The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection

Adrian Dabrowski[1](✉), Georg Petzl[2], and Edgar R. Weippl[1]

[1] SBA Research, Vienna, Austria
{adabrowski,eweippl}@sba-research.org
[2] T-Mobile Austria, Vienna, Austria
Georg.Petzl@t-mobile.at

Abstract. An IMSI Catcher, also known as *Stingray* or *rogue cell*, is a device that can be used to not only locate cellular phones, but also to intercept communication content like phone calls, SMS or data transmission unbeknown to the user. They are readily available as commercial products as well as do-it-yourself projects running open-source software, and are obtained and used by law enforcement agencies and criminals alike. Multiple countermeasures have been proposed recently to detect such devices from the user's point of view, but they are limited to the nearby vicinity of the user.

In this paper we are the first to present and discuss multiple detection capabilities from the network operator's point of view, and evaluate them on a real-world cellular network in cooperation with an European mobile network operator with over four million subscribers. Moreover, we draw a comprehensive picture on current threats against mobile phone devices and networks, including 2G, 3G and 4G IMSI Catchers and present detection and mitigation strategies under the unique large-scale circumstances of a real European carrier. One of the major challenges from the operator's point of view is that cellular networks were specifically designed to reduce global signaling traffic and to manage as many transactions regionally as possible. Hence, contrary to popular belief, network operators by default do not have a global view or their network. Our proposed solution can be readily added to existing network monitoring infrastructures and includes among other things plausibility checks of location update trails, monitoring of device-specific round trip times and an offline detection scheme to detect cipher downgrade attacks, as commonly used by commercial IMSI Catchers.

1 Introduction

IMSI Catchers are MITM (Man-in-The-Middle) devices for cellular networks [28]. Originally developed to steal IMSI (International Mobile Subscriber Identity) numbers from nearby phones, later versions offered call- and message interception. Today, IMSI Catchers are used to (i) track handsets, (ii) deliver geo-target spam [32], (iii) 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 [39]), (iv) directly attack SIM cards with encrypted SMS [33] that are filtered

F. Monrose et al. (Eds.): RAID 2016, LNCS 9854, pp. 279–302, 2016.
DOI: 10.1007/978-3-319-45719-2_13

by most operators by now, and (v) also can potentially intercept mobile two-factor authentication schemes (mTAN). IMSI Catchers have become affordable, and can be build for less then USD 1,500 [14]. Pell and Soghoian [36] argue that we are currently on the brink of age where almost everyone is able to eavesdrop phone calls, similar to the 1990ies when cheap analog scanners were used to listen to mobile phones in the US and Europe.

In brief, these devices exploit the phone's behavior of preferring the strongest cell phone tower signal in the 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 can therefore be easily 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) and Long Term Evolution (LTE, 4G) require mutual two-way authentication, but are still not completely immune to IMSI Catchers. Tracking and identifying IMSI Catchers are build on the weakness that a network has to be able to identify its subscriber before it can authenticate him/her. Additionally, unauthenticated commands can be used to downgrade a phone into using 3G or the less secure 2G (GSM) only, eventually giving way to a full Man-in-the-Middle attack. Additionally, some phones execute unauthenticated commands, even though the standard demands prior authentication [35].

This issue gains additional momentum as commercial networks increasingly surpass dedicated administrative and governmental networks in coverage and data rates and thus carry more and more increasingly sensitive data. Additionally, today, many economic sectors critically depend on a reliable and secure mobile communication infrastructure (e.g., logistics).

While previous work [15,31,34,37,40] mainly focused on the detection of rouge base stations on the consumer side, this paper takes the approach from the network operator's perspective and discusses novel detection capabilities from an academic as well as practical point of view.

The cooperation with a mobile phone network operator with over four million subscribers enabled us to test theories, identify detection artifacts and generate statistics out of core network data. We focused on passive detection methods, readily available data in today's monitoring solutions and the identification of changes that promise better detectability and scalability.

The scope of this paper is the detection of attacks on the radio access network (RAN) in 2G (GE/RAN), 3G (UTRAN), and LTE networks (E-UTRAN). While there are attacks on the backbone and interconnection interface, or within a mobile network provider, we focus on the last-mile radio link between the cell tower and the terminal device. The traditional telecommunication network model centers all the intelligence in the network and attaches (dumb) end devices that have to obey the network. Thus, these types of attacks give an attacker a lot of control over the end user device.

The pivotal sections of the paper are as follows:

- Evaluation of 22 phones on (i) how they interact with the genuine network once released from an IMSI Catcher (Sect. 5.1) and (ii) which artifacts are produced.
- Development and implementation of detection strategies based on the artifacts and test of their fitness including their limitations on real-world data of a network operator (Sects. 5 and 6)

2 Background

Previous work [15,31,34,37,40] focused on the subscriber (customer) side; this paper shifts perspectives and addresses the detection of such attacks from the operator side. The particular challenge lies in the structure of digital mobile networks: They where drafted in a time of low bandwidth connections, when signaling traffic occupied a significant amount of the network infrastructure. Therefore, these networks were designed in a highly hierarchical and geographically distributed fashion with as much signaling traffic as possible being handled locally or regionally, thus, offloading the backbone. This poses unique challenges when acquiring and correlating the necessary data in order to detect anomalies in the network. Additionally, the legacy of having a GSM network being upgraded to UMTS and later again upgraded to LTE implies that the structure and the used data formats are not as clean and neat as one would expect from a freshly built LTE network with additional 2G and 3G radio front-ends.

Compared to the time when 2G networks were designed, today the ratio between user data and signaling data has completely changed. With LTE, users are offered 100 MBit or more.

The lowered backbone bandwidth costs and the (now) relatively low volume of signaling data allows mobile phone operators to en-bloc collect and monitor more data parameters than before. Many cellular network operators routinely collect data on different network levels and elements (e.g., from switches, servers, and via network probes) to detect, track and debug malfunctions and optimize their network. The strength of such Network Intelligence systems is to correlate transactions over different levels and protocols in the network structure, extract important values, and build an extensive index of the latter. This is done for several million signaling packets per minute. The limitation is that these indices are primarily built to search for traffic based on simple identifiers such as a specific customer, network element, protocol, or transaction type. Our goal is to use this monitoring systems to find far more complex symptom patterns that are typically produced by IMSI Catchers.

2.1 Working Principles of a Mobile Phone Network

Mobile phone networks became much more complex over the years. Each new generation or access technology (e.g., 2G GSM, 3G UMTS, 4G LTE) introduced a new terminology which complicates the description in an access-technology-neutral fashion.

For example, the base station (the radio front end of the network) with roughly the same functionality is called *Base Transceiver Station* (BTS) in GSM, *Node B* in UMTS, and *evolved Node B* (eNodeB or eNB) in LTE. Likewise, a mobile phone is called *Mobile Station* (MS) in GSM and *User Equipment* (UE) in UMTS as well as LTE. However, apart from the radio layer and some distinct organizational differences, they have many similarities on higher (more abstract) levels. Regardless of the access technology, the network needs to know how and (roughly) where to reach every subscriber, even when they are idle. This is solved by grouping radio cells into *Location Areas* (GSM, UMTS), *Routing Areas* (GPRS, UMTS; a subdivision of a Location Area), or *Tracking Areas* (LTE). In the phone's idle state, the network only knows the Location/Routing/Tracking Area where the subscriber is located, but not the exact cell. The phone (MS, UE) can listen to the broadcast channel of any cell as an incoming phone call, message, or data triggers a paging of the subscriber in all cells of a Location/Routing/Tracking Area. Upon a received page, the phone will contact the network and request a dedicated (logical) channel for further communication, thus giving away its position on cell level.

Only if the UE/MS switches to another Location/Tracking Area, it will tell the network about it, using a *Location Update Request* (GSM, UMTS) or *Tracking Area Update* (LTE). This method substantially reduces the signaling traffic caused by the subscribers' mobility.

In general, all subscribers are not identified by their phone ID (the 14-digit *International Mobile Equipment Identity*, IMEI), but by their *Subscriber Identity Module* (SIM) on GSM, or*Universal Subscriber Identity Module* (USIM) on UMTS and LTE which provides a 15-digit unique *International Mobile Subscriber Identity* (IMSI). However, sending the IMSI over the air would make subscribers easily trackable. Therefore, the network frequently (re)assigns a *Temporary Mobile Subscriber Identity* (TMSI) that is used instead[1] of the IMSI on 2G and 3G. 4G extends the TMSI by multiple *Radio Network Temporary Identifiers* (RNTI) for different use cases (e.g., paging, random access). TMSIs are meant to be reassigned on Location/Tracking Area changes, and some networks even reassign them on every interaction (e.g., call, text message) between the phone (MS, UE) and the network.

On a Location/Tracking Area Update message the phone will (usually) transmit its current TMSI and the old Location Area Identity (LAI, consisting of the *Mobile Country Code* MCC, *Mobile Network Code* MNC, and the *Location Area Code* LAC on GSM and UMTS) or *Tracking Area Identity* (TAI, comprising MCC, MNC, and the *Tracking Area Code* TAC). The *Mobile Switching Center* (MSC) for a Location/Tracking Area can now fetch all the data about the subscriber from the old Location/Tracking Area and inform the central user database (*Home Location Register* HLR on GSM and UMTS, *Home Subscriber Server* HSS on LTE) about where to reach that subscriber from now on.

[1] Except for the very first initial registration.

Location/Tracking Area Update Messages are the Swiss army knife of the *Mobility Management* (MM) in mobile networks: A phone freshly turned on will first try to make a *Location/Tracking Area Update Request* (LUR, TAUR) using its last known (cached) values. If its TMSI hasn't expired and is valid in this Location/Tracking Area, the network will accept the phone. Otherwise it will trigger a re-authentication. Therefore, even a phone arriving on a plane from another continent will first try to perform an LUR/TAUR providing the LAI/TAI data from another network. This is intended, as it allows for national roaming and seamless handover of active calls across an international border. (In LTE, the network can additionally provide an individual set of Tracking Areas for each UE, so that a group of subscribers – e.g., on a train – do not perform a Tracking Area Update all at once.)

Additionally, a ME/UE will perform periodic Location/Tracking updates, even when not moved in an interval configured by the network (e.g., 24 h) to assure the network of its continued presence.

Periodically during operation and at shutdown, parts of the baseband state are stored on the SIM card and the phone itself. For example, instead of performing a full frequency scan for all receivable base stations at power on, the phone will first try the frequency range where it received signals from its mobile phone network before. Also, it will retry its old TMSI in an attempt to speed up the procedure. (After all, if the phone has not been offline for too long, it still could be valid.)

3 Capabilities of IMSI Catchers

In general, IMSI Catchers come in two variants: (i) a tracking or identifying IMSI Catcher and (ii) capturing or Man-in-the-Middle IMSI Catchers. The first read out specific data from a phone or launch a specific attack before releasing the phone back into the genuine network. This is useful for enumerating phones in the vicinity or check for a specific device in radio range. The latter holds the phone captured in its fake cell and can relay traffic to the outside world.

While IMSI Catchers originally exploit a specific vulnerability in 2G networks, they are still a relevant threat in 3G and LTE networks, for several reasons: First, the weakest-link principle applies. As long as users can be deliberately downgraded to a less secure system, the weakest link sets the limit. Additionally, it has been recently shown that IMSI Catchers are possible on 3G and 4G in either a tracking-only setup or for full traffic interception in combination with backbone attacks (SS7, Diameter). These protocols are often used for interconnection and roaming of phone calls, but also of cryptographic material such as keys. In the roaming case the remote network has to be able to fulfill the same cryptographic operations as the home network. Engel [19] also presented sole backbone attacks, but they are out of this paper's scope.

3.1 Access Technology

2G/GSM. The original IMSI Catcher was build for GSM. Originally used only for identifying users (tracking), later devices allowed full man-in-the-middle attacks. GSM networks are specifically easy to impersonate, as the standard does not require encryption nor support mutual authentication.

3G/UMTS. Recent datasheets [22] show (limited) 3G capabilities of commercial available IMSI Catchers. For man-in-the-middle attacks they often downgrade users to 2G and capture them there. Osipov and Zaitsev [35] presented a de-facto 3G IMSI Catcher by using a reverse engineered femtocell. They also discovered that contrary to the standard, many phones accept unauthenticated SMS messages or time synchronization.

4G/LTE. Similar to UMTS, tracking IMSI Catchers are possible and phones tend to ignore integrity for many messages [38].

3.2 Catching Capability

Tracking or Identification Mode (Catch and Release). In this mode, the IMSI Catcher is luring phones into its fake cell, reading out IMSI and IMEI and pushing them back into the real network. For a target with known IMSI or IMEI this method can be used to check his/her presence in vicinity (omnidirectional antenna) or position (directional antenna). When used with a directional antenna, this can also be used to (visually) correlate a person to his/her IMSI and IMEI (see Sect. 5).

Capturing or MITM Mode (Catch and Hold). In this case the MS/UE is held in the cell and not pushed back into the real network. There exist several methods to decrypt, relay, and/or modify the traffic (see Sect. 6).

Passive Monitoring. This mode can be used e.g., after a target has been identified. Since the attacker does not have control over the phone it can switch to different cells and Location/Tracking Areas anytime. It has to follow the target across different frequencies and cells.

3.3 Cryptographic Capabilities

On GSM an attacker can choose between several methods. The easiest one, is to downgrade the client side and the network side to A5/0 (i.e. no encryption). However, many networks started prohibiting clients using A5/0. This can be problematic if legacy clients do not support any encryption. The GSM export-grade cypher A5/2 has been broken by Goldberg et al. in 1999 [23] and phased out by GSMA (GSM Association) by 2006 [25]. Barkham et al. presented a

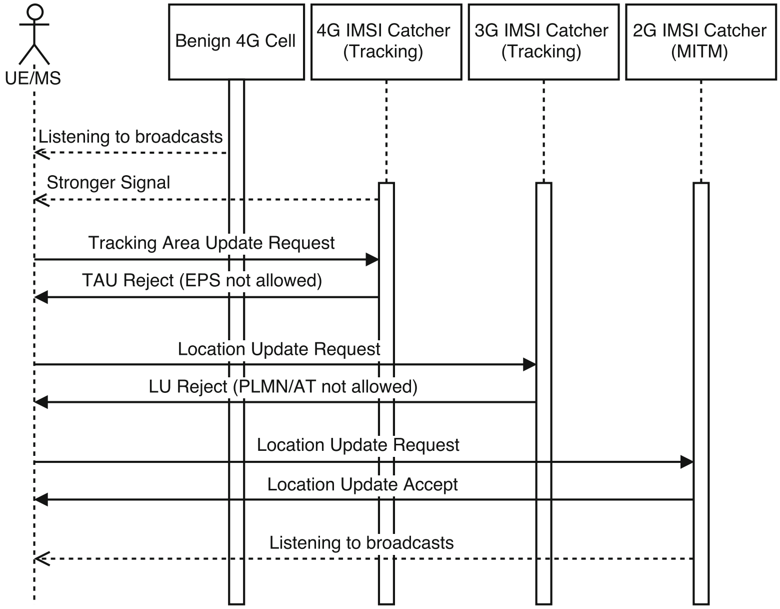


Fig. 1. Downgrade attack from 4G to 2G using *Access Technology not allowed* messages (simplified)

realtime ciphertext-only attack on A5/2 [10] in 2008. However, the GSM standard cipher A5/1 is also not secure; a number on publications [10,18,26] showed severe weaknesses and later 2 TB rainbow tables for decryption within seconds became freely available [29]. Thus, we must assume [3], that reasonable new IMSI Catcher are able to decrypt A5/1 and A5/2. Recently, many operators implemented A5/3 – a backport of the KATSUMI based UMTS cipher – for which no practical attacks are known. However, only newer handsets support this mode (cf. Fig. 4), and are easily downgrade-able by a fake cell (Sect. 3.4 below).

For UMTS and LTE encryption no practical cryptanalytic attacks are known, and mutual authentication is needed for (most) transactions. However, vulnerabilities in the SS7/Diameter exchange between providers allow the recovery of sessions keys [19,34] and therefore either decrypting traffic or impersonating a network.

3.4 Access Technology Downgrade Capability

For UMTS and LTE a downgrade to a less secure access technology (such as GSM) is also an option.

Jamming. A simple but brutal way is to jam the frequency band. In an attempt to restore connection to the network, the phone will try other (potentially less secure) access technology: e.g., jamming the UMTS band will encourage phones to connect via GSM. Longer jamming sessions will show up in the operator's network quality metrics and allow radio technicians to pin-point the source. Therefore, this method is only suitable for short term operations. In general, an attacker might strive for more subtle and less detectable ways.

Spoofing No-Authorization for a Specific Access Technology. A BTS, NodeB and eNodeB has the ability to deny access to a specific cell, location/tracking area or access technology for a number of reasons (e.g., no resources left, no subscription for a specific service, no authorization, etc.). Depending on the error code from the network, the phone will not retry and revert to other methods (e.g., another access technology) [8,9,24]. An error code for a permanent error will be cached by the MS/UE until next reboot. 3GPP defined rules on how to allow a network operator to expel a mobile from one access technology e.g., for LTE [9,38, c.f. reject cause #7] or 3G [24]. Therefore, a chain of tracking IMSI Catchers denying access and forcing a cell re-selection with another access technology can downgrade a client step by step (Fig. 1). Once arrived at 2G/GSM without mutual authentication the attacker can capture the phone and hold it in the fake cell.

These Location/Tracking Update Reject messages are intentionally not covered by the mutual authentication in UMTS and LTE, as a (foreign) network must be able to reject a user that has no subscription or no roaming agreement with the home network.

4 Design and Data Sources

For the development of our detection methods, we tested the interaction of 22 phones between an IMSI Catcher based on an USRP [20] and a mobile phone network. After that, we ware able to retrieve log and PCAP files from the mobile phone network's monitoring system for analysis. Based on that we developed detection strategies and implemented them. We tested them on real monitoring data and counter checked them with statistics from the real network.

Based on our NDA and the secrecy of telecommunications laws we had to work on site and where not allowed to take any actual data outside of the building. Additionally, the limitations of the current monitoring systems only allowed us to retrieve data based on simple queries and a specific buffer size. For example, we could either retrieve data for a specific IMSI (e.g. our test SIM card) or a specific cell for longer periods of time, or a specific transaction type nationwide but only for a short time period (e.g. minutes), but not both.

The problem lies in the scattered transactions in mobile phone networks that forbid a natural global view on the status of a network. Thus, state-of-the-art mobile network monitoring put probes next to the MSCs which preselect and extract key values out of the signaling traffic. This signaling traffic is heavily depended on the access technology. A database cluster collects this data and makes it available based on simple queries on the extracted features. This system has to deal with high loads: e.g. just the Location Updates for 2G and 3G peak at roughly 150,000 transaction per minute during daytime, whereas the 3G transaction are more complex and consist of more packets than on 2G.

The number of returned transactions on a query is limited by a (rather small) return buffer. However, data can be retrieved and reassembled to complete transactions which include everything from the initial mobile request, its way through the network instances up to the database access at the HLR and back to the mobile. This data can be exported to text and PCAP files for further analysis. Basically, any data extraction has to be reimplemented for each access technology. Even if the hight level behavior (e.g. Location Updates) are quite similar, the signaling traffic is completely different on a technical level.

This setup sets limits in the ability to analyze data for complex anomalies such as finding network areas with higher than usual non-adjacent neighbor location updates (see Sect. 6.3). Therefore, we tested our programs and made our statistics on data sets consisting of several thousands up to 47,000 transactions, based on the type of transaction. With small changes in the monitoring system (e.g. extraction and indexing of additional values by the probes) our solutions below can work on much larger data sets or on real-time data (e.g. they can request a much more focused selection of packets, and don't have to filter them themselves).

5 Tracking IMSI Catcher

A tracking (or identifying) IMSI Catcher does not hold a mobile device in the fake cell, but drops it back into the real network immediately. For an attacker it is advantageous to simulate a new Cell-ID as well as a new LAC as this will always trigger an active communication (Location/Tracking Update) from the attracted mobile device.

Simulation of a new Cell without a LAC leaves the attacker without knowledge which phones are currently listening to the broadcast channel. He/she could only page previously known subscribers (based on IMSI) to verify their existence. Additionally, it will disturb the availability of the attracted phones for the complete operating time of the IMSI Catcher.

Unless for very specific operations, for the above mentioned reasons, an attacker will most likely choose a fake Location/Tracking Area Code (LAC) (or one that is unused in the geographical area) so that every mobile phone attaching to this cell initiates a Location/Tracking Update procedure. This informs the attacker of every phone entering the cell, gives him/her the ability to download identification data and then reject the Location/Tracking Update. Depending on the error cause used, the phone might return later (temporary error), or put the LAC or MNC on a blacklist (permanent error). An attacker wishing to enumerate all phones again simply chooses another LAC. This procedure disturbs each phone for less than a second per scan and has no major implications on availability.

Figure 2 (upper part) presents the message flow. Known IMSI Catchers download the IMSI and IMEI since both are easily retrievable. The IMEI is also

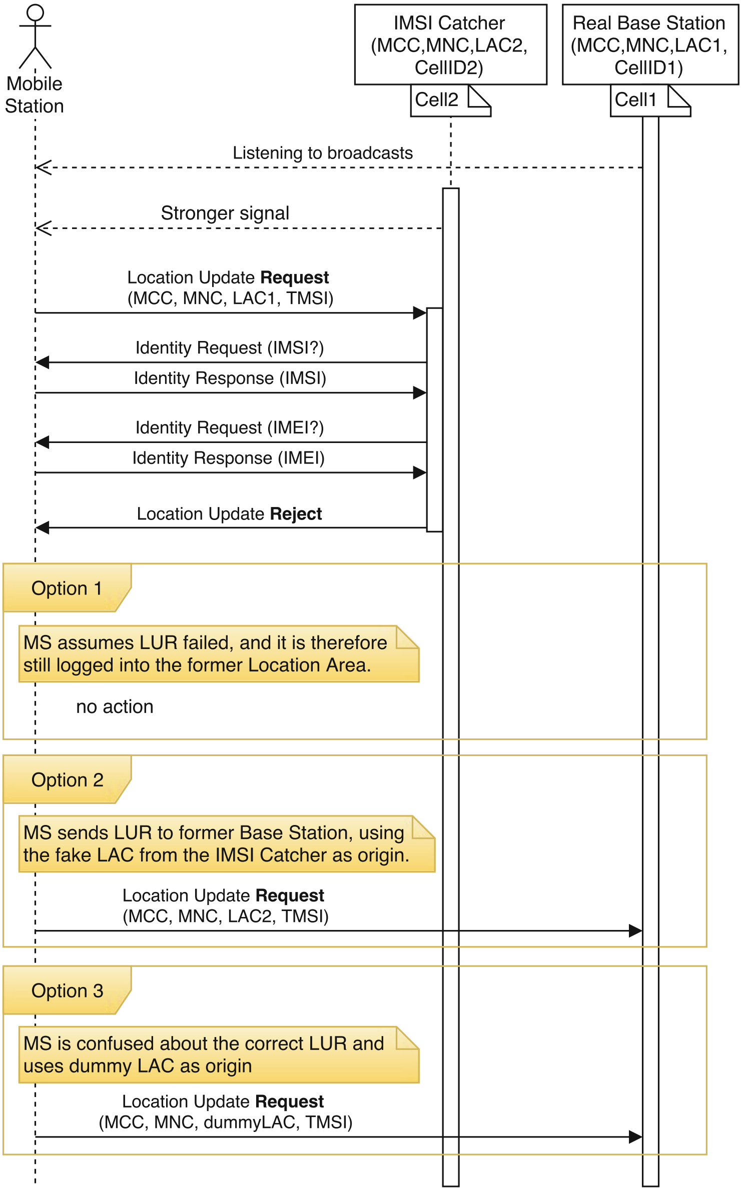

Mobile Station
IMSI Catcher (MCC,MNC,LAC2, CellID2)
Cell2
Real Base Station (MCC,MNC,LAC1, CellID1)
Cell1
Listening to broadcasts
Stronger signal
Location Update **Request** (MCC, MNC, LAC1, TMSI)
Identity Request (IMSI?)
Identity Response (IMSI)
Identity Request (IMEI?)
Identity Response (IMEI)
Location Update **Reject**
Option 1
MS assumes LUR failed, and it is therefore still logged into the former Location Area.
no action
Option 2
MS sends LUR to former Base Station, using the fake LAC from the IMSI Catcher as origin.
Location Update **Request** (MCC, MNC, LAC2, TMSI)
Option 3
MS is confused about the correct LUR and uses dummy LAC as origin
Location Update **Request** (MCC, MNC, dummyLAC, TMSI)

Fig. 2. A tracking IMSI Catcher identifies a phone and drops it back into the real network.

commonly downloaded by genuine networks in order to apply the correct protocol (workaround) policy based on the phone model.

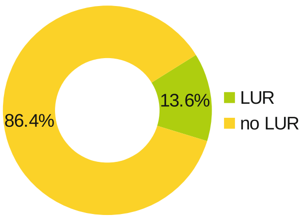


Fig. 3. Phone models that produce a new LUR after a Location Update Reject (n = 22 test phones)

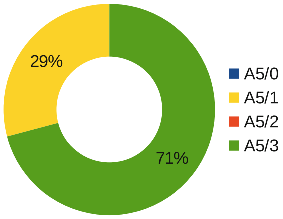


Fig. 4. Cipher usage on 2G nationwide (n = 7402 call setups)

5.1 Detecting Phones When Reattaching to the Original Network

From the operator's point of view, a phone leaving the network for a fake cell is invisible. If there should be a page request in the mean time, the phone will not receive it. However, since the phone is away for only a short period of time, it will likely receive a retransmit of that page request.

Once the phone receives a *Location Update Reject* message, it has three options (cf. Fig. 2):

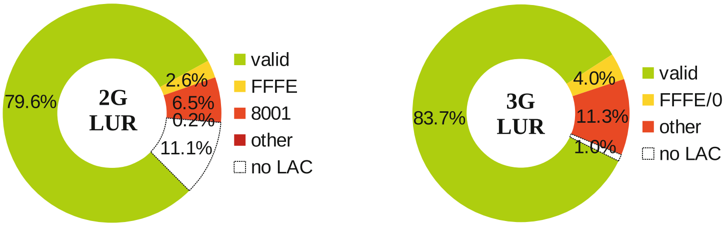
1. Assume that it is still known by the network at its old location. Therefore, no new message is needed.
2. A new Location Update Request is sent to the network using the IMSI Catcher's Location Area Code as origin (see also Sect. 6).
3. A new Location Update Request is sent using a dummy Location Area Code, since the last LAC value isn't valid.

We tested 22 different phone models[2] for their behavior after they dropped back into the genuine network in 2G (Fig. 3). 86 % produced no Location Update (Option 1) and 14 % generated[3] a Location Update Request with a dummy origin-LAC 0xFFFE (65534). The special values 0 and 0xFFFE are reserved when no valid LAC is available by the MS/UE [1,7]. Additionally, on GSM many phones also use 0 × 8001 (32769).

However, these dummy LACs are no direct indicator for an IMSI Catcher even for this minority of phones, as they are used quite regularly. In a dataset containing all nationwide 2G Location Update Requests within one minute (day-time) we found 9.1 % of all transactions using a dummy LAC and 11.1 % using no LAC at all (see Fig. 5a) without any geographical pattern. The numbers for 3G (Fig. 5b) are smaller: 4 % of Location Update Requests contained a dummy LAC (0 × FFFE or 0 × 0000) from the same network. 1 % contained also dummy values for the Mobile Country Code (MCC) and Mobile Network Code (MNC).

[2] Nokia Lumia 920.1, E71, 6310, 6150, 3210, 3710A-1, LG Nexus 4, Nexus 5, Apple IPhone 4, IPhone 6, Nexus One, Motorola Moto G2, Moto G XT1032, Samsung Galaxy Nexus, Galaxy S3, Galaxy Xcover2, Galaxy S5, Sony Xperia Z2-SCR10, BG Aquaris E4.5 Ubuntu Phone, Kyocera Torque KS-701, Sony Ericsson ST17I.

[3] All Nokia models introduced before 2000.



(a) 2G nationwide (n=47K)

(b) 3G nationwide (n=17K)

Fig. 5. Origin LAC provided at Location Update Requests. *Valid* means that the LAC is within the local LAC plan. *0*, *0x8001*, and *0xFFFE* are literal (dummy) values. *Other* are LACs from outside the network (e.g. international or national roaming, accepted and rejected). *No LAC* describes the requests that do not provide a valid LAC or that provide dummy Values for MNC and MCC as well (such as 0 × 00 or 0 × FF)

64 % of our test phones generated a *GPRS Attach*[4] request within the next two minutes, if and only if it had a data connection before and did not have an additional WiFi connection. This is due to the fact that our test setup did not indicate GPRS support for the fake cell. Such a GRPS Attach request is nothing extraordinary and happens regularly (42 % of all Location Updates on a real network contain such a header) for example if a phone drops out of WiFi and needs an Internet connection.

18 % of this *GPRS Attach* messages had the *No Valid TMSI available* flag set. However, on a real network 4.5 % of LUR messages have this flag set.

6 Capturing IMSI Catcher

An IMSI Catcher of this type holds the mobile in the cell and can therefore man-in-the-middle any transaction, and has control over the mobile phone by means of any network management commands (Fig. 6).

6.1 Detection of Cipher Downgrades

A man-in-the-middle IMSI Catcher has to forward the traffic to the network. An easy way, is to tap into the cipher negotiation sequence and change the set of supported ciphers. The easiest choice for attackers is A5/0 (no encryption) and A5/2 (the weakened export-variant of A5/1), as described in Sect. 3.3. However, many networks (incl. T-Mobile Austria) banned these ciphers for years.

Instead, they started to support the A5/3 cipher [2]. On GSM this is the only cipher without (publicly) available rainbow tables or other decryption methods.

[4] Technically, this is an Location Update Request with *Origin LAC* set to the current LAC and an optional GRPS header with the Attach-Bit set.

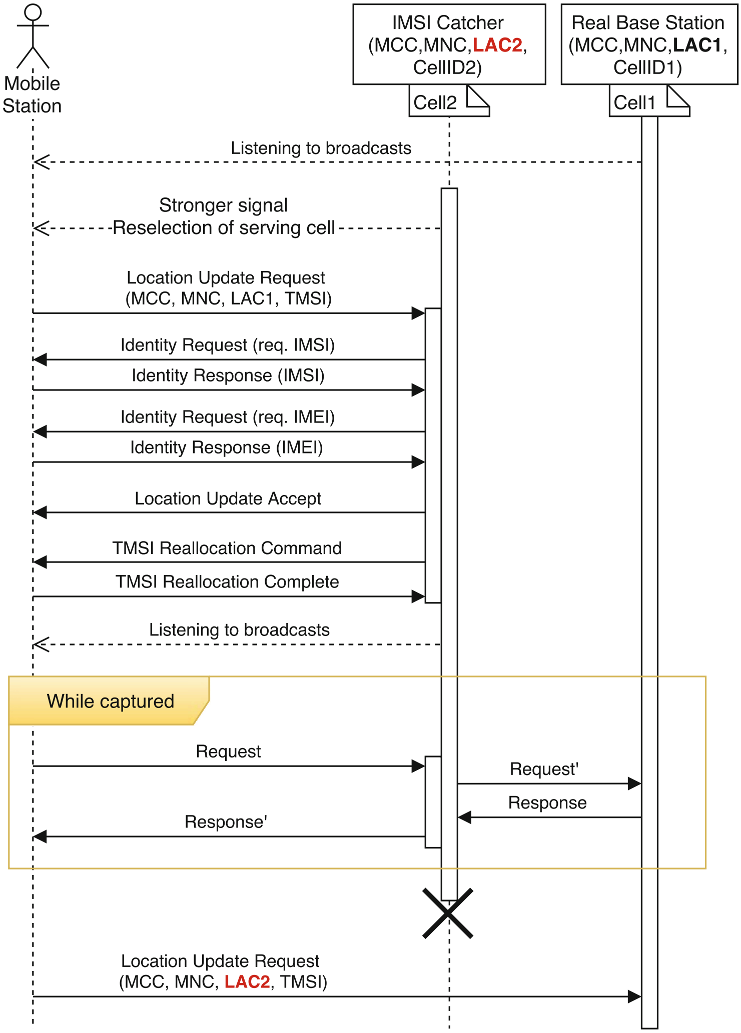

Mobile Station
IMSI Catcher (MCC,MNC,LAC2, CellID2)
Cell2
Real Base Station (MCC,MNC,LAC1, CellID1)
Cell1
Listening to broadcasts
Stronger signal
Reselection of serving cell
Location Update Request (MCC, MNC, LAC1, TMSI)
Identity Request (req. IMSI)
Identity Response (IMSI)
Identity Request (req. IMEI)
Identity Response (IMEI)
Location Update Accept
TMSI Reallocation Command
TMSI Reallocation Complete
Listening to broadcasts
While captured
Request
Request'
Response
Response'
Location Update Request (MCC, MNC, LAC2, TMSI)

Fig. 6. A man-in-the-middle IMSI Catcher identifies a phone and withholding it from the real network. During fall-back into the real network, the captures phone gives away the LAC of the IMSI Catcher.

However, many MS still do not support this mode. On our network, in September 2015, 29 % used A5/1 and 71 % A5/3 (Fig. 4, n = 7402). Other cipher modes where prohibited in this network.

An operator-run database of {IMEI, highest-used-cipher}-tuples provides the basis to detect cipher downgrades. This database is updated on first contact with the network and whenever a device uses a higher ranked[5] encryption than the

[5] A5/0 < A5/2 < A5/1 < A5/3.

one stored. As long as there is no SS7/Diameter standard on exchanging this form of information, every operator has to run their own database (or include it into the HLR/HSS). Once the highest available cipher of a device is established, the network should not accept a lower one, or at least generate a warning. Thus, making a downgrade attack visible to the operator except when the user is attacked on the very first contact with a new network. Except for a firmware bug, there is no reason why a device should stop supporting higher cipher levels.

6.2 Detection of Relayed Traffic

The most compatible and least interfering way for a capturing IMSI Catcher to operate is to relay all traffic. If it is encrypted with A5/1 or A5/2 the decryption can be done separately, otherwise it has to be downgraded. Based on enough traces, the session key K_c can be reconstructed [27,29]. In conjunction with another vulnerabilities (e.g., weak COMP128), also the secret authentication key K_i can be read and the SIM card cloned [12]. Once K_c is known, this allows an IMSI Catcher to decrypt A5/3 as well, since the K_c is used for all ciphers. For SIM cards with only a 64 bit key, the K_c is doubled $K = \{K_c || K_c\}$ to 128 bit and therefore allows decryption of UMTS as well[6].

We tested if the analysis of the round-trip times can be a good measure to uncover traffic relay. Therefore, we analyzed authorization round trips in the wild of 4165 random transactions within one minute, nationwide. The histogram in Fig. 7 shows a high deviation ($\bar{x} = 0.586$ sec, $\delta = 0.334$) of response times

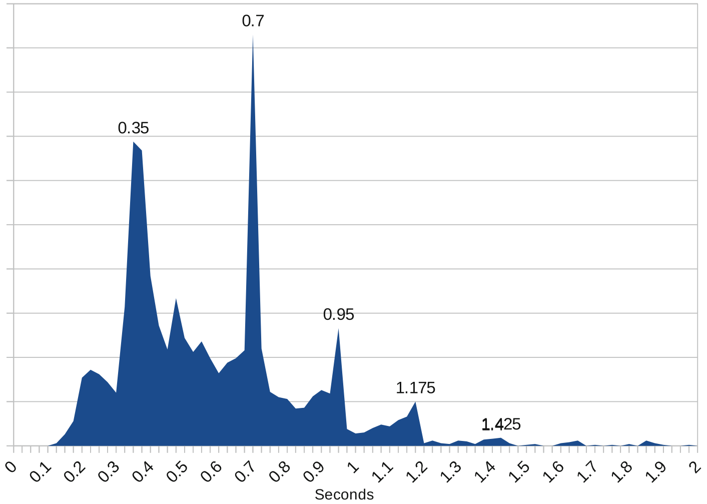


Fig. 7. Authorization round trip time: distribution of time between *Authentication Request* and *Authentication Response* on a real network.

[6] The attacker has to brute-force the 48-bit sequence number, though.

with a notable retransmission interval of about 0.25 s. We estimate that a well-designed traffic-forwarding IMSI catcher could relay the traffic in 100 ms or less, thus being far from statistically significant in single instances.

Further analysis presented vast differences between manufacturers as well as handset types. Based on the *Type Allocation Code* (TAC)[7] we run independent nationwide collections. Figure 8 shows 12 diverse popular handset types and highlights three different iPhones to illustrate their different behavior (based on an average of 3,400 transactions per phone type). Since this values have a much smaller standard deviation (e.g., $\sigma_{\text{GalaxyS4}} = 0.198$, $\sigma_{\text{IPhone3gs}} = 0.200$, $\sigma_{\text{IPhone4s}} = 0.206$), they are a better basis to detect relay delays (i.e. average authorization round trip time increases on multiple occasions for a single user). Additionally, a provider side detection can correlate such changes geographically (i.e. average authorization round trip time increases in a geographical area).

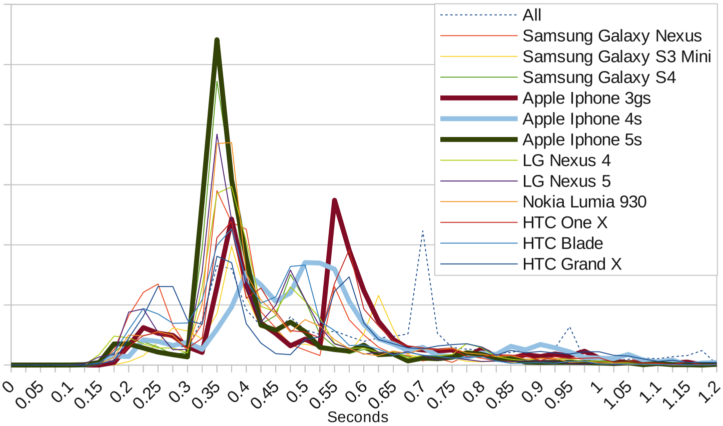


Fig. 8. Normalized distribution of authorization round trip time broken up by phone models. Three Apple phones highlighted to show the distinct differences in their authorization response time. (n ≈ 3400 for each phone type)

6.3 Detection of Unknown, Unusual or Implausible Origin-LAI/TAI in Location Update Requests

Eventually, every IMSI Catcher victim falls back into the genuine network (Fig. 6). During this step, the LAC of the attacker is leaked back into the real network[8]. As stated above, it is favorable for an attacker to choose an unused LAC as this forces

[7] TAC are the first 8 digits of an IMEI that encode the manufacturer and phone model. Popular models might end up with multiple assigned TACs. This is somewhat similar to the assigned OUI prefix in Ethernet MAC addresses: they encode the manufacturer.

[8] See Sects. 7.3 and 7.4 for further discussion and possible mitigations.

every victim to actively contact the fake base station on entrance and therefore inform the attacker about its capture. This LAC is either completely unknown in the genuine network or far away.

We investigated the possibility of creating shadow instances that follow every location area update and reject implausible location changes. While the current monitoring infrastructure does not allow to monitor all location updates nationwide for all mobile phones (Sect. 7.3), we scaled down and implemented a prototype that is able to follow individual UE/MS through different access technologies based on PCAP files from the core network. The two main investigated properties are (i) the correctness and completeness of location update trails and (ii) the geographical plausibility of location updates (i.e. only adjacent locations).

The *correctness and completeness of location update trails* means that location trails form an uninterrupted chain. A gap would be a strong hint for a visited LAC to not be under the control of the operator. The *geographical plausibility* checks if updates only occur between geographically neighboring locations. This neighbor property does not have to be derived geographically, but can be established statistically (i.e. recording frequent location updates between Location Areas). Unless operators agreed on national roaming, the phone stays on the home network, so no operator collaboration is necessary.

In the following evaluation we discovered a number of corner cases that complicate the interpretation of the results.

Power on at a New Location. UE/MS not always correctly detach from a network when turned off (e.g. battery loss, temporary reception loss during power off). At the next power on, the UE/MS will use the previous LAC as origin for a location update. Imagine this plausible case as depicted in Fig. 9: A flight passenger turns off the phone at takeoff in one city, but the *IMSI deattach* message was not produced or did not arrive at the network. After landing, the passenger turns the phone back on during the train ride from the airport to the city. In most cases, the phone will send a location update to the network as if it just passed the border between the two location areas. This even happens after intercontinental flights. Airport cells could be whitelisted to some extent, but they will not catch all cases (such as in the example above).

Because such (tunneled) location update are indistinguishable from a direct location changes, they are not immediately a red flag.

Additionally, road and railway tunnels also offer geographical shortcuts, but – unlike plane routes – the ends of the tunnel only connect two points and will be statistically assigned as neighbors, since a large number of passengers traverse without turning off their phones.

Old Baseband State Restoration. Phones regularly and at certain events save parts of the baseband state information to non-volatile memory. For faster boot

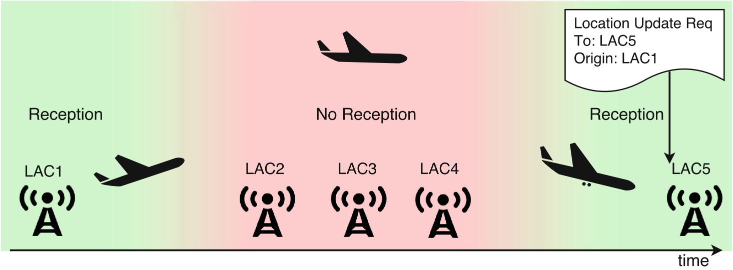


Fig. 9. Location update tunneling effect: Because a detach message is not guaranteed, location/tracking area updates happen between non-adjacent cells.

times, the phone can facilitate this information (e.g. already knows the frequency range of the preferred operator and does not has to scan the whole frequency range). This includes the last known LAC.

One of our test phones had a defective power button which lead to random reboots. In the traces we discovered that the phone sometimes used obsolete LAC information as origin (i.e. reused a LAC as origin a second time, because another location change was not recorded properly before reboot).

6.4 Detection of a Access Technology Downgrade

As described in Sect. 3.4 and Fig. 1, access technology downgrades are easy to perform and included in todays commercially available IMSI Catchers [22]. A phone camping on 2G even though 3G or 4G should be available in the area is not a strong indicator. In some cases, structural properties can lead to better reception of certain frequency ranges (e.g., 2G on lower frequencies is usually better receivable underground). On the other hand, a MS/UE can be set intentionally to use 2G only for power conservation. A provider could install an application on the SIM to monitor the access technology and location updates; however, this is out of scope for this paper.

7 Discussion

We identified strong and weak indicators based on the statistics of certain features in real-world data. Strong indicators have low potential for false positives.

A **per device (IMEI) database of the highest-used cipher** can reliably detect cipher downgrades or deactivation of ciphering. Additionally, we have shown that mobile phones **leak the (fake) LAC of the capturing IMSI Catcher to the real network**. This case can trivially be detected based the on analysis of Location Update Requests. If the attacker misuses a genuine LAC, it can still be detected by a **consistence check of the Location Update trail**. Based on certain corner cases, the latter has the potential for false positives

(LUR tunnel effect, restoration of old baseband states) and therefore needs to be backed up by additional geographical, temporal and subscriber based correlation.

Another method is the **transmission delay introduced by an MITM attack**. We tested this technique based on the authorization round trip times. In general, the deviation is quite large, but can be narrowed if the device type is considered as well. Every device has a very specific distribution of round trip times. However, for a statistically significant result (e.g. for a device under attack), multiple measurements have to be collected.

From the provider point of view, the hardest attack to detect is that of a tracking-only IMSI Catcher. Except for a few very old phones, this particular attack does not produce any messages in the core network. It has still to be explored if certain frequency-monitoring functions on BTS, NodeBs, and eNodeBs can be repurposed to detect such rouge base stations.

7.1 Ethical Considerations

As described in the research set up (Sect. 4) we have used real data only under very strict conditions to comply with ethical and legislative requirements. We have only worked on signaling data and never had access to user data or personal subscriber information.

7.2 Comparison with Client Detection Methods

Operator detection of IMSI Catchers does not supersede client detection (c.f. Sect. 8.1). It complements it and gives the operator the opportunity to monitor such attacks in its network regardless of precautions by individual subscribers. However, since the detection schemes can only find phones that are either under the control of an attacker - or just switched back to the genuine network - the operator can only warn the user in question post-attack.

On the other hand, client based techniques give the user the ability to detect a current attack against his/her very device. On tracking IMSI Catchers this technique provides better detection rates.

7.3 Limitations

The current implementation of our detection methods is based on the old somewhat limited monitoring system deployed in the network. It can filter some preextracted of each packet and transaction against a query containing a limited set of operators and literal values (i.e. filter by a specific cell, IMSI, IMEI, protocol type, etc.). It can not compare between cells or apply more complex filters. Additionally, the return buffer size is limited to 10 K–30 K results, depending on the search mode. This limits our current implementations to single users (or single cells) at a time. This is the reason we could not run a nation wide search so far.

7.4 Future Work

Our results show that detection from the operator side is possible and tested its usefulness within the limitations of the current monitoring system. We suggest that parameters such as ciphering and origin LAC in Location Area Updates should be extracted directly at the probes and made available. This pre-selection step will eliminate current limitations. For example, it will allow to search for inconsistencies in used ciphers, based on the IMEI (or TAC). Additionally, a new monitoring system based on Apache Hadoop is currently in development that is expected to remove most limitations of the current system.

With the large number of dummy LACs used by phones, one can wonder if an attacker could use dummy LACs such as 0xFFFE for masking their existence. Another way, to mask the fake LAC of an IMSI Catcher is, to announce a neighbor frequency occupied by a second IMSI Catcher with a reasonable LAC. While doubling the hardware costs for an attacker, this might whitewash the *Origin LAC* field used in Sect. 6.3. Both ideas need further testing with end devices to confirm or deny their practical feasibility. As discussed before (Sect. 6.4), a SIM card application can monitor and report certain network parameters back to the network (e.g., keep a local copy of a CellID/LAC trail) and detect both cases. However, over time, many different cards from different vendors have been acquired so developing and maintaining such an application poses a financial burden and an operational risk.

Furthermore, we plan to refine the timing models used in Sect. 6.2 to become more accurate and create better models for timing delays introduced by traffic relaying.

8 Related Work

8.1 IMSI Catcher Detection

So far, IMSI Catcher detection has almost exclusively been tackled from the clients' point of view. Malete and Nohl first developed a solution for OsmocomBB phones, and later on for rooted Android phones with a very specific Qualcomm chipset [31,40]. Other applications replicated similar client side detection without the need for a rooted phone [15,37].

Van den Broek et al. proposed a pseudo-random IMSI that will not allow others than the home operator to distinguish particular users [13]. However, this will introduce a higher overhead in the roaming case and needs to be extended to cover cases where IMSI Catchers use additional identification numbers (such as IMEI).

Van Do et al. are so far the only ones to look at the provider side [16]. Their solution is based on encryption elimination detection and anomalies such as disappearance of a large group of phones in a geographical area, fed into a machine learning system. However, their approach has limited applicability, for real world networks: Disabling encryption is only found in older capturing IMSI catchers and disappearance detection has a latency up to 24 h – the time scale of periodic location updates (i.e. the mobile phone's periodic reassurance to the network). This will only detect IMSI Catchers operating for an extended amount of time.

8.2 Working Principle of IMSI Catchers

Osipov and Zaitsev reverse-engineered a Huawei Femtocell and were able to create a 3G IMSI Catcher and test phone implementations for messages where integrity is ignored [35]. Shaik et al. researched 4G IMSI Catchers and their possibilities [38]. Dunkelman et al. did research on the KATSUMI algorithm on which A5/3 is based, but the attack is not practical in real-world networks [17].

8.3 Related Attacks on Cellular Devices

There are many attacks that are relevant as they are performed directly or in conjunction with an IMSI Catcher.

SS7 MSISDN Lookup. IMSI Catching does not reveal the telephone number (known as *Mobile Station International Subscriber Directory Number*, MSISDN) of the subscriber. If not blocked by a firewall, an attacker with access to the international interconnect network using Signaling System 7 (SS7) can request subscriber information based on the IMSI (or the TMSI), just as any roaming network would do [19].

SS7 Session Keys. An attacker with access to the international interconnect network based on SS7 is able to retrieve RAN session keys [19,34]. The key retrieval is a legitimate function required for roaming support: The roaming network needs to authenticate on behalf of the home network. SS7 stateful firewalls (e.g., keep track if and where a user is roaming) can block such requests.

SIM Card Rooting. Several SIM card attacks described by Nohl et al. [33] have been blocked by the network operators worldwide. However, an IMSI Catcher is directly communicating with the UE/MS. This gives the attacker the ability to perform attacks such as the retrieval of SIM card application keys, eventually giving him/her the control over the installation of new SIM card applications on the victims device.

SIM Card Cloning. In 1998, Briceno, Goldberg, and Wagner reverse engineered and broke the COMP128 [11] key derivation algorithm which enabled cloning of GSM SIM cards of many network operators [12]. In 2015, Liu et al. [30] found that AES-based MILENAGE algorithm on some USIM implementations is prone to power-based side-channel analysis and thus giving way to clone these cards as well. Unfortunately, they never named the manufacturers of the USIMs.

Unauthenticated SMS. 2G as well as some 3G devices [35] allow the reception of SMS messages while captured by the rouge base station. The results for 3G are somewhat surprising, since this is actually prohibited by current standards. However, many phones do accept these messages nonetheless. SMS in 4G works entirely differently and is therefore not affected by this vulnerability, although recent results [41] show that vulnerabilities exist in other constellations.

Presidential Alert Cell Broadcast. A feature dubbed *presidential alert messages* [6] is a special form of short messages that cannot be suppressed and interrupt the phone in whichever state it is to be shown to the user. A fake base station can send out this kind of messages.

GPS Lookup Initialized by Network. The *Radio Resource Location Services (LCS) protocol* (RRLP) is an extension [4] to GSM and UMTS that allows the network (real or fake) to trigger a GPS localization on the phone and submitting the location back to the network. Harald Welte [42] demonstrated that this happens without any authentication.

Measurement Triangulation. The network has the ability to request measurement reports to other cells in the vicinity. A fake base station can use these reports to estimate the position of the phone based on signal levels and known positions of the cells. This is also possible on 4G [38].

Disable GPS. Because of (former) Egyptian regulations prohibiting the usage of GPS, some older phones (iPhone [21], Nokia [5]) are known to disable the GPS receiver when either associated or just in the vicinity of a network using the Egyptian Mobile Country Code. An attacker can use this to disable the GPS receiver on certain phones.

9 Conclusion

IMSI Catchers are still a major problem for todays networks: (i) Tracking IMSI Catchers work directly on GSM, UMTS, and LTE networks as Location/Tracking Update Rejects are excluded from cryptographic message integrity checks. Mutual authentication only prevent plain capturing IMSI Catchers. (ii) These reject messages can be used to downgrade a phone until the next reboot to a lower access technology (e.g. GSM) without mutual authentication. Therefore, the weakest-link principle applies.

In this paper we analyzed the different types of IMSI Catchers and their working principles as well as if and how they can be detected from the network operator's side. Due to our cooperation with an European carrier we have been able to systematically perform real-world experiments and test our detection methods on real world-data.

Strong indicators we identified are for example the usage of invalid LACs (which are transmitted by the phones when they fall back to the genuine network after an attack), or the usage of weak ciphers to detect downgrade attacks for devices that were previously able to use strong ones. Additionally we showed that a number of weak indicators can be correlated geographically, temporally, and on subscriber basis e.g., for detecting targeted attacks, similar to current fraud detection schemes used by credit card companies. This includes fingerprinting devices based on profiles, unusual movements, and implausible location update trails. We also addressed corner cases and how to deal with them.

As mobile networks where initially designed with the reduction of signaling traffic in mind, not all of the necessary information is readily available for analysis, or even not collected centrally and in a scalable fashion. Some of the indicators we identified therefore demand changes in the monitoring systems currently used in such networks. However, based on already available data from a real-world mobile network, we were able to show the practical applicability for multiple of our methods.

Acknowledgments. We want to thank the whole crew of the core network security team and radio access network team at T-Mobile. They have been a great help. We are very grateful for the reviewers' comments and help to improve the quality of the paper and point to new interesting future work opportunities. This research was partially funded by the COMET K1 program through the Austrian Research Promotion Agency (FFG).

References

1. Digital cellular telecommunications system (Phase 2+); Interworking between Phase 1 infrastructure and Phase 2 Mobile Stations (MS). http://www.etsi.org/deliver/etsi_ts/101600_101699/101644/05.01.00_60/ts_101644v050100p.pdf
2. GSM security map. http://gsmmap.org/
3. How the NSA pinpoints a mobile device. http://apps.washingtonpost.com/g/page/world/how-the-nsa-pinpoints-a-mobile-device/645/. Accessed 30 Oct 2015
4. Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP), 3GPP TS 04.31 version 8.18.0 (2007). http://www.etsi.org/deliver/etsi_ts/101500_101599/101527/08.18.00_60/ts_101527v081800p.pdf
5. Egypt tries to control the use of GPS by banning except with individual licences (2008). http://www.balancingact-africa.com/news/en/issue-no-429/top-story/egypt-tries-to-contr/en
6. Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service (2012). http://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.01.01_60/ts_102900v010101p.pdf
7. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (2014). http://www.etsi.org/deliver/etsi_ts/123000_123099/123003/12.04.01_60/ts_123003v120401p.pdf
8. 3rd Generation Partnership Project: Non-Access-Stratum (NAS) Functions related to Mobile Station (MS) in Idle Mode, 3GPP TS 23.122 v8.2.0

9. 3rd Generation Partnership Project: Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS), 3GPP TS 24.301
10. Barkan, E., Biham, E., Keller, N.: Instant ciphertext-only cryptanalysis of GSM encrypted communication. J. Cryptol. **21**(3), 392–429 (2008)
11. Briceno, M., Goldberg, I., Wagner, D.: An implementation of the GSM A3A8 algorithm. (Specifically, COMP128.). http://www.scard.org/gsm/a3a8.txt. Accessed 24 Jun 2016
12. Briceno, M., Goldberg, I., Wagner, D.: GSM Cloning. http://www.isaac.cs.berkeley.edu/isaac/gsm.html. Accessed 24 Jun 2016
13. van den Broek, F., Verdult, R., de Ruiter, J.: Defeating IMSI catchers. In: 22nd ACM Conference on Computer and Communications Security (CCS 2015), pp. 340–351. ACM (2015)
14. Paget, C. (Kristin Paget): Practical Cellphone Spying. In: DEFCON 19 (2010)
15. Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., Weippl, E.: IMSI-Catch me if you can: IMSI-catcher-catchers. In: Proceedings of the Annual Computer Security Applications Conference (ACSAC 2014). ACM, December 2014
16. van Do, T., Nguyen, H.T., Momchil, N., et al.: Detecting IMSI-catcher using soft computing. In: Berry, M.W., Mohamed, A.H., Yap, B.W. (eds.) Soft Computing in Data Science. CCIS, vol. 545, pp. 129–140. Springer, Heidelberg (2015)
17. Dunkelman, O., Keller, N., Shamir, A.: A practical-time attack on the A5/3 cryptosystem used in third generation GSM telephony. IACR Cryptology ePrint Archive 2010, 13 (2010)
18. Ekdahl, P., Johansson, T.: Another attack on A5/1. IEEE Trans. Inf. Theor. **49**(1), 284–289 (2003)
19. Engel, T.: SS7: Locate. Track. Manipulate, at 31C3 (2014). https://events.ccc.de/congress/2014/Fahrplan/events/6249.html. Accessed 30 Oct 2015
20. Ettus Research: Universal Software Radio Peripheral. https://www.ettus.com/product
21. Farivar, C.: Apple removes GPS functionality from Egyptian iPhones (2008). http://www.macworld.com/article/1137410/Apple_removes_GPS_func.html
22. Gamma Group: 3G-GSM Interctiopn and Target Location. Sales brochure. https://info.publicintelligence.net/Gamma-GSM.pdf. Accessed 2 Nov 2015
23. Goldberg, I., Wagner, D., Green, L.: The (Real-Time) Cryptanalysis of A5/2. In: Rump Session of Crypto 1999 (1999)
24. GSM Association: IR.50 2G 2.5G 3G Roaming v4.0 (2008). http://www.gsma.com/newsroom/all-documents/ir-50-2g2-5g3g-roaming/. Accessed 25 Sep 2015
25. Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support. http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip
26. Güneysu, T., Kasper, T., Novotny, M., Paar, C., Rupp, A.: Cryptanalysis with COPACOBANA. IEEE Trans. Comput. **57**(11), 1498–1513 (2008)
27. Steve, H.D.: Cracking GSM. In: Black Hat DC, March 2008 (2008)
28. Joachim, F., Rainer, B.: Method for identifying a mobile phone user or for eavesdropping on outgoing calls, patent, Rohde & Schwarz, EP1051053 (2000)
29. SR Labs: Kraken: A5/1 Decryption Rainbow Tables. via Bittorent (2010). https://opensource.srlabs.de/projects/a51-decrypt. Accessed 12 Nov 2015
30. Liu, J., Yu, Y., Standaert, F.X., Guo, Z., Gu, D., Sun, W., Ge, Y., Xie, X.: Small tweaks do not help: differential power analysis of MILENAGE implementations in 3G/4G USIM cards. In: Pernul, G., Ryan, P.Y.A., Weippl, E. (eds.) ESORICS 2015. LNCS, vol. 9326, pp. 468–480. Springer, Heidelberg (2015)

31. Malette, L.: Catcher Catcher. https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/CatcherCatcher. Accessed 12 Nov 2015
32. Muncaster, P.: Chinese cops cuff 1,500 in fake base station spam raid. The Register, 26 March 2014. http://www.theregister.co.uk/2014/03/26/spam_text_china_clampdown_police/
33. Nohl, K.: Rooting SIM cards. In: Blackhat (2013)
34. Nohl, K.: Mobile self-defense, 31C3 (2014). https://events.ccc.de/congress/2014/Fahrplan/events/6122.html. Accessed 30 Oct 2015
35. Osipov, A., Zaitsev, A.: Adventures in Femtoland: 350 Yuan for invaluable fun. In: Black Hat USA 2015, August 2015
36. Pell, S.K., Soghoian, C.: Your secret stingray's no secret anymore: the vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy. Harvard J. Law Technol. **28**(1) (2014)
37. SecUpwN (Pseudonym, Maintainer): Android IMSI-Catcher Detector. https://secupwn.github.io/Android-IMSI-Catcher-Detector/. Accessed 12 Nov 2015
38. Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., Seifert, J.: Practical attacks against privacy and availability in 4G/LTE mobile communication systems (2015). http://arxiv.org/abs/1510.07563
39. Solnik, M., Blanchou, M.: Cellular exploitation on a global scale: the rise and fall of the control protocol. In: Blackhat 2014, Las Vegas (2014)
40. SR Labs: Snoopsnitch, December 2014. https://opensource.srlabs.de/projects/snoopsnitch. Accessed 12 Nov 2015
41. Tu, G., Li, Y., Peng, C., Li, C., Raza, M.T., Tseng, H., Lu, S.: New threats to sms-assisted mobile internet services from 4G LTE networks (2015). http://arxiv.org/abs/1510.08531
42. Welte, H.: OpenBSC - running your own GSM network, talk at Hacking at Random, August 2009. https://openbsc.osmocom.org/trac/raw-attachment/wiki/FieldTests/HAR2009/har2009-gsm-report.pdf