Demystifying SDR Hacking: A Deep Dive into Wireless Protocols Part:4

KISHORERAM

KISHORERAM

Follow

8 min read

·

Oct 14, 2023

Listen

Share

More

GSM HACKING

Understanding GSM Architecture:

GSM (Global System for Mobile Communications) is a digital mobile network that is widely used around the world. It operates across four different frequency bands: 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz. GSM uses a combination of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) to efficiently utilize these frequency bands.

Press enter or click to view image in full size

Photo by Kabiur Rahman Riyad on Unsplash

GSM comprises three essential subsystems:

Base Station Subsystem (BSS): BSS manages traffic and signaling between mobile phones and the network switching subsystem. It consists of two key components, the Base Transceiver Station (BTS) and the Base Station Controller (BSC).

Network and Switching Subsystem (NSS): NSS serves as the core network, overseeing call and mobility management functions for mobile devices. It encompasses components such as the Visitor Location Register (VLR), Home Location Register (HLR), and Authentication Center (AUC).

Operating Subsystem (OSS): OSS functions as a monitoring and control system for network operators. The Operation and Maintenance Center (OMC) is a crucial part of OSS, ensuring cost-effective support for all GSM-related maintenance services.

Press enter or click to view image in full size

Components of GSM Subsystems:

Mobile Station (MS): MS, short for Mobile System, comprises user equipment and a Subscriber Identity Module (SIM). These mobile stations connect to towers through Transceivers (TRX), facilitating both transmission and reception of signals.

Base Transceiver Station (BTS): BTS, found in every tower, facilitates wireless communication between user equipment and the network.

Base Station Controller (BSC): BSC serves as a local exchange, managing multiple towers and their respective BTS units.

Mobile Switching Center (MSC): MSC handles communication switching functions, including call setup, release, and routing, as well as services like call tracing and call forwarding. VLR, HLR, AUC, EIR, and PSTN are integral components of MSC.

Visitor Location Register (VLR): VLR maintains the real-time location data of mobile subscribers within the service area of the MSC, ensuring seamless mobility across regions.

Home Location Register (HLR): HLR is a database containing subscriber-specific information, such as plan details, caller tunes, and identity data.

Authentication Center (AUC): AUC authenticates mobile subscribers seeking to connect to the network.

Equipment Identity Register (EIR): EIR maintains records of allowed and banned devices, ensuring network security and integrity.

Public Switched Telephone Network (PSTN): PSTN connects to MSC and has evolved from analog to a mostly digital network, encompassing mobile and fixed telephones.

Operation Maintenance Center (OMC): OMC plays a pivotal role in monitoring and maintaining the performance of mobile stations, BSCs, and MSCs in the GSM system.

Understanding GSM Sniffing and IMSI Numbers

What is GSM Sniffing?

GSM sniffing is a method used to intercept and decode the communication between mobile devices and cellular networks.

Press enter or click to view image in full size

Source :https://www.pentotest.com/

What is an IMSI Number?

The International Mobile Subscriber Identity (IMSI) is a unique number that identifies every user of a cellular network. It is usually presented as a 15-digit number. The IMSI number is crucial in GSM sniffing as it allows the identification of individual mobile devices within the network.

Sourcehttps://www.tech-invite.com/

IMSI Catcher

An IMSI Catcher, also known as an International Mobile Subscriber Identity catcher, is a device that intercepts mobile phone communications and tracks the location data of mobile phone users. It operates by posing as a fake mobile phone tower, creating a connection between the target mobile phone and the service provider’s actual towers, making it a man-in-the-middle (MITM) attack.While 3G or 4G wireless cellular networks require mutual authentication from both the handset and the network, sophisticated IMSI catchers may have the capability to downgrade 3G and LTE to non-LTE network services. These services do not require mutual authentication, making them vulnerable to interception.

Tools for GSM Sniffing

Gqrx

Gqrx is a software-defined radio (SDR) receiver that can control and use a variety of SDR hardware. To install Gqrx on Debian-based systems, you can use the following command:

Sudo apt-get install gqrx

Kalibrate-rtl

Kalibrate-rtl, or Kal, can scan for GSM base stations in a given frequency band . To install it on Debian-based systems, use the following command:

Sudo apt-get install kalibrate-rtl

OR

Sudo apt-get update

Git clone <https://github.com/steve-m/kalibrate-rtl>

Cd kalibrate-rtl

./bootstrap && CXXFLAGS=’-W -Wall -O3’

./configure

Make

Sudo make install

To find gsm frequency

Kal -g 40 -s GSM900

Press enter or click to view image in full size

Gr-gsm

Gr-gsm is a set of tools designed to understand and demodulate GSM signal. To install gr-gsm, you can follow these commands:

Sudo apt install python3-numpy python3-scipy python3-scapy

Sudo apt-get install -y \

Cmake \

Autoconf \

Libtool \

Pkg-config \

Build-essential \

Python-docutils \

Libcppunit-dev \

Swig \

Doxygen \

Liblog4cpp5-dev \

Gnuradio-dev \

Gr-osmosdr \

Libosmocore-dev \

Liborc-0.4-dev \

Swig

Git clone <https://git.osmocom.org/gr-gsm>

Cd gr-gsm

Mkdir build

Cd build

Cmake ..

Make

Sudo make install

Sudo ldconfig

Install IMSI Catcher :

Git clone <https://github.com/Oros42/IMSI-catcher.git>

Cd IMSI-catcher

Sudo apt install python3-numpy python3-scipy python3-scapy

USAGE

We use grgsm\_livemon to decode GSM signals and simple\_IMSI-catcher.py to find IMSIs.

Python3 simple\_IMSI-catcher.py -h

Usage: simple\_IMSI-catcher.py: [options]

Options:

-h, --help show this help message and exit

-a, --alltmsi Show TMSI who haven’t got IMSI (default : false)

-i IFACE, --iface=IFACE

Interface (default : lo)

-m IMSI, --imsi=IMSI IMSI to track (default : None, Example:

123456789101112 or “123 45 6789101112”)

-p PORT, --port=PORT Port (default : 4729)

-s, --sniff sniff on interface instead of listening on port

(require root/suid access)

-w SQLITE, --sqlite=SQLITE

Save observed IMSI values to specified SQLite file

-t TXT, --txt=TXT Save observed IMSI values to specified TXT file

-z, --mysql Save observed IMSI values to specified MYSQL DB (copy

.env.dist to .env and edit it)

Capturing or Intercept of GSM traffic :

Open 2 terminals.

In terminal 1

Sudo python3 simple\_IMSI-catcher.py -s

In terminal 2

Grgsm\_livemon

Now, change the frequency until it display, in terminal, something like that :

15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b

25 06 21 00 05 f4 f8 68 03 26 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b

49 06 1b 95 cc 02 f8 02 01 9c c8 03 1e 57 a5 01 79 00 00 1c 13 2b 2b

Set the frequency for grgsm\_livemon,

Grgsm\_livemon -f 942.4M -g 45

IMSI Catchers: Detection Techniques

Using a signal detector, a portable device that can detect suspicious wireless signals in the vicinity. It can detect the presence of IMSI catchers by picking up on their GSM or LTE signals. Another project, known as AIMSICD (Android IMSI-Catcher Detector), attempts to detect IMSI-Catchers through various detection methods such as checking tower information consistency, checking LAC/Cell ID consistency, checking neighboring cell info, preventing silent app installations, monitoring signal strength, detecting silent SMS, and detecting FemtoCells.

<https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector>

While these methods can help in detecting IMSI Catchers, they may not provide complete protection against all types of IMSI Catcher attacks.

Decoding Morse Code with RTL-SDR

Morse code is a system of encoding messages using dots and dashes. It was developed in the early 1800s by Samuel Morse and Alfred Vail. Morse code is named after Samuel Morse, who was one of the inventors of the telegraph. Morse code can encode the 26 basic Latin letters A to Z, Arabic numerals, and a small set of punctuation and procedural signals.

Source:https://en.wikipedia.org/

What is RTL-SDR?

RTL-SDR is based on the Realtek RTL2832U chipset and is widely available for purchase at a low cost of around $20-$30 USD. It can receive live radio signals in a wide frequency range, typically from 500 kHz up to 1.75 GHz.

What is CwGet?

CwGet is a program that decodes Morse code (CW) via a sound card to text. It can work as a narrow-band sound DSP-filter also. No additional hardware is required — you need only receiver and computer with a sound card.

<https://www.dxsoft.com/en/products/cwget/>

To decode Morse code using RTL-SDR and CwGet, you would first need to set up your RTL-SDR dongle to receive the desired frequency range. Then, you would use CwGet to decode the Morse code signals received by the RTL-SDR. The decoded text would then be displayed in the CwGet interface.

Press enter or click to view image in full size

Amateur Radio Frequency Bands in India

Amateur radio, often referred to as ham radio, is a popular pastime among more than 16,000 licensed enthusiasts in India. The Wireless and Planning and Coordination Wing (WPC), a division of the Ministry of Communications and Information Technology, grants licenses. The Indian Wireless Telegraphs (Amateur Service) Rules, 1978 initially listed five license categories. To earn a license, applicants must pass the Amateur Station Operator’s Certificate examination administered by the WPC. Amateur radio operators in India have access to a range of frequencies. For instance, they can operate on 0.1357–0.1378 MHz (2200 m wavelength) in the LF band, 0.472–0.479 MHz (630 m) in the MF band, and 1.800–1.825 MHz (160 m) in the MF band, among others. Each band corresponds to the International Telecommunication Union (ITU) radio band designation.

Press enter or click to view image in full size

Source:https://hamradioprep.com/

<https://en.wikipedia.org/wiki/List_of_amateur_radio_frequency_bands_in_India>

Thanks For Reading ☺

Don’t miss out on my upcoming articles! Follow me on Medium for more insightful content. Clap and share this article to spread the knowledge among fellow bug bounty hunters and cybersecurity enthusiasts.

If you have any further questions or would like to connect, feel free to reach out to me

My LinkedIn handle: <https://www.linkedin.com/in/kishoreram-k/>

Hacking

Cybersecurity

Sdr