Mobilfunk

Für die Bedrohungen im Bereich Mobilfunk müssen zunächst einige Grundlagen erklärt werden. In diesem Artikel dreht es sich um die Frage, wie die Kommunikation eines einzelnen Handys mit dem Mobilfunknetz, in Form der Mobilfunkzelle [ugs.: Antennenmast]. Dabei tauchen die Begriffe IMSI und IMEI (und manchmal auch TMSI) häufiger auf, die hier ebenfalls kurz erläutert werden.

Wem gehören Mobilfunkzellen?

Mobilfunkzellen (MFZ) werden von Mobilfunkanbietern betrieben. Dementsprechend kontrollieren die jeweiligen Mobilfunkanbieter auch den Datenverkehr durch diese MFZ hindurch. In dem unteren Bild symbolisieren die verschiedenen Farben, verschiedene Anbieter, wie z.B. Telekom, Vodafon, O2, etc.

Karte, die symbolisch zeigt, wie mobilfunkzellen in einer Stadt verteilt sind

IMSI: SIM-Identifier

Jede SIM-Karte besitzt eine eindeutig identifizierbare Nummer, die International Mobile Subscriber Identity, kurz IMSI. Durch die Registrierungspflicht von SIM-Karten in den meisten europäischen Ländern lässt sich die SIM-Karte eindeutig einer Identität zuordnen. Das können die Repressionsbehörden einfach bei den Mobilfunkanbietern abfragen und machen es auch sehr regelmäßig:

Welche Nummern gehören Anna und Arthur ?

Welche Nummern gehören Anna und Arthur ?

Natürlich funktioniert diese Abfrage auch in die andere Richtung, von SIM-Karte zur Identität:

Wem gehört diese Nummer ? Natürlich funktioniert diese Abfrage auch in die andere Richtung, von SIM-Karte zur Identität:

Wem gehört diese Nummer ?

Quelle: Bestandsdatenauskunft 2022: Behörden fragen sekündlich, wem eine Nummer gehört

IMEI: Geräte-Identifier

Auch Mobilfunkmodems (also der Chip im Handy der sich mit dem Mobilfunknetz verbinden kann), besitzen eine eindeutige Nummer, die International Mobile Equipment Identity, kurz IMEI. Diese IMEI sind in der Regel 15-Stellen lang und global einzigartig. Der Aufbau schaut wie folgt aus:

- die ersten 8 Ziffern sind, einfach gesagt, Typen spezifisch. Zum Beispiel haben alle Google Pixel 7a als erste 8 Stellen: 35917382
- die nächsten 8 Ziffern sind Seriennummern
- *die letzte Ziffer ist zur Fehlerkorrektur (error correction)*

picture of IMEI sets of different models from same and different vendors next to each other.

Wie wird sichergestellt, dass diese Nummern einzigartig sind?

Da viele verschiedene Firmen solche Mobilfunkmodems produzieren ist es notwendig, sich untereinander abzusprechen. Sonst würden bei den täglich abertausend produzierten Modems schnell Nummern multiple Male vergeben werden.

Darum kümmert sich die **GSMA** (Global System for Mobile Communications Association). Der Name spricht hier für sich selbst.

- Will ein Hersteller also ein neues Modell auf den Markt bringen, gehen sie zur GSMA und bitten um einen "Nummernraum", die 8 ersten Stellen. Nun dürfen sie alle produzierten Chips dieses Modells mit diesem Nummernraum benennen, also IMEIs vergeben.
- Die Seriennummern dienen zur Unterscheidung einzelner Geräte des selben Modells.
- Die Fehlerkorrektur ist ein bisschen schwarze Magie und kann hier wirklich vernachlässigt werden.

EIR: (Equipment Identity Register)

EIRs (Equipment Identity Register) sind im Grunde Datenbanken mit IMEIs. Meistens werden dort IMEIs gestohlener Handys in "blacklists" verwaltet (siehe weiter unten). Der Standard sieht aber auch "whitelists" vor. Das würde bedeuten, dass alle produzierten IMEIs erfasst werden und nur diese erfassten auch am Netzwerk teilhaben dürfen. Das wäre dann ein bedeutendes Sicherheitsrisiko, wenn ein Handy mit zurückverfolgbaren Zahlungsmethoden gekauft wird.

Beispiele für Modemhersteller: Qualcomm, Huawei, ZTE, Sierra Wireless, Netgear, Alcatel, TP-Link

Durch die IMEI ist also jedes mobilfunkfähige Gerät identifizierbar.

Wenn ein Gerät gleichzeitig mit mehreren SIM-Karten verwendet werden kann (egal ob bspw. 2 physische SIMs, oder 1 e-SIM & 1 physische SIM), hat es auch entsprechend viele IMEIs.

Warnung

Oft ist es aber ziemlich einfach eine Verbindung zwischen diesen beiden IMEIs herzustellen:

- Oft werden die Seriennummern einfach hochgezählt *(außer die error correction)*
- Wenn dauerhaft zwei IMEIs immer am selben Ort sind lässt sich das korrelieren
- Die Hersteller und Händler kennen die Korrelation der beiden IMEIs
- Sollte hier ein EIR im Spiel sein, sind diese beiden IMEIs im EIR auch miteinander verknüpft. Ist also eine der beiden IMEIs bekannt, ist aus dem EIR auch die Zweite ersichtlich.

Die IMEIs lassen sich nicht ohne Weiteres ändern. In vielen Ländern ist ihre Manipulation sogar strafbar und erfordert zudem spezielle Hardware, die am ehesten aus China bezogen werden kann.

Probleme beim Kauf von Handys

Kauft Ihr also ein Handy im Laden und bezahlt mit Karte, liegt danach dem Laden die Verknüpfung eurer Karte und der IMEI(s) eures Handys vor. Kauft Ihr ein Gerät sogar direkt bei eurem Mobilfunkanbieter, kann sogar durch die oben gezeigten Abfragen wie "Welche Nummern gehören dieser Person?" bei den Anbietern direkt auch euer genaues Gerät bestimmt werden (also inklusive Seriennummer, IMEI, etc). Kauft Ihr also ein Handy im Laden und bezahlt mit Karte, liegt danach dem Laden die Verknüpfung eurer Karte und der IMEI(s) eures Handys vor. Kauft Ihr ein Gerät sogar direkt bei eurem Mobilfunkanbieter, kann sogar durch die oben gezeigten Abfragen wie "Welche Nummern gehören dieser Person?" bei den Anbietern direkt auch euer genaues Gerät bestimmt werden (also inklusive Seriennummer, IMEI, etc).

Als Konsequenz daraus ist es Behörden möglich, durch Abfragen bei Verkäufern und Geräteherstellern, die per Werk vergebenen IMEIs zu spezifischen Geräten zurück zu verfolgen.

Und damit besteht, wenn das Handy über die eigene Identität gekauft wurde, auch diese Zuordnung.

Uns ist allerdings bisher nicht bekannt ob und wie oft Behörden diese Zuordnung abfragen.

- Identifier eines Gerätes, nicht der SIM-Karte
- weltweit einzigartig
- wird an Mobilfunkanbieter übertragen, wenn mit Mobilfunknetz verbunden (siehe [Authentifizierung](./mobilfunk.md#authentifizierung))

Authentifizierung

Schematische Darstellung des Authentifizierungsprozesses zwischen Sim und Mobilfunkzelle

- Erkennt das Handy das Signal einer MFZ, versucht es bei ihr mit einer Art "HALLO" anzuklopfen, um zu sehen, ob die MFZ überhaupt erreichbar ist und sagt ihr, das falls das der Fall ist, das es sich gerne ins Netz einloggen möchte.
- Wenn die MFZ diese Nachricht empfangen konnte, fragt sie zuerst einmal nach der Identität des Handys, um sicher zu gehen, dass es überhaupt das Recht hat, sich bei ihr einzuloggen.
- Daraufhin schickt das Handy die IMSI seiner SIM-Karte um zu beweisen, dass es das Recht hat sich zu verbinden. Gleichzeitig schickt es aber auch die IMEI seines Mobilfunkmodems (also des Handys) mit.
  - Eine Telekom MFZ würde also eine Vodafon Sim-Karte ablehnen und ihr sagen, dass sie kein Recht hat das Telekom-Netz zu benutzen.
- Damit ist die Authentifizieren quasi abgeschlossen und eine Verbindung kann aufgebaut werden. Was es mit der TMSI auf sich hat ist hier zweitrangig und deshalb übersichtshalber in den Details eingeklappt.
- Dem Standard nach können solche Verbindungen auch nur "verschlüsselt" aufgebaut werden. Warum das hier in Anführungszeichen steht, kannst du hier nachlesen.

Was ist die TMSI?

Würde nun einfach eine Verbindung aufgebaut werden, könnte jede*r in der Nähe mit geeigneter Hardware (bspw. Software Defined Radios ab 20€) sehen, welche Handys gerade mit welchen Sim-Karten im Netz eingeloggt und wie viel sie kommunizieren. Damit das nicht geschieht, geht das Prozedere noch um einen Schritt weiter: Die MFZ gibt dem Handy eine TMSI (Temporary Mobile Subscriber Identifier). Das Handy nutzt von nun an, aber auch nur in dieser Session, diese TMSI zur Identifikation. Loggt sich das Handy irgendwann aus dieser MFZ wieder aus und später wieder ein, beginnt das gesamte Prozedere von vorn und eine neue TMSI wird vergeben.

Falls du dich jetzt noch fragst, wofür das Handy sich nach der ersten Authentifizierung überhaupt noch weiter identifizieren muss: Versendete Pakete benötigen natürlich immer Empfänger (und Absender). Damit dein Handy also während einer Verbindung mit bspw. einer Webseite wieder gefunden werden kann, um dir die Inhalte zu präsentieren, muss "das Netz" natürlich wissen, welches Gerät du denn überhaupt bist.

Sowohl die IMSI als auch die IMEI werden bei der Authentifizierung mit dem Mobilfunknetz übertragen. Damit entstehen bei den Mobilfunkanbietern Tabellen (Datenbanken), die eine eindeutige Zuordnung zwischen IMSI und IMEI, also Handy und SIM-Karte, ermöglichen. Bei den Anbietern liegen diese Daten zwar nicht lange rum (zum Zeitpunkt des Schreibens dieses Artikels gibt es in Deutschland noch **keine** Vorratsdatenspeicherung). Dennoch sollte einem diese Gefahr bewusst sein, wenn ein Handy verwendet wird welches vorher bereits mit einer anderen SIM-Karte

verwendet wurde, welche wiederum Rückschlüsse auf die eigene Identität zulässt. Außerdem kann das Handy auch vorher mit einer anderen SIM in einer Funkzellenabfrage gelandet sein.

Version #2
Erstellt: 14 Januar 2025 18:52:56 von ESC-IT Migration Bot
Zuletzt aktualisiert: 15 Januar 2025 12:22:02 von ESC-IT Migration Bot