IMSI-Catcher: Warum Überwacher es so einfach haben

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel <figure class=„printversionlogo“></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild: Kurt Bauschardt CC BY-SA 2.0) </figcaption></figure> Handys überprüfen nicht gleich, woher Mitteilungen kommen. Das öffnet Spionen Tür und Tor. Abhilfe ist nicht in Sicht, wurde auf der Usenix Enigma deutlich. In Städten und an Flughäfen stellen Überwacher besonders gerne IMSI-Catcher auf, nicht immer in Einklang mit dem geltenden Recht. Mit diesen Überwachungsgeräten können massenhaft beliebige Mobiltelefone erfasst, verfolgt und bisweilen auch abgehört werden. Unter Umständen können sogar Verbindungen aufgebaut und einem ahnungslosen Opfer untergeschoben werden. Die Überwachung ist erstaunlich einfach, Gegenwehr erstaunlich schwierig, wie Yomna Nasser am Montag auf der Konferenz Usenix Enigma erklärt hat. „Die Wurzel des Übels ist, dass Mobiltelefone in den frühen Phasen einer Verbindung die Identität der Mobilfunk-Basisstation nicht überprüfen können“, sagte Yomna Nasser, Technikerin bei der Electronic Frontier Foundation (EFF). Mobilfunknetze sind so standardisiert, dass sie immer unverschlüsselte Nachrichten an die Endgeräte schicken können. Und das Handy bestätigt den Empfang, womit es zumindest die der SIM-Karte zugeordnete ID (International Mobile Subscriber Identity, IMSI) preisgibt. Bekanntes Beispiel für unterschlüsselte Übertragungen sind behördliche Notfall-Mitteilungen [1], die sich entsprechend leicht fälschen lassen. Es gibt allerdings laufend technische Nachrichten, die Endbenutzer nie zu sehen bekommen. Theoretisch könnte sich das Netz gegenüber Endgeräten auch bei unverschlüsselten Nachrichten mittels kryptographischer Zertifikate ausweisen. Das ist aber nicht vorgesehen, nicht einmal bei 5G. (Bei 5G soll immerhin die IMSI verschleiert werden können, Anmerkung.) <h3 class=„subheading“ id=„nav_absicherung0“>Absicherung bleibt Theorie</h3> Zwar hätten Forscher rund um <a

href=„https://www.researchgate.net/publication/333184137_Insecure_connection_bootstrapping_in_cellular_networks_the_root_of_all_evil“ rel=„external noopener“ target=„_blank“>Syed Rafiul Hussain in einer Teststellung gezeigt, dass kryptographische Identifikation zu Mobilfunk [2] hinzugefügt werden kann, praktisch sei das aber schwer umzusetzen. Denn jede Lösung müsse abwärtskompatibel sein, da bereits Milliarden Endgeräte ohne dieses Zusatzmerkmal im Umlauf sind. Hinzu komme, dass die Paketgröße bei der Signalisierung limitiert ist, man also nicht beliebige digitale Signaturen mitschicken könne. <figure class=„a-u-inline-right a-inline-image a-u-inline“> <figcaption class=„a-caption“> Yomna Nasser bei ihrem Vortrag auf der Usenix Enigma 2020 (Bild: Daniel AJ Sokolov) </figcaption></figure> Auch die Frage, wo die Zertifikate auf Nutzerseite gespeichert werden sollen, sei ungelöst, zumal die auf der SIM-Karte gespeicherten Daten wiederum durch Netzmitteilungen umgeschrieben werden können. Keine Kleinigkeit sei der Umstand, dass Mobilfunknetze im Detail sehr unterschiedlich konfiguriert sind. Zudem gäbe es ungelöste Probleme mit Replay-Attacken und wie kompromittierte Zertifikate zurückgezogen werden sollen. Und sobald auch Roaming funktionieren solle, werde die Zahl der zu verwaltenden Zertifikate enorm. In einem EFF-Bericht hat Nasser vergangenes Jahr den Stand des Wissens über IMSI-Catcher [3] zusammengefasst. Die Erforschung dieser Überwachungsgeräte selbst gestaltet sich allerdings schwierig, weil sowohl Hersteller als auch Kunden auf Geheimhaltung bedacht sind. „Über kommerzielle IMSI-Catcher ist wenig bekannt“, bedauert Nasser, „Daher herrscht Verwirrung darüber, was sie alles tun können.“ Gesichert sei, dass sie sowohl zur Überwachung Einzelner als auch zehntausender Bürger gleichzeitig eingesetzt werden können. Von einem genutzten Typ sei eine Reichweite von mindestens zwei Kilometern dokumentiert. <h3 class=„subheading“ id=„nav_aclu_verklagt1“>ACLU verklagt USA auf Herausgabe von Akten</h3> Die US-Regierung habe sich geweigert, Auskunftsanträge nach dem Informationsfreiheitsgesetz zu beantworten. Die Bürgerrechtsorganisation ACLU (American Civil Liberties Union) habe daher kürzlich die US-Regierung verklagt. <div class=„collapse-boxtarget collapse-boxcontent a-inline-textboxcontent a-inline-textboxcontent–horizontal-layout“ data-collapse-target=„“> <figure class=„a-inline-textboximage-container“></figure> Keine News verpassen! Mit unserem täglichen Newsletter erhalten Sie jeden Morgen alle Nachrichten von heise online der vergangenen 24 Stunden. <ul class=„a-inline-textboxlist“><li class=„a-inline-textboxitem“>Newsletter jetzt abonnieren [4] Gleichzeitig sei die akademische Forschung zu dem Thema nicht einfach. Mobiltelefon-Firmware werde stets geheimgehalten, einschlägige Funkausrüstung sei teuer, die Spezifikationen von Endgeräten und Netzen seien sehr umfangreich und schwankten

zudem stark von Netz zu Netz. Schließlich gäbe es noch juristische Hürden: In manchen Ländern seien sogar passive Scans verboten; in Tunesien sei eine Person wegen bloßen Besitzes eines Software Defined Radio im Gefängnis gelandet. Und auf den von Mobiltelefonen empfangbaren Funkfrequenzen dürfe stets nur mit behördlich genehmigten Geräten gesendet werden. Aufgrund dieser hohen Hürden beschäftigen sich nur wenige Wissenschaftler mit dem Thema IMSI-Catcher. <h3 class=„subheading“ id=„nav_netzbetreiber2“>Netzbetreiber und Dienste schauen zu</h3> Einer davon ist Dr. Adrian Dabrowski. Ihn hat heise online gefragt, warum sich nicht die Netzbetreiber stärker gegen die IMSI-Catcher wehren: „Die Netzbetreiber mögen die IMSI-Catcher gar nicht, weil sie das Netz stören. Aber sie können selbst nichts tun, wenn, wie heise online berichtet hat, sogar der US-Heimatschutz illegale IMSI-Catcher unbehelligt lässt [5]“, schätzt Dabrowski die Lage ein, „Andererseits fürchten die Netzbetreiber vermutlich um ihr Image, wenn sie ihre Kunden warnen; sie können ihren Kunden ja keinen konkreten Rat zur Vermeidung der Überwachung geben, zudem könnte es sich um einen Fehlalarm handeln.“ Endbenutzer haben in der Tat wenig Handhabe, bestätige Nasser. Zwar habe es verschiedene Ansätze mit Apps gegeben, die beispielsweise Downgrades auf besonders unsicheren GSM-Mobilfunk oder unerwartet neu auftauchende Basisstationen melden sollen. Doch hätten diese Apps zuviele Fehlalarme produziert, um praxistauglich zu sein. Im übrigen funktionierten sie nur mit ausgewählten Endgeräten. Wie verzwickt die Lage ist, zeigt der Umstand, dass Spionageabwehren in verschiedenen Länder, darunter die USA und Kanada, offenbar wenig gegen fremde IMSI-Catcher in den Hauptstädten ausrichten [6]. Reine Spekulation bleiben heimliche Stillhalteabkommen zwischen Geheimdiensten unterschiedlicher Länder, die sich nicht in die Quere kommen wollen. ()<br class=„clear“/> <hr/> URL dieses Artikels:
<small>

```
http://www.heise.de/-4646749
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong> https://www.heise.de/meldung/USA-bauen-Notfall-Mitteilungen-an-Handys-aus-3338437.html
```

</small>
<small>

```
<strong>[2]</strong> https://www.researchgate.net/publication/333184137_Insecure_connection_bootstrapping_in_cellular_networks_the_root_of_all_evil
```

</small>
<small>

```
<strong>[3]</strong> https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks
```

</small>
<small>

```
<strong>[4]</strong> https://www.heise.de/newsletter/manage/ho?wt_mc=nl
```

```
.red.ho.daily.meldung.link.link
```

</small>
<small>

```
<strong>[5]</strong> https://www.heise.de/meldung/US-Heimatschutz-laesst-illegale-IMSI-Catcher-unbehelligt-4011143.html
```

</small>
<small>

```
<strong>[6]</strong> https://www.heise.de/meldung/Weiter-Aufregung-um-IMSI-Catcher-in-Kanada-3676299.html
```

</small>
<small>

```
<strong>[7]</strong> mailto:ds@heise.de
```

</small>
 Copyright © 2020 Heise Medien </html>