Where is Wally?
IMSI-Catchers

MUNDO HACKER DAY

PEDRO C. AKA S4UR0N (CS³ GROUP SECURITY SERVICES)

Whoami

```
class PedroC:
    def __init__(self):
     self.name =  ‘Pedro Candel’
     self.email =  ‘s4ur0n@s4ur0n.com’
     self.work =  ‘CS3 Group Security Services’
     self.web =  ‘https://www.s4ur0n.com’
     self.nick =  ‘@NN2ed_s4ur0n’
     self.role =  ‘Security Researcher’
     self.work =  [ ‘Reversing’, ‘Malware’, ‘Offensive Security’]
```

Whoami

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.

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.

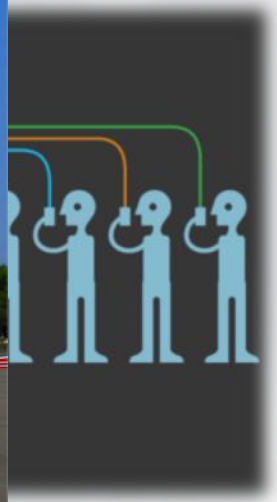
The 3G/4G/5G wireless standard mitigates some risk due to mutual authentication required from both the handset and the network.

However, “sophisticated” attacks may be able to downgrade 3G and LTE to non-LTE network services which do not require mutual authentication.

Source: https://en.wikipedia.org/wiki/IMSI-catcher

Tipos:

- Pasivo (
- Activo (e



MUNDO HACKER DAY

SIM 101

File Name	File ID	Size
EF LP	6F05	1-n bytes ...th language code
EF IMSI	6F07	9 bytes
EF KC	6F20	9 bytes
EF HPPLMN	6F31	1 byte
EF SST	6F38	X bytes X >= 2
EF BCCH	6F74	16 bytes
EF ACC	6F78	2 bytes
EF FPLMN	6F7B	12 bytes
EF LOCI	6F7E	11 bytes

...STER FILE (MF)

IMSI 101 (International Mobile Subscriber Identity)

Es un número de 15 dígitos que reconoce el operador que está usando su teléfono. Cada IMSI es un código único.

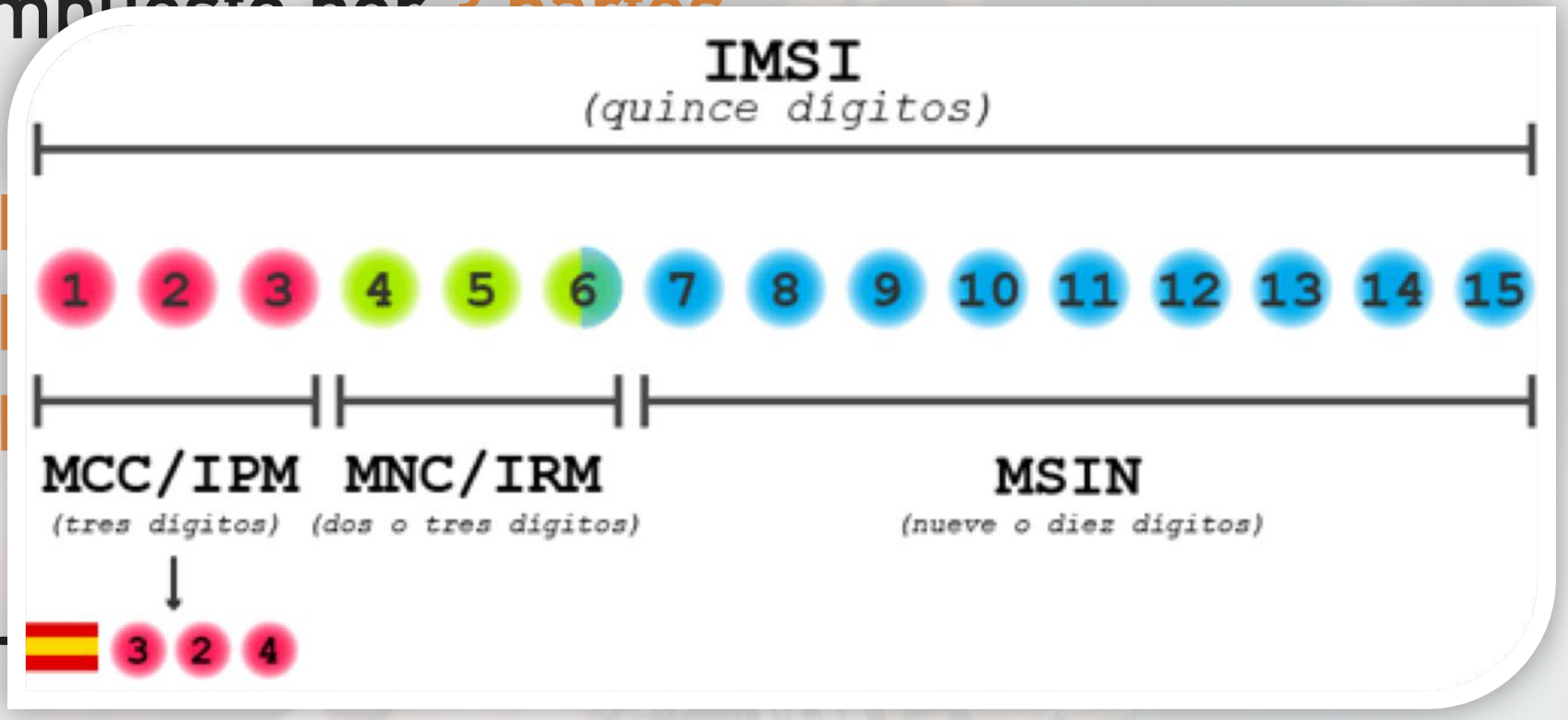
El dispositivo lo almacena y lo envía de forma segura a su red para identificarlo.

Los números IMSI están asociados a redes móviles, tanto GSM como UMTS.

Compuesto por 3 partes

-
-
-

AT-



La conexión inicial le da al dispositivo móvil un código temporal de identidad de abonado móvil (TMSI).

Se utiliza para las identificaciones de suscriptores cada vez que accede a la red móvil.

El número temporal se genera mientras el teléfono se está inicializando.

El número IMSI original no se puede transmitir. El dispositivo sólo genera un número temporal de TMSI y la red lo usa para identificarlo.

Las bases de datos de suscriptores permanentes incluyen HLR (Home Location Register) y VLR (Visitor Location Register).

El código IMSI obtiene la información detallada sobre el dispositivo móvil en la base de datos HLR y VLR.

Para que no pueda ser obtenido, el IMSI…

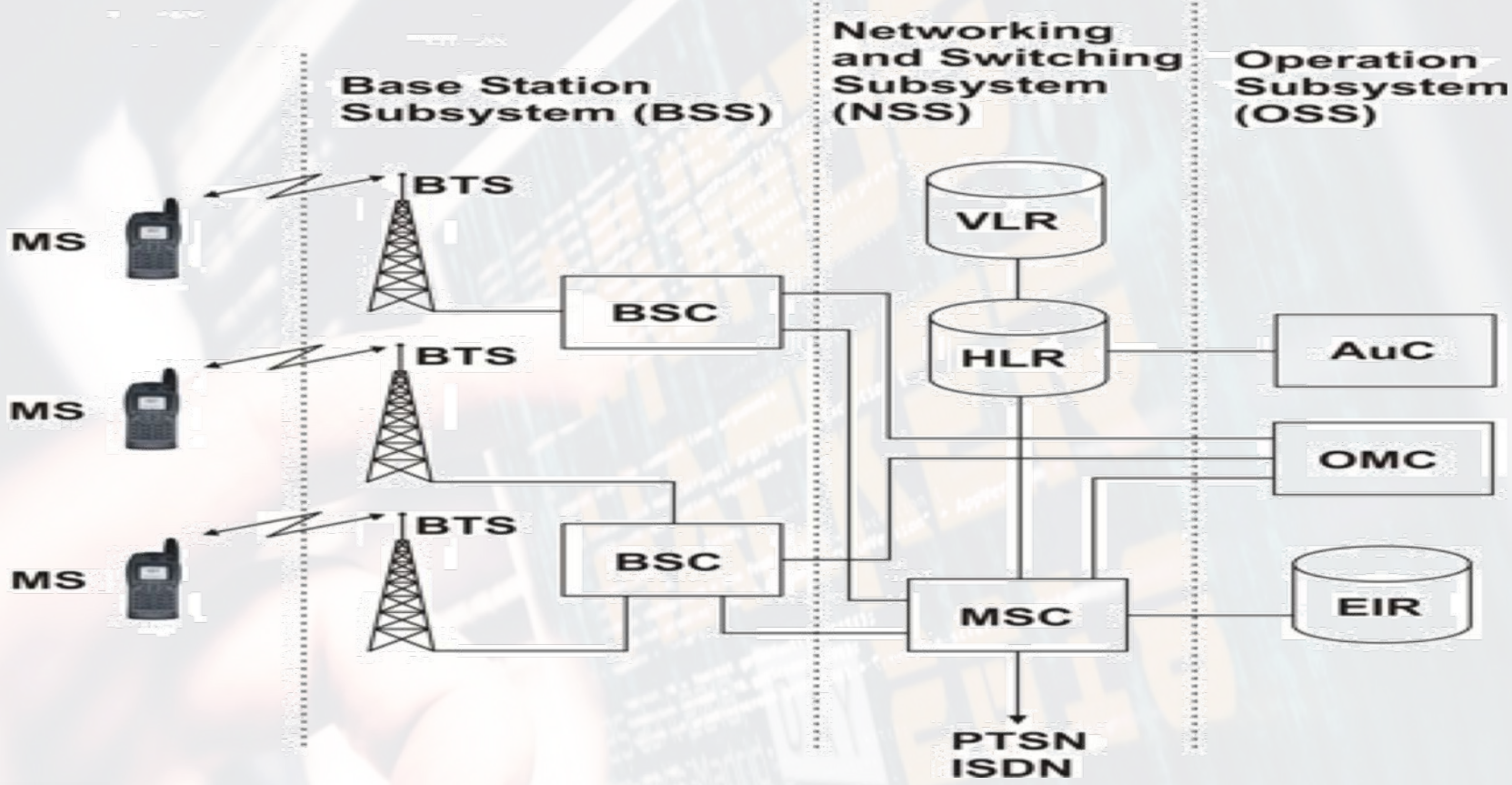
- Sólo se usa cuando el TMSI (Temporary Mobile Subscriber Identity) *no se encuentra disponible*, p.e. en la conexión inicial.
- El VLR es responsable de la *localización actual* de un suscriptor y asigna un TMSI.
- El terminal almacena el TMSI en la SIM y en el VLR
- Consulta al HLR de origen los permisos del usuario (si puede hacer llamadas o no).

HLR (Home Location Registrer)

- Almacena la posición del usuario dentro de la red, si está conectado o no y las características de su abono (servicios que puede y no puede usar, tipo de terminal, etc.)
- Es de carácter más bien permanente
- Cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.

Al recibir una llamada, el MSC pregunta al HLR correspondiente al número llamado si está disponible y dónde está (es decir, a qué BSC hay que pedir que le avise) y *enruta la llamada* o da un *mensaje de error*.

Conexiones 101



Productos comerciales

Whoami

Where is Wally? Pedro C. aka s4ur0n

IMSI con SDR

https://gi

IMSI-catcher

This program shows you IMSI numbers

What you need

1 PC
1 USB DVB-T key (RTL2832U) with antenna (less than 15$) or a OsmocomBB phone or HackRF

Setup

```
sudo apt install python-numpy python-scipy python-scapy

sudo add-apt-repository -y ppa:ptrkrysik/gr-gsm
sudo apt update
sudo apt install gr-gsm
```

If gr-gsm failled to setup. Try this setup : https://github.com/ptrkrysik/gr-gsm/wiki/Installation
Debian : https://tracker.debian.org/pkg/gr-gsm

```
$ sudo apt-get update && apt-get upgrade
$ sudo apt-get -y install wim net-tools git python-pip gnutls-dev cmake libboost-all-dev libcppunit-dev swig doxygen liblog4cpp5-dev python-numpy python-scipy python-scapy automake autoconf libhackrf-dev wireshark sqlite3
```

```
$ pip install PyBOMBS
$ pybombs auto-config
$ pybombs recipes add-
defaultspybombs prefix init
/usr/local -a default -R gnuradio-
default
$ pybombs install gr-gsm
```

```
$ cd /usr/local
$ git clone
https://github.com/pothosware/SoapySDR.git
$ cd SoapySDR
$ mkdir build
$ cd build
$ cmake ..
$ make -j4
$ sudo make install
$ sudo ldconfig –v
```

```
$ cd /usr/local
$ git clone https://github.com/ptrkrysik/gr-gsm.git
$ cd gr-gsm
$ mkdir build
$ cd build
$ cmake ..
$ make
$ sudo make install
$ sudo ldconfig -v
```

```
$ cd /usr/src
$ git clone https://github.com/steve-m/kalibrate-rtl
$ cd kalibrate-rtl/
$ ./bootstrap
$ ./configure
$ make
$ sudo make install
```

```
$ cd /usr/src
$ git clone git://git.osmocom.org/gr-osmosdr
$ cd gr-osmosdr
$ mkdir build
$ cd build
$ cmake ../
$ make
$ sudo make install
$ sudo ldconfig -v
```

```
$ cd /usr/src
$ git clone
https://github.com/0ros42/IMSI-
catcher
```

```
$ cd /usr/
$ python
$ grgsm_l
serverport
$ sudo wi
gsmtap' -
```

Conclusiones: Problemas

```
$ cmake ../ -DINSTALL_UDEV_RULES=ON
-DDETACH_KERNEL_DRIVER=ON
```

```
Etc, etc, etc…
```

Demo

MUNDO HACKER DAY

CS³ IIC (Interactive IMSI Catcher)

MUCHAS GRACIAS