

WIKIPEDIA

IMSI-catcher

An **International Mobile Subscriber Identity-catcher**, or **IMSI-catcher**, is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users.^[1] Essentially a "fake" mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack. The 3G wireless standard has some risk due to mutual authentication required from both the handset and the network.^[2] However, sophisticated attacks may be able to downgrade 3G and LTE to non-LTE network services which do not require mutual authentication.^[3]

IMSI-catchers are used in the United States and other countries by law enforcement and intelligence agencies, but their use has raised significant civil liberty and privacy concerns and is strictly regulated in some countries such as under the German *Strafprozessordnung* (StPO / Code of Criminal Procedure).^{[1][4]} Some countries do not even have encrypted phone data traffic (or very weak encryption), thus rendering an IMSI-catcher unnecessary.

Contents

Overview

Functionalities

- Identifying an IMSI

- Tapping a mobile phone

Universal Mobile Telecommunications System (UMTS)

Disclosing facts and difficulties

Detection and counter-measures

See also

Footnotes

Further reading

External links

Overview

A virtual base transceiver station (VBTS)^[5] is a device for identifying the International Mobile Subscriber Identity (IMSI) of a nearby GSM mobile phone and intercepting its calls. It was patented^[5] and first commercialized by Rohde & Schwarz in 2003. The device can be viewed as simply a modified cell tower with a malicious operator, and on 4 January 2012, the Court of Appeal of England and Wales held that the patent is invalid for obviousness.^[6]

The GSM specification requires the handset to authenticate to the network, but does *not* require the network to authenticate to the handset. This well-known security hole is exploited by an IMSI catcher.^[7] The IMSI catcher masquerades as a base station and logs the IMSI numbers of all the mobile stations in the area, as they attempt to attach to the IMSI-catcher.^[8] It allows forcing the mobile phone connected to it to use no call encryption (A5/0 mode) or to use easily breakable encryption (A5/1 or A5/2 mode), making the call data easy to intercept and convert to audio.

The 3G wireless standard mitigates risk and enhanced security of the protocol due to mutual authentication required from both the handset and the network and removes the false base station attack in GSM.^[2] Some sophisticated attacks against 3G and LTE may be able to downgrade to non-LTE network services which then does not require mutual authentication.^[3]

Body-worn IMSI-catchers that target nearby mobile phones are being advertised to law enforcement agencies in the US.^[9]

IMSI-catchers are often deployed by court order without a search warrant, the lower judicial standard of a pen register and trap-and-trace order being preferred by law enforcement.^[10] They can also be used in search and rescue operation for missing persons.^[11] Police departments have been reluctant to reveal use of these programs and contracts with vendors such as Harris Corporation, the maker of Stingray and Kingfish phone tracker devices.^[12]

In the UK, the first public body to admit using IMSI catchers was the Scottish Prison Service,^[13] though it is likely that the Metropolitan Police Service has been using IMSI catchers since 2011 or before.^[14]

Functionalities

Identifying an IMSI

Every mobile phone has the requirement to optimize the reception. If there is more than one base station of the subscribed network operator accessible, it will always choose the one with the strongest signal. An IMSI-catcher masquerades as a base station and causes every mobile phone of the simulated network operator within a defined radius to log in. With the help of a special identity request, it is able to force the transmission of the IMSI^[Criminal LAw 1].

Tapping a mobile phone

The IMSI-catcher subjects the phones in its vicinity to a man-in-the-middle attack, acting to them as a preferred base station in terms of signal strength. With the help of a SIM, it simultaneously logs into the GSM network as a mobile station. Since the encryption mode is chosen by the base station, the IMSI-catcher can induce the mobile station to use no encryption at all. Hence it can encrypt the plain text traffic from the mobile station and pass it to the base station.

There is only an indirect connection from mobile station via IMSI-catcher to the GSM network. For this reason, incoming phone calls cannot generally be patched through to the mobile station by the GSM network, although more modern versions of these devices have their own mobile patch-through solutions in order to provide this functionality.

Universal Mobile Telecommunications System (UMTS)

False base station attacks are prevented by a combination of key freshness and integrity protection of signaling data, not by authenticating the serving network.^[15]

To provide a high network coverage, the UMTS standard allows for inter-operation with GSM. Therefore, not only UMTS but also GSM base stations are connected to the UMTS service network. This fallback is a security disadvantage and allows a new possibility of a man-in-the-middle attack.^[16]

Disclosing facts and difficulties

The assignment of an IMSI catcher has a number of difficulties:

1. It must be ensured that the mobile phone of the observed person is in standby mode and the correct network operator is found out. Otherwise, for the mobile station, there is no need to log into the simulated base station.
2. Depending on the signal strength of the IMSI-catcher, numerous IMSIs can be located. The problem is to find out the right one.
3. All mobile phones in the area covered by the catcher have no access to the network. Incoming and outgoing calls cannot be patched through for these subscribers. Only the observed person has an indirect connection.
4. There are some disclosing factors. In most cases, the operation cannot be recognized immediately by the subscriber. But there are a few mobile phones that show a small symbol on the display, e.g. an exclamation point, if encryption is not used. This "Ciphering Indication Feature" can be suppressed by the network provider, however, by setting the OFM bit in EF_{AD} on the SIM card. Since the network access is handled with the SIM/USIM of the IMSI-catcher, the receiver cannot see the number of the calling party. Of course, this also implies that the tapped calls are not listed in the itemized bill.
5. The assignment near the base station can be difficult, due to the high signal level of the original base station.
6. While most of the mobile phones prefer faster mode of communication such as 4G or 3G, it will be tough downgrading to 2G while blocking ranges for 4G and 3G^[17]

Detection and counter-measures

Some preliminary research has been done in trying to detect and frustrate IMSI-catchers. One such project is through the Osmocom open source mobile station software. This is a special type of mobile phone firmware that can be used to detect and fingerprint certain network characteristics of IMSI-catchers, and warn the user that there is such a device operating in their area. But this firmware/software-based detection is strongly limited to a select few, outdated GSM mobile phones (i.e. Motorola) that are no longer available on the open market. The main problem is the closed-source nature of the major mobile phone producers.

The application Android IMSI-Catcher Detector (AIMSICD) is being developed to detect and circumvent IMSI-catchers, StingRay and silent SMS.^[18] Technology for a stationary network of IMSI-catcher detectors has also been developed.^[7] Several apps listed on the [Google Play Store](#) as IMSI catcher detector apps include SnoopSnitch, Cell Spy Catcher, and GSM Spy Finder and have between 100,000 and 500,000 app downloads each. However, these apps have limitations in that they do not have access to phone's underlying hardware and may offer only minimal protection.^[19]

See also

- [Telephone tapping](#)
- [Stingray phone tracker](#)
- [Mobile phone jammer](#)
- [Verrimus - Mobile Phone Intercept Detection \(http://www.verrimus.com/mobile-phone-interception/\)](http://www.verrimus.com/mobile-phone-interception/)

Footnotes

1. ["Police's growing arsenal of technology watches criminals and citizens" \(http://www.startribune.com/police-s-new-arsenal-of-technology-to-watch-criminals-and-citizens/420760943/\)](http://www.startribune.com/police-s-new-arsenal-of-technology-to-watch-criminals-and-citizens/420760943/). *Star Tribune*. Retrieved 2017-04-30.
2. ["Analysis of UMTS \(3G\) Authentication and Key Agreement Protocol \(AKA\) for LTE \(4G\) Network" \(http://www.ijritcc.org/download/1430372773.pdf\)](http://www.ijritcc.org/download/1430372773.pdf) (PDF). Retrieved 2017-04-30.
3. ["Practical attacks against privacy and availability in 4G/LTE mobile communication systems" \(https://arxiv.org/pdf/1510.07563v1.pdf\)](https://arxiv.org/pdf/1510.07563v1.pdf) (PDF). Retrieved 2017-04-30.
4. "Section 100i - IMS I-Catcher", *The German Code Of Criminal Procedure* (http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf) (PDF), 2014, pp. 43–44
5. EP 1051053 (<https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=EP1051053>), Frick, Joachim & Rainer Bott, "Verfahren zum Identifizieren des Benutzers eines Mobiltelefons oder zum Mithören der abgehenden Gespräche", issued 2003-07-09
6. *MMI Research Ltd v Cellxion Ltd & Ors* [2012] EWCA Civ 7 (24 January 2012) (<http://www.bailii.org/ew/cases/EWCA/Civ/2012/7.html>), Court of Appeal judgment invalidating Rohde & Schwarz patent.
7. ["Digitale Selbstverteidigung mit dem IMSI-Catcher-Catcher" \(http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html\)](http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html). *c't* (in German). 27 August 2014.
8. ["The Spyware That Enables Mobile-Phone Snooping" \(http://www.bloombergview.com/articles/2013-11-27/the-spyware-that-enables-mobile-phone-snooping\)](http://www.bloombergview.com/articles/2013-11-27/the-spyware-that-enables-mobile-phone-snooping). *Bloomberg View*. 27 November 2013.
9. ["The body-worn 'IMSI catcher' for all your covert phone snooping needs" \(https://arstechnica.com/security/2013/09/the-body-worn-imsi-catcher-for-all-your-covert-phone-snooping-needs/\)](https://arstechnica.com/security/2013/09/the-body-worn-imsi-catcher-for-all-your-covert-phone-snooping-needs/). *Ars Technica*. 1 September 2013.
10. Farivar, Cyrus (13 April 2015). ["County prosecutor says it has no idea when stingrays were used, so man sues" \(https://arstechnica.com/tech-policy/2015/04/county-prosecutor-says-it-has-no-idea-when-stingrays-were-used-so-man-sues/\)](https://arstechnica.com/tech-policy/2015/04/county-prosecutor-says-it-has-no-idea-when-stingrays-were-used-so-man-sues/). *Ars Technica*. Retrieved 12 March 2016.
11. ["Wingsuit-Flieger stürzt in den Tod" \(http://www.blick.ch/news/schweiz/zentralschweiz/am-gitschen-im-kanton-uri-wingsuit-flieger-stuerzt-in-den-tod-id3961344.html\)](http://www.blick.ch/news/schweiz/zentralschweiz/am-gitschen-im-kanton-uri-wingsuit-flieger-stuerzt-in-den-tod-id3961344.html). *Blick* (in German). 10 July 2015. Retrieved 11 July 2015.

12. ["Police's growing arsenal of technology watches criminals and citizens"](http://www.startribune.com/police-s-new-arsenal-of-technology-to-watch-criminals-and-citizens/420760943/) (<http://www.startribune.com/police-s-new-arsenal-of-technology-to-watch-criminals-and-citizens/420760943/>). *Star Tribune*. Retrieved 2017-04-30.
 13. <https://theferret.scot/imsi-catcher-trial-scottish-prison-service/>
 14. Corfield, Gareth (27 February 2017). "New prison law will let mobile networks deploy IMSI catchers" (https://www.theregister.co.uk/2017/02/27/prison_courts_bill_imsi_catcher_wireless_interference/). *The Register*. Retrieved 27 February 2017.
 15. Chris Mitchell, Paulo Pagliusi: Is Entity Authentication Necessary?, in Security Protocols, Springer LNCS 2845, pages 20-29, 2004
 16. Meyer, Ulrike; Wetzels, Susanne (1 October 2004). "A Man-in-the-Middle Attack on UMTS. ACM workshop on Wireless security, 2004" (<http://www.cs.stevens.edu/~swetzels/publications/mim.pdf>) (PDF). Retrieved 12 March 2016.
 17. "The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF" (<http://www.delaat.net/rp/2015-2016/p86/report.pdf>) (PDF). *Kenneth van Rijsbergen*: 8–9. Retrieved July 7, 2017.
 18. "Android IMSI-Catcher Detector (AIMSICD) Wiki, Development status" (<https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/wiki/Development-Status>). 9 December 2015. Retrieved 10 October 2016. In alpha stage in October 2016.
 19. "IMSI Catcher Detection Apps Might Not Be All That Good, Research Suggests" (https://motherboard.vice.com/en_us/article/need5g/stingray-detection-apps-might-not-be-all-that-good-research-suggests). *Motherboard*. Retrieved 2017-08-14.
-
1. Rolón, Darío Nicolás. "Intercepción de metadatos de comunicaciones por teléfonos móviles. El IMSI-Catcher y su regulación en el ordenamiento procesal penal alemán" (<https://rej.uchile.cl/index.php/RECEJ/article/view/47961>). *Revista de Estudios de la Justicia*. Retrieved 4 January 2018.

Further reading

- Soltani, Ashkan; Timberg, Craig (Sep 17, 2014). "Tech Firm Tries to Pull Back Curtain on Surveillance Efforts in Washington" (https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html). *Washington Post*.
- Barrett, Devlin (Nov 13, 2014). "Americans' Cellphones Targeted in Secret U.S. Spy Program" (<https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>). *The Wall Street Journal*. Retrieved Nov 14, 2014.

External links

- [Mobile Phone Networks: a tale of tracking, spoofing and owning mobile phones](http://www.slideshare.net/iazza/dcm-final-23052013fullycensored) (<http://www.slideshare.net/iazza/dcm-final-23052013fullycensored>)
- [IMSI-catcher Seminar paper and presentation](http://www.emsec.rub.de/teaching/seminars/seminar_ss07) (http://www.emsec.rub.de/teaching/seminars/seminar_ss07)
- [Mini IMSI and IMEI catcher](http://www.septier.com/368.html) (<http://www.septier.com/368.html>)
- [The OsmocomBB project](http://bb.osmocom.org/) (<http://bb.osmocom.org/>)

- **MicroNet: Proximus LLC GSM IMSI and IMEI dual band catcher**
(http://www.proximus.com.ua/MicroNet_GSM_daul_band_catcher.html)
 - **MicroNet-U: Proximus LLC UMTS catcher** (http://www.proximus.com.ua/Micronet-U_UMTS_catcher.html)
 - **iParanoid: IMSI Catcher Intrusion Detection System presentation**
(<http://www.slideshare.net/mobile/iazza/mobile-cell-networksintrusiondetectionsystemiparanoidlucabongiorni>)
 - **Vulnerability by Design in Mobile Network Security** (<http://folk.uio.no/josang/papers/JMD2015-JIW.htm>)
-

Retrieved from "<https://en.wikipedia.org/w/index.php?title=IMSI-catcher&oldid=830213177>"

This page was last edited on 13 March 2018, at 13:22.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.