Imsi-Catcher

> [!toc] Table of Contents

An IMSI catcher, also known as Cell-Site Simulator or "Stingray", is a surveillance device that "masquerade as legitimate cell-phone tower, tricking phones within a certain radius into connecting to the device rather than a tower" 1.

In general, standard telecommunication works as follows:

1. End devices, such as your phone, log in to the cell-phone tower with the strongest signal.
2. Upon receiving a request from your device, the tower performs an “Identity Request”
3. Your device then authenticates themselves with their IMSI + IMEI, and receive a TMSI from the tower.

IMSI catchers abuse the above to track the location of cell phones and gather data from nearby devices without the users' knowledge.

A rough distinction can be made between passive and active IMSI catchers:

- **Passive IMSI catchers** simply wait for clients to attempt to authenticate themselves with their identifiers at the cell-phone tower. This allows detailed information to be collected about who or how many people are present at a demonstration, for example. Clients do not notice the deception due to the GSM protocol.
- **Active IMSI catchers** do not just wait for the client's synchronization request. They instead give your device a TMSI (comparable to a local IP) and establish a legitimate connection to a real cell-phone tower on the device's behalf. This allows full-fledged 'machine-in-the-middle attacks' to be carried out.

What security vulnerability is being exploited here?

The problem lies in the authentication between the phone and the cell-phone tower. The phone must verify itself to the tower (as shown below) with its unique identifiers (IMSI, IMEI) to prove that it has the right to use the mobile network.

However, the cell-phone tower does **not** authenticate itself to the phone. Therefore, the phone can never know for sure whether it is actually communicating with a normal, commercial cell-tower or with a clone, operated by the authorities.

Active IMSI catcher - system

IMSI catcher schematic

Why is communication between the phone and the police unencrypted?

The answer can be found in the vulnerability in the communication protocol during authentication described above. By taking certain steps, the IMSI catcher can force the phone to use an old mobile phone standard (usually 2G) during the authentication process. This downgrade is possible in order to use the existing 2G infrastructure in situations where modern standards (3G/4G) do not provide reception. 2G is often somewhat more resistant in terms of territorial coverage than the more modern standards. The 2G standard, on the other hand, has long been obsolete and is not recommended for security reasons. Apart from government agencies, even private individuals can very quickly decrypt 2G “encrypted” communications and read/listen to them. For this reason, we classify this communication as “unencrypted” in practice.

> [!technical] Why is communication between police and mobile phone cells encrypted?
>
> To counteract so-called “eavesdropping,” i.e., being listened in on, the cell-phone towers of the new standards only accept communications that have been encrypted with their respective standard. To ensure that your phone does not notice that it is actually connected to a malicious tower, the IMSI catcher must also establish a real working connection to the legitimate mobile network. To do this, it must re-encrypt the connection to the cell-phone tower.

Practical threats

> [!warning] This means: {static}

> - Cell phones with private SIM cards and IMEI numbers can be identified and located
> - “Anonymous” SIM cards and cell phones are not necessarily anonymous

It should be noted that this poses a potential risk if an “anonymous” cell phone is reused. In connection with radio cell inquiries, it may be possible to create and contextualize movement profiles of these devices.

A potential example scenario could look like this:

You use your action cell phone at several actions/demonstrations, preferably in different cities or states. During these demonstrations, you (and therefore your IMSI+IMEI) end up in cell-phone inquiries multiple times. At first, no one can do anything with this information except say that this device was present at all of these events. However, you might walk past IMSI catchers at further demonstrations and be checked or filmed. Over time, this could establish a correlation between you and the device.

Hardware for professional IMSI catchers in Germany and the surrounding area usually comes from Rhode&Schwarz. Their devices are known and popular worldwide, not only with law enforcement agencies. This state-of-the-art technology is also correspondingly expensive, with prices in the 4-5 digit range.

However, simple passive IMSI catchers can also be implemented with ~€25 SDR dongles (software-defined radios). These are only capable of reading existing traffic, but not of setting up a fake radio cell and carrying out actual MITM attacks.

Recommendation

We recommend reading this article from the Electronics Frontier Foundation, which introduces Rayhunter. A software, that can be flashed onto specific types of mobile routers to detect present IMSI-Catchers.

Sources

- https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks
- SnoopSnitch talk: https://media.ccc.de/v/ber15-5-detecting_imsi-catchers_and_other_mobile_network_attacks, although the app itself does not work.

Version #2
Erstellt: 2026-02-15 16:17:30 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-03-18 13:29:13 UTC von ESC-IT Migration Bot