Glossary of Terms

Jump to bottom

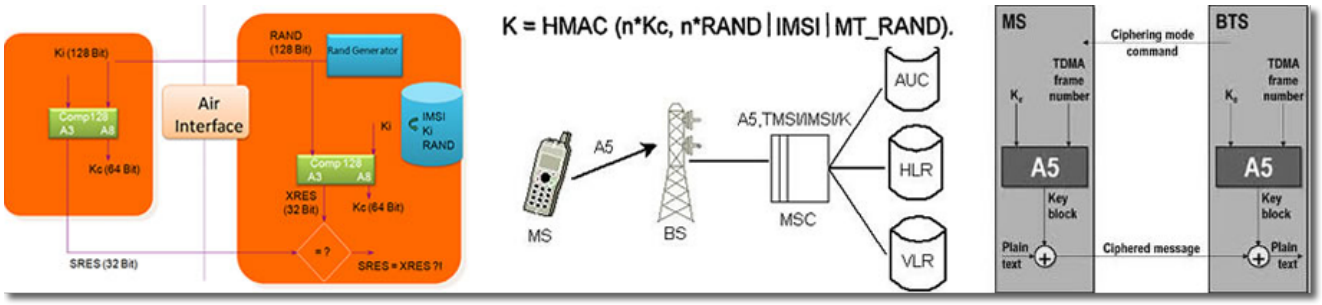
Security: Pwned edited this page on Feb 9, 2016 · 19 revisions

This page shall help you understand all the abbreviations we use in our project.

Index of Terms

- GSM Handover
- GSM Security
- IMEI
- IMSI-Catcher
- IMSI-Catcher Software
- LAC
- MCC
- MNC
- MSISDN
- PSC
- SIM Card
- Silent Call
- Silent SMS
- Spy Call
- TMSI
- Triangulation

A5/0, A5/1, A5/2, A5/3, A5/4



The GSM ciphering algorithm is called A5. For technical details and attacks see the Cryptome GSM Files. There are four variants of A5 in GSM, only the first three are widely deployed:

- A5/0: No ciphering at all
- A5/1: Strong(er) ciphering, intended for use in North America and Europe
- A5/2: Weak ciphering, intended for other countries, now deprecated by GSMA
- A5/3: Even stronger ciphering with open design, also called KASUMI
- A5/4: The essential change is the key length input from 64 bits to 128 bits

A5/1

> Is a stream cipher used to provide over-the-air communication privacy in the GSM

> cellular telephone standard. It was initially kept secret, but became public knowledge through leaks and reverse engineering. A number of serious weaknesses in the cipher have been identified. A5/1 is used in Europe and the United States.

A5/2

> Is a stream cipher used to provide voice privacy in the GSM cellular telephone protocol. A5/2 was a deliberate weakening of the algorithm for certain export regions. The cipher is based around a combination of four linear feedback shift registers with irregular clocking and a non-linear combiner.

A5/3

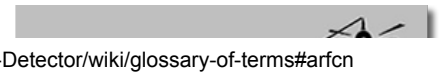
> KASUMI was designed for 3GPP to be used in UMTS security system by the Security Algorithms Group of Experts (SAGE), a part of the European standards body ETSI. Because of schedule pressures in 3GPP standardization, instead of developing a new cipher, SAGE agreed with 3GPP technical specification group (TSG) for system aspects of 3G security (SA3) to base the development on an existing algorithm that had already undergone some evaluation.

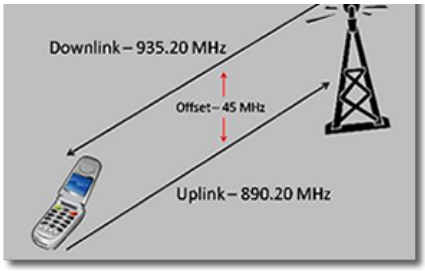
A5/4

> Based on A5/3, the only essential change is the external key length input from 64 bits to 128 bits. For more information please see the Specification of the A5/4 Encryption Algorithms and GSMA Security Algorithms. Although A5/4 was developed and clearly specified at the same time as A5/3, there are no known mobile network providers who have implemented this, as of today.

ARFCN

> In GSM cellular networks, an absolute radio-frequency channel number (ARFCN) is a code that specifies a pair of physical radio carriers used for transmission and reception in a land mobile radio system, one for the uplink signal and one for the downlink signal. This network parameter is used to force the cell phones to send registration requests to a false BTS (IMEI/IMSI-Catcher).





Authentication Key (Ki)

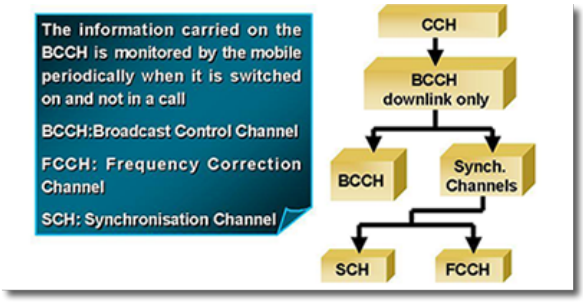
> The Authentication Key or Ki is a 128 bit key used in the authentication and cipher key generation process. In a nutshell, the key is used to authenticate the SIM on the GSM network. Each SIM contains this key which is assigned to it by the operator during the personalization process. The SIM card is specially designed so the Ki can't be compromised using a smart-card interface.

Ciphering Key (Kc)

> The SIM contains the Ciphering Key generating algorithm (A8) which is used to produce the 64-bit Ciphering Key (Kc). The Ciphering Key is computed by applying the same random number (RAND) used in the authentication process to the Ciphering Key generating algorithm (A8) with the individual subscriber authentication key (Ki). The Ciphering Key (Kc) is used to encrypt and decrypt the data between the MS and BS. However, a passive GSM Interceptor can extract and calculate remotely the Ciphering Key and using it for deciphering in real time.

BCCH

> A broadcast control channel (BCCH) is a point to multipoint, unidirectional (downlink) channel used in the Um interface of the GSM cellular standard. The BCCH carries a repeating pattern of system information messages that describe the identity, configuration and available features of the base transceiver station (BTS).



BCCH Manipulation

> A special technique. GSM Interceptors (IMEI/IMSI-Catchers) uses BCCH manipulation to give a "virtual power" effect of up to several hundred watts. By doing that, a GSM Interceptor will trick the handsets, which will always choose the "BTS" with the strongest signal. As well, by changing Cell ID (all other network parameters remains the same - MCC, MNC, LAC) and ARFCN, the Interceptor is forcing the cell phones within the area to send registration requests, collecting this way phones identifiers: IMSI, IMEI, classmark, etc.

BTS

> The Base Transceiver Station contains the equipment for transmitting and receiving radio signals (transceivers), antennas, and equipment for encrypting and decrypting communications with the base station controller (BSC).

Carrier/Provider

> A company that provides GSM telecommunications services.

Cell

> In personal communications systems (cellular mobile phone systems) a cell is the geographic area served by a single base station. Cells are arranged so that base-station frequencies can be reused between cells. The area surrounding a cell site. The area in which calls are handled by a particular cell site.

Cell ID

> A GSM Cell ID (CID) is a generally unique number used to identify each Base transceiver

> A GSM Cell ID (CID) is a generally unique number used to identify each Base transceiver station (BTS) or sector of a BTS within a Location area code (LAC) if not within a GSM network. In some cases the last digit of CID represents cells' Sector ID. This network parameter is used in so called BCCH manipulation by GSM Interceptors. By changing Cell ID (all other network parameters remains the same - MCC, MNC, LAC) and ARFCN, the system is forcing the cell phones within the area to send registration requests, collecting this way phones identifiers: IMSI, IMEI, classmark, etc.

Cell Site

> The transmission and reception equipment, including the base station antenna, that connects a cellular phone to the network.

Channel Coding

> Channel coding is the technique of protecting message signals from signal impairments by adding redundancy to the message signal.

Fade

> A fade is a slow change in signal strength.

GSM 1800

> The GSM 1800 band provides for a GSM uplink in the range 1710-1785 MHz, a GSM downlink in the range 1805-1880 MHz.

GSM 1900

> The GSM 1900 band provides for a GSM uplink in the range 1850-1910 MHz, a a GSM downlink in the range 1930-1990 MHz

GSM 900

> The GSM 900 band provides for a GSM uplink in the range 890-915 MHz, a a GSM downlink in the range 935-960 MHz.

GSM Air Interface

> The GSM air interface operates in the UHF frequency band.

GSM Architecture

> A GSM network consists of the mobile station, the base station system, the switching system, and the operation and support system. GSM Base Station System (BSS) The GSM base station system (BSS) provides the interface between the GSM mobile phone and other parts of the GSM network.

GSM Channels

> GSM provides two types of channel: traffic channels and signalling channels.

GSM Handover

> Handover refers to the process by which a GSM mobile phone's affiliation is transferred from one base station to another.

GSM Security

> GSM provides a number of security services, including authentication, key generation, encryption and limited privacy.

IMEI

> The International Mobile Station Equipment Identity or IMEI is a number, usually unique, to identify 3GPP (i.e., GSM, UMTS and LTE) and iDEN mobile phones, as well as some satellite phones. On most phones you can dial `*#06#` to see this number. The IMEI number is used by a GSM network to identify valid devices and is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. It is also used by IMEI/IMSI-Catchers / GSM Interceptors in order to identify your phone and performing call interception.

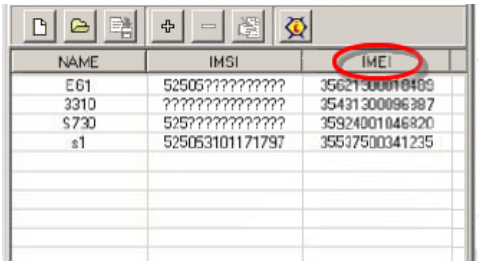
IMSI-Catcher

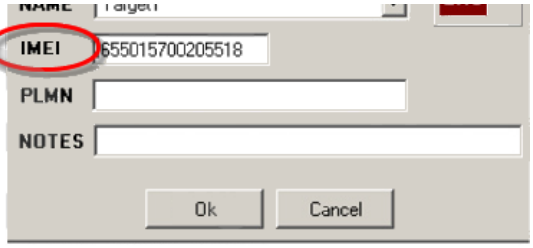
IMSI-Catchers

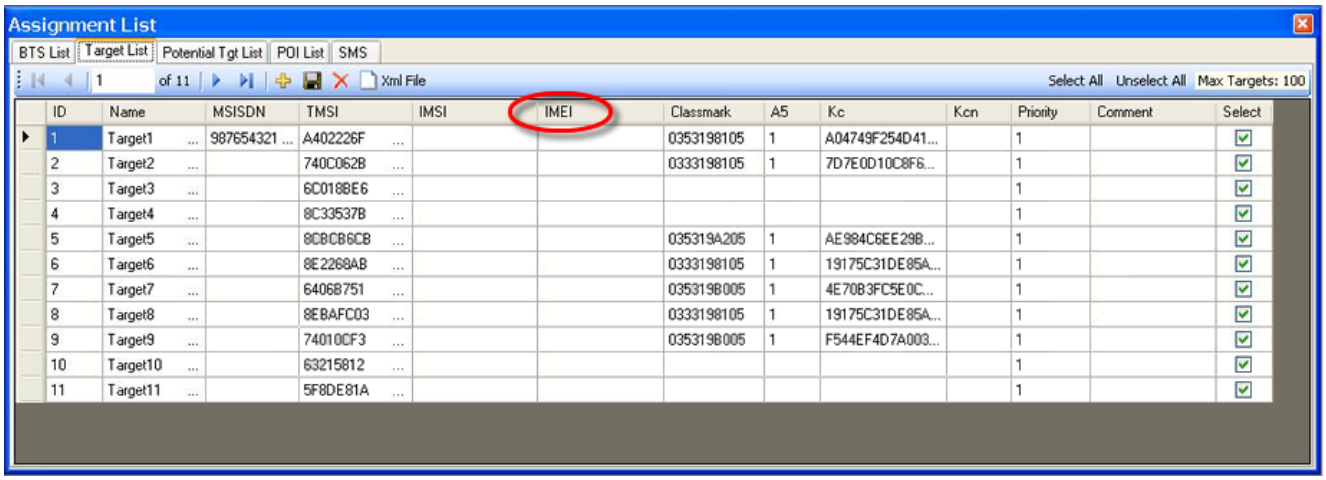
> Is essentially a false mobile tower acting between the target mobile phone(s) and the service providers real towers. As such it is considered a Man In the Middle (MITM) attack. It is used as an eavesdropping device used for interception and tracking of cellular phones and usually is undetectable for the users of mobile phones. Such a virtual base transceiver station (VBTS) is a device for identifying the International Mobile Subscriber Identity (IMSI) of a nearby GSM mobile phone and intercepting its calls. The IMSI-Catcher masquerades as a base station and logs the IMSI numbers of all the mobile stations in the area, as they attempt to attach to the IMSI-Catcher. It allows forcing the mobile phone connected to it to use no call encryption (i.e., it is forced into A5/0 mode), making the call data easy to intercept and convert to audio.

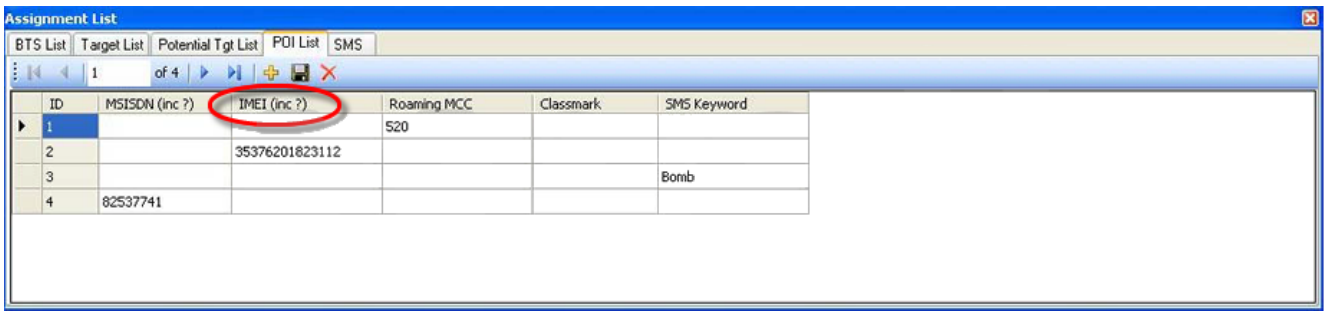
IMSI-Catcher Software

While there exist many software interfaces, here are some leaked screenshots:

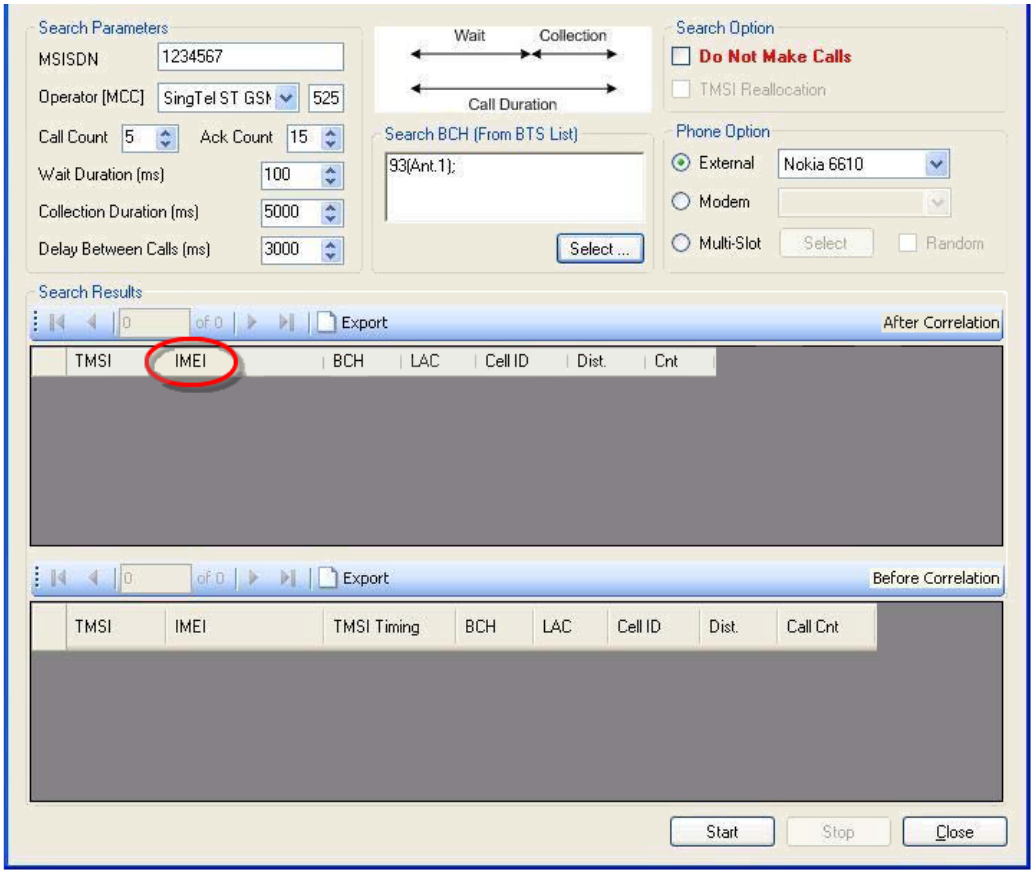

NAME
IMSI
IMEI
E61
525057??????????
3310
????????????????
S730
525?????????????
s1
525053101171797

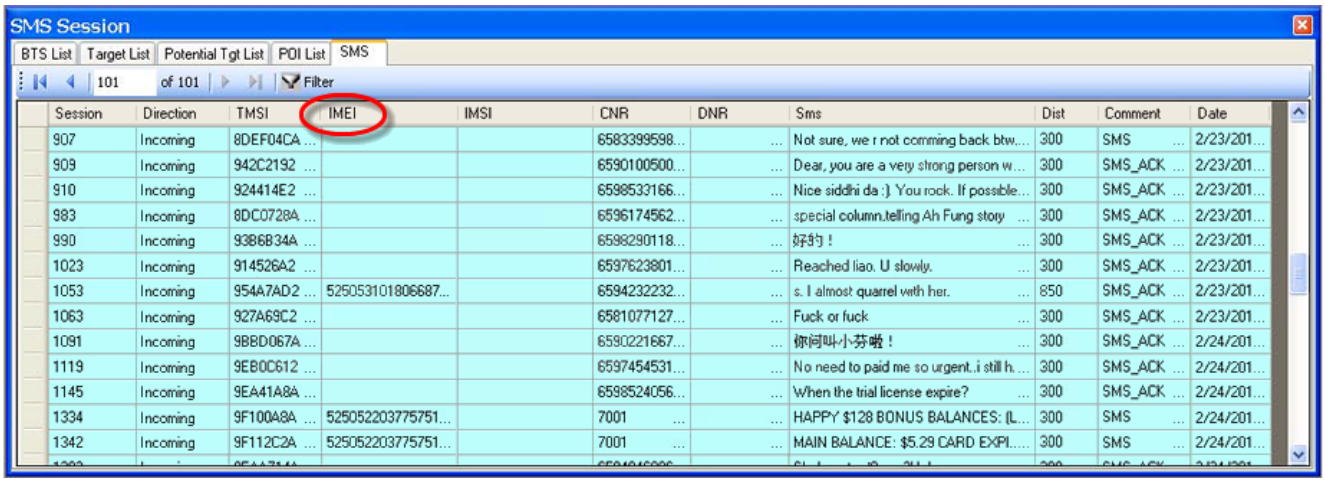

IMEI
355015700205518
PLMN
NOTES
Ok
Cancel


Assignment List
BTS List
Target List
Potential Tgt List
POI List
SMS
Xml File
Select All
Unselect All
Max Targets: 100
ID
Name
MSISDN
TMSI
IMSI
IMEI
Classmark
A5
Kc
Kcn
Priority
Comment
Select
1 Target1 987654321 A402226F 0353198105 1 A04749F254D41... 1
2 Target2 740C062B 0333198105 1 7D7E0D10C8F6... 1
3 Target3 6C018BE6 1
4 Target4 8C33537B 1
5 Target5 8CBCB6CB 035319A205 1 AE984C6EE29B... 1
6 Target6 8E2268AB 0333198105 1 19175C31DE85A... 1
7 Target7 64068751 035319B005 1 4E70B3FC5E0C... 1
8 Target8 8EBAFC03 0333198105 1 19175C31DE85A... 1
9 Target9 74010CF3 035319B005 1 F544EF4D7A003... 1
10 Target10 63215812 1
11 Target11 5F8DE81A 1


Assignment List
BTS List
Target List
Potential Tgt List
POI List
SMS
of 4
ID
MSISDN (inc ?)
IMEI (inc ?)
Roaming MCC
Classmark
SMS Keyword
1 520
2 35376201823112
3 Bomb
4 82537741


Silent Call





LAC

> Location Area Code, unique number broadcast by a "base transceiver station" in GSM. A "location area" is a set of base stations that are grouped together to optimise signalling. Typically, tens or even hundreds of base stations share a single Base Station Controller (BSC) in GSM, or a Radio Network Controller (RNC) in UMTS, the intelligence behind the base stations. The BSC handles allocation of radio channels, receives measurements from the mobile phones, controls handovers from base station to base station.

MCC

> Mobile Country Code (MCC), used in wireless telephone network station addressing.

MNC

> A Mobile Network Code (MNC) is used in combination with a mobile country code (MCC) (also known as a "MCC / MNC tuple") to uniquely identify a mobile phone operator/carrier using the GSM/LTE, CDMA, iDEN, TETRA and UMTS public land mobile networks and some satellite mobile networks.

MSISDN

> Is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. Simply put, it is the telephone number to the SIM card in a mobile/cellular phone. This abbreviation has several interpretations, the most common one being "Mobile Subscriber Integrated Services Digital Network-Number". See also Silent Call.

PSC

The following well-written comment has been found on StackOverflow:

> In UMTS, the PSC is a kind of local cell identifier. It is "locally" unique in that all neighboring cell, as well as all neighbors of these cells, are guaranteed to have a different PSC than the current cell. It also means that you will not ever encounter two neighboring cells with the same PSC. However, there may well be cells with the same PSC located in different parts of the country.

> The NeighboringCellInfo for a UMTS cell will only have the PSC set while all other fields (MCC, MNC, LAC, CID) will be invalid. The only way to find out these parameters would be to store all fields (MCC, MNC, LAC, CID as well as PSC) for every cell you encounter, then upon getting an "unknown" PSC look it up in the stored data. (You would need to filter for neighbors of the serving cell, as the PSC is only a locally unique ID, not a globally unique one).

> As an alternative, the PSC of a cell along with the MCC/MNC/LAC/CID tuple of one of its neighbors is also a globally unique ID that you could use. Be aware, however, that each cell would have multiple such identifiers (one for each neighbor).

SIM Card

> The Smart Card gives GSM phones their user identity. SIM Cards make it easy for phones to be rented or borrowed.

Silent Call

> In terms of GSM interception, a silent call is a call originated from the GSM Interceptor to a specific IMEI/IMSI, in order to make correlations between IMEI/IMSI and MSISDN (Mobile Subscriber Integrated Services Digital Network-Number, which is actually the telephone number to the SIM card in a mobile/cellular phone). By using the silent call, an GSM Interceptor can find out a certain phone number alocated to a specific IMEI/IMSI. Silent calls are a result of process known as pinging. This is very similar to an Internet Protocol (IP) ping. A silent call cannot be detected by a phone user. Not to be confused with Spy Call, which mean listen to phone surroundings.

Silent SMS

Many foreign police and intelligence services use clandestine "Silent" SMS to locate suspects or missing persons. This method involves sending an SMS text message to the mobile phone of a suspect, an SMS that goes unnoticed and sends back a signal to the sender of the message.

> Also known as Type0-SMS, the Silent SMS uses an invisible return signal, or "ping"

> Also known as "type 0" SMS, the Silent SMS uses an invisible return signal, or "ping".
> Developers from the Silent Services company, who created some of the first software for sending this type of SMS, explain: "The Silent SMS allows the user to send a message to another mobile without the knowledge of the recipient mobile's owner. The message is rejected by the recipient mobile, and leaves no trace. In return, the sender gets a message from a mobile operator confirming that the Silent SMS has been received." Silent SMS were originally intended to allow operators to ascertain whether a mobile phone is switched on and to "test" the network, without alerting the users. But now, intelligence services and police have found some other uses for the system. Neil Croft, a graduate of the Department of Computer Science at the University of Pretoria in South Africa, explains: "Sending a Silent SMS is like sending a normal SMS, except that the mobile does not see the message it has received. The SMS's information is modified, within the data coding scheme, so that the user who receives the message doesn't notice anything. A Silent SMS can help police to detect a mobile without the person concerned being aware of the request."

> Technical bit: in order to tamper with the SMS's information and make it silent, the security services go through a network for sending and receiving SMS known as an SMS gateway, such as the Jataayu SMS gateway. This allows them to interconnect the processing and GSM systems. This method of mass sending appears to be widely used by these security services. In November 2011, Anna Conrad of the left party in Germany, posed a written question to her local state assembly concerning the use of Silent SMS by the German police. Her local assembly responded: in 2010, Germany conducted 778 investigations and sent 256,000 Silent SMS.

> Mathias Monroy, a journalist with Heise Online, argues this surveillance technology is flourishing largely as a result of a legal vacuum: "This is very problematic for privacy, because legally it is unclear whether or not a Silent SMS counts as a communication (...) The state found that it was not one, since there is no content. This is useful, because if it is not a communication, it does not fall under the framework of the inviolability of telecommunications described in Article 10 of the German Constitution." On December 6, the German Interior Minister Hans-Peter Friedrich announced that German police and intelligence had been sending an average of 440,000 Silent SMS a year since they began using the system. After each SMS was sent, investigators went to the four German mobile operators – Vodafone, E-Plus, O2 and T-Mobile – in order to access the recipient's information. To aggregate this raw data provided by operators, the police use Koyote and rsCase, software supplied by Rola Security Solutions, a company that develops "software solutions for the police".

> Silent SMS allow the user to precisely locate a mobile phone by using the GSM network

Silent SMS allow the user to precisely locate a mobile phone by using the GSM network, as Karsten Nohl explains: "We can locate a user by identifying the three antennas closest to his mobile, then triangulating the distance according to the speed it takes for a signal to make a return trip. A mobile phone updates its presence on the network regularly, but when the person moves, the information is not updated immediately. By sending a Silent SMS, the location of the mobile is instantly updated. This is very useful because it allows you to locate someone at a given time, depending on the airwaves." This technique is much more effective than a simple cellular location (Cell ID), as François-Bernard Huyghe, a researcher at IRIS, sets out: "This is the only instantaneous and practical method to track a mobile constantly when it's not in use. We're talking then about geopositioning rather than geolocation. After that, either the police track the information via the operators, or private companies process the data and, for example, refer the investigator to a map where the movements of the monitored phone appear in real time."

The benefits of Silent SMS don't stop there: by sending a large number of these SMS, security services can also disrupt the mobile or remotely reactivate its signal and wear out the battery. A spokesman for the German Interior Ministry tells OWNI: "German police and intelligence services use Silent SMS to reactivate inactive mobile phones and refine the geolocation of a suspect, for example when they move during an interview. The Silent SMS is a valuable investigative tool, which is used only as part of a telecommunications surveillance operation sanctioned by a judge, in a specific case, without violating the fundamental right to protection of privacy."

In France, police and intelligence services work with Deveryware, a "geolocation operator". Deveryware also market a "geolocation employee punchcard", the Geohub, to businesses. Deveryware combine cellular localization, GPS, and other "real-time location" techniques. Questioned by OWNI whether Silent SMS were one of these techniques, the company's response was evasive: "Regretfully we are unable to provide an answer, given the confidentiality imposed on us by legal requisitions." Deveryware's applications enable investigators to map and compile a history of a suspect's movements. Laurent Ysern, head of investigations for SGP Police, states: "All investigative services have access to the Deveryware platform. With this system, one can follow a person without having to be behind them. There's no need for shadowing, so less staff and equipment needs to be mobilized."

While in Germany the Ministry of the Interior responded within 48 hours, the French

> While in Germany the Ministry of the Interior responded within 48 hours, the French government remains strangely silent. There has been one single response, from the Press Department of the National Police: "Unfortunately, no one at the PJ (Police Judiciare) or the public safety office is willing to comment on the subject, these are investigative techniques ..." Silence too from the French telecoms operators SFR and Bouygues Telecom. Sebastien Crozier, a union delegate at France Telecom-Orange, says: "Operators always collaborate with the police, it's a public service obligation: they act in accordance with judicial requests...There is no definitive method, sending SMS is one of the methods used to geolocate a user. We mainly use this technique to "reactivate" the phone."

> By 2013, the use of these surveillance methods is expected to reach an industrial scale. The Department of Justice will set up, with the help of the arms company Thales, a new national platform of judicial interception (PNIJ), which is expected to centralize all legal interception, i.e, phone-tapping, but also summons such as requests for cell location. Sebastien Crozier remarks: "This interface between police officers and operators will streamline court costs and reduce processing costs by half, because until now summons have been handled station by station...There will be more applications, but it will be less expensive for operators like the police." (source)

Spy Call

> A Spy Call is a call made from a GSM Interceptor to a mobile phone, in order to listen to phone surroundings. This call cannot be detected by the phone user.

TMSI

> The Temporary Mobile Subscriber Identity (TMSI) is the identity that is most commonly sent between the mobile and the network. TMSI is randomly assigned by the VLR to every mobile in the area, the moment it is switched on. The number is local to a location area, and so it has to be updated each time the mobile moves to a new geographical area.

> The network can also change the TMSI of the mobile at any time. And it normally does so, in order to avoid the subscriber from being identified, and tracked by eavesdroppers on the radio interface. This makes it difficult to trace which mobile is which, except briefly, when the mobile is just switched on, or when the data in the mobile becomes invalid for one reason or another. At that point, the global "international mobile subscriber identity" (IMSI) must be sent to the network. The IMSI is sent as rarely as possible, to avoid it being identified and tracked.

Triangulation

- How does the pinpointing of mobile users work, and just how accurate is it?

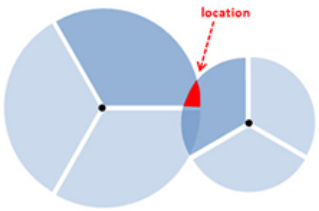
> There are two methods for pinpointing the location of cell phone users. Cell phones equipped with Global Positioning System (GPS) capability, use signals from satellites to pinpoint location very accurately. The second, and less-accurate method is often called “Cell Tower Triangulation”, referring to how the cell towers which receive a phone’s signal may be used to calculate its geophysical location. According to some industry research estimates, only about 11% of phones manufactured this year will have the GPS capability, so the remaining 89% of phones without GPS would have to depend upon “Cell Tower Triangulation” in order to disclose geolocation data for applications.

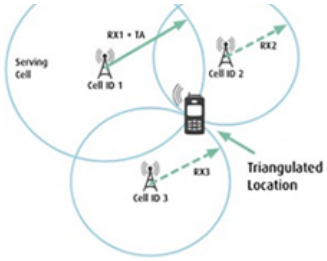
- Just what is Cell Tower Triangulation?

> In a best-case-scenario, a cell phone's signal may be picked up by three or more cell towers, enabling the "triangulation" to work. From a geometric/mathematical standpoint, if you have the distance to an item from each of three distinct points, you can compute the approximate location of that item in relation to the three reference points. This geometric calculation applies in the case of cell phones, since we know the locations of the cell towers which receive the phone's signal, and we can estimate the distance of the phone from each of those antennae towers, based upon the lag time between the towers ping sent to the phone and the answering ping back.

> In many cases, there may actually be more than three cell towers receiving a phone’s signal, allowing for even greater degrees of accuracy (although the term “triangulation” isn’t really correct if you’re using more than three reference points). In densely developed, urban areas, the accuracy of cell phone pinpointing is considered to be very high because there are typically more cell towers with their signal coverage areas overlapping. In cases where a cell user is inside large structures or underground, cell tower triangulation may be the only location pinpointing method since GPS signal may not be available.

> For many cell tower networks, the pinpointing accuracy may be even greater, since directional antennae may be used on the tower, and thus the direction of the cell phone’s signal might be identifiable. With the signal direction plus the distance of the phone from the cell tower, accuracy might be pretty good, even with only two towers.





> However, there are many places where there are fewer cell towers available, such as in the fringes of the cities and out in the country. If you have fewer than three cell towers available, pinpointing a mobile device can become a lot less precise. In cities where there are a lot more vertical structures which can be barriers to cell phone broadcasting and receiving, there have to be many more cell towers distributed in order to have good service. In the countryside, there are relatively fewer cell towers and a phone's signal may be picked up only by a single one at much greater distance. Those areas where a phone is only getting picked up by a single tower, and if it's equipped with only omnidirectional antennae, the accuracy becomes even less. In rural areas, coverage of the cell tower can vary from about a quarter of a mile to several miles, depending upon how many obstacles are blocking the tower's signal.

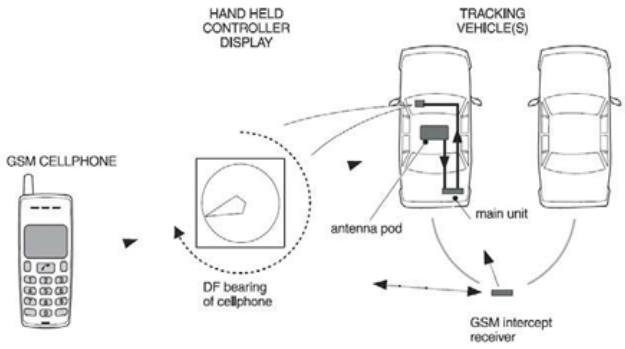
- How extensive is government monitoring?

> No civilian is authorised to know. Some governments in the EU, such as the UK government, have laws and practices that allow the government to collect and use intelligence in legal cases without disclosing their sources or methods. Chapter 8 of the Crown Prosecution Service's Disclosure Manual includes: "the ability of the law enforcement agencies to fight crime by the use of covert human intelligence sources, undercover operations, covert surveillance, etc" and "the protection of secret methods of detecting and fighting crime". According estimates made by whistleblower William Binney, a former director of the US NSA's World Geopolitical and Military Analysis Reporting Group), the US NSA alone has assembled 20 trillion "transactions" − phone calls, emails and other forms of data − just from Americans (April, 2012). Government agencies are not the only organisations interested in the personal data stored on, or transmitted through, your mobile phone. Self-styled cyber criminals are now jumping on the bandwagon to reap benefits previously enjoyed only by government and intelligence agencies.

- Target phone location performed by GSM Interceptor with target location capabilities

> The method of operation is based on two vehicles. First vehicle with the interception

> The method of operation is based on two vehicles. First vehicle with the interception system that forces the target phone to send continues signal transmission. The second vehicle is deployed with the Interceptor and location components. The direction to target is displayed as a compass pointer and the relative signal strength is shown as a bar graph and numerically. The audio tone increases in frequency as Interceptor gets closer to the target giving a clear warning of a close encounter.



Certain Images and texts were kindly provided by

Questions or need help? Get in touch, post in our development thread or open an Issue!

▸ **Pages** 33

Project Information

- Unmasked Spies
- Glossary of Terms
- General Overview
- Technical Overview

Getting started

- Building
- Requirements
- Installation
- Permissions
- Status Icons

Developers

- Development Status

- Development Status
- Testing Devices
- Detection Tests
- Contributing
- Style Guide
- Resources
- Privacy

Navigation Menus

- Disclaimer
- Main Screen
- Navigation Drawer
- Preferences
- About AIMSICD

Important Functions

- Cell Monitoring
- Current Threat Level
- AT Command Interface
- Database Viewer
- Antenna Map Viewer
- Special SMS

Support

- FAQ
- Contact
- Problems
- Donations

Gimme moar!

- Media Material
- Press Releases
- Recommendations
- Similar Projects

Clone this wiki locally

```
https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector.wiki.git
```