IMSI-Catcher: Überwachung auch in 5G-Netzen möglich

Originalartikel

Backup

<html> <figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: Jan Hrezik / Shutterstock.com)</figcaption></figure> Trotz neuer Authentifizierungsverfahren und weiterer Maßnahmen in 5G-Netzen ist es für Dritte weiterhin möglich, die IMSI-Nummer von Smartphones auszuspähen. Eine der wichtigsten Sicherheitsanforderungen der Telekom an den 5G-Übertragungsstandard war es, das Einschleusen von IMSI-Catchern in 5G-Netze unmöglich zu machen. Im 5G-Standard sind daher zusätzliche Authentifizierungs- und Verschlüsselungsverfahren verankert, um diese Art von Überwachungsequipment schachmatt zu setzen. Die Annahme, dass IMSI-Catcher deshalb im 5G-Zeitalter aussterben würden, erweist sich nun als falsch. Auf der weltgrößten Überwachungsmesse ISS World in Prag Anfang Juni stellte die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) ihre Methode vor, mit der sich die Sicherheitsmechanismen von 5G-Netzen aushebeln lassen. Auch die Überwachungsfirmen Utimaco (Aachen) und Rohde & Schwarz (München) waren mit Vorträgen zum Einsatz von IMSI-Catchern unter 5G vertreten. Die Münchner Firma Trovicor bietet solche Geräte bereits an. In Deutschland wurden IMSI-Catcher von Polizeibehörden 2022 [1] insgesamt 38 Mal eingesetzt, die Dauer dieser Einsätze ist allerdings ebenso unter Verschluss wie die Zugriffe der Geheimdienste. IMSI-Catcher können alle Mobiltelefone in ihrer Umgebung nach ihrer Identität (IMSI) abfragen, indem sie eine Basisstation des jeweiligen Mobilfunknetzes simulieren. Sie werden beispielsweise von Polizeibehörden eingesetzt, um vor Ort festzustellen, ob ein bestimmtes Mobiltelefon in dieser Funkzelle eingebucht ist. Dieses Handy kann dann über die Funkzellen geortet werden. In der Mobilfunkbranche sind IMSI-Catcher äußerst unbeliebt [2], da sie Anomalien in den Netzen verursachen, deren Ursache nicht sofort erkennbar ist. <figure class=„a-inline-image a-u-inline“> <img alt=„Auszug aus dem Programm der ISS World“ class=„legacy-img“ height=„352“ src=„https://heise.cloudimg.io/width/696/q85.png-lossy-85.webp-lossy-85.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD1_ISS_WORLD_IMSI-d2a7a07ef8c30f6e.png“ srcset=„https://heise.cloudimg.io/width/336/q70.png-lossy-70.webp-lossy-70.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD1_ISS_WORLD_IMSI-d2a7a07ef8c30f6e.png 336w,

https://heise.cloudimg.io/width/1008/q70.png-lossy-70.webp-lossy-70.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD1_ISS_WORLD_IMSI-d2a7a07ef8c30f6e.png 1008w, https://heise.cloudimg.io/width/1392/q70.png-lossy-70.webp-lossy-70.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD1_ISS_WORLD_IMSI-d2a7a07ef8c30f6e.png 2x“ width=„696“ referrerpolicy=„no-referrer“ /> <figcaption class=„a-caption“>Auf der ISS World waren (6. bis 8. Juni) in Prag alle Präsentationen zu IMSI-Catchern in Track 8 versammelt [3]. Akkreditierungen für Journalisten gibt es bei dieser Messe keine, die rund um das Jahr nacheinander in Prag, Singapur, Washington, Panama City und Dubai gastiert.(Bild: Erich Moechel)</figcaption></figure><h3 class=„subheading“ id=„nav_überleben_in0“>Überleben in 5G-Netzen</h3> Wie der Titel der Vortragsreihe schon andeutet, sind Mitarbeiter von Behörden bereits in den praktischen Einsatz von IMSI-Catchern in 5G-Netzen [4] eingeführt worden. Es muss also bereits Prototypen oder erste Kleinserien von Herstellern geben, die auch die 5G-Protokolle beherrschen. Angriffe auf Smartphones sind bei 5G nur während des Login-Prozesses möglich, der zu Beginn noch unverschlüsselt ist. Die mit Abstand häufigste Angriffsart auf IMSI-Nummern sind bisher Downgrade-Attacken, das heißt, der IMSI-Catcher gibt gegenüber dem Smartphone vor, nur 2G zu beherrschen und greift dann die IMSI über die GSM-Protokolle ab. Die IMSI (International Mobile Subscriber Identity) setzt sich zusammen aus dem Mobilfunk-Ländercode, gefolgt vom Code des Providers und schließlich der Identifikationsnummer der jeweiligen SIM-Karte. Die neuen Geräte wurden in Prag ausschließlich Polizei- und Geheimdienstangehörigen vorgestellt. Zivile Messebesucher oder Mitarbeiter anderer Überwachungsfirmen waren daher nicht nur vom ersten Vortrag zum Thema „Das Überleben von IMSI-Catchern in 5G-Netzen“ der Aachener Utimaco, sondern von allen Vorträgen zum Thema IMSI-Catcher ausgeschlossen. <h3 class=„subheading“ id=„nav_supi_catcher1“>SUPI-Catcher für 5G</h3> Im Produktkatalog von Utimaco findet sich zwar kein IMSI-Catcher, aber ein Hardwaremodul namens Identity De-concealing [5] für die Telekommunikationsindustrie, das sehr ähnliche Funktionen aufweist. Dieses Modul kann laut Utimaco die sogenannte SUCI-Nummer (Subscription Concealed Identifier) eines Smartphones abfangen. Damit lässt sich auch in 5G-Netzen die SUPI-Nummer (Subscriber Permanent Identifier) eines Smartphones ermitteln, wie die IMSI unter 5G genannt wird. Die SUCI entspricht der temporären TIMSI in 2G. Aus der Beschreibung geht hervor, dass dieses Hardwaremodul an der Peripherie der Mobilfunknetze installiert wird, nämlich in Mobilfunkanlagen auf Flugplätzen und in Gefängnissen, in Sicherheitstrakten und exponierten Gebäuden von Behörden und Militär. Das Modul ist über einen gesicherten Server mit dem Netz des jeweiligen Mobilfunkbetreibers verbunden. Im Falle eines Falles ist es mit dieser Konfiguration möglich, die Person oder Firma, die eine bestimmte SIM/eSIM vor Ort registriert hat, nahezu in Echtzeit zu identifizieren. In diesem Fall handelt es sich wahrscheinlich um ein fest installiertes Gerät, das Alarm schlägt, wenn ein „Smartphone of Interest“ in der betreffenden Funkzelle auftaucht. <figure class=„a-inline-image a-u-inline“> <img alt=„Features eines IMSI-Catchers“ class=„legacy-img“ height=„379“ src=„https://heise.cloudimg.io/width/696/q85.png-lossy-85.webp-lossy-85.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD2_Trovicor-f6b3dcbdee1b73df.png“ srcset=„https://heise.cloudimg.io/width/336/q70.png-lossy-70.webp-lossy-70.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD2_Trovicor-f6b3dcbdee1b73df.png 336w, https://heise.cloudimg.io/width/1008/q70.png-lossy-70.webp-lossy-70.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD2_Trovicor-f6b3dcbdee1b73df.png 1008w,

https://heise.cloudimg.io/width/1392/q70.png-lossy-70.webp-lossy-70.foil1/_www-heise-de_/imgs/18/4/2/5/7/0/7/3/BILD2_Trovicor-f6b3dcbdee1b73df.png 2x“ width=„696“ referrerpolicy=„no-referrer“ /> <figcaption class=„a-caption“>Das ist das Angebot an IMSI-Catchern von Trovicor [6] für 2/3/4/5G-Mobilfunknetze. Die Gerätschaften können die exakte Geolokation der eingebuchten Smartphones feststellen und eignen sich so auch für den operativen Einsatz, etwa in Autos. Interessanterweise lässt sich damit auch eruieren, ob andere IMSI-Catcher in derselben Funkzelle aktiv sind. Das Gerät von Trovicor kann also auch als IMSI-Catcher-Catcher eingesetzt werden.(Bild: Erich Moechel)</figcaption></figure><h3 class=„subheading“ id=„nav_imsi_catcher_fän2“>IMSI-Catcher-Fänger</h3> Das Münchner Messtechnik- und Analyseunternehmen Rohde & Schwarz bietet – zumindest auf seiner Website – nur den passiven, ersten Teil des Angriffsszenarios auf die SUPI-Nummer an, kann aber „verdächtige Zellen“ in einem Mobilfunknetz untersuchen. Damit können auch andere IMSI- bzw. SUPI-Catcher im Mobilfunknetz lokalisiert werden. Hardwareseitig wird einer der Funkscanner der Firma benötigt, auf dem die Funkzellenerfassungssoftware Nestor [7] installiert ist. Für die Auswertung ist ein herkömmliches Tablet oder Notebook mit Windows 10 sowie eine App erforderlich. Das Gerät kann auch mobil eingesetzt werden. Die niederländische Überwachungsfirma Group2000 hingegen präsentierte mit der Überwachungssuite LIMA CellPro [8] das volle Programm, nämlich eine „strategische netzwerkbasierte Plattform, die temporäre und versteckte IDs aus der Luftschnittstelle abgreift“ und mit einer bereits bekannten IMSI oder SUPI abgleicht. Das Set-up enthalte auch „die notwendigen Schnittstellen und Netzwerkprotokolle, um die permanente ID des Smartphones abzugreifen“. Damit wird es „für viele Behörden möglich sein, weiterhin Nachrichtenaufklärung an den Luftschnittstellen durchzuführen“. <figure class=„a-inline-image a-u-inline“> <figcaption class=„a-caption“>Die Grafik stammt aus einer Studie der Ruhr-Universität Bochum von 2021 [9] und zeigt wie ein zweiphasiger IMSI-Abfragevorgang durchin einem 5G-Netz funktioniert. Der Angriff erfolgt in zwei Phasen und um die Verwirrung komplett zu machen, wird das Überwachungsgerät hier SUCI-Catcher genannt.(Bild: Ruhr-Universität Bochum)</figcaption></figure><h3 class=„subheading“ id=„navkriegen_sie3“>„Kriegen sie wirklich noch alle?“</h3> Und so soll der Angriff funktionieren, wenn die IMSI/SUCI-Nummer eines gesuchten Smartphones bereits bekannt ist. In einem ersten Schritt werden die SUCIs aller aktuell in einer Funkzelle eingebuchten Geräte abgefangen. Anschließend wird auf Basis der bekannten IMSI/SUPI eine Reihe von true/false ID-Abfragen an alle eingebuchten Smartphones gesendet, wie in der Grafik dargestellt. Auf diese Weise kann ein gesuchtes Smartphone auch in 5G-

Netzen identifiziert werden. Ob damit tatsächlich alle in einer Funkzelle eingebuchten Smartphones abgefragt werden können, stellt das Autorenteam bereits im Titel dieser Studie in Frage: „5G SUCI-Catcher: „Kriegen sie wirklich noch alle?“. Diese Frage kann in diesem Zusammenhang allein nicht beantwortet werden. Denn die Verschlüsselung von Teilen der SUCI/IMSI ist optional, eigenständige 5G-Netzabschnitte sind noch selten, da gemischte 4G/5G-Netze die Regel sind. Eine neue Studie über 5G-Deployments in spanischen Mobilfunknetzen [10] von Mitte Mai ergab, dass die vier großen Mobilfunkbetreiber bis dahin weniger als ein Drittel der 5G-Sicherheitsmechanismen [11] implementiert hatten. Die Meldungen über den bevorstehenden Tod der IMSI-Catcher durch 5G sind also stark übertrieben, um den amerikanischen Schriftsteller Mark Twain zu paraphrasieren. () URL dieses Artikels:<small><code>https://www.heise.de/-9190322</code></small> Links in diesem Artikel:<small><code>[1] https://www.heise.de/news/Heimliche-Ueberwachung-Deutlich-mehr-Funkzellenabfragen-weniger-stille-SMS-8717037.html</code></small><small><code>[2] https://www.heise.de/news/IMSI-Catcher-Warum-Ueberwacher-es-so-einfach-haben-4646749.html</code></small><small><code>[3] https://www.issworldtraining.com/iss_europe/index.htm</code></small><small><code>[4] https://www.mpirical.com/blog/5g-anonymity-and-the-suci</code></small><small><code>[5] https://utimaco.com/solutions/applications/subscriber-identity-de-concealing</code></small><small><code>[6] https://trovicor.com/solutions/tactical-solutions/</code></small><small><code>[7] https://www.rohde-schwarz.com/at/produkte/aerospace-verteidigung-sicherheit/analyse-von-zellularen-netzen/rs-nestor-funkzellenerfassungssoftware_63493-115470.html</code></small><small><code>[8] https://group2000.com/dont-let-the-new-5g-sa-privacy-features-stop-you-from-catching-imsis</code></small><small><code>[9] https://dl.acm.org/doi/pdf/10.1145/3448300.3467826</code></small><small><code>[10] https://arxiv.org/pdf/2305.08635.pdf</code></small><small><code>[11] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539</code></small><small><code>[12] mailto:mki@heise.de</code></small> Copyright © 2023 Heise Medien </html>