模拟器: 在（微型）预算上的 SIM 追踪

Gabriel K. Gegenhuber
University of Vienna
Faculty of Computer Science
Doctoral School Computer Science
Vienna, Austria

Philipp É. Frenzel
SBA Research
Vienna, Austria

Adrian Dabrowski
University of Applied Sciences
FH Campus Wien
Vienna, Austria

摘要

SIM 跟踪——即检查、修改和转发 SIM 卡与调制解调器之间通信的能力——已成为蜂窝网络研究中一项重要的技术。它使实现关键的安全性和开发相关应用成为可能，例如模糊测试通信接口、提取会话密钥、监控隐藏的 SIM 活动（如主动 SIM 命令或空中更新），并通过重复使用 SIM 卡促进可扩展和分布式的测量平台。传统上，实现这些功能依赖于专门的硬件，这可能会给研究人员带来财务和物流上的负担，尤其是对于那些刚进入该领域的人来说。

在这项工作中，我们展示了使用简单的、广泛可用的组件（如 UART 接口和 GPIO 端口）可以实现完整的 SIM 跟踪功能。我们将这些能力移植到了低成本微控制器上，以 Raspberry Pi Pico（4 USD）为例。与其他方法不同的是，它通过电气上分离 SIM 和调制解调器，并且仅在 APDU 级别传输数据来大幅降低硬件复杂性。

通过大幅降低硬件要求和相关成本，我们旨在使 SIM 跟踪技术为更广泛的科研人员和爱好者社区所接受，促进在蜂窝网络研究中的广泛探索和实验。

CCS Concepts

• **Networks** → **Mobile networks**; **Network measurement**.

Keywords

SIM 追踪，SIM 隧道，蜂窝网络，电信

ACM Reference Format:
Gabriel K. Gegenhuber, Philipp É. Frenzel, and Adrian Dabrowski. 2025. 模拟器: 在（微型）预算上的 SIM 追踪. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025), June 30-July 3, 2025, Arlington, VA, USA*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3734477.3736151

WiSec 2025, June 30-July 3, 2025, Arlington, VA, USA

ACM ISBN 979-8-4007-1530-3/2025/06.
https://doi.org/10.1145/3734477.3736151

1 介绍

检查、重写和中继 SIM 卡通信的能力，也称为 SIM 跟踪，已被证明是蜂窝网络研究人员的重要工具。其中包括：i) 模糊测试通信接口 ~ [5]，ii) 提取会话密钥或观察隐藏的 SIM 卡通信 ~ [2]，以及 iii) 在不同地点复用 SIM 卡（通过 SIM 隧道）来构建可扩展的测量平台 ~ [4, 3]。

尽管这些操作场景已经具备专业设备（例如，Osmocom SIMtrace 2[1]），并非所有研究实验室都能接触到这类专用硬件，从而为那些希望进入蜂窝网络研究领域的研究人员或业余爱好者设置了入门障碍。

与现有项目相比，我们的方法通过使 SIM 隧道的两端在电气上独立来降低复杂性和成本——解耦电压电平、通信速度和时钟域。通信完全在 APDU 级别处理，实现了清晰且模块化的接口。

通过引入 MobileAtlas 测量框架 [4] 用于移动网络中的分布式大规模测量，我们迈出了证明仅需基本硬件（即 UART 接口和 GPIO 端口）就足以实现相同的 SIM 卡追踪功能的第一步。虽然 MobileAtlas 基于 Raspberry Pi 4 提供了一体化的实验解决方案，但许多应用程序只需要其部分功能，特别是 SIM 卡追踪和中继功能。为了推广 SIM 卡追踪并降低入门门槛，我们从 MobileAtlas 概念中分离出来，并将其重新实现在超低成本设备（即 4 USD 的 Raspberry Pi Pico）上，鼓励其他研究人员深入研究这个课题。

2 SIMulator

模拟器 的主要目标是通过利用现成且廉价的硬件来降低 SIM 追踪的成本和准入门槛。基于现有的 MobileAtlas 代码库 [2]，模拟器 减少了 SIM 隧道与测量平台之间的紧密耦合，从而实现更高的模块化和灵活性。为了进一步拓宽潜在应用场景，我们将支持范围扩展到 SIM 卡以外的其他类型接触式智能卡（即 T=0 和 T=1 卡），从而也实现了对支付卡通信的内省和中继（参见附录中的图 5）。

2.1 架构

SIMulator 的架构（图 1）结构如下：

- 一种 A **调制解调器**（或智能手机），其 SIM 卡被模拟。
- 一个**树莓派 Pico** 连接到调制解调器的 SIM 卡槽，以通过 USB 暴露相应的 SIM 接口。

[1]https://osmocom.org/projects/simtrace2/wiki

[2]https://github.com/sbaresearch/mobile-atlas

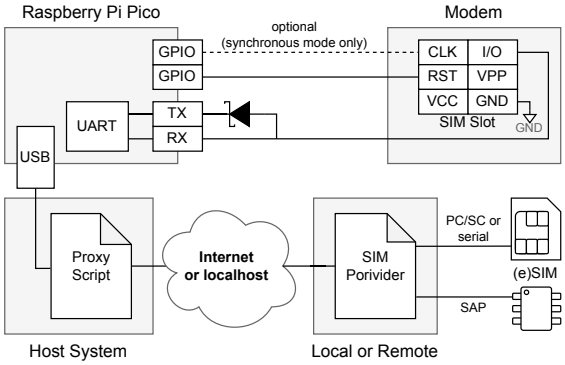

图 1: 我们的微控制器与调制解调器之间的接线图。U(S)ART 输入/输出引脚与肖特基二极管结合，创建了一个开漏双向总线。

- 在主机系统上运行以转发 USB 接口之间的通信**中继脚本**
- 基于 MobileAtlas 的 **SIM 服务提供商**最终通过连接的 SIM 卡或 eSIM 终止 SIM 通信。

这种低成本架构使用廉价且易于获得的硬件实现了完整的 SIM 追踪功能。

解耦架构。保持成本低的关键在于我们的系统相比其他项目降低了复杂性（见表 1）。SIM 卡操作使用不同的电压、时钟速度和分频器，这增加了实现的复杂性。我们的架构通过将 SIM 读取器（连接到 SIM 卡）与 SIM 模拟器（连接到调制解调器）电气隔离来简化这一点，使它们能够独立运行和协商参数，仅交换 APDU 命令。它们也可以托管在通过 TCP 链接的不同机器上。

同步（USART）和异步（UART）模式。Raspberry Pi Pico 在连接到调制解调器时可以有两种工作模式：i) 同步模式，需要额外的电线但能够自动适应不同的时钟（CLK）频率；ii) 异步模式，简化了布线但需要手动一次设置 CLK 频率（基于之前的频率测量，例如使用示波器进行测量，如在 [4] 中所做的）。

完整的 SIM 追踪功能。如表 1 所示，模拟器 支持追踪（即检查）、重写和中继 SIM 卡和调制解调器之间发送的 APDU 命令。与现有解决方案相比，它以显著降低的成本提供了更高的灵活性。

启用模拟器 的 eSIM。除了支持物理 SIM 卡（例如，通过 PC/SC 或超便宜的基于串行的读卡器），我们还实现了对 SIM 访问配置文件（SAP）[1] 的支持，这是一种旧式协议，用于较旧的汽车，可在选定的 Android 智能手机上使用（例如，Google Pixel 设备）。SAP 允许我们的 SIM 提供商请求直接（APDU 级别）访问智能手机的 SIM 卡之一，包括 eSIM。

通过在智能手机上将 eSIM 保持离体状态，也可以检查应用程序控制的 eSIM。例如，这类应用程序可能在每次边境过境时用一个新的（国内）IMSI 或整个 eSIM 来替换原有的，从而消除漫游（如主要市场中的 Google Fi）。相比之下，使用嵌入 eSIM IC 的物理 SIM 卡进行变通的方法一旦从原手机中取出便无法即时更新。

2.2 评估

我们成功使用了七种不同的调制解调器（Quectel RM520N-GL、Quectel RM500Q、Quectel EG25-G、华为 ME909s-120、Telit LE910、SIMCom SIM7600E-H 和 Sierra MC8355）以及四种不同的智能卡终端对模拟器 进行了评估。在所有情况下，APDU 检查、重写和中继功能在同步和异步模式下都可靠地工作。

SIM 隧道传输本质上引入了往返延迟。我们实现了 ISO 7816 等待时间扩展（WTX）来应对这些高延迟情况。我们在多个运营商上进行了测试，并人工加入了 1,000 毫秒的延迟，观察到没有失败或性能下降的情况。因此，该系统也适用于通过卫星互联网连接隧道传输 SIM 卡通信。

3 结论

在这项工作中，我们介绍了模拟器，这是一个轻量级且成本效益高的 SIM 追踪平台，显著降低了研究人员的入门门槛。通过仅依赖价格仅为 4 美元的现成组件，我们将先进的 SIM 追踪功能提供给更广泛的受众。项目 [3] 的开源性质进一步鼓励了研究社区的重复使用、适应和扩展。展望未来，我们设想将模拟器 扩展到完整的 SIM 虚拟化（例如，在 [5] 中所做的那样），无需物理 SIM 卡即可实现对 SIM 功能的完全仿真。

[3]https://github.com/sbaresearch/mobile-atlas#simulator

	SIMtrace 2	SIM Interposer*	模拟器
Approx. Price	120 USD	4 USD	4 USD
APDU Inspection	✓	×	✓
APDU Rewriting	✓	✓	✓
APDU Relaying	✓	×	✓
Android eSIM	×	×	✓
Galvanic Separation	(✓)†	×	✓

* 被 [5] 使用，例如。https://turbosim.cn/collections/heicard † 可能有两个单位。

表 1: SIM 内省和中继工具的能力比较。设备的所有成本，不含电缆。

References

[1] 2003. Bluetooth SIM Access Profile Specification. Tech. rep. 3GPP.

[2] Sreepriya Chalakkal, Henrik Schmidt, and Shinjo Park. 2017. Practical Attacks on VoLTE and VoWiFi. *ERNW Enno Rey Netzwerke, Tech. Rep.*

[3] Gabriel K. Gegenhuber, Wilfried Mayer, and Edgar Weippl. 2022. Zero-Rating, One Big Mess: Analyzing Differential Pricing Practices of European MNOs. In *IEEE Global Communications Conference (GLOBECOM).*

[4] Gabriel K. Gegenhuber, Wilfried Mayer, Edgar Weippl, and Adrian Dabrowski. 2023. MobileAtlas: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research. In *USENIX Security 23.*

[5] Tomasz Piotr Lisowski, Merlin Chlosta, Jinjin Wang, and Marius Muench. 2024. SIMurai: Slicing Through the Complexity of SIM Card Security Research. In *USENIX Security 24.*

致谢

我们想感谢 Fabian Funder 在模拟器 上的实际工作。

SBA Research (SBA-K1 NGC) 是 COMET 中心之一，位于 COMET —— 优秀技术卓越中心计划内，并由 BMIMI、BMWET 和维也纳联邦州资助。COMET 计划由 FFG 管理。

图 2: 低成本的 SIM 卡读取设备（基于 PC/SC 或串行接口），这些设备受到 MobileAtlas 基础 SIM 提供程序的支持。

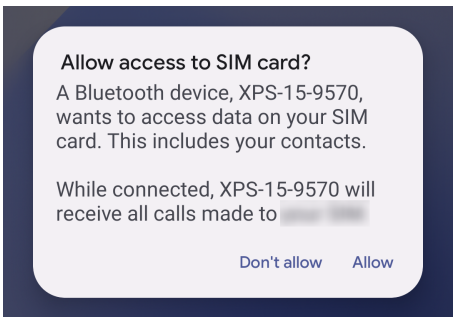

图 3: 除了图 2 中展示的 SIM 卡读取设备外，我们还通过 Android 的（远程）SIM 访问配置文件支持 eSIM，该配置文件可以通过蓝牙进行访问。

A 附录

A.1 支持的 SIM 卡读取设备

A.2 将 Pico 连接到手柄和智能卡终端

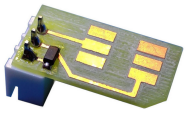

图 4: 虽然可以使用临时焊接来连接调制解调器或智能手机的 SIM 卡插槽，但我们还开发了一种与各种调制解调器适配器兼容的 SIM 卡适配器 PCB。

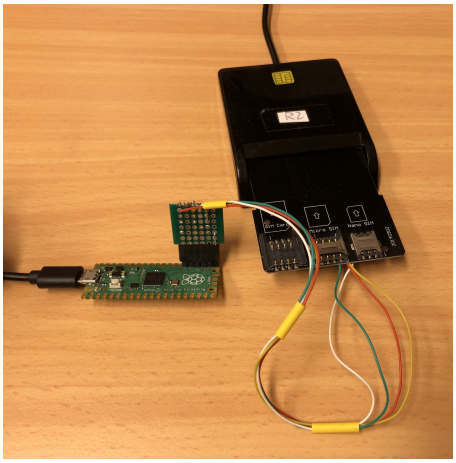

图 5: 除了在蜂窝领域中的应用外，我们的解决方案支持 T=1 协议，从而与常规的接触式智能卡（如支付卡）兼容。

SIMulator: SIM Tracing on a (Pico-)Budget

Gabriel K. Gegenhuber, Philipp É. Frenzel (University of Vienna & SBA Research), Adrian Dabrwoski (FH Campus Wien)

```
GSM SIM     67    ISO/IEC 7816-4 SELECT /EF.ICCID
GSM SIM     98    ISO/IEC 7816-4 GET RESPONSE
GSM SIM     75    ISO/IEC 7816-4 READ BINARY Offset=0
GSM SIM     67    ISO/IEC 7816-4 SELECT File EF.ELP
GSM SIM     98    ISO/IEC 7816-4 GET RESPONSE
GSM SIM     75    ISO/IEC 7816-4 READ BINARY Offset=0
GSM SIM     95    ETSI TS 102.221 TERMINAL PROFILE
```

Problem & Motivation

- Inspecting, rewriting and relaying **SIM card communication** (i.e., *SIM tracing*) can be used to
  - extract session keys or observe hidden SIM card communication,
  - fuzz communication interfaces,
  - reuse SIM cards at different locations.
- Professional equipment (e.g. the Osmocom SIMtrace 2) is **not available in every research lab**.
- The *MobileAtlas* measurement framework introduced an approach to **emulate a SIM card using basic hardware** (i.e., a serial UART interface).
  - SIM card communication is tunneled over the Internet (geographic decoupling of modem and SIM).
  - Allows flexible SIM card switching and reuse within all deployed measurement probes.

Previous Work: MobileAtlas

mobileatlas.eu

The measurement framework can be structured into three components:

- **SIM providers** that allow sharing SIM card access,
- **measurement probes** that act as a local breakout to the cellular network, and
- a **management server**, that connects the prior two components and acts as command and control unit for the measurement probes.

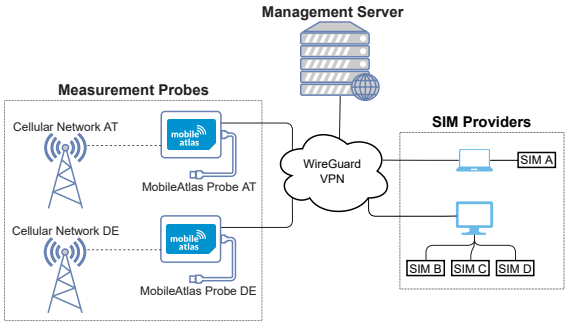

Figure 1: Our architecture allows every probe to use SIM cards attached to SIM providers, independent from the geographical location of probe and SIM card.

We can dynamically form a **virtual circuit** between any SIM card and measurement probe by connecting them **remotely** via a **SIM tunnel**. This boosts the **scalability** and **flexibility** of the measurement platform and allows easy measurements of **roaming** scenarios.

SIMulator: Goals

- **Lower cost and entry barrier** for SIM tracing.
  - Using **easily available hardware**.
- Leverage the existing *MobileAtlas* codebase.
  - **Reduce coupling** between SIM tunnel and measurement platform.
  - Add support for other smartcard types (e.g. T=0, T=1).
  - Achieve broader modem (or smartphone) support.

SIMulator: Architecture

SIMulator consists of three parts:

- The **cellular modem** for which the SIM card is emulated.
- A **Raspberry Pi Pico** connected to the modem's SIM slot, providing access to the modem's SIM interface via USB.
- A **relaying script** running on a host system forwarding communication between the USB interface and a *MobileAtlas* SIM provider.

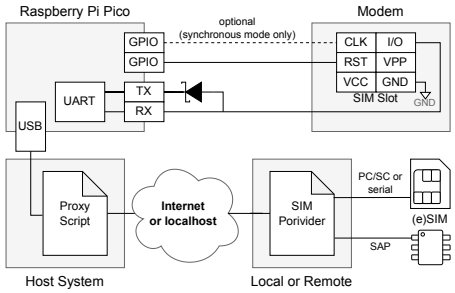

Figure 2: Our low-cost architecture supports full SIM tracing capabilities.

The Raspberry Pi Pico can either be used in synchronous- (UART), or in asynchronous (USART) mode:

- The **synchronous mode** requires an extra wire, but automatically adapts to different CLK frequencies.
- The **asynchronous mode** requires manually setting the CLK frequency.

Conclusion

- SIMulator **considerably lowers the entry barrier** for SIM tracing.
  - Only using readily available components for **less than 5 USD**.
  - **Open-source** development allows reuse by other researchers.
- Exposing the modem's SIM interface via USB **enables novel** SIM relaying- and inspection **applications**.
  - E.g., using multiple SIM tunnels and modems on one host system.
- Future work: **SIM virtualization** to achieve full emulation capabilities (i.e., without SIM provider).

Gabriel K. Gegenhuber, Wilfried Mayer, Edgar Weippl, and Adrian Dabrowski. MobileAtlas: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research. In *32nd USENIX Security Symposium*, 2023.

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.