MobileAtlas
Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research

Gabriel K. Gegenhuber, Wilfried Mayer, Edgar Weippl, Adrian Dabrowski
Problem and Motivation: Cellular Measurement Platforms

• Lack of large-scale cellular measurement platforms
• Cellular networks differ in terms of measurement requirements
  - (Fixed-line) Internet measurements: RIPE Atlas
  - Mobile networks are complex (Legacy) protocols: E.g., 2G, 3G, OTA updates, SMS, delivery reports, etc.

Complexity vs. security
Problem and Motivation: Cellular Measurement Platforms

- Lack of large-scale cellular measurement platforms
Problem and Motivation: Cellular Measurement Platforms

- Lack of large-scale cellular measurement platforms
- Cellular networks **differ** in terms of **measurement requirements**
  - (Fixed-line) Internet measurements: *RIPE Atlas*
Problem and Motivation: Cellular Measurement Platforms

- Lack of large-scale cellular measurement platforms
- Cellular networks differ in terms of measurement requirements
  - (Fixed-line) Internet measurements: RIPE Atlas
- Mobile networks are complex
  - (Legacy) protocols: E.g., 2G, 3G, OTA updates, SMS, delivery reports, etc.
  - Complexity vs. security
Cellular Measurement Approaches

- **Crowd-based** measurements
  - Smartphone App (e.g., *Wehe*)
  - Pros.: Low economic effort, easy to increase coverage
  - Cons.: Too little control/insights, background activity, user liable for roaming charges

- Dedicated test units
  - Deployed and fully controlled by the test operator (e.g., *MONROE*)
  - Pros.: More control/insights, accurate measurement results
  - Cons.: High setup costs, limited scaling, cumbersome maintenance of test units
Cellular Measurement Approaches

- **Crowd-based** measurements
  - Smartphone App (e.g., Wehe)
    - Pros.: Low economic effort, easy to increase coverage
    - Cons.: Too little control/insights, background activity, user liable for roaming charges

- **Dedicated test units**
  - Deployed and fully controlled by the test operator (e.g., MONROE)
    - Pros.: More control/insights, accurate measurement results
    - Cons.: High setup costs, **limited scaling**, cumbersome maintenance of test units
Platform Requirements

- Scalable, cost-efficient
- Flexible roaming measurements
- Controlled measurement environment
- Versatile measurement capabilities, low-level insights
  - Internet measurements
  - Calling, SMS
  - Billing, APDU analysis
MobileAtlas Measurement Platform

- SIM card limits scaling
  - For each operator one SIM card per test unit is needed
  - Physical remote SIM card switching is cumbersome
MobileAtlas Measurement Platform

- **SIM card limits scaling**
  - For each operator **one SIM card per test unit** is needed
  - Physical remote **SIM card switching** is cumbersome

- **Our approach**
  - Geographically **detach the SIM card from the modem**
    - **Tunneling** the SIM card’s protocol over the Internet
Traditional Approach vs. SIM Tunnel

**Traditional Approach**

Location A

- SIM Card
- Modem

**Decoupling**

Location A

- SIM Card
- SIM Reader

Location B

- Modem
- SIM Emulation
- Measurement Probe

**Internet**

**SIM Tunnel**
Traditional Approach vs. Decoupling

- Simple example:
  - Two countries, four SIM cards
  - Traditional: $2 \times 4 = 8$ SIMs
  - Decoupled: 4 SIMs

- Problem:
  - Increases rapidly
  - E.g., 10 countries => 40 SIMs

Figure 2: Traditional approach with poor scalability: Every new location needs a new set of all SIMs and mobile plans.

Figure 3: Decoupling the station from the SIM via tunneling requires only one set of SIMs.
MobileAtlas Measurement Platform: Components

Management Server

Measurement Probes

Cellular Network AT
MobileAtlas Probe AT

Cellular Network DE
MobileAtlas Probe DE

SIM Providers

WireGuard
VPN

SIM A

SIM B
SIM C
SIM D
MobileAtlas Components: SIM Provider

- SIM provider allows **remote sharing of SIM cards**
  - Measurement probes can **use** the shared cards at **remote locations**
- Various SIM reader types supported
  - PC/SC reader,
  - Serial based SIM card reader,
  - Bluetooth rSAP
    - eSIM support
MobileAtlas Components: Measurement Probe

- Main components (revision 2)
  - Raspberry Pi 4
  - Modem adapter (mPCIe -> USB)
  - Quectel EG25G (same as PinePhone)

- SIM tunneling
  - SIM pins of modem are connected to Raspberry GPIOs
  - UART is used to emulate the SIM

- Ca. $200 hardware cost (+ $100 case)
MobileAtlas Components: Measurement Probe

- SIM Adapter
- GPIO Ports (UART)
MobileAtlas Coverage
Showcase Measurements (Selection)
Platform Coverage and used SIMs

• We obtained SIMs from the major operators of five European countries
  ◦ Austria, Croatia, Romania, Slovakia, Slovenia
  ◦ Total: 14 SIM cards
  ◦ Measured at all available countries and operators
Showcase: Ringback Tone Fingerprinting

- Ringback tone is **issued by the operator** that is **terminating the call**
  - I.e., the **roaming partner**

- **Different ringback tones in different countries**
  - This can be abused to **deduce** the (country-level) **location** of the called person
  - Obvious differences between continents (e.g., US and EU), noticeable differences on country or operator levels
    - Can be used to identify the current operator
    - Potential abuse for SIM swapping attacks (within home country)
Ringback Tone Comparison: 1) RO Vodafone
Ringback Tone Comparison: 2) DE Telekom
Ringback Tone Comparison: 3) DE O2
Showcase: Ringback Tone Fingerprinting

- Amplitude
- Base frequency
- Overtones
- Duty cycle (on/off timing)

Figure 6: Fingerprinting ringback tones (without VoLTE).
Showcase: APDU Analysis

- **SIM card** is an often underestimated microprocessor
  - Can run JAVA cardlets
  - **Proactive** SIM commands: send SMS, display text, etc.
- We have **full insight** into APDU traffic between modem and SIM card
- We found two SIM cards that **covertly send binary SMS** messages to the operator
  - SMS sometimes is billed during roaming
Other Showcases: Internet Measurements

- Network- and Firewall Configuration
  - Home routing, local breakout, CGNAT
- **Billing mechanisms** in domestic and roaming environments
  - Identify **metrics** that are used for **zero-rating**
    - Some metrics (e.g., host/SNI header) can be used for free-riding
- More detailed **zero-rating analysis** can be found in **separate paper**:
  
  *Zero-Rating, One Big Mess: Analyzing Differential Pricing Practices of European MNOs*
Questions?

• Contact us
  ◦ Mail: gabriel.gegenhuber@univie.ac.at, adrian.dabrowski@cispa.de
  ◦ Twitter: @GGegenhuber, @atrox_at

mobileatlas.eu

github.com/sbaresearch/mobile-atlas
Ethical Considerations

- Legal
  - Radio regulatory
  - SIM registration
- Operator
  - Live network influence
  - Economic losses (free-riding tests)
- Probe hoster security
Ongoing Challenges and Future Steps

- Extending coverage
  - Finding probe locations (e.g., at other Universities)
- Extending codebase
  - Automatic measurement scheduling
  - Allowing other researchers to easily use our platform
- 5G probe version
- Probe maintenance
- Doing actual measurements :)

USENIX Security '23