IMSI-catcher

From Wikipedia, the free encyclopedia

An **IMSI catcher** is an eavesdropping device used for interception of cellular phones and usually is undetectable for users of mobile phones. Such a **virtual base transceiver station** (VBTS)[1] is a device for identifying the International Mobile Subscriber Identity (IMSI) of a nearby GSM mobile phone and intercepting its calls. It was patented[1] and first commercialized by Rohde & Schwarz.

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 can be exploited by an IMSI catcher.

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. It allows forcing the mobile phone connected to it to use no call encryption (i.e., it is forced into A5/0 mode), making the call data easy to intercept and convert to audio.

IMSI catchers are used in some countries by law enforcement and intelligence agencies, but based upon civil liberty and privacy concerns, their use is illegal in others. Some countries do not even have encrypted phone data traffic (or very weak encryption) rendering an IMSI catcher pointless.

Contents

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.

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 be patched through to the mobile station by the GSM network.

UMTS

Since UMTS employs mutual authentication, a man-in-the-middle attack as on GSM is not successful. But, 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 disadvantage concerning the security and allows a new possibility of a man-in-the-middle attack. For further information see [2].

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 catchment area 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 implicates 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.

Products

- Meganet
    - VME Interceptor

- NeoSoft
  - NS-17-1
  - NS-17-2

- Shoghi Communications
  - SCL-5020
  - SCL-5020SE

See also

- Telephone tapping

References

1. ^ *a* *b* EP 1051053 (http://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 (Method for identifying a mobile phone user or for eavesdropping on outgoing calls)", issued 2003-07-09
2. ^ Ulrike Meyer and Susanne Wetzel: A Man-in-the-Middle Attack on UMTS. ACM workshop on Wireless security, 2004 (http://www.cs.stevens.edu/~swetzel/publications/mim.pdf)

External links

- Seminar IMSI Catcher (http://www.crypto.rub.de/imperia/md/content/seminare/itsss07/imsi_catcher.pdf)

Retrieved from "http://en.wikipedia.org/w/index.php?title=IMSI-catcher&oldid=459323035"

Categories: Surveillance | Telephony equipment | Law enforcement equipment

- This page was last modified on 6 November 2011 at 18:09.
-