# Busting Rogue Base Stations using CellGuard and the Apple Cell Location Database

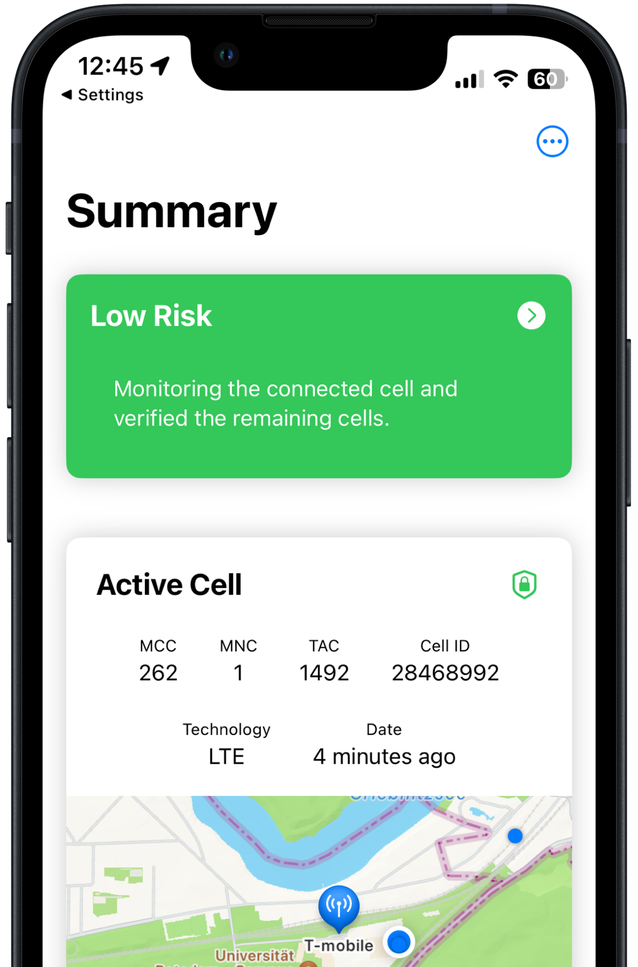
Lukas Arnold, Matthias Hollick, Jiska Classen

TECHNISCHE UNIVERSITÄT DARMSTADT

HPI Hasso Plattner Institut

Open6GHub

ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit




RAID 2024

# Cellular Security

## Attacker Goals

Personal Information &
Location Tracking

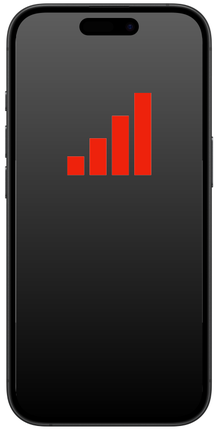
Traffic Interception &
Manipulation

Baseband Vulnerability
Exploitation

## Attacker Model

Adversaries can **block**, **intercept**, and **modify** over-the-air signals

Rouge Base Station



Genuine Base Station

# Cellular Security

## Attack Vectors

### 2G

Downgrade attacks

Missing mutual authentication

### 3G & 4G

Missing integrity protection

Identity information leakage

### 5G

Improves security

Targeted information leakge

### General

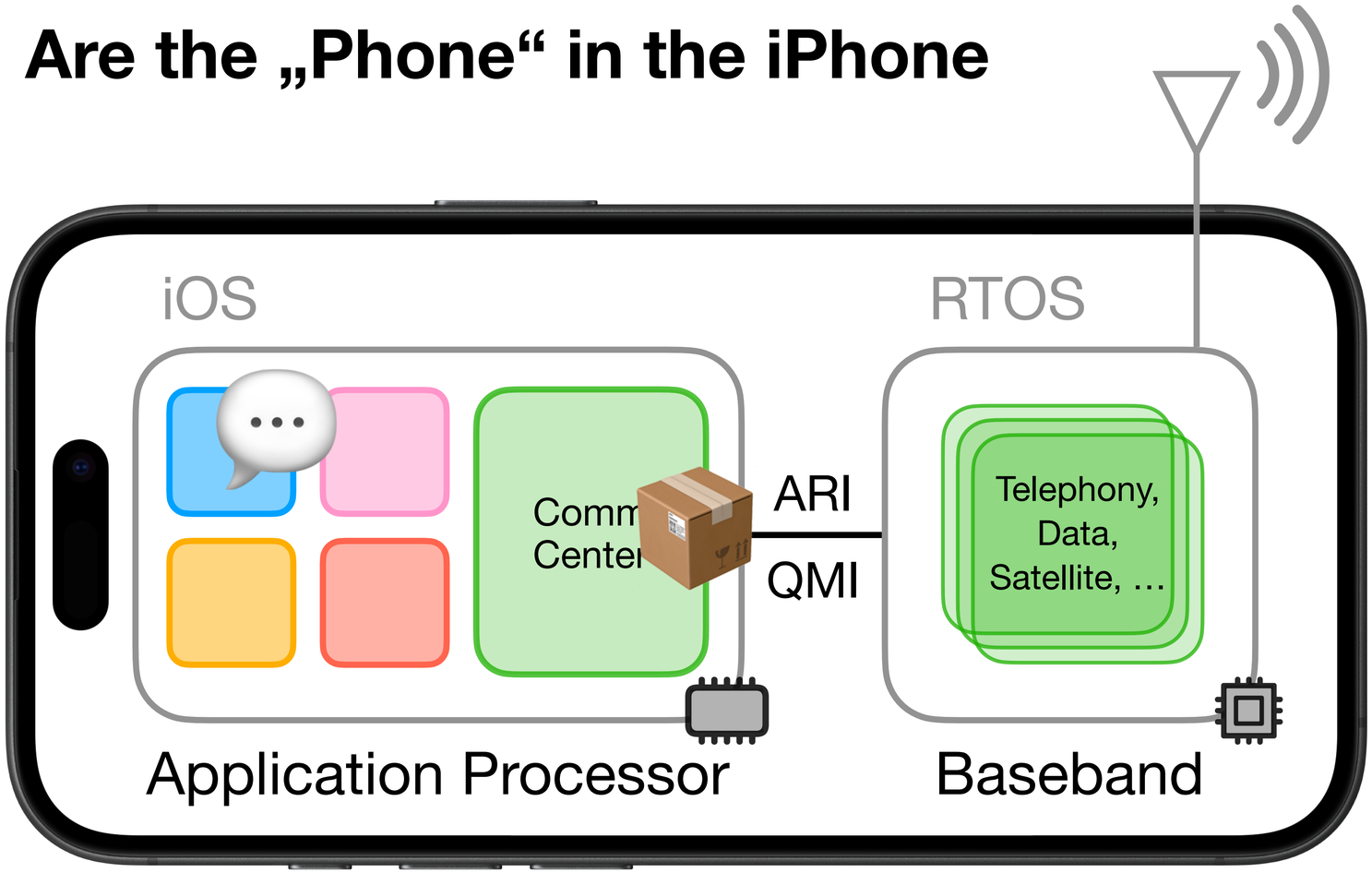
Roaming abuse

Baseband exploits

**Protect** yourself by disabling 2G

# iPhone Basebands

## Are the „Phone“ in the iPhone




Manufacturers

intel
Protocol
**Apple Remote Invocation**

Qualcomm
Protocol
**Qualcomm MSM Interface**

5
6
7
8
X
XR
XS
11
12
13
14
15
16

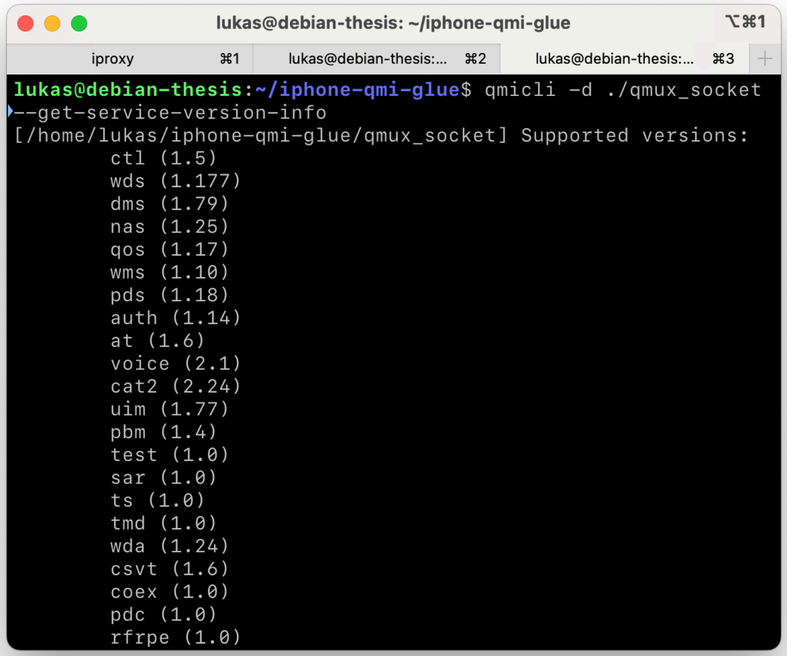
Basebands provide a **packet-based interface** for the OS

# BaseTrace

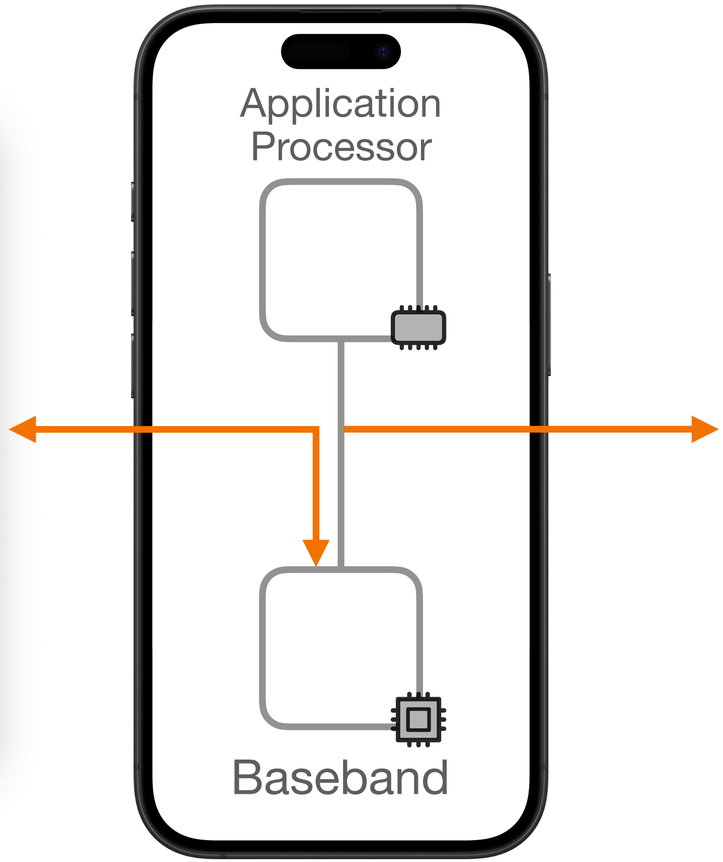
## iPhone Baseband Security Analysis Framework

libqmi

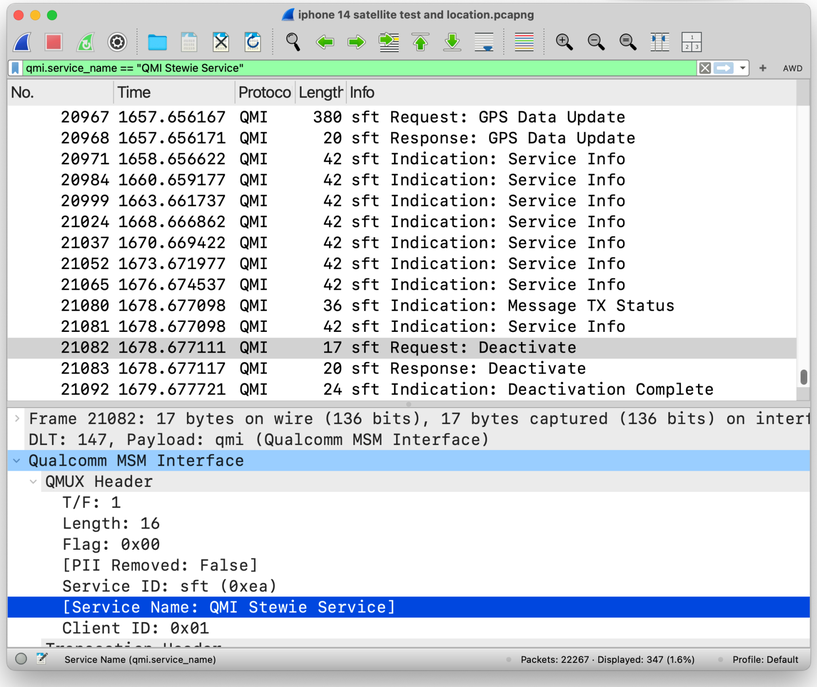
### Packet Injection




Requires Jailbroken iPhone



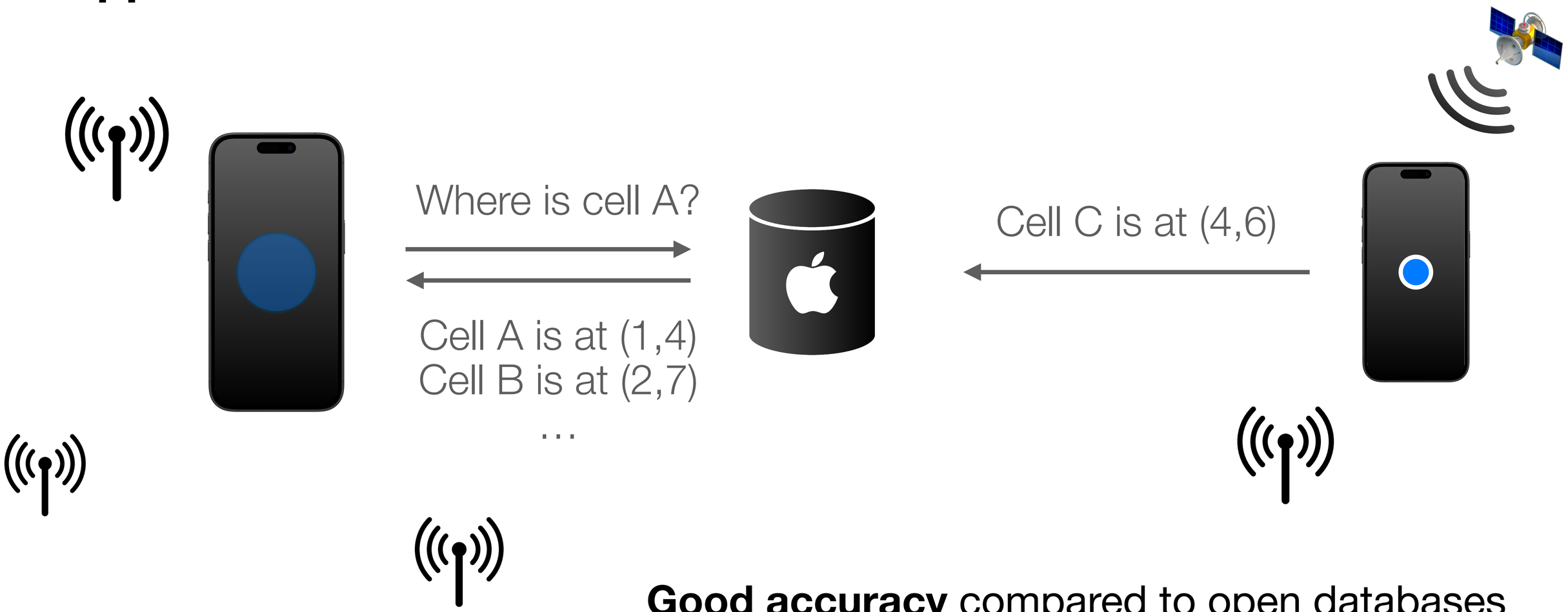

### Packet Dissection




Works with all iPhones

# Apple Location Services

## Is Apple's Closed-Source Location Database

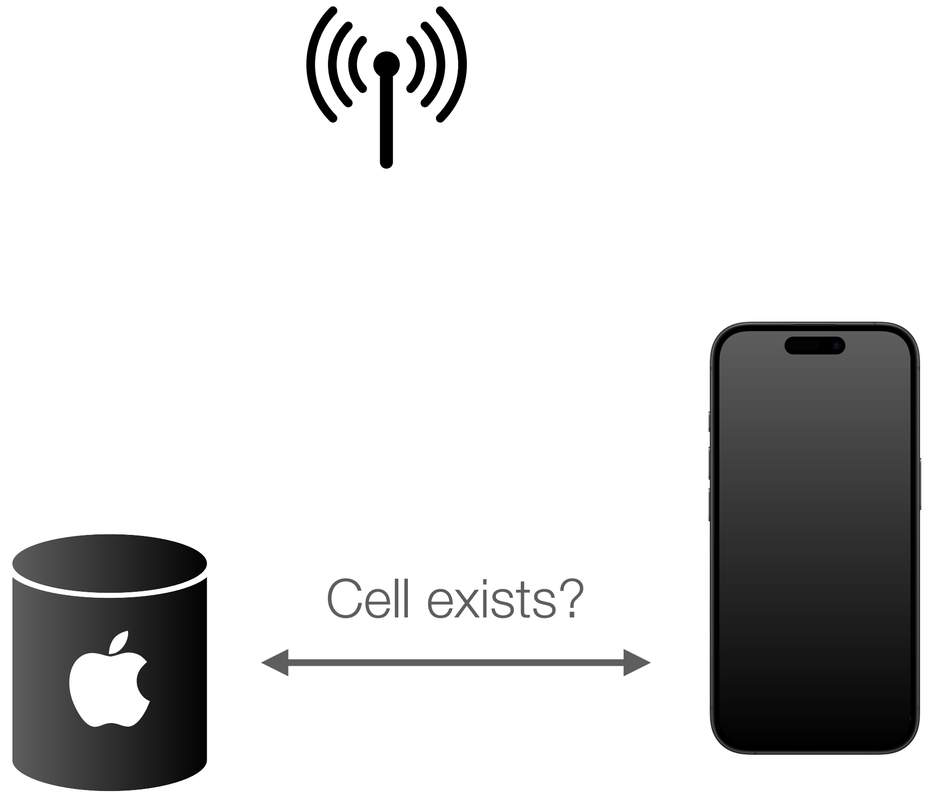



**Good accuracy** compared to open databases
OpenCelliD and Mozilla Location Services

# Rouge Base Station Detection

## With Apple Location Services (ALS)

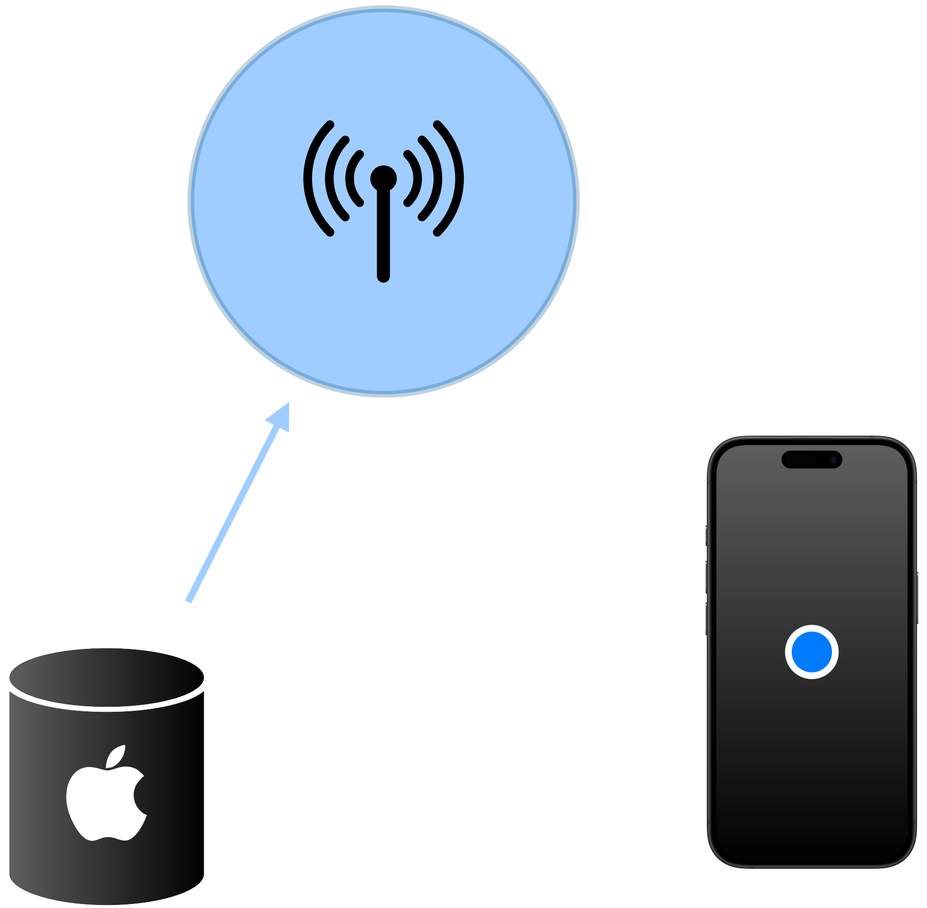
1. Confirm existance of cell with ALS (20P)



# Rouge Base Station Detection

## With Apple Location Services (ALS)

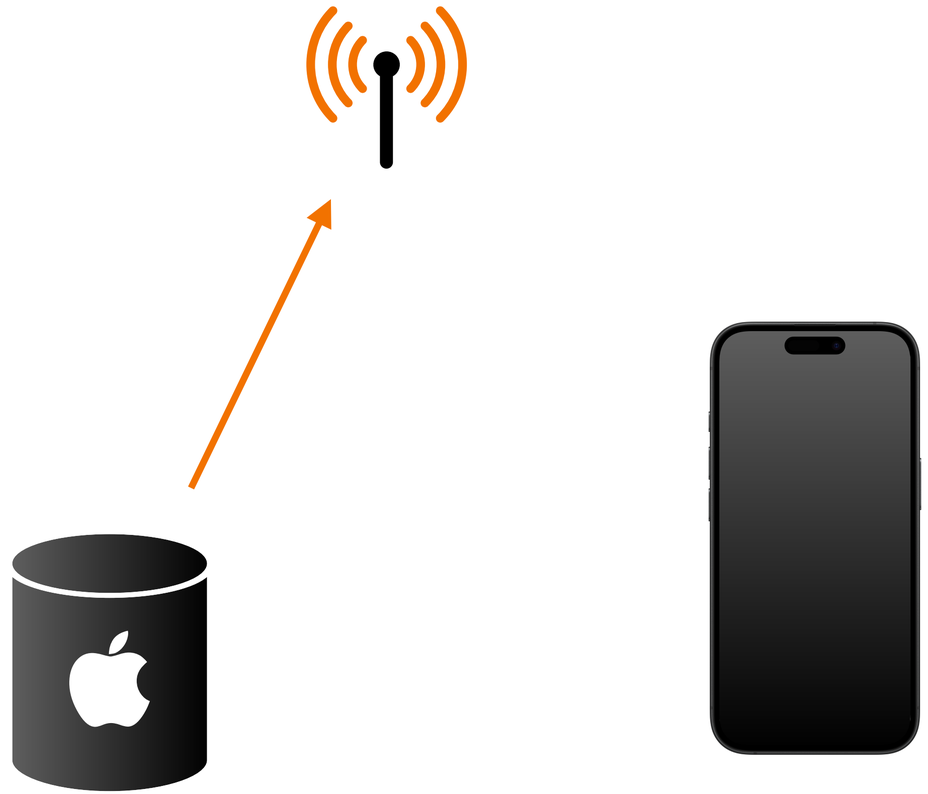
1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)



# Rouge Base Station Detection

## With Apple Location Services (ALS)

1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)



# Rouge Base Station Detection

## With Apple Location Services (ALS)

1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)
4. Low Bandwidth (2P)

# Rouge Base Station Detection

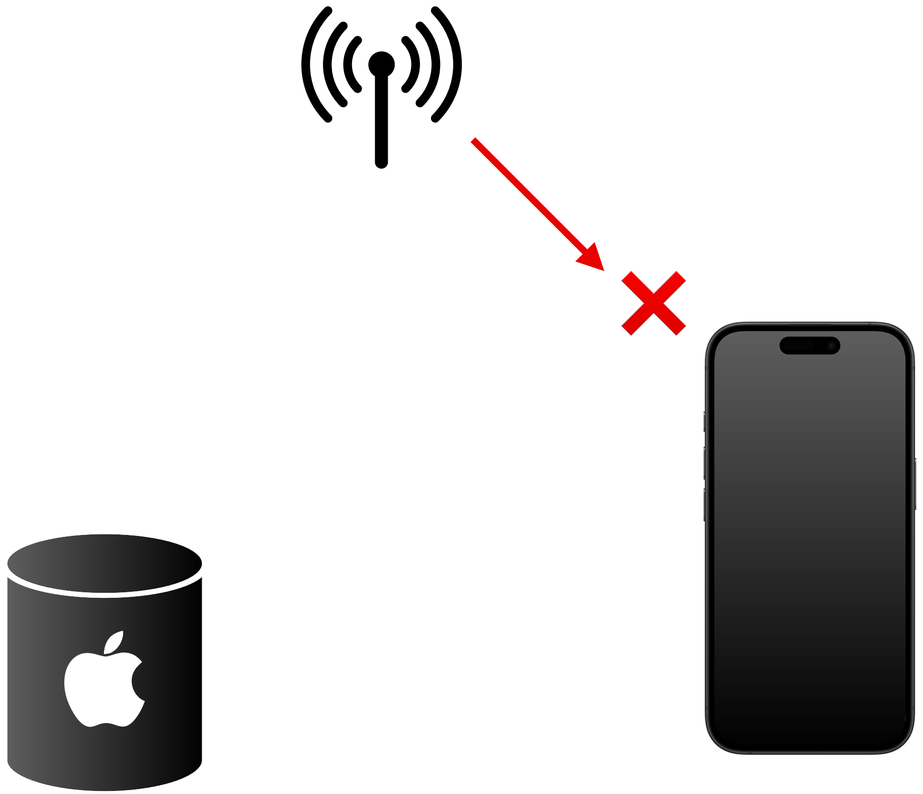
## With Apple Location Services (ALS)

1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)
4. Low Bandwidth (2P)
5. High Signal Strength (30P)

# Rouge Base Station Detection

## With Apple Location Services (ALS)

1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)
4. Low Bandwidth (2P)
5. High Signal Strength (30P)
6. Unexpected Network Reject (30P)



# Rouge Base Station Detection

## With Apple Location Services (ALS)

1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)
4. Low Bandwidth (2P)
5. High Signal Strength (30P)
6. Unexpected Network Reject (30P)

**Verdict**

Trusted (100P - 95P)

Anomalous (50P - 94P)

Suspicious (45P - 0P)

# CellGuard

## iOS App for RBS Detection

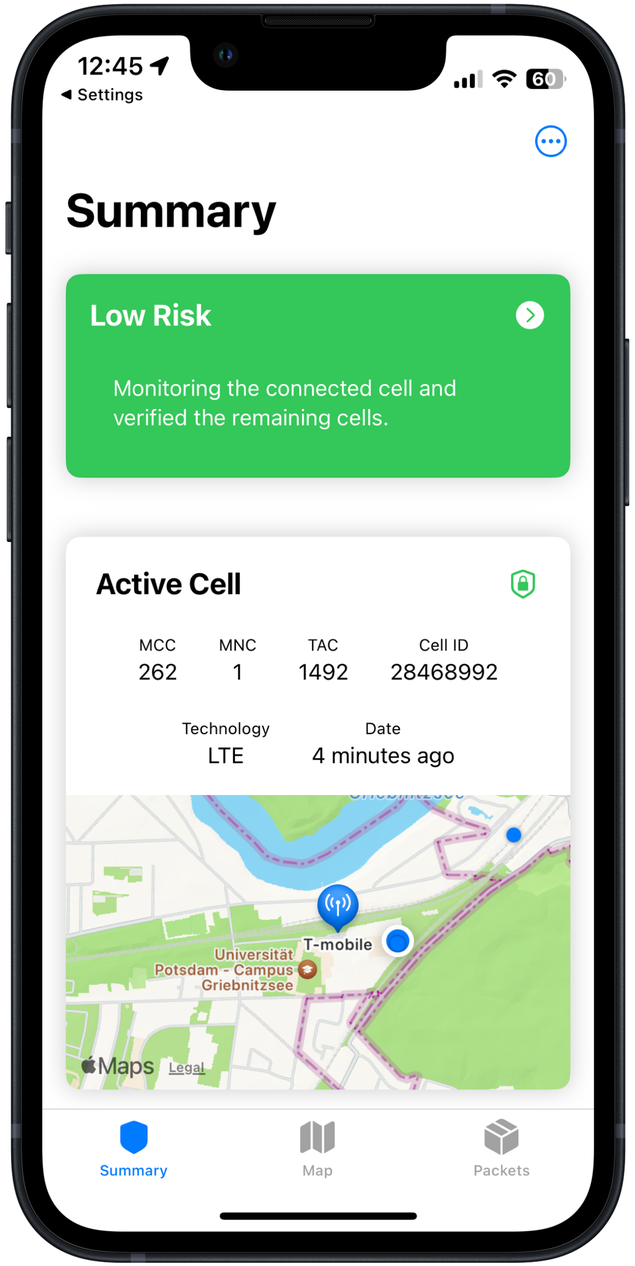
Supports iOS 14 - 18

### Standard iPhone

Install debug profile and import diagsnotics snapshot



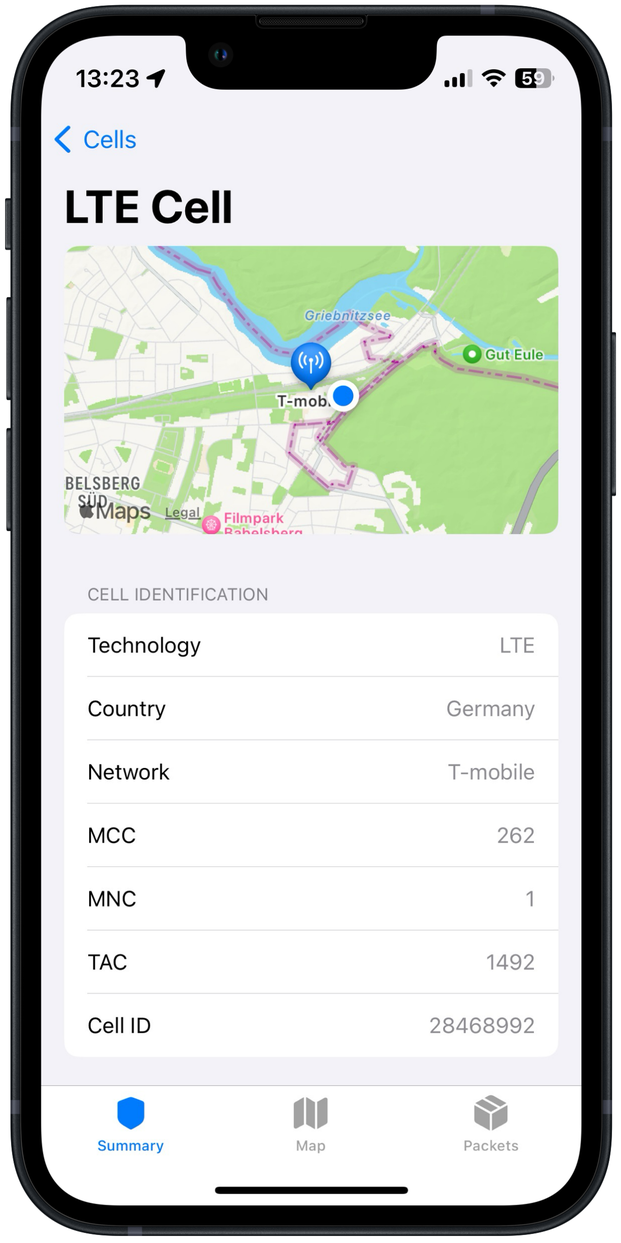
Use on primary device with Lockdown mode



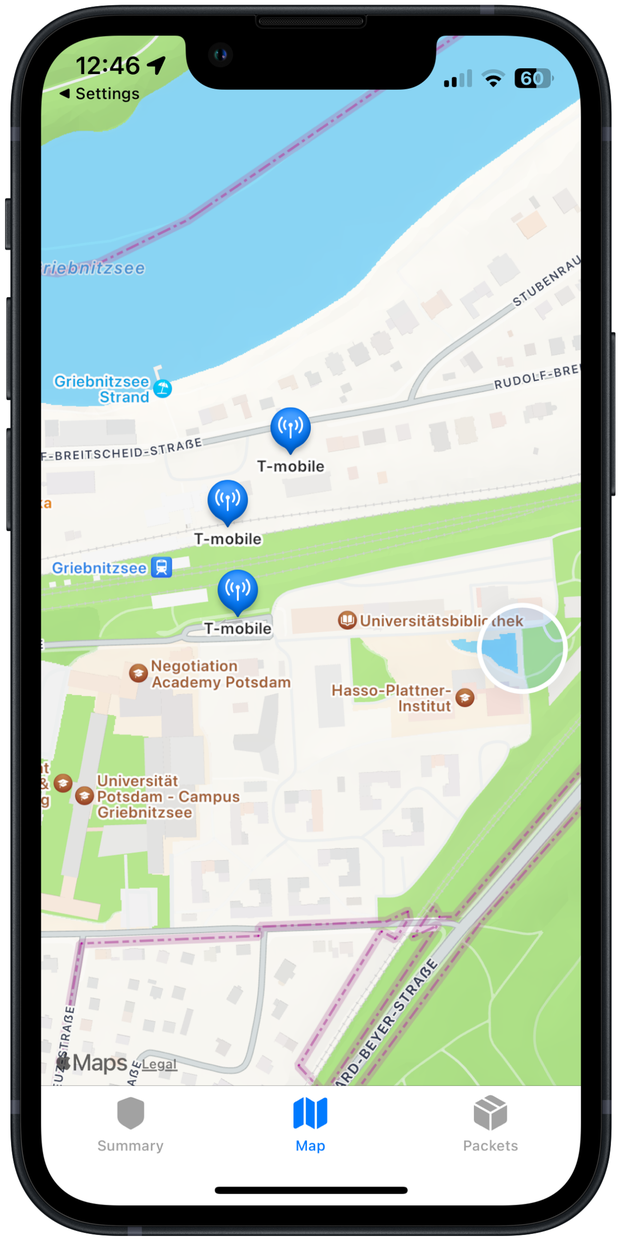

### Jailbroken iPhone

Install components for con-tinous background verification

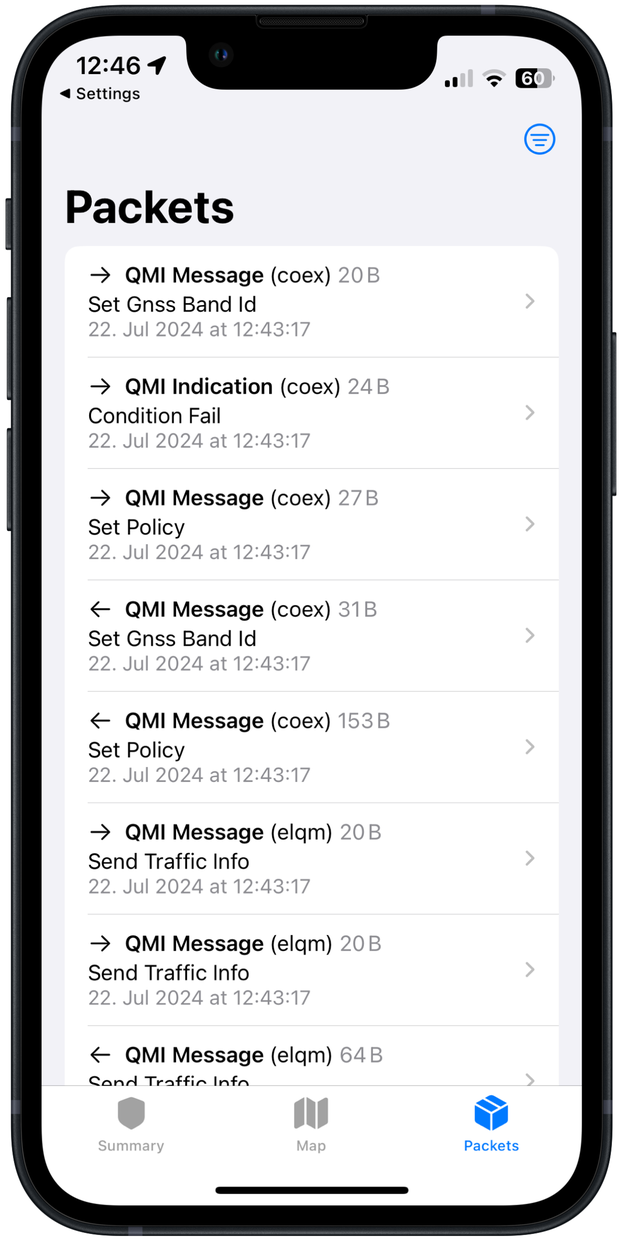
Use on secondary device functioning as sensor




Dive into Details




Explore Nearby Cells




Dissect Packets

# Evaluation of CellGuard

## In our lab and in the wild

Datasets from across Europe collected over multiple months

1.6% anomalous
0.0% suspicious

Excellent coverage of Apple Location Services

Detection of anomalous activity but confirmation difficult

Lab setup with evil twin rogue base stations

# CellGuard is Public

## Join the beta and contribute to our large-scale study

Continous development of CellGuard & tooling

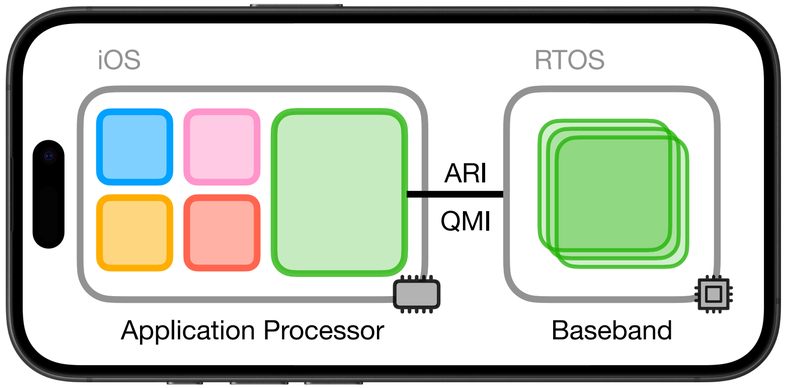
Download CellGuard at cellguard.seemoo.de

Open-source release next week

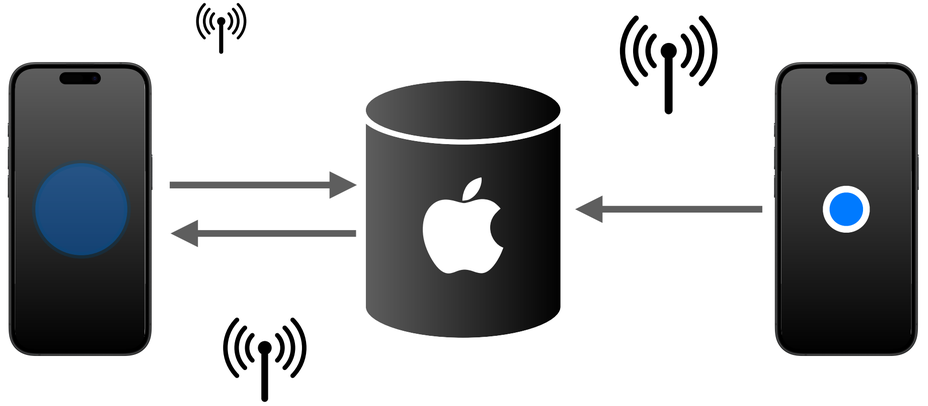
# Conclusion

## Busting Rogue Base Stations using CellGuard and ALS

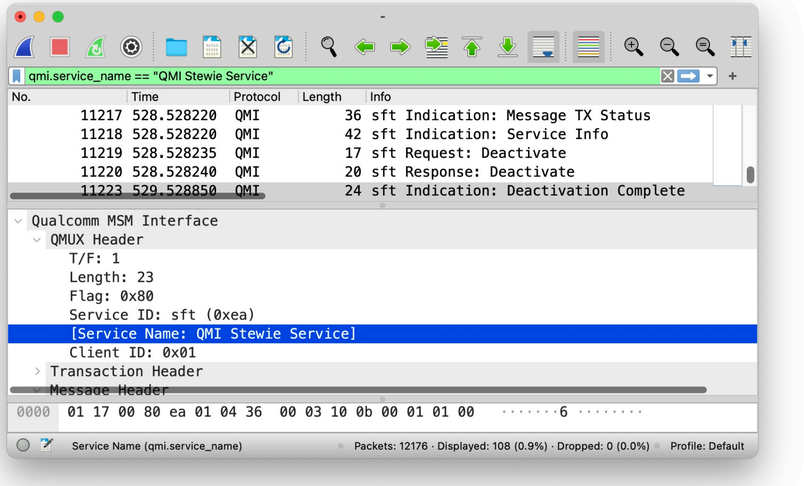
Reversing of iOS baseband architecture



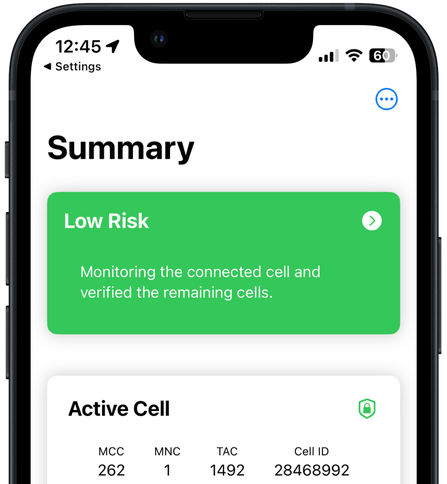

Evaluation of Apple Location Services



BaseTrace: Framework for baseband anaylsis




CellGuard with RBS detection algorithm



# Q&A

**Read our Paper**

**Download CellGuard**

larnold@seemoo.tu-darmstadt.de

@lukasarnld