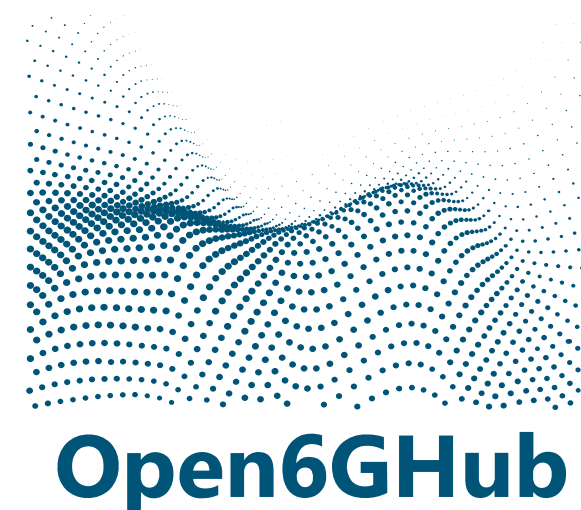
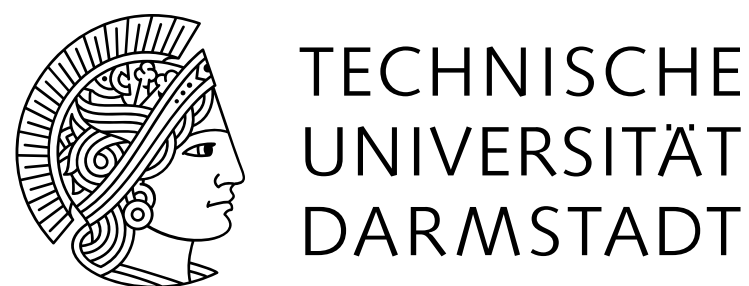
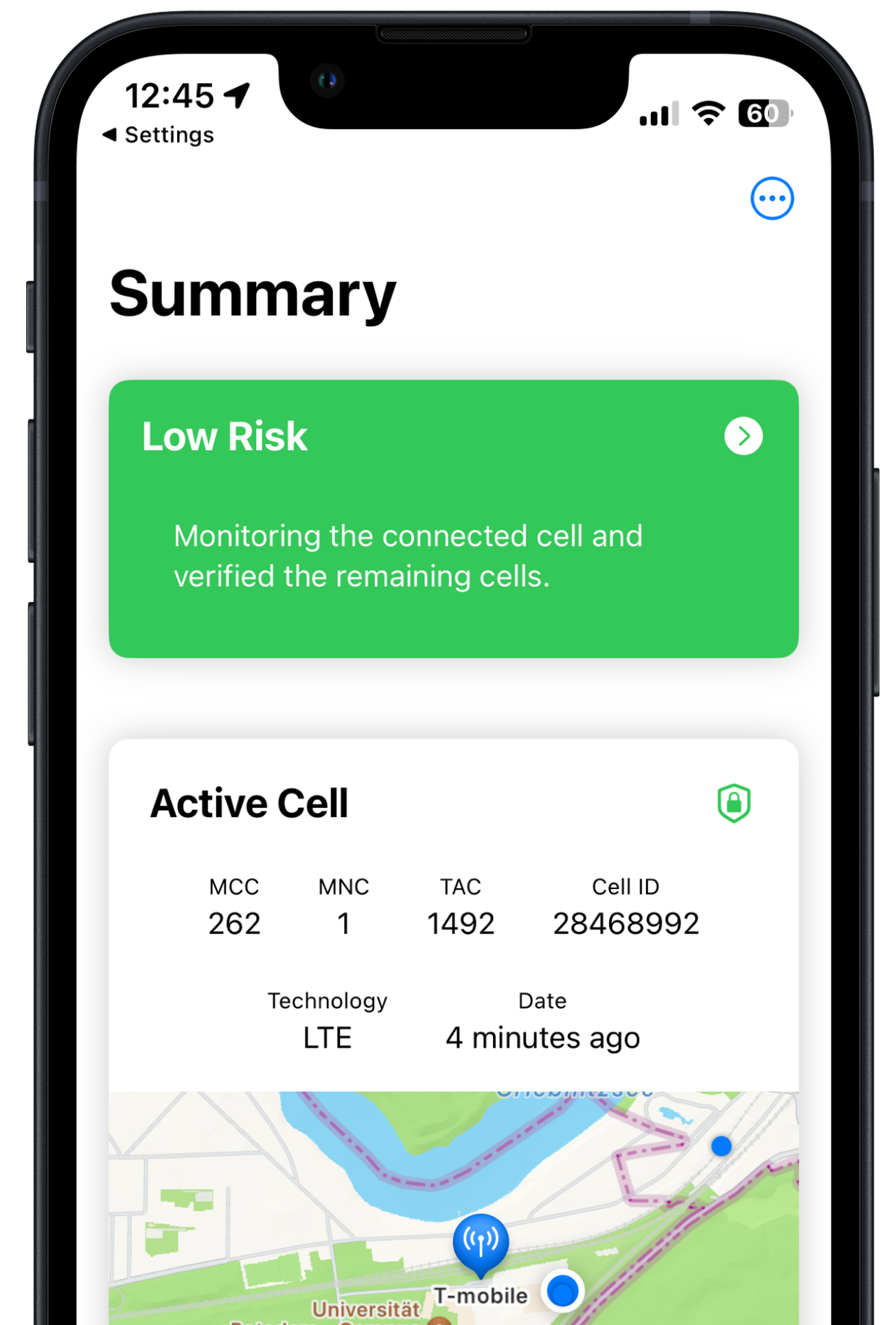


Busting Rogue Base Stations using CellGuard and the Apple Cell Location Database

Lukas Arnold, Matthias Hollick, Jiska Classen



RAID 2024



Cellular Security

Attacker Goals



Personal Information &
Location Tracking



Traffic Interception &
Manipulation



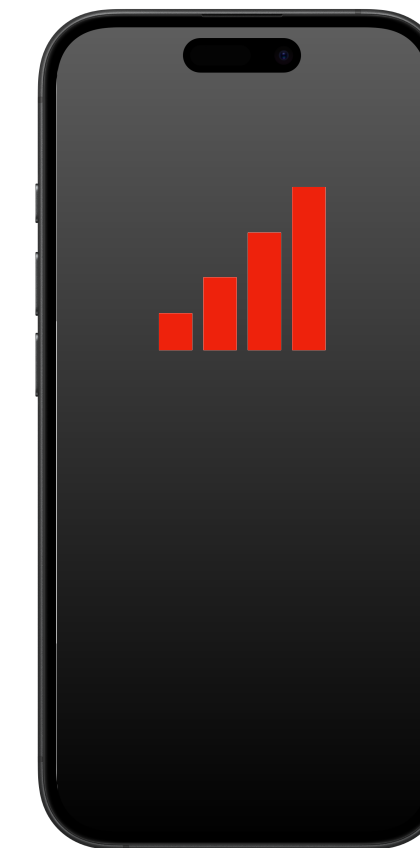
Baseband Vulnerability
Exploitation

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

5G

Improves security

Targeted information leakage

3G & 4G

Missing integrity protection

Identity information leakage

General

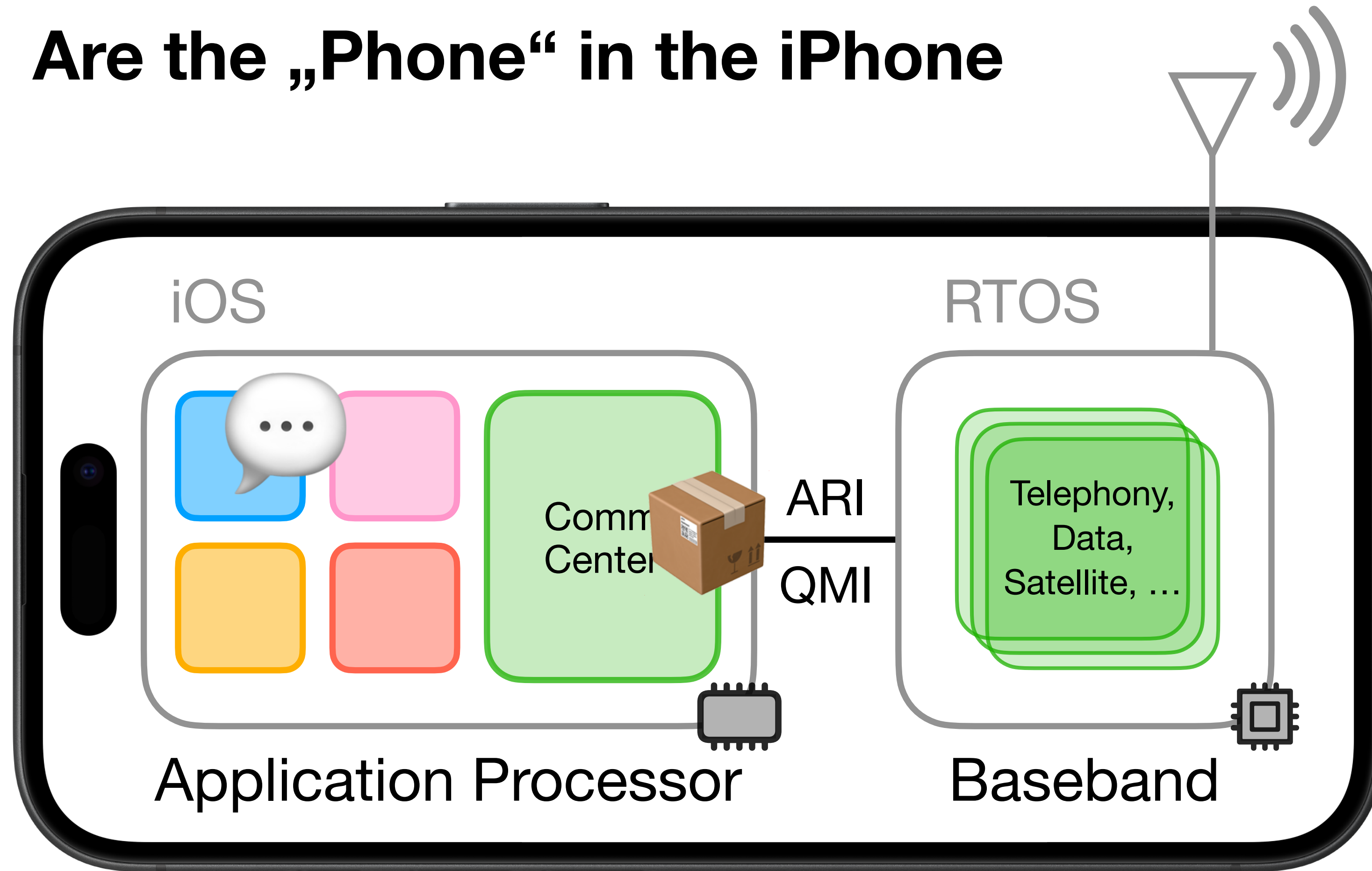
Roaming abuse

Baseband exploits

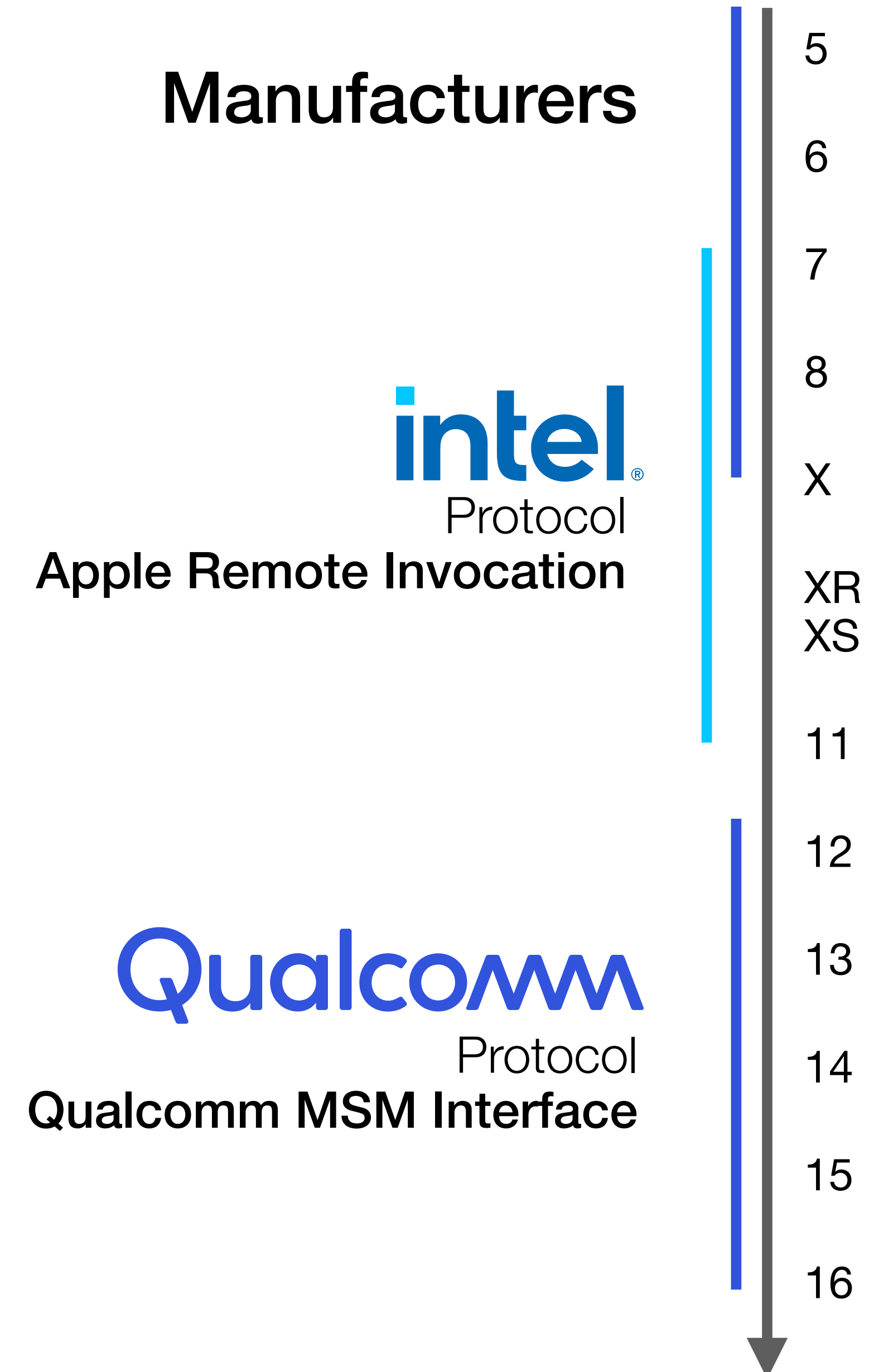
Protect yourself by disabling 2G

iPhone Basebands

Are the „Phone“ in the iPhone



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



BaseTrace

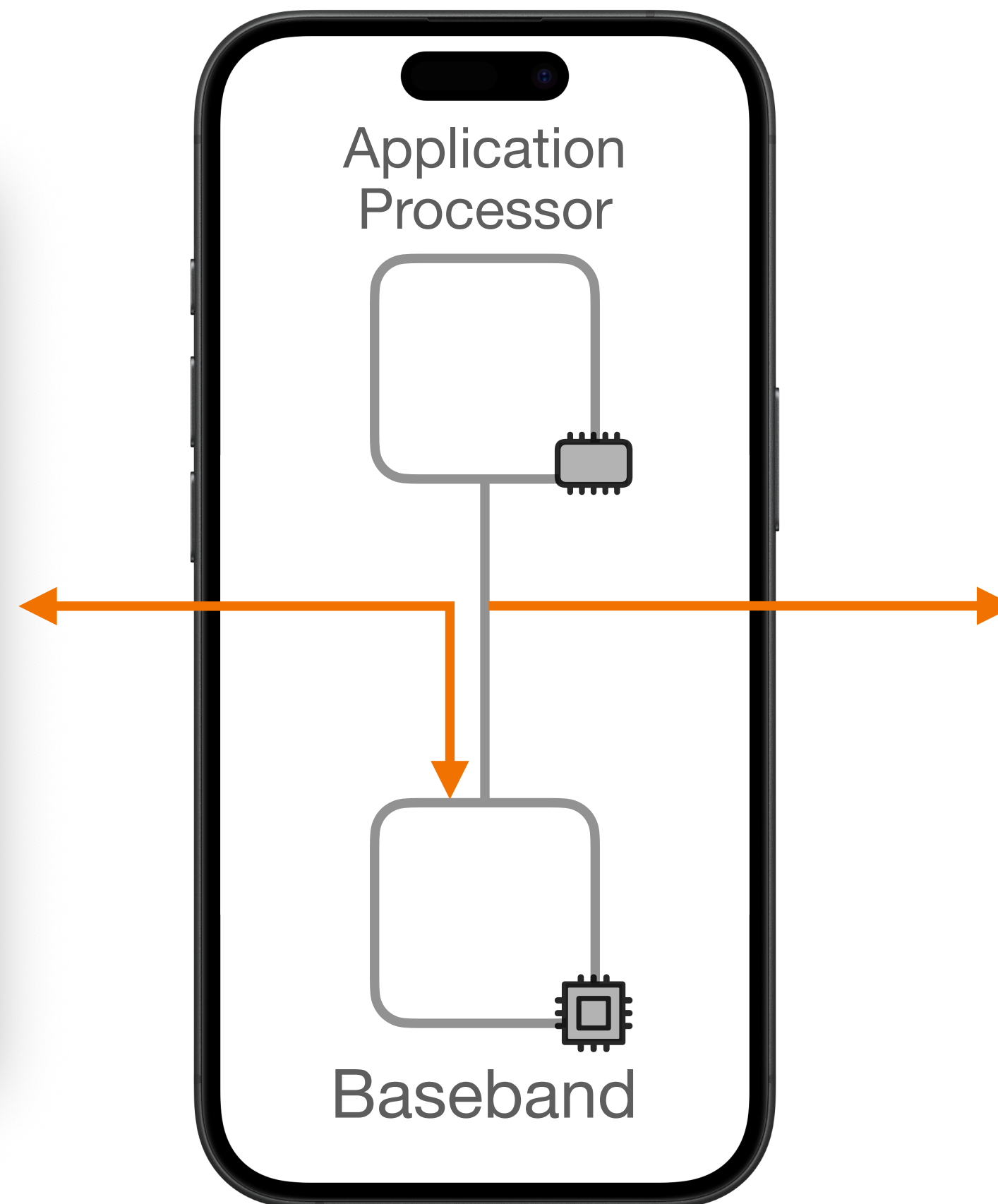
iPhone Baseband Security Analysis Framework



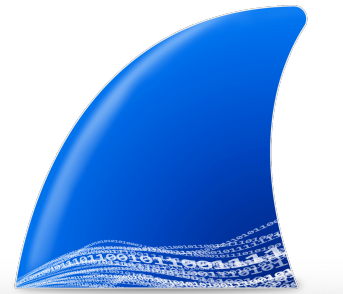
Packet Injection

```
lukas@debian-thesis: ~/iphone-qmi-glue
┌─── iproxy  ───  ┌─── lukas@debian-thesis:~  ───  ┌─── lukas@debian-thesis:~  ───
└───┘          └───┘                          └───┘
lukas@debian-thesis:~/iphone-qmi-glue$ qmicli -d ./qmux_socket
--get-service-version-info
[/home/lukas/iphone-qmi-glue/qmux_socket] Supported versions:
ctl (1.5)
wds (1.177)
dms (1.79)
nas (1.25)
qos (1.17)
wms (1.10)
pds (1.18)
auth (1.14)
at (1.6)
voice (2.1)
cat2 (2.24)
uim (1.77)
pbm (1.4)
test (1.0)
sar (1.0)
ts (1.0)
tmd (1.0)
wda (1.24)
csvt (1.6)
coex (1.0)
pdc (1.0)
rfrpe (1.0)
```

Requires Jailbroken iPhone



Packet Dissection



No.	Time	Protocol	Length	Info
20967	1657.656167	QMI	380	sft Request: GPS Data Update
20968	1657.656171	QMI	20	sft Response: GPS Data Update
20971	1658.656622	QMI	42	sft Indication: Service Info
20984	1660.659177	QMI	42	sft Indication: Service Info
20999	1663.661737	QMI	42	sft Indication: Service Info
21024	1668.666862	QMI	42	sft Indication: Service Info
21037	1670.669422	QMI	42	sft Indication: Service Info
21052	1673.671977	QMI	42	sft Indication: Service Info
21065	1676.674537	QMI	42	sft Indication: Service Info
21080	1678.677098	QMI	36	sft Indication: Message TX Status
21081	1678.677098	QMI	42	sft Indication: Service Info
21082	1678.677111	QMI	17	sft Request: Deactivate
21083	1678.677117	QMI	20	sft Response: Deactivate
21092	1679.677721	QMI	24	sft Indication: Deactivation Complete

Frame 21082: 17 bytes on wire (136 bits), 17 bytes captured (136 bits) on interface
DLT: 147, Payload: qmi (Qualcomm MSM Interface)

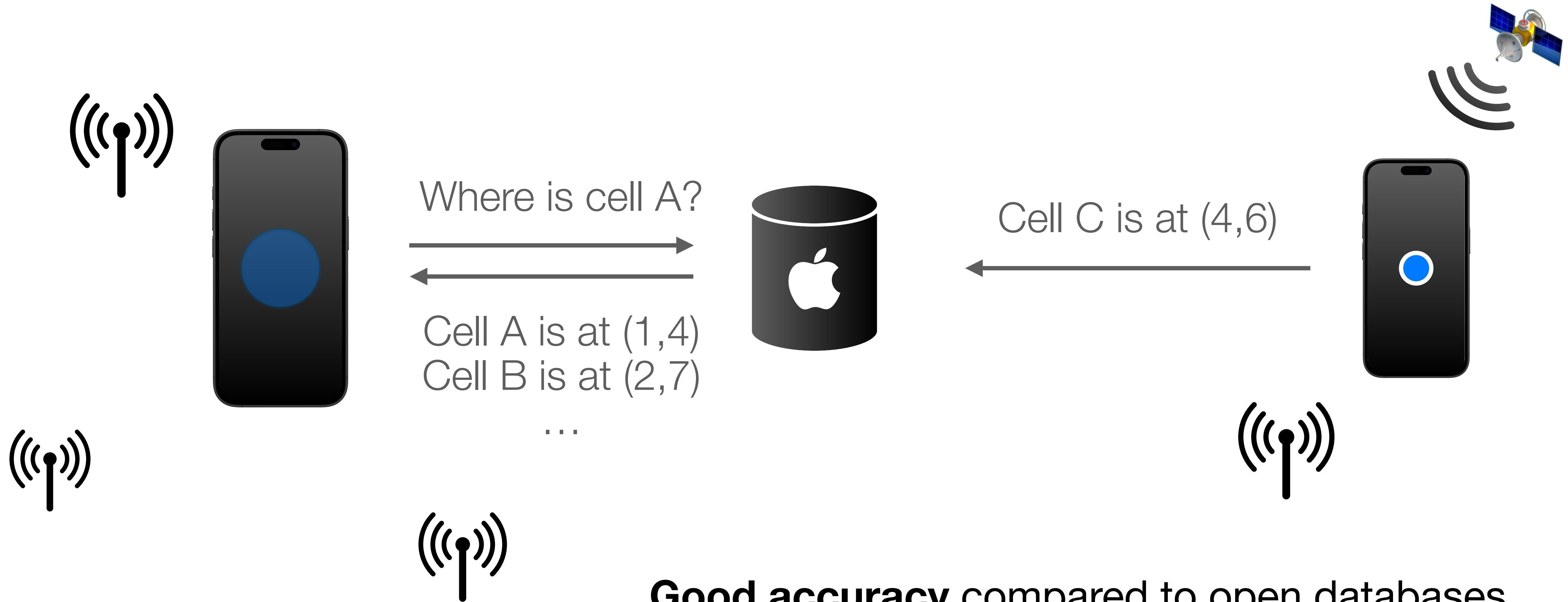
Qualcomm MSM Interface

- QMUX Header
 - T/F: 1
 - Length: 16
 - Flag: 0x00
 - [PII Removed: False]
 - Service ID: sft (0xea)
 - [Service Name: QMI Stewie Service]
 - Client ID: 0x01

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)



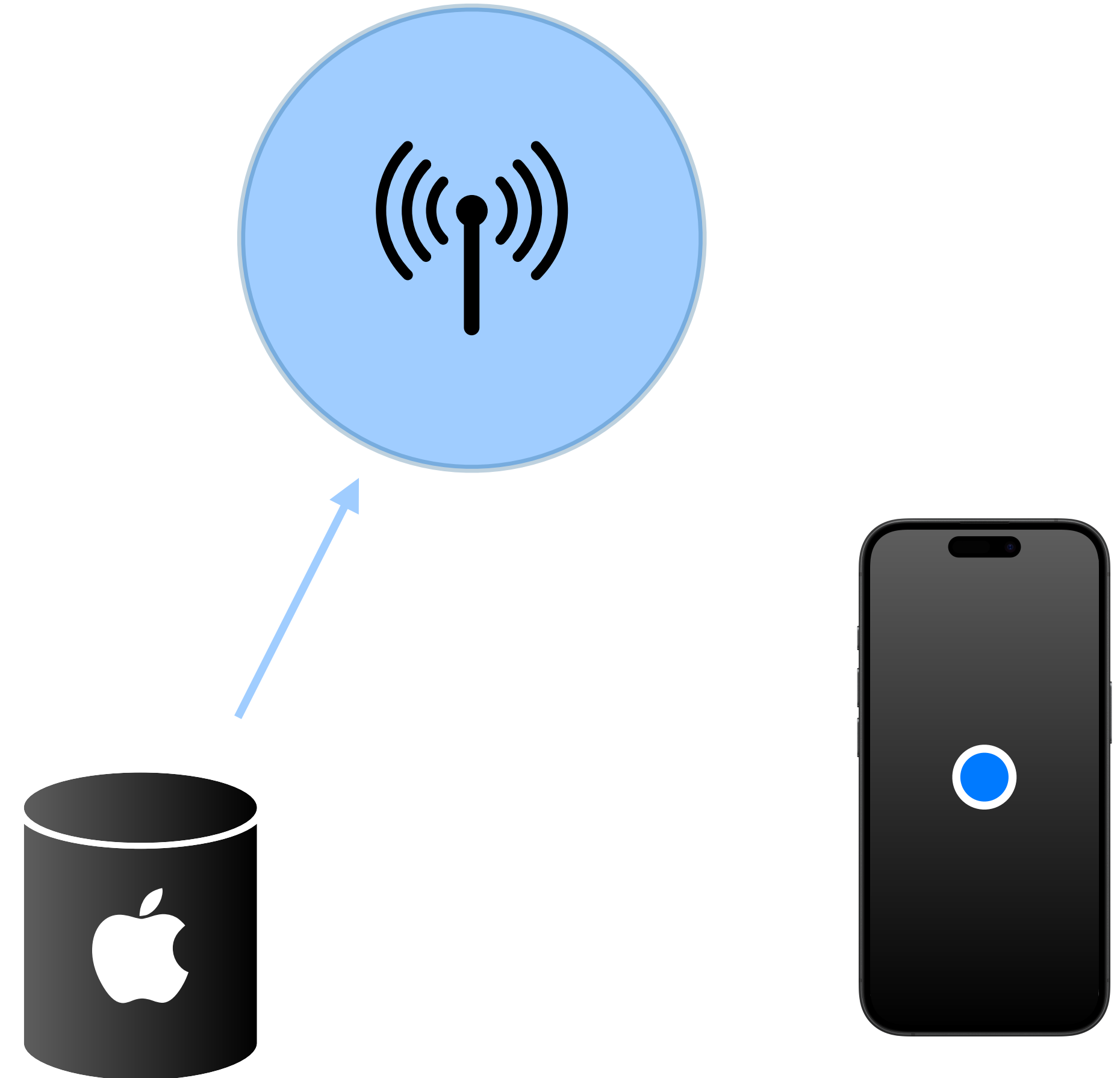
Cell exists?

A horizontal double-headed arrow pointing both left and right, positioned below the text "Cell exists?".

Rouge Base Station Detection

With Apple Location Services (ALS)

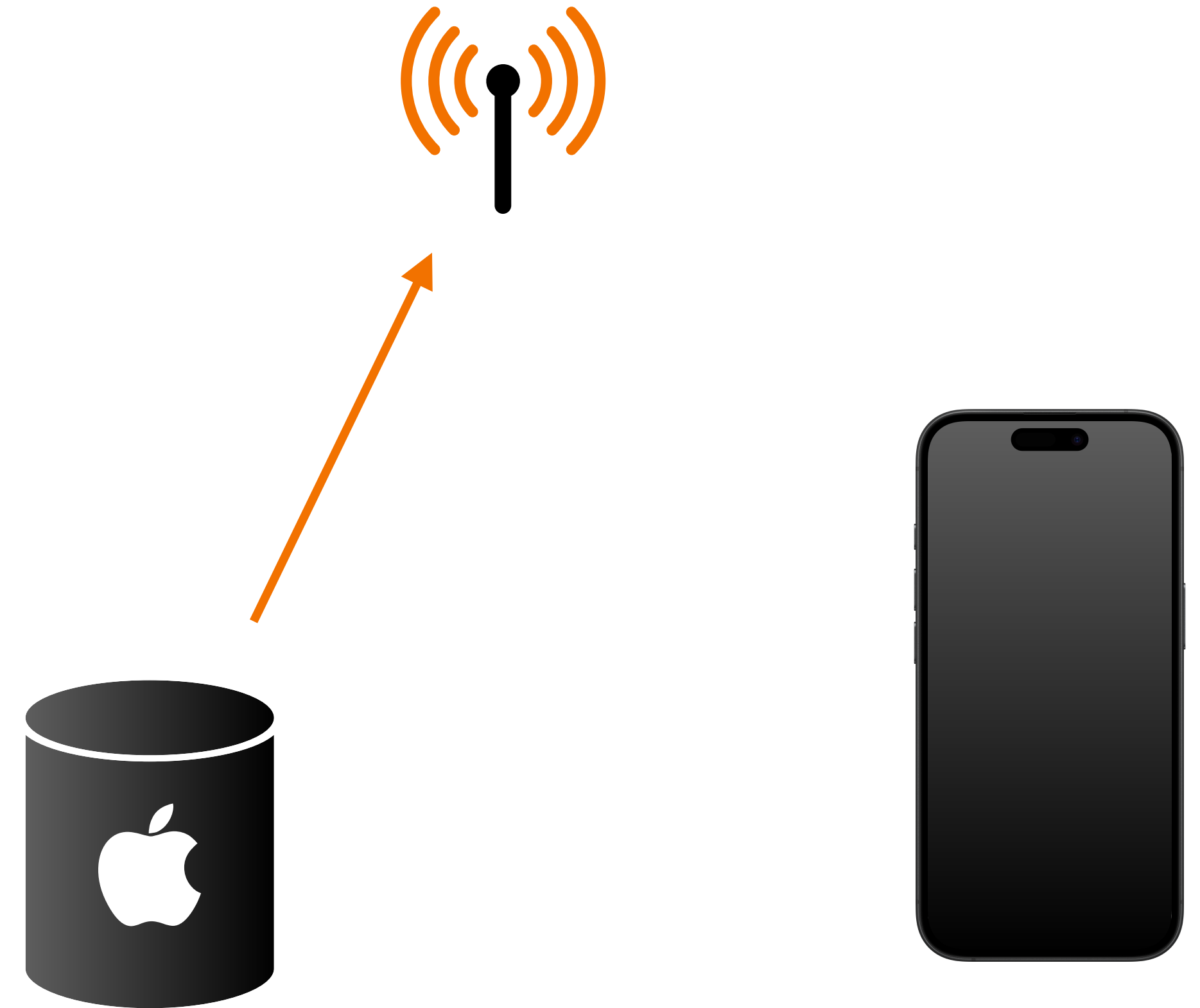
1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)



Rouge Base Station Detection

With Apple Location Services (ALS)

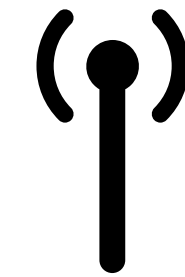
1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)



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)

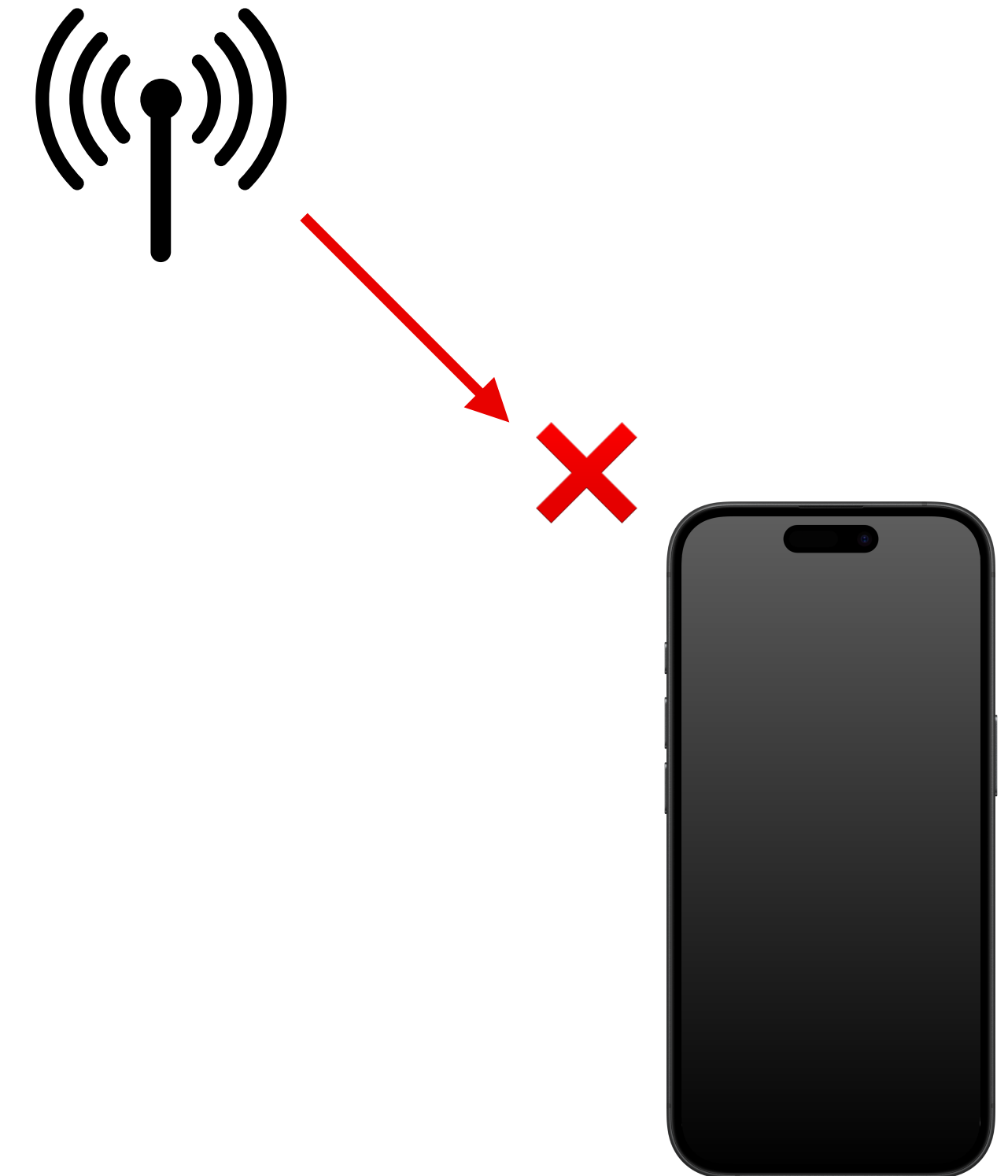
1. Confirm existance of cell with ALS (20P)
2. Calculate distance between recorded and ALS location (20P)
3. Check if frequency and physical cell identity match ALS (8P)
4. Low Bandwidth (2P)
5. High Signal Strength (30P)



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

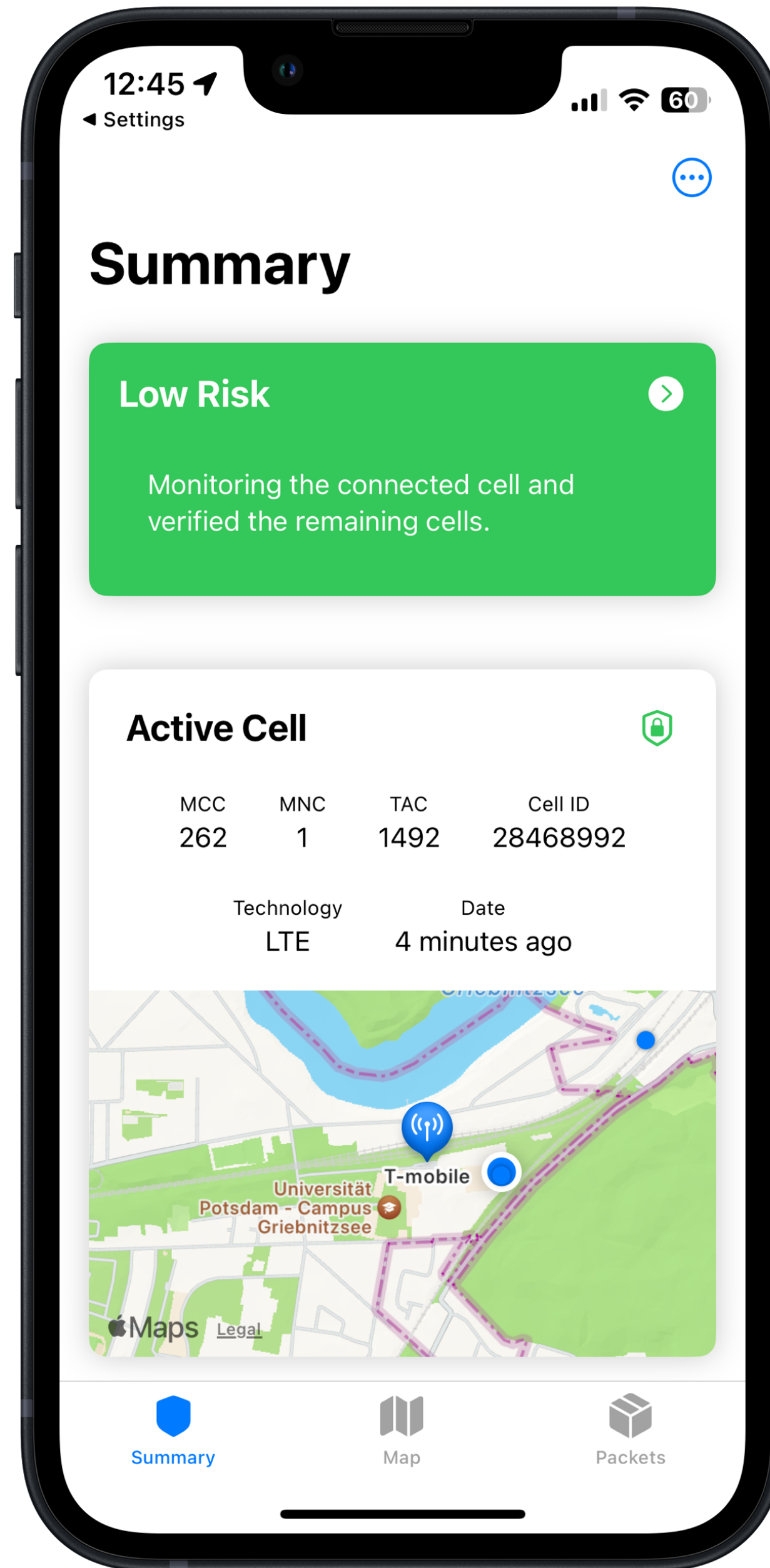
iOS App for RBS Detection

Standard iPhone

Install debug profile and import diagnostics snapshot



Use on primary device with Lockdown mode



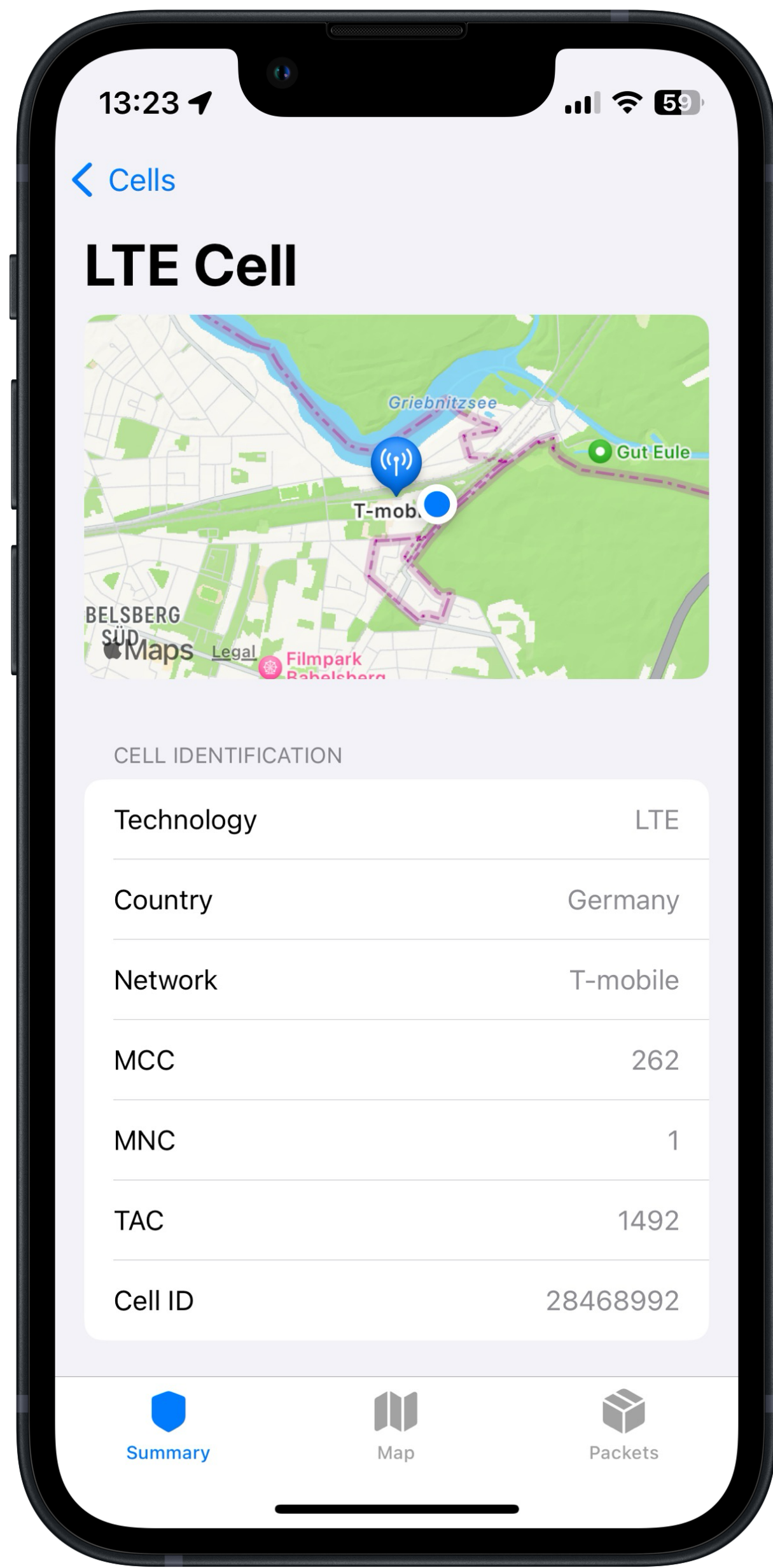
Supports iOS 14 - 18

Jailbroken iPhone

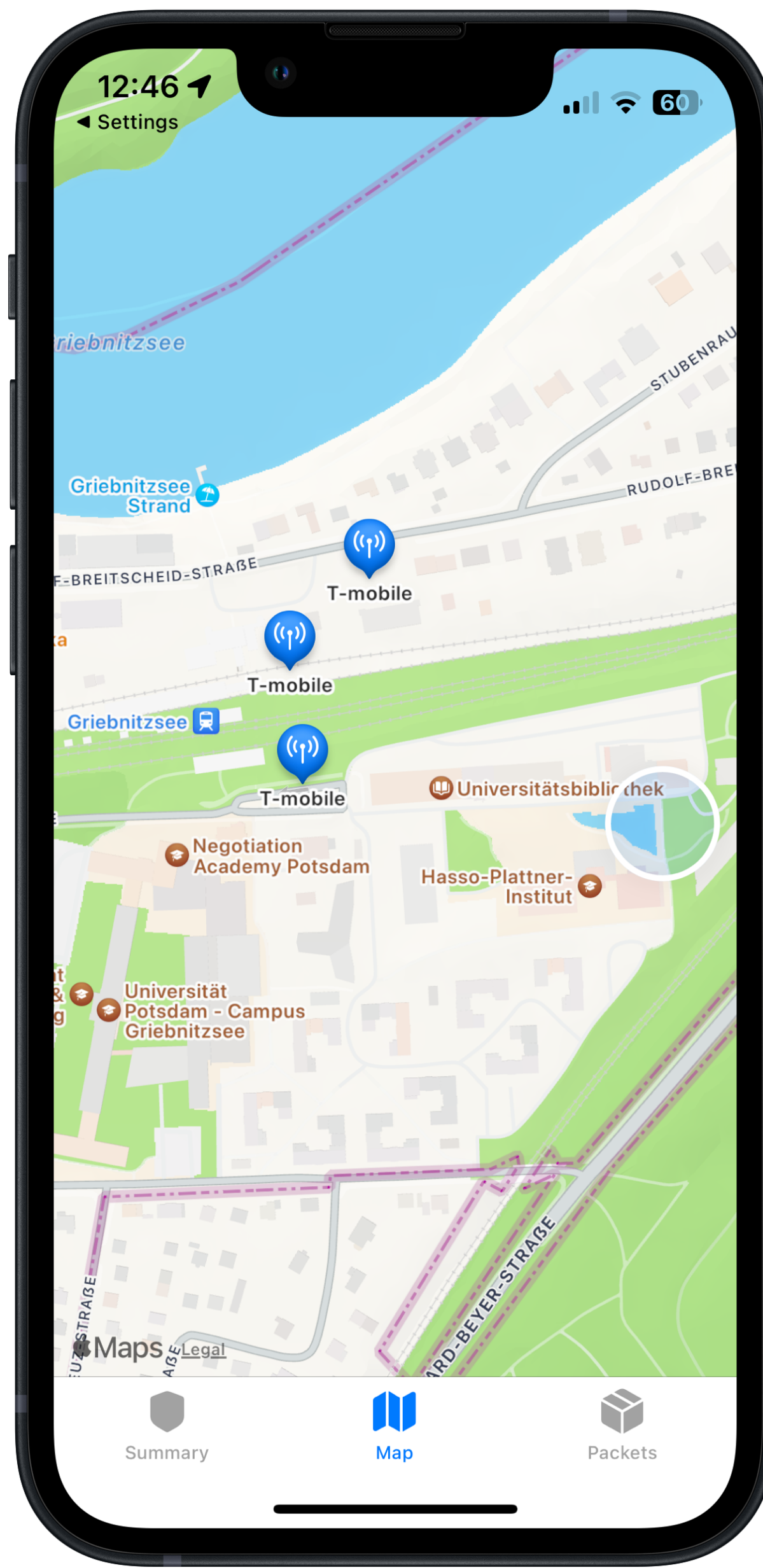
Install components for continuous background verification



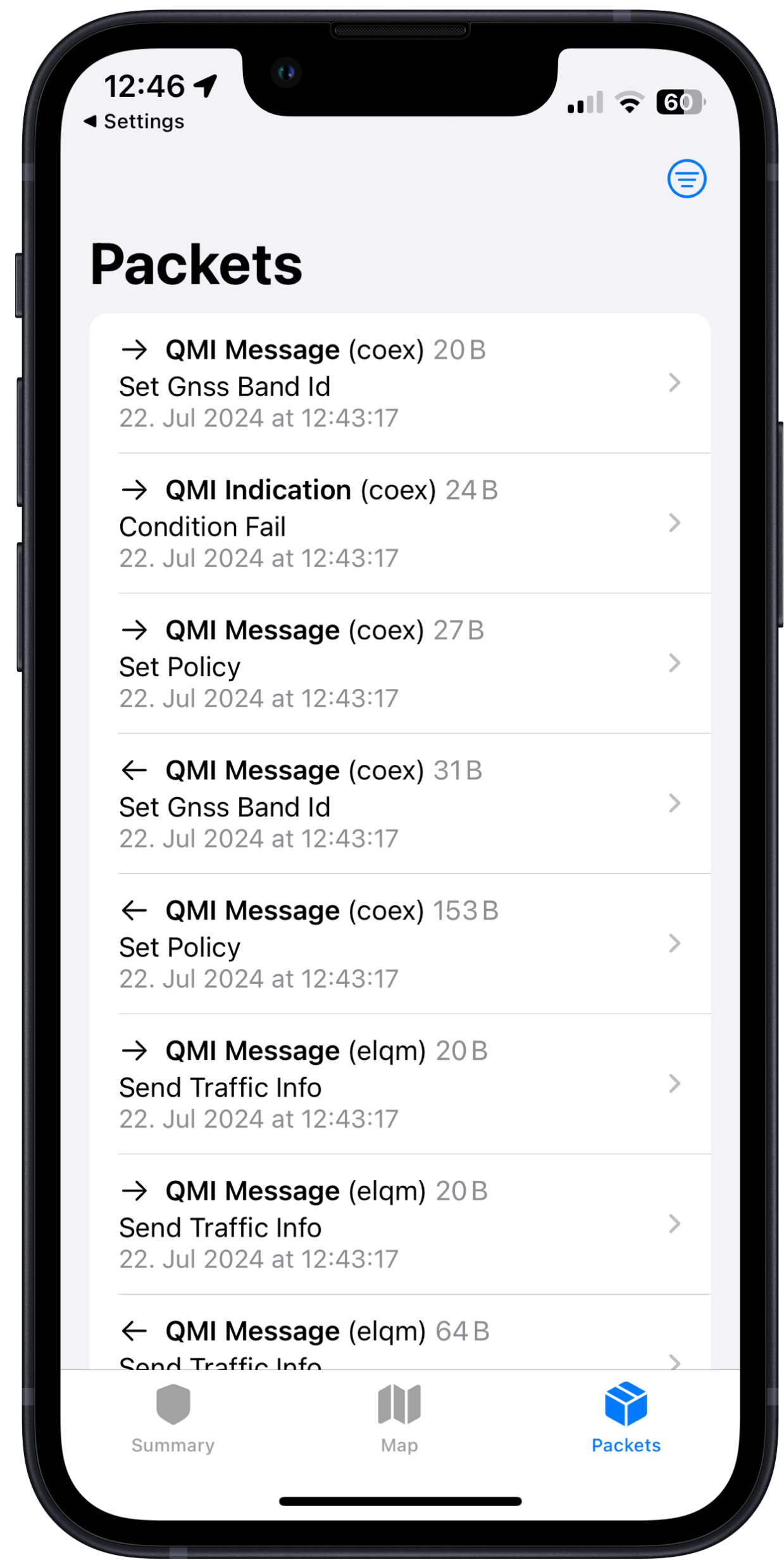
Use on secondary device functioning as sensor



Dive into Details



Explore Nearby Cells



Dissect Packets

Evaluation of CellGuard

In our lab and in the wild

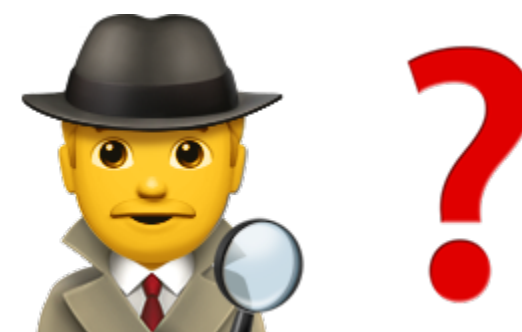


Datasets from across Europe collected over multiple months

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



Continuous development
of CellGuard & tooling



Download CellGuard at
cellguard.seemoo.de

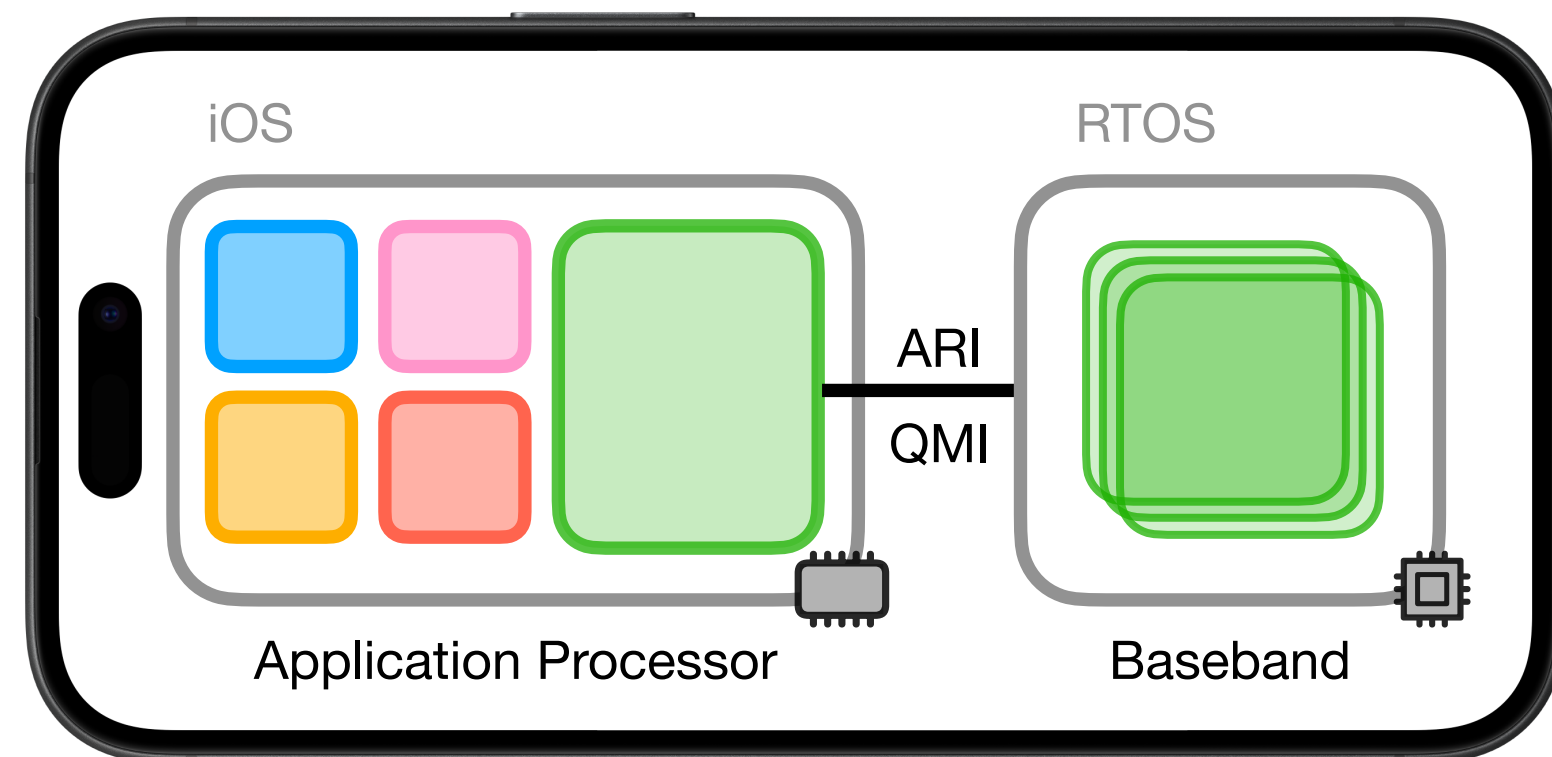


Open-source release
next week

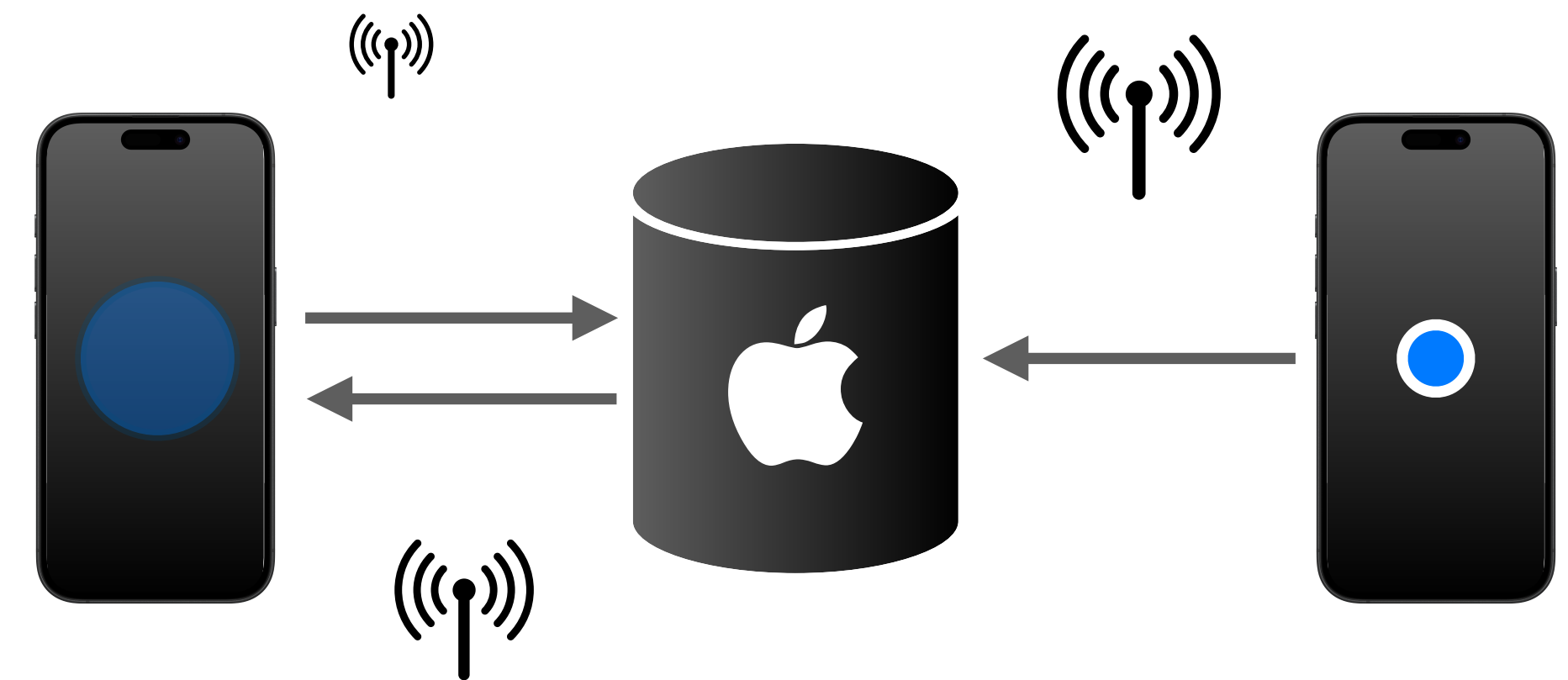
Conclusion

Busting Rogue Base Stations using CellGuard and ALS

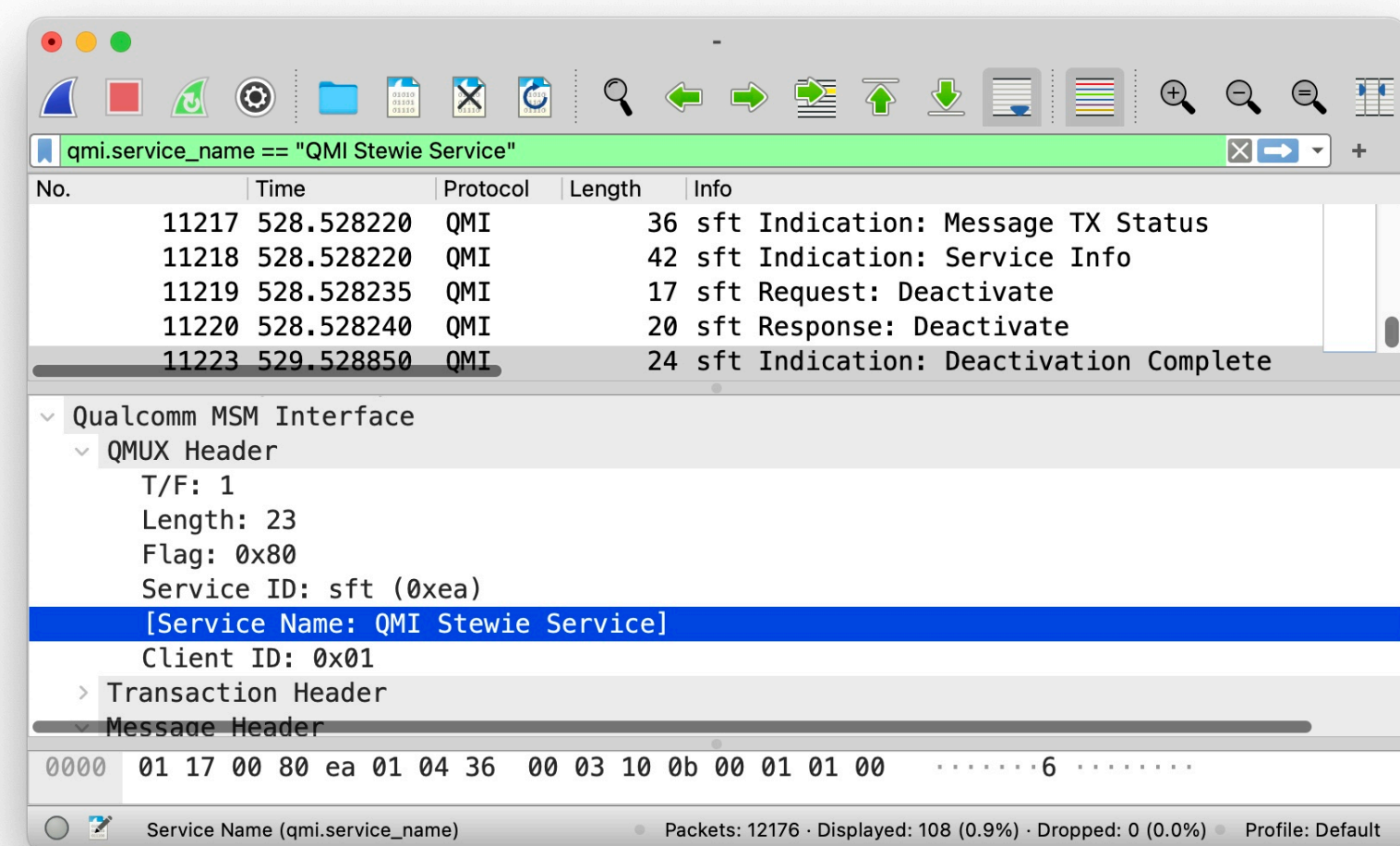
Reversing of iOS baseband architecture



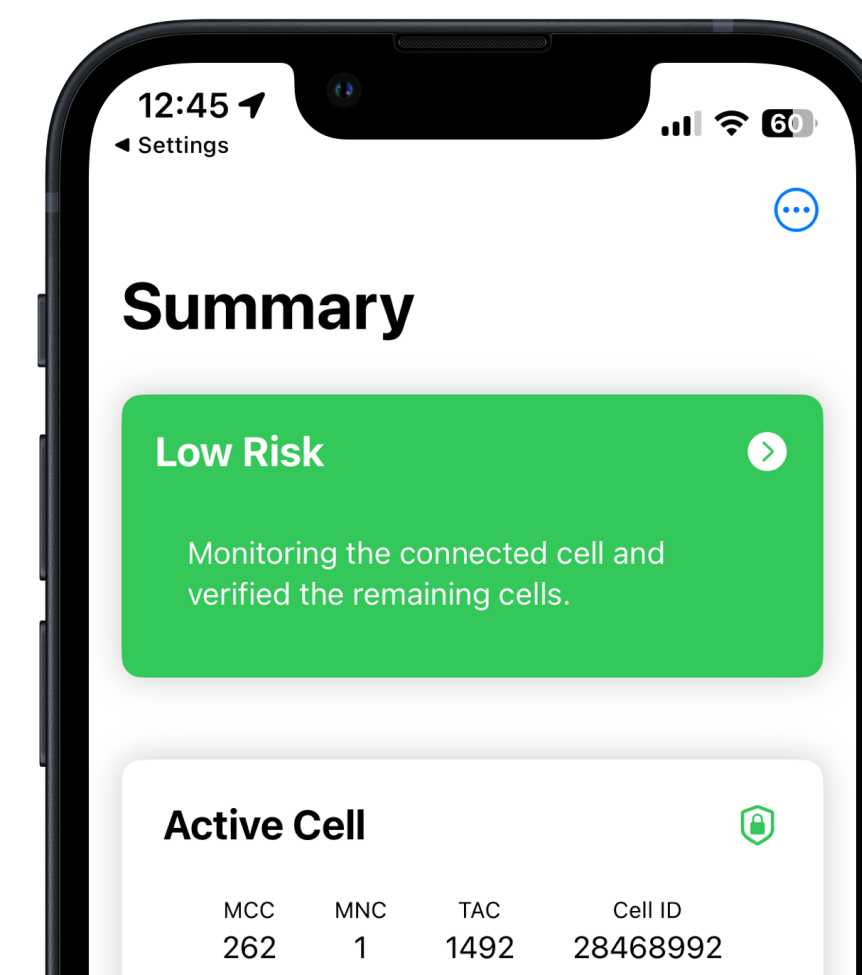
Evaluation of Apple Location Services



BaseTrace: Framework for baseband analysis



CellGuard with RBS detection algorithm



Q&A



Read our Paper



Download CellGuard

larnold@seemoo.tu-darmstadt.de

[@lukasarnld](https://twitter.com/lukasarnld)