

Imsi-Catcher

Ein IMSI-Catcher simuliert eine kommerzielle Mobilfunkzelle (MFZ), um die Clients dazu zu bewegen, mit ihnen eine Verbindung aufzubauen. Generell gilt:

- Endgeräte loggen sich bei MFZ mit stärkstem Signal ein.
- Funkzelle fordert „Identity Request“
- Endgeräte authentifizieren sich mit IMSI + IMEI (und erhalten TMSI von der MFZ).

Dabei kann im Groben zwischen passiven und aktiven IMSI-Catchern unterschieden werden:

Passive IMSI-Catcher warten nur darauf, dass Clients versuchen sich mit ihren Identifier bei der MFZ zu authentifizieren. Damit können detaillierte Informationen darüber gesammelt werden, wer, oder viele Personen sich bspw. bei einer Demo aufhalten. Den Clients fällt der Schwindel auf Grund des GSM-Protokolls nicht auf.

Aktive IMSI-Catcher warten nicht nur auf die Synchronisationsanfrage des Clients. Sie geben dem Client auch eine TMSI (kann hier mit lokaler IP verglichen werden) und bauen sogar in seinem Namen eine legitime Verbindung zu einer echten MFZ her. Damit können vollwertige 'machine-in-the-middle-attacks' realisiert werden.

Welche Sicherheitslücke wird hier ausgenutzt?

Das Problem liegt bei der Authentifizierung zwischen Telefon und der MFZ(Mobilfunkzelle). Das Telefon muss sich nämlich (wie unten dargestellt) gegenüber der MFZ mit seinen einmaligen/unverwechselbaren Identitäten (IMSI, IMEI) verifizieren, um zu beweisen, dass es das Recht hat, das Mobilfunknetz zu benutzen.

Die Funkzelle authentifiziert sich gegenüber dem Telefon jedoch **nicht**. Deshalb kann das Telefon auch nie sicher wissen, ob es gerade wirklich mit einer normalen, kommerziellen MFZ kommuniziert, oder nicht doch mit einem Klon der Behörden.

Aktiver IMSI-Catcher - Systematik

IMSI-Catcher Schematik

Warum ist die Kommunikation Telefon-Polizei unverschlüsselt?

Die Antwort findet sich in der oben beschriebene Schwachstelle im Kommunikationsprotokoll bei der Authentifizierung. Durch bestimmte Schritte ist es dem IMSI-Catcher möglich, das Telefon beim Authentifizierungsprozess auf einen alten Mobilfunkstandard (idR. 2G) herunter zu zwingen. Das ist allgemein möglich, um in Situationen, in denen moderne Standards (3G/4G) keinen Empfang bieten, die noch vorhandene 2G Infrastruktur nutzen zu können. Diese ist oft in der territoriale Abdeckung etwas resistenter als die moderneren. Der 2G-Standard wiederum ist schon lange überholt und Sicherheitstechnisch in keinem Fall zu empfehlen. Von staatlichen Akteuren einmal abgesehen, ist es sogar privaten Menschen möglich, 2G-"verschlüsselte" Kommunikation sehr schnell zu entschlüsseln und mitzulesen/hören. Deshalb Kennzeichnen wir diese Kommunikation in seiner Praxis als "unverschlüsselt"

Warum ist die Kommunikation Polizei-Mobilfunkzelle wiederum verschlüsselt?

Um sogenanntem "eaves dropping" – also dem belauscht werden – entgegen zu wirken, akzeptieren die MFZ der neuen Standards nur Kommunikation, die mit ihrem jeweiligen Standard verschlüsselt wurden. Damit das Telefon also nicht merkt, das es eigentlich mit einer falschen MFZ verbunden ist, muss der IMSI-Catcher also auch eine real-funktionierende Verbindung zum Mobilfunknetz aufbauen. Dafür muss er die Verbindung zur MFZ wieder verschlüsseln.

Praktische Gefahren

Das heißt

- Handy mit privater SIM & IMEI macht identifizierbar & ortbar
- "Anonyme" SIM-Karte und Handy ist nicht gleich anonym

Es ist zu beachten, dass dadurch potentiell Gefahr besteht, wenn ein "anonymes" Handy wiederverwendet wird. In Zusammenhang mit Funkzellenabfragen lassen sich unter Umständen Bewegungsprofile dieser Geräte herstellen und kontextualisieren.

Ein potentielles Beispielszenario könnte so aussehen: Ihr benutzt euer Aktionshandy auf mehreren Aktionen/Demos, gerne auch in verschiedenen Städten/Bundesländern. Bei diesen Demos landet ihr (eure IMSI+IMEI) mehrfach in Funkzellenabfragen. Damit kann erst einmal niemand etwas anfangen, außer zu sagen, dass dieses Gerät auf all diesen Veranstaltungen präsent war. Nun läuft

ihr aber auf weiteren Demos an IMSI-Catchern vorbei und werdet ggf. dabei kontrolliert oder gefilmt. Dadurch könnte natürlich über die Zeit eine Korrelation zwischen euch und dem Gerät hergestellt werden.

Hardware für professionelle IMSI-Catcher kommt in in Deutschland und Umgebung in der Regel von Rhode&Schwarz. Deren Geräte sind global, nicht nur bei Strafverfolgungsbehörden, bekannt und beliebt. Diese State-of-the-Art Technik ist auch dementsprechend teuer, Preise bewegen sich in 4-5stelligen Bereichen.

Es lassen sich allerdings auch mit ~25€ "teuren" SDR-Dongles (Software Defined Radios) simple passive IMSI-Catcher realisieren. Diese sind allerdings nur dazu fähig, den existierenden Verkehr mitzulesen, jedoch nicht dazu, eine fake MFZ aufzusetzen und tatsächliche MITM Attacks auszuführen.

Empfehlung

Lukas Arnold beschreibt in seinem Talk auf dem 37c3 (CCC-Congress 2023), wie es mit ihrem selbst gebauten Tool möglich sein sollte, fake base stations mit Hilfe eines iPhones zu erkennen.

Quellen

- <https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks>
- SnoopSnitch-Talk (gehört in Empfehlungen): https://media.ccc.de/v/ber15-5-detecting_imsi-catchers_and_other_mobile_network_attacks

Statistik zu IMSI-Catchern

IMSI-Catcher - Statista

Version #2

Erstellt: 14 Januar 2025 18:52:48 von ESC-IT Migration Bot

Zuletzt aktualisiert: 15 Januar 2025 12:21:52 von ESC-IT Migration Bot