IMSI-catcher

An **IMSI catcher** is essentially a false mobile tower acting between the target mobile phone(s) and the service providers real towers. As such it is considered a Man In the Middle (MITM) attack. It is used as an eavesdropping device used for interception and tracking of cellular phones and usually is undetectable for the users of mobile phones. Such a **virtual base transceiver station** (VBTS) is a device for identifying the International Mobile Subscriber Identity (IMSI) of a nearby GSM mobile phone and intercepting its calls. It was patented and first commercialized by Rohde & Schwarz, although it would be hard to maintain such a patent, since in reality it is just a modified cell tower with a malicious operator. On 24 January 2012, the Court of Appeal of England and Wales held that the patent is invalid for obviousness.[1]

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 unnecessary.

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 generally be patched through to the mobile station by the GSM network, although more modern versions of these devices have their own mobile patch-thru solutions in order to provide this functionality.

UMTS

False base station attacks prevented by combination of key freshness and integrity protection of signaling data, not by authenticating the serving network.[2]

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.[3]

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.

Detection and counter measures

There are some preliminary research done in trying to detect and prevent 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 and outdated GSM mobile phones (i.e. Motorola) that is no longer available on the open market. The main problem is the closed source nature of the major mobile phone producers.

Products

- Septier Communication
  - Guardian
- Meganet
  - VME Interceptor
- NeoSoft
  - NS-17-1
  - NS-17-2
- Shoghi Communications
  - SCL-5020
  - SCL-5020SE
- Proximus LLC

  - MicroNet (GSM)
  - MicroNet-U (UMTS)
- Cyttek Consulting
  - Next Generation Phone catcher (NGPC)

References

[1] (http://www.bailii.org/ew/cases/EWCA/Civ/2012/7.html), Court of Appeal judgment invalidating Rohde & Schwarz patent.

[2] Chris Mitchell, Paulo Pagliusi: Is Entity Authentication Necessary?, in Security Protocols, Springer LNCS 2845,pages 20-29, 2004

[3] 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

- IMSI-catcher Seminar paper and presentation (http://www.emsec.rub.de/teaching/seminars/seminar_ss07)
- Mini IMSI and IMEI catcher (http://www.septier.com/368.html)
- The OsmocomBB project (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)

Article Sources and Contributors

IMSI-catcher *Source*: https://en.wikipedia.org/w/index.php?oldid=584968301 *Contributors*: David Chouinard, Dhuh, El Andaluz, Frap, Heretic1975, Hrgwea, Jahibadkaret, Jmax-, Kiwikibble, Markus Kuhn, Necrothesp, Oneiros, Proximus llc, Rjwilmsi, Shaddack, Sorsoup, Swpb, Ulf Abrahamsson, UnicornTapestry, Vasto4ni paren, Way1000, Yuri Nebosenko, Zntrip, 28 anonymous edits

License