SIMulator

A Security Assessment Tool for Mobile Communications

About us

- Sebastian Renner (sebastian1.renner@othr.de)
- Enrico Pozzobon (enrico@epozzobon.it)

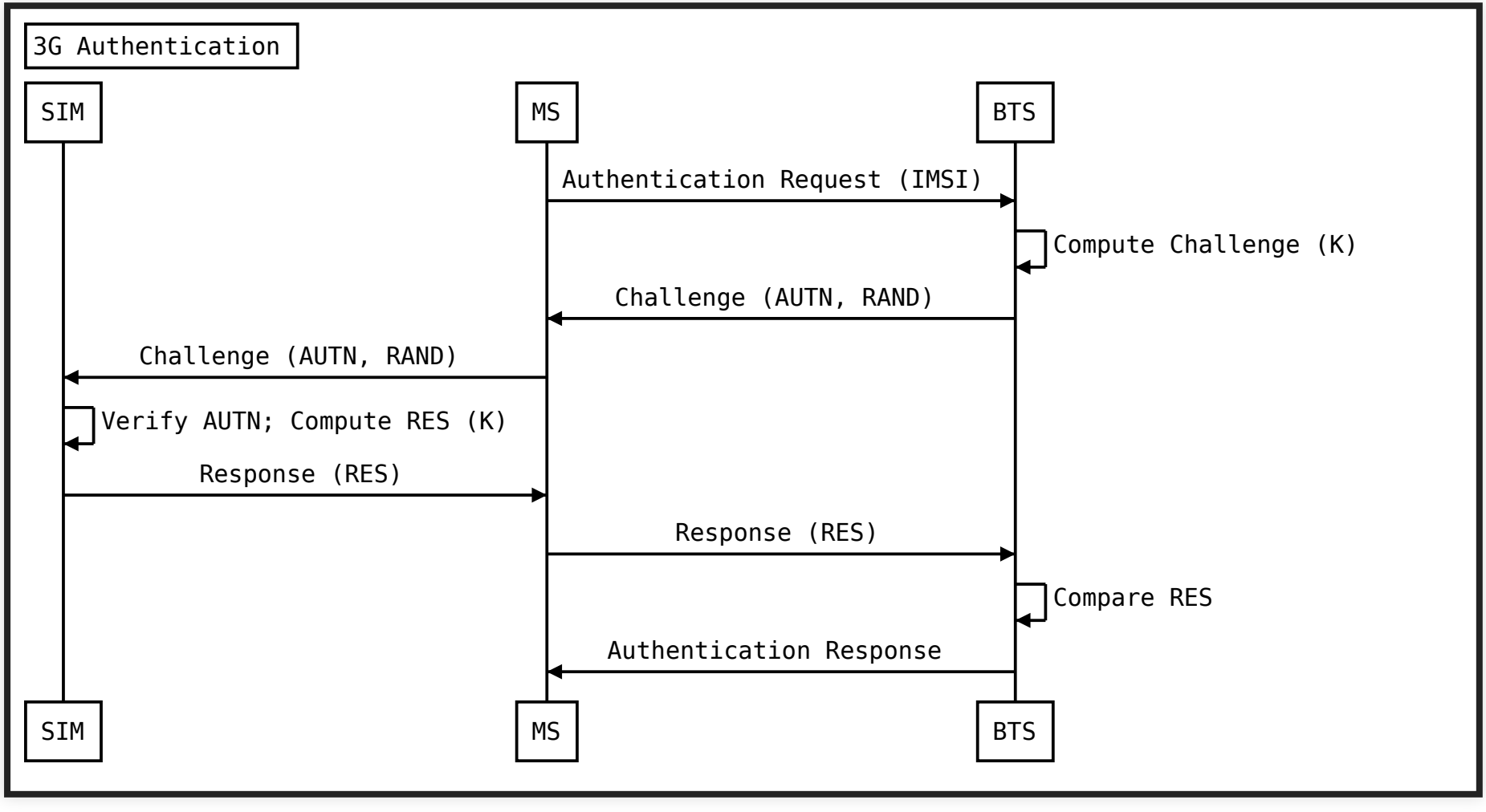
2G/3G+ Security Investigation on IoT Devices

2G Man-in-the-Middle (MITM) attack

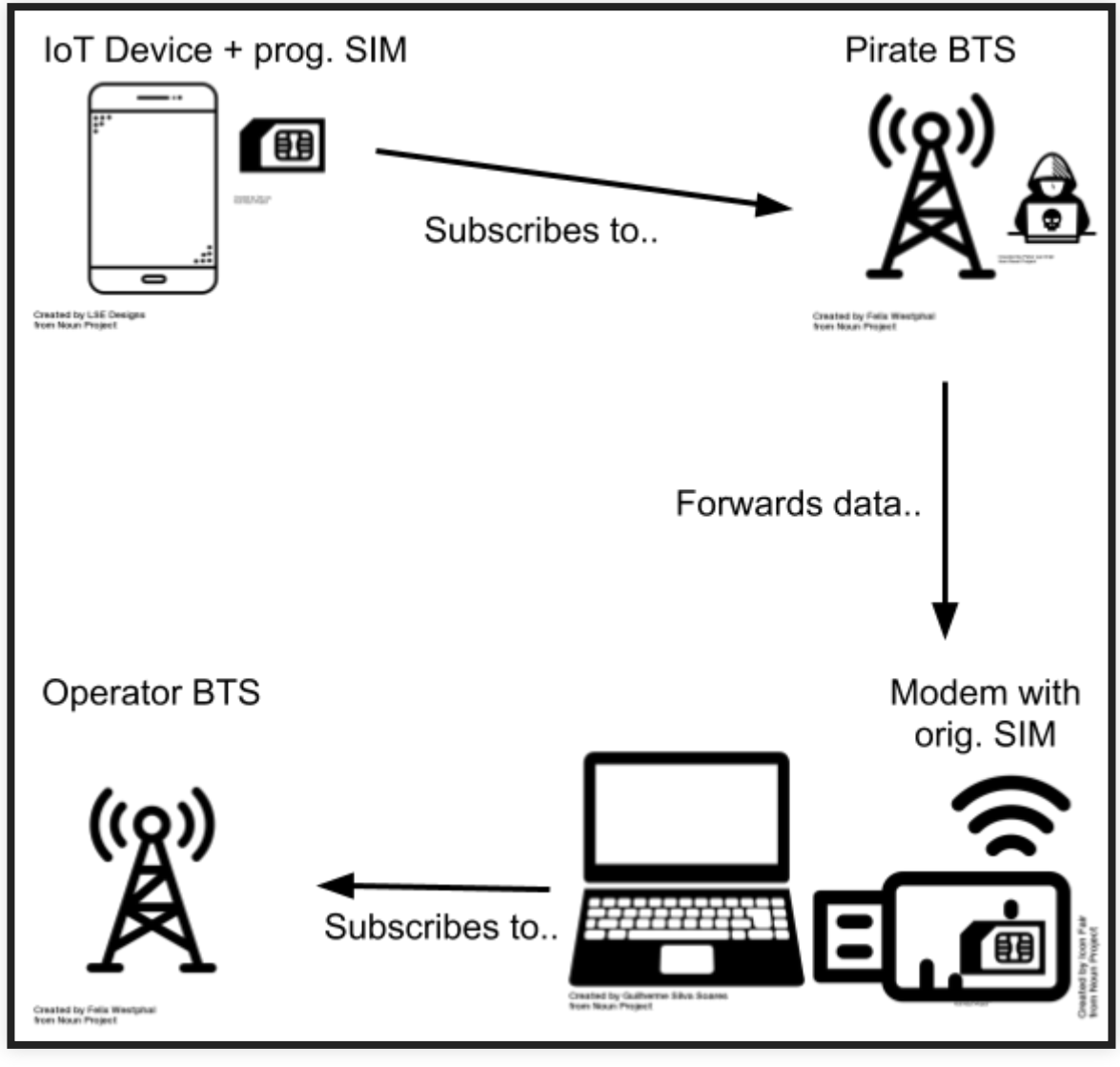
- Setting up a pirate base transceiver station (BTS)
- Make use of weak security mechanisms

Some data is not transferred via 2G!

3G Authentication



3G MITM attack (1/2)



3G MITM attack (2/2)

- Use programmable SIM cards!
- Exchange of the SIM card can be detected
- Tested SIMs were not fully reprogrammable

SIM Simulator aka. SIMulator

Objective

- Replicate/Clone existing SIM
- Inject custom key material

SIM Cards

- SIMs are basically smartcards
- Communication based on ISO 7816
  - Command

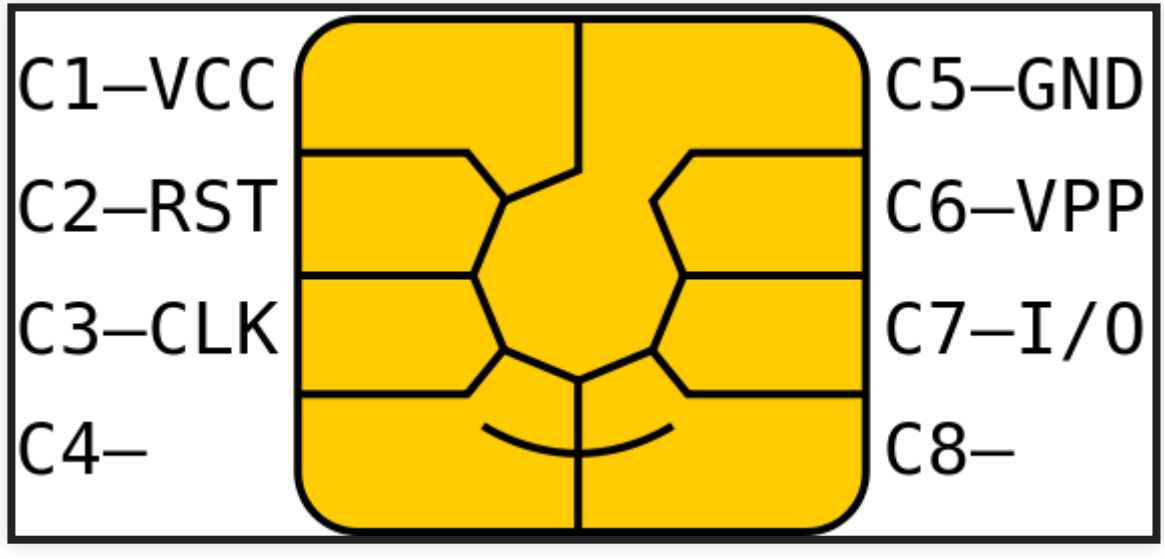
```
|CLA|INS|P1|P2|Lc|Data|Le|
```

  - Response

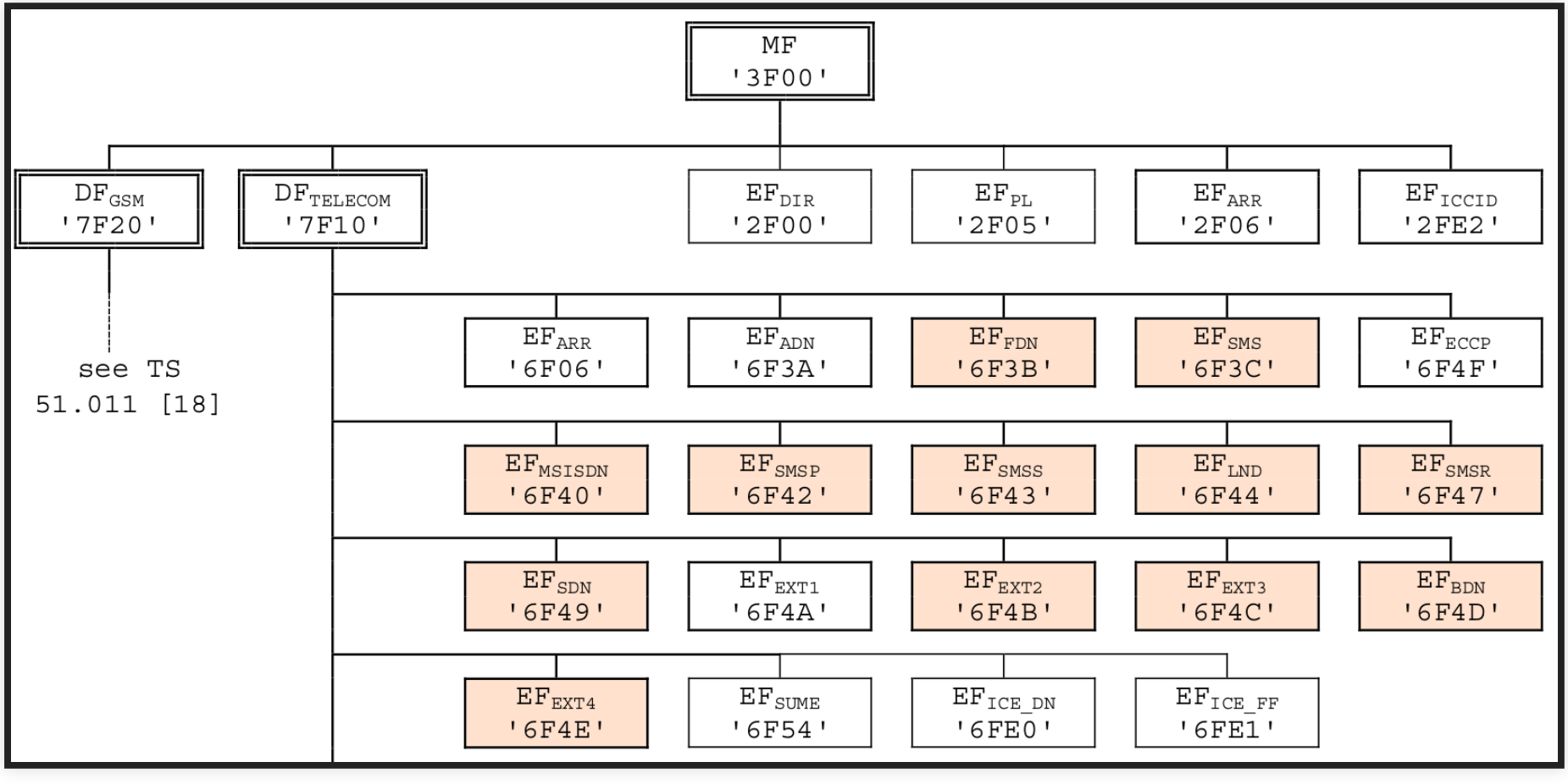
```
|Data|SW1|SW2|
```

- Files structered in a tree

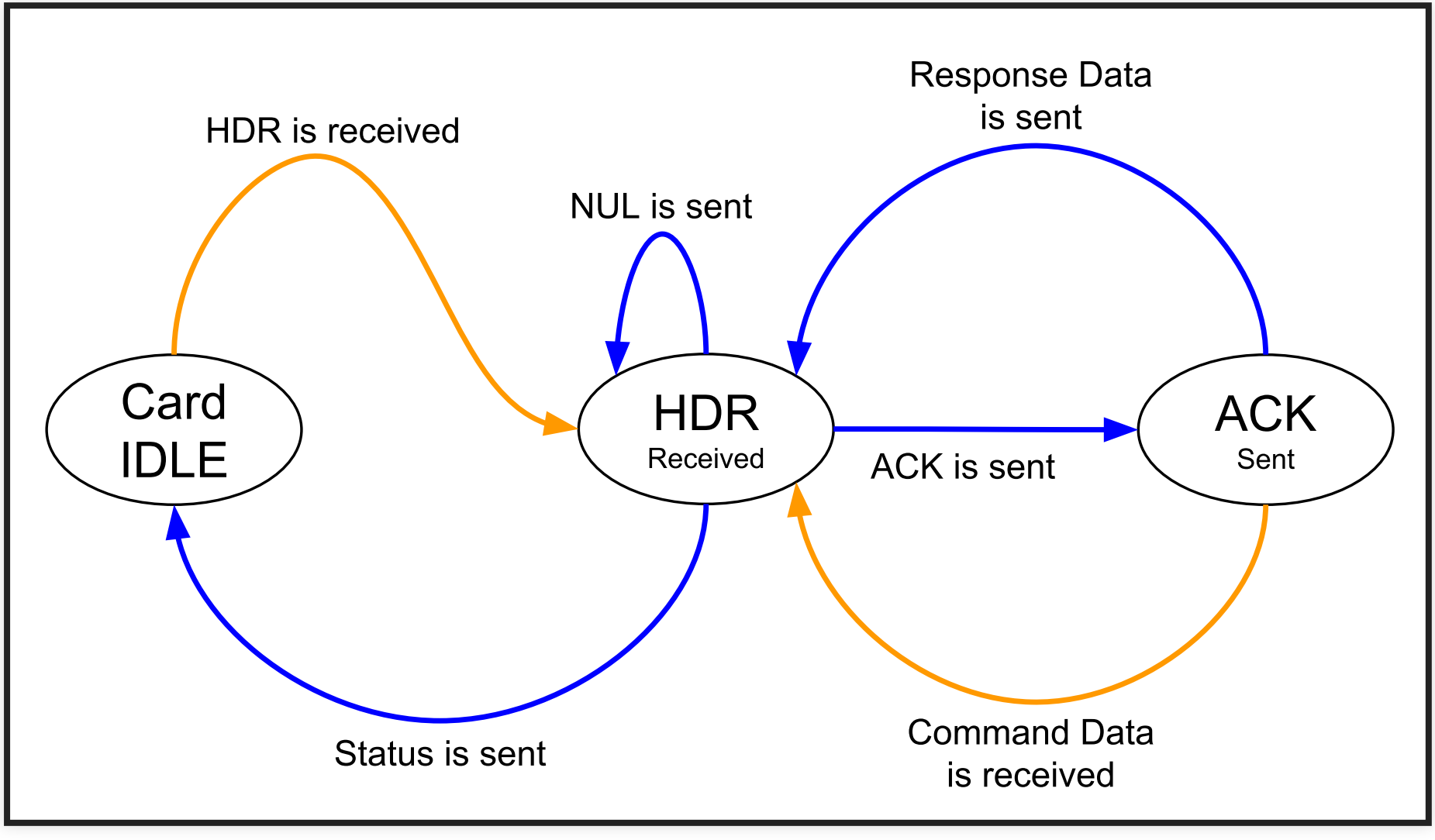
SIM Pinout [1]



SIM File Tree [2]



ISO7816 card state machine



Example: SELECT FILE

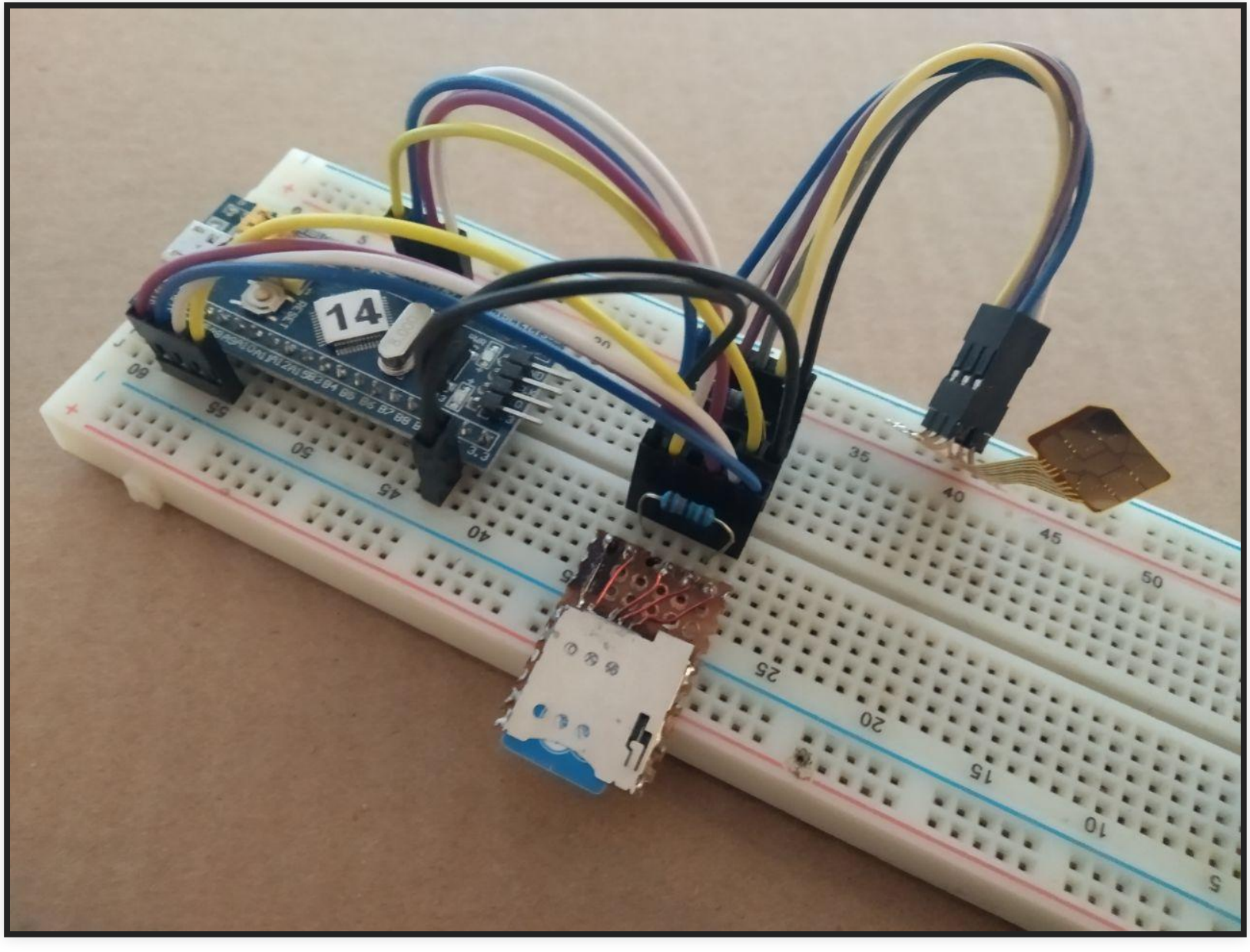
```
HDR: |00|a4|00|04|02|
ACK: a4
DATA: 3f00
NULL: 60
STATE: 612a
-----------------------
HDR: |00|c0|00|00|2a|
ACK: c0
DATA: 6228820278218..
STATE: 9000
```

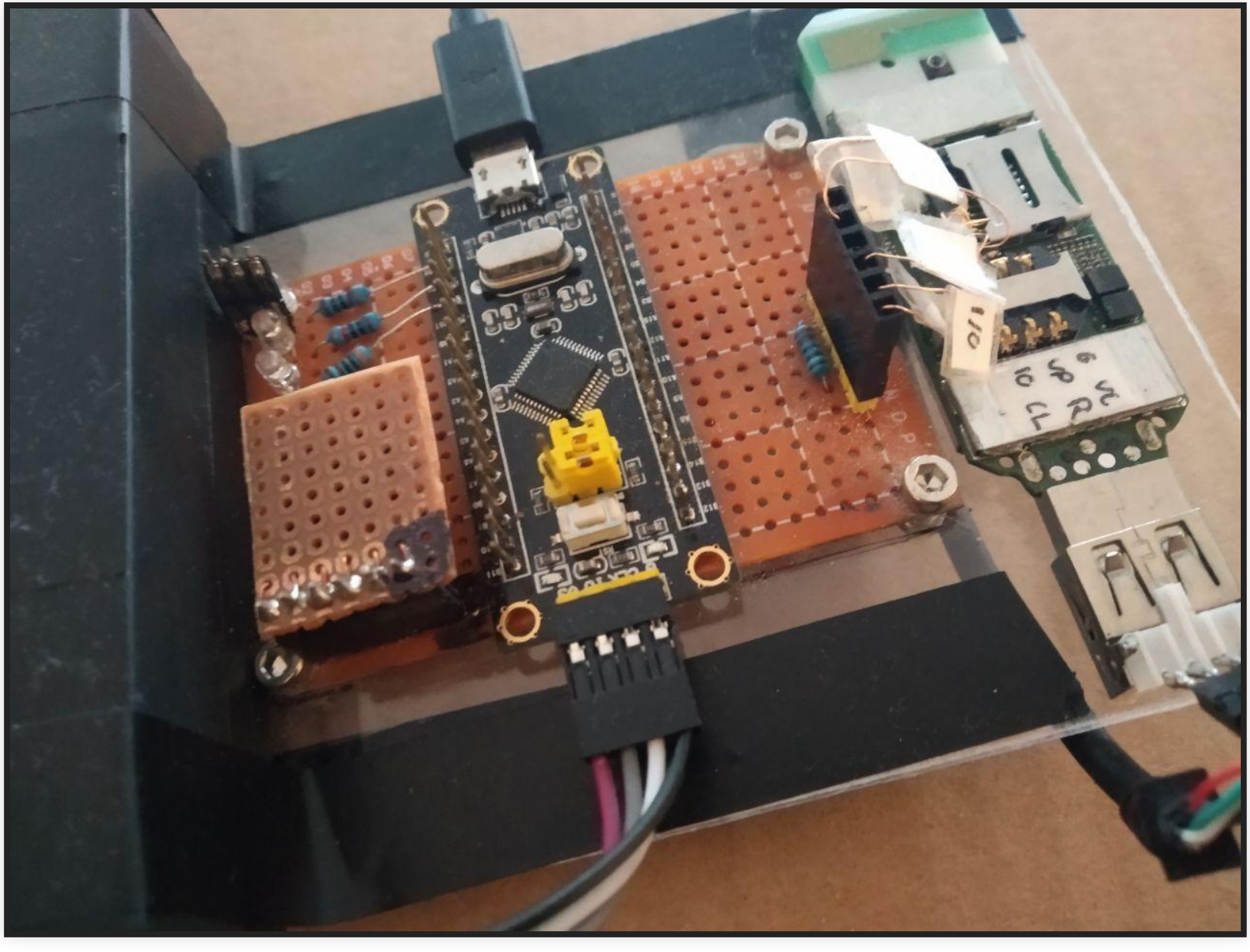
Architecture and Design

- STM32F103 for low layer communication
- JavaScript "driver" simulates the file system

STM32F103C8T6

- USB CDC serial device
  - No drivers are needed
- Super cheap
  - ~€1.50 for a complete board
- 5 UART interfaces
  - That can be configured as ISO7816 cards
  - Or as interfaces (card readers)


14



Node.js application

- SIM file system is defined in a JSON File
- Comes with some example emulated SIM cards
  - that can be easily extended
- Correctness of emulation can be "unit tested"
- The modem can not distinguish an emulated card and the real one


VINCENT?
WE HAPPY?

...but

- The whole file structure has to be described in JS
- The behaviour specific to the SIM card as well

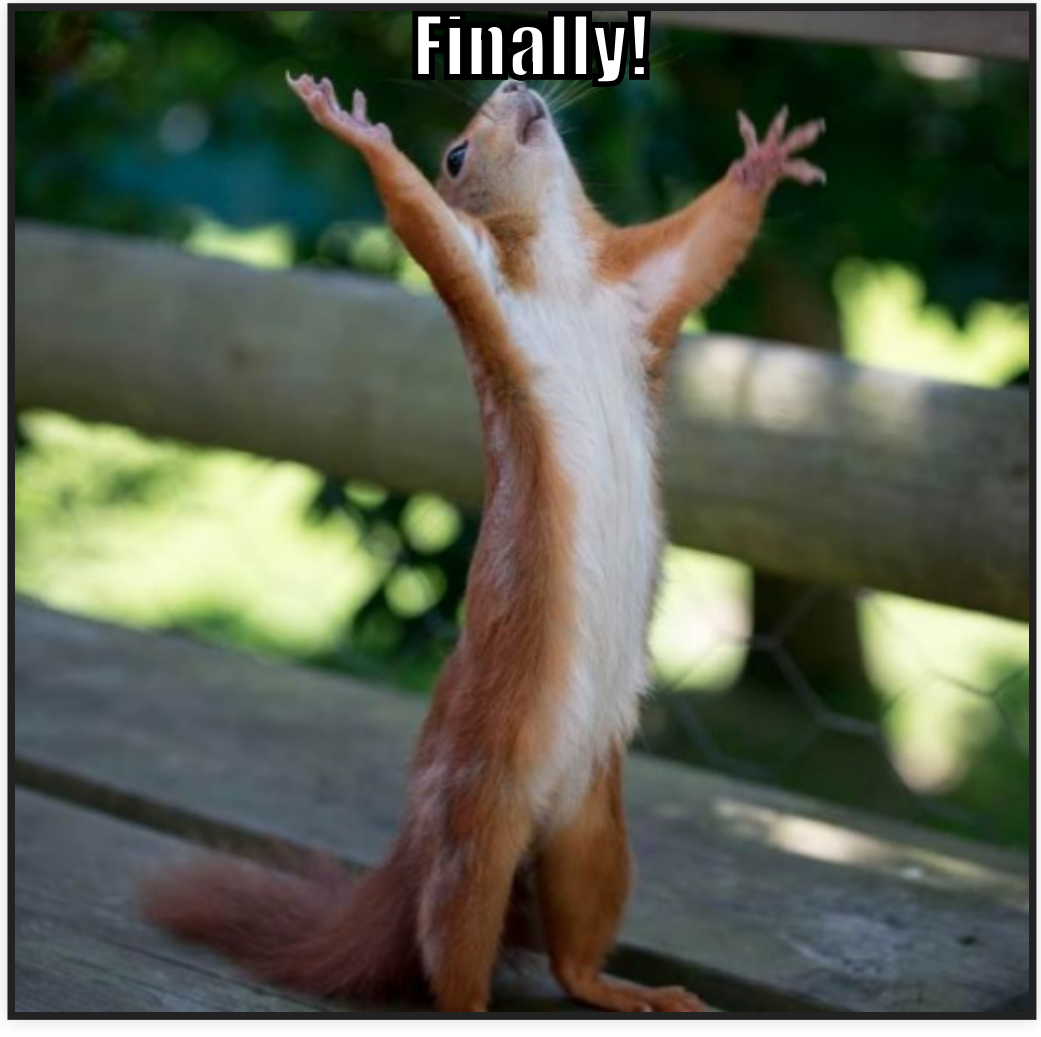
SIM MITM

- APDU forwarding from modem to original SIM
- SIMulator gets triggered on AUTHENTICATE APDU
- Response is spoofed

Use Cases

- Penetration testing modems
- Unit testing for smart card-interfacing applications
- Security investigations that include SIM/smart cards
- Relaying a smartcard over a long distance from a reader

Demo Time



https://www.youtube.com/watch?v=NcrZvowYPl8

Clone it on GitHub!

https://github.com/strbli/SIMulator

References

[1] Koscher, Karl and Butler, Eric. The Secret Life of SIM Cards. 2013. URL: https://simhacks.github.io/defcon-21/

[2] 3rd Generation Partnership Project. 3G TS 31.102 - Characteristics of the Universal Subscriber Identity Module (USIM) application. 1999.

Questions?