ISEC TU Graz

# Mobile Network Security

*Mobile Security 2025*

Florian Draschbacher
florian.draschbacher@tugraz.at

# Outline

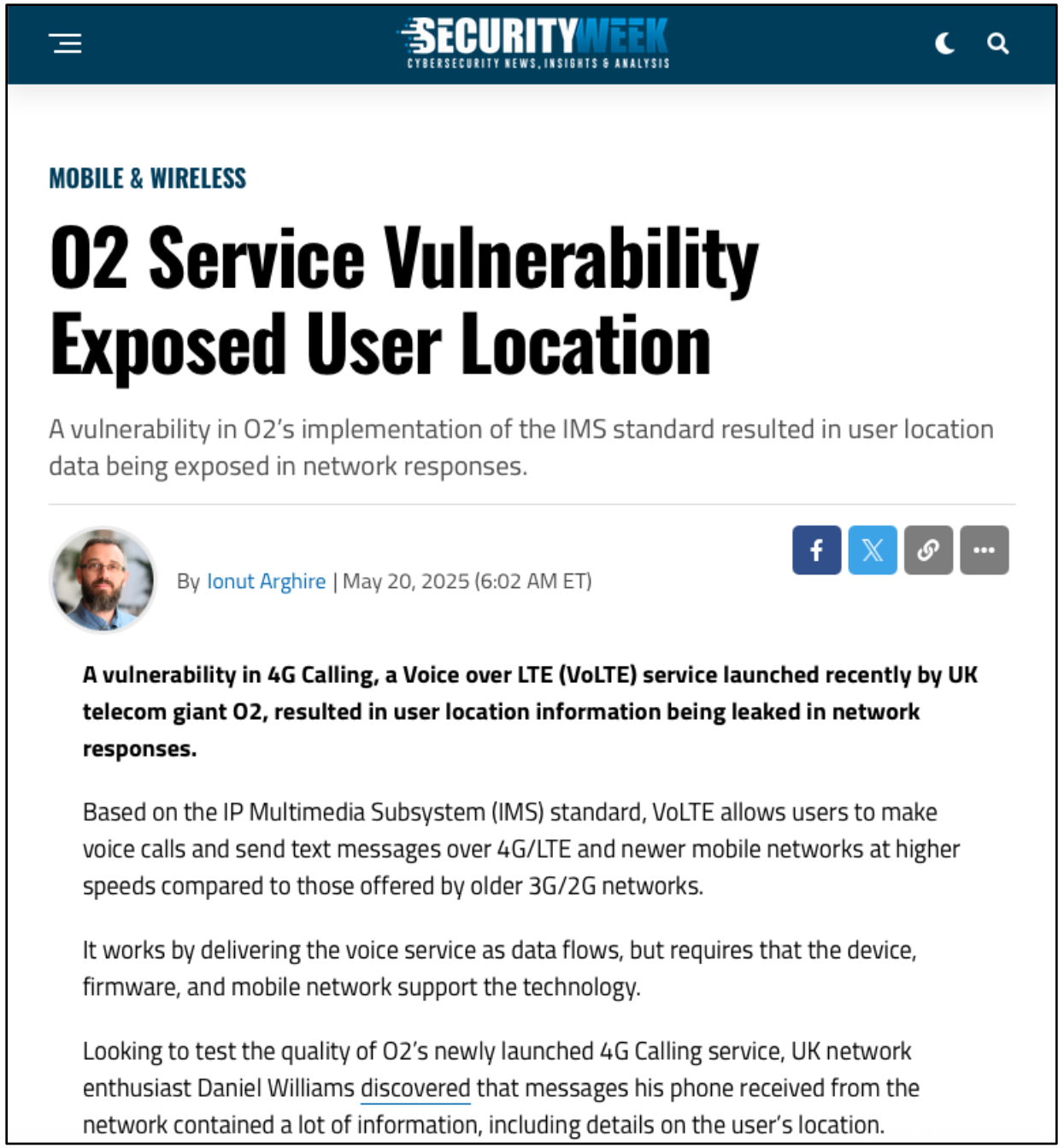
- Background
  - Evolution of cellular networks
  - Architecture
  - Security
- Attacks
  - Active, Passive
  - Built-in backdoors
- Protection Mechanisms
  - Are you protected? How to defend yourself?

# Introduction

- So far we concentrated on the **smarts** of smartphones
  - What about the phone part?

- How do phone calls, messaging and Internet over cellular networks work?
  - What components are involved?
  - What protocols and technologies do they use?

- What about the security of these technologies?
  - Who can intercept communication?
  - What are the privacy consequences of being reachable on-the-go?
  - …



SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

MOBILE & WIRELESS

# O2 Service Vulnerability Exposed User Location

A vulnerability in O2's implementation of the IMS standard resulted in user location data being exposed in network responses.

By Ionut Arghire | May 20, 2025 (6:02 AM ET)

**A vulnerability in 4G Calling, a Voice over LTE (VoLTE) service launched recently by UK telecom giant O2, resulted in user location information being leaked in network responses.**

Based on the IP Multimedia Subsystem (IMS) standard, VoLTE allows users to make voice calls and send text messages over 4G/LTE and newer mobile networks at higher speeds compared to those offered by older 3G/2G networks.

It works by delivering the voice service as data flows, but requires that the device, firmware, and mobile network support the technology.

Looking to test the quality of O2's newly launched 4G Calling service, UK network enthusiast Daniel Williams discovered that messages his phone received from the network contained a lot of information, including details on the user's location.

Source: securityweek.com

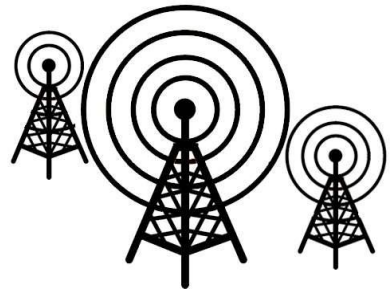
## What?

Misconfigured network leaked user location

## Problems?

- Mobile networks are incredibly complex systems
- They process a lot of sensitive user data
  - Communication:
    - Calls, Messages, Internet traffic, …
  - Metadata:
    - Who contacts whom
    - Nearest cell phone towers

# Introduction



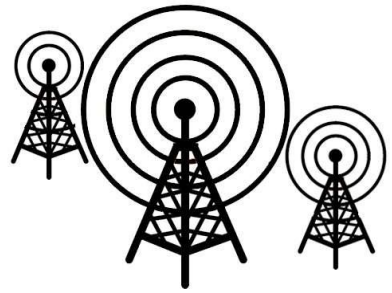
## Goals

- Protect business models and operational services
- Privacy for user identity, data confidentiality
- Regulatory issues → legal interception

## How to apply security?

- Minimize number of security threats
- Remember: Cost efficiency & high performance (load balancing)
- Interoperability with legacy systems (GSM <-> UMTS <-> LTE)
- Practical issues, e.g. end-to-end *vs.* hop-by-hop security?

# Introduction



## Technical objectives

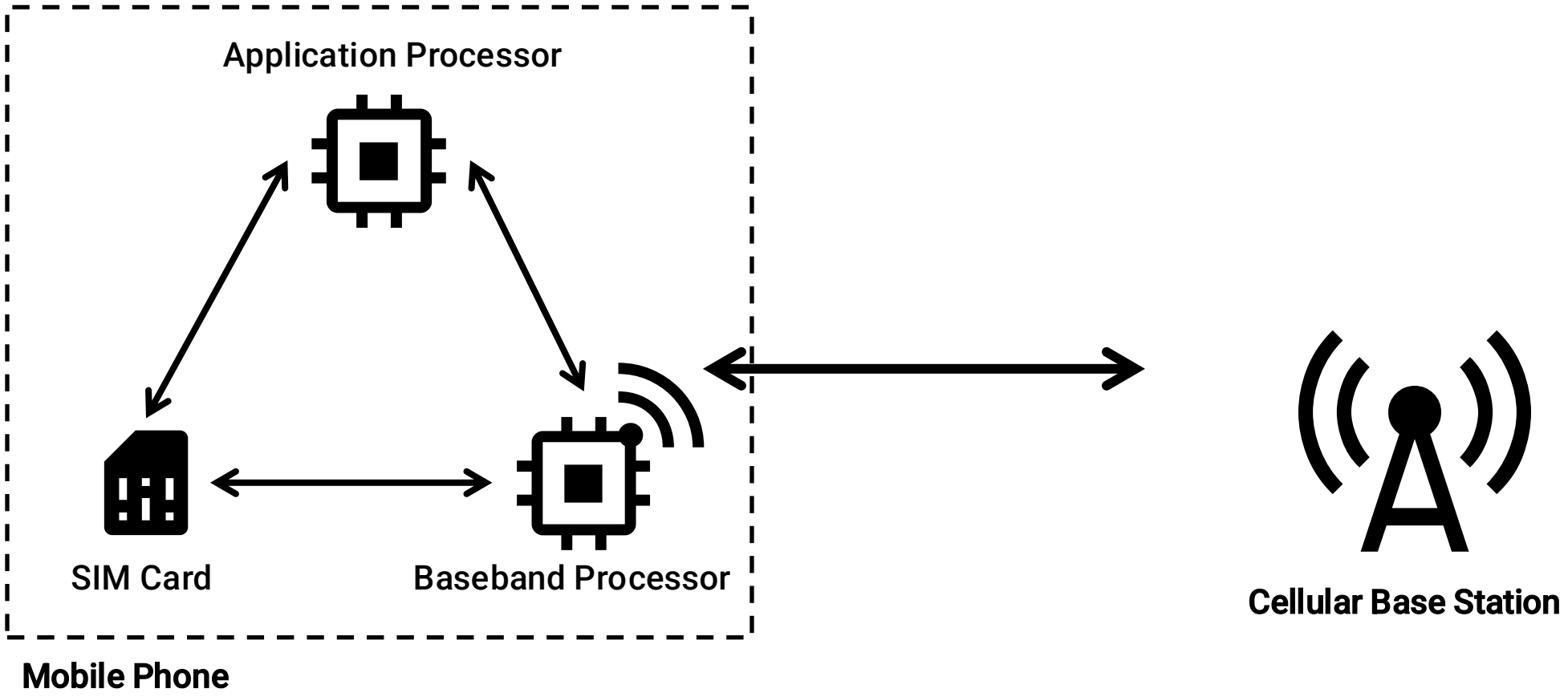
- Authentication of user and network
- Confidentiality
  - User data & signaling data
  - User & device identity
  - User location
- Signaling data integrity
- User untraceability(?)

→ Need strong algorithms for encryption and integrity checking,

→ Need algorithm extensibility for future-proofness

# Mobile Equipment
# (= Mobile Network Client)

# Mobile Equipment Architecture



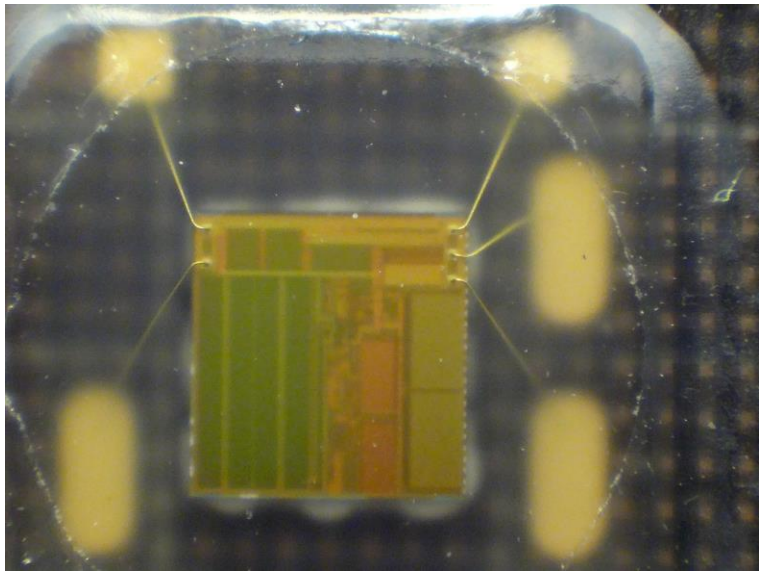

Pictures: Google / Apache 2.0

# Subscriber Identification Module (SIM) Card

aka. “Universal Integrated Circuit Card (UICC)”

- A smart card, containing microcontroller and (flash) memory

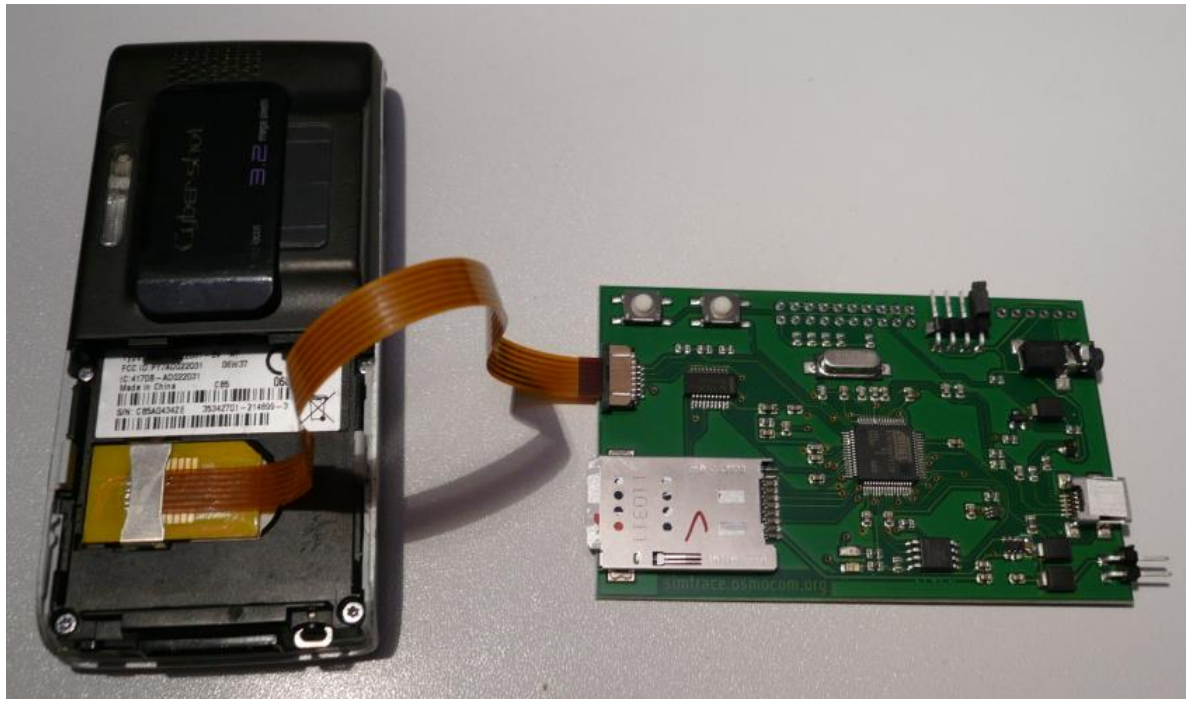
Source: wikipedia.org / Janke / CC BY-SA



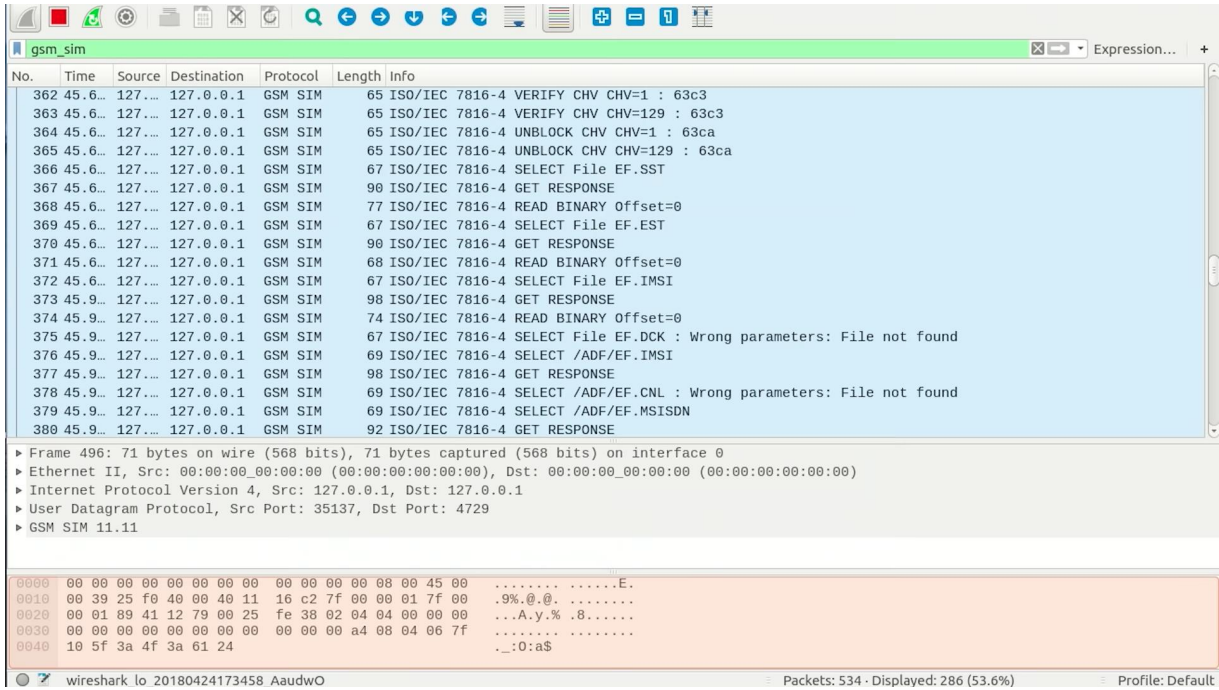
- Authenticates a client in the cellular network
  - Symmetric authentication key $K_i$
- Contains unique identifiers
  - IMSI: International Mobile Subscriber Identifier
  - ICCID: Integrated Circuit Card Identifier
- Also: Java programs, contacts, preferred roaming networks, …

# SIM Communication with Mobile Equipment

- ISO-standardised protocol commonly referred to as APDU
  - Application Protocol Data Unit
- May be intercepted using special hardware and software tools

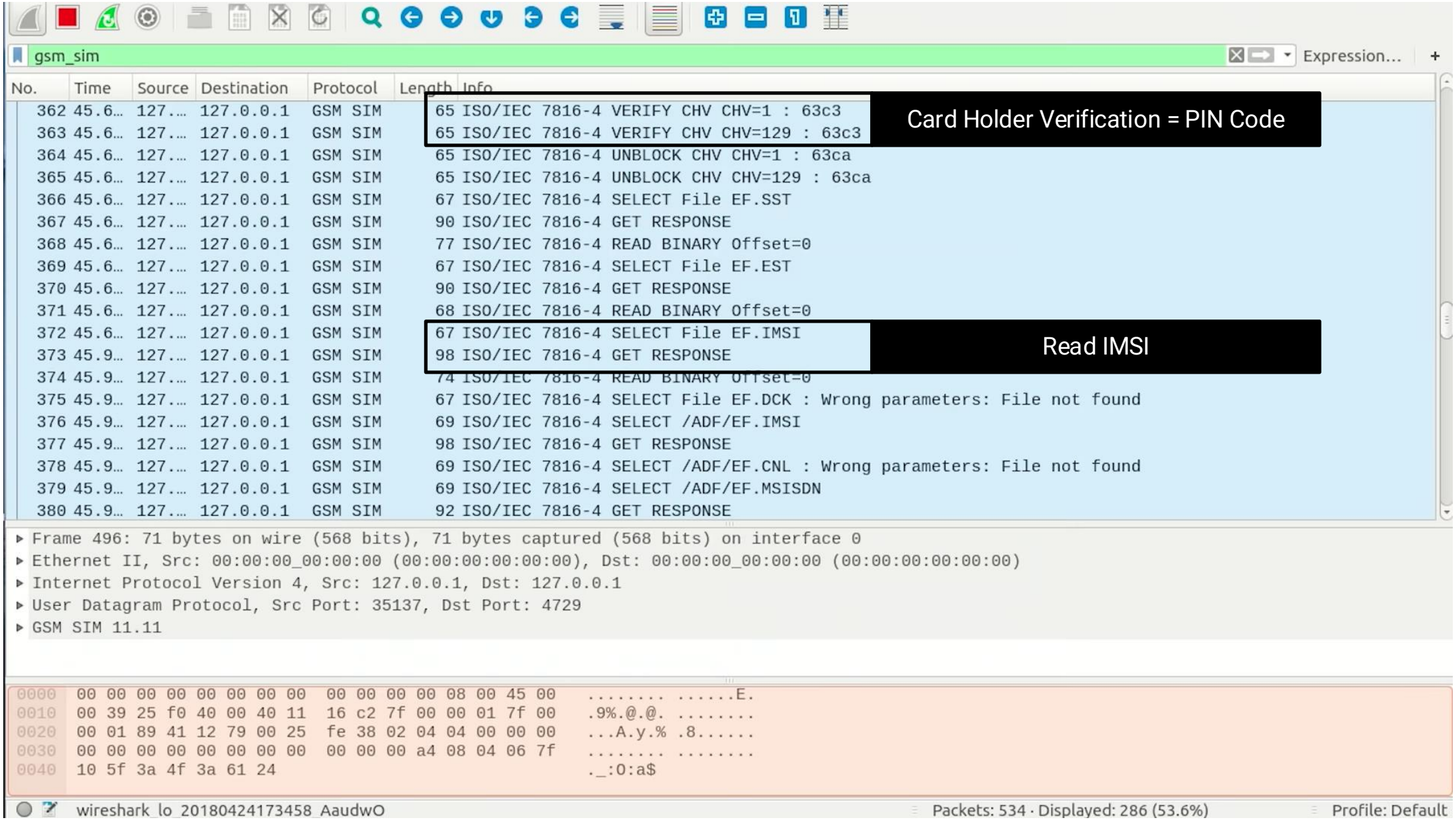


Source: osmocom.org




Source: Screenshot LiveOverflow

ISEC TU Graz




Source: Screenshot LiveOverflow

# Authentication Process

- The $K_i$ in SIM card is issued by network operator, stored in their database

1. Mobile Equipment (ME) passes PIN to SIM card to get IMSI
2. ME passes IMSI to network operator
3. Network operator generates random nonce RAND
4. Network operator computes SRES_1 = $A3_{Ki}$(RAND) and $K_C$ = $A8_{Ki}$(RAND)
5. Network operator sends RAND to ME
6. ME passes RAND to SIM card, which computes SRES_2 and $K_C$
7. ME sends SRES_2 to network operator
8. If SRES_1 equals SRES_2, the authentication succeeded
9. Subsequent communication will be encrypted using $K_C$

# SIM Cloning

- The authentication process was designed so that $K_i$ never leaves the SIM card
  - Legitimate SIM card required to access mobile network
- However, the COMP128 implementation of the A3/A8 algorithms vulnerable
  - Designed in secrecy, but reverse-engineered in 1998, attacks soon after
- $K_i$ could be calculated from a series of A3/A8 challenges to SIM card
  - 20k challenges (brute force: 2^128)
- $K_i$ and IMSI can be written into blank SIM cards to create SIM clone
- Modern mobile networks use improved COMP128, SIMs limit challenges

Source: https://www.tcs.hut.fi/Studies/T-79.514/slides/S5.Brumley-comp128.pdf

# SIM Cloning

- Cloned SIMs can authenticate to the network as the legitimate SIM card
  - Intercept or inject communication on behalf of original SIM holder
- Extraction from SIM cards is not the only way to obtain $K_i$
  - Access network operator database
  - Infiltrate SIM card manufacturer

## The NSA Reportedly Stole Millions Of SIM Encryption Keys To Gather Private Data

Alex Wilhelm, Sarah Buhr
/ 2:39 AM GMT+1 • February 20, 2015


The American National Security Agency (NSA), and the British Government Communications Headquarters (GCHQ), similar clandestine intelligence agencies, stole SIM card encryption keys from a manufacturer, allowing the groups to decrypt global cellular communications data.

Source: techcrunch.com

# Embedded SIM (eSIM)

- Originally, SIM was the term for the hardware (card) and its software
- Later versions denoted the card as Universal Integrated Circuit Card (UICC)
  - Running SIM application

- Further abstraction: Embedded SIM
  - eUICC: Chip statically mounted to Mobile Equipment
  - eSIM: Carrier profile installed onto eUICC

- Every eUICC is uniquely identified using eSIM ID (EID)

- Carrier profiles are provisioned encrypted
  - May only be decrypted inside eUICC

# SIM Swap Attacks / SIM Jacking

- A mobile numbers is not fixed to a SIM card
  - Mobile Number Portability (MNP) enables carrier migration

**Can be abused by attackers to gain control over a mobile number:**

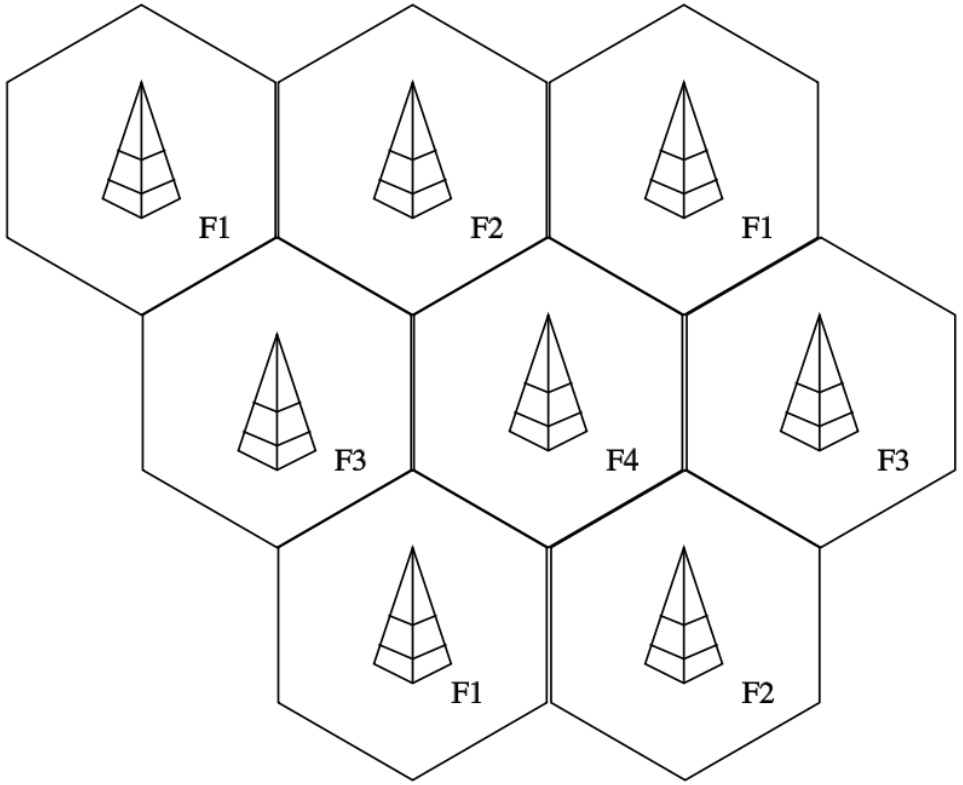
1. Collect personal information about victim
2. Initiate number migration to attacker's SIM through victim's carrier
3. Prove identity through stolen personal information
4. After migration, the victim loses control over the mobile number

- SMS is still commonly used for Two Factor Authentication!
- This attack has been used for high-profile hacks and is on the rise!

# Mobile Phone Networks

# Modern Mobile Phone Networks

- Distributed over land areas called „cells“
  - “Cellular network“
- Every cell is covered by >= 1 base stations
  - More depending on needed capacity
- Cells use different radio frequencies
  - Prevents interference of neighbouring cells
- Base stations are interconnected in multiple layers
  - And linked to landline network and Internet



# Cellular Network Generations

- Cellular Network technology is constantly advancing

- New technology generations are rolled out roughly every 10 years
  - First generation: 1980s
  - Currently: Roll-out of 5G in progess
  - 6G anticipated for 2030

- Generation: Improved technology that is incompatible with previous one
  - Still: Mobile Equipment is usually backwards-compatible

- The exact technology used for a generation depends on the region!
  - E.g. 3G in America (CDMA2000) is incompatible with 3G (UMTS) in Europe

# General Network Structure

- A network consists of functionality in multiple subsystems
  - Base Station Subsystem (BSS): Base stations for radio link
  - Core Network / Network Switching Subsystem: Managing calls
  - Data Core Network (eg. GPRS Core Network): Managing data transfers

- The radio link determines the physical data transfer protocol
  - Typically changes between different generations of cellular networks

- Rest of the infrastructure helps locate phones
  - Establishing calls, delivering data, … despite phone moving between cells
  - May be shared between different network generations

# Cellular Network Technologies (Europe)

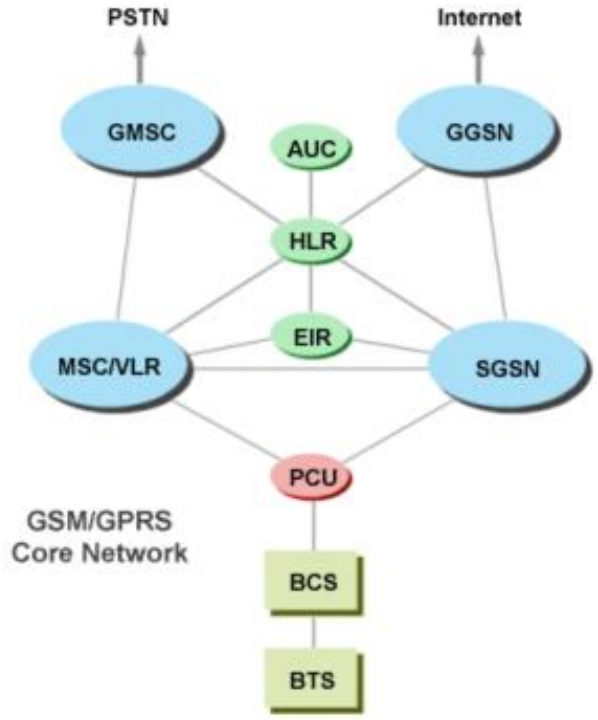
- **1. Generation**:
  - Analog audio transmission
  - Data only through a modem (modulator-demodulator)

- **2. Generation**: GSM
  - Encrypted digital audio between phone and base station
  - Later added GPRS and EDGE for packet-switched data communications

- **3. Generation to 5. Generation**: UMTS, LTE, 5G
  - Faster data communications
  - Improved bandwidth

# 2G Networks

- Commerical launch in 1992
- User authentication based on per-subscriber secret key in SIM
- TDMA-based, circuit switching
  - „Time Division Multiple Access“
  - Share same frequency channel for multiple users by dividing signal into different time slots




## Versions

- 2.5G: GPRS (added in 2000)
  - Theoretical speed: 171 kbps down, 40 kbps up
- 2.7G: EDGE
  - Theoretical speed: 384 kbps down, 108 kbps up

# 3G Networks

## Features

- Same core network as 2G
  - Still circuit-switched (GSM) & packet-switched hybrid (UMTS)
- No integrity protection (like LTE) → Downgrade attacks possible
- Almighty base station → Decides if, when, and how to authenticate / encrypt

## Versions

| | | |
|---|---|---|
| 3G | UMTS | max. 2 Mbps down, 384 kbps up |
| 3.5G | HSDPA | max. 14.4 Mbps down, 2 Mbps up |
| 3.6G | HSUPA | max. 14.4 Mbps down, 5.76 Mbps up |
| 3.75G | HSPA+ | max. 21 Mbps down, 5.8 Mbps up |
| 3.8G | HSPA+ Enhanced | max. 84 Mbps down, 20 Mbps up |
| 3.9G | LTE (**pre 4G!**) | max. 100 Mbps down, 50 Mbps up |

# Evolution: 4G Networks

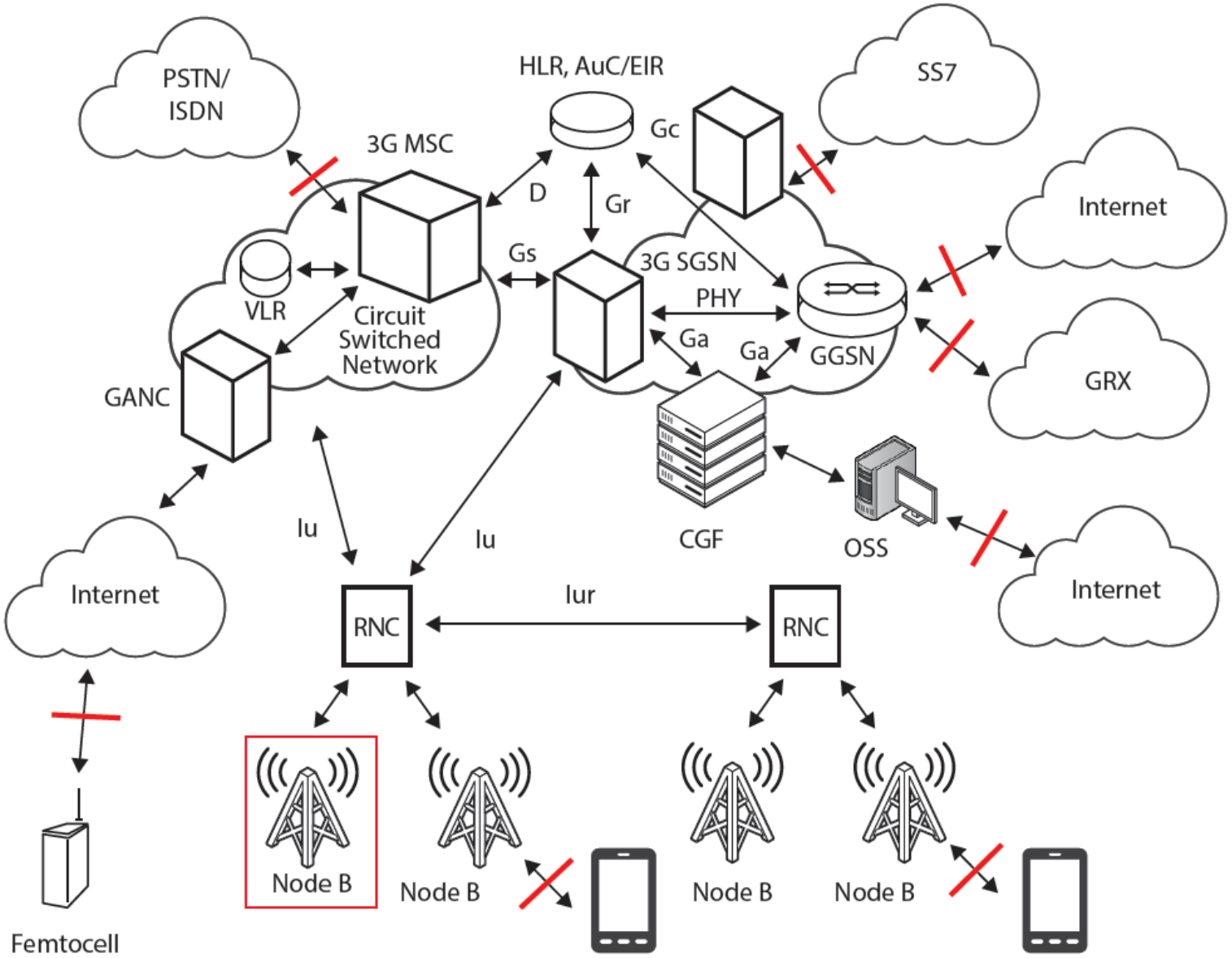
Currently: LTE Advanced (LTE-A) max. 1 Gbit down, 500 Mbit up

**Features**

- Only IP-based communication (also voice → VoLTE), no more circuit switching
  - Fallback support for circuit-switched calls
- Mutual authentication between base station & mobiles
- Mandatory integrity protection for signaling messages
- IMEI ciphered to protect user equipment privacy

- New algorithms and extensibility
  - Word-oriented stream cipher (128 bit key): SNOW 3G
  - Integrity, confidentiality: AES-GCM

# 3G/4G Network Structure




Source: https://goo.gl/V98GB5

## Legend

- Node B
  UMTS Base Station
- RNC
  Radio Network Controller
- SGSN
  Serving GPRS Support Node
- GGSN
  Gateway GPRS Support Node
- MSC
  Mobile Switching Center

# 3G/4G Network Workflow

GSM equivalent: Base Transceiver Station (BTS)

## 1) Node B

- Minimum functionality base station in UMTS networks
- Typically located near the antenna (but not necessarily)
- Controlled by RNC using a „Iub“ interface

## 2) RNC

- Main task: Manage connected Node Bs and radio resources
  - Channels, signal strength (power), cell handover
- Can build Mesh networks with other RNCs

**3a)** Speech: MSC (Mobile Switching Centre) → routing voice / SMS

**3b)** Data: SGSN → routing data

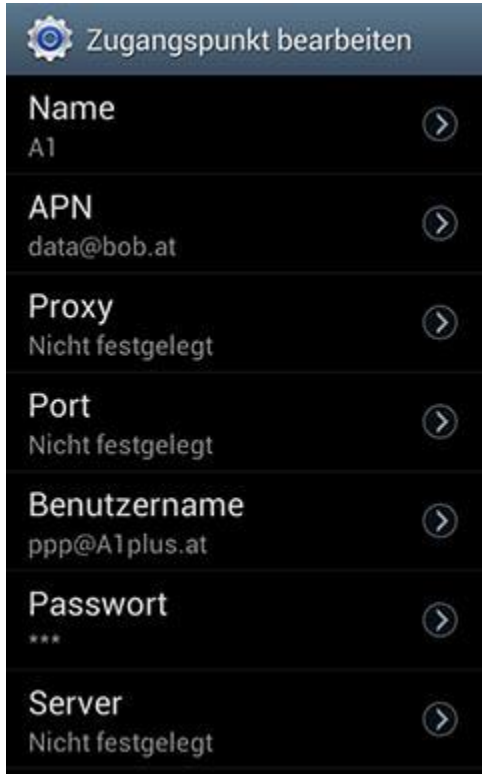
# 3G/4G Network Components

## SGSN

- Data delivery from/to mobile station in defined geographical service area
- (*De*-)tunnel packets from/to GGSN (*Downlink*, Uplink)
- Handover → phone moves from Routing Area A to Routing area B
- User data billing

## GGSN

- Inter-networking between internal network and external packet switched networks (Internet)
- Keeps your connections alive while moving around
- User authentication, IP pool management, QoS



# GSM Encryption

**How?** Stream ciphers to encrypt traffic on air interface

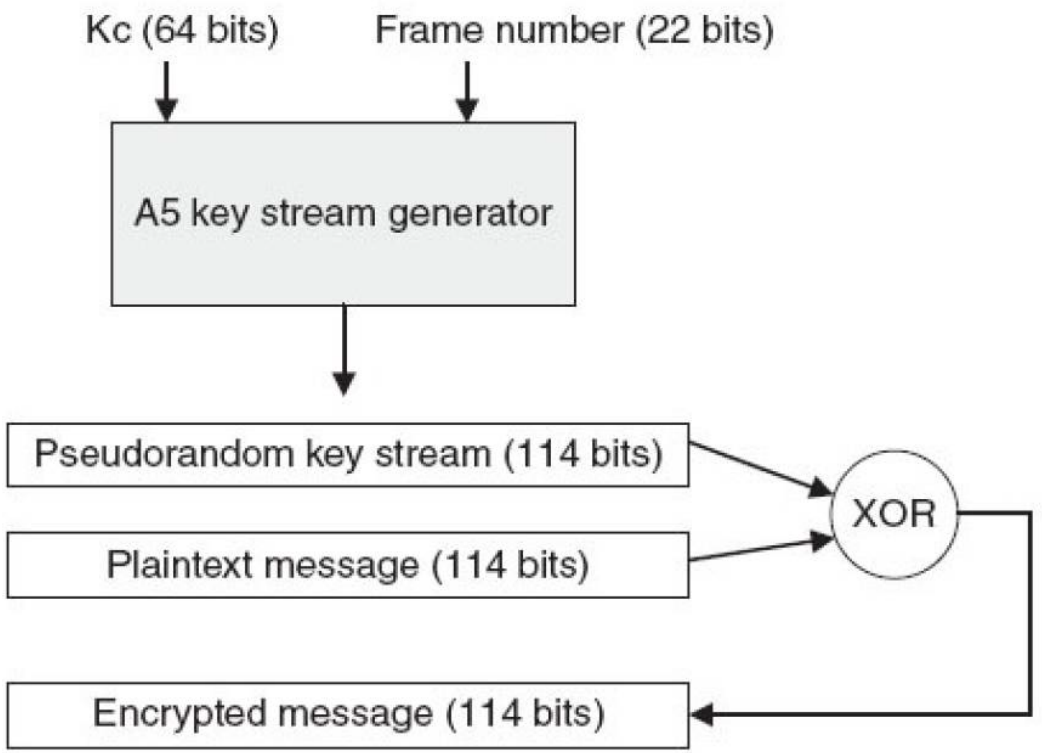
## Set of algorithms

- A5/0: Unencrypted, no cracking needed ☺
  → broken (and partly banned, e.g. by T-Mobile Austria (Magenta))
- A5/1: Combination of 3 linear feedback shift registers (LFSRs)
  → 64-bit key, broken using rainbow tables in 2009
- A5/2: export version of A5/1
  → broken in 1999, banned since 2006
- A5/3 + A5/4: Backport of Kasumi UMTS cipher (current standard)
  – 128-bit key, 64-bit input / output

# GSM Encryption A5/1

Key size: 64 bits (!!)

Avoid replay attacks



# (Recent) Attacks

# Scenarios

## Intercept

- Adversary records calls & SMS
  - Decryption in real time or batch process (after recording)

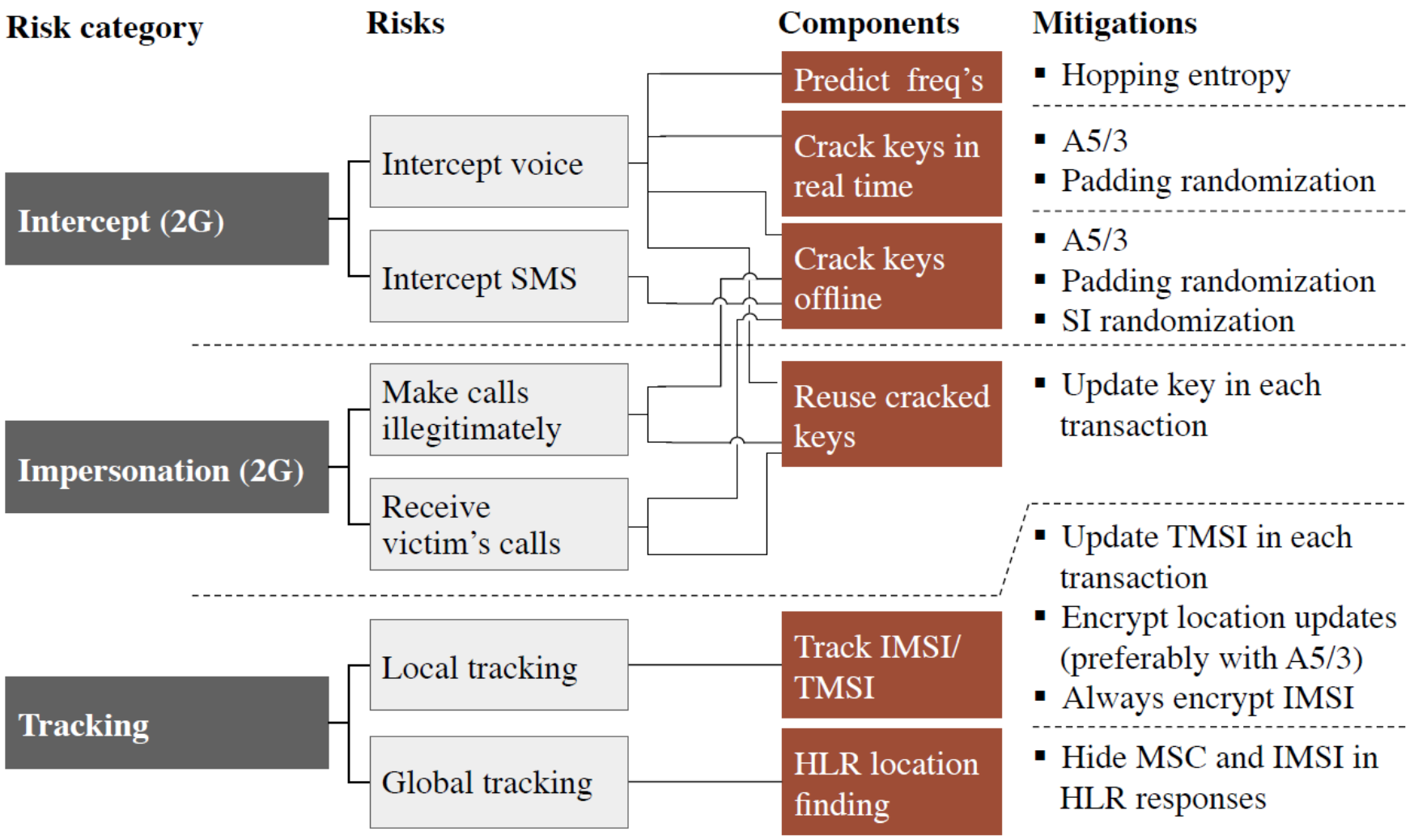
## Impersonation

- Calls or SMS spoofed
- Received using stolen mobile identity

## Tracking

- Tracing mobile subscribers

# Scenarios & Mitigations




Source: https://goo.gl/15pRhE

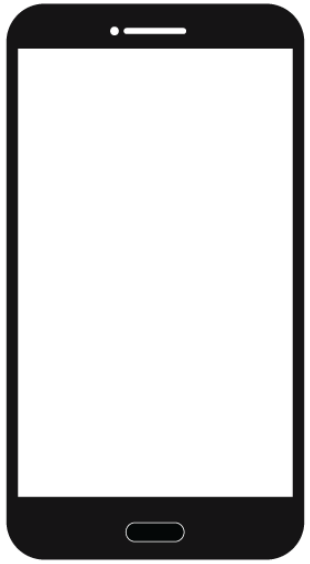
# Active Attack: Fake Base Stations

**= IMSI Catchers**

- Partially exploit weaknesses in GSM & 3G networks
- Used for
  - Tracking users (IMEI, IMSI, location)
  - Eavesdropping calls, data, SMS, etc.
  - Man-in-the-Middle
  - Attack phone using operator system messages,
    - e.g. Management Interface, re-program APN, HTTP proxy, SMS/WAP server, …
  - Attack SIM or phone baseband
  - Geo-targeting ads (SMS)
  - Intercept TAN, mobile phone authentication, …

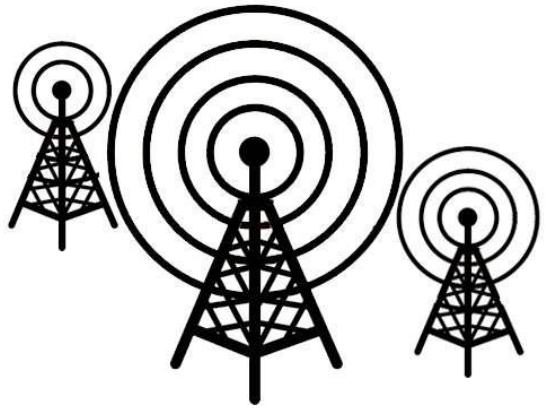
Tracking,
Call & Data interception

# How does it work?



Advertise base station on beacon channel

Phone sends IMSI / TMSI (sort of secret)



MCC: Mobile Country Code (232 for .at)

MNC: Mobile Network Code

- Country-specific tuple with MCC, e.g. 232-01 for a1.net

→ Phones will connect to *any* base station with spoofed MNC/MCC

- If you claim it, they will come because strongest signal wins ☺
- Crypto optional (until 4G) and set by base station!

Terminal 1

Fichier Édition Affichage Rechercher Terminal Aide

```
$ sudo python simple_IMSI-catcher.py
WARNING: No route found for IPv6 destination :: (no default route?)
cpt ; IMSI ; country ; brand ; operator
1 ; 234 20 730143[redacted] ; Guernsey (United Kingdom) ; 3 ; Hutchison 3G UK Ltd
2 ; 208 20 154308[redacted] ; France ; Bouygues ; Bouygues Telecom
3 ; 208 20 029666[redacted] ; France ; Bouygues ; Bouygues Telecom
4 ; 208 20 085162[redacted] ; France ; Bouygues ; Bouygues Telecom
5 ; 208 20 031381[redacted] ; France ; Bouygues ; Bouygues Telecom
6 ; 208 20 031233[redacted] ; France ; Bouygues ; Bouygues Telecom
7 ; 208 20 031343[redacted] ; France ; Bouygues ; Bouygues Telecom
8 ; 208 20 171286[redacted] ; France ; Bouygues ; Bouygues Telecom
9 ; 208 20 090096[redacted] ; France ; Bouygues ; Bouygues Telecom
10 ; 208 20 100817[redacted] ; France ; Bouygues ; Bouygues Telecom
11 ; 208 20 144546[redacted] ; France ; Bouygues ; Bouygues Telecom
12 ; 208 20 220088[redacted] ; France ; Bouygues ; Bouygues Telecom
13 ; 208 20 171268[redacted] ; France ; Bouygues ; Bouygues Telecom
14 ; 208 20 154457[redacted] ; France ; Bouygues ; Bouygues Telecom
15 ; 208 20 144758[redacted] ; France ; Bouygues ; Bouygues Telecom
16 ; 208 20 031231[redacted] ; France ; Bouygues ; Bouygues Telecom
17 ; 208 25 001134[redacted] ; France ; LycaMobile ; LycaMobile
18 ; 208 20 171275[redacted] ; France ; Bouygues ; Bouygues Telecom
19 ; 208 20 031317[redacted] ; France ; Bouygues ; Bouygues Telecom
20 ; 208 20 154456[redacted] ; France ; Bouygues ; Bouygues Telecom
21 ; 208 20 144857[redacted] ; France ; Bouygues ; Bouygues Telecom
22 ; 208 20 031261[redacted] ; France ; Bouygues ; Bouygues Telecom
23 ; 208 20 144819[redacted] ; France ; Bouygues ; Bouygues Telecom
24 ; 208 20 100230[redacted] ; France ; Bouygues ; Bouygues Telecom
```

Terminal 2

Fichier Édition Affichage Rechercher Terminal Aide

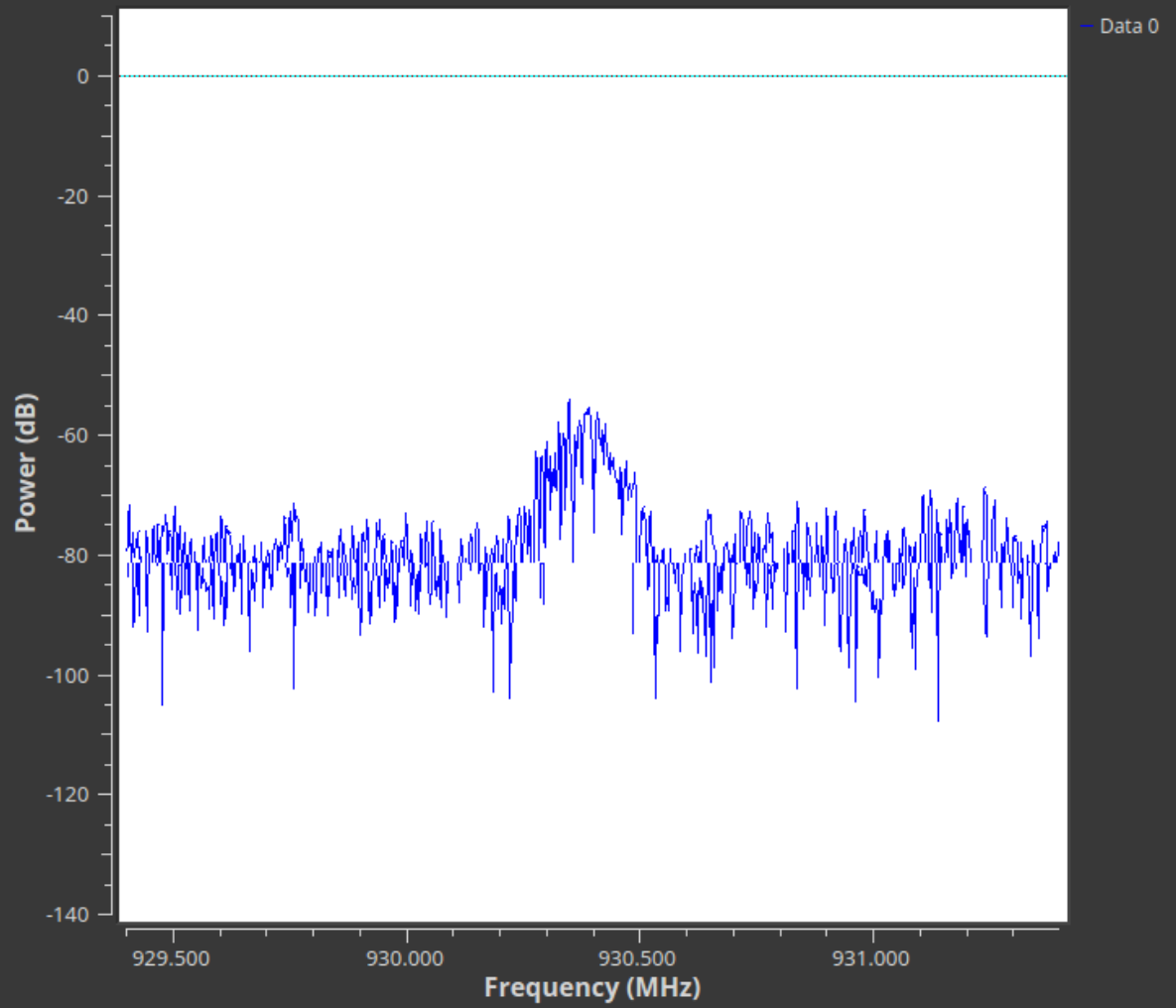
```
$ airprobe_rtlsdr.py
linux; GNU C++ version 5.3.1 20151219; Boost_105800; UHD_003.009.002-0-unknown

gr-osmosdr 0.1.4 (0.1.4) gnuradio 3.7.9
built-in source types: file osmosdr fcd rtl rtl_tcp uhd miri hackrf bladerf rfsp
ace airspy redpitaya
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Rafael Micro R820T tuner
[R82XX] PLL not locked!
Exact sample rate is: 2000000,052982 Hz
[R82XX] PLL not locked!
Using Volk machine: sse3_64_orc
 2d 06 22 00 d8 58 3a 30 a0 0d 25 b8 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 31 06 21 00 08 29 43 02 37 10 34[redacted] 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 2d 06 22 00 ec 58 13 18 80 06 e3 b9 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 59 06 1a 8f e7 90 80 ad 1c 60 49 00 00 00 00 00 00 00 ff 79 00 00
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 2d 06 22 00 90 0e 42 fa cf 58 e5 08 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 59 06 21 00 08 29 80 02 51 34 80[redacted] 17 08 29 80 02 20 69 66[redacted]
 25 06 21 00 05 f4 d1 68 9f 28 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 ff 68 0f 60 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

Gr-gsm Livemon

PPM Offset 0

Gain 30,000

Frequency 930400000




Source: https://goo.gl/5L29Ft

# IMSI Catchers in Practice

## User identification

- Retrieve IMSI / IMEI / TMSI
- Reject location update
- Tracking

## Traffic Man-in-the-middle

- Hold user in cell
- Actively intercept traffic
  - Relay to real network
  - Active or passive decryption

## UMTS Downgrade

- Blocking UMTS transmission
- Spoofing system messages

## Hold but intercept passively

- Imprison in cell
  → Phone not lost to neighbor cell

# Fake Base Stations

## Dirtboxes on a Plane

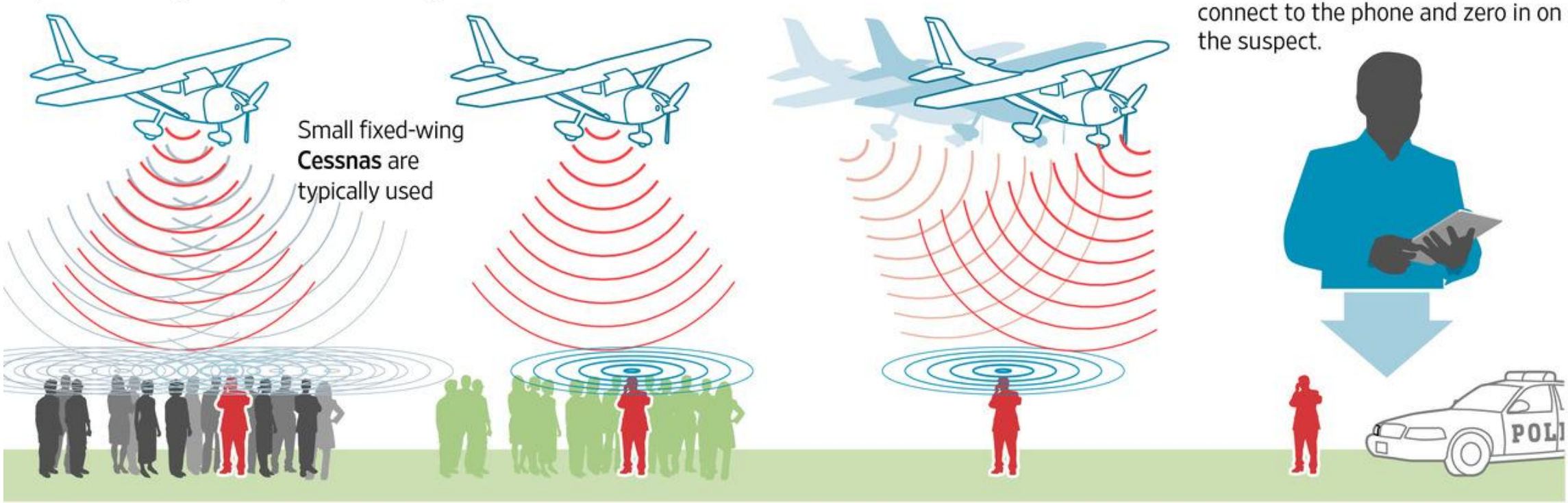
How the Justice Department spies from the sky

**1** Planes equipped with fake cellphone-tower devices or 'dirtboxes' can scan thousands of cellphones looking for a suspect.

**2** Non-suspects' cellphones are 'let go' and the dirtbox focuses on gathering information from the target.

**3** The plane moves to another position to detect signal strength and location...

**4** ...the dirtbox will 'let go' of the suspect's phone once officers move into position nearby. Those officers then use their handheld device to connect to the phone and zero in on the suspect.




Source: people familiar with the operations of the program

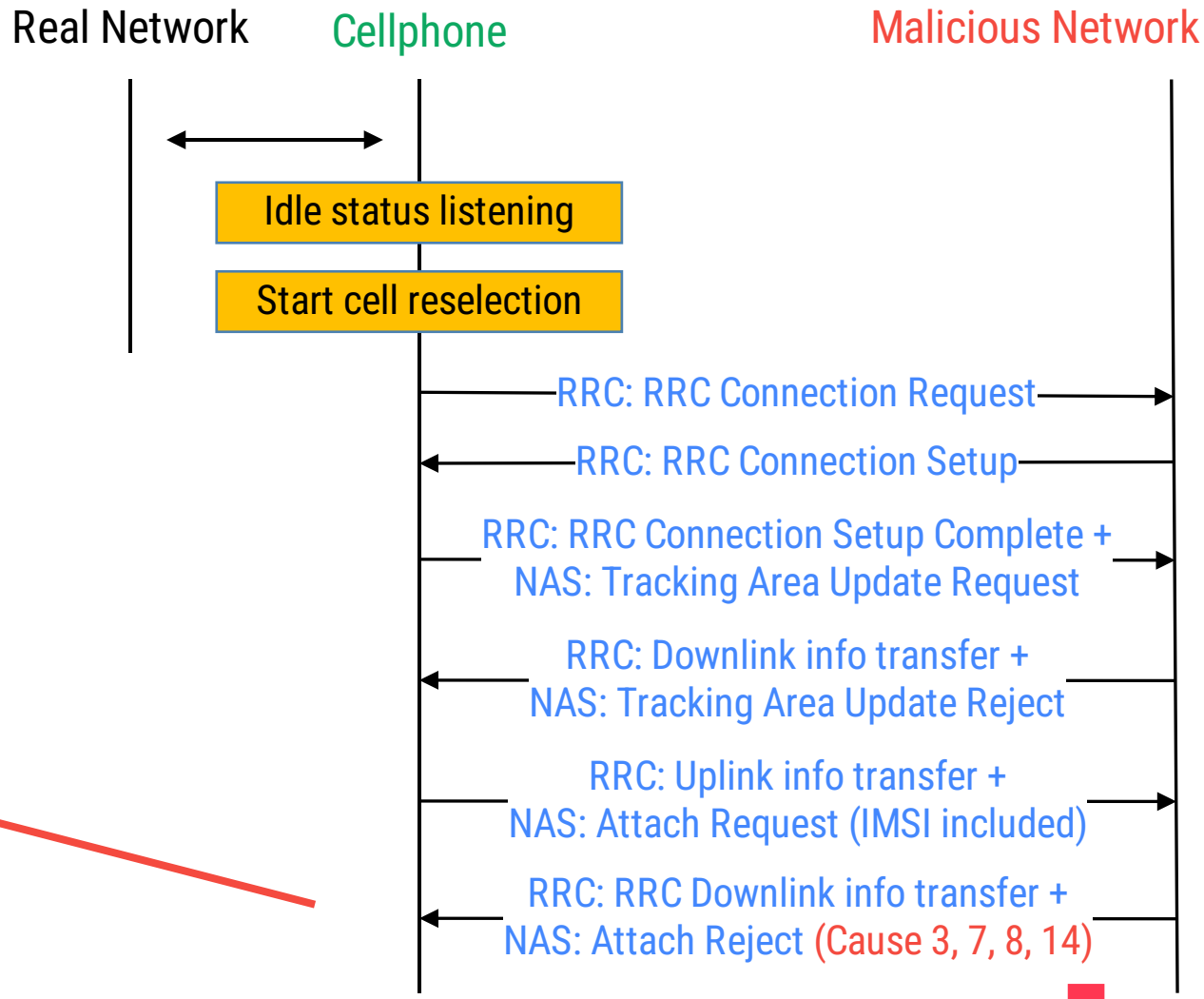
Brian McGill/THE WALL STREET JOURNAL.

Source: https://goo.gl/C2GUCK

# Active Attack: DoS

## Fake base station sending messages

- „You are an illegal cellphone“
- „No network available here. You can shut down your 2G/3G/4G modem.“




Attach Request message can include cause for reject
→ Some special causes result in no service…

# Passive Attack: Key Cracking

- A5/1 vulnerable to generic pre-computation attacks
  - Goal: Break session key for communication between base station and phone

**How to?**

1. Intercept GSM call with reprogrammed 20 euro phone
   - Idea: Cluster multiple phones for wide-scale capture
2. Crack A5/1 session key using rainbow tables (1-2 TB)
   - Done in a few seconds using GPU power


**Note**: Also A5/3 uses only 64 bit key on SIM & USIM

→ According to „Intercept“ broken by NSA Source: https://goo.gl/mPluNH

→ GSM A5/4 and UMTS UEA/1 considered secure with USIM (128 bit key)

# Signaling System 7

- Protocols used by most Telcos to identify network elements, clients, …
- Share session key in case of roaming (but works also without roaming!)

**Problem:**

- Walled-garden approach → we trust each other, need no auth
- Getting access is easy
  - Buy from telcos for < 1000 euro / month
  - Find equipment unsecured on internet (Shodan)

**Attacker‘s playground**

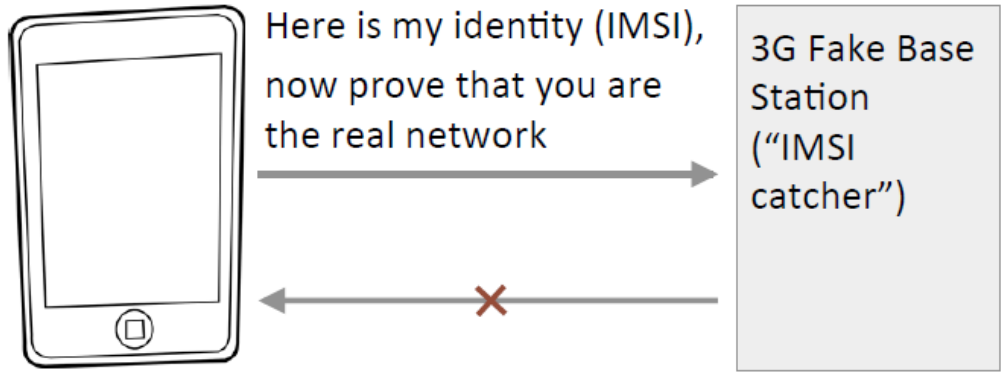
- Track any phone using a variety of signaling messages, e.g.
  - Phone number → `AnytimeInterrogation` → Get subscriber location (Cell ID)

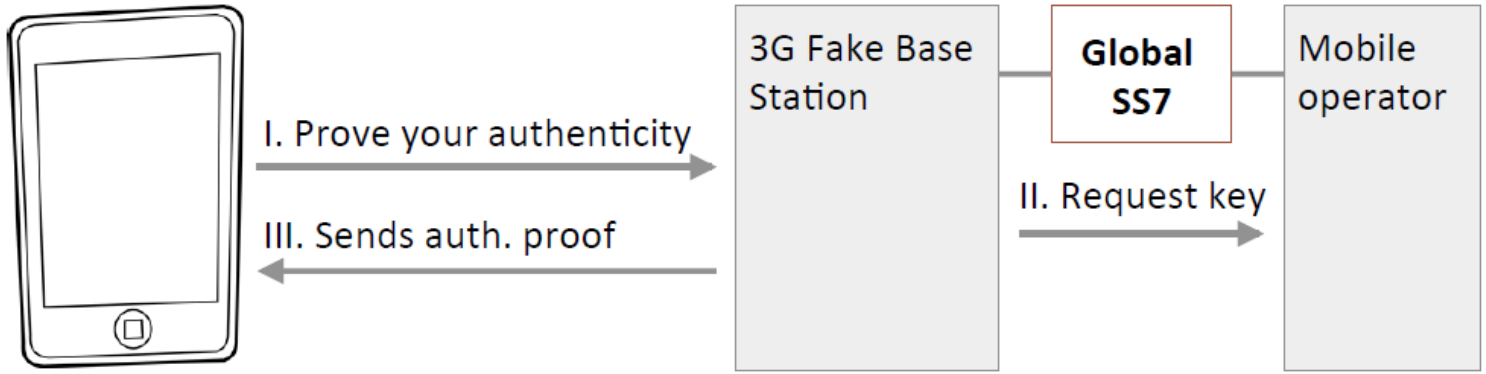
# Signaling System 7

Send from any international SS7 inter-connection → abuse legitimate messages

## Abuse Scenario

- Local passive intercept: `SendIdentification`
  → Easily blockable at network boundary
- 3G IMSI catcher: `SendAuthenticationInfo`
- Rerouting attacks: `UpdateLocation`
  → Message required for operations




Source: https://goo.gl/YBhvXw

# Signaling System 7

## How to intercept 3G (A5/3)?

1. Use software-defined radio (SDR) to capture 3G transactions
2. Query SS7 `SendIdentification` to get decryption key

*Note*: For many networks no SS7 needed for 3G interception!

| Network | Encrypts | Authenticates calls / SMS | Protects integrity |
|---|---|---|---|
|  | ✗ | ✗ | ✔ |
|  | ✗ | ✗ | ✔ |
|  | ✗ | ✗ | ✔ |
|  | ✗ | ✗ | ✔ |
|  | ✗ | ✗ | ✔ |

Source: https://goo.gl/YBhvXw

# LTE Security

Cipher & USIM improvements

→ No known ways to break used crypto, recover key from SIM, break authentication, encryption, or integrity protection

**But…**

- Not everything is encrypted
  - E.g. null encryption supported → Data is simply (unencrypted) plaintext
- Several messages allowed without integrity protection
  - E.g. null integrity for emergency calls, broadcast system, cell handover

# Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations

$1,400 device can track users for days with little indication anything is amiss.

The attacks target the LTE specification, which is expected to have a user base of about 1.37 billion people by the end of the year, and require about $1,400 worth of hardware that run freely available open source software. The equipment can cause all LTE-compliant phones to leak their location to within a 32- to 64-foot (about 10 to 20 meter) radius and in some cases their GPS coordinates,

Source: http://goo.gl/jID7jQ

## What?

Exploiting LTE *specification* flaws

## Problems?

- RRC Protocol
  - Measurement reports for handover
  - → Not authenticated, not encrypted
- EMM Protocol
  - Control device mobility
  - → Not integrity protected

## Attacker can

- Track user location / movements
- Downgrade to non-LTE

ISEC TU Graz

# LimeSDR: Flexible, Next-generation, Open Source Software Defined Radio

Open Hardware
Technology

Home | Updates 40 | Backers | History

Source: https://goo.gl/SD2ouo


$773,527 raised
of $500,000 goal

**Funded!** **Order Now**

| Jun 21 | 154% | 3,175 |
|---|---|---|
| funded on | funded | pledges |

**LimeSDR** $289

The LimeSDR is based on Lime Microsystem's latest generation of field programmable RF transceiver technology, combined with FPGA and microcontroller chipsets. These connect to a computer via USB3. LimeSDR then delivers the wireless data and the CPU provides the computing power required to process the incoming signals, and to generate the data to be transmitted by the LimeSDR to all other devices.

## Use with popular open source LTE projects

- OpenLTE See: https://goo.gl/GEUeHV
- Open Air Interface See: https://goo.gl/qSNrxk

# Other Attack Vectors

- Branded mobile equipment
  - 3G/4G USB modems
  - Routers / Access points See: http://goo.gl/kIAJpe
  - Smartphones, femtocell, branded apps


- (U)SIM cards
  - Cracking SIM update keys, deploy SIM malware See: https://goo.gl/WYxUTq

- Radio / IP access network
  - Radio access network
  - IP access (GGSN, Routers, GRX) See: http://goo.gl/c3CNZ0

# Protection Mechanisms

# Measures in Austria

- Numbers from 2014 (no LTE!)
- All 3G networks use A5/3 with encryption enabled
- Unclear if networks would accept unencrypted transactions as well (subscriber-initiated)
- Call/SMS impersonation possible in all 2G networks

| Attack vector | | Networks | | |
|---|---|---|---|---|
| | | A1 | T-Mobile | Three |
| 2G Over-the-air protection | | | | |
| - Encryption algorithm | A5/0 | 1% | 0% | 0% |
| | A5/1 | 8% | 31% | 35% |
| | A5/3 | **91%** | **69%** | **65%** |
| - Require IMEI in CMC | | ○ | ◑ | ◕ |
| - Hopping entropy | | ◔ | ◑ | ◔ |
| - Authenticate calls (MO) | | ◔ 21% | ◔ 23% | ◔ 14% |
| - Authenticate SMS (MO) | | ○ 9% | ◕ 67% | ◔ 10% |
| - Authenticate paging (MT) | | ◔ 11% | ◔ 16% | ◔ 16% |
| - Authenticate LURs | | ◑ 40% | ◑ 44% | ◕ 61% |
| - Encrypt LURs | | ● 100% | ● 100% | ● 100% |
| - Update TMSI | | ◔ 32% | ◕ 81% | ◑ 44% |
| 3G Over-the-air protection | | | | |
| - Encryption | | ● | ● | ● |
| - Update TMSI | | ○ 1% | ◕ 61% | ○ 1% |
| HLR/VLR configuration | | | | |
| - Mask MSC | | ● | ● | ● |
| - Mask IMSI | | ○ | ○ | ● |

Source: https://goo.gl/fCqBZW

# Abuse often detectable!

| | Attack scenario | Detection heuristic |
|---|---|---|
|  SMS Attacks | ▪ **SIM OTA attacks** | ▪ Unsolicited binary SMS |
| | ▪ Semi-lawful **Tracking** through silent SMS | ▪ Silent SMS |
| SS7 Attacks | ▪ SS7 abuse: **Tracking, Intercept**, etc. | ▪ Empty paging |
|  IMSI Catcher | ▪ **Tracking** or **Intercept** through 2G or 3G fake base station | ▪ Unusual cell configuration and cell behavior (detailed later in this chapter) |
|  Network Security | ▪ Insufficient encryption leads to **Intercept** and **Impersonation** | ▪ Encryption level and key change frequency |
| | ▪ Lack of TMSI updates enables **Tracking** | ▪ TMSI update frequency |

Source: https://goo.gl/jFtXYu

# SnoopSnitch

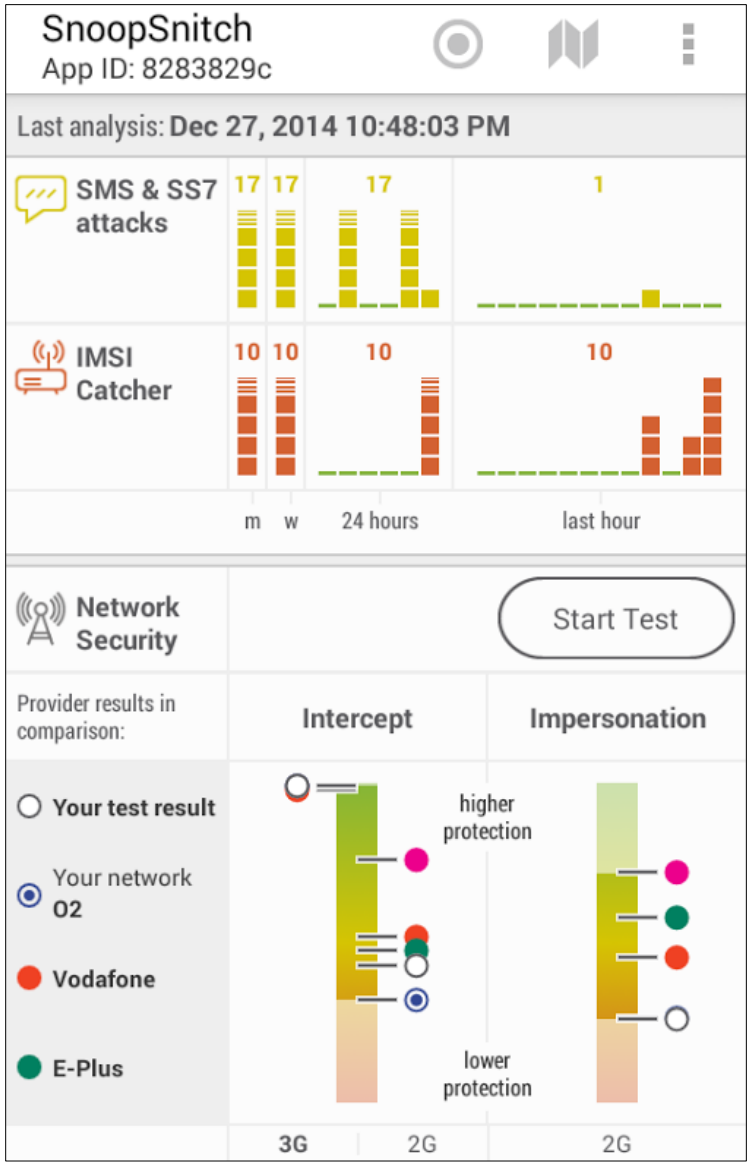
Collect network traces on Android → analyze for abuse

## Features

- Detection of fake base station (IMSI catcher)
  - Suspicious cell configuration / behaviour
- User tracking
- SS7 attacks

## Requirements

- Rooted phone with Android >= 4.1
- Qualcomm chipset
  - Samsung Galaxy S4/S5, Sony Z1, OnePlus 2, …




Source: https://goo.gl/KlhaZa

ISEC TU Graz

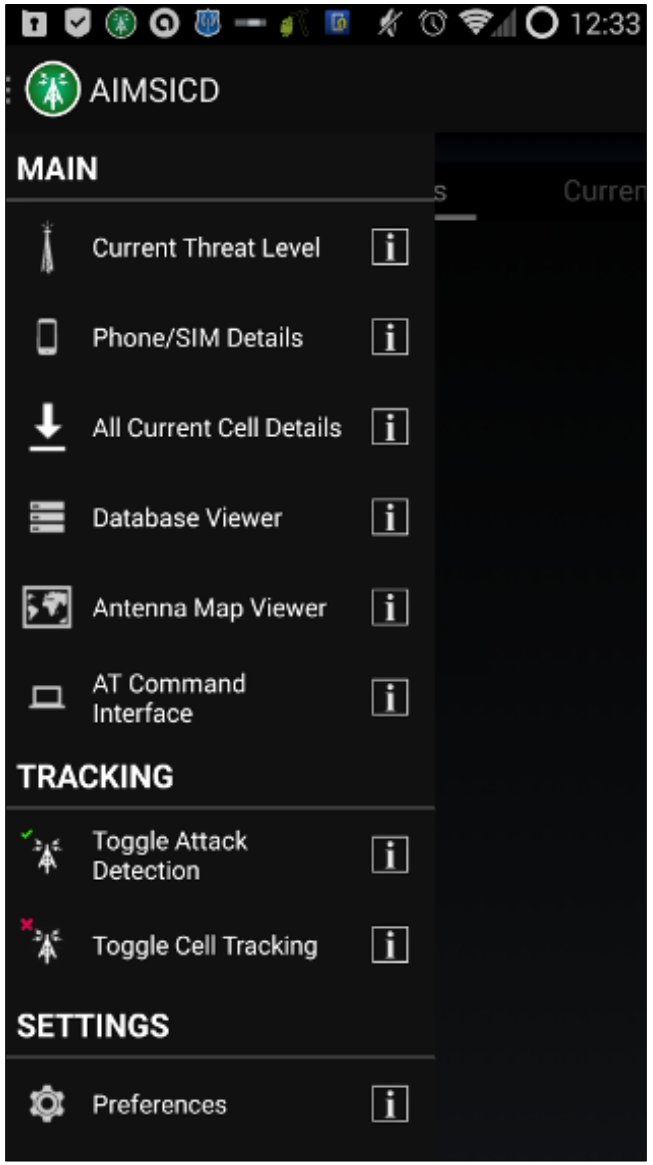
# AIMSICD

## Features

- Focus: Detecting IMSI catchers
- Check consistency of
  - Tower information
  - LAC / Cell ID
  - Signal strength
- Detect silent SMS (type 0 messages)
- Detect FemtoCells

## Requirements

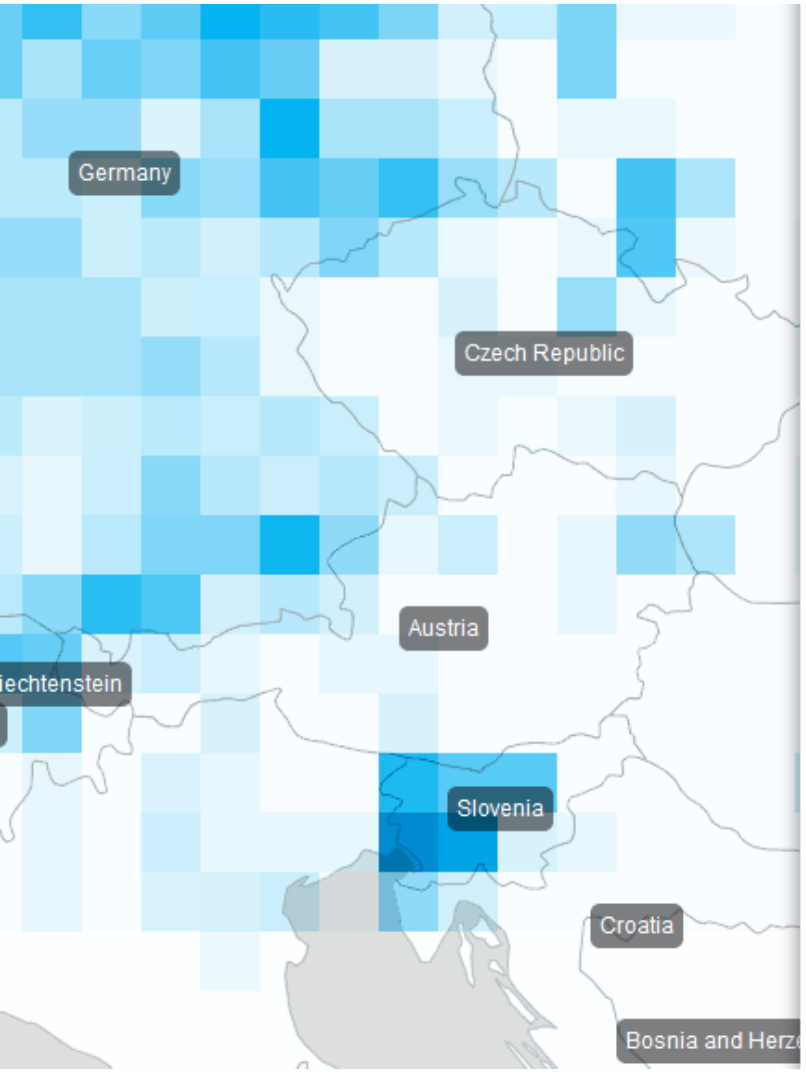
- Rooted Android
- Ability to send AT commands to modem

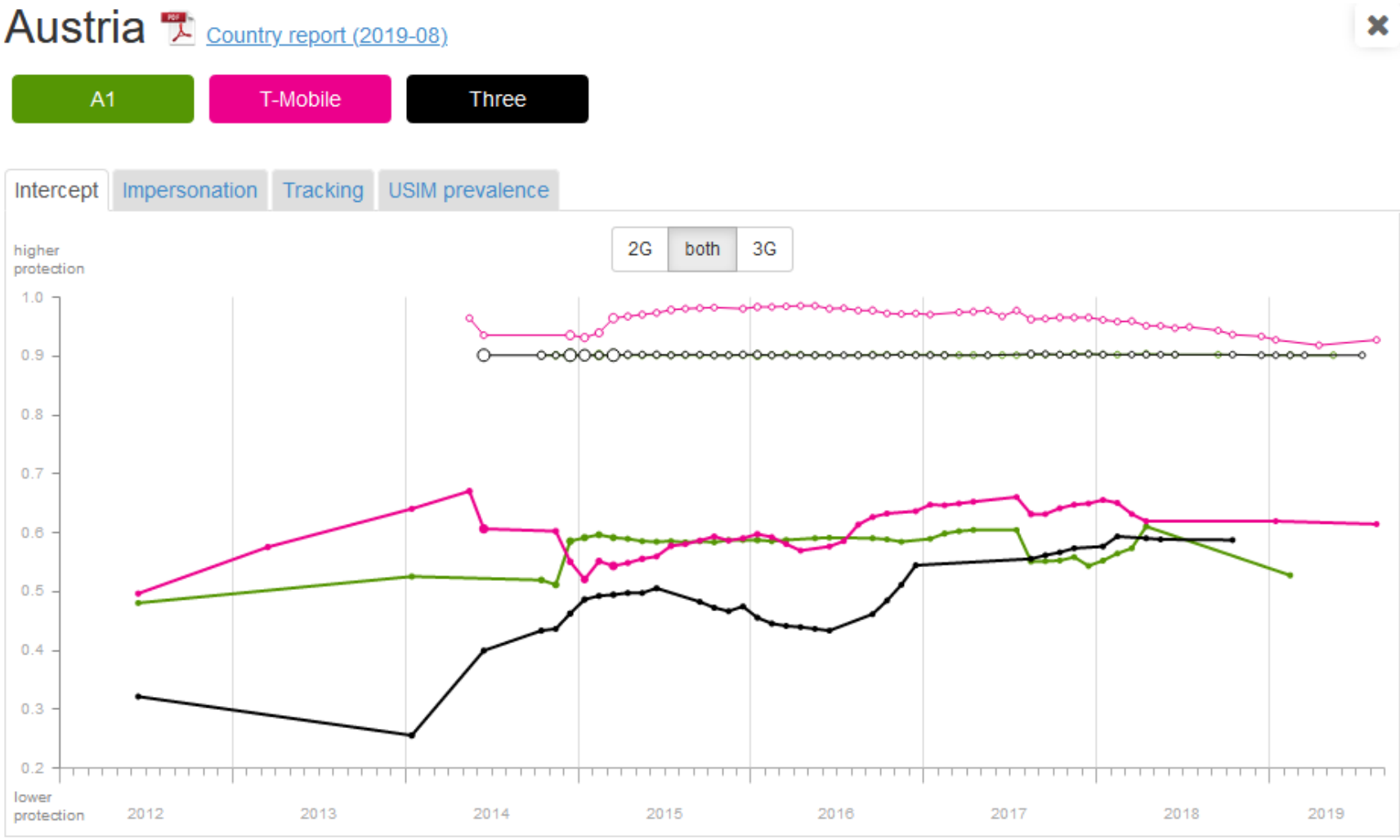



Source: https://goo.gl/mbZFgE

ISEC TU Graz

# Network Protection Status




Source: http://gsmmap.org

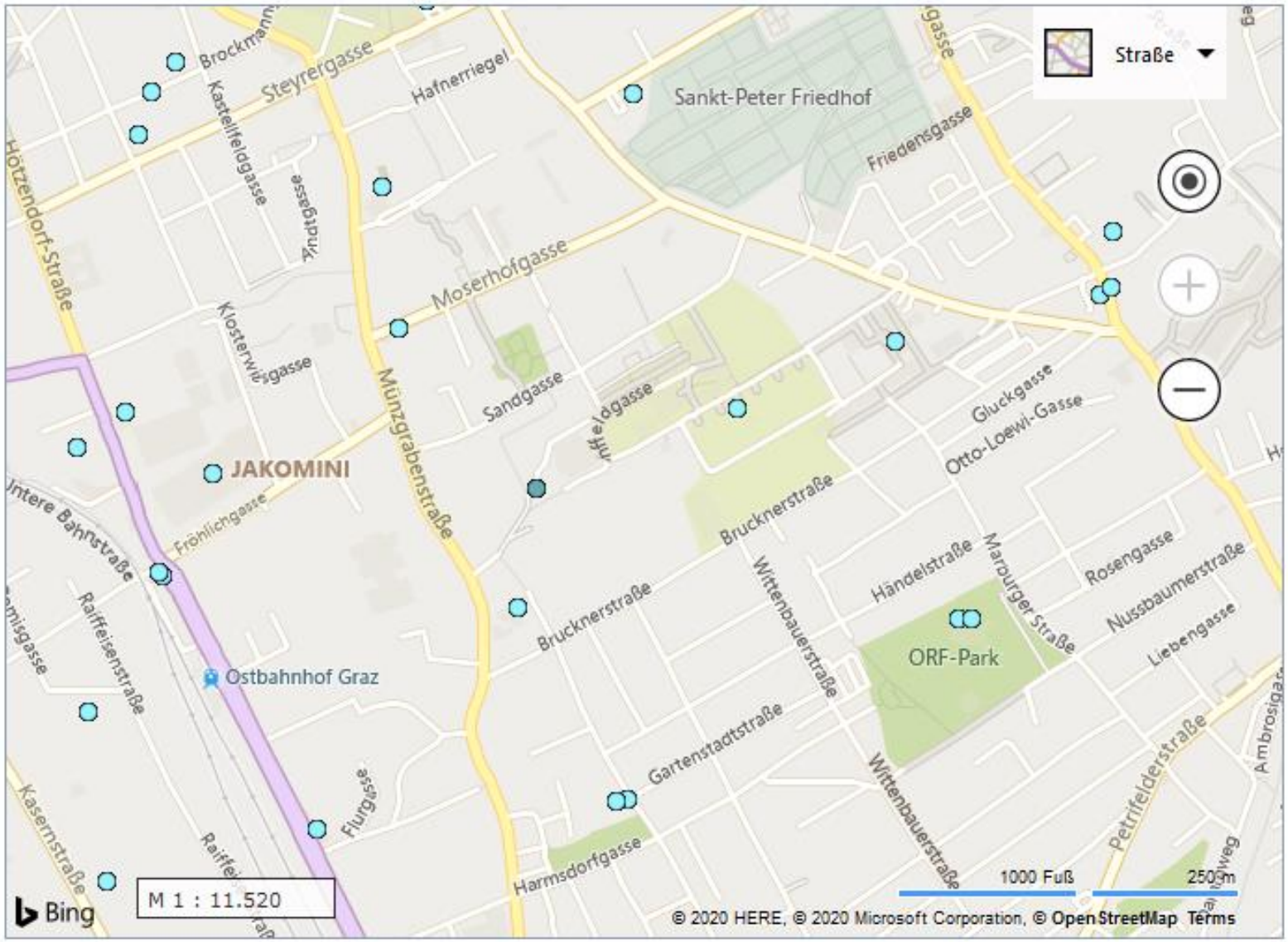
ISEC TU Graz

# Physical Cell Locations

**Tipp:** Um Standorte in Ihrer Umgebung zu finden geben Sie im Feld "Adresse, Ort oder PLZ" die Postleitzahl bzw. den Namen der gesuchten Gemeinde ein und klicken Sie an- schließend auf die Taste "Suchen".

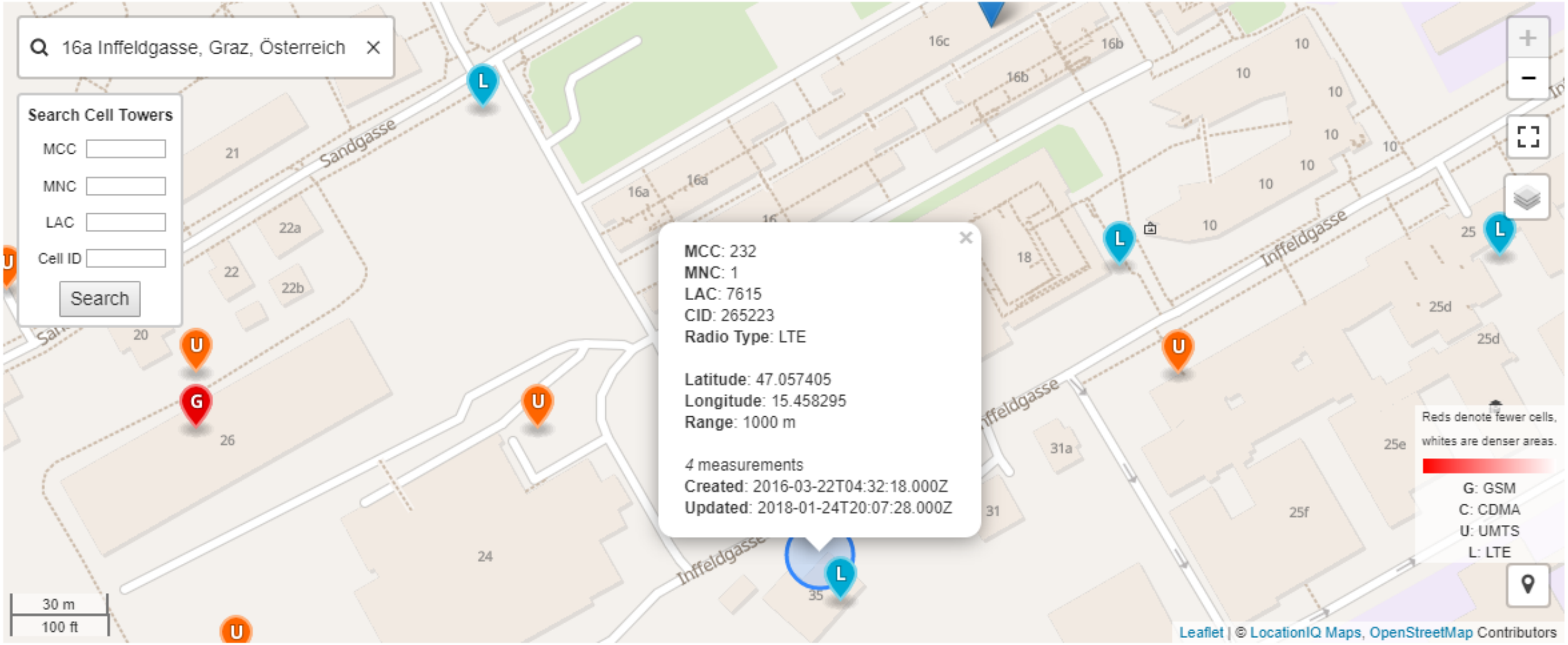
| Allgemeine Daten | |
|---|---|
| Standortanfrage versenden | |
| Funkdienst | Mobilfunk |
| Trägerstruktur | Mast |
| Gemeinsame Nutzung (Sharing) | Nein |
| **Station1** | |
| Protokoll(e) | GSM, UMTS, LTE, 5G |
| Sendeleistung | 380-400 W |

Mehr Informationen finden Sie im Kapitel **Erläuterungen** und **Technik**




Source: https://www.senderkataster.at

# Physical Cell Locations




Source: https://opencellid.org

# Outlook

- 13.06.2025
  - Assignment 2 Presentations (Part 1)

- 20.06.2025
  - Assignment 2 Presentations (Part 2)
  - Mobile Security Research