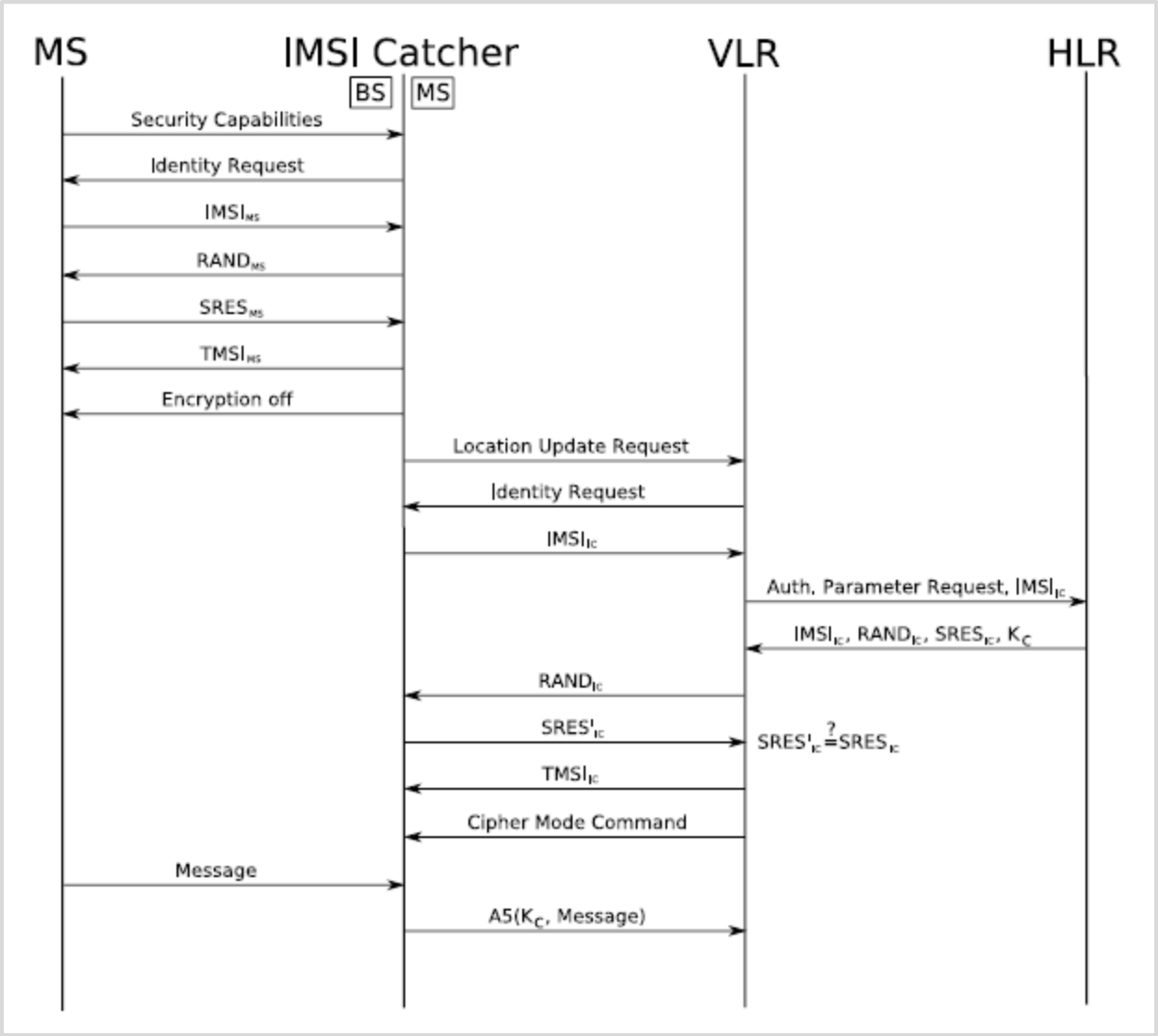

Figure 4: Man-in-the-middle attack using an IMSI catcher [9]

3.3 Capabilities

The initial function of the IMSI catcher is to obtain the IMSI numbers of cell phones operating in the vicinity, as the name suggests. This can also be performed on 3G networks (see Section 4.6).

Next, because base stations do not need to authenticate themselves to mobile phones in the GSM protocol (as explained in Section 3.2.3), it is trivial for IMSI catchers to obtain outgoing information from the mobile phone and communicate directly with the mobile phone, acting as the phone network and relaying fake information from the network to the mobile phone.

More advanced functions require a full man-in-the-middle attack, with the IMSI catchers authenticating themselves (as mobile phones) to the phone network and relaying both outgoing and incoming communications. Capabilities of IMSI catchers vary widely with the technological

complexity of the device, even among law enforcement agencies. The sheriff's department in Maricopa Country, Arizona, claimed in 2011 that their StingRays only allowed them to pinpoint a cell phone's location and did not grant the ability to listen in on conversations [32]. Dirtboxes used by the U.S. Marshals Service on planes can pinpoint a suspect's cell phone down to approximately 10 feet.

More advanced IMSI catchers are able to intercept texts and eavesdrop on calls [27]. They may also be capable of intercepting data transmissions, including numbers dialed, web pages visited and other such information [33]. IMSI catchers are often equipped with jamming equipment (in order to force 3G and 4G phones down to a 2G connection) and other such denial-of-service capabilities [34]. Some IMSI catchers may be able to retrieve files from the target phone, such as photos and texts [35].

Based on documents leaked by Edward Snowden, the National Security Agency (NSA) had already developed a technique in 2004 to locate cell phones even when they were turned off, called "The Find", mostly used to locate terrorist suspects [36]. This was accomplished through the use of IMSI catchers, which could wirelessly send a command to the phone's baseband chip to fake any shutdown and stay on [37]. The phone could then be instructed to keep just the microphone on, in order to eavesdrop on conversations, or periodically send location pings. The only hint that the phone was still on was if it continued to feel warm even though it had been shut off, suggesting that the baseband processor was still running. IMSI catchers used by London's Metropolitan Police are also reportedly able to shut down targeted phones remotely [38].

3.4 Suppliers

In 1996, the German company Rohde & Schwarz started selling the first IMSI catcher, GA 090. It allowed the user to force an unidentified subscriber to transmit the SIM's IMSI. In 1997, the next model, GA 900, additionally allowed the user to tap outgoing phone calls.

Currently, GSMK (who sells the CryptoPhone that protects against IMSI catchers) claims that they know of at least six different companies producing IMSI catcher devices. Most of these commercially available IMSI catchers are approximately the size of a household Internet router.

The most well-known manufacturer of IMSI catchers is Harris Corporation, which first developed the StingRay device for the military and intelligence community. The original StingRay costs $68,479 and the StingRay II costs $134,952 [34]. Its devices are only sold to law enforcement and government agencies [32].

Figure 5: Harris Corporation's StingRay II [39]

Digital Receiver Technology, Inc. (DRT), formerly known as Utica Systems [40], also designs and sells IMSI catchers to U.S. law enforcement agencies [35], in addition to a wide range of other antennas, transceiver systems and software-defined radios. Their device, the DRTBOX (pronounced "dirtbox"), has been used in a U.S. Marshals Service program to scan thousands of cell phones from overhead planes (see Section 3.5.1).

Meganet Corporation, a data security company, sells the VME Dominator, which offers a full suite of IMSI catcher features including "voice manipulation, up or down channel blocking, text intercept and modification, calling & sending text on behalf of the user, and directional finding of a user during random monitoring of calls" [41]. In accordance with federal law 47 U.S.C. 302a, Meganet only sells these products to U.S. government agencies and authorized parties.

The Gamma Group is an international firm that manufactures and sells surveillance and monitoring technology [42]. In 2013, leaked brochures showed that it also sold body-worn IMSI catchers measuring just 41 x 33 x 18 cm [43]. However, the body-worn IMSI appears only to be able to obtain IMSI numbers, whilst other devices (also sold by the Gamma Group) are required in order to intercept calls and SMS.

Septier, which produces solutions for the security and telecommunications market, also markets full-size and mini IMSI catchers. They also have an add-on 3G module that allows for extraction of IMSI numbers from 3G cell phones [44]. However, it is unclear if the 3G module allows for the tapping of cell phones on 3G connections.

PKI also sells both a GSM IMSI catcher and a 3G UMTS IMSI catcher. The PKI 3G IMSI catcher appears to function by jamming the 3G signal and "redirecting [the phones] to specific GSM frequencies, in order to monitor the conversation" [45].

In 2010, white hat hacker Chris Paget (now known as Kristin Paget) famously demonstrated at the RSA Security Conference in San Francisco that it was possible to build a homemade IMSI catcher for about $1,500 using a software-defined radio, two directional antennas, and a laptop running OpenBTS and Asterisk [46].

3.5 Usage

Users of the CryptoPhone have reported multiple potential IMSI catchers operating from all over the United States. In 2014, Popular Science published a map of 17 fake cell towers detected by CryptoPhones over the course of a single month, shown below in Figure 6 [47]. This created a buzz of excitement and alarm among the security community because it suggested that the use of IMSI catchers was much more widespread than previously anticipated. One CryptoPhone user reported detecting up to 8 fake cell towers when driving from Florida to North Carolina. During other test runs with the CryptoPhone in Washington, D.C., up to 18 IMSI catchers were detected over two days of driving in the city [48].

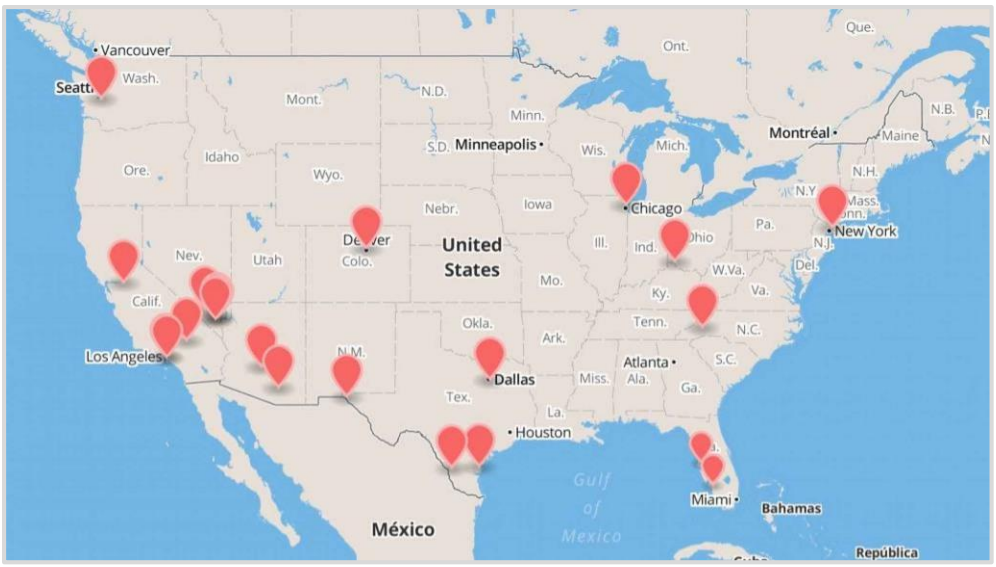

Figure 6: Locations of 17 IMSI catchers detected across the U.S [47]

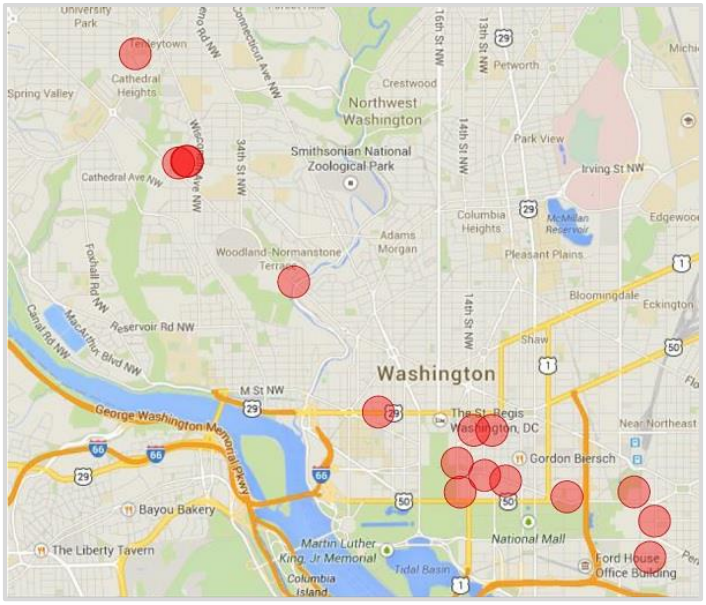

Figure 7: Locations of 18 IMSI catchers detected in Washington, D.C. [48]

In March 2015, ESD America reported that they had found 54 IMSI catchers, up from the initial number of 17 [49].

IMSI catchers are known to be used by government agencies, foreign governments, and criminal organizations alike.

3.5.1 By Home Government Agencies

StingRay devices, manufactured by the Harris Corporation, have been notoriously used by law enforcement agencies in the United States for at least the past 20 years, particularly by the Federal Bureau of Investigation (FBI) [50]. In a 2009 case, an FBI agent described using cell site

emulators more than 300 times over the course of a decade [51]. Figure 8 below shows 21 states in which state and/or local police have been known to use IMSI catchers [52]. A list of the federal agencies that have been known to use IMSI catchers can also be found in Appendix 6.1.

Police departments have used these devices to track cell phones, particularly stolen ones [53]. In some cases, the police have mistakenly entered houses and arrested civilians at gunpoint before realizing that the StingRay had identified the wrong apartment.

In December 2014, protestors in Chicago expressed their outrage at the grand jury's decision not to indict the New York Police Department officer who had choked Eric Garner to death in a controversial incident. On the streets, participants reported seeing a van follow the protest and messing up their cell phone connections whenever it drove by [54]. The hacker group Anonymous later released a recording of police radio transmissions revealing that they had been tapping cell phone activity at the protests [55]. Speculators suspect that the Chicago Police Department were using a StingRay device in the van to monitor cell phone use at the protests.

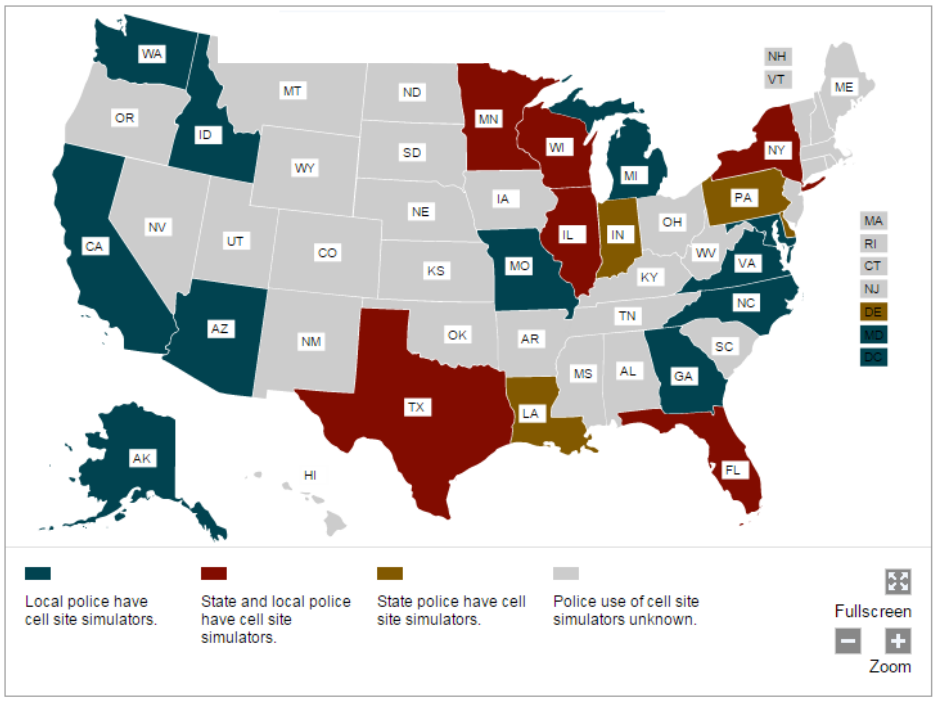

Figure 8: Police use of IMSI catchers by state [52]

In 2014, a Wall Street Journal article revealed that since 2007, the U.S. Marshals Service had been flying Cessna planes equipped with IMSI catchers made by DRT, also known as "dirtboxes" [35]. On each of these flights, the dirtboxes collect the IMSI numbers and locations of tens of thousands of cell phones. They are also capable of focusing their information gathering on suspects and "letting go" of non-suspect phones. Justice Department officials have neither confirmed nor denied such a program and it is unclear how closely they are monitoring it.

Government use of StingRays has historically been kept a close secret. In the past, law enforcement agencies used to assert that a probable-cause warrant was not required to employ StingRay devices because they did not intercept the contents of calls and texts, but only collected

header information [51]. Published records show that police departments have frequently used StingRays without seeking warrants beforehand [56] [57]. When they do, they have been known to describe StingRays as "pen register devices", which merely record all numbers called from a particular phone number, grossly misrepresenting the capabilities of their StingRays.

Before selling their devices, Harris Corporation has required law enforcement officials to sign a nondisclosure agreement (NDA) that barred them from revealing almost anything about the technology [58]. The FBI has cited these NDAs as a basis for withholding information about the technical specifications of StingRays, even from judges [59]. After loaning StingRays to the Sarasota and the North Point Police departments in Florida, the U.S. Marshals Service instructed them to conceal the use of the devices in court documents, simply stating that information was received "from a confidential source regarding the location of the suspect" [60]. In some cases, they have even been willing to drop criminal charges rather than risk sharing information about cell site simulators [26]. Multiple civil liberties organizations have since requested information about StingRays under the Freedom of Information Act, and in 2015, TheBlot Magazine received a heavily redacted copy of a 2010 StingRay user manual, with nearly all of the information blotted out [39].

With increased public scrutiny of StingRays in recent years, several states have specifically mandated the requirements of warrants in order to use the devices, with more looking to pass similar bills [61] [62] [63]. The FBI has also publicly announced that it requires a search warrant in order to use StingRays in places where there is a reasonable expectation of privacy [64].

Government use of IMSI catchers at protests is not limited to the United States. During the Kiev protests in 2014, cell phones in the vicinity received an ominous text message, "Dear subscriber, you are registered as a participant in a mass disturbance" [65]. Since network operators can easily identify cell phones in a particular geographic area by identifying the cell towers that they are connected to, this would actually be a trivial task for them. However, mobile operators in Kiev denied involvement [66], suggesting instead that an IMSI catcher was used to identify the nearby phones and send them the SMS [67].

3.5.2 By Others

Statements by Leo Goldsmith, CEO of ESD America, suggest that a significant amount of IMSI catcher activity in the United States is conducted by parties unrelated to the U.S. government [49]. According to Goldsmith, the largest group of interceptors use the open-source software OpenBTS, suggesting that these are laptop devices connected to software-defined radios configured by hobbyists to act as IMSI catchers. The next largest group are "commercial-grade from overseas", suggesting that they are employed by foreign intelligence services. There is little public information regarding the use of IMSI catchers by criminal organizations, although Czech police reported the use of unauthorized IMSI catchers in 2012 [38].

In 2014, the Federal Communications Commission (FCC) established a task force to investigate the illegal use of IMSI catchers and similar technology by criminal organizations and foreign intelligence services [68].

4 COUNTERMEASURES

4.1 Detection Indicators

As the design and production of IMSI catchers has historically been kept secret, not much information is publicly available about how specific models of IMSI catchers work. However, based on investigative research and working prototypes such as Chris Paget's homebuilt IMSI catchers, there are some unusual behaviors of IMSI catchers that can be used to differentiate them from legitimate base stations. Some of these have been identified as proposed heuristics and are laid out below, following the material in [27].

These detection indicators can be monitored on either the user's mobile phone (see Sections 4.2 and 4.3) or on separate hardware (see Section 4.4). Such apps or devices may be called "IMSI catcher catchers" or "IMSI catcher detectors". Implementation of these indicators has also been limited by access to baseband chip functions, which has typically been restricted by chipmakers[7].

4.1.1 Off-band Frequency Usage

In order to increase signal quality and reduce noise, IMSI catchers may choose to operate on an unused frequency, such as channels reserved for testing or buffer channels between different operators. The drawback of using these frequencies is that the mobile stations may prefer neighboring cell frequencies (as advertised by the original base station they are connected to) instead, reducing the probability of the mobile station connecting to the IMSI catcher. Alternatively, the IMSI catcher can operate on an advertised frequency that is not actually in use at that time in the vicinity.

This behavior can be detected by cross-checking the operating frequencies of the cell towers in the vicinity against the current frequency band plan as designated by local authorities. According to [27], "radio regulatory bodies and frequency plans are available for almost all countries."

4.1.2 Unusual Cell ID

GSM Cell IDs (CIDs) are unique numbers identifying each base station within a Location Area Code (LAC) in a GSM network. Valid CIDs range from 0 to 65535 (i.e. 2^{16}-1) for GSM and CDMA networks. In order to avoid protocol mismatch with the real base stations and to elicit a Location Update request from mobile phones, IMSI catchers usually introduce a new CID previously unused within the operating geographic region.

This behavior can be detected by cross-checking the base station CIDs in the vicinity with a database of registered base stations, their CIDs, and their registered geographic locations. These databases are available from government sources, for example, the Federal Communications

[7] In his presentation of SnoopSnitch, Nohl explains that the development team would have implemented detection measures for additional heuristics if they could, but were instead limited by restricted access to information from the Qualcomm baseband chip [18].

Commission (FCC) makes information on registered base stations publicly available [69]. CIDs that are unregistered or far away from their registered geographic location can be marked as suspicious.

4.1.3 Base Station Capabilities and Network Parameters

Base stations usually offer a suite of supported features, such as GPRS or EDGE. Some of these services are complex to implement, and it is unlikely that any but the most sophisticated of IMSI catchers will support these protocols. In addition, mobile stations convey basic network parameters about the organization of the mobile network, including threshold values, time slot organization, and timeout values. According to [27], these parameters vary between different operators but are usually uniform across base stations for the same operator. Rudimentary IMSI catchers may not copy all of this data comprehensively because it is peripheral to the core attack functionality.

This behavior can be detected by cross-checking the detected base station capabilities against a database of registered base stations (as described above in Section 4.1.2) and their reported capabilities. If the offered services do not match the database, the base stations can be marked as suspicious. Likewise, irregularities in network parameters can be used to highlight suspicious base stations.

4.1.4 Radio Frequency (RF) Jamming

In order to expedite the process of luring the mobile phone to disconnect from a real base station and connect to the IMSI catcher, the attacker may choose to jam other frequencies. The mobile phone's connection will be interrupted and after failing to connect to any other advertised neighboring base stations, the phone will conduct a full scan of nearby base stations and connect to the IMSI catcher. The jammer also allows the IMSI catcher to jam 3G and 4G signals and "downgrade" a 3G or 4G mobile phone to its 2G GSM capability in order to exploit its 2G vulnerabilities. There are several options on the market for turnkey products with the ability to jam specific phones, for example [70] and [71].

Jamming can be detected by a mobile station by monitoring the noise levels on relevant frequencies, such as its currently used frequency and those of base stations on the neighbor list.

4.1.5 Attacks on Inter-operating GSM/UMTS Networks

The aforementioned Meyer and Wetzel attack on inter-operating GSM/UMTS networks as described in [29] will allow IMSI catchers to downgrade a 3G UMTS mobile connection to 2G GSM and carry out its man-in-the-middle attack, an alternative solution to 3G signal jamming.

This behavior can be detected by observing when a mobile station downgrades to a GSM connection in an area where UMTS connection should be available, based on registered base station databases.

4.1.6 Absence of Encryption

As described earlier in Section 3.2.3, IMSI catchers can easily instruct mobile phones on the GSM protocol to set cipher mode A5/0 i.e. use no encryption (also described in Section 3.2.4, more advanced IMSI catchers may choose to set cipher mode A5/1 or A5/2 and break it in real-time).

Given the wide variance in encryption standards implemented on operator networks, the absence of encryption alone is insufficient to suggest IMSI catcher activity. However, if a mobile phone had already established an encrypted session and its communications suddenly become unencrypted, this can be highlighted as a suspicious indicator.

4.1.7 Lack of Neighboring Cell Information

As described in Section 3.2.5, IMSI catchers may choose to broadcast empty or invalid neighboring cell lists in order to keep the connected mobile phone "captive".

This behavior can be detected by having the mobile station monitor the availability and authenticity of the neighboring cell lists. It can also be cross-checked against registered databases to better recognize suspicious lists that do not seem consistent with the information of the cell towers registered in the area.

4.1.8 Traffic Forwarding

Once the IMSI catcher has established connections with both the mobile station and the network (see Sections 3.2.3 and 3.2.4), it will need to relay communications between both parties. In the most basic setup, the IMSI catcher is unable to handle any incoming calls to mobile station, as was the case with Rohde & Schwarz's GA 090 and GA 900, described in [9]. In order to forward calls, data, and SMS to the phone network, basic IMSI catchers may choose to use another SIM card and mobile station. In this case, it will appear to recipients of communication from the attacked mobile phone that the call is being made from an unknown phone number. The IMSI catcher may choose to disable caller ID presentation in order not to alarm the recipient.

This behavior can be detected by making test calls from the mobile phone and checking the caller ID on the recipient device.

However, more advanced IMSI catchers can choose to forward the information through other means, such as routing them directly into a trusted wholesale or exchange telecommunications partner network or using a more advanced relaying setup that enables a proper man-in-the-middle attack and full relaying of two-way communications.

4.1.9 Short Base Station Lifetimes

IMSI catchers are usually operated for short periods of time. When used to locate phones with unknown IMSI numbers or used to sweep geographic areas to collect IMSI numbers, they operate very briefly. When used to intercept communications and eavesdrop, they may only be

operated for the duration of one or a few calls. Thus, they are usually only detectable by mobile stations for relatively short periods of times, compared to legitimate base stations.

This behavior can be detected by flagging base stations that suddenly appear on the network but only for a short period of time, especially when these base stations have a particularly strong signal strength when they appear.

4.1.10 Changing/Inconsistent LAC [72]

If the mobile station has already established a connection with a legitimate network using a specified TMSI, it may not connect to a nearby IMSI catcher even if the latter is broadcasting with more power than the original base station. Thus, the IMSI catcher may change its LAC in order to trigger a Location Update request from the mobile phone.

This behavior can be detected by monitoring the consistency of LAC/CID pairs. If a nearby cell tower with a particular CID suddenly changes its LAC, this can be highlighted as suspicious behavior. In addition, the legitimacy of LAC/CID pairs can be cross-checked with a database of registered base stations.

4.2 Secure Mobile Phones

From a Blackberry-dominated market in the 2000s, the market for high security smartphones has quickly expanded in recent years to include a range of offerings from various boutique security firms. Currently, the CryptoPhone and Stealth Phone are the only options that protect against IMSI catcher attacks. Nevertheless, the Blackphone and FreedomPop's Privacy Phone are also given brief mention in this section as they offer some enhanced security features.

4.2.1 GSMK's CryptoPhone

Located in Berlin, Germany, GSMK primarily manufactures and sells mobile phones, landline phones, and satellite phones that leverage the processing capacity of the mobile device to ensure strong end-to-end voice encryption. They serve "very demanding clients that cannot afford the security of their communications to be compromised", which include governments, international institutions, private individuals and organizations from over 50 countries worldwide [73]. GSMK prides themselves as having the only commercial smartphone with both state-of-the-art encryption and published source code available for independent review.

The GSMK CryptoPhone uses a unique audio compression algorithm (codec) and offers both Circuit Switch Data (CSD), found in GSM networks, and IP modes. To encrypt their mobile traffic, each call uses a 256-key generating using a 4096-bit Diffie Hellman shared secret exchange, which hashes the resulting 4096 bits to the 256-bit session key using SHA256. The subsequent hash verification prevents man-in-the-middle attacks such as those by IMSI catchers.

The 256-bit keys are used to encrypt calls using both AES and Twofish, providing a double layer of encryption security in case cryptanalysis discovers a weakness in one of the algorithms in

the near future. For calls, a new key exchange is generated for every call. For SMS, the initial key exchange is stored securely on the phone and used through means of a hash-chain.

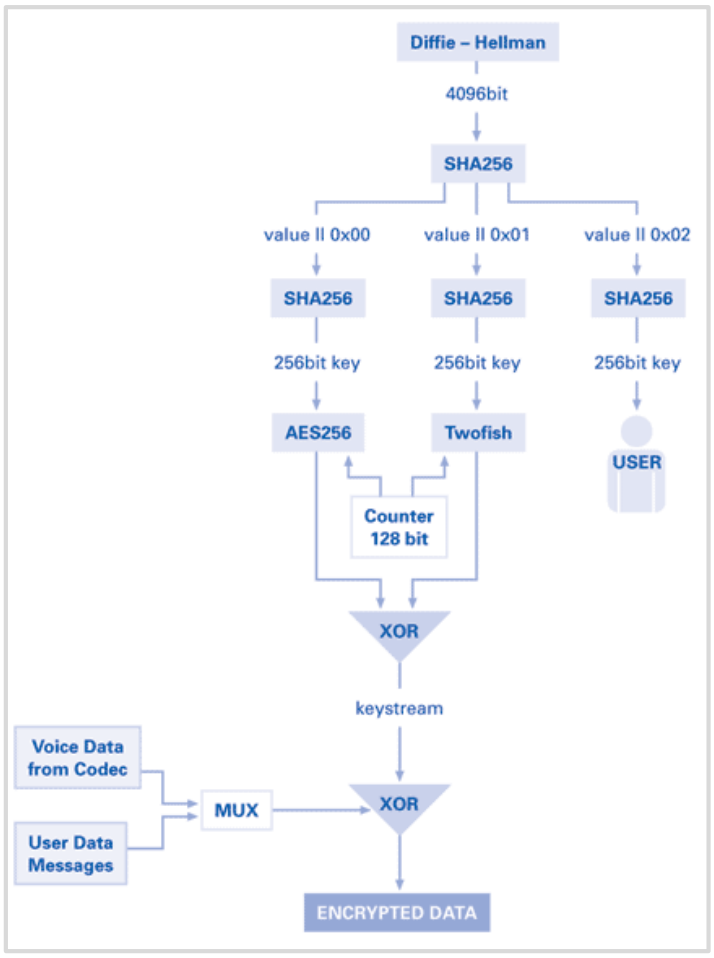

Figure 9: CryptoPhone Encryption Process

The flagship model, the GSMK CryptoPhone 500, runs on a Samsung Galaxy S3 with a proprietary OS and costs approximately $3,500 [74]. ESD America estimated that there were already 30,000 CryptoPhones in the United States and 300,000 worldwide, as of September 2014 [48].

CryptoPhone security is also fortified using a proprietary baseband firewall [75]. The firewall monitors all connections to the phone's baseband and reports suspicious activities to the user, including:

- Cell towers that lack an identifying CID
- Cell towers with a suspiciously different signal strength
- Cell towers operating as expecting or trying to manipulate phones
- When the mobile network's encryption is deactivated
- When the cell phone abruptly switches from a 3G or 4G network to a 2G network
- When I/O devices are activated through baseband without instructions from OS
- When phone makes suspicious connections despite no user activity or ongoing updates

The CryptoPhone uses three main heuristics to measure the likelihood that an IMSI catcher is operating in the vicinity [48]. Although the detection process is still not watertight, when all three indicators are present simultaneously, there is a reasonably good chance that an IMSI catcher is present nearby. These indicators are:

- When the phone shifts from a 3G network to a 2G network
- When the phone connection removes encryption
- When the cell tower does not provide a list of "neighboring" cell towers

Figure 10: CryptoPhone Warning Screen

4.2.2 XCell's Stealth Phone

XCell Technologies, located in Geneva, primarily produces Stealth Phones with a variety of security features [76]. The basic phones alert the user to nearby interceptors (IMSI catchers) and call interception whilst the most advanced phones allow for dynamic IMEI changing to prevent phone tracking. Its phones range from €400 to €800. A table of prices and capabilities can be found in Appendix 6.2.

4.2.3 SGP Technologies' Blackphone

The Blackphone is a security-enhanced smartphone developed by SGP Technologies, a joint venture between the Spanish smartphone company, GeeksPhone, and the encrypted communications firm, Silent Circle. The Blackphone runs on an Android-based proprietary PrivatOS and routes mobile communications using VoIP through a Virtual Private Network (VPN) for additional security, supporting 2G, 3G and 4G bands [77]. It offers a bundled suite of Silent Circle security apps that allow various functions such as voice or video calls or encrypted text messaging. The Blackphone primary targets prosumers, a market segment between professional and consumer.

The Blackphone BP1 began shipping on June 30, 2014, for $629 per unit [78]. The phone comes with a 1-year subscription to the Silent Circle bundled apps, thereafter costing $10 /month. Pre-orders reportedly sold out quickly, with regular sales resuming soon after [79]. On March 2, 2015, a sequel, the Blackphone 2, was announced, in addition to a secure tablet device, the

Blackphone+. With these subsequent releases, SGP Technologies plans to cater more to enterprise solutions in response to growing demand from enterprises.

The Blackphone reportedly provides safeguards against femtocell man-in-the-middle attacks [80]. However, the Blackphone does not offer the same baseband firewall as the CryptoPhone [81]. If attackers are able to access the baseband OS, then the Blackphone's communication encryption becomes irrelevant from a security standpoint as the attacker can disable encryption or choose a form of encryption that it can break in real-time (see Sections 3.2.3 and 3.2.4).

4.2.4 FreedomPop's Privacy Phone

FreedomPop offers a Samsung Galaxy II-based Privacy Phone that it has nicknamed the "Snowden Phone". Launched in March 2014, the Privacy Phone encrypts voice calls and text messages with 128-bit encryption whilst application and Internet data is sent through an encrypted VPN. In addition, owners can change their phone number at will.

The Privacy Phone costs $189. It comes without a contract but with 3 months of unlimited voice calls and texting, as well as 500MB of data. Subsequently, subscription costs $10 per month.

FreedomPop's target audience are consumers who want to remain anonymous amid privacy violations across social networks and mobile devices. It even offers Bitcoin payment options for heightened anonymity. However, its security features appear to be limited to communication encryption, which is not a unique mobile product offering. For example, Blackberry emails are encrypted, and apps like Signal on iOS allow for encryption of voice calls, text messaging and even data communications [82]. The Privacy Phone does not appear to provide any protection against man-in-the-middle IMSI catcher attacks.

4.3 Mobile Phone Software

4.3.1 Open-source Detection Software

A number of open-source projects aiming at detecting IMSI catchers have been started in recent years. Among these projects, SnoopSnitch appears to be the most comprehensive in terms of ability to detect IMSI catchers. Most of the other projects are in various stages of development.

SnoopSnitch is an Android app developed by Security Research Labs, a German firm founded by Karsten Nohl [83]. It was first presented by Nohl at the Chaos Computer security conference in Hamburg on December 27, 2014, and is available for free on the Google Play Store [84]. SnoopSnitch is deployable on Android phones that, at a minimum, have Qualcomm chipsets and root privileges available. The app "collects and analyzes mobile radio data to make you aware of your mobile network security" and warns users when it suspects IMSI catcher activity and other mobile threats, although it is unable to prevent mobile phones from connecting to IMSI catchers. SnoopSnitch also allows users to draw on the data collected in the GSM security map and to contribute their own data to the map [85].

CatcherCatcher was the Security Research Labs' precursor to SnoopSnitch [18]. Although it also offered detection of IMSI catchers, it was only available on mobile phones with the OsmocomBB software, which greatly limited the models of phones that it could be installed on (only a few versions of Motorola, Sony Ericsson, and some other models) [86].

Android IMSI-Catcher Detector (AIMSICD) is an open-source project managed by SecUpwN and started in 2012 [87]. The app is still in development and has only implemented a handful of detection mechanisms, including the cross-checking of CIDs collected by the phone against public base station databases and checking for "changing LACs" (see Section 4.1.10) of CIDs that have been collected by the phone [88]. It aims to expand its detection indicators to eventually include checking neighboring cell info, signal strength monitoring, and other heuristics.

Darshak is an open-source Android app available for free on the Google Play Store [89]. It was developed by post-doctorate researcher Ravishankar Borgaonkar (Technical University Berlin) and Master's student Swapnil Udar (Aalto University). Darshak monitors the receipt of silent SMS and displays information about the current status of network connections, including IMSI catcher suspicion. A test version is available for Galaxy S2 and S3 phones with an Intel chipset [90].

Spidey is an open-source app currently being developed by Jeffrey Warren, a graduate student at MIT [91]. Spidey aims to be able to monitor base stations in the vicinity of the mobile phone and alert the user to possible use of IMSI catchers in the vicinity.

4.3.2 Enterprise-level Detection Software

Zimperium Mobile Security markets a suite of enterprise-level mobile security products, including zIPS (Zimperium Intrusion Prevention System), that detect and prevent man-in-the-middle attacks, among other security capabilities [92]. Zimperium initially raised $8.0mm from Sierra Ventures in December 2013 [93]. In July 2014, they became the first company to offer enterprise-level security software for iOS devices [94].

4.4 Standalone Hardware

4.4.1 Pwnie Express' Detector

Pwnie Express is a maker of wired, WiFi, and Bluetooth monitoring devices. As recently as April 20, 2015, at the cryptography RSA Conference in San Francisco, they unveiled a live prototype sensor that would be able to detect a range of cellular threats, from cell jammers to IMSI catchers [95].

Pwnie Express is still in the process of refining the heuristics it uses to detect rogue and malicious cell towers and reducing the occurrence of false positives. Some of the heuristics it uses to determine whether a cell tower is a potential threat include:

- Unauthorized or unknown cell providers, based on their Mobile Network Code (MNC) and Mobile Country Code (MCC)
- Sudden changes in cell tower signal strength

- New cell towers suddenly appearing
- Cell service going down to a 2G network
- Cell towers claiming to be from a major carrier but only providing 2G service
- Cell towers based on open source software, e.g. Yate default base station configurations[8]

Since the prototype was only announced recently, little is known about the extent or effectiveness of its detecting capabilities. However, this sensor, along with the CryptoPhone and Stealth Phone, appear to be the only commercially-available turnkey hardware products capable of detecting IMSI catchers with considerable reliability.

4.4.2 SBA Research's IMSI Catcher Catcher

SBA Research, a joint academic research center based in Vienna, announced a prototype stationary IMSI catcher catcher in August 2014 [96]. The device was built from a Telit modem without a SIM card and a Raspberry Pi Linux computer, costing about €100 in parts. It was capable of detecting between 270 to 400 base stations in the center of Vienna, and approximately 20 to 30 such devices would be required to cover an area of 20 km^2. The laboratory results of the use of the device is still pending.

4.4.3 Open-source Portable-IMSI-Catcher-Detector

An open-source project to create a portable, ARM-based detector, Portable-IMSI-Catcher-Detector, also exists [97]. However, the project is still in its "very early stages of development" and is incomplete.

4.4.4 ESD America's Overwatch

ESD America is a Las Vegas-based company that specializes in defense and law enforcement technology [98]. They are also the manufacturers of the GSMK CryptoPhone. After detecting multiple IMSI catchers across the United States whilst testing the CryptoPhone, ESD America decided to develop and launch its latest product, ESD Overwatch, a comprehensive system to identify and locate IMSI catchers, announced in March 2015 [49]. The system will use a network of ESD-built, briefcase-sized devices that monitor base station connections in a specific area. Alternatively, ESD can also modify Samsung Galaxy S3, S4, or S5 smartphones to act as detectors. ESD Overwatch will be marketed exclusively to the U.S. government and other governments "strictly allied" to it, with at least 14 governments already having expressed interest in the program

4.5 Android Cell Tower Enumeration App

This project involved developing a proof of concept Android app to enumerate nearby cell tower locations.

[8] This indicates that the cell tower operator has configured the cell tower as a gateway for phone calls or other malicious purposes.

The app allows an LG Nexus 5 smartphone to record basic cell tower information and upload the data to a server. Using this information, we can estimate the physical positions of cell towers in a geographic region and cross-check the information against the FCC's database of registered base stations for possible discrepancies.

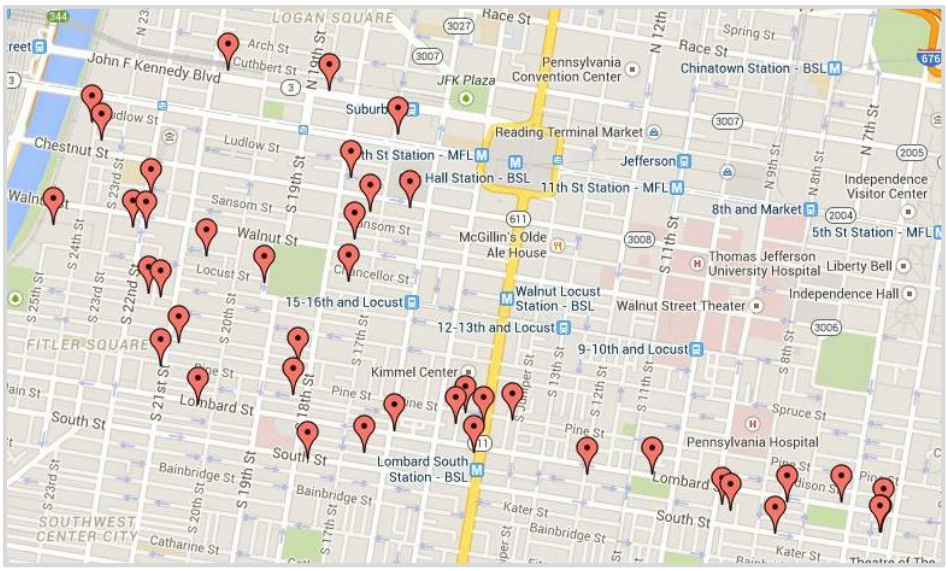

Figure 11: Mapping of Cell Towers in Center City, Philadelphia

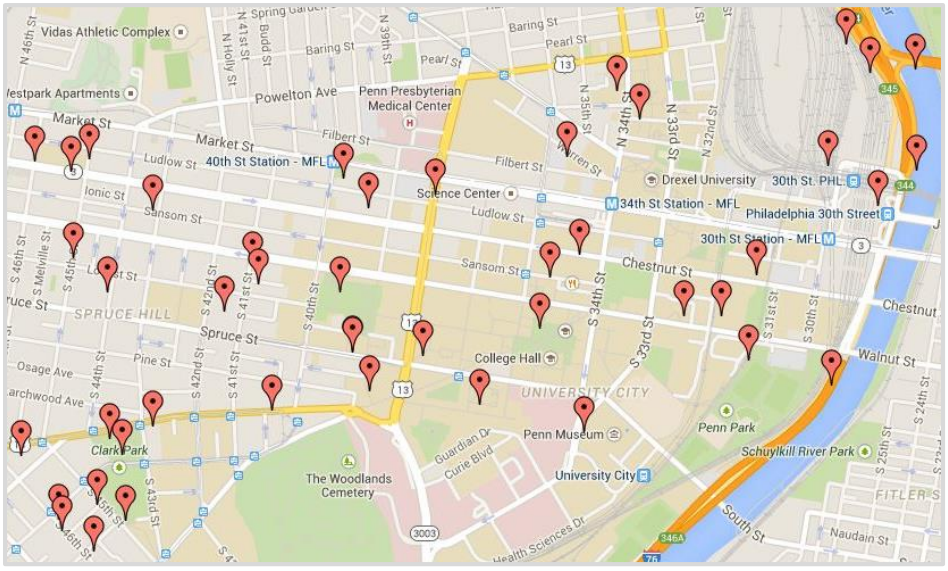

Figure 12: Mapping of Cell Towers in University City, Philadelphia

A sample of the relevant Android source code from the Data Collection App used to survey this information on an LG Nexus 5 can be found in Appendix 6.3.

As demonstrated in Appendix 6.3, the primary method used to retrieve information on cell phone communications with nearby cell towers was the `getNeighboringCell()` function. However, this method returns static information as recorded by the cell tower that the cell phone is currently connected to, instead of returning real-time information as observed by the cell phone.

It appears that gaining access to first-hand nearby cell tower information as observed by the cell phone may require special access to the baseband chip in the SIM.

Future steps could involve obtaining this baseband access to gain first-hand cell tower information, and using other heuristics to detect when a phone may be pinged by or connected to a fake cell tower, emulating the reported functionality of other IMSI catcher detectors.

4.6 Upgrading of 2G Networks and Phone Capabilities

Attacks on GSM encryption have been shown as early as 1987, then re-iterated in 1994. Most recently, Karsten Nohl and Chris Paget demonstrated in 2010 that cracking GSM encryption can be done "at home", using commercial software-defined radios (SDR) and Rainbow Tables [99]. The security researchers are part of an ongoing effort that calls for the overhauling of the highly-vulnerable 2G network and phone capabilities. If cellular networks and cell phones no longer support the GSM standard, then current IMSI catcher technology will be rendered obsolete.

As of 2014, GSM continues to be the dominant standard for cellular networks worldwide. In the United States, some major carriers like Verizon and AT&T are starting to phase out their 2G networks (see Table 1 below). However, others like Sprint are instead taking advantage of the opportunity to grab some of the migrating customers to their 2G networks. In addition, even if network providers phase out the GSM standard, cell phones that still have baseband chips with 2G GSM functionality may still be susceptible to IMSI catcher attacks. In other countries, some major carriers have also begun shutting down their GSM networks, for example, Telstra (Australia) plans to do this by the end of 2016 [100].

Table 1: 5 Largest U.S. Wireless Service Providers

Carrier	Subscribers [101] (in millions)	2G Network
Verizon Wireless	131.9	Plans to shut down 2G (and 3G) network by approximately 2021 [101].
AT&T	120.6	Plans to shut down 2G GSM network by approximately Jan 2017 [102].
Sprint	55.5	
T-Mobile	55.0	Upgrading GSM networks to LTE and HSPA+ since 2012; plans to leave some 2G bandwidth in place [103]
US Cellular	4.8	

At the December 2014 Chaos Computer security conference, Karsten Nohl pointed out vulnerabilities in the 3G network that exploit the SS7 telephony signaling protocols [18]. SS7 enables the setting up and management of calls in a separate network rather than the same network that the call is made from, allowing for services like call forwarding and wireless roaming [104].

Nohl explained that in 3G networks, although IMSI catching is still technically possible in the sense that catchers can force mobile phones to broadcast their IMSI numbers, direct man-in-the-middle attacks that allow IMSI catchers to eavesdrop and mimic mobile communications are not possible because IMSI catchers are unable to authenticate their identity (as base stations) to the mobile phone [18]. However, by exploiting global SS7 networks, IMSI catchers can obtain authentication proof from the mobile operator and falsely authenticate their identity to the mobile phone.

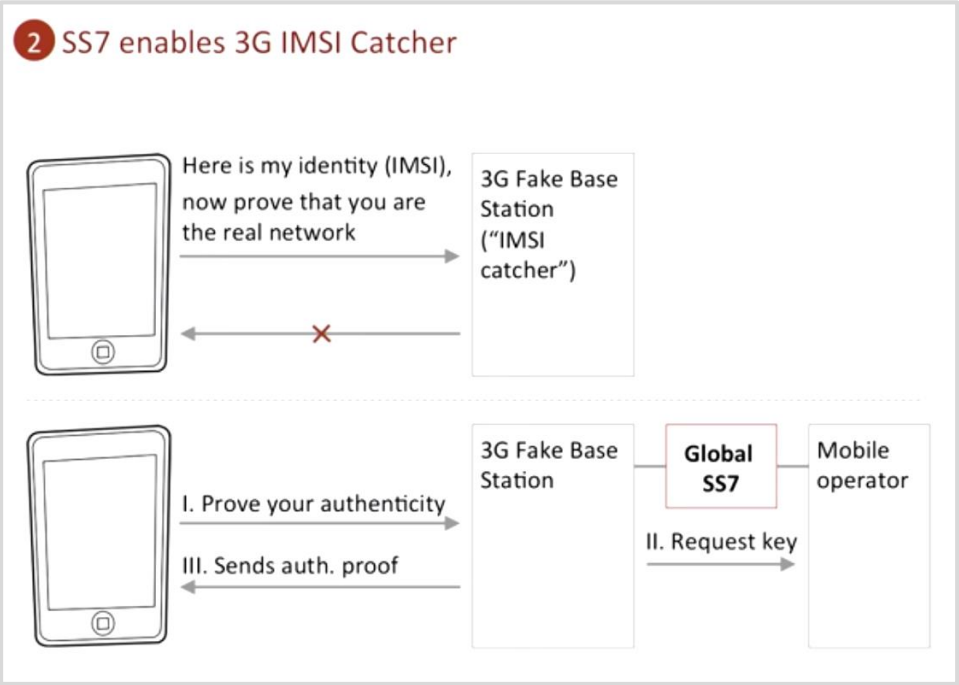

Figure 13: Man-in-the-middle attack on 3G networks exploiting SS7 vulnerability

In 2014, the News Tribune in Tacoma, Washington, unearthed a March purchase order from the Drug Enforcement Administration (DEA) for a "StingRay II to Hailstorm Upgrade" [105]. Hailstorm reportedly gives StingRay devices the capability to intercept 4G LTE phones even after 2G networks have been phased out, which imply that overhauling the GSM standard may not render all IMSI catchers obsolete. Martone Radio Technology also seems to advertise products with the capability to intercept 4G LTE phones [106], although this may merely be an ability to jam 4G signals and force the phone into a 2G connection before carrying out a man-in-the-middle attack. Apart from these two exceptions, no other 4G IMSI catchers are currently known to exist.

4.7 Wireless Network Providers

Since IMSI catchers must simultaneously connect to the target mobile phone and the original cell tower, it is possible for network operators to detect IMSI catcher activity [99]. In the words of security researcher Karsten Nohl, "The network operator, in any given country, knows where IMSI catchers are operating."[9]

[9] Note that this assertion stands in contrast to Strobel's assertion in [9] that IMSI catchers can tap mobile phones in such a way that "even the network operator cannot notice anything".

However, network operators have thus far been silent on the issue of IMSI catchers, as far as the public is concerned. Verizon has denied any knowledge of the use of dirtboxes by the U.S. Marshals Service [35]. Since some of the largest users of IMSI catchers are likely to be government agencies themselves, there is little incentive for network operators to highlight IMSI catcher use to government authorities. In fact, operators have instead continuously asserted the security of their wireless networks.

5 CONCLUSION

Although IMSI catchers have been in use by government agencies for many years, the availability of affordable software-defined radios and expertise to build IMSI catchers have made them more easily accessible than ever to hobbyists. Since it still costs upwards of $1,500 to build or purchase an IMSI catcher, basic threat modelling suggests that the general public has little to fear from the use of IMSI catchers with regards to their everyday communications.

However, the use of IMSI catchers by government agencies may eventually be of significant concern. Whilst the use of IMSI catchers to apprehend criminal suspects is highly desirable, unrestrained use of the devices could lead to gross violations of privacy, especially given programs such as the U.S. Marshals Service's dragnet plane surveillance, coupled with the capabilities of advanced IMSI catchers.

In addition, IMSI catchers may be a popular tool for corporate espionage. Whilst the price tag of IMSI catchers is certainly too steep for personal use, it may not be a large deterrent for business opportunists seeking to capitalize on information that could be worth millions of dollars.

Finally, the use of IMSI catchers by foreign intelligence services and criminal organizations is of great concern to government agencies, especially given the fact that very little is known about the extent of their use.

Fortunately, even as use of IMSI catchers has been growing more prevalent, the range of solutions has also been growing rapidly. For the everyday (Android) phone user, SnoopSnitch seems to be a reliable app to detect IMSI catchers operating nearby. For the business user, more expensive options like the GSMK CryptoPhone and XCell Stealth Phone exist to ensure a higher level of communication security. Zimperium's enterprise solution for business groups is another corporate-level solution. For government agencies, the recently-announced ESD Overwatch system could potentially be a powerful firewall, if they do not already have their own detection systems in place.

Whilst IMSI catcher capabilities have certainly been expanding rapidly and IMSI catcher use is more widespread than previously suspected, given the rapid improvement in countermeasures, it seems that there will be ways to deal with IMSI catcher attacks, at least in the near future. In the meantime, the public release of information regarding the use and functionality of IMSI catchers will serve to improve efforts to establish reasonable countermeasures and to allay concerns of the general public over misuse of IMSI catchers.

6 APPENDIX

6.1 List of Federal Agencies known to use IMSI catchers

Federal Agencies:

- Federal Bureau of Investigation (FBI)
- Drug Enforcement Administration (DEA)
- U.S. Secret Service
- Immigration and Customs Enforcement (ICE)
- U.S. Marshals Service
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- U.S. Army
- U.S. Navy
- U.S. Marine Corps
- U.S. National Guard
- U.S. Special Operations Command
- National Security Agency (NSA)

6.2 XCell Technologies' Stealth Phone Prices and Capabilities

Special Features	XCell Basic	XCell Advanced	XCell Crypt	XCell Dynamic IMEI	XCell Dynamic IMEI v2
GSM Interceptor Proximity Alert	Yes	Yes	Yes	Yes	Yes
Call Interception Alert	Yes	Yes	Yes	Yes	Yes
Dynamic IMEI				Yes	Yes
A5 Change Alert (No/Change Encryption Alert)	Yes	Yes	Yes	Yes	Yes
UnPing (Localization Alert)					Yes
Channel Lock (ARFCN Lock)					Yes
Show TMSI					Yes
Clear Call Log					Yes
Voice Call Recording					Yes
Hunting Mode				Yes	Yes
Anti Interception Mode				Yes	Yes
SMS Encryption			Yes		
Forensic Bullet-Proof	Yes	Yes	Yes	Yes	Yes
Price	€400	€500	€600	€800	€800

6.3 Data Collection App source code snippet

The Data Collection App was initially written by graduate students involved in researching cell towers under Professor Nadia Heninger's guidance. In the spring 2015 semester, this author worked on debugging the app to allow stable data collection and adding functionality to the user interface, in order to embark on the first round of cell tower data collection in Philadelphia (see Section 4.5).

Below is a snippet from the `DataCollectionActivity.class` file of the Data Collection App, which manages the core function that collects information about cell towers in the vicinity whenever the mobile phone detects a change in signal strength.

```
// Check that min required time has elapsed since last data entry
timeElapsed = System.nanoTime() - lastCollectedTime;
if (timeElapsed >= delayNanoSec) {
    // Logs time since last data entry
    Log.d(COLLECTION, "Proceed - " +
            (float) timeElapsed/1000000000 +
            " sec since last entry");

    // Check that data collection count doesn't exceed maximum before collecting
    if (current_count_coll_json_obj < MAX_COLLECTIONS_JSON_OBJECTS) {
        StringBuffer display_string = new StringBuffer();
        List<NeighboringCellInfo> neighborList = telephonyManager
                .getNeighboringCellInfo();

        // Check that NeighboringCellInfo list is not empty
        if (neighborList != null) {
            // Report the number of NeighboringCellInfo objects received
            Log.d(COLLECTION, String.valueOf(neighborList.size()) +
                    " neighboring cells found.");

            // Process each NeighboringCellInfo packet
            for (int i = 0; i < neighborList.size(); i++) {
                NeighboringCellInfo neighboringCellInfo =
                        (NeighboringCellInfo) neighborList.get(i);

                // Print neighboring cell information to screen
                display_string.append("CID: "
                        + neighboringCellInfo.getCid()
                        + "  LAC: "
                        + neighboringCellInfo.getLac()
                        + "  PSC: "
                        + neighboringCellInfo.getPsc()
                        + "  RSSI: "
                        + neighboringCellInfo.getRssi()
                        + "\n\n");

                // Record transaction information to cell JSONObject
                JSONObject entry = new JSONObject();
                try {
                    // Add cell tower signal information to cell JSONObject
                    entry.put("cid",
                            neighboringCellInfo.getCid());
                    entry.put("lac",
                            neighboringCellInfo.getLac());
                    entry.put("psc",
                            neighboringCellInfo.getPsc());
                    entry.put("rssi",
                            neighboringCellInfo.getRssi());

                    // Add latitude longitude information to cell JSONObject
```

```
GPSTracker gps = new GPSTracker(
        DataCollectionActivity.this);
entry.put("latitude", gps.getLatitude());
entry.put("longitude",
        gps.getLongitude());

// Display latitude longitude information on screen
post_server_response_textview.setText("Data Collection In" +
        " Progress\n\n"
        + "Latitude: "
        + Double.toString(gps
        .getLatitude())
        + "\nLongitude: "
        + Double.toString(gps
        .getLongitude()));

// Add time information to cell JSONObject
Calendar c = Calendar.getInstance();
entry.put("time", c.getTimeInMillis());
//Log.d("time in millis", Long.toString(c
//      .getTimeInMillis()));

// Add cell JSONObject to array of cell JSONObjects
data_Array.put(entry);

// Increment count of cell JSONObjects
signal_strength_transactions++;

// If max number of cell JSONObjects per data collection
// is reached, record array of cell JSONObjects as a data
// collection and add to array of data collections; reset
if (signal_strength_transactions ==
        MAX_SIGNAL_STRENGTH_TRANSACTIONS) {
    // Create data collection to store cell JSONObjects
    JSONObject temp = new JSONObject();

    // Record Android ID to collection
    temp.put("id", Secure.getString(getBaseContext()
                    .getContentResolver(),
            Secure.ANDROID_ID));
    /*  Unnecessary - commented out
    String devId = Secure.getString(getBaseContext()
            .getContentResolver(),
            Secure.ANDROID_ID);
    Log.d("Dev ID: ", devId );
    */

    // Record cell JSONObjects to collection
    temp.put("information", data_Array);
    //Log.d("json data : ",temp.toString());

    // Check that max collections is not exceeded
    if (current_count_coll_json_obj < MAX_COLLECTIONS_JSON_OBJECTS) {
        // Add collection to array of collections
        collection_JSON_objects[current_count_coll_json_obj] =
                temp;
    }

    // Re-initialize the array to store cell JSONObjects
    data_Array = new JSONArray();

    // I don't know what this does yet
    data_display_textview
            .setText("found1");

    // Increment the count of collections
    current_count_coll_json_obj++;
```

```
                    // Reset count of cell JSONObjects
                    signal_strength_transactions = 0;

                    // If max number of cell JSONObjects per data collection
                    // has not yet been reached
                } else {
                    // Just do nothing?

                }

                // Display total transactions on screen
                count_textview.setText("Cell transactions received: "
                        + (MAX_SIGNAL_STRENGTH_TRANSACTIONS
                        * current_count_coll_json_obj
                        + signal_strength_transactions)
                        + "\nCell transactions ready to be sent: "
                        + MAX_SIGNAL_STRENGTH_TRANSACTIONS
                        * current_count_coll_json_obj
                        + "\nTotal transactions sent to server: "
                        + transactions_sent);

            } catch (JSONException e1) {
                // TODO Auto-generated catch block
                // e1.printStackTrace();
                data_display_textview
                        .setText("JSON Exception");
            }
        }

        // Print time elapsed since last data entry
        display_string.append(
                numberFormat.format((float) timeElapsed / 1000000000) +
                " sec since last data entry.");

        data_display_textview.setText(display_string
                .toString());

        // Record number of data collections to log
        Log.d(COLLECTION,
                current_count_coll_json_obj +
                        " data collections collected.");

        // Record number of cell JSONObjects to log
        Log.d(COLLECTION,
                (current_count_coll_json_obj
                        * MAX_SIGNAL_STRENGTH_TRANSACTIONS
                        + signal_strength_transactions)
                        + " cell transactions collected.");


        // Report empty NeighboringCellInfo list
    } else {
        Log.d(COLLECTION, "Empty NeighboringCellInfo list.");
    }

// If data collection count exceeds maximum
} else {    // current_count_coll_json_obj >= MAX_COLLECTIONS_JSON_OBJECTS
    // If existing data connection
    if (isConnectedToNw()) {

        // Only send if data has been collected
        if (current_count_coll_json_obj > 0) {
            try {
                // send all the collected data one by one
                spinner.setVisibility(View.VISIBLE);
                post_server_response_textview
```

```
                        .setText("Data sending in progress ...");
                for (int i = 0; i < current_count_coll_json_obj; i++) {
                    NetworkAsyncTask nat = new NetworkAsyncTask(
                            DataCollectionActivity.this,
                            collection_JSON_objects[i],
                            DataCollectionActivity.this);
                    nat.execute(SERVER_URL);

                    // Increment count of sent transactions
                    transactions_sent += MAX_SIGNAL_STRENGTH_TRANSACTIONS;
                }

                // Reset counter
                current_count_coll_json_obj = 0;

                // Reset data collections
                collection_JSON_objects =
                        new JSONObject[MAX_COLLECTIONS_JSON_OBJECTS];

            } catch (Exception e) {
                // TODO: handle exception
                Log.d(SENDING, "Failed to send data to server.");
                post_server_response_textview
                        .setText("Error sending data to server");
            }
            // If no data has been collected, print error message.
        } else {
            Log.d(SENDING, "No data collected yet.");
            post_server_response_textview
                    .setText("No data collected yet.");
        }

        // If no existing data connection, print error message
    } else {
        Context context = getApplicationContext();
        CharSequence text = "Check the Internet connection and try again";
        int duration = Toast.LENGTH_SHORT;
        Toast toast = Toast.makeText(context, text, duration);
        toast.show();
    }

    Log.d(COLLECTION, "Halted; max data collection limit reached.");

    data_display_textview
            .setText("Exceeded the maximum amount of data that can " +
                    "be stored on the phone");
}

// Reset data entry timestamp
 lastCollectedTime = System.nanoTime();

}
```

WORKS CITED

[1] AT&T Tech Channel, "Testing the First Public Cell Phone Network," [Online]. Available: http://techchannel.att.com/play-video.cfm/2011/6/13/AT&T-Archives-AMPS:-coming-of-age. [Accessed 28 April 2015].

[2] W. R. Young, "AMPS: Introduction, Background, and Objectives," *Bell System Technical Journal*, vol. 58, no. 1, pp. 1-14, 1979.

[3] D. Matuszewski, "GSM Security," Instituto de Matemática e Estatística, Universidade de São Paulo, 2012.

[4] K. R. Poranki, Y. Perwej and A. Perwej, "The Level of Customer Satisfaction related to GSM in India," *Research Journal of Science & IT Management*, vol. 4, no. 3, pp. 30-36, 2015.

[5] World Time Zone, "GSM," [Online]. Available: http://www.worldtimezone.com/gsm.html. [Accessed 28 April 2015].

[6] International Telecommunication Union, "About mobile technology and IMT-2000," 4 April 2011. [Online]. Available: https://www.itu.int/osg/spu/imt-2000/technology.html. [Accessed 28 April 2015].

[7] Engineers Garage, "Difference between 2G and 3G Technology," [Online]. Available: http://www.engineersgarage.com/contribution/difference-between-2g-and-3g-technology#. [Accessed 28 April 2015].

[8] T. Bradley, "GSM Phone Hack FAQ: What You Should Know," PCWorld, 1 August 2010. [Online]. Available: http://www.pcworld.com/article/202317/gsm_phone_hack_faq_what_you_should_know.html. [Accessed 28 April 2016].

[9] D. Strobel, "IMSI Catcher," Ruhr-Universität Bochum, 2007.

[10] 3GPP, "Specifications," [Online]. Available: http://www.3gpp.org/specifications/79-specification-numbering. [Accessed 28 April 2015].

[11] A. Biryukov, A. Shamir and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," in *Fast Software Encryption*, Springer Berlin Heidelberg, 2001, pp. 1-18.

[12] GSM Arena, "GPRS," [Online]. Available: http://www.gsmarena.com/glossary.php3?term=gprs. [Accessed 28 April 2015].

[13] GSM Arena, "EDGE (Enhanced Data for Global Evolution)," [Online]. Available: http://www.gsmarena.com/glossary.php3?term=edge. [Accessed 28 April 2015].

[14] BBC News, "First 3G mobiles launched in Japan," 1 October 2001. [Online]. Available: http://news.bbc.co.uk/2/hi/business/1572372.stm. [Accessed 28 April 2015].

[15] Mobithinking, "Global mobile statistics 2014 Part B: Mobile Web; mobile broadband penetration; 3G/4G subscribers and networks; mobile search," MobiForge, 2 May 2014. [Online]. Available: http://mobiforge.com/research-analysis/global-mobile-statistics-2014-part-b-mobile-web-mobile-broadband-penetration-3g4g-subscribers-and-ne. [Accessed 28 April 2015].

[16] S. Tindal, "Telstra boosts Next G to 21Mbps," ZDNet, 8 December 2008. [Online]. Available: http://www.zdnet.com/article/telstra-boosts-next-g-to-21mbps/. [Accessed 28 April 2015].

[17] I. Poole, "EV-DO Rev. B," RadioElectronics.com, [Online]. Available: http://www.radio-electronics.com/info/cellulartelecomms/3gpp2/cdma2000-1xevdo-rev-b.php. [Accessed 28 April 2015].

[18] K. Nohl, "Mobile Self-defense (SnoopSnitch)," Chaos Computer Security Conference 2014, 28 December 2014. [Online]. Available: http://searchnetworking.techtarget.com/definition/Signaling-System-7. [Accessed 27 April 2015].

[19] O. Dunkelman, N. Keller and A. Shamir, "A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony," *IACR Cryptology ePrint Archive*, p. 13, 2010.

[20] U. Meyer and S. Wetzel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, 2004.

[21] International Telecommunication Union, "Requirements related to technical performance for IMT-Advanced radio interface(s)," [Online]. Available: http://www.itu.int/pub/R-REP-M.2134-2008/en. [Accessed 28 April 2015].

[22] 3GPP, "LTE," [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte. [Accessed 28 April 2015].

[23] Radio Electronics, "IEEE 802.16 WiMAX standards," [Online]. Available: http://www.radio-electronics.com/info/wireless/wimax/ieee-802-16-standards.php. [Accessed 28 April 2015].

[24] International Telecommunication Union, "ITU World Radiocommunication Seminar highlights future communication technologies," 6 December 2010. [Online]. Available: http://www.itu.int/net/pressoffice/press_releases/2010/48.aspx#.VT81-SFViko. [Accessed 28 April 2015].

[25] D. Murphy, "Spring to Scrap WiMAX by Late 2015," PC, 11 October 2014. [Online]. Available: http://www.pcmag.com/article2/0,2817,2470209,00.asp. [Accessed 28 April 2015].

[26] CNN Money (New York), "FBI lets suspects go to protect 'Stingray' secrets," CNN, 18 March 2015. [Online]. Available: http://money.cnn.com/2015/03/18/technology/security/police-stingray-phone-tracker/. [Accessed 28 April 2015].

[27] A. Dabrowski, M. Mulazzani, N. Pianta, E. Weippl and T. Klepp, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014.

[28] H. Federrath, "Protection in Mobile Communications," in *Multilateral Security in Communications*, Addison-Wesley-Longman, 1999, pp. 349-364.

[29] U. Meyer and S. Wetzel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS netowrks," *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, vol. 4, pp. 2876-2883, 2004.

[30] "A5/1 Decryption," [Online]. Available: https://opensource.srlabs.de/projects/a51-decrypt/files. [Accessed 28 April 2015].

[31] 3GPP, [Online]. Available: http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip.

[32] J. Valentino-Devries, "'Stingray' Phone Tracker Fuels Constitutional Clash," The Wall Street Journal, 22 September 2011. [Online]. Available: http://www.wsj.com/articles/SB10001424053111904194604576583112723197574. [Accessed 28 April 2015].

[33] S. K. Pell and C. Soghoian, "A Lot More Than A Pen Register, and Less than A Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities," 2014.

[34] R. Gallagher, "Meet the machines that steal your phone's data," Ars Technica, 25 September 2013. [Online]. Available: http://arstechnica.com/tech-policy/2013/09/25/meet-the-machines-that-steal-your-phones-data/. [Accessed 28 April 2015].

[35] D. Barrett, "Americans' Cellphones Targeted in Secret U.S. Spy Program," The Wall Street Journal, 13 November 2014. [Online]. Available: http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533. [Accessed 28 April 2015].

[36] D. Priest, "NSA growth fueled by need to target terrorists," The Washington Post, 21 July 2013. [Online]. Available: http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html. [Accessed 28 April 2015].

[37] CNN Money, "How the NSA can 'turn on' your phone remotely," CNN, 6 June 2014. [Online]. Available: http://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/. [Accessed 28 April 2015].

[38] R. Gallagher, "Criminals May Be Using Covert Mobile Phone Surveillance Tech for Extortion," Slate, 22 August 2012. [Online]. Available: http://www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_enforcement_using_high_tech_portable_devices_to_intercept_communications_.html. [Accessed 28 April 2015].

[39] M. Keys, "FCC FOIA: StingRay, KingFish User Manual (2010)," TheBlot Magazine, 25 March 2015. [Online]. Available: http://www.scribd.com/doc/259987684/FCC-FOIA-StingRay-KingFish-User-Manual-2010. [Accessed 28 April 2015].

[40] Digital Receiver Technologies, Inc., "DRT Company History," [Online]. Available: http://www.drti.com/about_print.htm. [Accessed 28 April 2015].

[41] Meganet Corporation, "Meganet Products - Cell Phone Interceptors," [Online]. Available: http://www.meganet.com/meganet-products-cellphoneinterceptors.html. [Accessed 27 April 2015].

[42] Gamma Group, "Gamma Group," [Online]. Available: https://www.gammagroup.com/. [Accessed 28 April 2015].

[43] D. Goodin, "The body-worn "IMSI catcher" for all your covert phone snooping needs," ArsTechnica, 1 September 2013. [Online]. Available:

http://arstechnica.com/security/2013/09/01/the-body-worn-imsi-catcher-for-all-your-covert-phone-snooping-needs/. [Accessed 28 April 2015].

[44] Septier, "Septier IMSI Catcher," [Online]. Available: http://www.septier.com/146.html. [Accessed 28 April 2015].

[45] PKI, "3G UMTS IMSI Catcher," [Online]. Available: http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/. [Accessed 28 April 2015].

[46] maninthemiddle100, "GSM Cell Phone Interception 1," 10 Mar 2010. [Online]. Available: https://www.youtube.com/watch?v=o6aKuDSg_CQ. [Accessed 28 April 2015].

[47] A. Rosenblum, "MYSTERIOUS PHONY CELL TOWERS COULD BE INTERCEPTING YOUR CALLS," Popular Science, 27 August 2014. [Online]. Available: http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls. [Accessed 28 April 2015].

[48] A. Soltani and C. Timberg, "Tech firm tries to pull back curtain on surveillance efforts in Washington," 17 September 2014. [Online]. Available: http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html. [Accessed 28 April 2015].

[49] B. Levine, "Spy cell towers: A new service is hunting for you," VentureBeat, 26 March 2015. [Online]. Available: http://venturebeat.com/2015/03/26/spy-cell-towers-a-new-hunting-service-is-looking-for-you/. [Accessed 27 April 2015].

[50] K. Zetter, "Florida Cops' Secret Weapon: Warrantless Cellphone Tracking," Wired, 3 March 2014. [Online]. Available: http://www.wired.com/2014/03/stingray/. [Accessed 28 April 2015].

[51] K. Zetter, "Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight," Wired, 9 April 2013. [Online]. Available: http://www.wired.com/2013/04/verizon-rigmaiden-aircard/. [Accessed 28 April 2015].

[52] American Civil Liberties Union, "Stingray Tracking Devices: Who's Got Them?," [Online]. Available: https://www.aclu.org/map/stingray-tracking-devices-whos-got-them. [Accessed 28 April 2015].

[53] K. Klonick, "Stingrays: Not Just for Feds!," Slate, 10 November 2014. [Online]. Available: http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.html. [Accessed 28 April 2015].

[54] "Looks like Chicago PD had a stingray out at the Eric Garner protest last night," 5 December 2014. [Online]. Available: https://privacysos.org/node/1609.

[55] "CPD possible Stingray use at #BrownFriday protest," [Online]. Available: https://clyp.it/sv23cozu. [Accessed 27 April 2015].

[56] N. F. Wessler, "Police Hide Use of Cell Phone Tracker From Courts Because Manufacturer Asked," American Civil Liberties Union, 3 March 2014. [Online]. Available: https://www.aclu.org/blog/police-hide-use-cell-phone-tracker-courts-because-

manufacturer-asked?redirect=blog/national-security-technology-and-liberty/police-hide-use-cell-phone-tracker-courts-because. [Accessed 28 April 2015].

[57] K. Zetter, "NY Cops Used ‘Stingray’ Spy Tool 46 Times Without Warrant," Wired, 7 April 2015. [Online]. Available: http://www.wired.com/2015/04/ny-cops-used-stingray-spy-tool-46-times-without-warrant/. [Accessed 28 April 2015].

[58] C. Farivar, "Non Disclosure Agreement," Ars Technica, [Online]. Available: https://www.documentcloud.org/documents/1727748-non-disclosure-agreement.html#document/p3/a212440. [Accessed 28 April 2015].

[59] J. Glenza and N. Woolf, "Stingray spying: FBI's secret deal with police hides phone dragnet from courts," The Guardian, 10 April 2015. [Online]. Available: http://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police. [Accessed 28 April 2015].

[60] M. Geuss, "Cops hid use of phone tracking tech in court documents at feds’ request," Ars Technica, 20 June 2014. [Online]. Available: http://arstechnica.com/tech-policy/2014/06/19/cops-hid-use-of-phone-tracking-tech-in-court-documents-at-feds-request/. [Accessed 28 April 2015].

[61] J. Stone, "Washington Stingray Bill Demands Police Obtain Warrant Before Deploying Phone Tracker," International Business Times, 27 April 2015. [Online]. Available: http://www.ibtimes.com/washington-stingray-bill-demands-police-obtain-warrant-deploying-phone-tracker-1898166. [Accessed 28 April 2015].

[62] C. Farivar, "California bill requires warrant for stingray use," Ars Technica, 25 March 2015. [Online]. Available: http://arstechnica.com/tech-policy/2015/03/25/california-bill-requires-warrant-for-stingray-use/. [Accessed 28 April 2015].

[63] S. Nelson, "Utah May Ban Warrantless Use of 'Stingray' Devices," US News, 4 March 2014. [Online]. Available: http://www.usnews.com/news/articles/2014/03/04/utah-may-ban-warrantless-use-of-stingray-devices. [Accessed 28 April 2015].

[64] Cushing, Tim, "FBI Says It Has A Warrant Requirement For Stingray Use; Has Exception Broad Enough To Ensure It Never Needs A Warrant," Tech Dirt, 6 January 2015. [Online]. Available: https://www.techdirt.com/articles/20150105/12590129600/fbi-says-it-has-warrant-requirement-stingray-use-has-exception-broad-enough-to-ensure-it-never-needs-warrant.shtml. [Accessed 28 April 2015].

[65] H. Murphy, "The New York Times," The New York Times, 22 January 2014. [Online]. Available: http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/?action=click&contentCollection=Europe&module=RelatedCoverage&region=Marginalia&pgtype=article&_r=3&gwh=66F66BFA4C84D20C5C976374F4. [Accessed 27 April 2015].

[66] M. Rachkevych, "Kyiv Post," Kyiv Post, 21 January 2014. [Online]. Available: http://www.kyivpost.com/content/kyiv/mobile-phone-providers-deny-sending-text-messages-to-euromaidan-participants-335349.html. [Accessed 27 April 2015].

[67] L. Franceschi-Bicchierai, "Mashable," Mashable, 21 January 2014. [Online]. Available: http://mashable.com/2014/01/21/kiev-protesters-text-message/. [Accessed 27 April 2015].

[68] C. Timberg, "Feds to study illegal use of spy gear," The Washington Post, 11 August 2014. [Online]. Available: http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/11/feds-to-study-illegal-use-of-spy-gear/. [Accessed 28 April 2015].

[69] Federal Communications Commission, "CDBS Public Access," Federal Communications Commission, [Online]. Available: http://licensing.fcc.gov/prod/cdbs/pubacc/prod/cdbs_pa.htm. [Accessed 27 April 2015].

[70] Ability Computers and Software Industries Ltd., "3G Interception," [Online]. Available: https://wikileaks.org/spyfiles/files/0/80_ABILITY-GSM_3G_Intercept.pdf. [Accessed 27 April 2015].

[71] Gamma Group, "3G-GSM Interception & Target Location," [Online]. Available: https://info.publicintelligence.net/Gamma-GSM.pdf. [Accessed 27 April 2015].

[72] SecUpwN, "Changing LAC on same CID #91," [Online]. Available: https://github.com/SecUpwN/Android-IMSI-Catcher-Detector/issues/91. [Accessed 28 April 2015].

[73] GSMK, "GSMK CryptoPhone," [Online]. Available: http://www.cryptophone.de/en/. [Accessed 28 April 2015].

[74] A. Boxall, "Paranoid much? Demand for secure CryptoPhone is so high, company can't keep up," Digital Trends, 20 March 2014. [Online]. Available: http://www.digitaltrends.com/mobile/cryptophone-demand-exceeds-supply/. [Accessed 28 April 2015].

[75] K. Zetter, "Phone Firewall Identifies Rogue Cell Towers Trying to Intercept Your Calls," 3 September 2014. [Online]. Available: http://www.wired.com/2014/09/cryptophone-firewall-identifies-rogue-cell-towers/. [Accessed 28 April 2015].

[76] XCell Technologies, "XCell Technologies," [Online]. Available: http://x-cellular.com/index.html. [Accessed 27 April 2015].

[77] SGP Technologies, "Blackphone," [Online]. Available: https://blackphone.ch/. [Accessed 28 April 2015].

[78] S. Knight, "Privacy-centric Blackphone now shipping to pre-order customers," Techspot, 30 June 2014. [Online]. Available: http://www.techspot.com/news/57266-privacy-centric-blackphone-now-shipping-to-pre-order-customers.html. [Accessed 28 April 2015].

[79] T. Maytom, "Shipping Starts on Blackphone, World's First Privacy-Optimised Smartphone," Mobile Marketing, 30 June 2014. [Online]. Available: http://mobilemarketingmagazine.com/shipping-starts-on-blackphone-first-privacy-optimised-smartphone. [Accessed 28 April 2015].

[80] J. Kopstein, "A Phone for the Age of Snowden," New Yorker, 30 January 2014. [Online]. Available: http://www.newyorker.com/tech/elements/a-phone-for-the-age-of-snowden. [Accessed 28 April 2015].

[81] L. Armasu, "Fake Cell Towers Could Be Attacking Your Cellphone Up To 80-90 Times Per Hour," Tom's Hardware, 2 September 2014. [Online]. Available: http://www.tomshardware.com/news/cryptophone-gsmk-esd-baseband-firewall,27585.html. [Accessed 28 April 2015].

[82] A. Greenberg, "There's Now a Free iPhone App That Encrypts Calls and Texts," Wired, 2 March 2015. [Online]. Available: http://www.wired.com/2015/03/iphone-app-encrypted-voice-texts/. [Accessed 28 April 2015].

[83] Security Research Labs, "SnoopSnitch," [Online]. Available: https://opensource.srlabs.de/projects/snoopsnitch. [Accessed 27 April 2015].

[84] J. Scharr, "Android App Stops Smartphone Spies," Tom's Guide, 2 January 2015. [Online]. Available: http://www.tomsguide.com/us/android-snoop-snitch-stingrays,news-20086.html. [Accessed 27 April 2015].

[85] "GSM Security Map," [Online]. Available: http://gsmmap.org/.

[86] OsmocomBB, "OsmocomBB - Phones," [Online]. Available: http://bb.osmocom.org/trac/wiki/Hardware/Phones. [Accessed 27 April 2015].

[87] SecUpwN, "AIMSICD Wiki Home," [Online]. Available: https://github.com/SecUpwN/Android-IMSI-Catcher-Detector/wiki. [Accessed 27 April 2015].

[88] SecUpwN, "AIMSICD Development Status," [Online]. Available: https://github.com/SecUpwN/Android-IMSI-Catcher-Detector/wiki/Development-Status. [Accessed 27 April 2015].

[89] Darshak, "Darshakframework," [Online]. Available: https://github.com/darshakframework/darshak. [Accessed 27 April 2015].

[90] Aalto University, "A new app reveals if a phone is at risk of being hacked," 25 June 2014. [Online]. Available: http://sci.aalto.fi/En/current/current_archive/news/2014-06-25/. [Accessed 27 April 2015].

[91] J. Warren, "Github - Spidey," [Online]. Available: https://github.com/jtwarren/spidey. [Accessed 27 April 2015].

[92] Zimperium Mobile Security, "Zimperium Mobile Security - Products," [Online]. Available: https://www.zimperium.com/zips-mobile-ips. [Accessed 27 April 2015].

[93] A. Williams, "Zimperium Raises $8M For Mobile Security That Turns The Tables On Attackers," TechCrunch, 20 December 2013. [Online]. Available: http://techcrunch.com/2013/12/20/zimperium-raises-8m-for-mobile-security-that-turns-the-tables-on-attackers/. [Accessed 27 April 2015].

[94] Zimperium Mobile Security, "Zimperium Launches First-Ever iOS Security Solution That Protects Employees' Devices From Cyberattacks Wherever They Go," 31 July 2014. [Online]. Available: https://www.zimperium.com/press-zimperium-launches-first-ever-ios-solution. [Accessed 27 April 2015].

[95] Pwnie Express, "Pwnie Express – Cell Network Threat Detection Announcement," 20 April 2015. [Online]. Available: https://www.pwnieexpress.com/pwnie-express-cell-network-threat-detection-announcement/. [Accessed 28 April 2015].

[96] D. A. Sokolov, "Digitale Selbstverteidigung mit dem IMSI-Catcher-Catcher," Heise Forums, 27 August 2014. [Online]. Available: http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html. [Accessed 27 April 2015].

[97] Woazboat, [Online]. Available: https://github.com/Woazboat/portable-imsi-catcher-detector. [Accessed 27 April 2015].

[98] ESD America, "ESD America," [Online]. Available: http://esdamerica.com/. [Accessed 27 April 2015].

[99] CCCen, "GSM: SRSLY? [26C3]," 3 January 2012. [Online]. Available: https://www.youtube.com/watch?v=9K4EDAF5OlM. [Accessed 28 April 2015].

[100] Telstra, "It's time to say goodbye old friend," 23 July 2014. [Online]. Available: http://exchange.telstra.com.au/2014/07/23/its-time-to-say-goodbye-old-friend/. [Accessed 28 April 2015].

[101] JMA Wireless, "Grading the top 8 U.S. wireless carriers in the fourth quarter of 2014," 3 March 2015. [Online]. Available: http://www.fiercewireless.com/special-reports/grading-top-us-wireless-carriers-fourth-quarter-2014. [Accessed 28 April 2015].

[102] AT&T, "It's time to develop a migration plan for M2M," [Online]. Available: http://www.business.att.com/enterprise/Family/mobility-services/machine-to-machine/m2m-applications/cd2migration/page=addl-info/. [Accessed 28 April 2015].

[103] GigaOM, "T-Mobile may be sunsetting 2G, but its M2M biz keeps growing," 12 June 2012. [Online]. Available: https://gigaom.com/2012/06/12/t-mobile-may-be-sunsetting-2g-but-its-m2m-biz-keeps-growing/. [Accessed 28 April 2015].

[104] M. Rouse, "Signaling System 7 (SS7)," Tech Target, April 2005. [Online]. Available: http://searchnetworking.techtarget.com/definition/Signaling-System-7. [Accessed 27 April 2015].

[105] C. Farivar, "Cities scramble to upgrade "stingray" tracking as end of 2G network looms," Ars Technica, 1 September 2014. [Online]. Available: http://arstechnica.com/tech-policy/2014/09/01/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/. [Accessed 28 April 2015].

[106] Martone Radio Technology, "MRT - Products," [Online]. Available: http://zblgeo.com/content/products/. [Accessed 28 April 2015].

[107] DEFCON Conference, "DEF CON 18 - Chris Paget - Practical Cellphone Spying," 13 November 2013. [Online]. Available: https://www.youtube.com/watch?v=fQSu9cBaojc. [Accessed 28 April 2015].

[108] GSMK, "GSMK CryptoPhone - Products," [Online]. Available: http://www.cryptophone.de/en/products/. [Accessed 28 April 2015].

[109] K. Klonick, "Stingrays: Not Just for Feds!," Slate, 10 November 2014. [Online]. Available: http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.html. [Accessed 28 April 2015].