UNIVERSITY OF BIRMINGHAM

Fuzzware

ARTIFACT EVALUATED USENIX AVAILABLE

ARTIFACT EVALUATED USENIX FUNCTIONAL

ARTIFACT EVALUATED USENIX REPRODUCED



CATana



On the *Dangers* of *SIM*-Originating *AT* Commands



Tomasz Lisowski

University of Birmingham



Kristian Covic

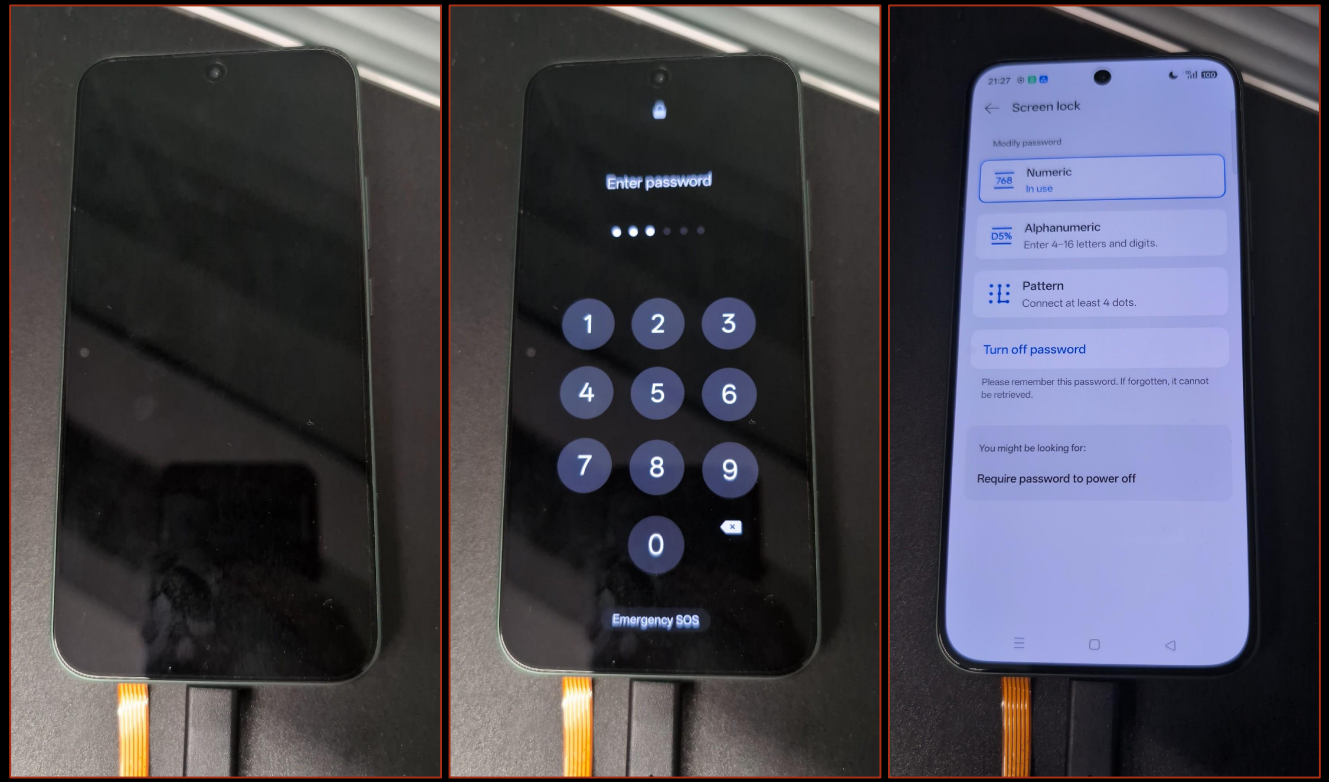
Fuzzware



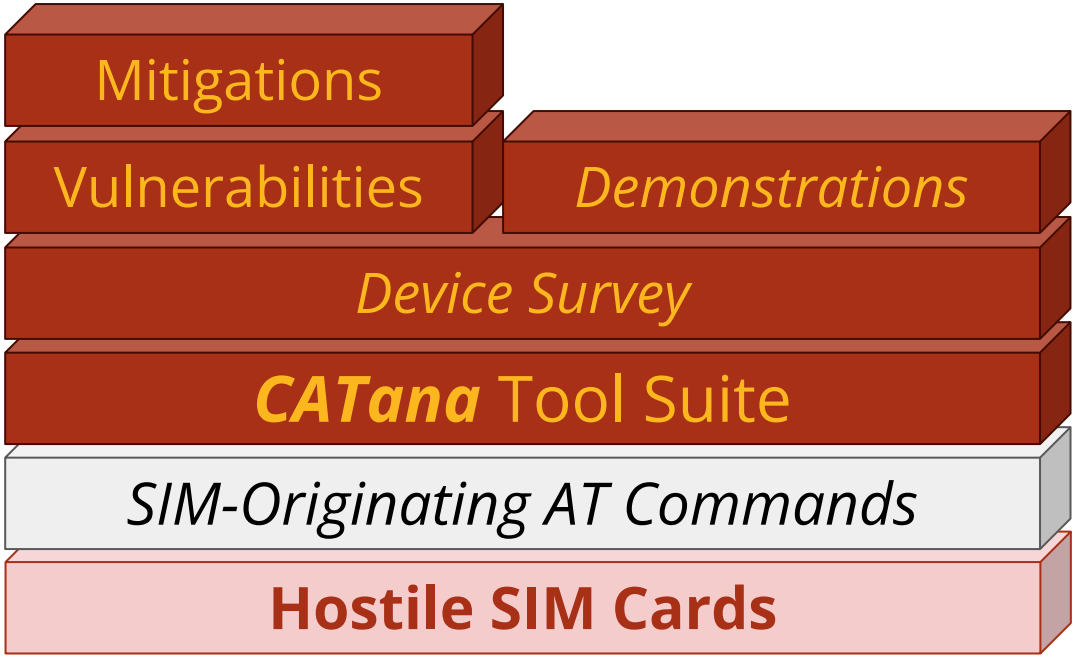
Marius Muench

University of Birmingham

PIN? Fingerprint? Face unlock? *SIM unlock*



Summary

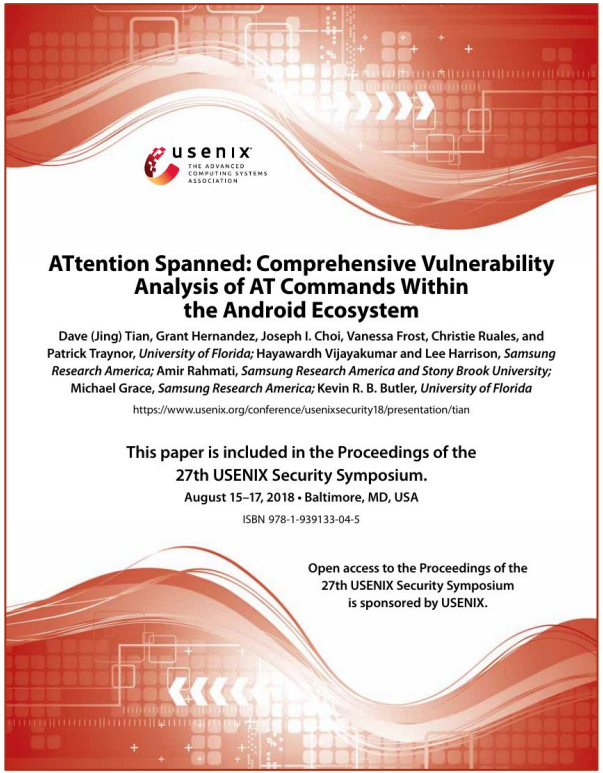

Mitigations
Vulnerabilities
Demonstrations
Device Survey
CATana Tool Suite
SIM-Originating AT Commands
Hostile SIM Cards

Background

AT Commands

- Modem *configuration* commands
- Command and response are *strings*
- Around since 1980s
- Still implemented today

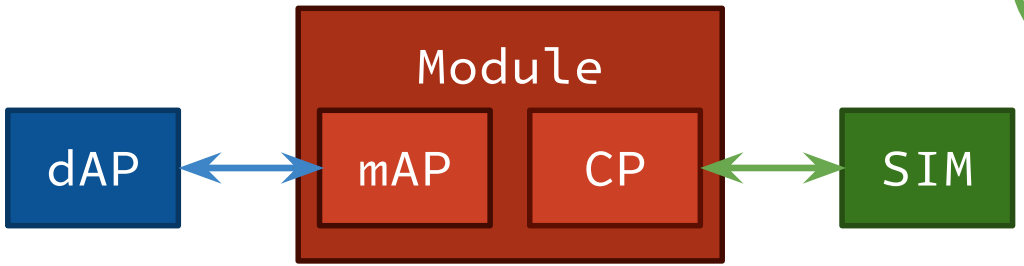
- AT commands are a known risk
- Lots of (potentially) buggy parsers
- Many phones do not expose it over USB by default (anymore)

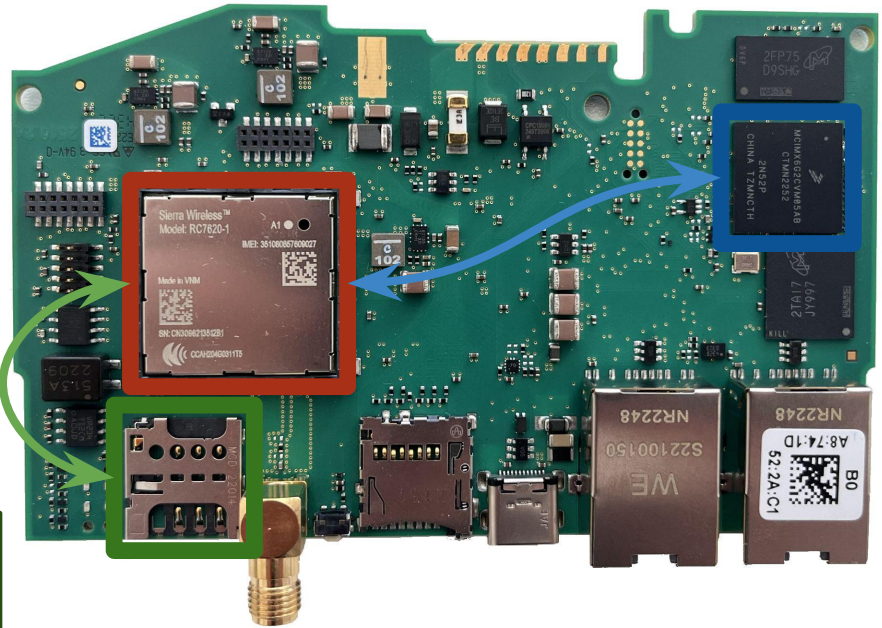


SIM Card Interface

- “Terminal” sends commands.
- SIM sends responses.

Typical Embedded Modem Architecture:

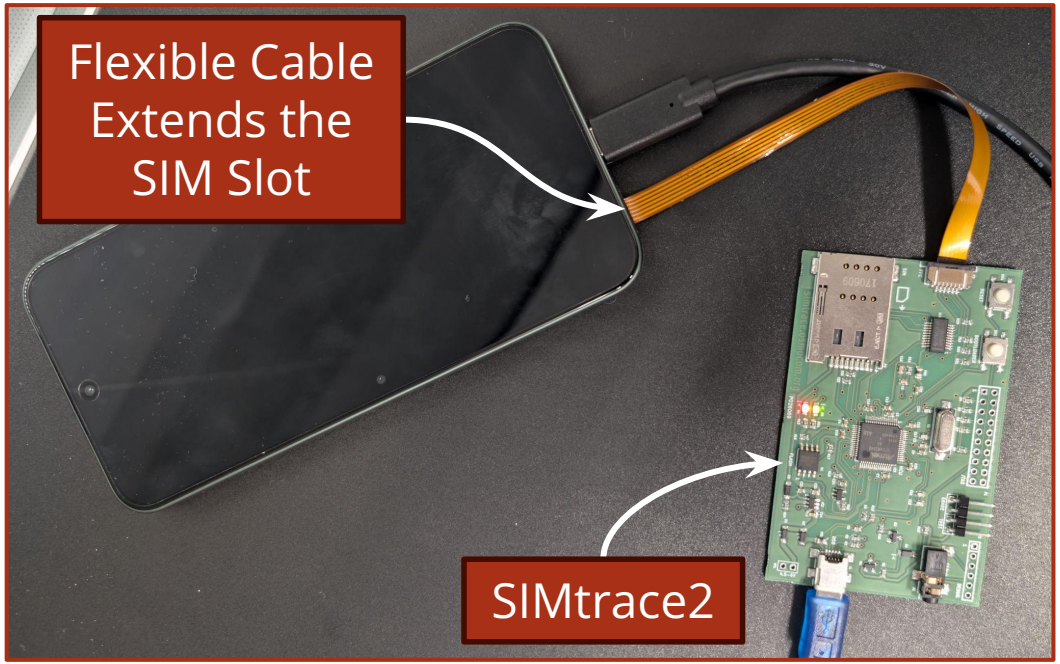




Software Research SIM

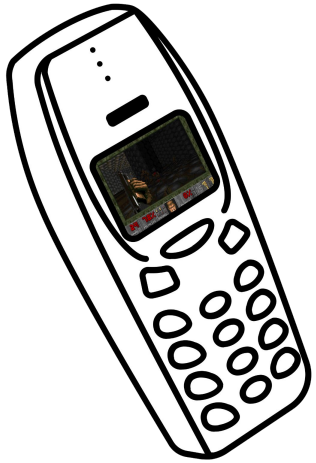
- A SIM card emulator is practical
- We use: ***swSIM*** [1]

1. ***swSIM*** runs on the host
2. *SIMtrace2* bridges the host and the SIM slot
3. Target recognizes our SIM



[1] SIMurai: Slicing Through the Complexity of SIM Card Security Research

SIM AT Commands



STATUS

"Proactive command is present"

FETCH

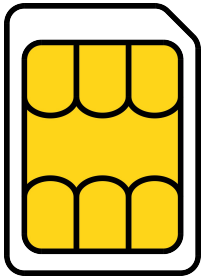
RUN AT Proactive Command

TERMINAL RESPONSE (Status Code)

ACK

ENVELOPE (AT Response String)

ACK

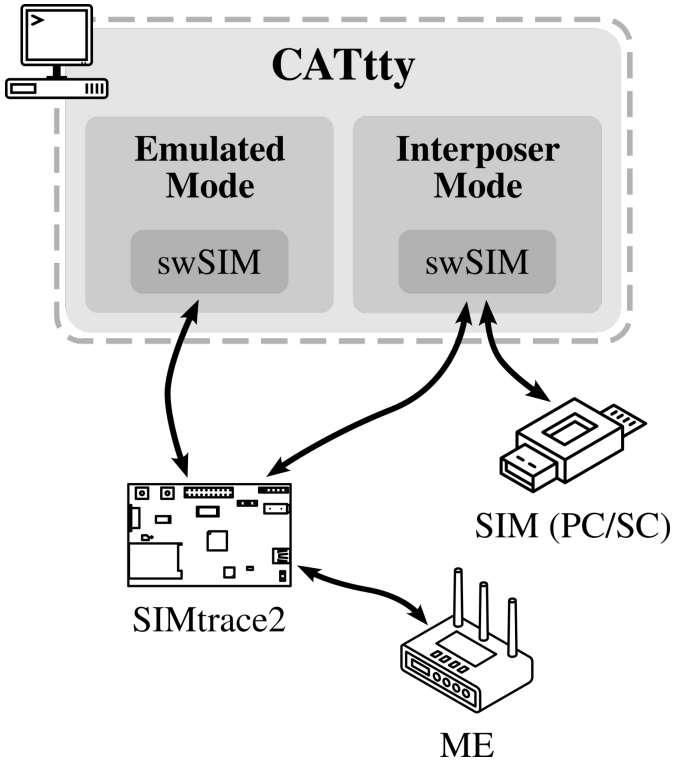


CATana Tool Suite

CATtty

- *CLI* tool to issue AT commands *interactively* using *swSIM*

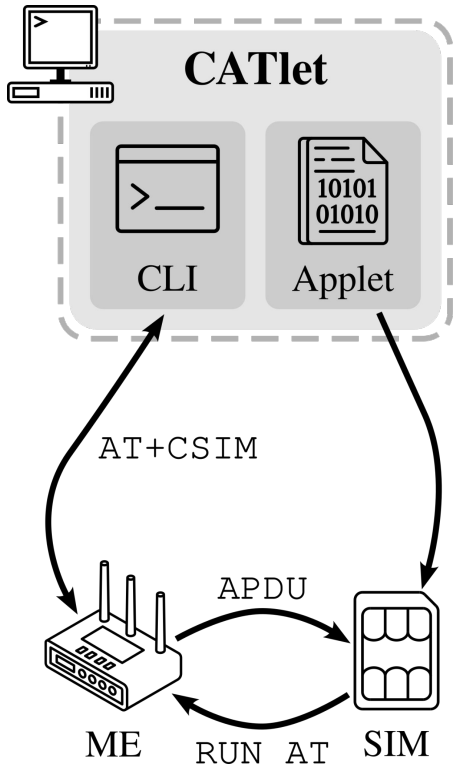
- CATtty extends swSIM with *interposing* capabilities
- Real cards can be *transparently forwarded*



CATlet

- Plug-n-Play experience without SIMtrace2
- Simpler to deploy

- Control the SIM applet with a CLI and an auxiliary AT interface

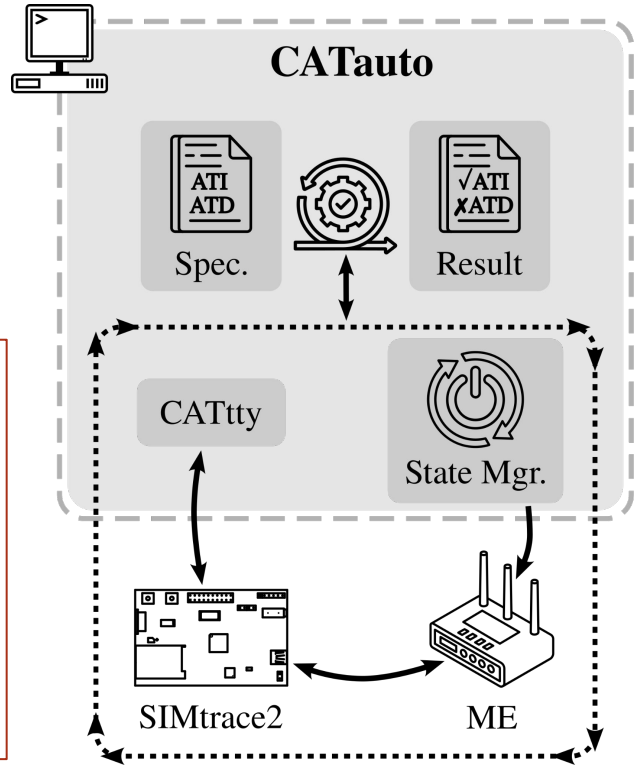


CATauto

- Automate CATtty
- Test *thousands* of AT commands
- *Survey the attack surface*

```
=== CATauto time__epoch_ns=1769372790624709831 ===

[0] time=1769372790625102382 cmd.len=8 cmd="AT$CCLK?"
[0] time=1769372850384140487 res.len=100 res="810300340...
[1] time=1769372851423454274 cmd.len=8 cmd="AT$CR10?"
[1] time=1769372906830475106 res.len=46 res="8103003400...
[2] time=1769372907872298069 cmd.len=7 cmd="AT$CSQ?"
[2] time=1769372963423614730 res.len=102 res="810300340...
[3] time=1769372964465728173 cmd.len=12 cmd="AT$QCACQDBC?"
[3] time=1769373020837001979 res.len=46 res="8103003400...
[4] time=1769373021892908401 cmd.len=10 cmd="AT$QCAPNE?"
```



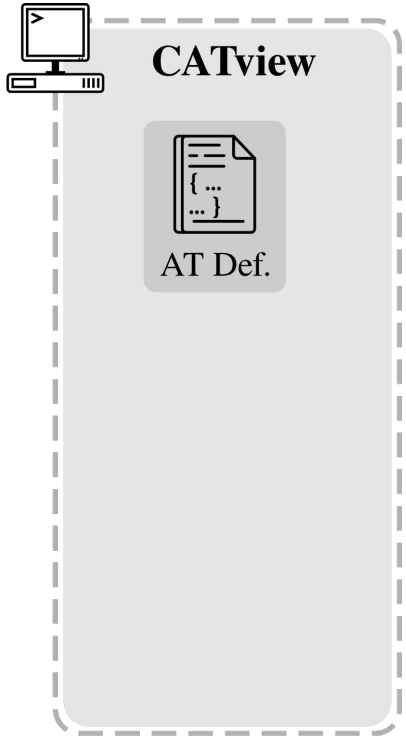
CATview

- Human- readable JSON from CATauto outputs

CATview

- Human- readable JS
  from CATauto outpu

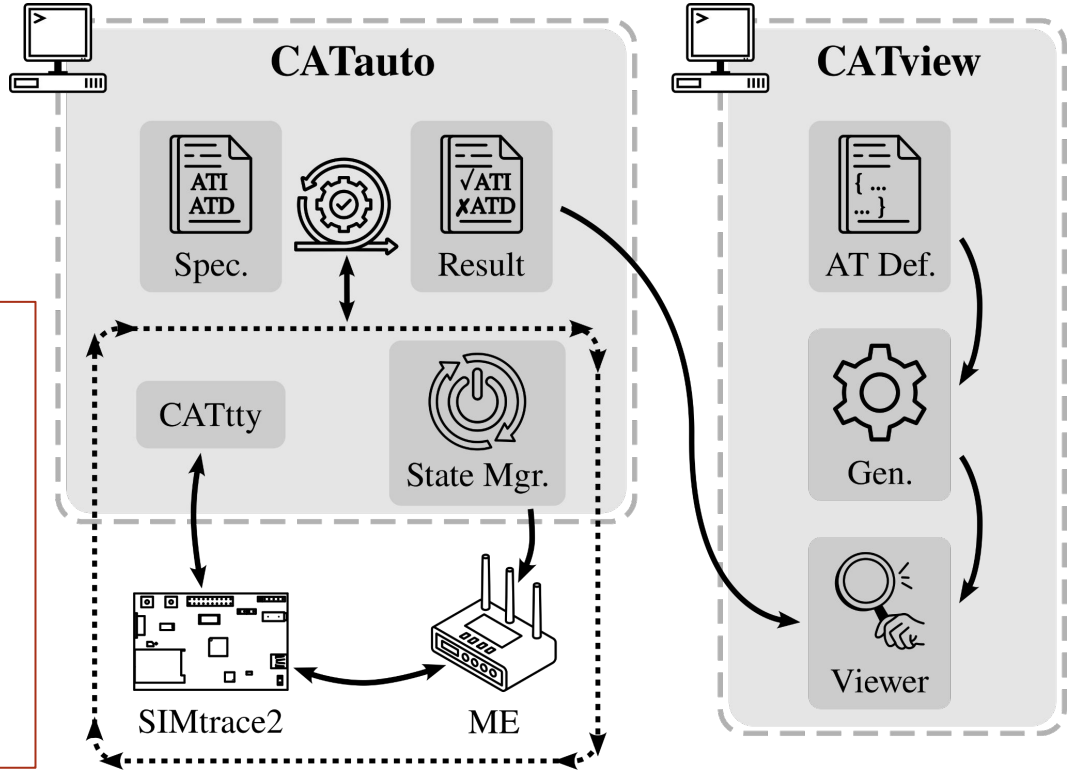

```
"title": "Available AT Commands",
"description": "Execution command causes the MT...
"base": "AT+CLAC",
"variant": [
 {
  "description": "Test",
  "suffix": "=?",
  "argument": []
 },
 {
  "description": "Execute",
  "suffix": "",
  "argument": []
 }
],
"comment": "Clause 8.8."
```

CATview

- Human- readable JSON from CATauto outputs

```
"title": "List Available AT Commands",
"description": "AT$QCCLAC is used to list all...
"base": "AT$QCCLAC",
"variant": [
 {
  "suffix": "?",
  "response": [
   "\r\n&C\r\n&D\r\n&E\r\n&F\r\n&S\r\n&V\r\n&W\r\n
  ]
 },
```



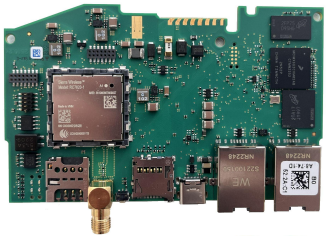
Equipping the CATana

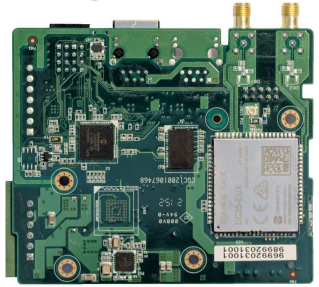
Research Questions

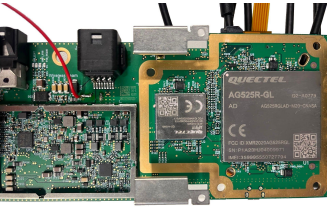
1. Is SIM AT present in modern devices?

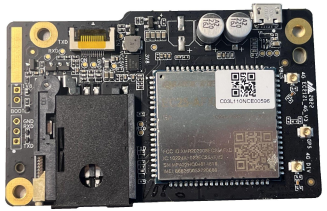
2. How dangerous is the SIM AT attack surface?
    a. We scratch the surface.
    b. The attack surface is large.

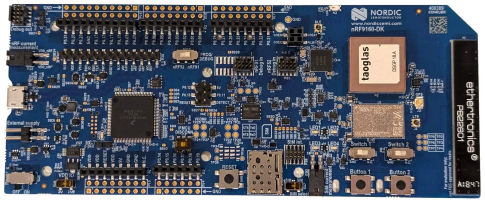
Device Survey









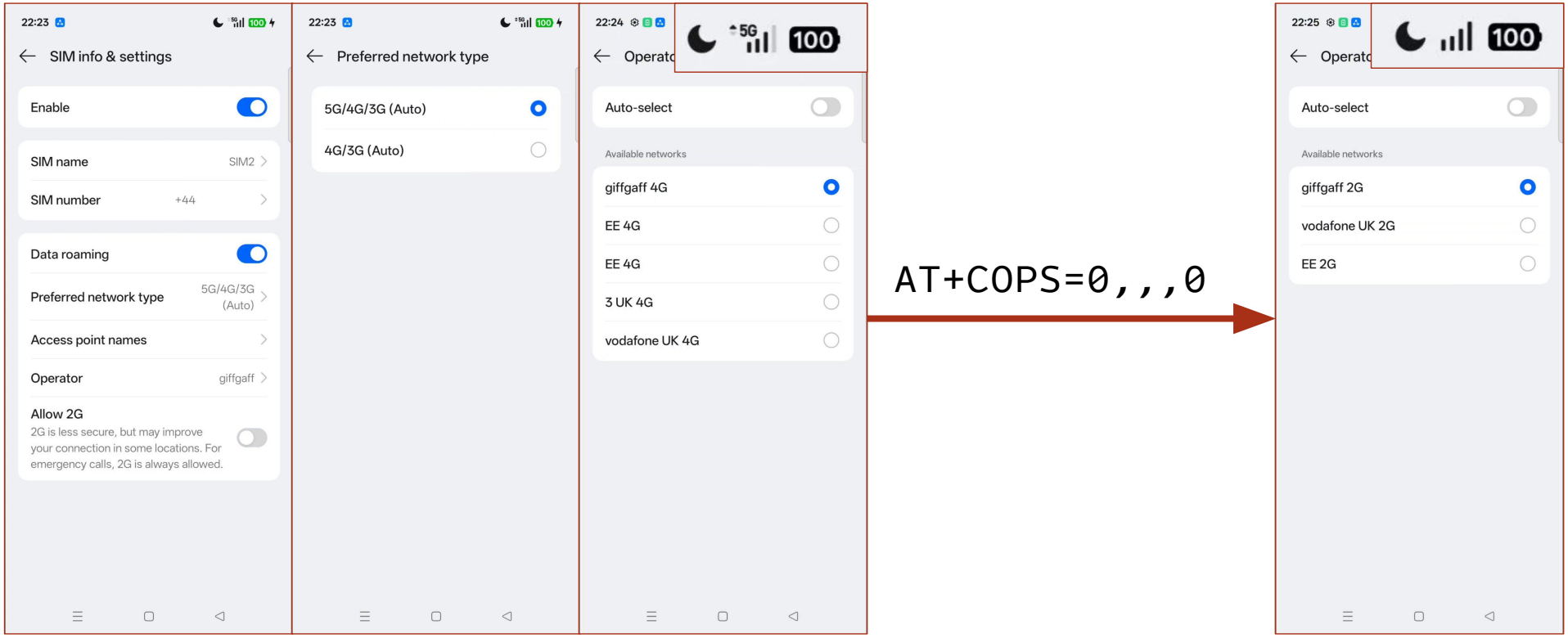


- We surveyed 26 devices: *18 phones*, *8 embedded*
- Embedded modems used in: *Payment terminals*, *cars*, *car chargers*, *IoT* devices, …

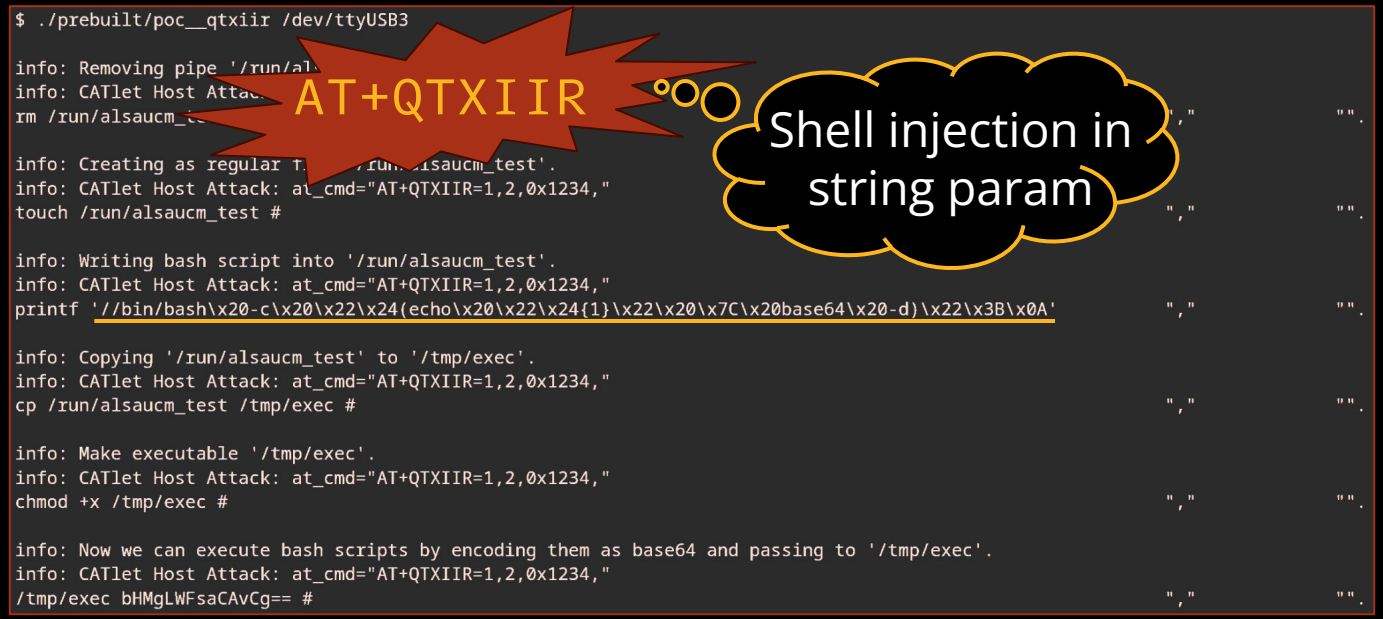
SIM AT Supported
OPPO Find X5
OPPO Reno14 F 5G
Asus Zenfone 9
Quectel EC25-AFX
Quectel EC25-EUX
Quectel EC25-G
Quectel RM520N-GL
Quectel AG525R-GL
Sierra Wireless RC7620

SIM AT Unsupported
Apple iPhone 15
Apple iPhone 16e
Google Pixel 7
Google Pixel 9
Motorola One Vision
Motorola One G32
OnePlus 5T
OnePlus Nord CE 2
Samsung Galaxy A14
Samsung Galaxy A72
Samsung Galaxy S22
Samsung Galaxy Z Flip6
Huawei P40 Lite
Oukitel C19
ZTE Blade A54
Nordic nRF9160-DK
Simcom SIM800C

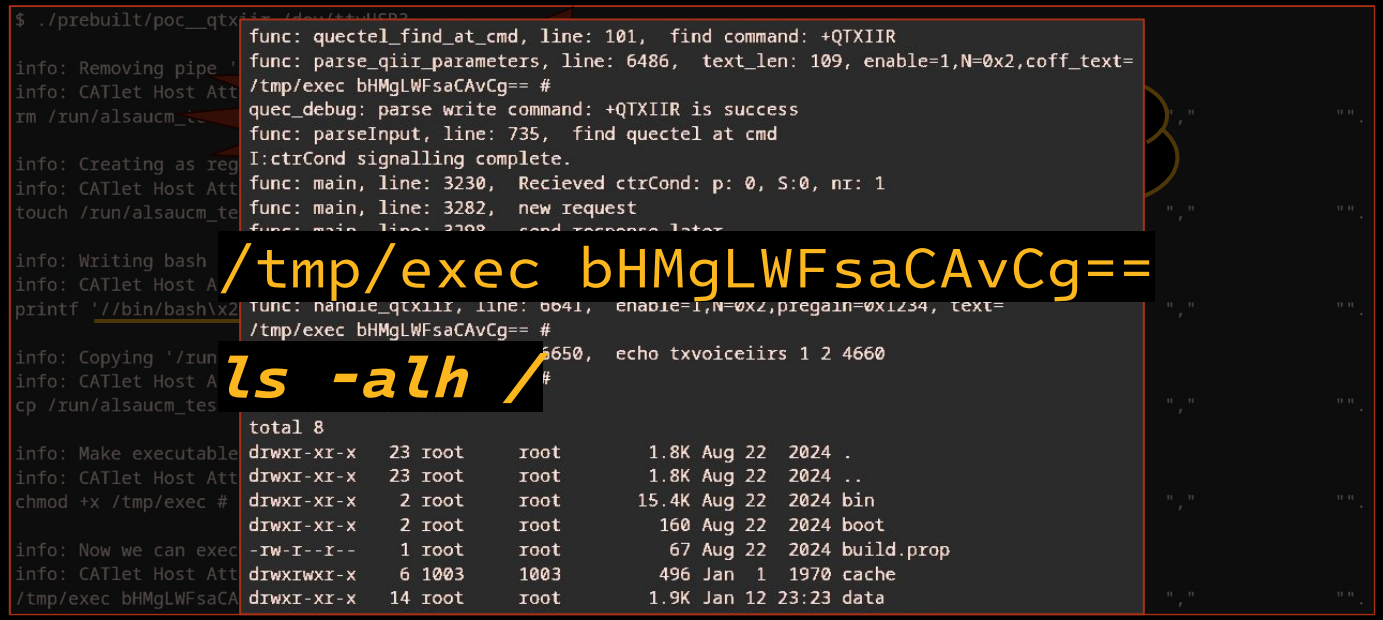
Vuln: *2G Downgrade*



Vuln: *Code Execution (Quectel EC25)*



Vuln: *Code Execution (Quectel EC25)*



Mitigations

- Qualcomm:
  Default hardened configuration for vendors
- Quectel:
  Removed the SIM AT interface and fixed vulnerabilities
- Sierra Wireless:
  Plan to ***Mainline*** the Qualcomm patch
- GSMA:
  CVD ***panel agreed*** + will **inform *3GPP & ETSI*** of the findings

Questions?



https://www.usenix.org/conference/woot26/presentation/lisowski

Paper



https://doi.org/10.5281/zenodo.21843736

Artifact

Summary

- ***CATana*** tool suite for exploring the *SIM AT interface*
- 4 vulnerabilities
- 26 devices surveyed
- Qualcomm disabled SIM AT by default on vendor configs
- Quectel removed SIM AT