



UNIVERSITY OF  
BIRMINGHAM



CISPA

HELMHOLTZ CENTER FOR  
INFORMATION SECURITY



# SIMurai: Slicing Through the Complexity of SIM Card Security Research



**Tomasz Lisowski**

University of Birmingham



**Jinjin Wang**

University of Birmingham



**Merlin Chlosta**

CISPA Helmholtz Center  
for Information Security



**Marius Muench**

University of Birmingham

```
t swsim_init(swsim_st *const swsim_st
char const *const path_j
nset(swsim_state, 0U, sizeof(*swsim_s
nset(swicc_state, 0U, sizeof(*swicc_s
cc_state->userdata = swsim_state;
```

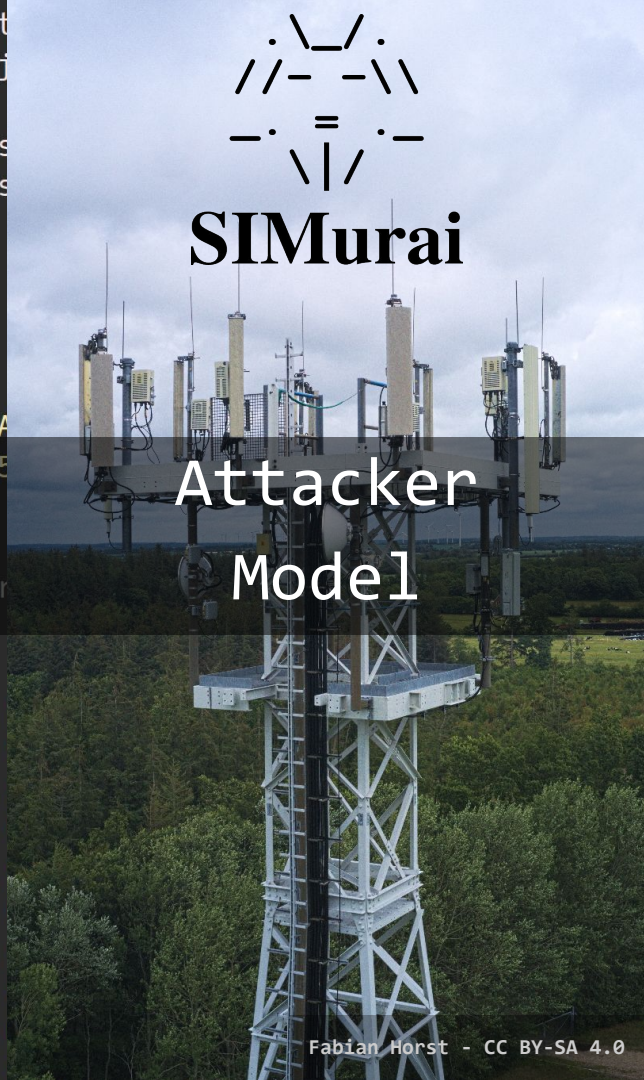
```
milenage_st milenage_init = {
.op_present = false,
.op_c = {0xA6, 0x4A, 0x50, 0x7A
0xB4, 0x21, 0x01, 0x35
```

# SIM Card Emulator

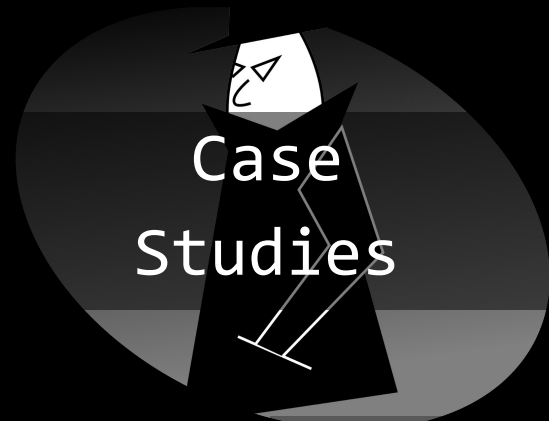


## SIMurai

# Attacker Model



Fabian Horst - CC BY-SA 4.0



# Case Studies

Setreset - CC BY-SA 3.0

CVE-2024-27209: Send SMS

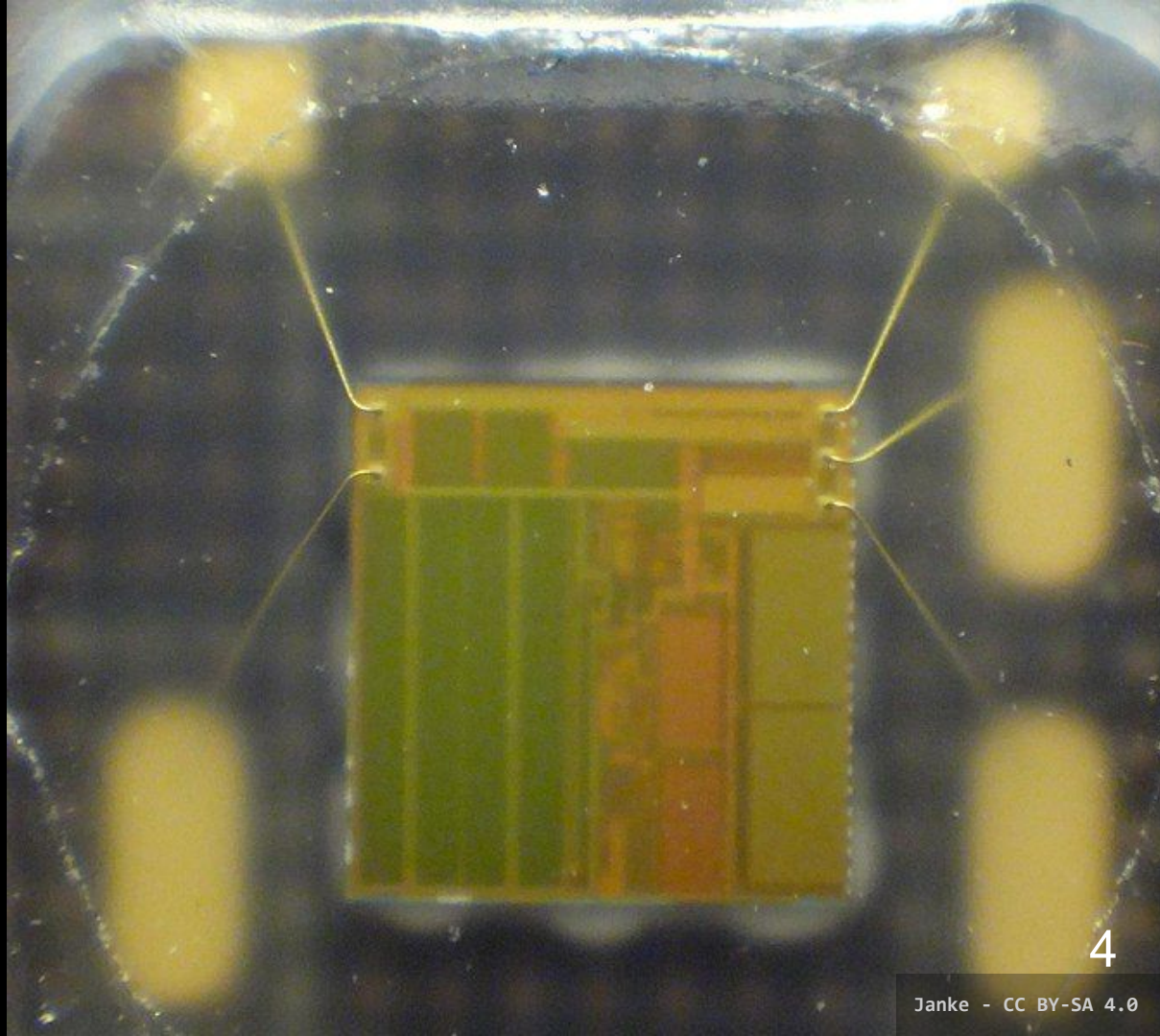
2 High-Severity Vulnerabilities

CVE-2023-50806: Send SS  
2

What is a SIM card?

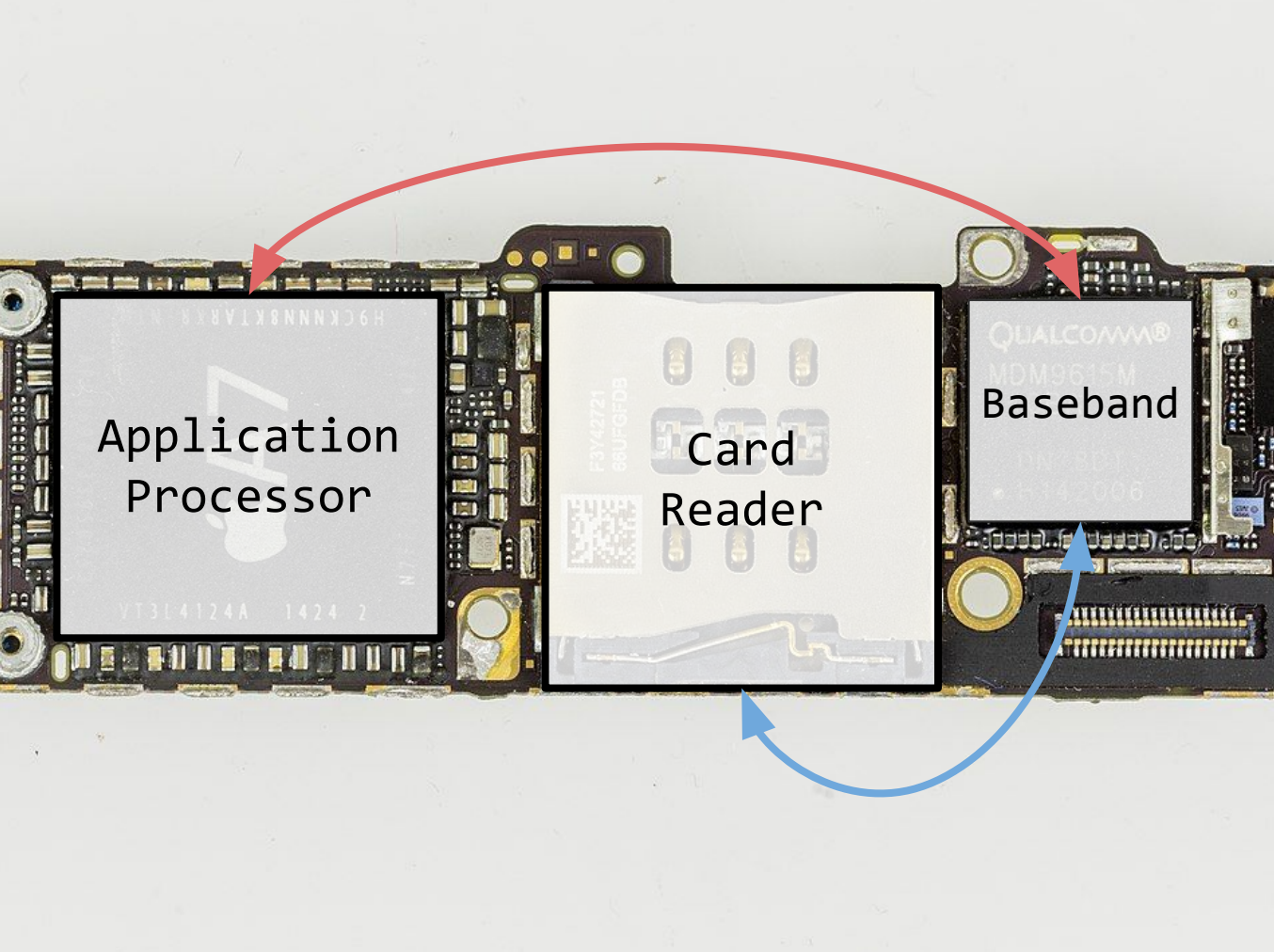
It's a computer!

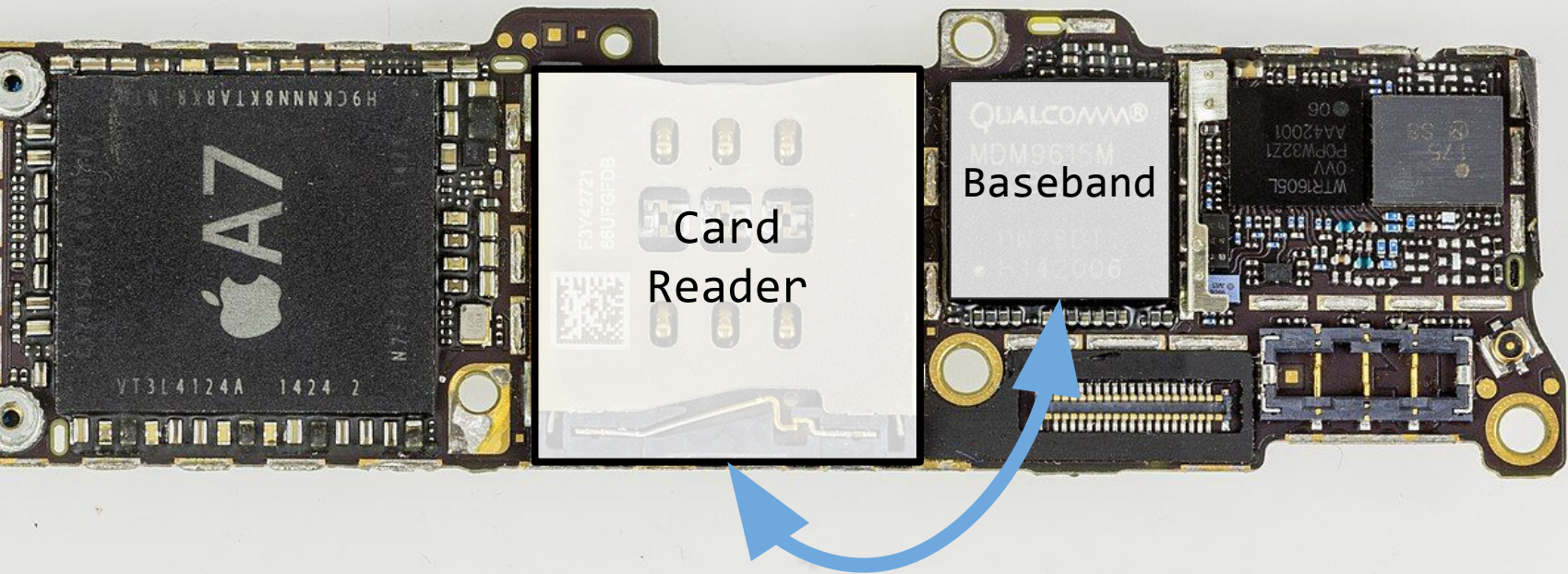
- A “smartcard”.
- Can run apps.



# SIM from the Phone's Perspective







# Attack Vectors

Application  
Processor

Hardware  
OS  
App  
Vendor  
Updates  
Accessories  
...

Baseband

Hardware  
OS  
Vendor  
Updates  
AP  
...  
**SIM?**

SIM Card

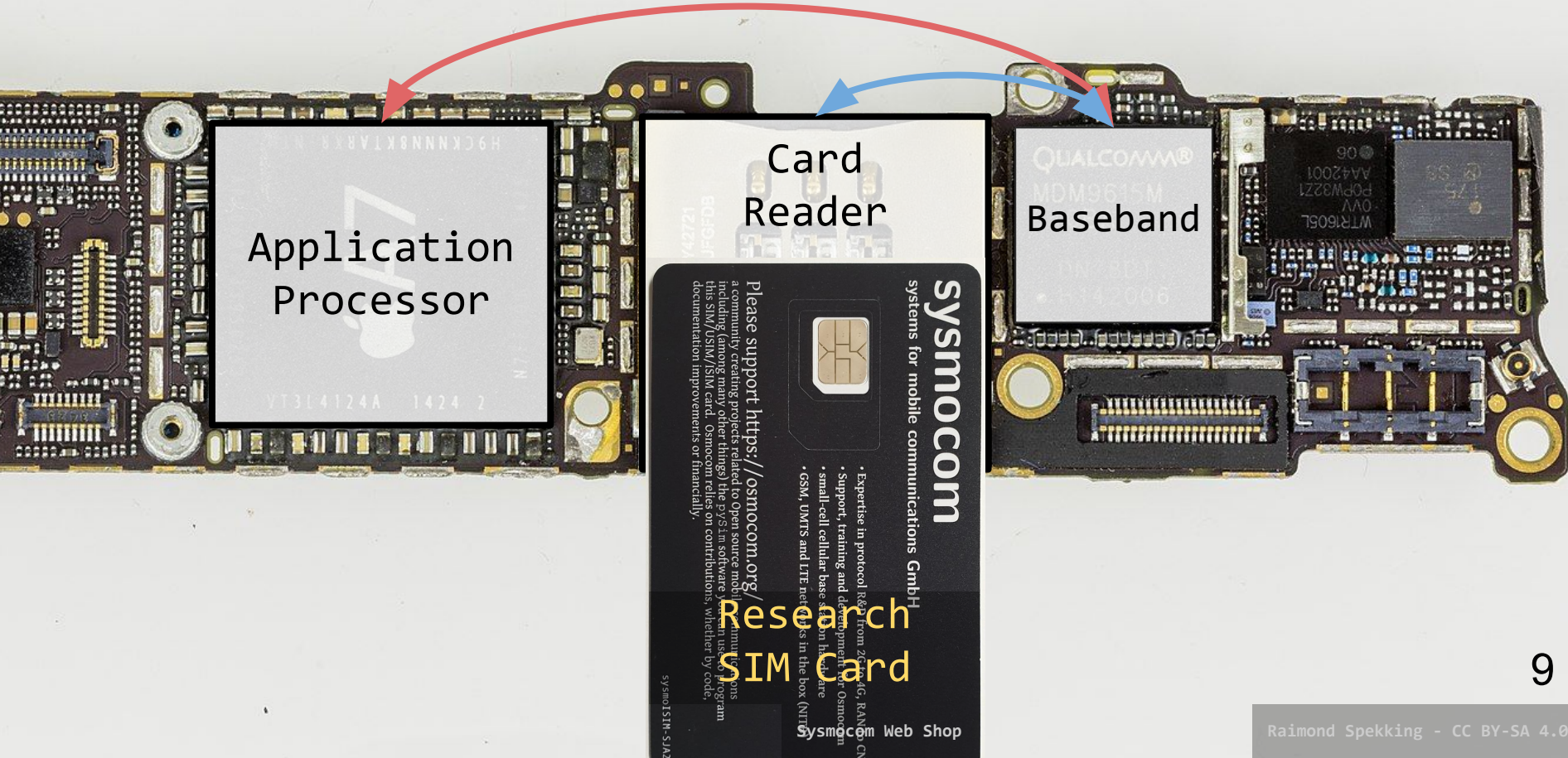
Hardware  
Card OS  
**Operator?**  
**MITM?**

Network

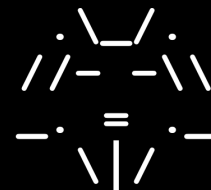
Hardware  
OS  
Operator  
MITM  
Vendor  
Updates  
...



# Exploring the SIM-Band Interface: State-of-the-Art



# SIMurai: Design & Implementation



**SIMurai**

Research platform:

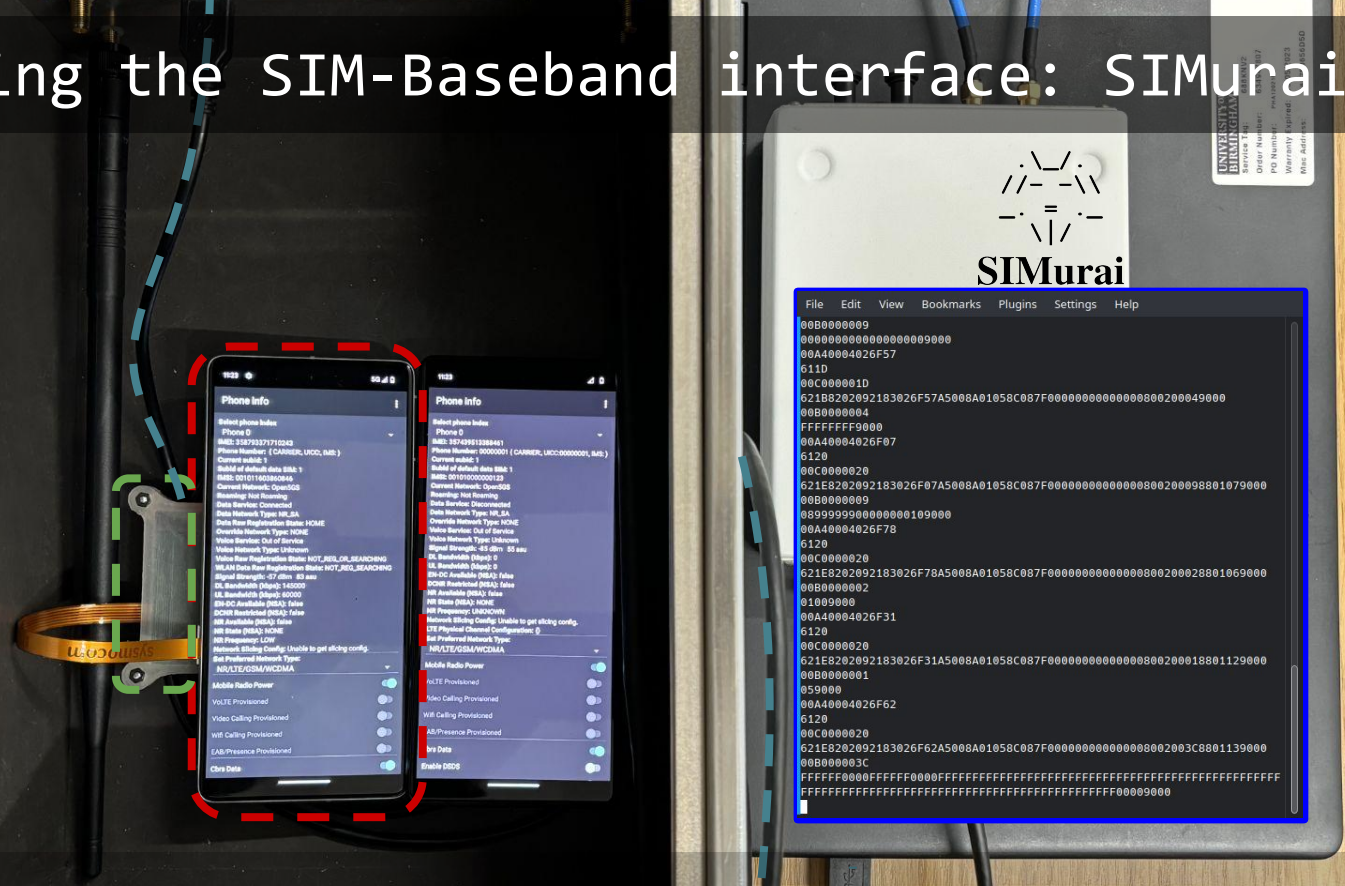
- Library,
- Framework,
- and emulator.

From scratch: ~14,000 lines of C code.

Designed for research.

Drop-in replacement for physical cards (using SIMtrace 2).

# Exploring the SIM-Bandbase interface: SIMurai.



Phone

SIMtrace 2

Workstation

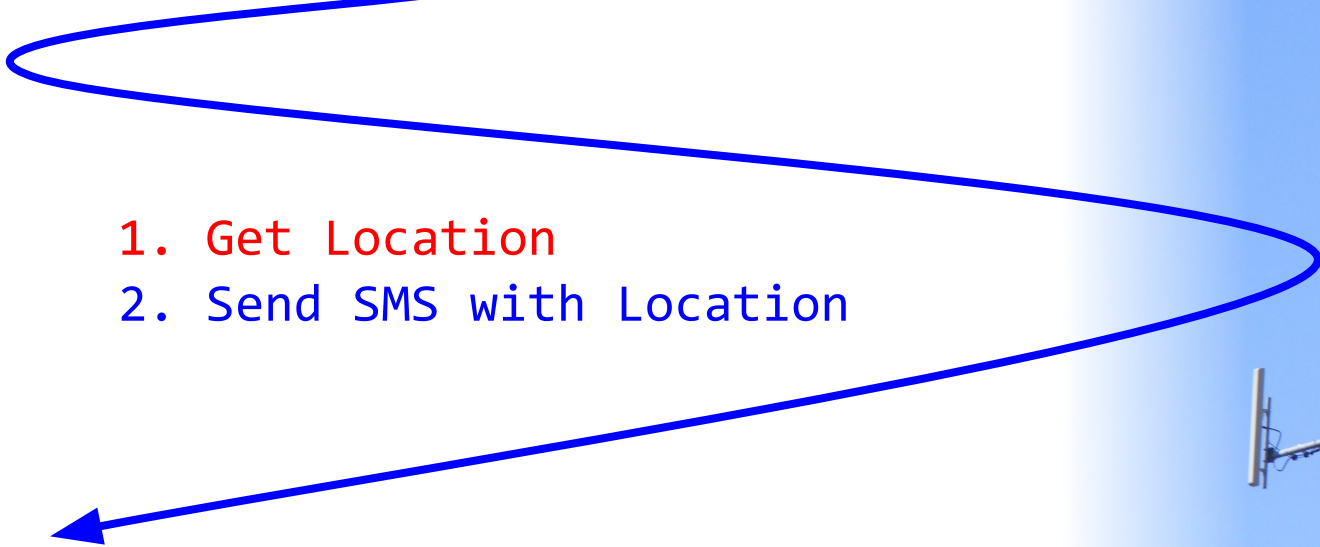
SIMurai



# SIMurai: Spyware Implementation



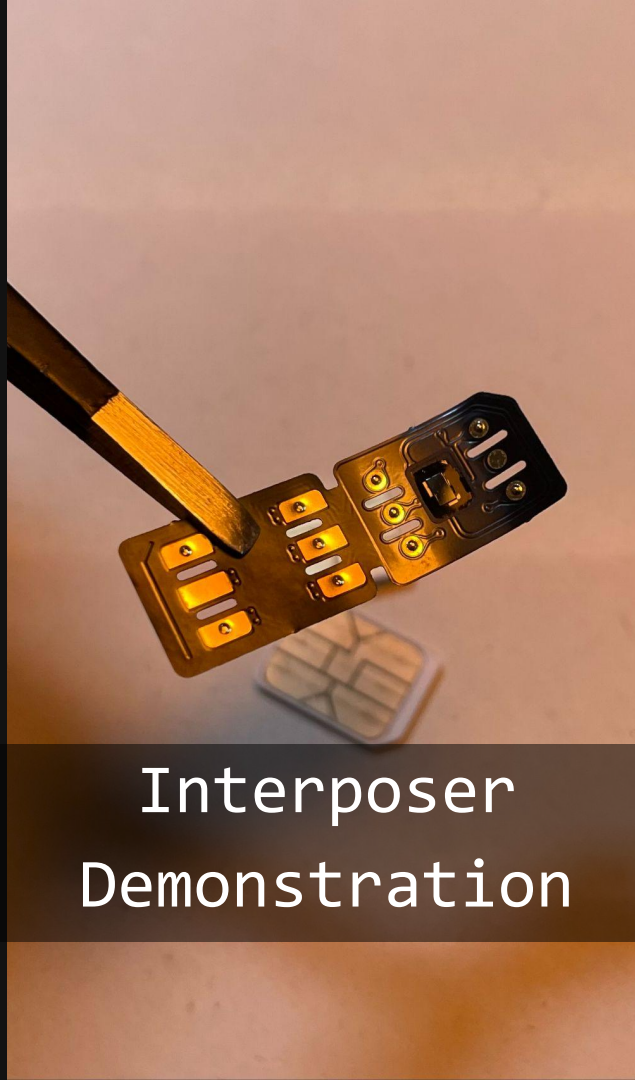
1. Get Location
2. Send SMS with Location







SIMurai-aided  
Fuzzing



Interposer  
Demonstration

Integration  
Into Setups



## SIMurai: Evaluation

Compatible with many devices.

Plug'n'play!

Much easier than research cards.

**Case studies:** Spyware, and more.

High-severity vulnerabilities found through **SIMurai-aided fuzzing**.

## Tested compatibility:

- Apple iPhone 15
- Apple iPhone X
- Samsung Galaxy A14
- Samsung Galaxy S22
- Samsung Galaxy A52s 5G
- Samsung Galaxy A41
- Samsung Galaxy S10e
- Google Pixel 7
- Google Pixel 6
- OnePlus Nord CE2
- Oppo Find X5
- ZTE Blade A54
- Motorola One Vision
- And more...

# SIMurai: Summary

- **SIMurai**: SIM emulator & research platform.
- **Case study**: Spyware, fuzzing, and more.
- **Integration** into common research setups.
- **Attacker Model**: Expand to consider SIM.
- Aiding discovery of 2 high-severity vulnerabilities.



SIMurai Paper



SIMurai Artifact