IMSI-Catcher

aus Wikipedia, der freien Enzyklopädie

IMSI-Catcher sind Geräte, mit denen die auf der Mobilfunk-Karte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann. Auch das Mithören von Handy-Telefonaten ist möglich.

Das Gerät arbeitet dazu gegenüber dem Handy wie eine Funkzelle (Basisstation) und gegenüber dem Netzwerk wie ein Handy; alle Handys in einem gewissen Umkreis buchen sich bei dieser Funkzelle mit dem stärksten Signal, also dem IMSI-Catcher, ein. Der IMSI-Catcher simuliert also ein Mobilfunknetzwerk.

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 Handys lahm, so dass 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 von Strafverfolgungsbehörden und Nachrichtendiensten.

Inhaltsverzeichnis

Funktionsweise

Der Catcher simuliert eine bestimmte Mobilfunkzelle des Netzbetreibers. Der Catcher steigt in der Kanal-Nachbarschaftsliste des Handys als Serving-cell auf. Der IMSI-Catcher strahlt eine veränderte Location Area Identity aus und veranlasst somit die Handys dazu, Kontakt zum (simulierten) Mobilfunk-Netz aufzubauen („Location Update"-Prozedur). Der Catcher fordert daraufhin einen „Identity Request" Befehl an. Das Handy antwortet mit einem Identity Response, welcher IMSI oder TMSI (temporary IMSI) sowie IMEI enthalten kann. Die erhaltenen Daten müssen dann mit vorhandenen Datenbeständen verglichen werden.

Der gesamte Vorgang wird dadurch ermöglicht, dass ein Handy sich zwar gegenüber dem Mobilfunknetz authentifiziert, nicht aber das Mobilfunknetz sich gegenüber dem Handy. Nachdem der Catcher als Basisstation das Handy übernommen hat, bringt er das Handy über einen dafür vorgesehenen

Signalisierungsweg im GSM-Protokoll in den unverschlüsselten Übertragungsmodus. Somit wird ein über den Catcher geführtes Gespräch abhörbar. Um das abgehörte Gespräch weiterzuleiten (Man-In-The-Middle-Angriff), muss sich der IMSI-Catcher gegenüber dem Mobilfunknetz als Handy ausgeben. Dabei kann er die unverschlüsselt abgehörten Nachrichten nicht unverschlüsselt weiterleiten, da das Mobilfunkgerät zwar von der Basisstation dazu gebracht werden kann, unverschlüsselt zu senden, diesen Modus aber nicht von sich aus wählen darf. Deshalb benötigt der IMSI-Catcher eine eigene SIM-Karte und leitet die abgehörten Daten als eigenes Gespräch weiter. Anrufe, die von einem abgehörten Handy aus getätigt werden, zeigen dem Angerufenen daher auch nicht die Telefonnummer des tatsächlichen Anrufers an, sondern die des IMSI-Catchers, bzw. sie werden nicht angezeigt.

Obwohl die Firmware eines Handys den unüblichen Modus der Nicht-Verschlüsselung von Gesprächen dem Benutzer signalisieren könnte, wird darauf verzichtet. Lediglich bei einigen Modellen ist es möglich, Aufschluss zu erlangen, ob das Mobilfunkgerät im verschlüsselten Modus überträgt. Hierzu muss ein interner Netzwerkmonitor des Geräts aktiviert werden. Dieser ist jedoch zumeist nicht benutzerfreundlich und erfordert Fachkenntnisse, um die angezeigten Werte richtig zu deuten. Ohnehin ist bei Mobilfunkgesprächen ebenso wie bei Festnetzgesprächen zu beachten: Staatliche Abhörmaßnahmen finden direkt bei der Mobilfunk- / Telefongesellschaft statt und sind aus Gründen, die sich aus der Systematik der Abhörmethode ergeben, nicht am Endgerät feststellbar.

Beispielszenario

Eine Zielperson befindet sich in ihrer Wohnung. Ermittler nähern sich der Zielperson mit einem Fahrzeug, in welchem der Catcher untergebracht ist, und führen je eine Simulation pro Netzbetreiber durch. Nun dürften gerade in einer Großstadt pro Messung und Netz eine Menge an Kennungs-Paaren „IMSI“ oder „TMSI“, „IMEI“ gefangen werden. Dieser Umstand dürfte es erforderlich machen, mehrere Messungen durchzuführen.

Nun verlässt die Zielperson die Wohnung und fährt z. B. in eine andere Stadt. Die Ermittler verfolgen die Zielperson und führen evtl. schon auf der Fahrt erneut Messungen durch. Durch den Abgleich der ersten Serie an Messungen mit der zweiten oder weiteren Messungsserien kann herausgefunden werden, welche Kennungen gleich sind. Die IMSI und IMEI, welche bei der ersten sowie der zweiten Messungsserie identisch sind, gehören mit hoher Wahrscheinlichkeit zur Zielperson.

Auch wenn die Person die SIM-Karte wechselt, bleibt immer noch die IMEI des Handys gleich. Aus diesem Grund sind Kriminelle dazu übergegangen, neben dem Wechsel der SIM-Karte ein anderes Mobiltelefon einzusetzen, also mehrere verschiedene Handys mit unterschiedlichen SIM-Karten zu benutzen. Durch Vergleich mit allen gesammelten Daten sind Rückschlüsse auf den Tauschzyklus möglich.

Bei manchen älteren Handys lässt sich über eine besondere Software mit Hilfe eines Datenkabels auch die IMEI abändern. Beim Wechsel der IMEI sollte darauf geachtet werden, eine solche Kennung zu vergeben, wie sie auch in der Praxis von den Herstellern vergeben wird (stimmiger Type Approval Code und stimmiger Ländercode).

BKA und Verfassungsschutz verwenden Geräte, welche Gespräche abhören können (z. B. GA 090), nach eigener Auskunft noch nicht (Stand 2002). Sie gelten allerdings – bei einem Preis von 200.000 bis 300.000 € – bereits als Exportschlager.

Weitere Einsatzfelder

Eine vielfach nicht erwähnte und auch unterschätzte Problematik stellt die Besonderheit von IMSI-Catchern dar. Sie können die in ihrem Wirkungsbereich befindlichen Mobiltelefone blockieren, sodass auch ein Notruf an Polizei, Feuerwehr oder Notarzt während eines solchen Einsatzes unmöglich ist.

Gerade damit lässt sich aber auch eine gewollte Kommunikationsunterdrückung im Rahmen von polizeilichen Überwachungs- und Zugriffsmaßnahmen realisieren.

Schutzmaßnahmen

- In Großstädten dürfte es nur sehr schwer möglich sein, die IMSI und IMEI eines Handynutzers anhand nur eines Standortes in kurzer Zeit zu ermitteln. Wenn das Handy also nur an einem bestimmten Ort eingesetzt wird (z. B. ein Haus mit vielen Parteien) und die Position nicht verändert wird, geht das gesuchte Handy in der Menge der anderen unter und ist schwerer zu identifizieren. Darüber hinaus müsste das simulierte Signal des IMSI-Catchers über längere Zeit wesentlich stärker sein, als die Funknetzversorgung des Netzbetreibers. Dies würde zu einer schnellen Enttarnung des IMSI-Catchers führen.

Nachweisbarkeit

Mit Hilfe von spezieller Monitor-Software, die ununterbrochen alle Signale aufzeichnet (z. B. Zellen-ID, Kanal, Location-Area, Empfangspegel, Timing Advance, Mindest-/Maximal-Pegel) kann der Einsatz eines IMSI-Catchers unter Umständen nachvollzogen werden. Da IMSI-Catcher auch von Geheimdiensten eingesetzt werden, ist anzunehmen, dass jene gut getarnt sind. Dies bedeutet, dass eine Netzbetreiberzelle 1-zu-1 kopiert wird.

Auffällig ist jedoch, dass bei allen Handys eines Netzbetreibers in der Nähe des Catchers zur gleichen Zeit „Kommunikation“ stattfindet. Dies ist beispielsweise durch Monitor-Software feststellbar. Noch auffälliger: Dieses Phänomen wiederholt sich in kurzen Abständen bei allen Netzbetreibern in der Nähe des Catchers. Um dies festzustellen wären also mindestens zwei Handys pro Netzbetreiber nötig, deren Daten per Software laufend ausgewertet werden.

Beispiel eines möglichen Signalisierungsprofil – als // dargestellt – und vier Mobile Network Codes (Netzbetreiber). Für jeden MNC werden 2 Handys eingesetzt, daher der Doppelstrich (//). Die Reihenfolge der MNCs ist unerheblich. Ein einfacher Strich (/) ist z. B. ein Periodic Location Update.

```
t (Zeitachse) -------->
MNC1......//............../..........
MNC2........//.........................
MNC3...........//........../..........
MNC4.....//.....//.....................
```

Die Treppenstruktur weist auf einen Fremdeingriff durch einen Catcher in das Mobilfunknetz hin.

Ein normales Profil ohne Standortwechsel und eigenen Eingriff ist völlig unstrukturiert:

```
t (Zeitachse) ----->
MNC1.........................../........
MNC2...../.............................../.
MNC3................./...................
MNC4........./................./.......
```

Da der IMSI-Catcher zwar gegenüber dem Mobiltelefon ein GSM-Netzwerk simulieren kann, jedoch nicht gegenüber dem Netzwerk ein Handy, ist ein Scanvorgang mit IMSI-Catcher auch recht einfach durch einen Telefonanruf zu enttarnen: man ruft das fragliche Handy an. Wenn es nicht klingelt, wurde die vom „echten" Netz kommende Signalisierung verschluckt. Ein erfolgreicher terminierter Anruf kann den Einsatz eines „einfachen" IMSI-Catchers ausschließen (z. B. R&S GA 090). Mittlerweile gibt es jedoch intelligentere IMSI-Catcher, die nur halbaktiv arbeiten. Somit lassen sich auch eingehende Gespräche belauschen. Ein paar Mobiltelefone (z. B. frühere Geräte von SonyEricsson) zeigen jedoch eine deaktivierte Verschlüsselung an, was auf den Einsatz eines IMSI-Catchers zurückzuführen sein kann. Davon unbeeinträchtigt sind jedoch Überwachungsfunktionen, die direkt vom echten Netzwerk vollkommen ohne IMSI-Catcher gesteuert werden.

Rechtsgrundlage

In Deutschland ist der am 14. August 2002 in Kraft getretene § 100i der Strafprozessordnung die Rechtsgrundlage für den Einsatz eines IMSI-Catchers durch Strafverfolgungsbehörden.[1] Die Vorschrift dient unter anderem der Fahndung sowie der Begründung von Sachbeweisen. In einem Beschluss vom 22. August 2006 [2] bestätigte das Bundesverfassungsgericht die Vereinbarkeit des Einsatzes von IMSI-Catchern zur Strafverfolgung mit dem Grundgesetz. Nach Ansicht der Richter verstößt dieser Einsatz weder gegen Datenschutzbestimmungen noch gegen Grundrechte wie das Fernmeldegeheimnis oder das allgemeine Persönlichkeitsrecht.

In Österreich ist die Verwendung des IMSI-Catchers durch eine Novelle des Sicherheitspolizeigesetz seit 1. Januar 2008 auch ohne richterliche Erlaubnis möglich. Da dies eine enorme Bedrohung der Privatsphäre darstellt, initiierten Die Grünen eine Petition, die eine erneute Prüfung dieser Gesetzesänderung verlangte; jedoch wurde dieser Forderung von den zuständigen Ministerien nicht nachgegangen. Eine parlamentarische Anfrage des Abgeordneten Alexander Zach (Liberales Forum) an den damaligen Innenminister Günther Platter ergab, dass innerhalb der ersten vier Monate, also von Januar bis April 2008 bereits über 3800 Anfragen (32 mal pro Tag) zur Überwachung von Handy und Internet erfolgten.[3]

Problematik

Normalerweise werden Telefonüberwachungen über den Betreiber abgewickelt und werden von diesen erst nach richterlicher Genehmigung vorgenommen. IMSI-Catcher kann die Polizei (technisch gesehen) jederzeit einsetzen und somit die richterliche Überprüfung umgehen. Dieses Vorgehen ist zwar illegal, nachzuweisen ist das jedoch nur schwer.

Präventiv ist die Nutzung in den jeweiligen Polizeigesetzen im Abschnitt der Datenerhebung geregelt.

Geräte

In Deutschland am weitesten verbreitet ist wohl das „GA 090" der Firma Rohde & Schwarz. In Österreich befinden sich bereits mehrere Geräte der Firma Rohde & Schwarz im Einsatz, die Anschaffung eines Geräts mit UMTS-Tauglichkeit wurde beschlossen.[4]

Mit einem Aufwand von ca. 1500 EUR ist es möglich einen IMSI-Catcher selbst zu bauen.[5]

Weblinks

- *IMSI-Catcher – Wanzen für Handys*. (http://www.webcitation.org/5sATybEve) 31. Oktober 2008, archiviert vom Original (http://hp.kairaven.de/miniwahr/imsi.html) am 22. August 2010, abgerufen am 22. August 2010.
- IMSI-Catcher (http://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf) (PDF; 48 kB)
- Bundesverfassungsgerichtsentscheidung (http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html)
- Vortrag auf dem 18C3 (http://ftp.ccc.de/congress/2001/mp3/vortraege/tag2/saal2/28-s2-1300-IMSI-Catcher.mp3) mit technischen Details
- Strafprozessuale Maßnahmen bei Mobilfunkendgeräten – Die Befugnis zum Einsatz des sog. IMSI-Catchers (http://www.hrr-strafrecht.de/hrr/archiv/09-05/index.php?sz=8)

Einzelnachweise

1. *Katz und Maus: Die Hell's Angels und die Polizei*. (http://www.heise.de/ct/Katz-und-Maus-Die-Hell-s-Angels-und-die-Polizei--/artikel/143343) In: c't, 11. August 2009
2. Beschluss 2 BvR 1345/03 (http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html)
3. *Handy- und Internetüberwachung*. (http://derstandard.at/?url=/?id=3391080%26sap=2%26_pid=9882745) DER STANDARD, 3. Juli 2008, abgerufen am 21. Januar 2009.
4. platterwatch.at (http://www.platterwatch.at/blog/24-1-2008/PLATTER-BLOG.html)
5. *IMSI-Catcher für 1500 Euro im Eigenbau*. (http://www.webcitation.org/5rgp2JlUf) Heise online, 1. August 2010, archiviert vom Original (http://www.heise.de/newsticker/meldung/IMSI-Catcher-fuer-1500-Euro-im-Eigenbau-1048919.html) am 2. August 2010, abgerufen am 2. August 2010.

Von „http://de.wikipedia.org/wiki/IMSI-Catcher“
Kategorien: Fahndung | Mobilfunk | Identifikationstechnik