IMSI-Catcher

<<TableOfContents>>

= IMSI-Catcher =

WikiPedia:IMSI-Catcher sind kleine inoffizielle GSM-Funkzellen. Sie spiegeln Mobiltelefonen in der unmittelbaren Umgebung (10 bis 100 Metern) einen starken Sendemast vor. Telefone, die nicht vom Netz gemanagt werden (also im Groben solche, mit denen gerade nicht telefoniert wird) versuchen sich daraufhin, sich auf die "gefälschte" Funkzelle einzubuchen. Da dies einen Location Update bewirkt, kann der IMSI-Catcher die [[https://de.wikipedia.org/wiki/International_Mobile_Subscriber_Identity|IMSI]] (also die Teilnehmerkennung) der im betroffenen Netz aktiven Telefone auslesen. Auch das Mithören von Mobilfunktelefonaten ist möglich. Dabei werden allerdings auch Daten Unbeteiligter im Funknetzbereich des IMSI-Catchers erfasst, ohne dass diese es erfahren.

Der IMSI-Catcher legt darüber hinaus unter Umständen den gesamten Mobilfunkverkehr der betroffenen Mobiltelefone lahm, sodass auch Notrufe nicht möglich sind. IMSI-Catcher werden hauptsächlich zur Bestimmung des Standortes und zum Erstellen eines Bewegungsprofils von Personen benutzt. Eingesetzt werden IMSI-Catcher hauptsächlich von Strafverfolgungsbehörden und Nachrichtendiensten, können aber mittlerweile leider auch für wenig Geld [[http://heise.de/-1048919|nachgebaut]] werden. Eigenkonstruktionen werden von [[https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/|Kriminellen in China]] zum Beispiel schon lange dazu genutzt, um SPAM-SMS zu verschicken.

Die krasseste Verwendung erfolgt jedoch durch die NSA, welche mit IMSI-Catchern ausgestattete Drohnen dazu nutzt um Menschen vollautomatisch und ohne jegliche menschliche Nachkontrolle auf Basis von Metadaten zu töten - siehe [[https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/|NSA’s Secret Role in the U.S. Assassination Program]]. Dabei sterben nicht nur die Zielpersonen, sondern auch unzählige Zivilisten. Da IMSI-Catcher im Prinzip nichts anderes tun, als still und heimlich die Daten der Telefone von Zielpersonen massenhaft abzugreifen und ihnen dann durch die weiteren Maßnahmen der Behörden Schaden zuzufügen, ist die Open-Source Community aktiv geworden und entwickelt eine App für Android als Gegenmaßnahme. Sicherheitsbewusste Android-Entwickler werden gebeten, mit Ihrem Code und Engagement im Projekt die Welt zum Besseren zu verändern. Siehe [[http://www.datenschmutz.de/moin/IMSI-Catcher#Nachweis_eines_IMSI-Catchers|Nachweis eines IMSI-Catchers]].

== Einsatzgebiete von IMSI-Catchern ==

Die Bedarfsträger können dies auf zwei Arten nutzen:

- Feststellen, ob sich ein gesuchtes Telefon innerhalb der Reichweite befindet
- Ermittlung der IMSI von unbekannten Telefonen.

Die Lokalisierung von Telefonen scheint derzeit der Haupteinsatzzweck zu sein. Dies ist z.B. relevant, um eine Hausdurchsuchung zur Ergreifung von Flüchtlingen zu rechtfertigen.

Die Ermittlung von IMSIs kommt als Gegenmaßnahme für auf falsche Namen registrierte Telefone in Betracht. Dabei wird der IMSI-Catcher an zwei verschiedenen Orten gegen eine observierte Person eingesetzt; die beiden Datensätzen gemeinsame IMSI ist die des von der Person mitgeführten Telefons.

== Funktionsweise von IMSI-Catchern ==

IMSI-Catcher funktionieren so nur im GSM-Netz. UMTS-Telefone fallen allerdings meist auf GSM zurück, wenn es ein starkes GSM-Signal gibt, so dass sie derzeit meist noch gegen IMSI-Catcher anfällig sind.

Wie ein IMSI-Catcher 2011 aussieht, ist aus dem <<Doclink(2011-elaman-katalog.pdf,Elaman-Katalog von 2011)>> zu entnehmen (PDF-Seite 12); die dort versprochene Funktion, auch in UMTS-Netzen die Funktionalität von IMSI-Catchern bereitszustellen, bezieht sich aber nur auf die Lokalisierung von Endgeräten, nicht auf die Aufzählung von IMSIs in der Umgebung.

Während ein IMSI-Catcher läuft, sind betroffene Telefone nicht anrufbar und können idR auch selbst keine Gespräche anfangen (da der IMSI-Catcher ja keine echte Verbindung zum Netz hat). Der Ausfall beschränkt sich aber auf allenfalls wenige Minuten pro Netz. Laufende Telefongespräche werden nicht beeinflusst, da Telefone im dedicated mode die Funkzellen vom Netz zugewiesen bekommen und das Netz die vom IMSI-Catcher vorgetäuschte Funkzelle nicht kennt.

== Nachweis eines IMSI-Catchers ==

Es ist im Prinzip denkbar, die Aktivität eines IMSI-Catchers durch Beobachtung der vom Telefon bevorzugten Zelle festzustellen. Die Cell- und LA-ID lässt sich bei manchen Telefonen anzeigen. Programme wie [[http://www.gnokii.org/|gnokii]] erlauben dies bei Anschluss an den Rechner. [[http://www.opencellid.org/|opencellid.org]] erlaubt, nachzusehen, ob die Zelle plausibel ist.

Wer das per Hand machen will: Nach Aufbau einer seriellen Verbindung zum Telefon schickt man zunächst AT+CREG=2 an das Telefon. Das Kommando AT+CREG? gibt dann Location Area und Cell ID zurück. Mit Freier Baseband-Firmware wie [[http://bb.osmocom.org/trac/|osmocom]] lassen sich da noch weit bessere Systeme bauen.

Ein großartiges open-source Projekt auf GitHub zur Enttarnung von IMSI-Catchern sowie [[https://de.wikipedia.org/wiki/Stille_SMS|stillen SMS]] ist der sogenannte [[http://secupwn.github.io/Android-IMSI-Catcher-Detector/|Android IMSI-Catcher Detector (AIMSICD)]]. Dieses mutige Projekt sucht dringend noch sicherheitsbegeisterte Android-Entwickler und Tester. Teilt den Link in allen sozialen Netzwerken!

== Weiteres ==

- Für die geplante Beschaffung von IMSI-Catchern gab es 2000 einen [[http://www.bigbrotherawards.de/2000/.pol|Big Brother Award]] für Eckart Werthebach als damaligen Innensenator von Berlin.

- Im Zusammenhang der [[TK-Verkehrsdaten#Sachsen-Sumpf|19/2-Verfahren in Dresden]] ([[Sachsen]]) wurden IMSI-Catcher eingesetzt, um zwei Verdächtige des [[129a Verfahren|129er-Verfahrens]] zu orten.
- [[Überwachungstechnik]]

Version #1
Erstellt: 2025-10-27 22:27:35 UTC von Datenschmutz Migration Bot
Zuletzt aktualisiert: 2025-10-27 22:27:35 UTC von Datenschmutz Migration Bot