IMSI-Catch Me If You Can: IMSI-Catcher-Catchers

Adrian Dabrowski
SBA Research
Vienna, Austria
adabrowski@sba-research.org

Nicola Pianta
Università di Cagliari
Cagliari, Italy
nicola.pianta@gmail.com

Thomas Klepp
Vienna University of Technology
thomas.klepp@student.tuwien.ac.at

Martin Mulazzani
SBA Research
Vienna, Austria
mmulazzani@sba-research.org

Edgar Weippl
SBA Research
Vienna, Austria
eweippl@sba-research.org

ABSTRACT

IMSI Catchers are used in mobile networks to identify and eavesdrop on phones. When, the number of vendors increased and prices dropped, the device became available to much larger audiences. Self-made devices based on open source software are available for about US$ 1,500.

In this paper, we identify and describe multiple methods of detecting artifacts in the mobile network produced by such devices. We present two independent novel implementations of an *IMSI Catcher Catcher* (ICC) to detect this threat against everyone's privacy. The first one employs a network of stationary (sICC) measurement units installed in a geographical area and constantly scanning all frequency bands for cell announcements and fingerprinting the cell network parameters. These rooftop-mounted devices can cover large areas. The second implementation is an app for standard consumer grade mobile phones (mICC), without the need to *root* or *jailbreak* them. Its core principle is based upon geographical network topology correlation, facilitating the ubiquitous built-in GPS receiver in today's phones and a network cell capabilities fingerprinting technique. The latter works for the vicinity of the phone by first learning the cell landscape and than matching it against the learned data. We implemented and evaluated both solutions for digital self-defense and deployed several of the stationary units for a long term field-test. Finally, we describe how to detect recently published denial of service attacks.

1. INTRODUCTION

IMSI Catchers are MITM (man in the middle) devices for cellular networks [20]. Originally developed to steal IMSI (International Mobile Subscriber Identity) numbers from nearby phones (hence the name), later versions offered call- and message interception. Today, IMSI Catchers can also be used to track handsets, intercept mobile two-factor authentication schemes (mTAN), geo-targeted spam [24], send operator messages that reconfigure the phone (e.g. installing a permanent MITM by setting a new APN, http-proxy, or attack the management interface [32]), or attack SIM cards with encrypted SMS [26] that are filtered by most operators by now.

In brief, these devices exploit the phone's behavior to prefer the strongest cell phone tower signal in vicinity to maximize the signal quality and minimize its own power consumption. Additionally, on GSM networks (2G), only the phone (via the SIM, Subscriber Identification Module) needs to authenticate to the network but not vice versa and therefore can easily be deluded to disable content data encryption. This enables an attacker to answer a phone's requests as if the phone was communicating with a legitimate cell phone network.

In contrast, the Universal Mobile Telecommunication System (UMTS, 3G) requires mutual two-way authentication, but can be circumvented using the GSM compatibility layer present in most networks [23], or mobiles can be forced to downgrade to a 2G connection by other means. Additionally, network operators use GSM as a fallback network where UMTS is not available. This makes GSM security still relevant and important in today's mobile network world.

The contributions we like to highlight are:

- Survey of network level artifacts caused by an IMSI Catcher. (Section 4).
- Concept of a usable and customer grade warning system (Section 5).
- Determination of which detection methods are available and implementable with what consumer grade hardware (Section 6).
- Implementation and evaluation of these methods (Section 7).
- Detectability of large scale denial of service attacks such as [17] (Section 9.1).

2. MOTIVATION

The first IMSI Catchers date back as early as 1993 [31] and were big, heavy, and expensive. Only a few manufacturers existed and the economic barrier limited the device's use mostly to governmental agencies. However, in recent years, a number of smaller and cheaper as well as self-built projects appeared making cellular network snooping attacks feasible to much larger audiences.

This paper is a pre-print of a paper to appear at ACSAC 2014, December 8-12, New Orleans.

ACSAC XXXXXXX XXXXXXXXXXX XXXXX

Chris Paget built an IMSI Catcher for about US$1,500 [12] and presented it at DEFCON 2010. His setup consists of a *Software Defined Radio* [15] and free open source software such as GNU Radio, OpenBTS, and Asterisk. Several other (academic) projects also built such devices [29, 36] based on similar setups. Appropriate patches and configuration guides are publicly available.

In 2010, Nohl and Manaut [25, 27] presented practical snooping attacks on GSM's main cipher suite using custom firmware on modified mobile phones. However, such a solution can only monitor a very small number of frequencies at once and is likely to lose the intercepted phone on handovers to other cells. Therefore, a professional attacker will still use IMSI Catcher-like functionality to lock the radio channel.

As IMSI Catchers perform an active radio attack, we put forward multiple passive ways to detect such an attack, both stationary and mobile. We facilitated ordinary mobile phones or easily acquirable hardware. This allows for easy deployment of the described techniques for end users or interested hobbyists. We therefore intentionally chose to exclude expensive protocol analyzers or complex self-built solutions.

3. BACKGROUND

In general a mobile network consists of *base stations* (BS) that use one or more radio interfaces to create geographically limited radio *cells*. Multiple cells of an operator are grouped to *Location Areas*. After power-up or when a *mobile station* (MS, e.g. phone, data modem) lost connection to its network, it will perform a *full scan* to find the frequencies of nearby cells based on *beacon* signals sent out by every cell on a regular basis. The MS registers into the operators network using its worldwide unique *International Mobile Equipment Identity* (IMEI), its *International Mobile Subscriber Identity* (IMSI) number and a secret key stored on the *Subscriber Identity Module* (SIM). The network (in this example GSM) will assign a *Temporarily Mobile Subscriber Identity* (TMSI) number for addressing purposes. TMSIs are volatile and therefore reduce the risk of tracking individual subscribers. The more often a network changes the TMSI, the harder it is to passively track a specific user. Regardless, the network needs to know where its subscribers are at any given time to be able to communicate with them, e.g. forward incoming calls. In order to reduce position updates (saves network traffic and battery power on the mobile phone), updates are only performed when a phone moves from one group of cells (*Location*) to another, i.e. not on every individual cell. In case of an incoming message, the phone is *paged* in all cells of a *Location Area* (LA) and then assigned a specific logical channel of a cell. Based on the network's generation, this is either a frequency and a time slot (2G GSM) or an encoding scheme (3G UMTS).

To help the phone keep track of nearby cells, the network advertises them to the phone. Therefore, the scan overhead is reduced compared to full scans, saving time and battery. The phone maintains a short *neighbor list* based on signal strength and reports them back to the network on request. This data is the primary decision source for *handovers*, when the phone needs to change to another cell during an active call.

In GSM, a cell is uniquely identified by the mobile country code (MCC), network code (MNC), location area code (LAC) and the cell ID (CI). The neighbor list typically includes additional per cell attributes like the frequency (ARFCN) and channel quality metrics. Given that UMTS networks are organized differently, LAC and CI are replaced by PSC (primary scrambling code) and CPI (Cell Parameter ID). For the sake of simplicity, we will call any tuple that uniquely identifies a network cell a *Global Cell ID* or *Cell ID* for short.

IMSI Catchers blend into the mobile network operator's infrastructure impersonating a valid cell tower and therefore attracting nearby phones to register to it. Two main operating modes can be distinguished.

Identification Mode.

As a phone is lured into the fake cell, the worldwide unique identifiers such as IMSI and IMEI are retrieved and the phone is sent back to its original network via denying its original *Location Update Request* with an *Location Update Reject*-Message. This procedure typically takes less then two seconds, whereas attracting the phone can take minutes. No other information besides the identification numbers is retrieved.

A law enforcement agency can then apply for a warrant and access the call- and meta information of a subject via the mobile network operator. This considerably saves the agency working hours, as no one has to operate the IMSI Catcher over the whole period of observation and follow the subject in its every move.

Other attackers can use this mode for tracking purposes or to lookup the exact phone model based on the IMEI to better tailor future attacks.

Camping Mode.

The phone is held in the cell of the IMSI Catcher and content data is collected. Traffic is forwarded to the genuine network so that the victim stays unaware of the situation.

IMSI Catcher users that do not have time for for a warrant or can't acquire a warrant (e.g. because they operate outside the law) use this method. It will also gain importance as A5/3 and A5/4 are introduced into GSM networks, making passive snooping attacks on the broken A5/1 and A5/2 ciphers useless. In UMTS networks, phones are additionally downgraded to GSM and its less secure ciphers.

4. IMSI CATCHER ARTIFACTS AND DETECTABILITY

An IMSI Catcher has many detail problems to overcome; the respective solutions will typically introduce irregularities in the network layer that leave hints for an educated observer. Due to the secret nature of the operation of these devices, not much information is available. Nevertheless, we generated the list below based on the material available and our own research. Some of the traits can be mitigated but most are of structural nature. However, not every IMSI Catcher will produce all of the artifacts described below.

4.1 Choosing a Frequency

To increase signal quality, avoid radio interference, and thus detection through the mobile provider's own radio quality monitoring system, an attacker has to use an unused frequency (i.e. ARFCN, Absolute Radio Frequency Channel Number) for its IMSI Catcher. A relatively safe choice for a frequency are unallocated radio channels (e.g. *guard channels* between different operators or reserved channels for

testing). However, it is less likely to lure a mobile phone onto this channel, as the phone (MS) will preferably only look on the advertised neighbor frequencies. Another method is to use an advertised frequency that is actually not being used or is not receivable in the specific geographical area under attack.
Detectability: Off-band frequency usage can be detected using a current frequency band plan as assigned by the local authorities. Radio regulatory bodies and frequency plans are available for almost all countries.

4.2 Choosing a Cell ID

Typically, an attacker will introduce a new cell ID (preferable including a new LAC) previously unused in the specific geographical region for two reasons: First, to not provoke an accidental protocol mismatch when the MS should receive the corresponding genuine BS by accident. Secondly, to provoke a *Location Update Request*[1] from the phone to be able to lure it in the fake cell.
Detectability: Our data shows, that cell IDs are very static. Many mobile operating systems use them together with Cell ID databases to coarsely estimate the phone's location where either GPS is unavailable, rough estimations are detailed enough, or to aid the GPS receiver during initialization. Using such a database and correlating its information with the real geographic location could reveal unusual cell IDs and frequency usage in a specific area.

4.3 Base Station Capabilities Fingerprinting

Each beacon signal of a base station is accompanied by a list of supported features (e.g. packet radio services such as GPRS or EDGE). If the attacker does not copy the capabilities of the original network precisely, the simulated cell will not provide all services like the original network. For example GPRS and EDGE are services that need very complex emulation layers. We don't expect many IMSI Catchers to support these protocols.
Detectability: A MS should denote such capabilities in the above Cell ID database (or a local one) and use them to find suspicious base stations not matching their previously known capabilities. Cell capabilities change very rarely, and if so, the network operator usually upgrades to new systems (e.g. GPRS to EDGE, HSDPA to HSUPA), but not vice versa.

4.4 Network Parameter Fingerprinting

Another information conveyed by the beacon signals to the mobile station are basic network parameters about the organization of the mobile network such as time slot organization, threshold values and timeout values. While they can differ from base station to base station, our research has shown that most of them tend to be uniform across a given network operator but vary between different operators. A IMSI Catcher operator might not always copy all of these parameters as they are not operationally important for an attack. Detection possible as described above (Section 4.3).

4.5 Forcing a MS to Register

Despite providing the better signal and simply waiting for a victim to voluntarily switch cells, an attacker can actively step in. An easy way to force a victim|s device to disconnect from the original network and register to a new (possible) fraudulent base station (as provided by the IMSI Catcher) is an RF jammer. After a fruitless scan of the advertised neighbor frequencies the phone eventually falls back to a full scan, therefore giving the IMSI Catcher the opportunity to attract the phone.

Several companies [8, 16] offer systems for targeted jamming of a specific phone.
Detectability: Jamming can be detected by a MS by watching channel noise levels (e.g. from the neighbor list).

4.6 Handling UMTS Clients

One possible way is to downgrade an UMTS capable MS to the less secure GSM network by rendering UMTS channels useless with an RF jammer (as above). Meyer and Wetzel [23] presented another way: a MITM attack for UMTS networks which facilitates its GSM compatibility layer. This layer is present in most deployed UMTS networks, as they use GSM for backward compatibility and to increase the coverage. Additionally, some companies [8, 16] claim, their equipment can transfer single targets from UMTS to GSM.
Detectability: Jamming can be detected as described above. A cell database can be used to spot unclaimed GSM usage where UMTS should be typically available.

4.7 Encryption

Older IMSI Catchers are likely to disable encryption (set cipher mode A5/0) in order to ease monitoring. However, current state-of-the-art attacks on GSM A5/1 and A5/2 cipher allow for a timely decryption and key recovery. Weaknesses found in the A5/2 cipher [11] have lead to its abolition by the GSM Association in 2006 [4]. However, the stronger variant A5/1 is also prone to precomputation attacks using rainbow tables. These are publicly available [6] and allow computers with a 2 TB hard disc and 2 GB RAM to recover the key in about two minutes [22]. While this makes completely passive eavesdropping on phone calls possible, phones can easily *get lost* by handing over to another cell (see next section). Furthermore, the newly introduced and currently rolled out [2] A5/3 and A5/4 ciphers (backported from UMTS) will force attackers back to active interception with IMSI Catchers to downgrade the encryption used. Known attacks on A5/3 are not yet feasible [10, 13, 21].
Detectability: The absence of a cipher alone is not a sufficient indicator: encryption might be unavailable in foreign roaming networks. However, once a phone had an encrypted session with a particular network and particular SIM card, it should assume that a sudden absence of any encryption is an alarming signal.

4.8 Cell Imprisonment

Once an attacker *caught* a phone, she/he will try to lock it in so it does not switch to another active cell. Therefore, it will either transmit an empty neighbor list to the phone or a list with solely unavailable neighbors. The base station can also manipulate the *receive gain* value [12]. This value is added to the actually measured signal levels by the MS to prefer a specific cell over another (hysteresis).
Detectability: A mobile station monitoring its neighbor list (e.g. together with a geographical database) is able to find such suspicious modifications.

[1] A low *T3212 Periodic Location Update Timer* is another technique, but the smallest possible value is 6 minutes.

4.9 Traffic Forwarding

The attacker needs to forward the calls, data and SMS to the public telephone system. There are multiple ways to achieve this. The simplest solution is to use another SIM card and a MS to relay calls into the mobile network. However, from the networks point of view these calls will be made under another identity. The attacker will most likely disable caller ID presentation to not immediately alarm the recipient. In this setup, the IMSI Catcher will not be able to handle any incoming calls for the surveyed station or any SMS.

Another setup could route these calls directly into a SS7 phone exchange network. Telecom operators usually trust their wholesale- and exchange partners with provider grade connections to set legitimate caller IDs. An attacker with access to such an interface could also spoof caller ID for outgoing phone calls and text messages. However, it is unlikely that the attacker can also manipulate the routing of incoming calls.

A third setup option (a full MITM attack) could facilitate a more advanced GSM frame relaying setup where data is handed over to the original network as if it where send by the victims phone.

Detectability: The first setup is detectable by making test calls and independently checking the caller ID (e.g. using an automated system).

4.10 Usage Pattern

IMSI Catcher in *identification mode* are operated for rather short periods of time to locate and verify an unknown phone such as prepaid phones or phones in an particular area. For tracking purposes and for eavesdropping the fake cell is active for the whole duration of the surveillance. Both operating times are considerably lower, than the average lifetime of a genuine cell.

Detectability: Cells that suddenly appear (with good signal quality) for a short period of time and cease to exists afterwards.

5. CATCHING AN IMSI CATCHER

Simple, cheap, and easily deployable *IMSI Catcher Catchers* (ICC) either need to run directly on a user's mobile phone or on affordable hardware (e.g. stationary device). While both concepts can be used to document IMSI Catcher use in a specific area, the former is also able to warn its user directly. In this section we describe both concepts, before we present our implementation in Section 6.

As Table 1 summarizes, the main detection method consists of a cell ID database. Commercial as well as free database projects exist. Most of them provide an online interface to their data. However, they neither guarantee to be complete nor correct, partly due to their croudsourcing nature. Also, they lack additional attributes needed for fingerprinting cell capabilities. Therefore, a IMSI Catcher Catcher (regardless if it is a mobile app or a dedicated stationary device) needs to be able to collect and maintain its own database regardless of any external databases (even when it is initially fed from another source). Furthermore, a mobile app can not assume online access is possible while being under attack.

Both types constantly collect all the data available about nearby cells. The mobile solution facilitates the almost ubiquitously built-in GPS receiver available in smart phones to correlate the data with its location. Therefore, from the phone's perspective the network topography is revealed similarly to *explorable maps* known from computer games, where the user only sees the areas of the map which he visited before (*Fog of War*). Visiting an already known area allows comparison of the current results with the stored data.

Additional tests include monitoring the noise levels of channels (RF jammer detection), network- and cell capabilities (e.g. cipher and GPRS availability), and sanity checks of network parameters (e.g. empty neighbor list might indicate a cell imprisoned phone). A caller ID test is implementable using an automated query system. However, regular calls to that system might result in non-negligible costs and have to be cryptographically authenticated.

The mobile app user (mICC) interface can be simplified to a user friendly four stage indicator:

Green No indicators of an IMSI Catcher attack found. Previously collected data matches the current network topography and all other tests completed negative.

Yellow Some indicators or tests show anomalies. However, these hints are not sufficient to postulate an IMSI Catcher attack. The user should avoid critical details in calls.

Red Indicators strongly suggest an IMSI Catcher attack or some other major network anomaly.

Grey Not enough data available (e.g. the user is in a previously unknown area).

An application with more intrusive access to the baseband might limit the phone's use to trusted cells only.

In contrast, a dedicated stationary IMSI Catcher Catcher (sICC) placed at a favorable position with a good antenna might receive a far greater radio cell neighborhood and allow to monitor a greater area non-stop (Figure 7). This is of great advantage when searching for a potentially transient event like the rather rare and short usage of an IMSI Catcher. Multiple devices can form a sensor network monitoring e.g. a whole city. As they don't move around, a GPS receiver is unnecessary. Most tests compare the collected data with the stations own history.

6. IMPLEMENTATION

Implementation poses some additional challenges: Only very limited baseband information is available to high level applications. In mobile operating systems, low level access is prohibited. System- and root applications can have access but are then limited to a very specific phone model (or chipset). This requires a *rooted* or *jail broke* phone. Additionally, only information is available that the chipset manufacturer has chosen to be disclosed. This also applies to commercial or industrial GSM/UMTS modules.

Among other baseband information, the neighbor cell list is an infamous example. Device support varies vastly, even for products of the same manufacturer. There is no identifiable pattern between low-end and high-end or older and newer products. Baseband information used to be called *engineering-*, *field test-*, or *network monitor* functionality for a long time. However, a few years ago, access to information such as the *serving cell* or *neighbor cell list* became popular for (coarse) locating devices in combination with a

Table 1: IMSI Catcher detection matrix

IMSI Catcher Artifact	Detection Method	Android API	iOS API[‡]	Telit [34]
Unusual Cell ID	Cell database	serving cell & neighbors[†]	serving cell only	yes
Unusual cell location		yes	yes	no
Unusual frequency usage		no	no	yes, ARFCN
Short living cells		yes	limited	yes
Unusual cell capabilities		serving cell & neighbors[†]	indirect	scan, neighbor
Guard channel usage	Band plan	no	no	yes
Network parameters	Network fingerprinting	no	no	limited (GPRS only)
RF jamming	Watching noise levels	limited	no	yes
Disabled cipher	Read cipher indicator	expected in future API [5]	no	no
Neighbor list manipulation	Cell DB & sanity check	limited[†]	no	limited
Receive gain	sanity check	no	no	no
Missing caller ID, SMS	Periodic test calls	yes	yes	yes

[†] Neighbor cells available via standard API, but not implemented in all phones.

[‡] Only via iOS private API. See Section 6.2 on reasons why iOS is not considered in this paper.

geolocation cell ID database, where GPS is not available, a loose estimation is detailed enough, or to simply aid the GPS during initialization. Therefore, recent smart phone operating systems provide a direct or indirect API interface to this information - even when it is unreliable in some cases.

When available, the next challenge is just around the corner: A MS is not required to keep a list longer than six nearby cells. Thus, the neighbor list provides only a very limited geographical view into the nearby network structure of the currently selected operator, despite some potentially more receivable cells. This is especially true in very dense networks such as in urban centers.

To extend the view and collect more data than the neighbor list length, a MS could be switched to use just a specific network band, such as 900 or 1800 Mhz GSM band or the 2100 Mhz UMTS band (many older phones and some data modules allow for this). Collecting disjunctive neighbor cell information for all bands separately extends the view on the network. Additionally, a device with a foreign SIM might be able to register at multiple (roaming) networks to investigate each one separately. However, both techniques interfere with the normal operation of a hand set. A mobile device constantly performing these kinds of investigations is not able to provide services for the end user in commonly expected quality. It would require a dedicated device for such measurements.

6.1 GSM Modems and Modules

For the dedicated stationary type of the IMSI Catcher Catcher (sICC) we tested several USB modems from ZTE, Nokia, and Huawei as well as MiniPCI modems from Qualcomm, none of which supported neighbor cell listing. Nokia and Huawei seem to support it on older devices, but dropped support on more recent ones.

Additionally, we started to test industrial modems such as devices from Telit. Among others, the Telit GT864 allow network registration and neighbor list scanning even without an inserted SIM card, allowing to scan each network in a region on each frequency band separately (see above). This provides a much greater view on the network structure than a simple mobile phone can provide.

On top of it, many Telit modems implement a cell beacon monitoring mode [34] that can be easily facilitated into a frequency band sweep cell beacon scan. Thus, allowing a complete view over the receivable network cells by frequency including their ID, some capabilities, signal, and noise levels. The latter also allows a simple jamming detection.

Our Implementation.

Our dedicated stationary setup (Figure 1) consists of a Telit GT864 [33] and a Raspberry Pi embedded Linux computer. Internet up-link (to collect the captured data) is either provided by an Ethernet network, power LAN, via WIFI (USB-Dongle), or an UMTS modem. Data is collected locally in an sqlite3 database and periodically uploaded to a central server. The whole setup including mounting material costs less than €200. As the device is able to perform full frequency scans for all providers without the limitation of length-limited neighbor cell lists, we placed these devices on rooftops to extend their range.

Currently, the network consists of four devices, the first one went online in July 2013. Our sICC is able to sweep through the whole 900 and 1800 Mhz GSM and EGSM bands within seven minutes. Besides the Cell ID, its main and auxiliary ARFCNs, it also records its receive levels and bit error rates as well as several GPRS configuration parameters (t3168 and t3192 timeouts, routing area codes, GPRS paging modes, etc).

6.2 iOS

iOS neither exposes high-level nor low-level baseband information (e.g. cell info) to applications through the official and public API. Methods such as `_CTServerConnectionCellMonitorGetCellInfo()` are available through a *private API*, whose documentation has leaked to the web. A field test App is available since iOS 5.1 by dialing `*3001#12345#*`. While the OS does not prevent the private API usage, it has been reported to be an immediate exclusion reason from the Apple App store. Applications using this API are only available to phones with a developer license or jail-broken phones and are therefore not of great use for a broader public.

Without a chance for widespread usage, we excluded iOS phones from further consideration.

6.3 Android OS

Android is a little more generous in providing access to baseband information. The `TelephonyManager` defines ac-

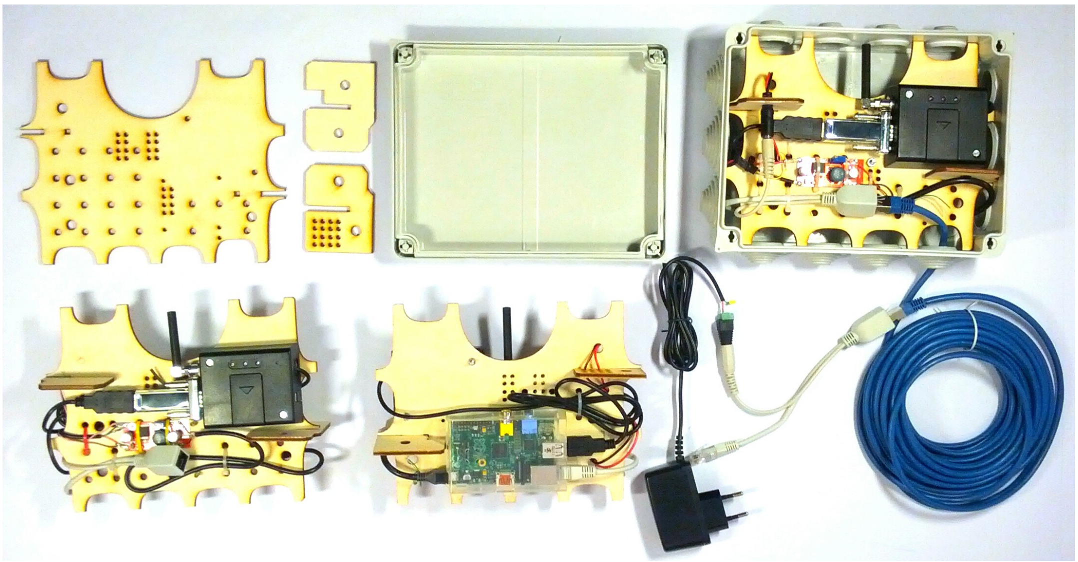


Figure 1: Construction of the dedicated stationary unit, using a laser-cut carrier (front and back)

cess to the important, but not all values on the wish list for the IMSI Catcher Catcher. Some values, such as the *cipher indication*, have been requested years ago and only recently got assigned for implementation [5].

The neighbor cell list problem described above also continues in the Android universe: The API defines the `TelephonyManager.getNeighboringCellInfo()` method. However, not even the long-time lead device *Google Galaxy Nexus* supports this method. Other devices only return meaningful values for this call for GSM type of networks, but not UMTS. It is not always clear if the underlying chipset does not provide this information or if the high level API lacks implementation by the phone manufacturer. A survey by the authors of the G-NetTrack application [1] reveals that this functionality is supported by less than half of the tested devices. Most devices report data only for the current serving cell. Recent devices have higher chances of implementing this method, most notably the *Google LG Nexus 4* and *Google LG Nexus 5*.

In contrast, Samsung Galaxy S2 and S3 expose many parameters unavailable through the standard API (such as the cipher mode [5]) via a Service Mode Application [7]. Some HTC devices offer similar hidden *Field Test Applications* [30]. This applications run under elevated privileges and often directly communicate with the baseband chipset via an operating system level device. Copying their interface will limit the application use to a rooted phone of a very specific model.

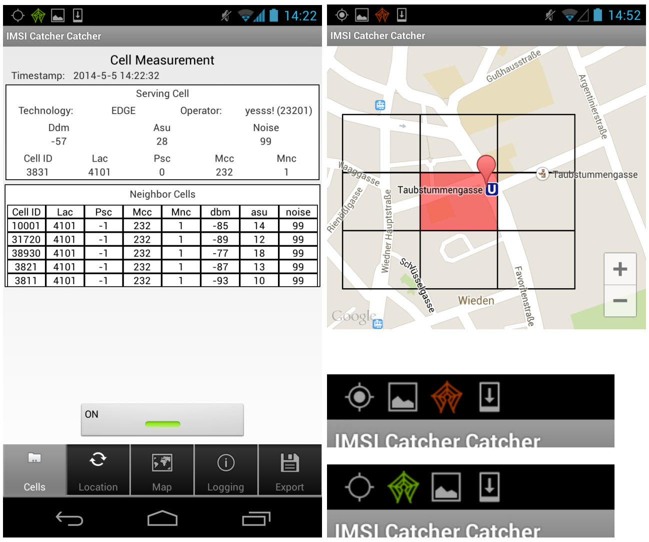
The absence of a neighbor list feature does not make a mobile IMSI Catcher Catcher (mICC) application impossible, but much less effective. This especially effects the speed of the network structure learning phase and some sanity checks on the network structure (e.g. cell lock-in by not having any neighbors). Another value offered by the API but not implemented in all phones is the noise level.

Our Implementation.

A background service[2] collects GPS position and cell related data (serving cell, neighbor cell, supported packet data modes). Measurements are triggered by the `PhoneStateListener.onCellInfoChanged()` - Callback and a regular 10-second timer (whichever comes first). This way, brief redirection to and from a cell (Section 3, Identification Mode) can be detected. For the sake of simplicity we group measurements in rectangular geographical tiles of about 150 × 100 meters and store them in an sqlite3 database. Some tiles might be in the learning phase while others are used for evaluation at the same time. We consider a tile fit for evaluation if the user collected cell data in this cell and all of its 8-connected tile neighborhood. Otherwise, nearby cells might easily create false alarms. A cell is considered valid for a given tile, if it was received as serving- or neighbor cell in one of the 9 tiles.

The app also runs in the background and displays the current evaluation result in the notification bar, so that it is visible in the system dialer and phone application.

7. RESULTS AND DISCUSSION



14:22

IMSI Catcher Catcher

Cell Measurement

Timestamp: 2014-5-5 14:22:32

Serving Cell

Technology: EDGE Operator: yesss! (23201)

Ddm	Asu	Noise
-57	28	99

Cell ID	Lac	Psc	Mcc	Mnc
3831	4101	0	232	1

Neighbor Cells

Cell ID	Lac	Psc	Mcc	Mnc	dbm	asu	noise
10001	4101	-1	232	1	-85	14	99
31720	4101	-1	232	1	-89	12	99
38930	4101	-1	232	1	-77	18	99
3821	4101	-1	232	1	-87	13	99
3811	4101	-1	232	1	-93	10	99

Figure 2: Screenshots of the mICC

[2] Note to the reviewer: A link to an open source repository will be added here.

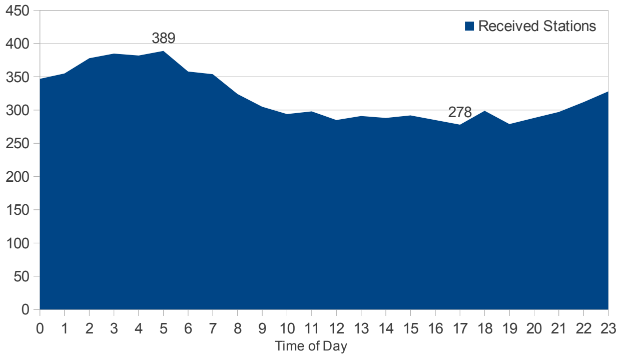


Figure 3: Maximum number of unique distinct cells received throughout the day (sICC)

The evaluations goal is to answer two main questions: (1) Are the two IMSI Catcher Catcher able to detect the presence of an IMSI Catcher? (2) Are IMSI Catchers used in our vicinity?

We evaluated both systems with lab tests as well as field tests. For our lab tests we used an USRP1 based IMSI Catcher running OpenBTS 2.6 in identification mode. Therefore, we patched OpenBTS to download the IMEI and IMSI of any phone and then reject the Location Update request - pushing the phone back into the genuine network based on [29]. Because of their very brief interaction with the phone, such IMSI Catchers are particularly hard to detect. Experiments were concluded in an controlled environment to not interfere with outside phones.

7.1 Stationary IMSI Catcher Catcher

In the lab experiment, the sICC was able to detect the new fake cell based on its cell id, parameters and capabilities.

For the field test, our first sICC was installed on a rooftop in Viennese city center in July 2013. Three additional stations have been installed in the first months of 2014. We collected over 40 million datasets. The range of some installations is remarkable (Figure 7): Under rare conditions we receive single stations up to 90 km away. Radio conditions vary among the day and so does the number of received cells (Figure 3). For maps based on Google's geolocation database see the Appendix. This external database is only used for visualization purposes and is not required for detection.

Regarding fingerprinting of cell parameters, we found many useful parameters[3]. In our test set of Austrian A1, T-Mobile, Orange/H3G, and Slovak O2 Telefonica network they all have the same value on all cells within a network, but distinct values between operators. Other values[4] displayed two distinct values within the Orange/H3G network.

CellIDs are very stable regarding their used ARFCN. However, on very received cells, one ARFCN can seem to have alternating different CellIDs. This can happen in situations, where the receiver sits in between two distant cells that are both using the same channel.

As Figure 4 shows, most cells remained static throughout the entire collection time. We attribute the bulk of very short-living cells to the following two effects: First, exceptional but transient weather and RF conditions that allowed the reception of cells very far away - often from foreign networks (Slovakia, Hungary, Czech Republic). We attribute this to *tropospheric scattering* and *ducting* caused by inversions [18, p.44]. These cell receptions are typically in the GSM 900 band and recorded as having very low signal levels and high bit error rates.

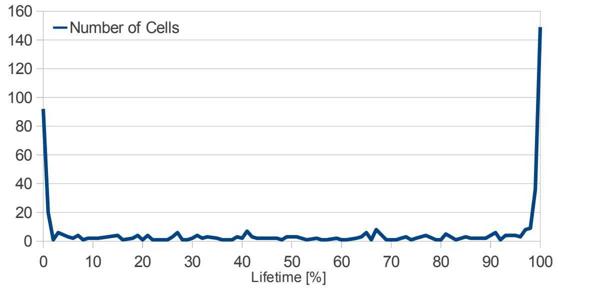


Figure 4: Cell ID lifetime throughout the experiment

Second, we noticed a bigger cell reorganization at one of the operators (*A1 Telekom Austria AG*) in the night from November 16th 2013. During a period of several hours, many cells appeared for only a brief period of time. We have not yet received any explanation from the operator. Also in November 2013, Orange/H3G received previously unassigned frequencies in the GSM 1800 band.

We found two additional irregularities in our collected data: (1) Some cells seemed to operate outside the official assigned frequency ranges. A request at the Austrian Regulatory Authority for Broadcasting and Telecommunication (RTR) revealed an error on their side in the published frequency band plan. This was later corrected [9]. (2) We received a cell with a valid looking Austrian MNC, LAC, and CI, but an unassigned network country code (NCC). We speculate that this could be either a transmission error or a base station in maintenance or test mode.

Under certain conditions it can make sense for an IMSI Catcher to emulate a foreign network to catch a roaming handset. However, in our case we are receiving different stations during nighttime over a span of multiple months. We therefore do not think these symptoms fits an IMSI Catcher and attribute them to natural effects (Section 9.2).

7.2 Mobile IMSI Catcher Catcher

For the prototype app we required at least 30 measurements and two re-entries into each map tile, before it finished the learning state. Additionally, the whole 8-neighborhood of the current tile must finish learning before it is considered for evaluation. The map view of our app supports the user in coloring tiles based on needed data. An always visible color coded icon in the notification bar indicates the warning level (Figure 2).

In our lab experiment, we were able to detect new and short living cells reliably, even when the *Location Update* was immediately rejected by our IMSI Catcher. Subtle differences exist in the implementation of the baseband to Android API interface. Some models report the new CellID and LAC for the ongoing but not completed cell change. Others only update the CellID immediately, while the LAC remains unchanged until the new base station accepts the *Location Update* request (e.g. Nexus 4).

For our biggest field test we chose a notoriously violent

[3] `PBCCH` existence, `SPGC`, `PAT`, `t3168`, `drmax`, `ctrlAck`, `alpha` and `pcMeasCh`

[4] `NMO` and `bsCVmax`

event in Vienna: a politically disputed ball taking place in the city center, and its counter-demonstrations. We anticipated that the authorities could use an IMSI Catcher to identify rowdies as suggested by media reports. We assembled a battery of three phones (Figure 5) for all three disjunctive GSM networks in Austria. We visited the demonstration route the day before and then attended the demonstration undercover. However, we could not find any indicators of an IMSI Catcher.

7.3 Limitations

Our geographical network topology correlation approach and the cell database in general assumes a rather static mobile network structure, as every change will be flagged as suspicious. In fact, network structure is very steady and this is actively utilized by mobile operating systems for coarse self-localization and commercial suppliers of geographical cell databases.

There are corner cases where the mobile IMSI Catcher Catcher needs refinement. One such case are tunnels and underground trains. In Vienna, the public metro enjoys an almost flawless GSM and UMTS coverage. However, without GPS reception these underground cells often get associated with the place of entrance into the underground structure, as the phone's GPS receiver needs some time to detect its failure.

Another problem are holes in the tile map. If a tile is entirely located within an inaccessible area (e.g. a large private property), the 8-connection neighborhood rule forces all nine cells to never advance from the learning state into the evaluation state. This could be mitigated by a hole filling algorithm (e.g. an interpolation). Additionally, setting appropriate warning thresholds needs extensive real world testing.

8. RELATED WORK

The osmocomBB Project [3] offers some IMSI Catcher indicators in their custom baseband firmware including cell fingerprinting and cipher indication. However, the project's target hardware platform are Texas Instruments' *Calypso* chipset based phones such as the (outdated) Motorola C123 or V171. This series of handsets appeared in 2005 and went out of production several years ago. Considering the fast production cycles and the non-disclosure policies in the mobile phone industry it is unlikely that such open source projects will develop similar custom firmware for recent phones any time soon.

Melette and Nohl, being aware of the latter, started investigating the possibilities to port at least a subset of this functionality to recent smart phone operating systems [22]. Problems include the limited access to baseband information. However, there has not been any activity on this project since January 2012. Another tool by Hummel and Neumann [19] works on a PC using an USB connection to a phone with an *Intel/Infineon X-Gold* baseband processor (Samsung Galaxy S2 and S3, but not S4).

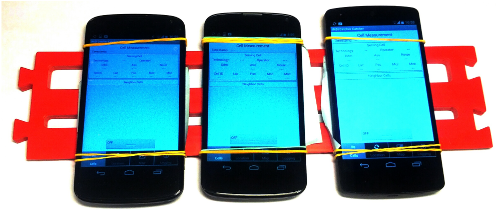


Figure 5: Field test for all three GSM networks

Vallina-Rodriguez et al. [35] also faced the problem of acquiring internal baseband values and decided to require root privileges.

Unlike previous works, our approach works by recording the geographical topography of a mobile network and is therefore able to detect structural changes that an active IMSI Catcher will cause. It facilitates the almost ubiquitously built-in Global Positioning System (GPS) receiver in smart phones. By using only standard API without any special permissions it ensures compatibility with as many phones as possible and is fit for public use.

9. FUTURE WORK

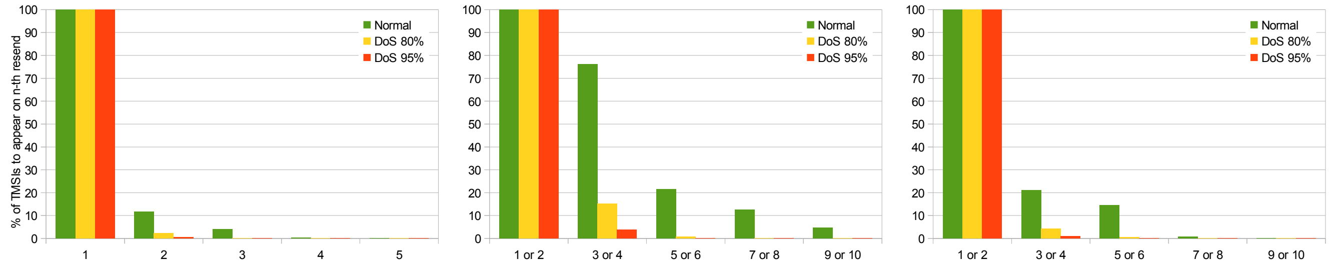
We are currently experimenting with a new RTL2832U based stationary IMSI Catcher Catcher prototype. The RTL2832U [28] is used in many DVB-T/DAB television and radio receiver USB sticks in the US$25 range. The chipset offers a way to bypass the DVB decoder and directly download 8-bit I/Q-samples with typically 2.8 MS/s turning it into a *Software Defined Radio* (SDR). Different tuner types exist, where the Elonics E4000 is the only one covering all major mobile phone bands by ranging up to 2200 Mhz. However, their extreme low price is to blame for the bad quality of many secondary components used. The oscillator accuracy can be as low as 50 ppm, leading to huge frequency offsets and shifts during operation. 30 kHz up or down is not a big deal, when receiving a multi-Mhz broad DVB-T signal. However, on a 200 kHz GSM signal they are very disruptive and need extra compensation.

Directly decoding the broadcast and control channels (i.e. BCCH and CCCH) gives much more insight and material for fingerprinting base stations (e.g. more details about the organization of logical channels, broadcast traffic)[5]. It does also allow for detecting other types of attacks, such as the *Let me answer that for you* type of denial of service attack by Golde at al. [17]. In general this attack exploits a race condition, in which a fraudulent array of phones with a custom firmware answer a paging request before the genuine phone does. The following cipher handshake will almost certainly fail, leaving the GSM state machine no other option than to drop the call. As paging is broadcast over the whole Location Area (LA) this potentially affect a huge number of subscribers even when deployed only in one spot. A single LA can cover large portions of a multi-million inhabitants city [17, Fig. 8].

9.1 Exposing Large Scale Denial of Service Attacks

Based on paging statistic of over 470,000 paging requests of all three Austrian GSM networks we simulated how the distribution of paging broadcasts re-transmits will change in a network under attack based on the retry policies of the individual networks. A certain number of mobile stations does not answer on the first paging request (e.g. caused by a dead spot or interference) and has to be paged again. Some networks switch over from TMSI to paging by IMSI

[5] This data is mostly privacy neutral, as it contains public system information about the network and pseudonymized paging requests.



(a) A1-mobilkom (b) T-Mobile (c) Orange/H3G

Figure 6: Number of TMSIs to (re)appear in the n-th paging resend within a 10 second window.

as a last resort. For our statistics we have to focus on TMSI paging, as there is no easy way to de-annonymize a large number of mobile stations at once. The distortions should be negligible for our purpose. We further conservatively assumed all paging requests within a 10 second window to belong to the original request. Only in very few cases (e.g. receiving many SMS messages in a brief period of time) this will not hold true.

Each paging request has a certain probability to not be answered by the target station on the first try and is therefore repeated. Based on the individual retry policy of each network, this produce a specific distribution on how many paging requests are tried a second, third, forth,... time. In our simulation we assumed a much less skillful attacker than in [17] with only 80% success rate and another one with 95% success rate. In both cases, the distribution of paging retries is severely distorted. Interestingly enough, some networks (i.e. T-Mobile and Orange) almost always page in pairs with just a few hundred milliseconds in between, in which case we grouped these requests.

Figure 6 displays how the retry-statistics is distorted from the normal empirical data (green) by applying a DOS attack with 80% respectively 95% success rate. Watching this relation can reveal such an attack against a whole Location Area, however it will not detect attacks against single phones (once the TMSI - IMSI pseudonmization is broken).

9.2 Inversions and Tropospheric Ducting

Based on laser ceilometer [14] data from the Austrian central institution for meteorology and geodynamics (ZAMG) we have found a slight correlation ($\phi = 0.21$) on reception of selected far off cells and border layers between 1000 and 2200 meters. This suggests that a better weather model might help us to understand the occasional excessive range of our stations. Eventually, this will allow us to clean up received data as these effects can produce similar short term reception patters to briefly operated IMSI Catchers.

10. CONCLUSION

IMSI Catchers – as man-in-the-middle eavesdropping devices for mobile networks – became cheap and relatively easily available. Even in UMTS 3G networks, GSM 2G security is still important, as these networks are closely linked together, and therefore the *weakest link* principle applies.

Our goal was to survey, implement, and evaluate *IMSI Catcher Catchers* (i.e. devices that detect *IMSI Catchers*). We therefore identified structural artifacts thanks to which IMSI Catchers can be detected. Some of these can be mitigated, but not evaded completely.

Our first implementation is based on a network of stationary measurement devices with cheap and easily acquirable hardware. Data is collected in a central database for long time observations and then analyzed. We collected over 40 million datasets in 10 months. The second one is based on the Android platform and uses only publicly available APIs. Thus, ensuring its operability in future versions and on as many devices as possible. Furthermore, it neither requires special permissions nor rooting (or jail-breaking) of the phone. Because of its simple color-based warning system it is suitable for daily use.

Both solutions are not dependent on any external databases, as they collect all needed information by themselves. With an OpenBTS based IMSI Catcher, we validated the described methods. Both of our IMSI Catcher Catchers were able to detect the attack reliably, even in *identification mode* where the phone is captured for less then two seconds. In the future, we like to extend our tests to commercial available products. Our long term observation of real mobile networks with our fixed measurement devices was inconclusive at the time of writing.

Our results indicate that the detection of this kind of attack became feasible with standard hardware. Additionally, we described how to detect additional attacks on mobile networks, such as an recently published DOS attack.

Both implementations will be released under an open source license.

Acknowledgements

The research was partly funded by the COMET K1 program by the *Austrian Research Funding Agency* (FFG). We like to thank *Technikum Wien* and *u'smile* (a Josef Ressel Center) for kind hardware support. Additional support by the *Institute of Telecommunications* (E389) at *Vienna University of Technology*, the *Austrian central institution for meteorology and geodynamics* (ZAMG), and *Funkfeuer Wien.* Special thanks for the valuable feedback from various telco employees and to *Manuel Leithner.*

11. REFERENCES

[1] G-NetTrack phone measurement capabilities. `http://www.gyokovsolutions.com/survey/surveyresults.php`, accessed July 15th 2013.

[2] GSM security map. `http://gsmmap.org/`.

[3] OsmocomBB open source GSM baseband software implementation. `http://bb.osmocom.org`.

[4] Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support.

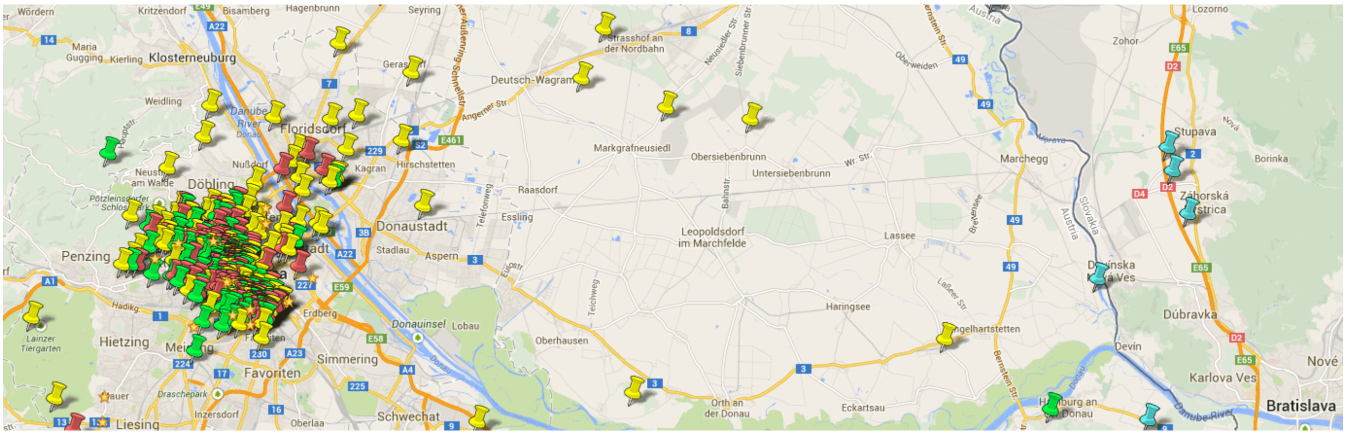


Figure 7: Stationary IMSI Catcher Catcher: Range up to 80 km. Color coded by operator. (Google Maps)

http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip.

[5] Android issue 5353: Ciphering indicator, 2009. https://code.google.com/p/android/issues/detail?id=5353, accessed July 14th 2013.

[6] A5/1 decryption rainbow tables. via Bittorent, 2010. opensource.srlabs.de/projects/a51-decrypt/files.

[7] Galaxy S III - ”secret codes” and hidden features, 2012. forum.xda-developers.com/a/ref-t1687249.

[8] Ability Computers and Software Industries Ltd. 3G Interception. Sales brochure. https://wikileaks.org/spyfiles/files/0/80_ABILITY-GSM_3G_Intercept.pdf, accessed Feb 25th 2014.

[9] Austrian Regulatory Authority for Broadcasting and Telecommunication RTR. Current utilization for GSM of the GSM 1800 frequency band. https://www.rtr.at/de/tk/1800MHzGSM.

[10] E. Biham, O. Dunkelman, and N. Keller. A related-key rectangle attack on the full KASUMI. In B. Roy, editor, *Advances in Cryptology - ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 443–461. Springer Berlin Heidelberg, 2005.

[11] M. Briceno, I. Goldberg, and D. Wagner. GSM voice-privacy algorithm A5/1, 1999. http://www.scard.org/gsm/, accessed July 17th 2013.

[12] Chris Paget aka Kristin Paget. Practical cellphone spying. In *DEFCON 19*, 2010.

[13] O. Dunkelman, N. Keller, and A. Shamir. A practical-time attack on the A5/3 cryptosystem used in third generation gsm telephony, 2010.

[14] S. Emeis, K. Schafer, and C. Munkel. Surface-based remote sensing of the mixing-layer height a review. *Meteorologische Zeitschrift*, 17(5):621–630, 2008.

[15] Ettus Research. Universal software radio peripheral. https://www.ettus.com/product.

[16] Gamma Group. 3G-GSM Interctiopn & Target Location. Sales brochure. info.publicintelligence.net/Gamma-GSM.pdf, accessed Aug 27th 2013.

[17] N. Golde, K. Redon, and J.-P. Seifert. Let me answer that for you: Exploiting broadcast information in cellular networks. In *Proceedings of USENIX Security 2013*, pages 33–48. USENIX, 2013.

[18] A. W. Graham, N. C. Kirkman, and P. M. Paul. *Mobile Radio Network Design in the VHF and UHF Bands*. John Wiley & Sons Ltd, 2007.

[19] T. Hummel and L. Neumann. Xgoldscanner, 12 2013. https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/Xgoldscanner, accessed Feb 19th 2014.

[20] F. Joachim and B. Rainer. Method for identifying a mobile phone user or for eavesdropping on outgoing calls, 2000. Patent, Rohde & Schwarz, EP1051053.

[21] U. Kühn. Cryptanalysis of reduced-round MISTY. In *Advances in Cryptology – EUROCRYPT 2001*, pages 325–339. Springer Verlag, 2001.

[22] L. Malette. Catcher Catcher. opensource.srlabs.de/projects/catcher, accessed July 12th 2013.

[23] U. Meyer and S. Wetzel. A man-in-the-middle attack on UMTS. In *3rd ACM workshop on Wireless security*, pages 90–97, 2005.

[24] P. Muncaster. Chinese cops cuff 1,500 in fake base station spam raid. The Register, 26 Mar 2014. http://www.theregister.co.uk/2014/03/26/spam_text_china_clampdown_police/.

[25] K. Nohl. Breaking GSM phone privacy. Blackhat 2010, Las Vegas, 2010.

[26] K. Nohl. Rooting SIM cards. Blackhat 2013, Las Vegas, 2013.

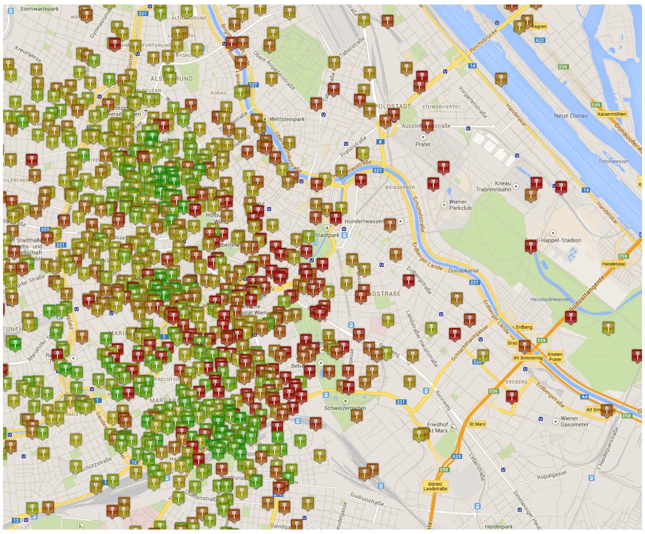


Figure 8: sICC: Color coded by signal strength. (Google Maps)

[27] K. Nohl and S. Munaut. Wideband GSM sniffing. Chaos Communications Congress (27C3), 2010.

[28] osmocom Project. RTL-SDR - osmcomSDR. `http://sdr.osmocom.org/trac/wiki/rtl-sdr`, accessed March 5th 2014.

[29] B. Postl. IMSI Catcher. Master's thesis, Technikum Wien, 2012.

[30] Richard's wireless blog. Hidden menus in android phone, 2009. `http://rwireless.blogspot.co.at/2009_03_23_archive.html`, accessed July 14th 2013.

[31] Rohde & Schwarz. Countering threats early on. `www.idexuae.ae/ExhibitorLibrary/1328/Countering_threats_early_on_2.pdf`, accessed July 14th 2013.

[32] M. Solnik and M. Blanchou. Cellular Exploitation on a Global Scale: The Rise and Fall of the Control Protocol. Blackhat 2014, Las Vegas.

[33] Telit Wireless Solutions. GT864-QUAD/PY - GSM/GPRS modules and terminals. `http://www.telit.com/en/products/gsm-gprs.php?p_ac=show&p=3`, accessed Feb 22th 2014.

[34] Telit Wireless Solutions. Easy Scan user guide, April 2013. `http://www.telit.com/module/infopool/download.php?id=6004`, accessed July 19th 2013.

[35] N. Vallina-Rodriguez, A. Auçinas, M. Almeida, Y. Grunenberger, K. Papagiannaki, and J. Crowcroft. RILAnalyzer: a Comprehensive 3G Monitor On Your Phone. In *Proceedings of the 2013 Internet Measurement Conference*, IMC '13, pages 257–264. ACM, October 2013.

[36] D. Wehrle. Open source IMSI-Catcher. Master's thesis, Albert-Ludwig-Universität Freiburg, 2009.