Roaming Agreements - The Hidden Attack Surface of 5G

Swantje Lange, Francesco Gringoli, Matthias Hollick, and Jiska Classen

HPI Hasso Plattner Institut

UNIVERSITÀ DEGLI STUDI DI BRESCIA

TECHNISCHE UNIVERSITÄT DARMSTADT

Open6GHub

TROOPERS

# whoami

- Swantje Lange
- PhD student at Hasso Plattner Institute in Potsdam, Germany
- Security in cellular networks

✉ swantje.lange@hpi.de
linkedin.com/in/swantje-lange
@swantje@chaos.social

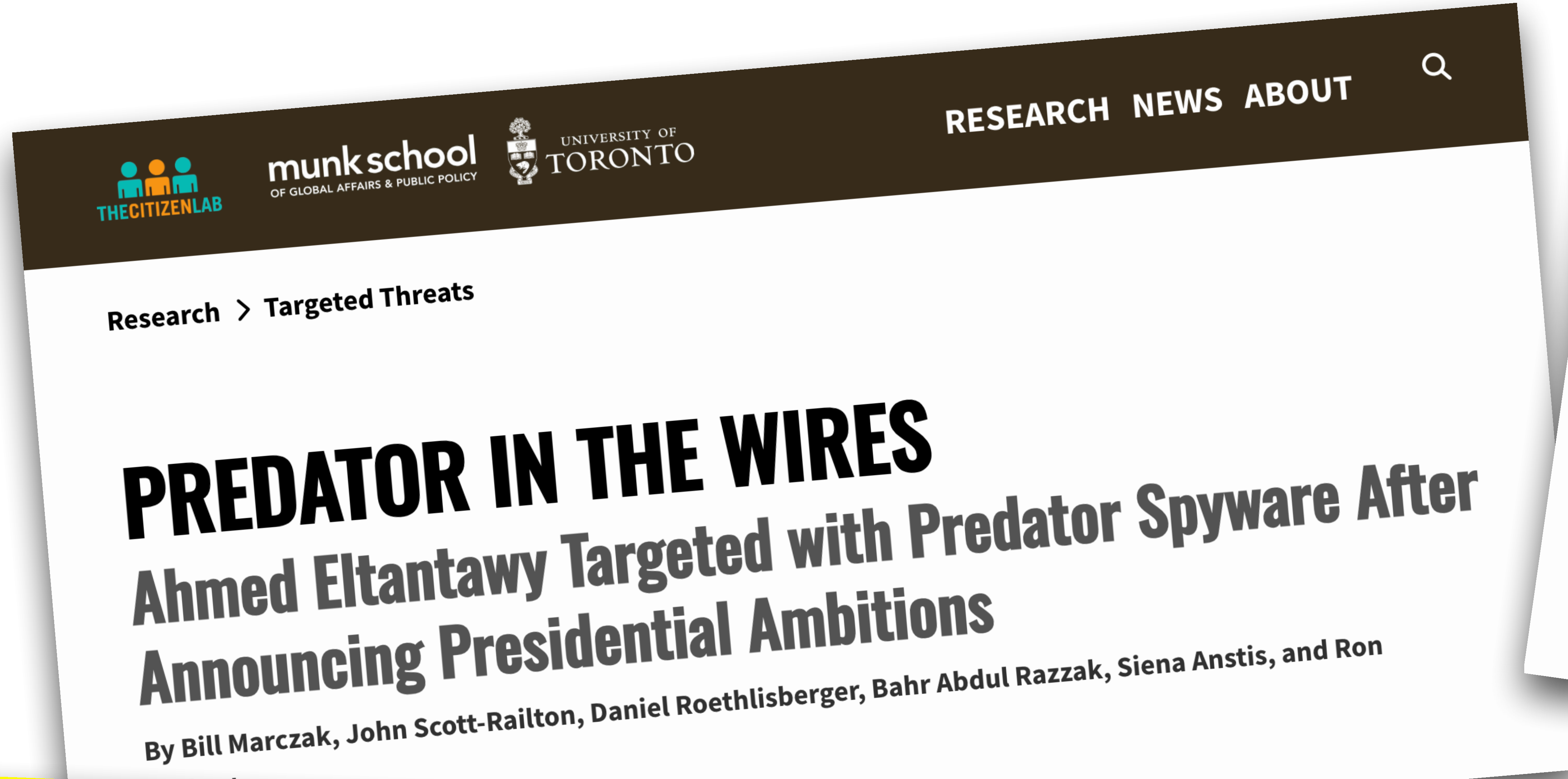
Roaming

Traveling

Single device

Single contract

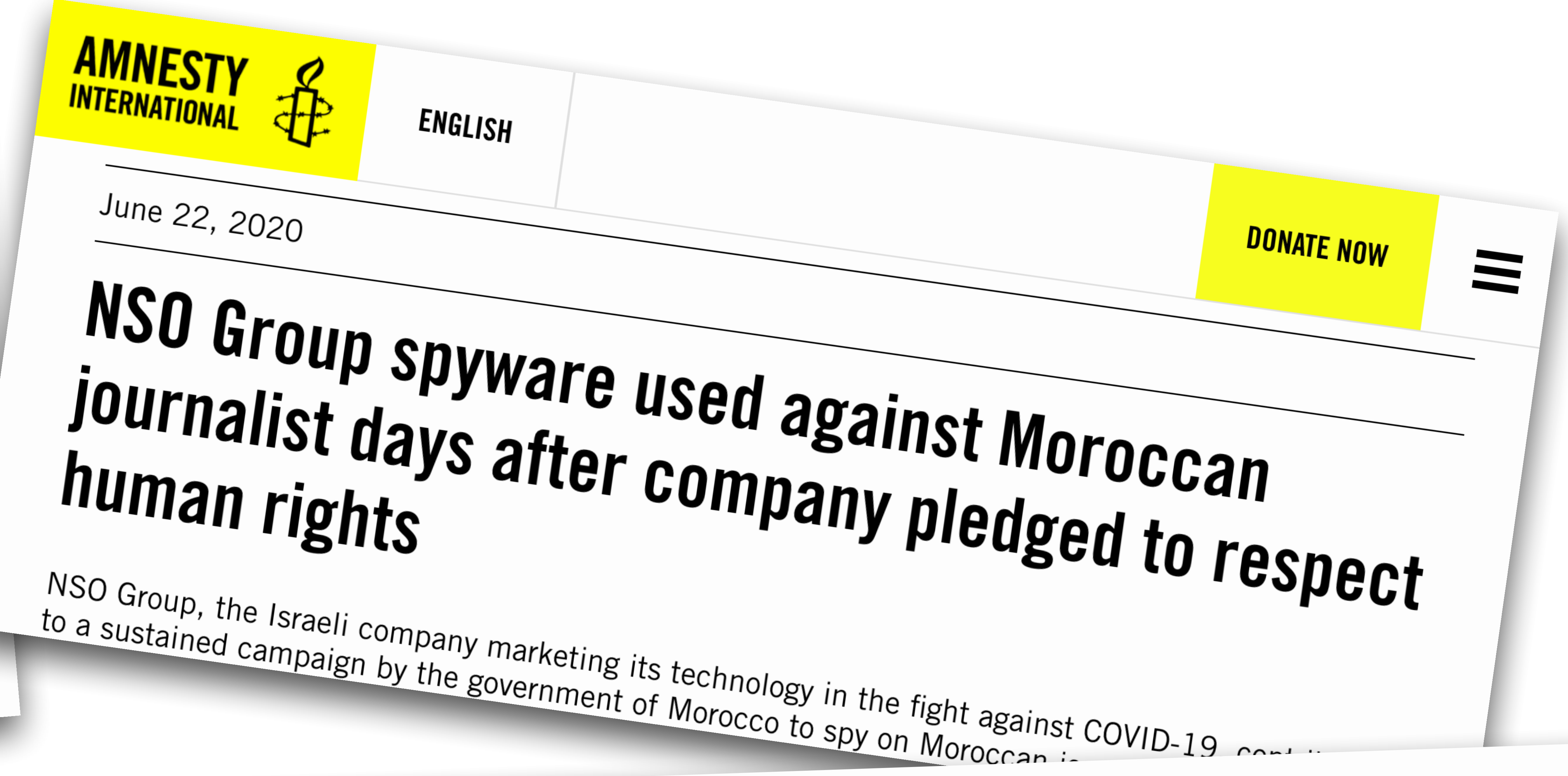
High-value Targets can Hardly Hide


THECITIZENLAB
munk school OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO
RESEARCH
NEWS
ABOUT
Research > Targeted Threats

PREDATOR IN THE WIRES

Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

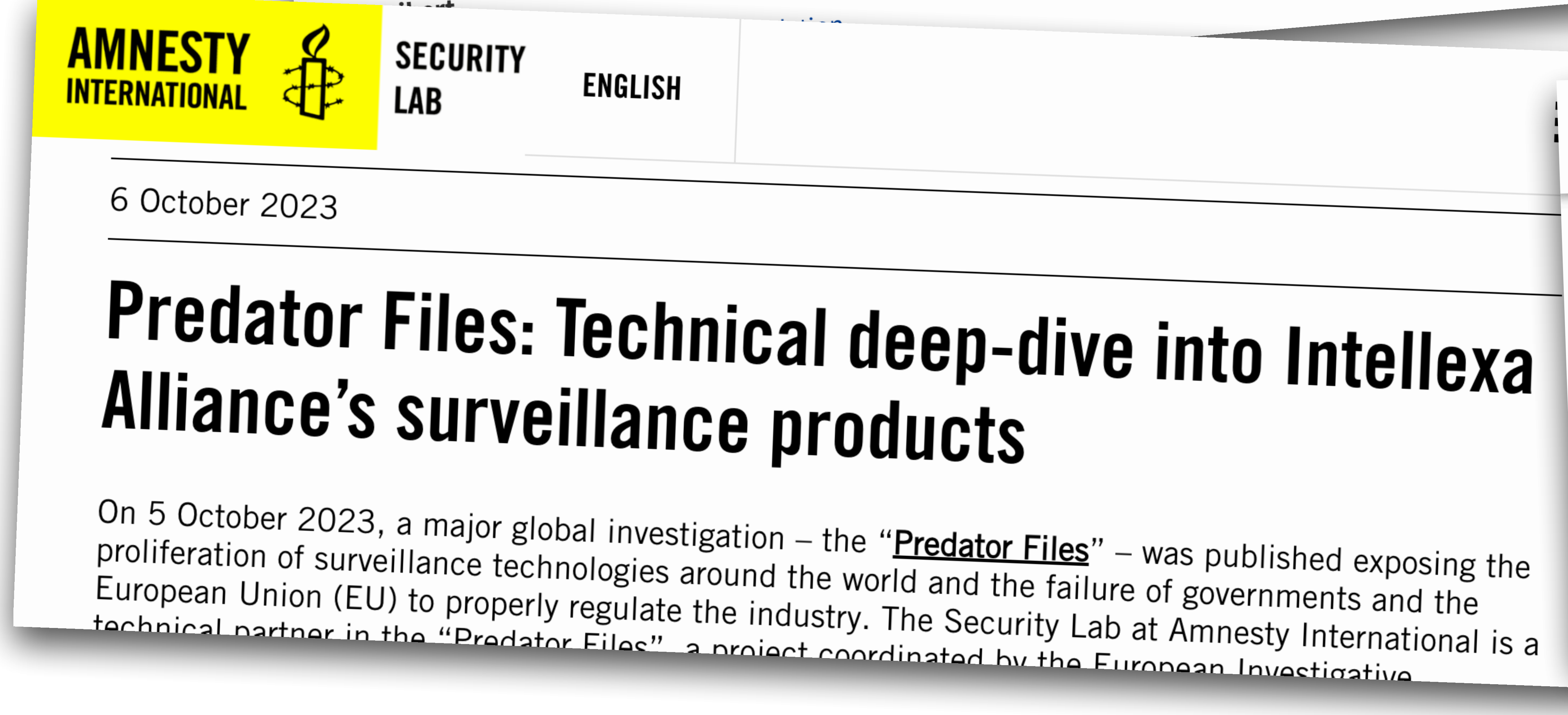
By Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, and Ron



June 22, 2020

NSO Group spyware used against Moroccan journalist days after company pledged to respect human rights

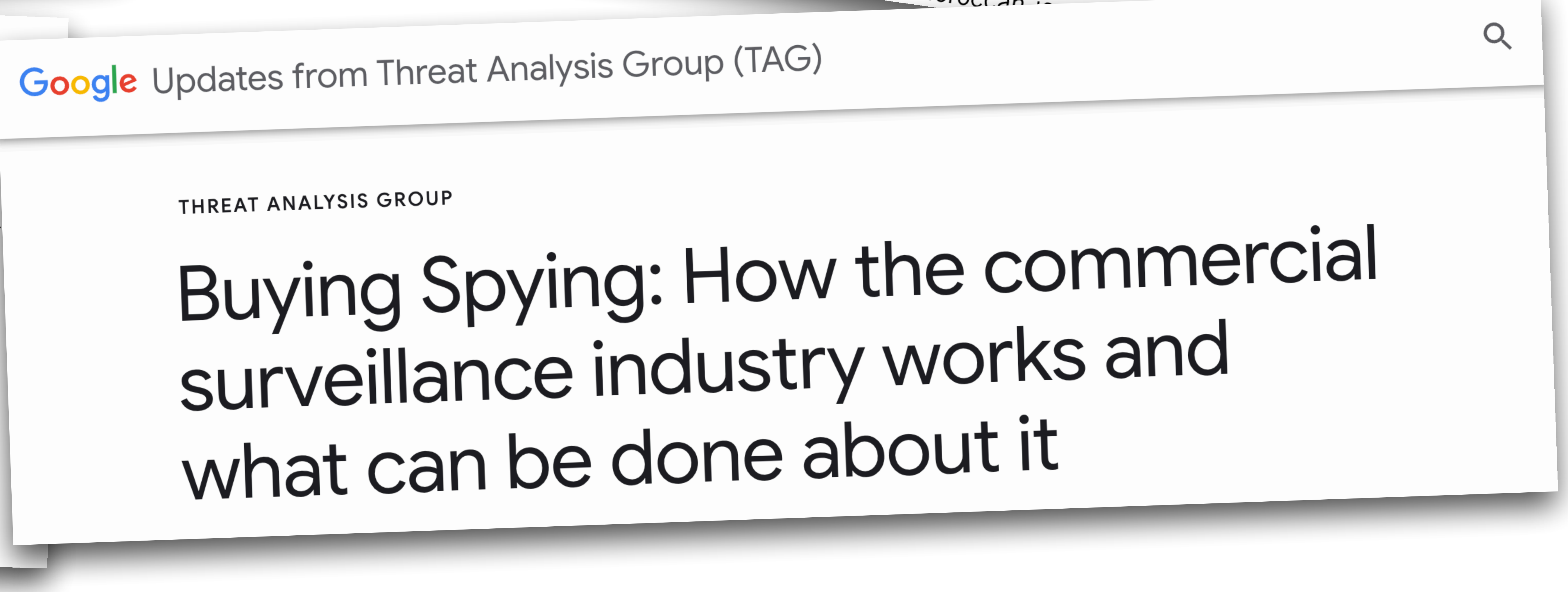
NSO Group, the Israeli company marketing its technology in the fight against COVID-19, con
to a sustained campaign by the government of Morocco to spy on Moroccan j



6 October 2023

Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products

On 5 October 2023, a major global investigation – the “Predator Files” – was published exposing the proliferation of surveillance technologies around the world and the failure of governments and the European Union (EU) to properly regulate the industry. The Security Lab at Amnesty International is a technical partner in the “Predator Files”, a project coordinated by the European Investigative



THREAT ANALYSIS GROUP

Buying Spying: How the commercial surveillance industry works and what can be done about it

Roaming as Attack Surface

2G

- Commonly used for Rogue Base Station attacks

→ turn off 2G

3G

- Introduces network authentication
- Limits attack surface to pre-authentication messages

→ use roaming for attacks

4G

- Binds session keys to roaming networks
- Session keys only valid for one roaming network

5G

- Adds proof of presence in roaming

Visited Network

Home Network

Authentication Vector

Legitimate Roaming

Collaborating Visited Network

Home Network

Authentication Vector

Abusing Roaming

Attacker Model

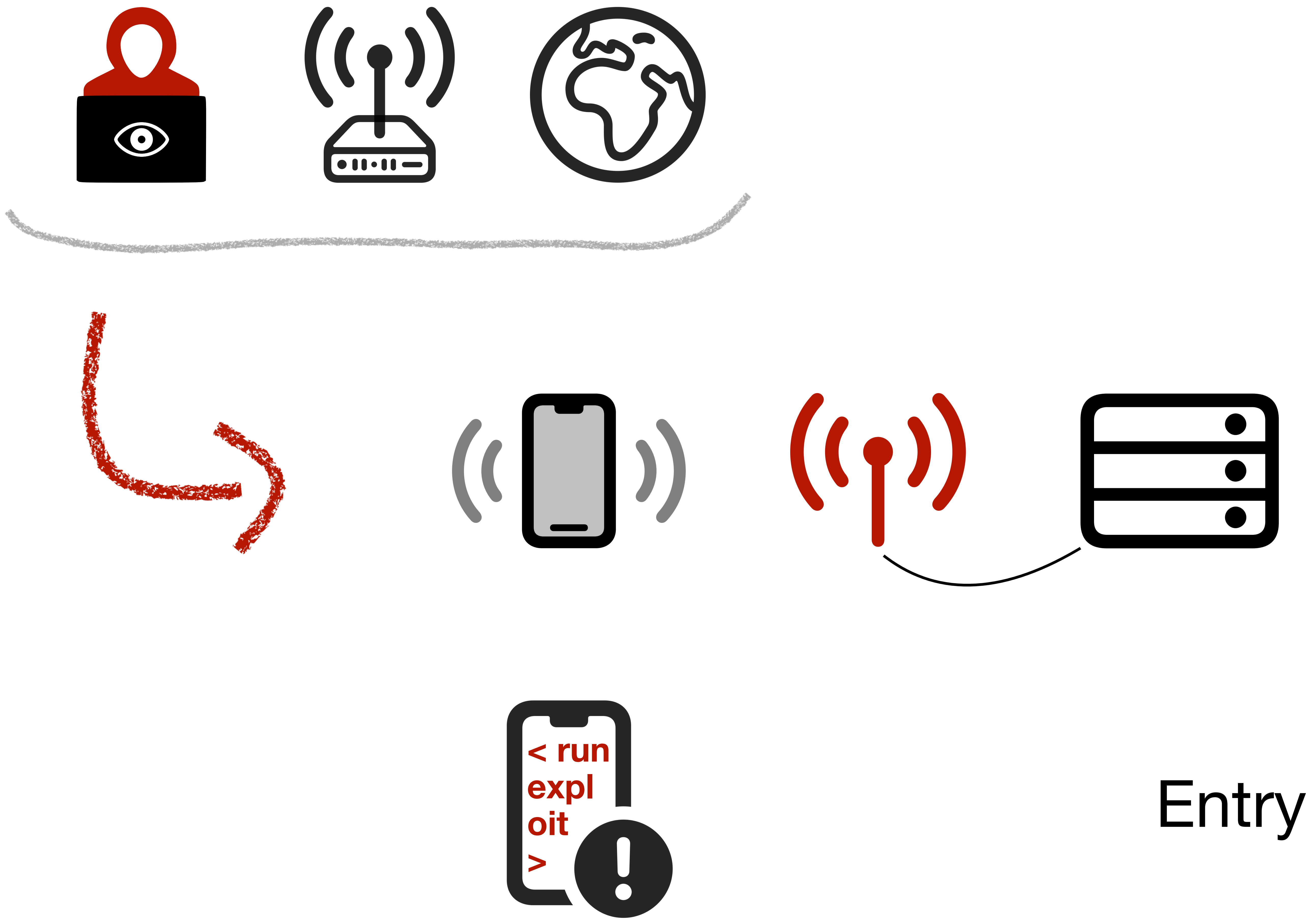
State-sponsored attacker collaborating with operator

Software-Defined Radio as Rogue Base Station

Same or different country as operator

Attacker Model

Goals



Machine-in-the-Middle attacks

Entry point for Remote Code Execution

Lab Setup

- Visited Network and Home Network with Open5GS roaming implementation

- srsRAN as RAN

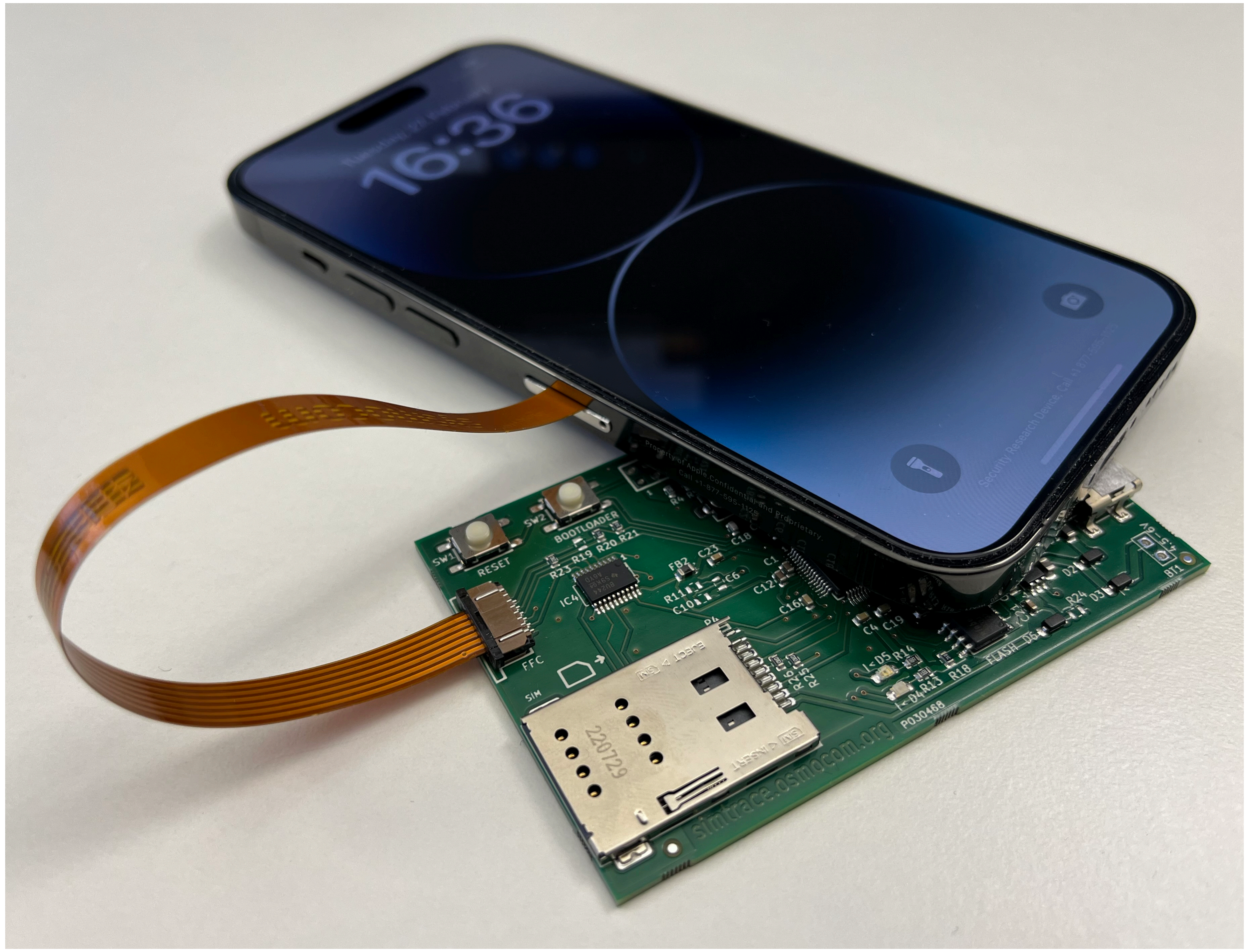
- Several phones

Lab Setup

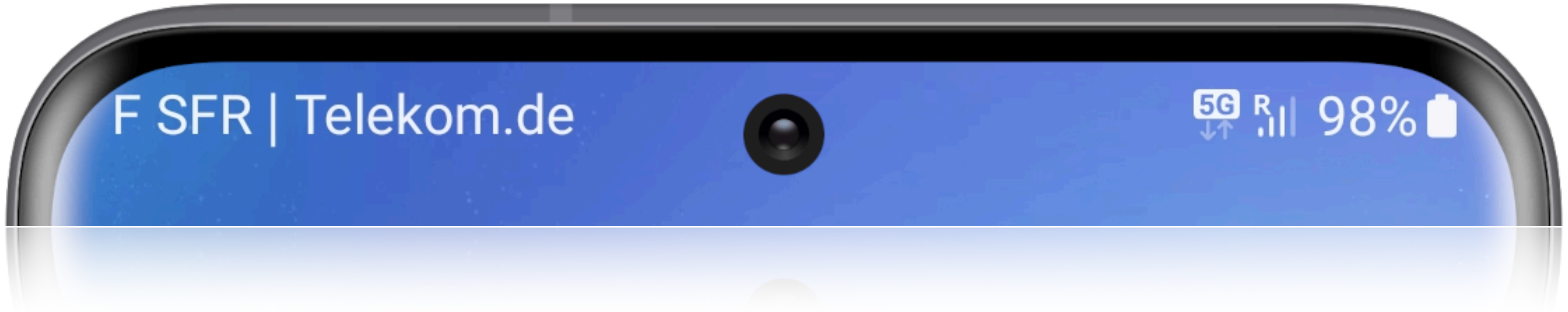
- Visited Network and Home Network with Open5GS roaming implementation
- srsRAN as RAN
- Several phones

Lab Setup

- SIMtrace2 to observe communication between phone and SIM card

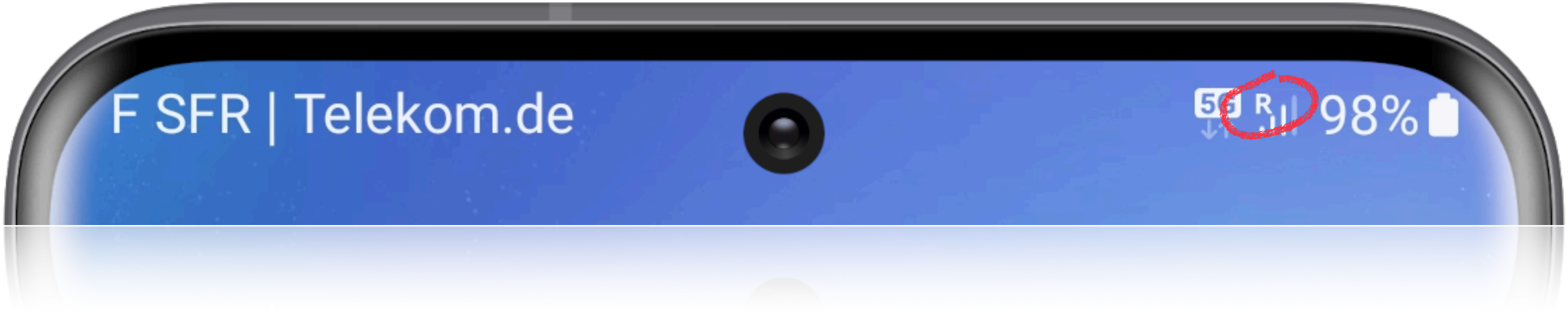


Fool the User 🤫

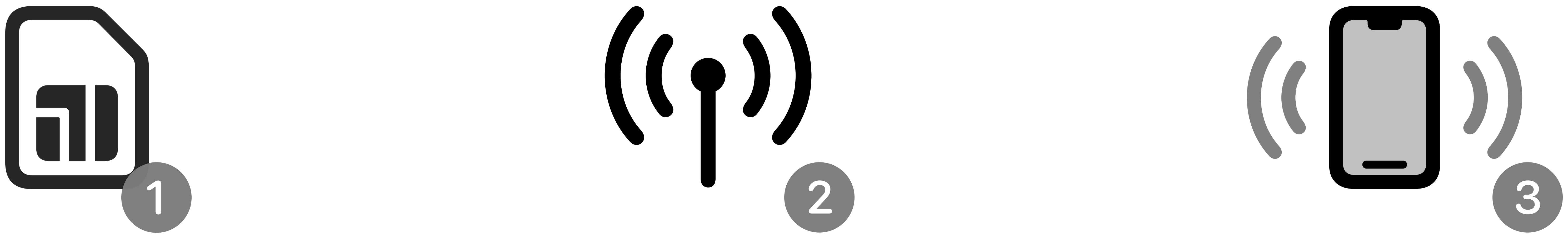


F SFR | Telekom.de

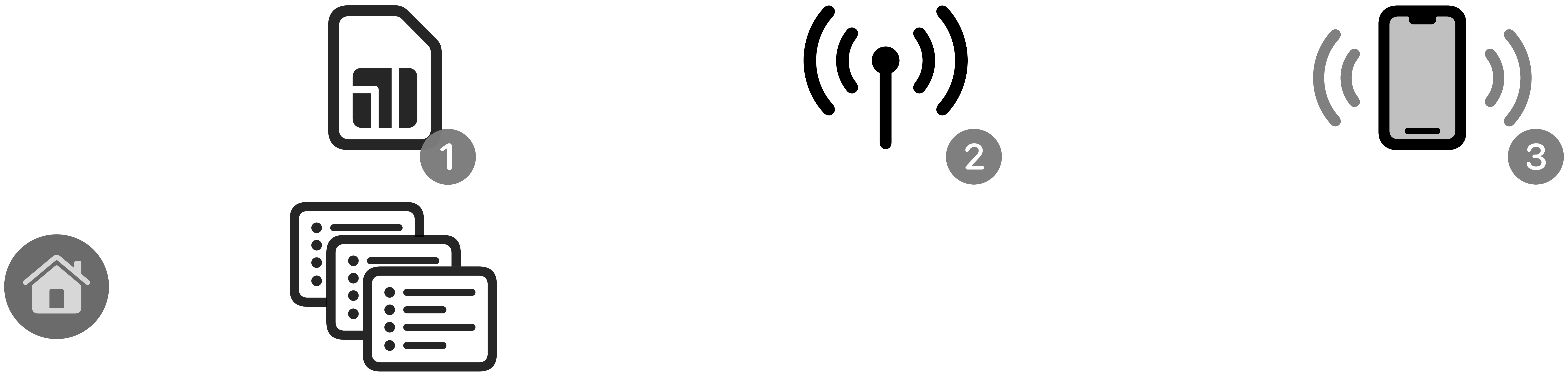
Fool the User 🤫



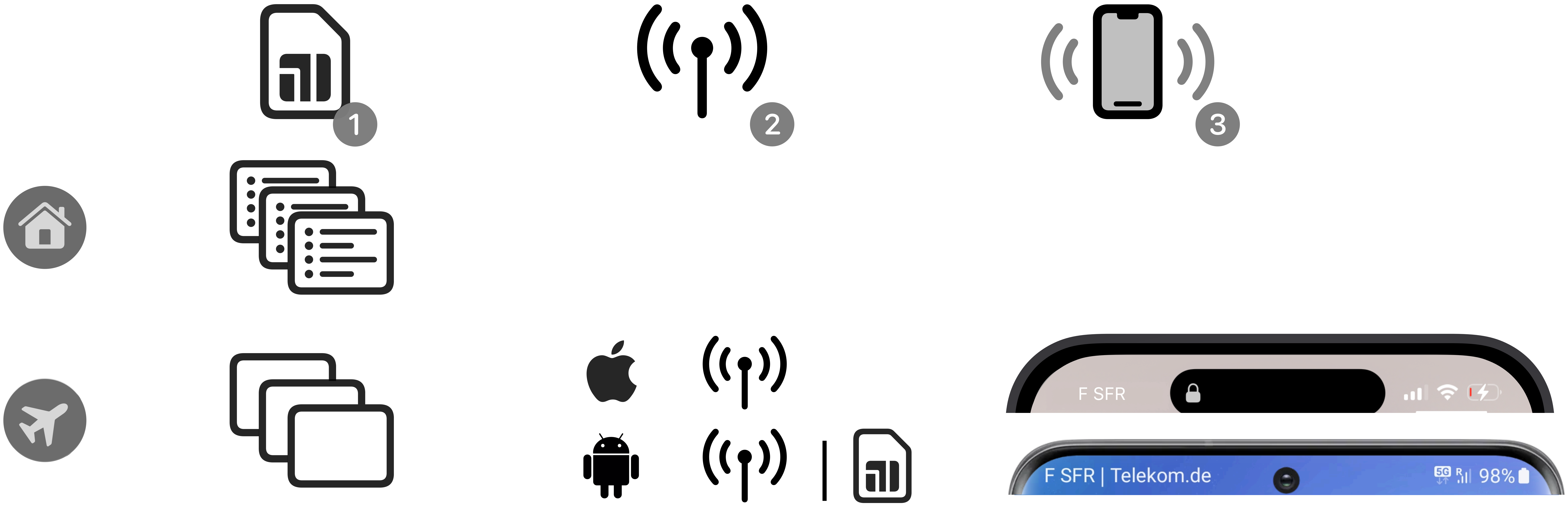
Where the Network Name Comes From



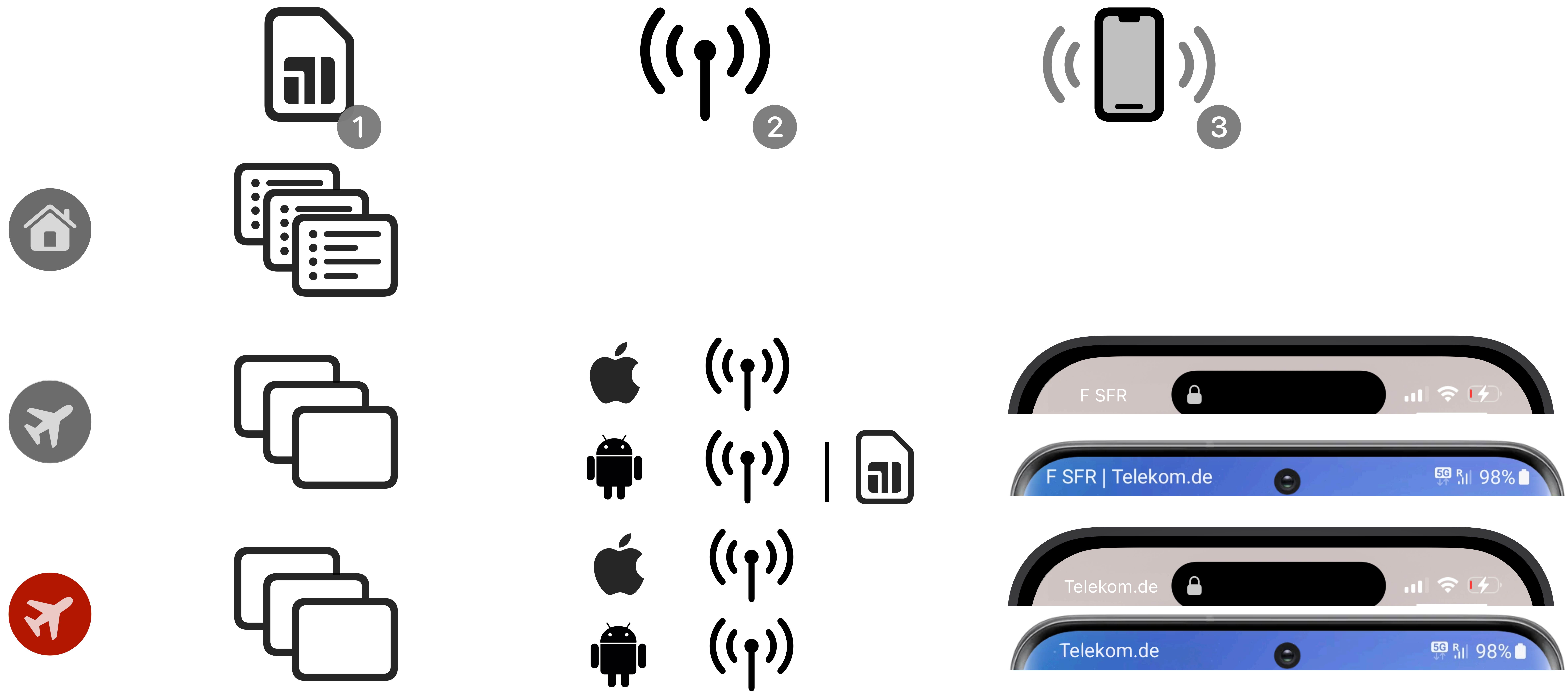
Where the Network Name Comes From



Where the Network Name Comes From

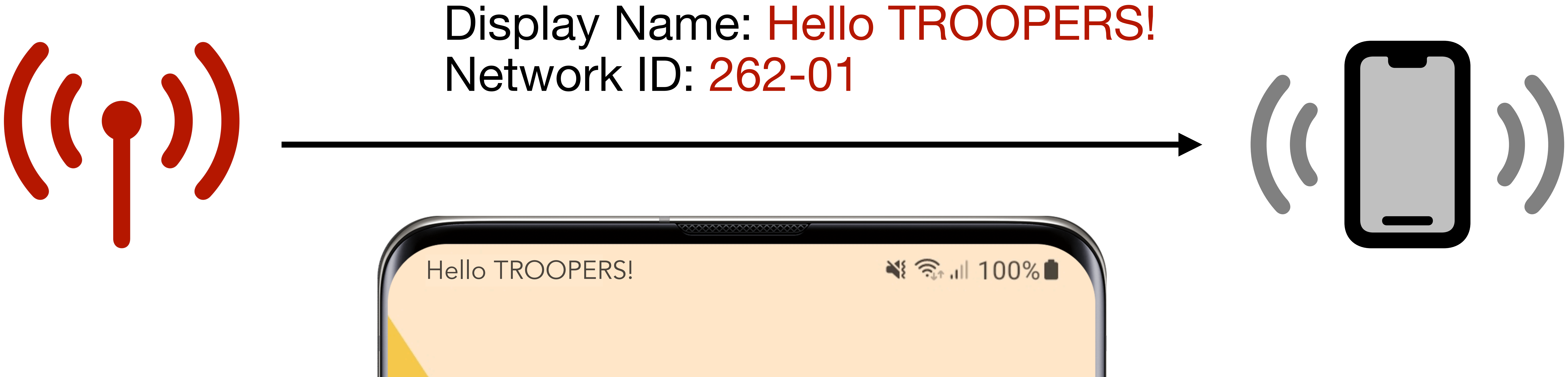


Where the Network Name Comes From



Network Name Displayed on Phone

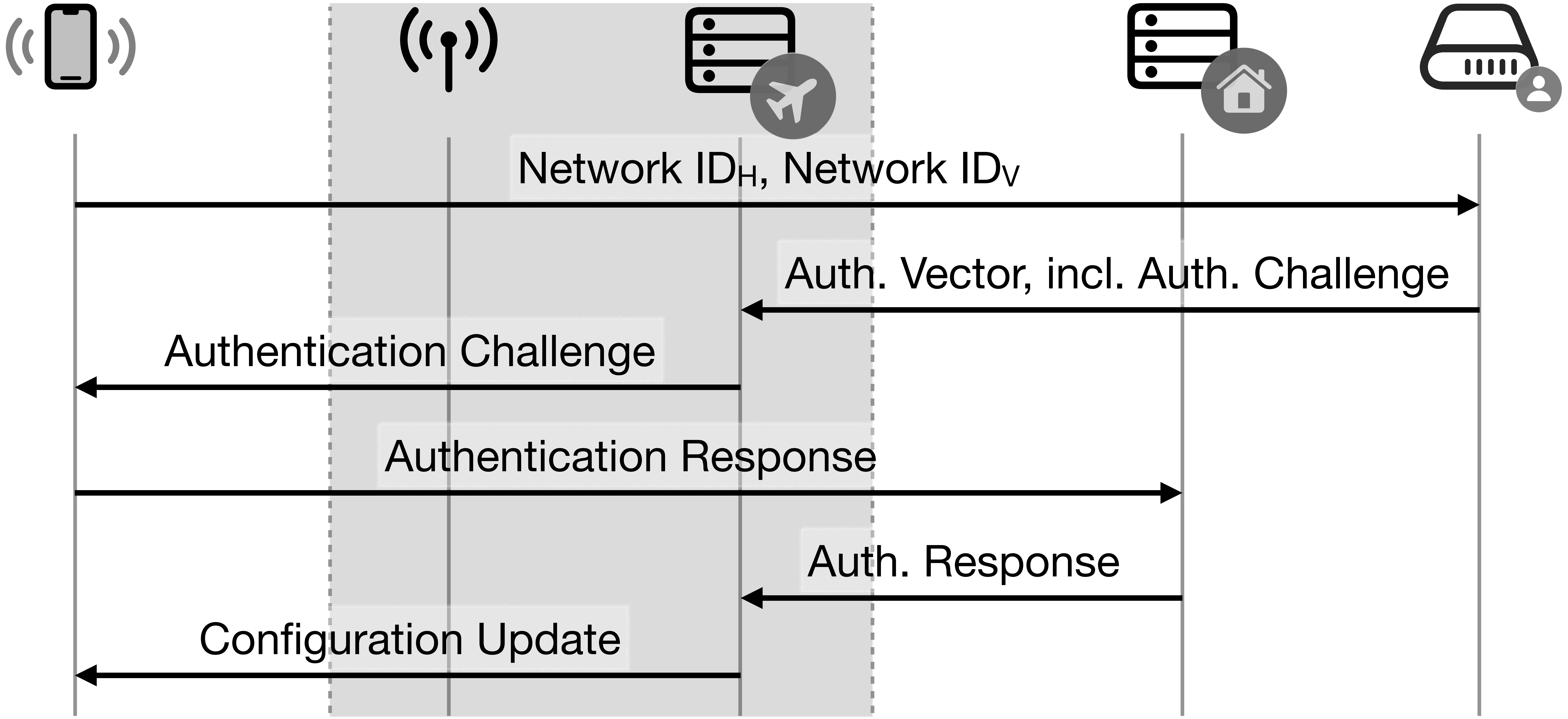
- Users have limited possibilities to observe roaming
- Network ID only information sent to the Home Network 🤯
- Manipulate Network ID to hide roaming indicator



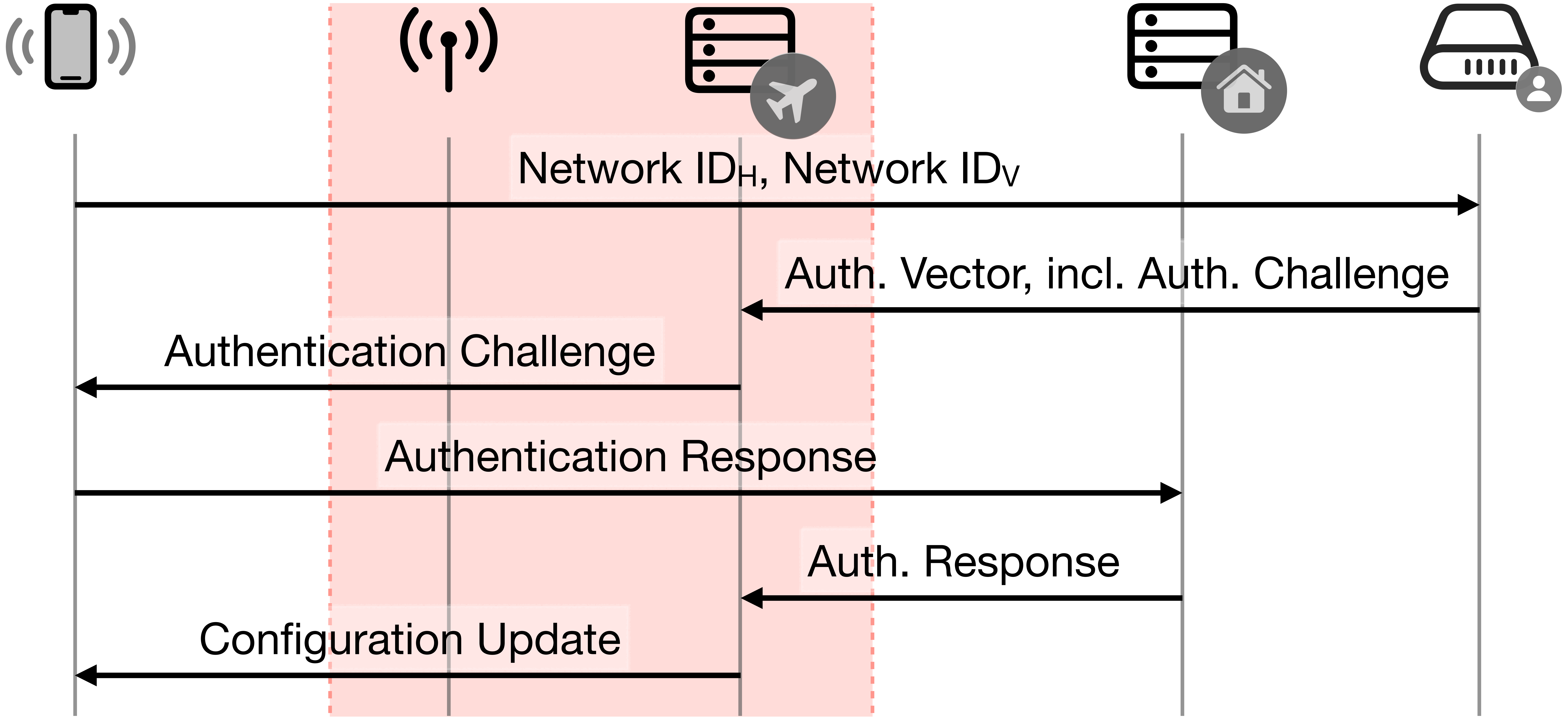
Display Name: Hello TROOPERS!
Network ID: 262-01

Hello TROOPERS!

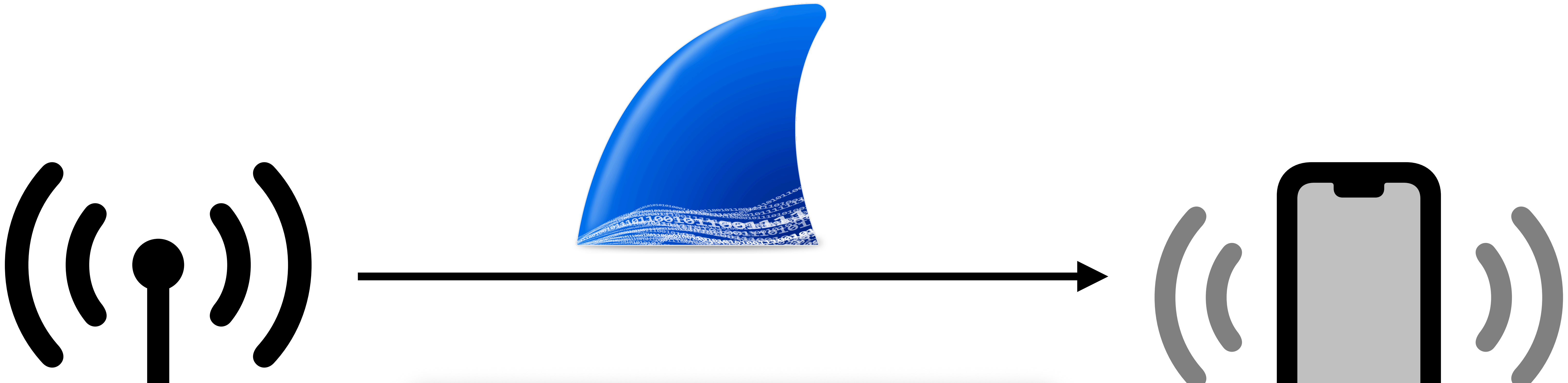
Why we don’t see what we would like to see

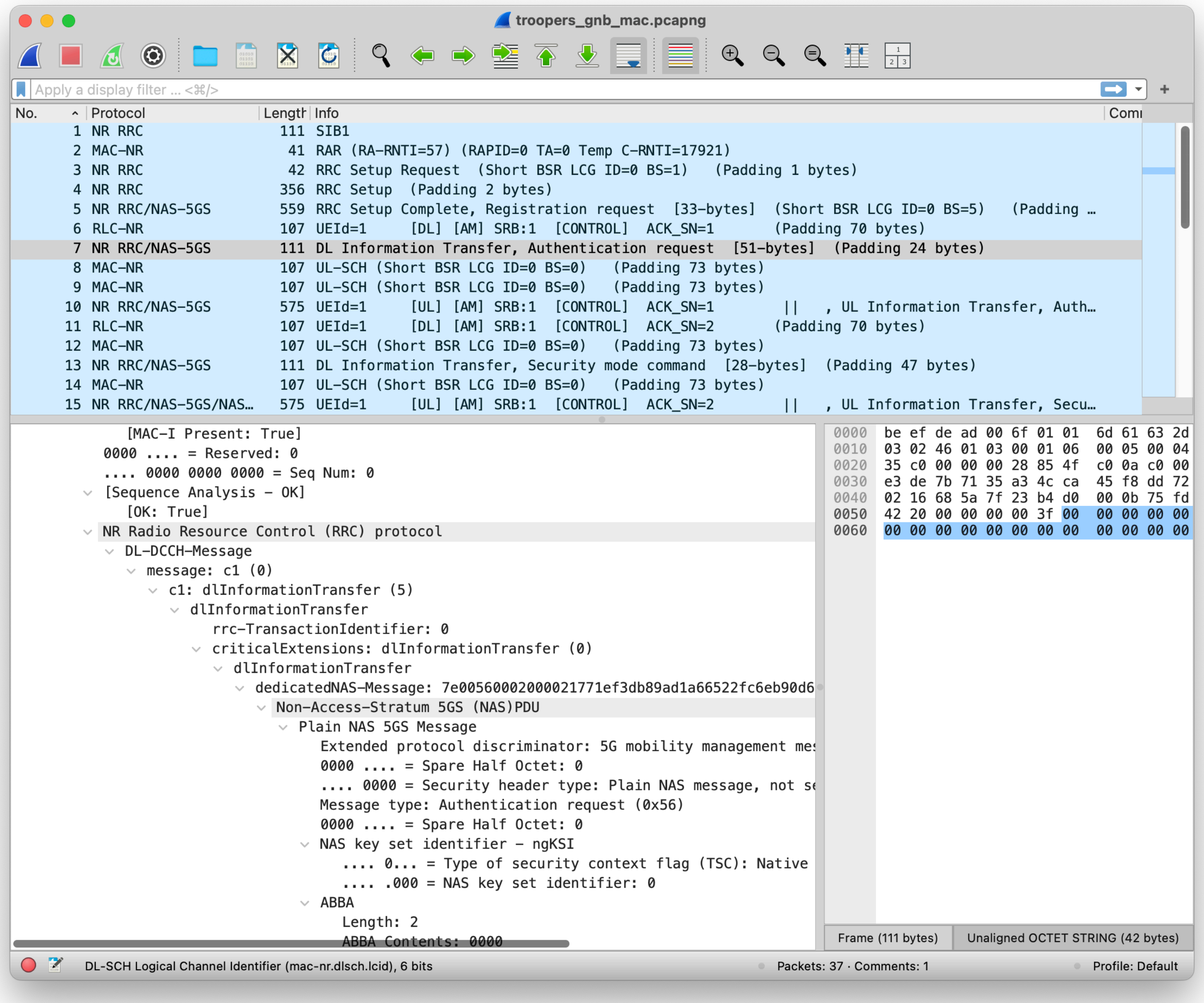


Why we don’t see what we would like to see



Demo





```
No.  ^ Protocol              Length Info                                                                                   Comı
     1 NR RRC                  111 SIB1
     2 MAC-NR                   41 RAR (RA-RNTI=57) (RAPID=0 TA=0 Temp C-RNTI=17921)
     3 NR RRC                   42 RRC Setup Request  (Short BSR LCG ID=0 BS=1)   (Padding 1 bytes)
     4 NR RRC                  356 RRC Setup  (Padding 2 bytes)
     5 NR RRC/NAS-5GS          559 RRC Setup Complete, Registration request  [33-bytes]  (Short BSR LCG ID=0 BS=5)   (Padding …
     6 RLC-NR                  107 UEId=1     [DL] [AM] SRB:1  [CONTROL]  ACK_SN=1       (Padding 70 bytes)
     7 NR RRC/NAS-5GS          111 DL Information Transfer, Authentication request  [51-bytes]  (Padding 24 bytes)
     8 MAC-NR                  107 UL-SCH (Short BSR LCG ID=0 BS=0)   (Padding 73 bytes)
     9 MAC-NR                  107 UL-SCH (Short BSR LCG ID=0 BS=0)   (Padding 73 bytes)
    10 NR RRC/NAS-5GS          575 UEId=1     [UL] [AM] SRB:1  [CONTROL]  ACK_SN=1        ||   , UL Information Transfer, Auth…
    11 RLC-NR                  107 UEId=1     [DL] [AM] SRB:1  [CONTROL]  ACK_SN=2       (Padding 70 bytes)
    12 MAC-NR                  107 UL-SCH (Short BSR LCG ID=0 BS=0)   (Padding 73 bytes)
    13 NR RRC/NAS-5GS          111 DL Information Transfer, Security mode command  [28-bytes]  (Padding 47 bytes)
    14 MAC-NR                  107 UL-SCH (Short BSR LCG ID=0 BS=0)   (Padding 73 bytes)
    15 NR RRC/NAS-5GS/NAS…     575 UEId=1     [UL] [AM] SRB:1  [CONTROL]  ACK_SN=2        ||   , UL Information Transfer, Secu…
```

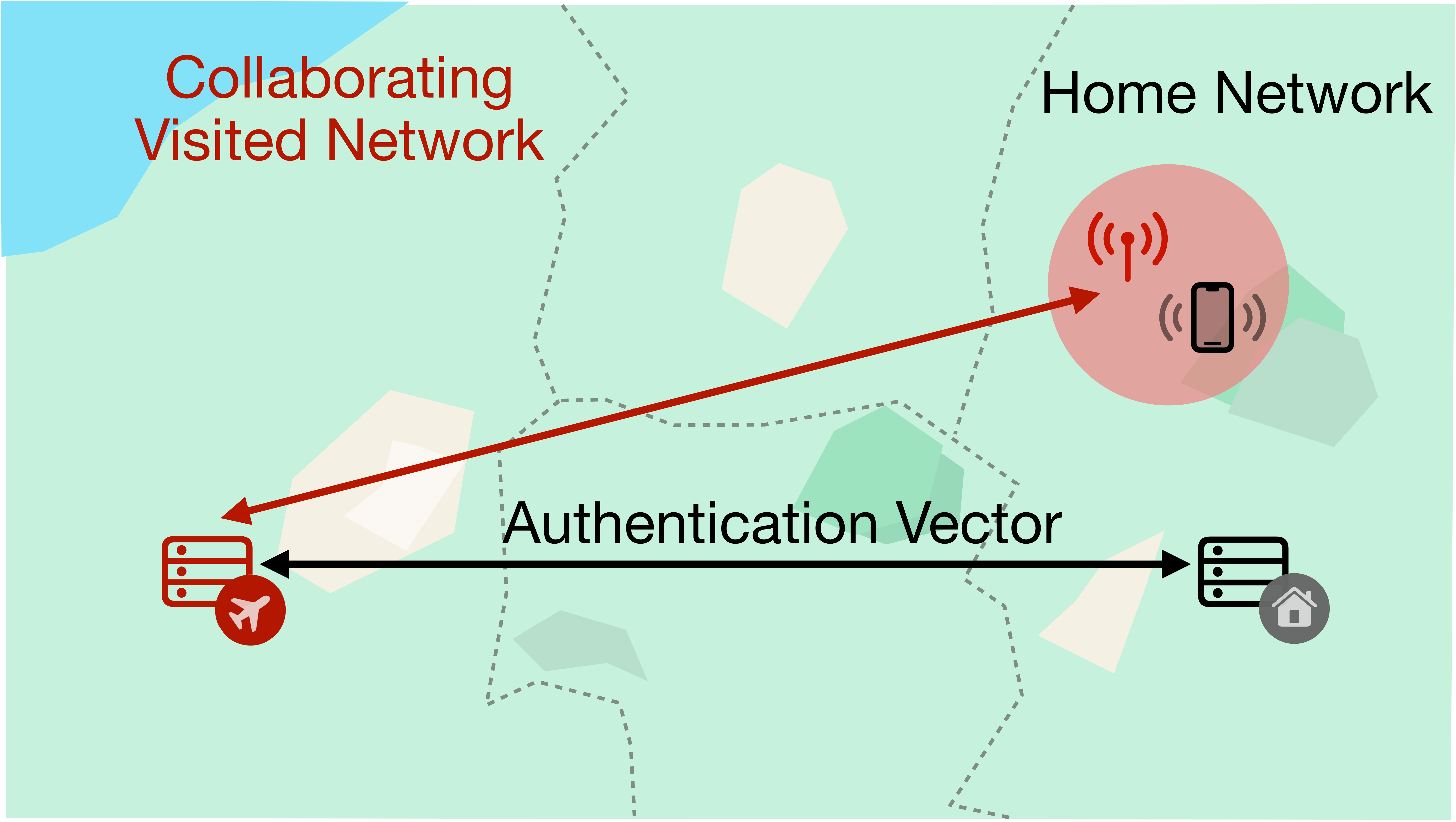
```
      [MAC-I Present: True]
    0000 .... = Reserved: 0
    .... 0000 0000 0000 = Seq Num: 0
  ⌄ [Sequence Analysis - OK]
      [OK: True]
  ⌄ NR Radio Resource Control (RRC) protocol
    ⌄ DL-DCCH-Message
      ⌄ message: c1 (0)
        ⌄ c1: dlInformationTransfer (5)
          ⌄ dlInformationTransfer
              rrc-TransactionIdentifier: 0
            ⌄ criticalExtensions: dlInformationTransfer (0)
              ⌄ dlInformationTransfer
                ⌄ dedicatedNAS-Message: 7e00560002000021771ef3db89ad1a66522fc6eb90d6
                  ⌄ Non-Access-Stratum 5GS (NAS)PDU
                    ⌄ Plain NAS 5GS Message
                        Extended protocol discriminator: 5G mobility management mes
                        0000 .... = Spare Half Octet: 0
                        .... 0000 = Security header type: Plain NAS message, not se
                        Message type: Authentication request (0x56)
                        0000 .... = Spare Half Octet: 0
                      ⌄ NAS key set identifier - ngKSI
                          .... 0... = Type of security context flag (TSC): Native
                          .... .000 = NAS key set identifier: 0
                      ⌄ ABBA
                          Length: 2
                          ABBA Contents: 0000
```

```
0000  be ef de ad 00 6f 01 01  6d 61 63 2d
0010  03 02 46 01 03 00 01 06  00 05 00 04
0020  35 c0 00 00 00 28 85 4f  c0 0a c0 00
0030  e3 de 7b 71 35 a3 4c ca  45 f8 dd 72
0040  02 16 68 5a 7f 23 b4 d0  00 0b 75 fd
0050  42 20 00 00 00 00 3f 00  00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00
```

Frame (111 bytes) | Unaligned OCTET STRING (42 bytes)

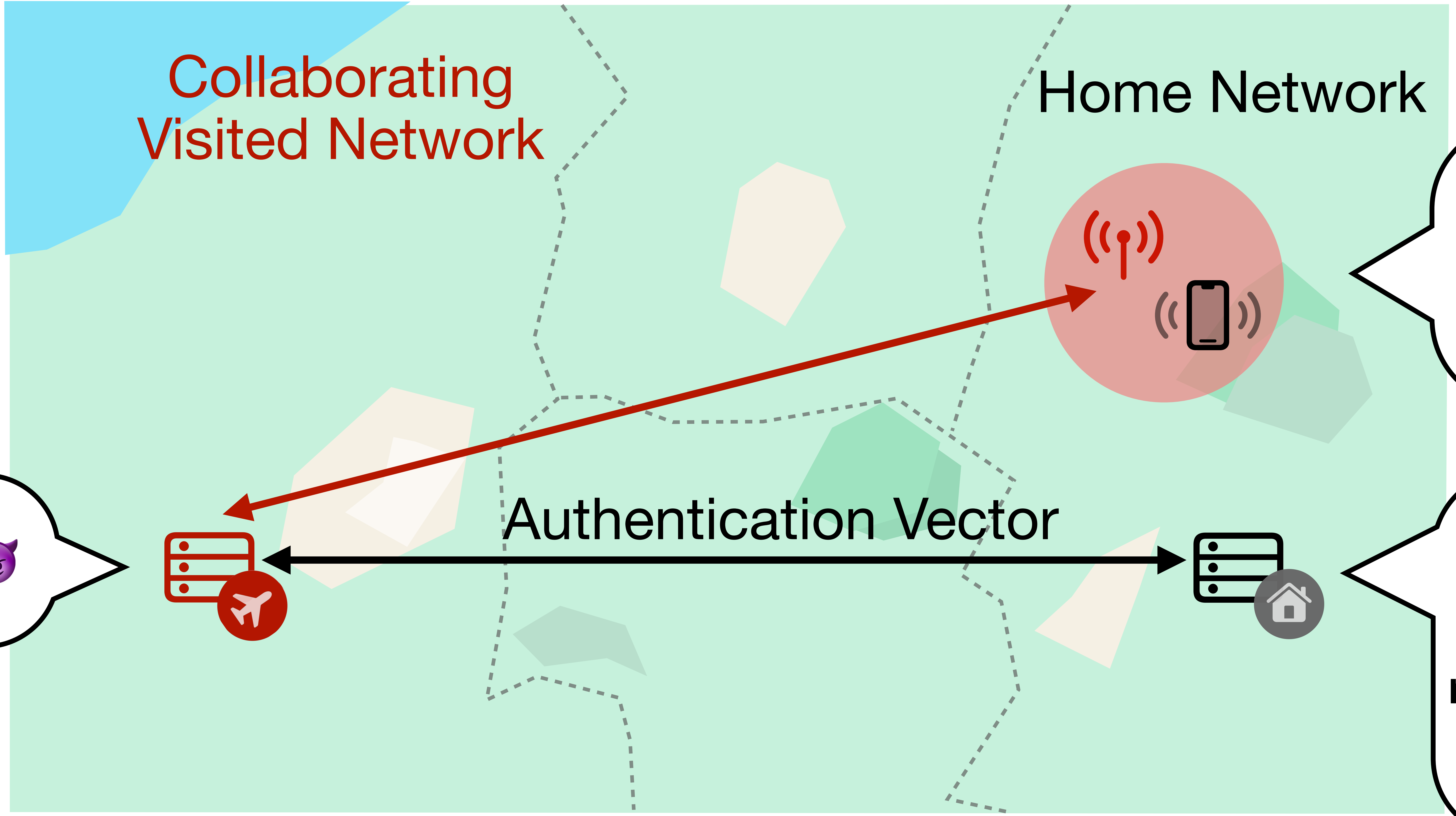
DL-SCH Logical Channel Identifier (mac-nr.dlsch.lcid), 6 bits · Packets: 37 · Comments: 1 · Profile: Default

Authentication Vector Abuse



Authentication Vector Abuse

Request AV 😈



Collaborating Visited Network

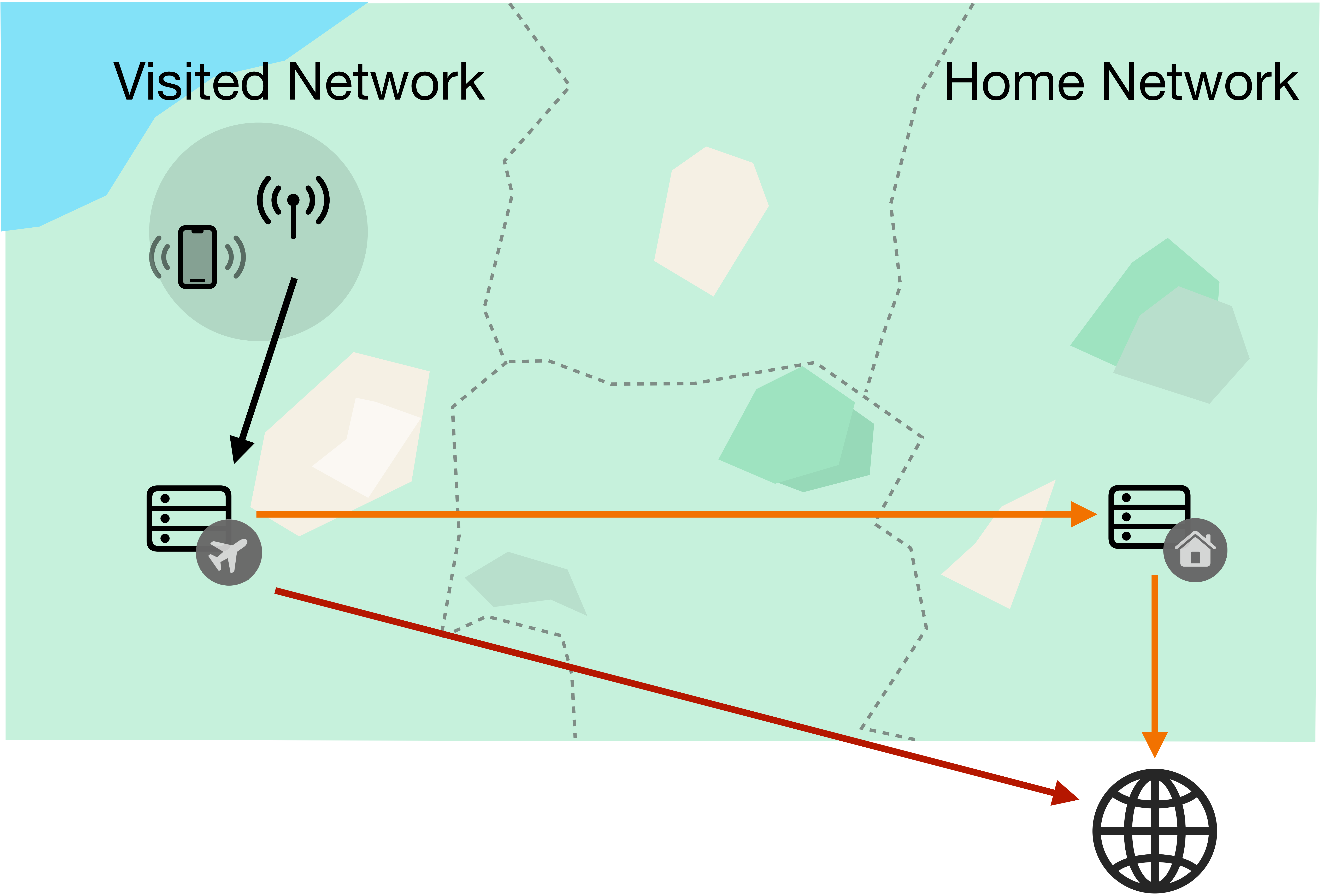
Home Network

Authentication Vector

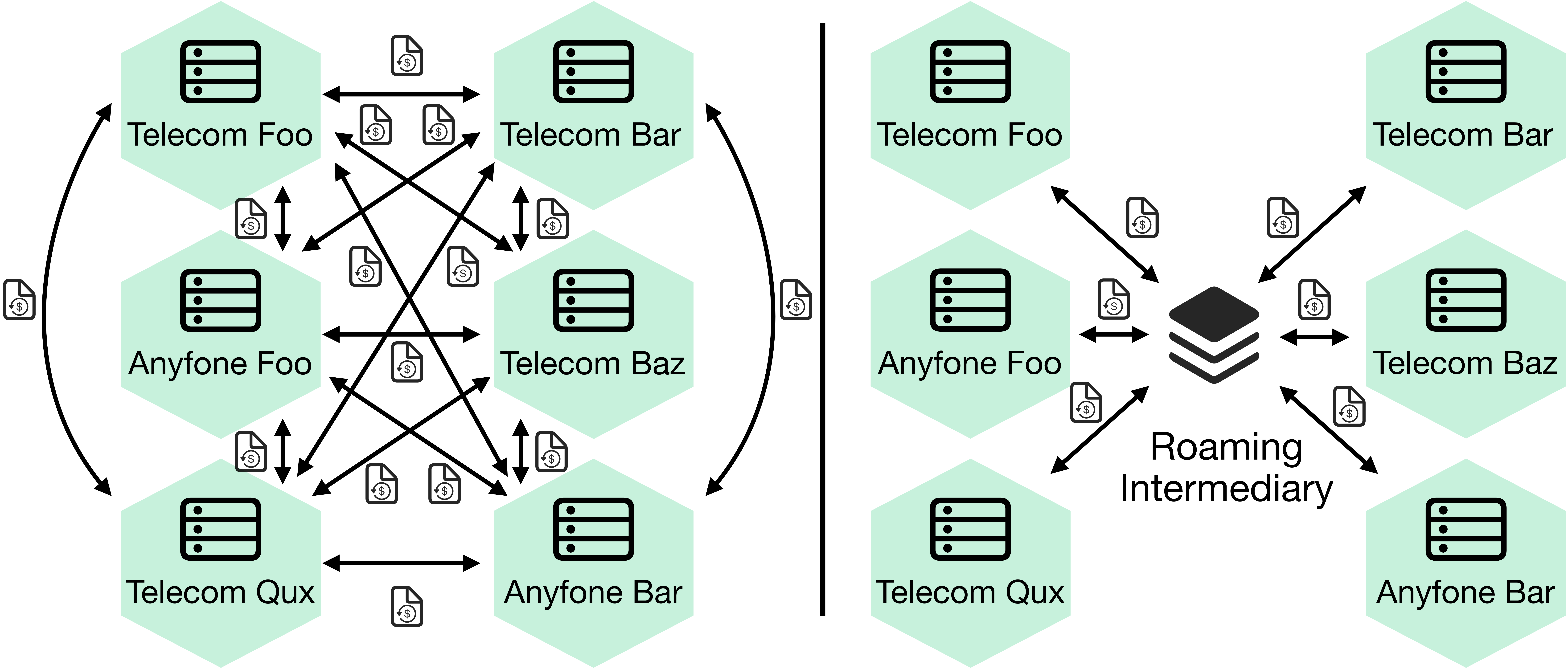
Cannot observe who requested AV, only if on bill 💸

Legit❓👮
→ only grant to roaming partners to ensure billing

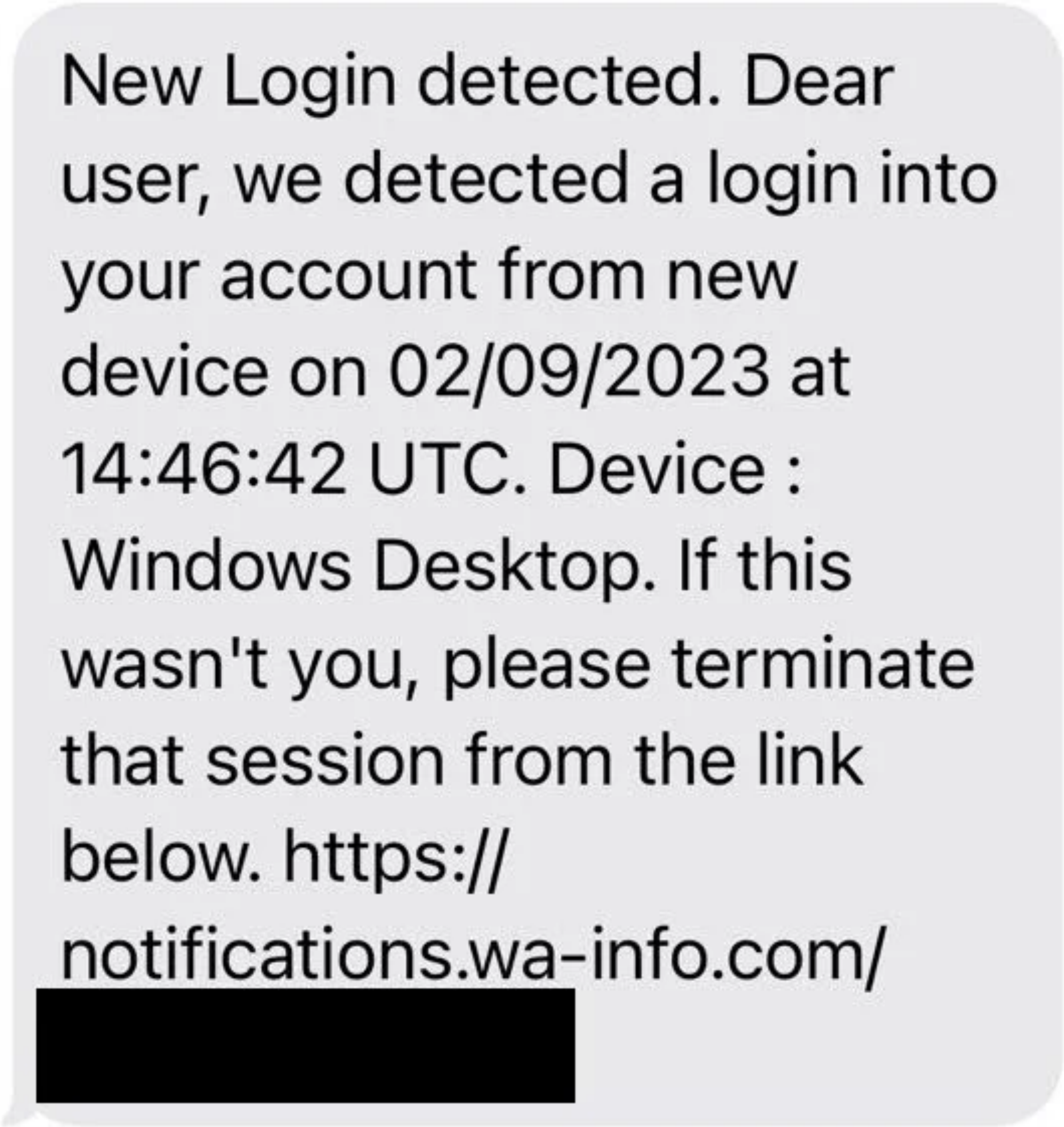
Network Traffic Rerouting



Unclear Roaming Partnerships



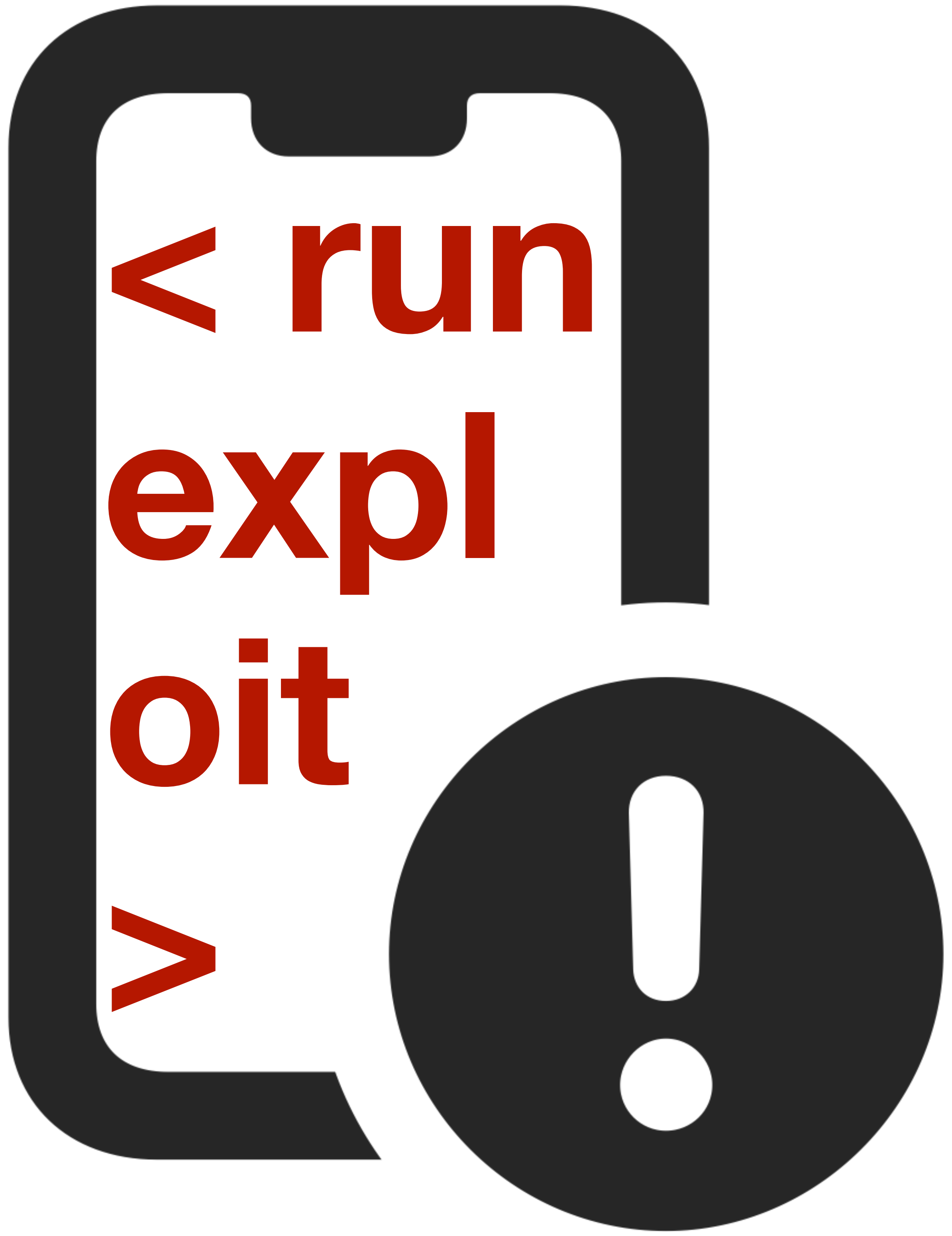
Possible Attacks



New Login detected. Dear user, we detected a login into your account from new device on 02/09/2023 at 14:46:42 UTC. Device : Windows Desktop. If this wasn't you, please terminate that session from the link below. https://notifications.wa-info.com/

[redacted]

Inject SMS

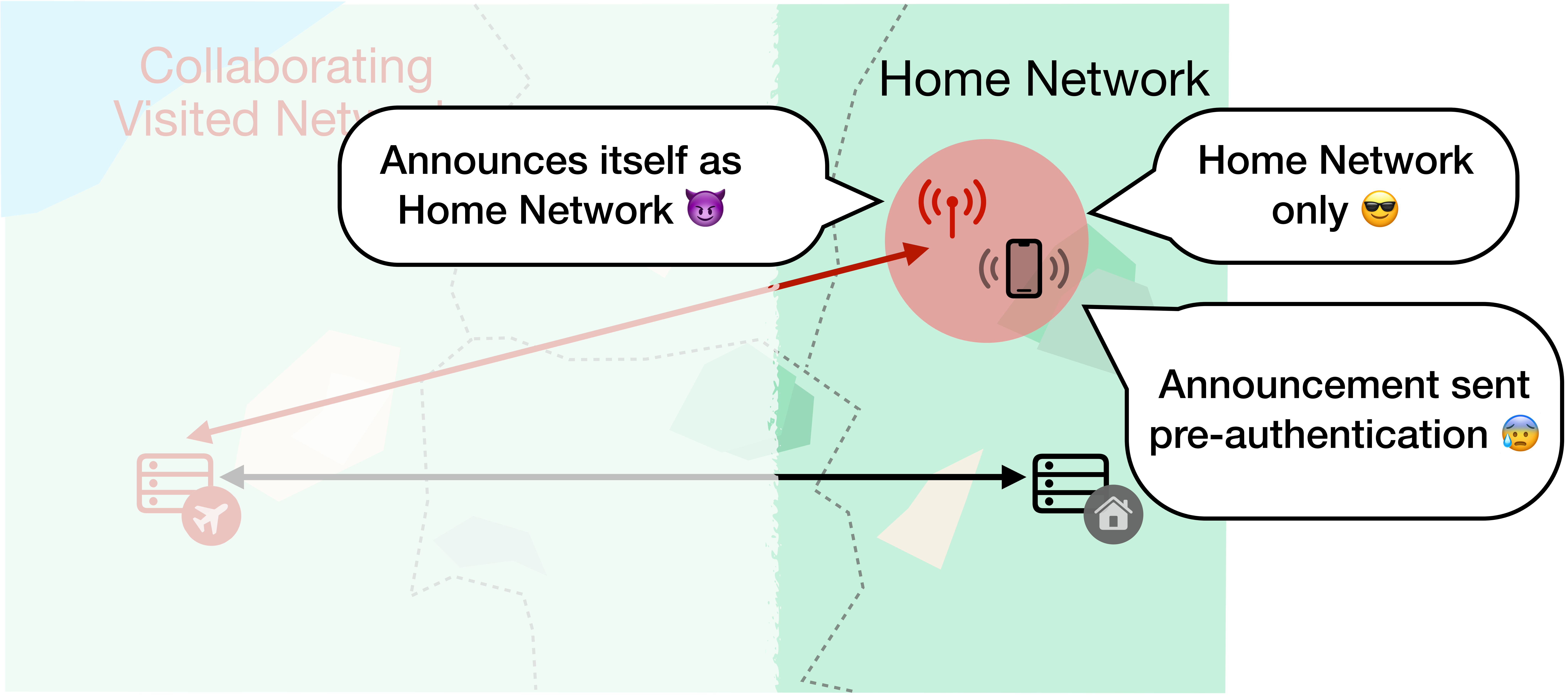


Baseband exploits for Remote Code Execution

https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

Mitigation ?

Turned off Roaming



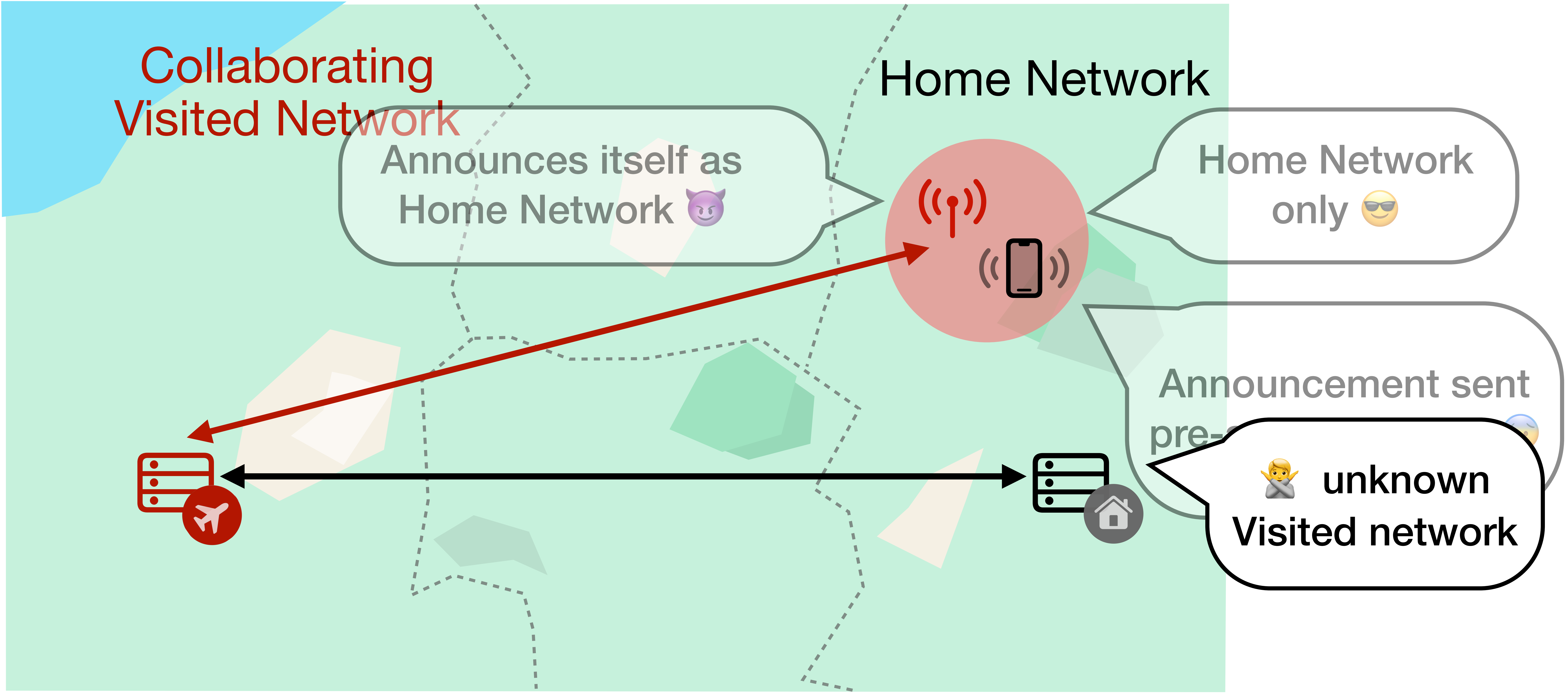
Announces itself as Home Network 😈

Home Network only 😎

Announcement sent pre-authentication 😰

Mitigation ?

Turned off Roaming



Collaborating Visited Network

Home Network

Announces itself as Home Network 😈

Home Network only 😎

Announcement sent pre-

🙅 unknown Visited network

Mitigation ?

Turned off Roaming

Collaborating Visited Network
Home Network
Announces itself as Home Network 😈
Legit & non-roaming ✅
Announcement sent pre-
Legit ✅
wn
work
Poses as Home Network 😈
Roaming Firewall?

Mitigations

End-to-end encryption 🔐

- Rogue Base Stations provide access to decrypted traffic of any connected phone

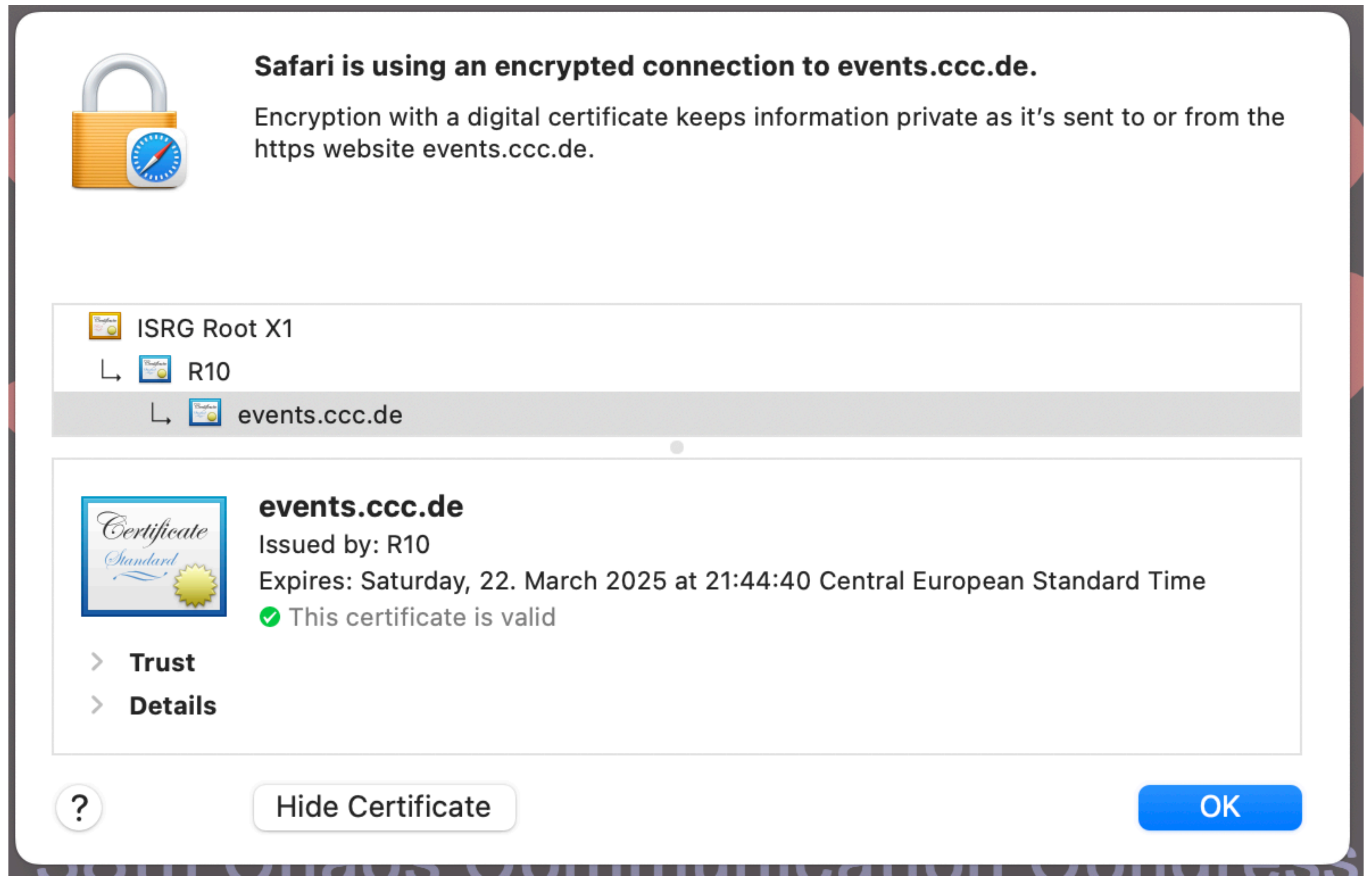
- Could be prevented by end-to-end encryption

- Would disable lawful interception interfaces

Mitigations

Visible Trust Chain

- Trust decision solely taken by core networks
  - Home Network checks identity of Visited Networks and roaming intermediaries ⚠️
- Indicate information used to build trust to user
- Enable user to inspect network properties



Safari is using an encrypted connection to events.ccc.de.

Encryption with a digital certificate keeps information private as it's sent to or from the https website events.ccc.de.

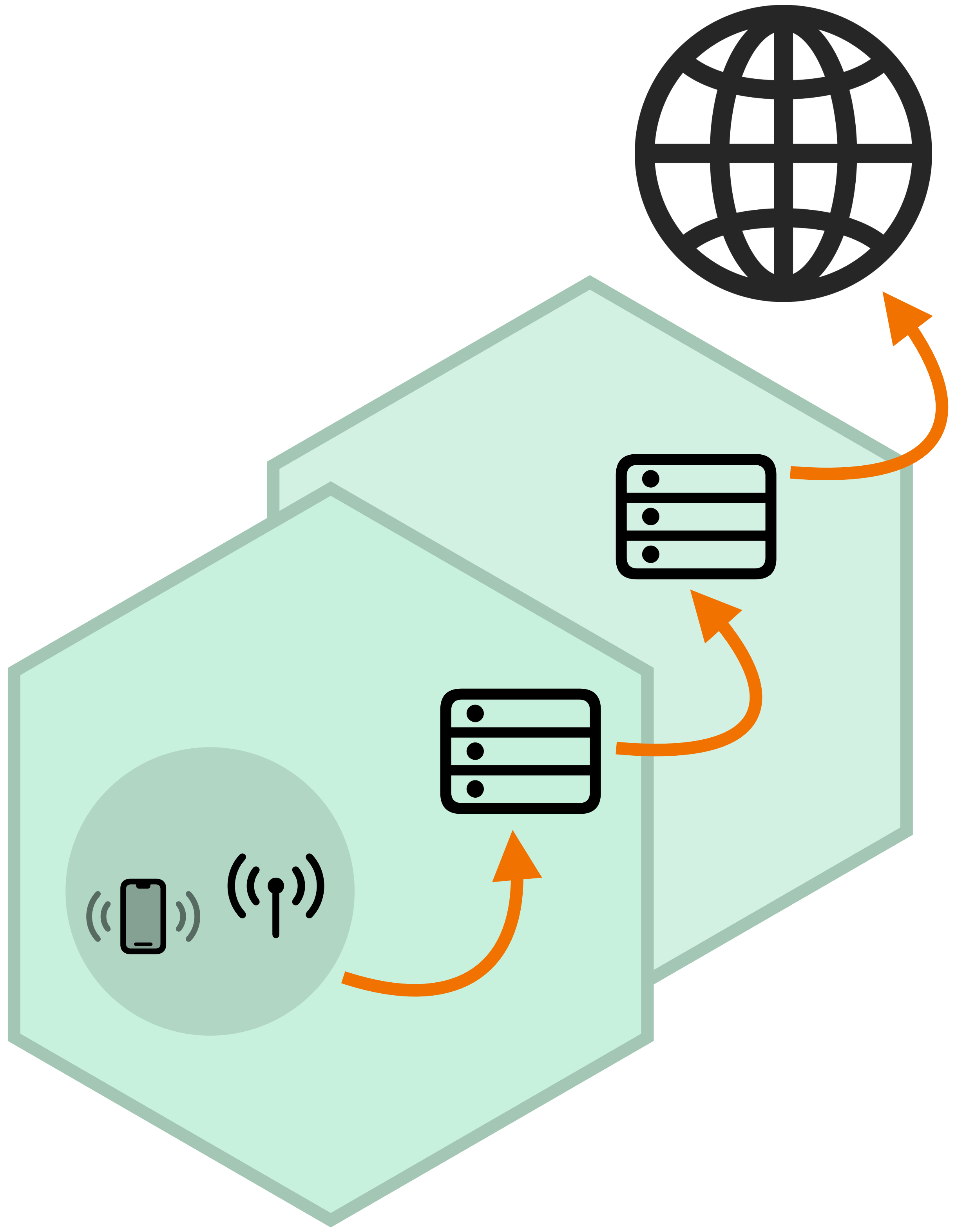
ISRG Root X1
└ R10
└ events.ccc.de

events.ccc.de
Issued by: R10
Expires: Saturday, 22. March 2025 at 21:44:40 Central European Standard Time
✓ This certificate is valid

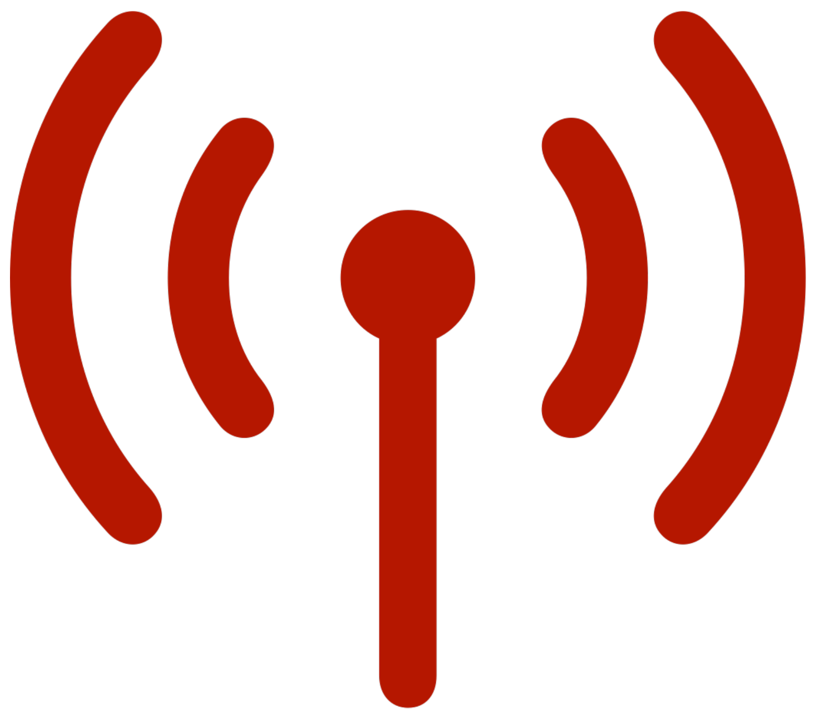
- Changes in specification and phones' interface design

Mitigations

Indicators of Roaming Abuse



Trace routing path

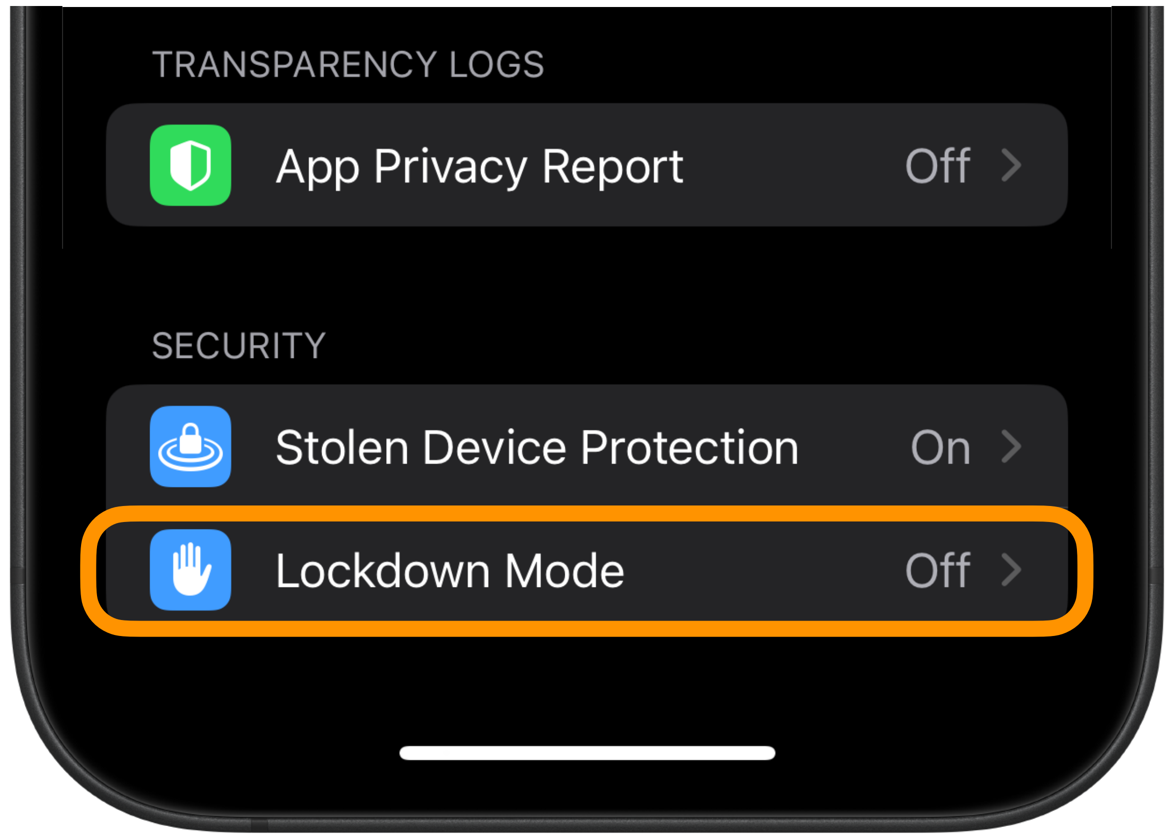


Detect Rogue Base Station

Measure duration of authentication

Mitigations

User's Settings



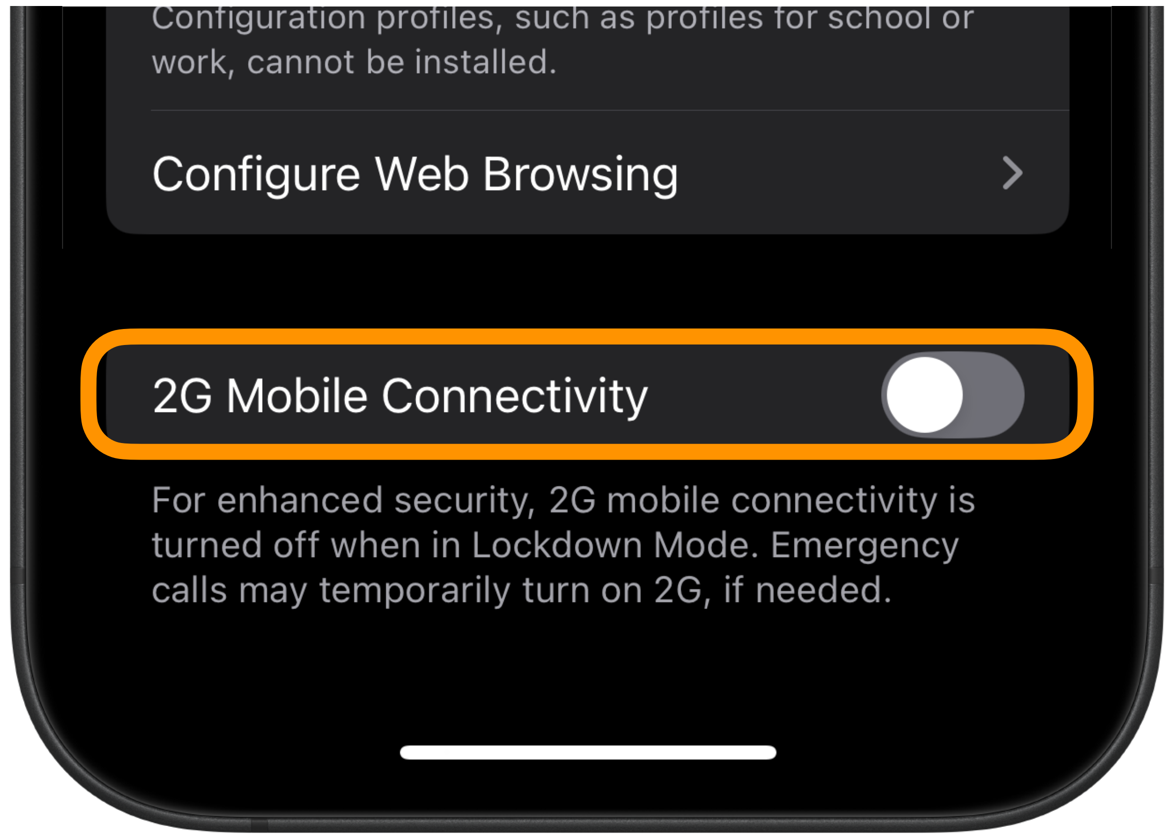
TRANSPARENCY LOGS

App Privacy Report Off

SECURITY

Stolen Device Protection On

Lockdown Mode Off



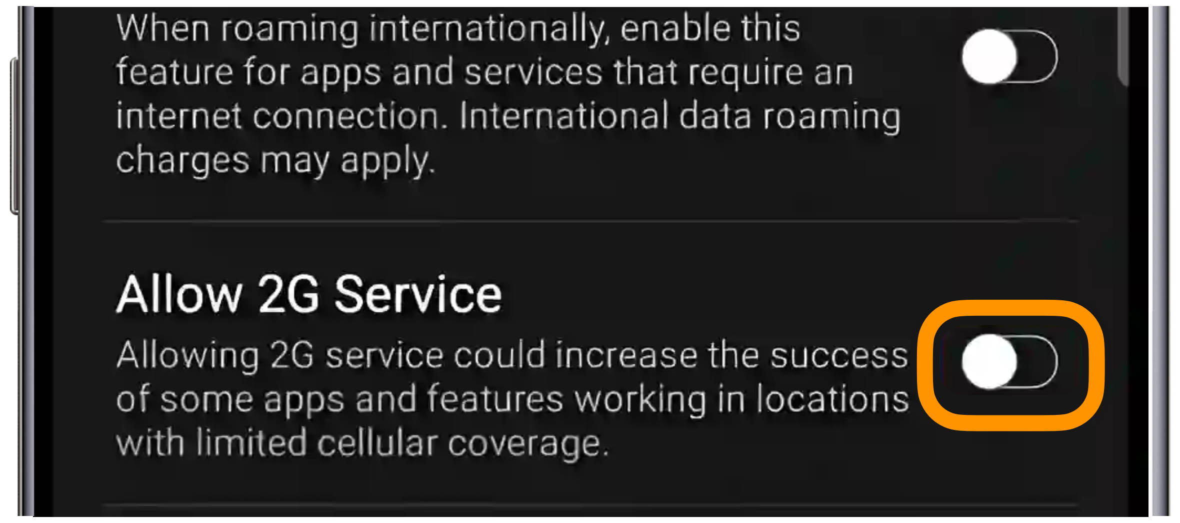
Configuration profiles, such as profiles for school or work, cannot be installed.

Configure Web Browsing

2G Mobile Connectivity

For enhanced security, 2G mobile connectivity is turned off when in Lockdown Mode. Emergency calls may temporarily turn on 2G, if needed.

Settings > Privacy & Security

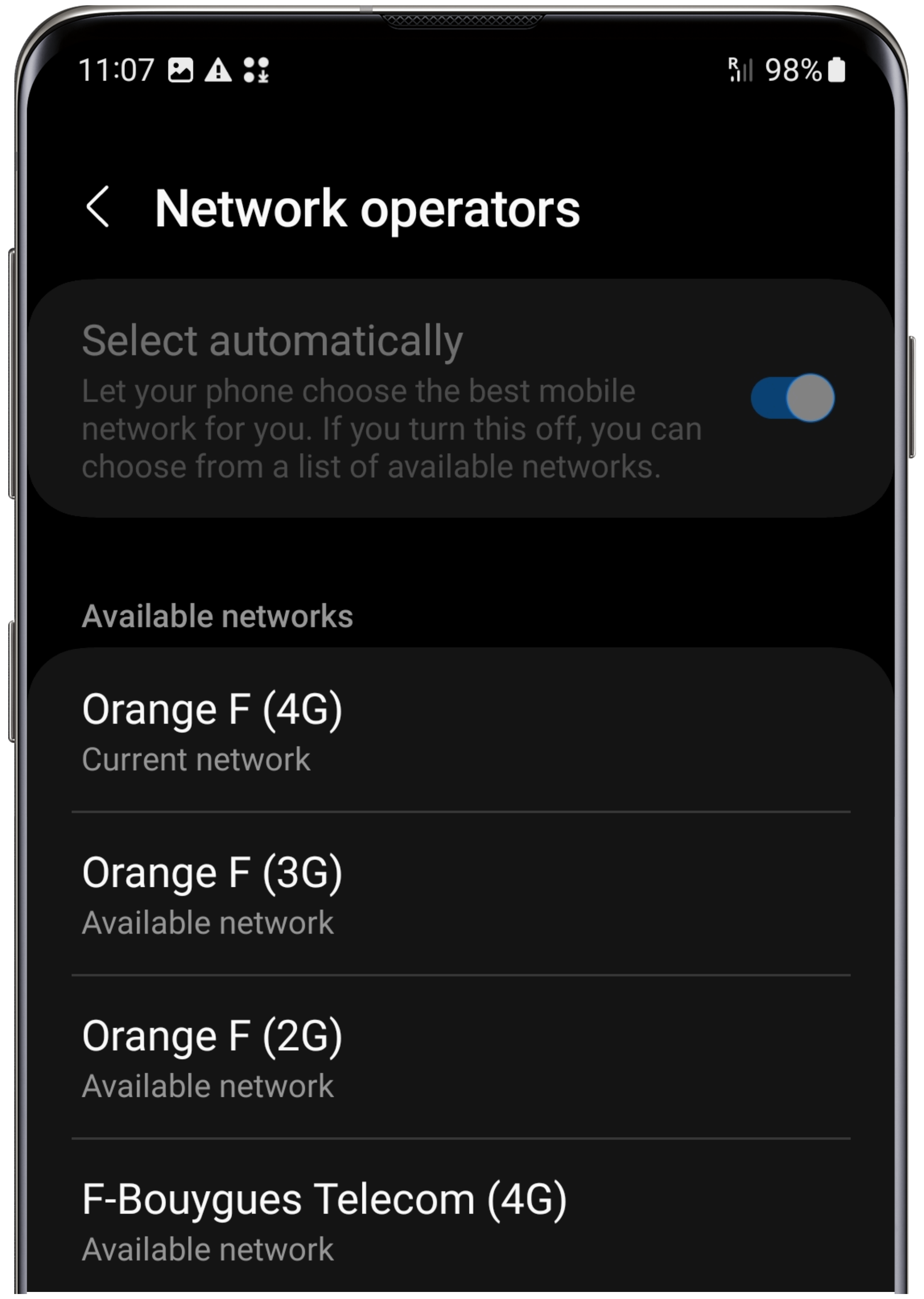


When roaming internationally, enable this feature for apps and services that require an internet connection. International data roaming charges may apply.

Allow 2G Service

Allowing 2G service could increase the success of some apps and features working in locations with limited cellular coverage.

Disable 2G



11:07 98%

Network operators

Select automatically

Let your phone choose the best mobile network for you. If you turn this off, you can choose from a list of available networks.

Available networks

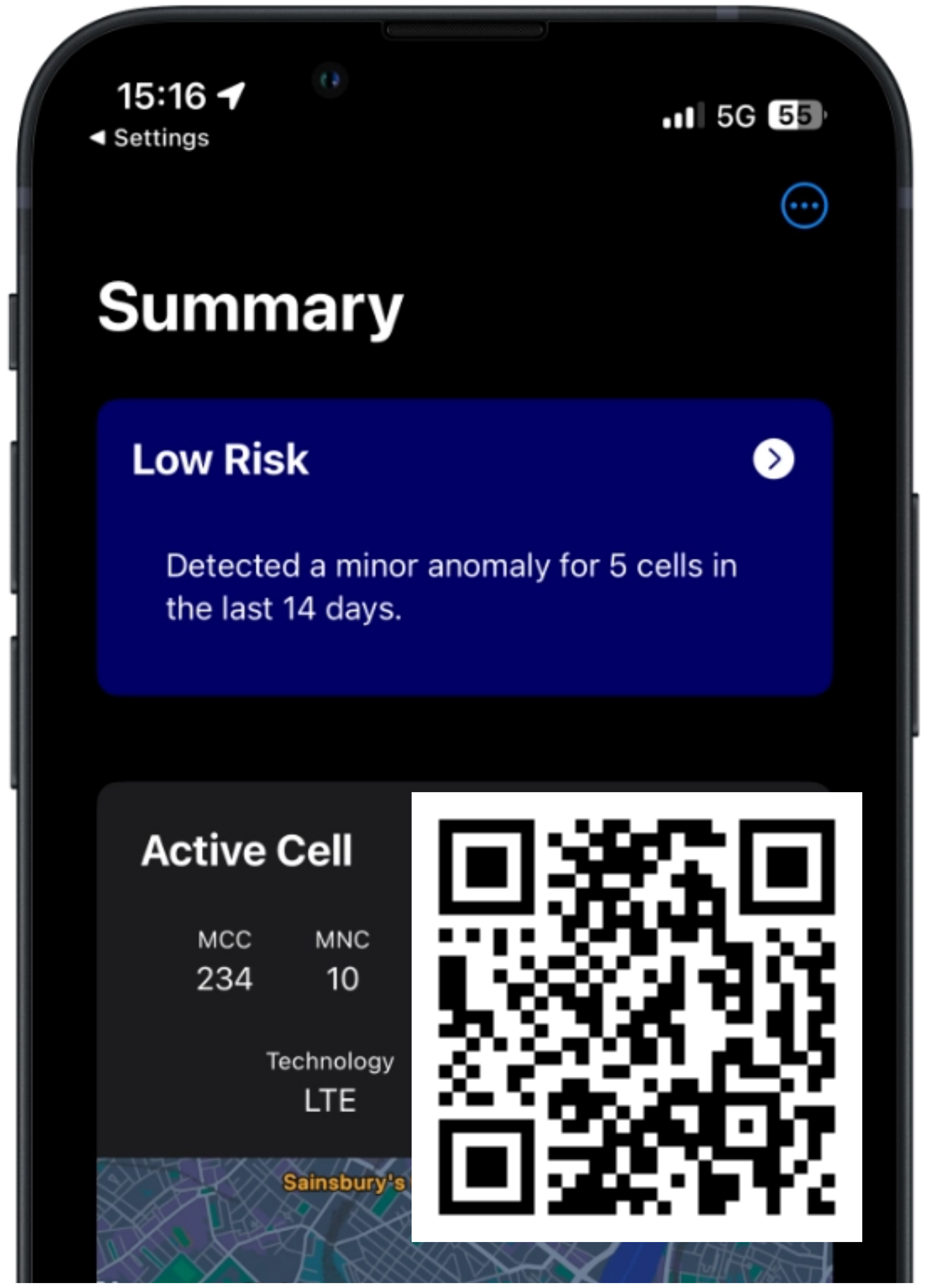
Orange F (4G)
Current network

Orange F (3G)
Available network

Orange F (2G)
Available network

F-Bouygues Telecom (4G)
Available network

Turn off automatic network selection



15:16 ◂ Settings 5G

Summary

Low Risk

Detected a minor anomaly for 5 cells in the last 14 days.

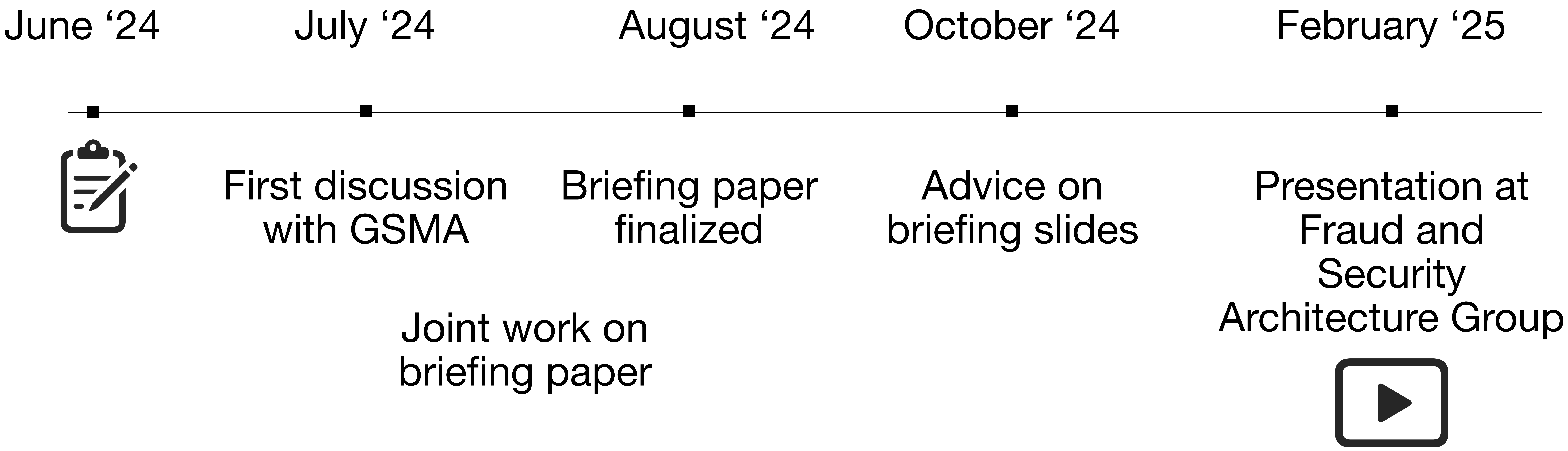
Active Cell

MCC	MNC
234	10

Technology
LTE

Join CellGuard beta test

Disclosure timeline



June ‘24

July ‘24
First discussion with GSMA

Joint work on briefing paper

August ‘24
Briefing paper finalized

October ‘24
Advice on briefing slides

February ‘25
Presentation at Fraud and Security Architecture Group

Roaming Agreements - The Hidden Attack Surface of 5G

Nation-state attackers may abuse 5G to get surveillance capabilities outside of their jurisdiction.

- Difficult for trusted operator to decide if authentication request is legitimate
- Smartphone unable to verify roaming decisions and trust assumptions
- Visited Network can arbitrarily choose network name displayed

Our Paper:

✉ swantje.lange@hpi.de
linkedin.com/in/swantje-lange

Lange, S., Gringoli, F., Hollick, M., Classen, J. (2024). Wherever I May Roam: Stealthy Interception and Injection Attacks Through Roaming Agreements.
In: Garcia-Alfaro, J., Kozik, R., Choraś, M., Katsikas, S. (eds) Computer Security – ESORICS 2024.