Hacking Tokens: A Massive PoC

Ismael Benito | Arnau Gàmez

UNIVERSITAT DE BARCELONA
Fisitrónica
HACKING LLIURE

/RootedCON

Agenda

- **About us**
- **Hacking Token Concept**
- **Hardware**
- **Software**
- **Results**
- **Conclusions**
- **Questions**

About us

Arnau Gàmez i Montolio | @arnaugamez

- 20yo. From Benigànim, València
- President of Hacking Lliure
- Maths & CS student @ UB
- Worked as software developer in research groups @ UB
- Participated in many CONs
- r2 evangelist
- Also interested in music: pianist

HACKING LLIURE

- Founded in late 2016
- Faculty of Mats & CS @ UB
- Ethical and social aspects of infosec
- Use and creation of FLOSS
- Technical workshops and talks in wireless security, IoT, RE, stego, etc.

https://hackinglliure.org

info@hackinglliure.org

@HackingLliure

Ismael Benito Altamirano | @ismansiete

- 26yo. From Nou Barris, Barcelona
- Former president of Fisitrónica
- B. Physics & Electronics Eng. @ UB
- MSc. in Photonics @ UPC
- Predoctoral researcher @ UB
- Assistant professor @ UB
- Also interest in politics, magic tricks, photography, all sci-fi Netflix series...

Fisitrónica

- Founded in 2011
- Faculty of Physics @ UB
- Aims to promote electronics & robotics among students.
- Several activities during the course such as courses, workshops

http://fisitronica.net

fisitronica@gmail.com

@Fisitronica

Hacking Token Concept

Hacking Token: from RootedCON 2017

Sweet Tools O'Mine by Hugo Teso: https://youtu.be/G8bccS3wla0

Hacking Token: candidates

Hacking Token as a PowerBank

- Battery pack for charging smartphones and other USB charge-capable devices.
- Extra powerful 20000 mAh charge capacity.
- Uses quality battery cells from well-known manufacturers.
- Dual USB ports, including one 2.4 A port for quick charging tablets and similar devices.
- Battery status indicator.

General specs of PowerBanks:

- Portables
- Charging & discharging circuits integrated
- LiPo Bat. up to >20000 mAh
- Charger current up to >2A
- USB and Micro-USB ports
- At least a ON/OFF Button
- LEDs (Interface & linter)
- Not yet idloTized

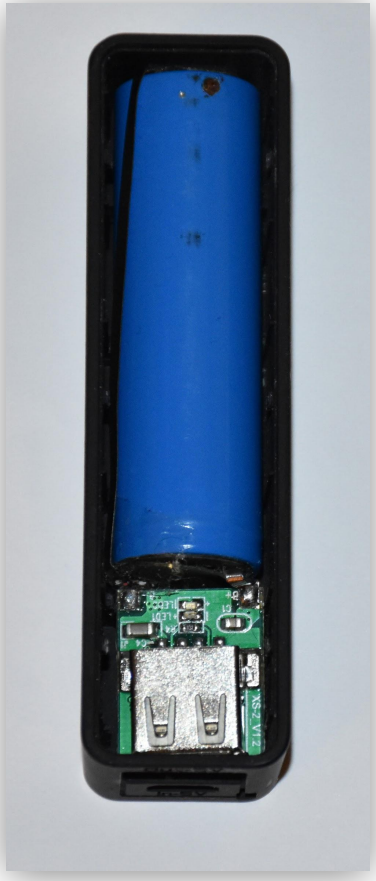
Hardware

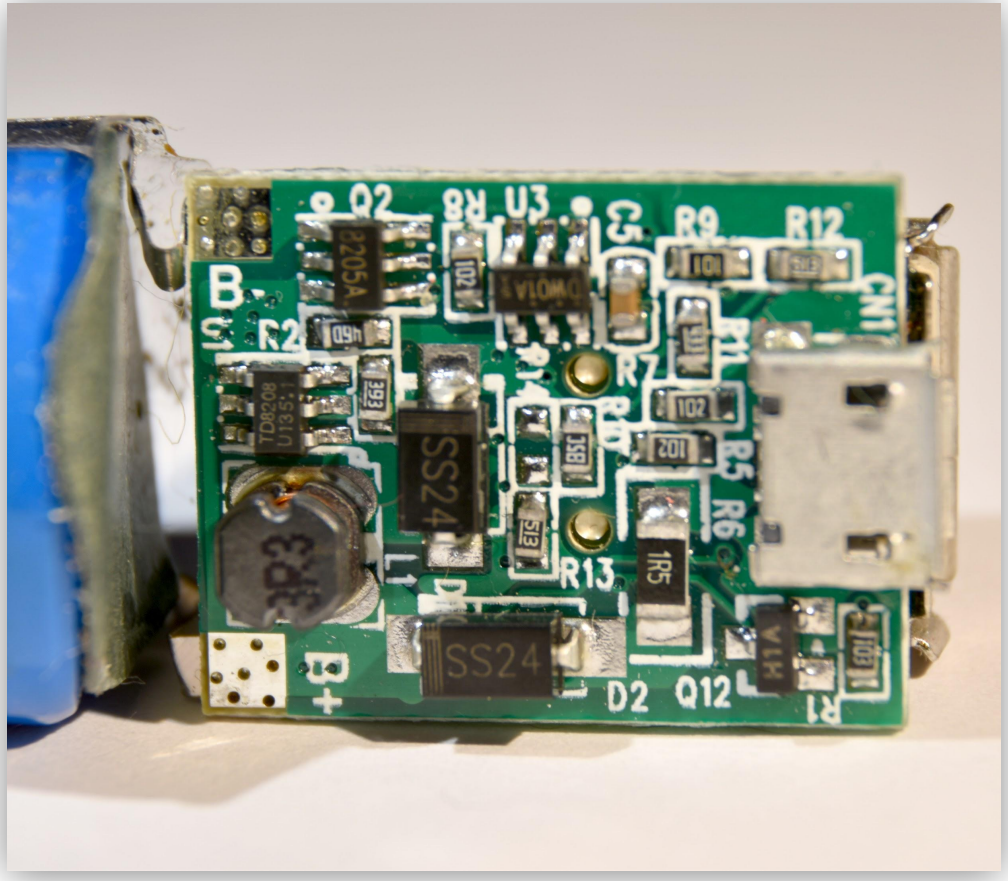
Hardware

Reversing a PowerBank

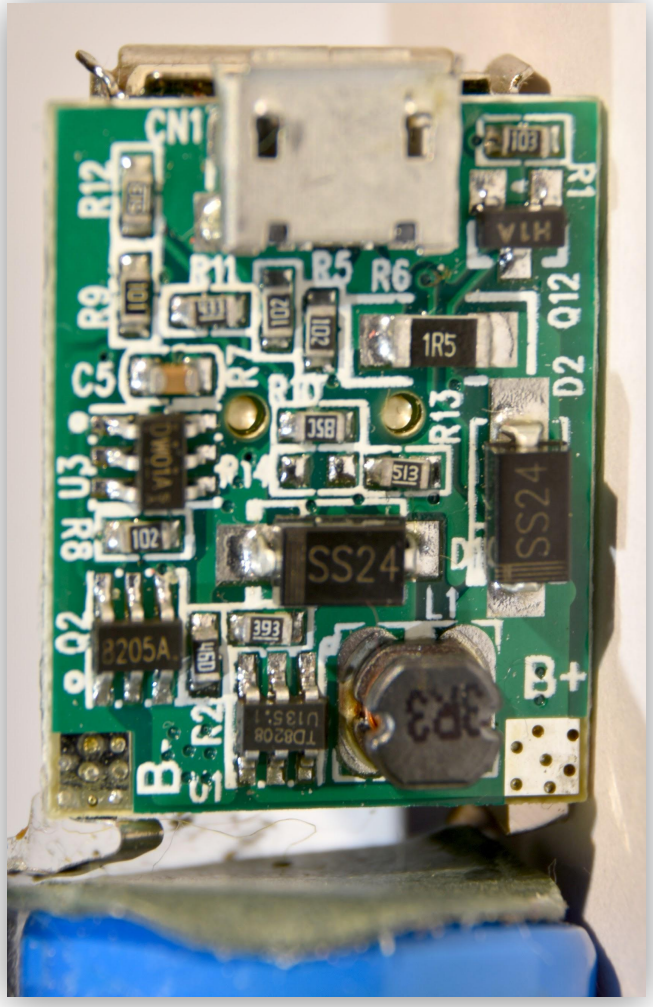
- **Learn about PowerBank internal circuits**
- **Charge and discharge a LiPo battery**
- **Protection circuit**
- **Typical schematics**

Hardware: reversing a PowerBank

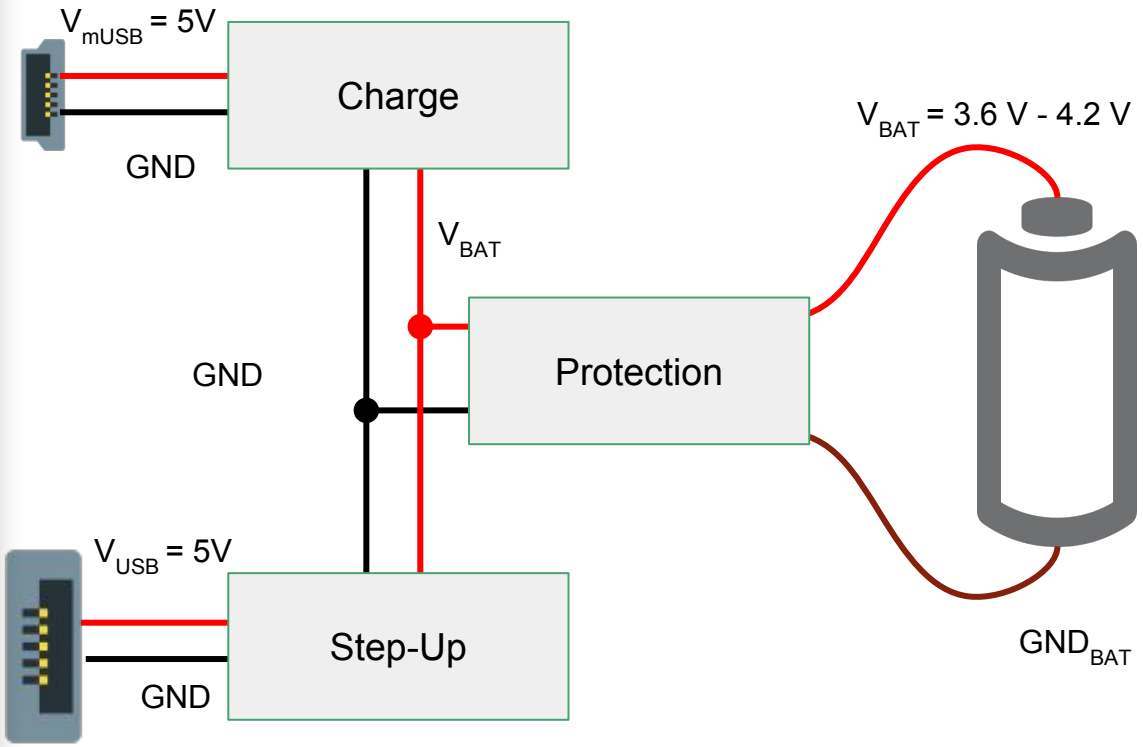




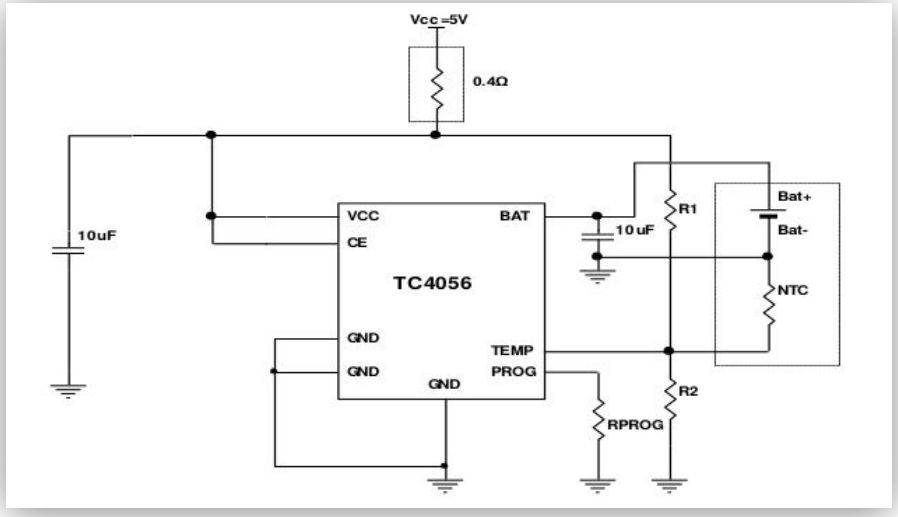
Hardware: reversing a PowerBank

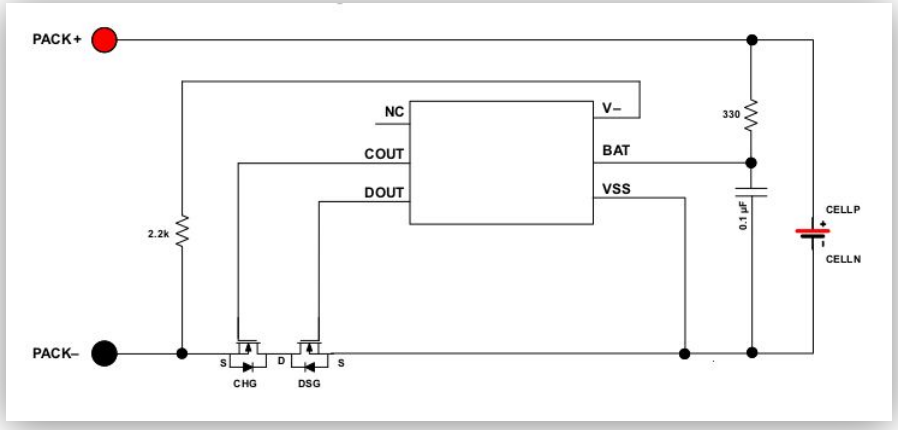


Block diagram



Hardware: reversing a PowerBank





from several datasheets

Charge circuit:

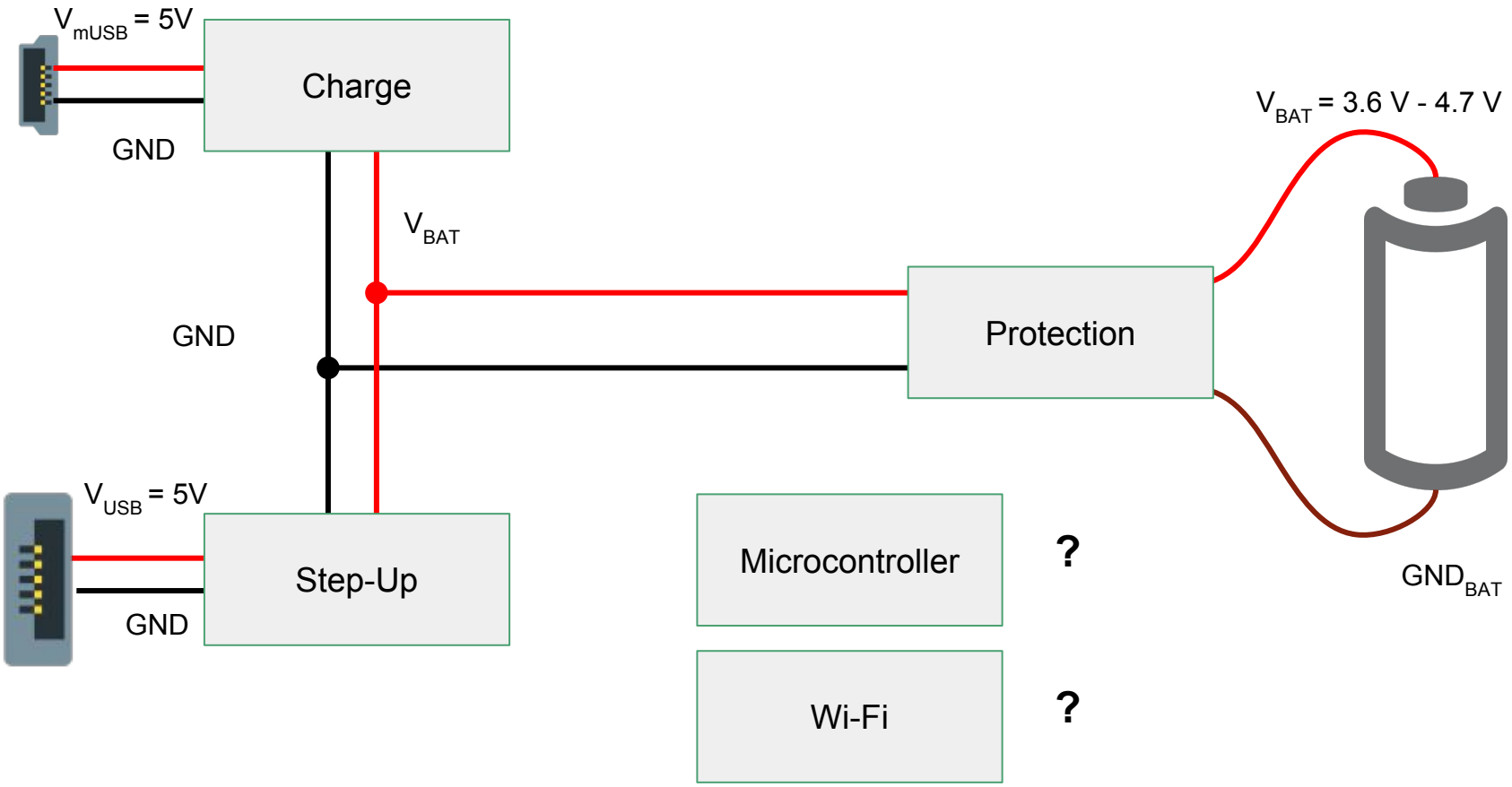
- Models: LTC4056, TP4056...
- Battery detection
- Match the correct I_{charge} for LiPo/Li-Ion Batteries

Protection circuit:

- Models: AP9101C, BQ2970, FS312F-G, S820A
- Overcharge voltage detection
- Overdischarge current detection
- Disconnects GND_{BAT} from GND when needed

Hardware: Microcontrollers

Block diagram

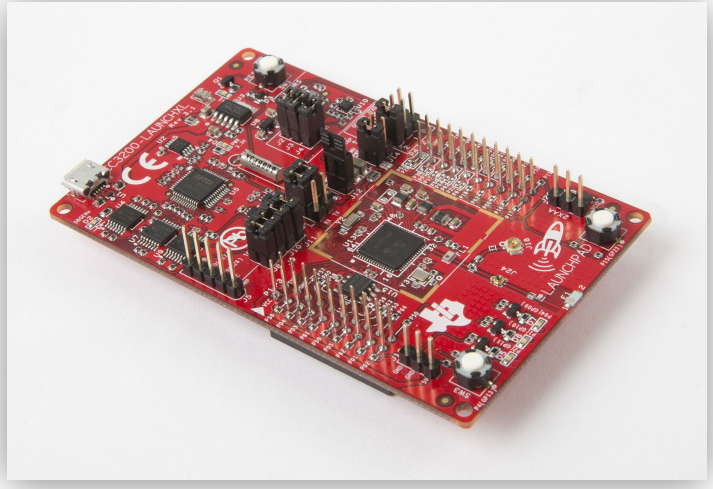


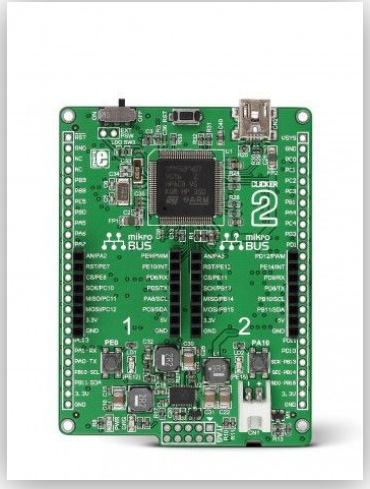
Hardware

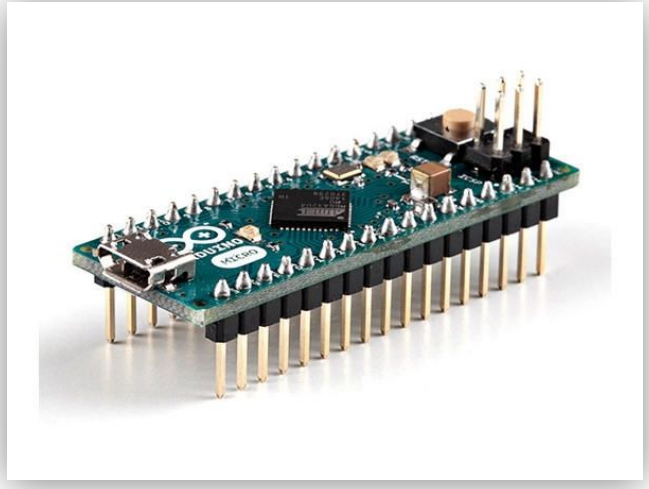
Microcontrollers (uC)

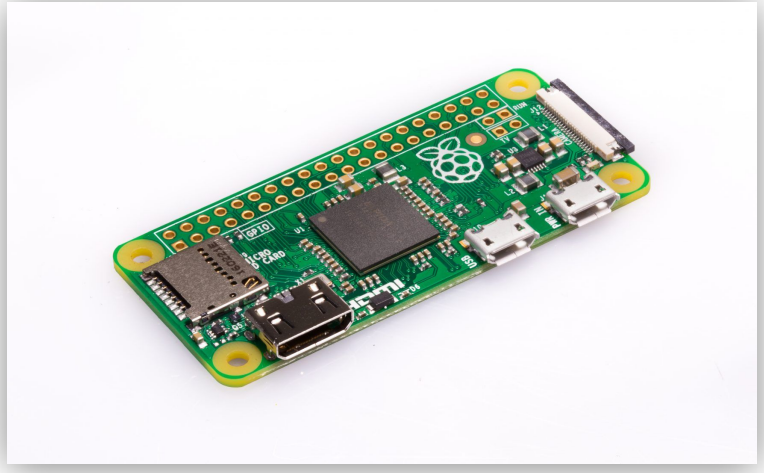
- **State of the art**
- **Choose low-power uC**
- **uC placement inside a PowerBank**

Hardware: Microcontrollers

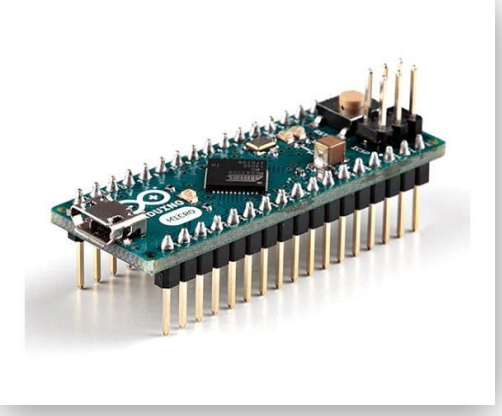








Hardware: Microcontrollers



Arduino (Pro) Micro (Atmega32u4):

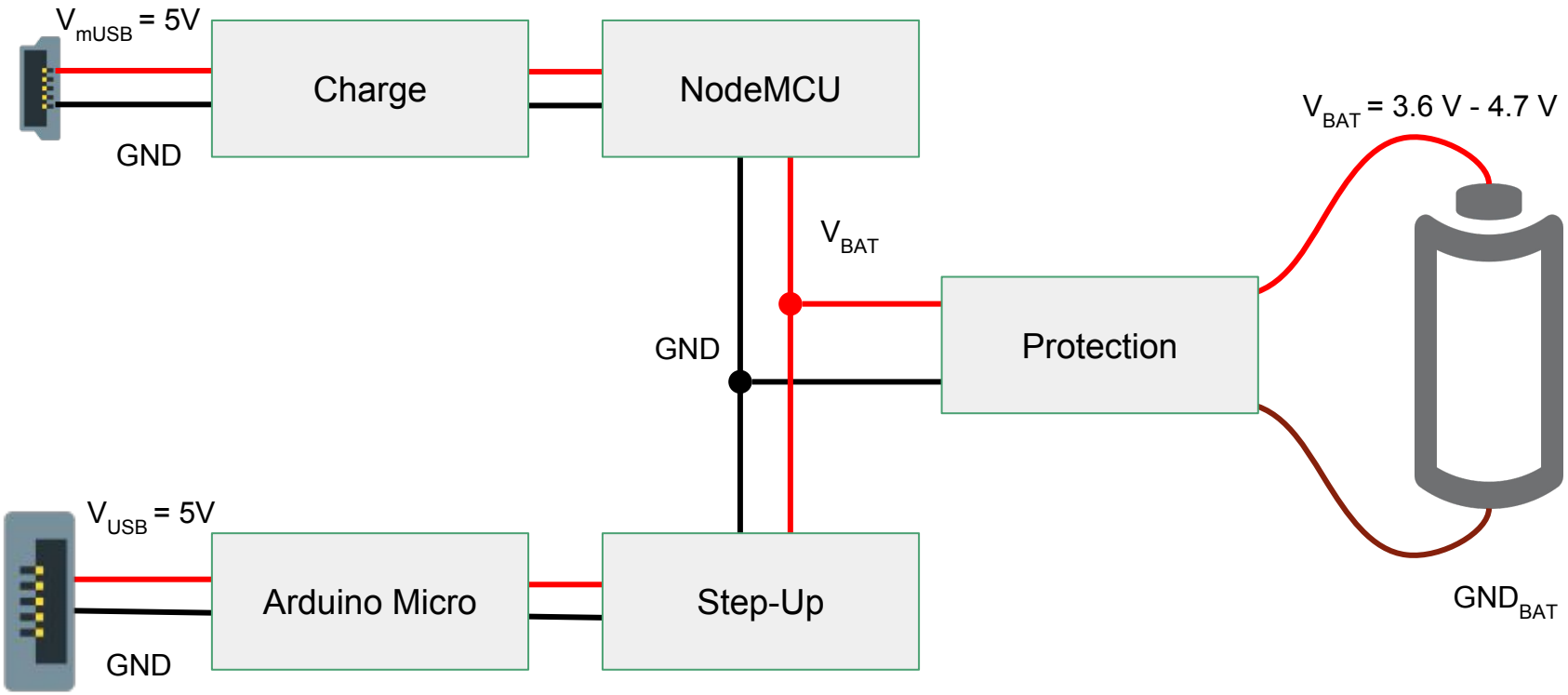
- Arduino-compatible
- Several factor forms: Micro, Leonardo, Esplora…
- Works with 5V and 3.3V logic
- USB stack

NodeMCU v3 (ESP8266):

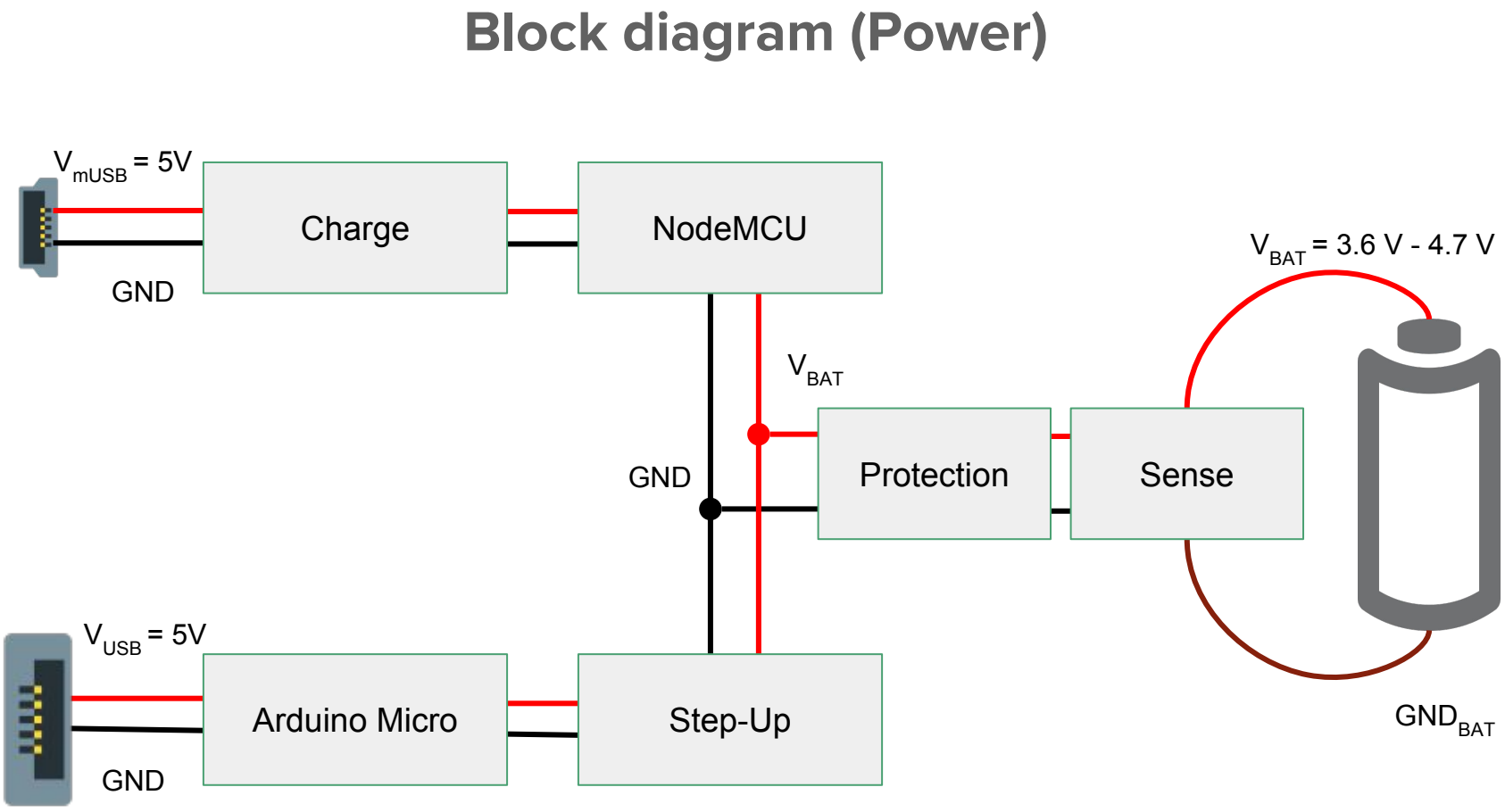
- Arduino-compatible
- Several factor forms: NodeMCU, Weedemos, Adafruit Huzzah…
- Works only with 3.3V logic
- WiFi + TCP/IP stack

Hardware: Microcontrollers

Block diagram

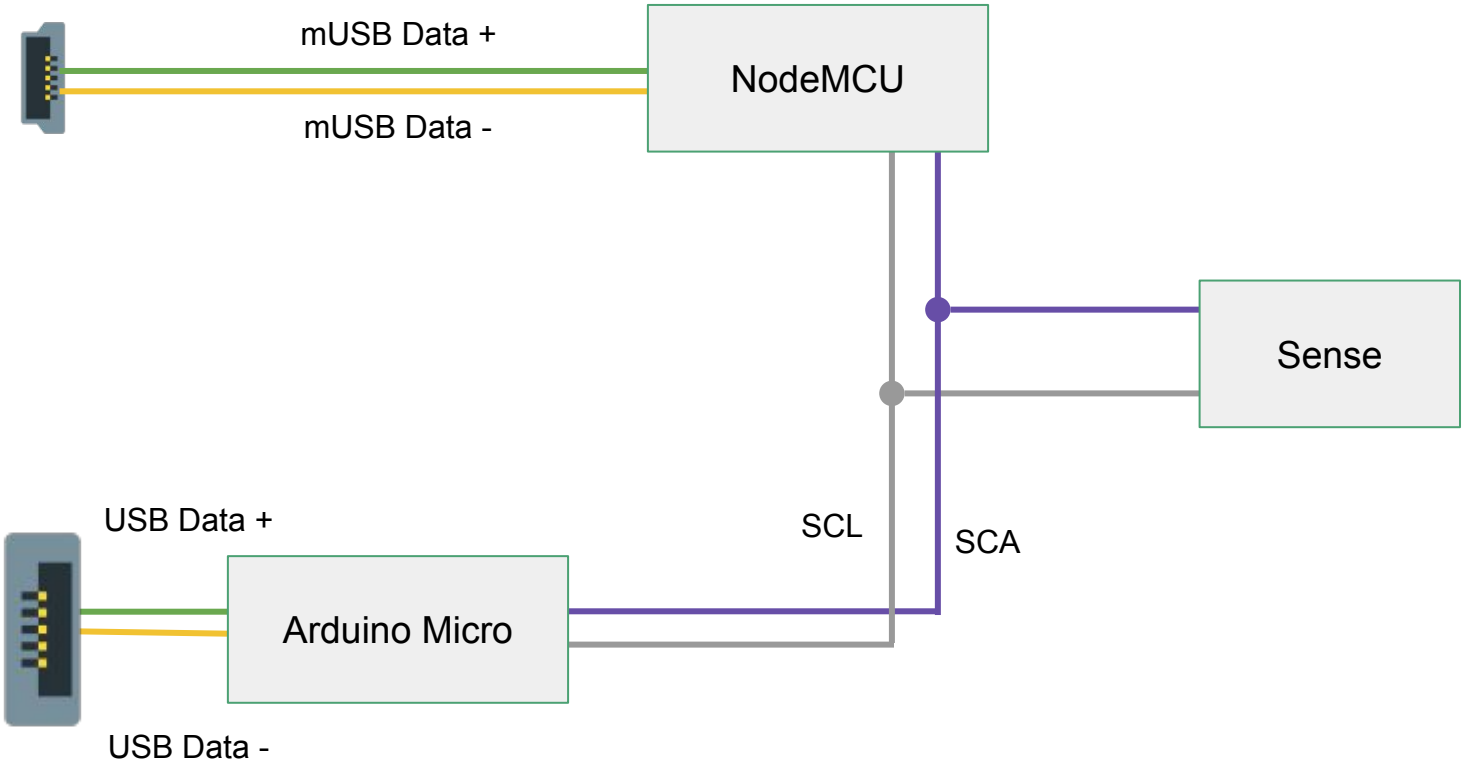


Hardware: Microcontrollers



Hardware: Microcontrollers

Block diagram (Communications)



Hardware: demo

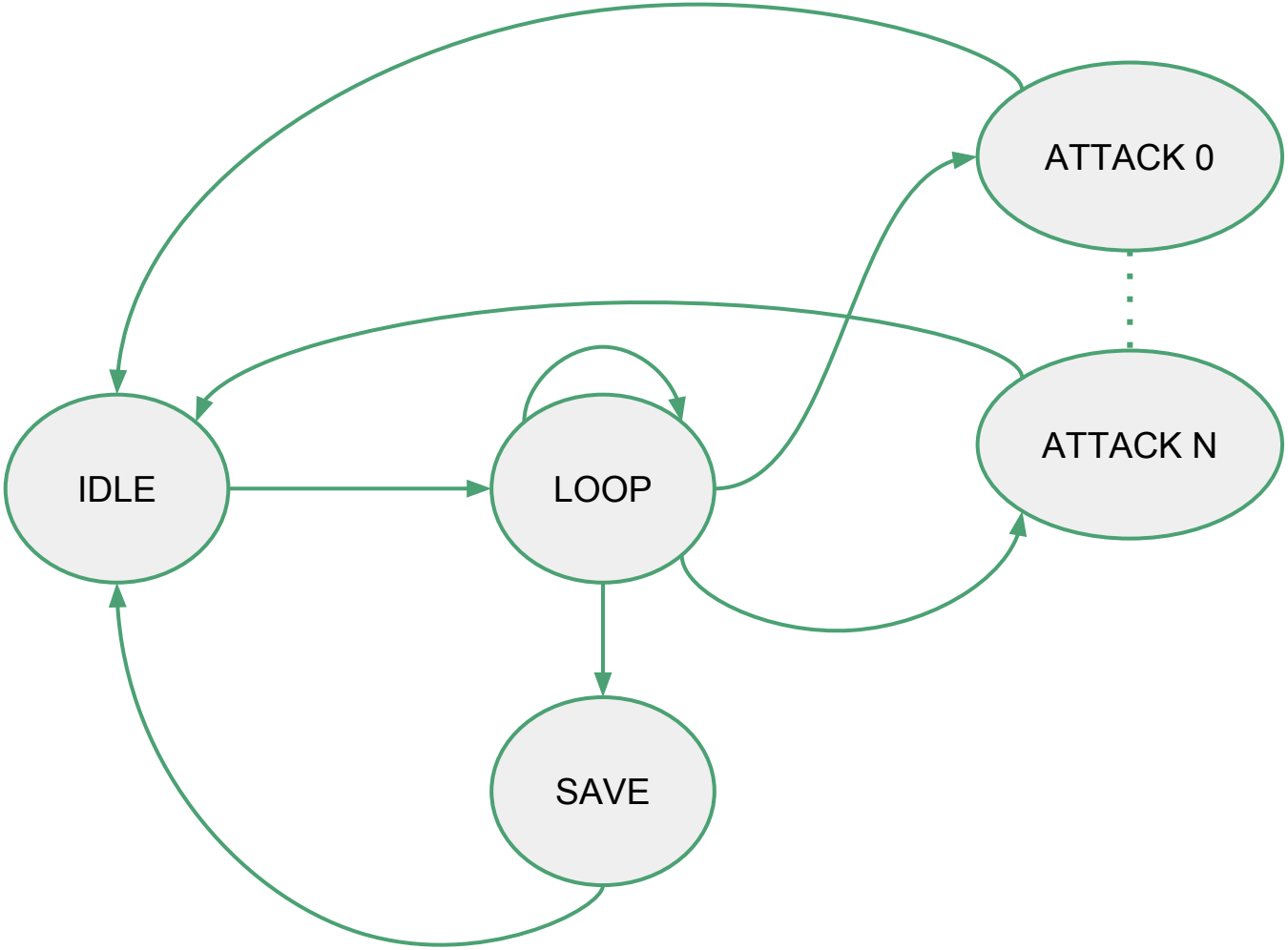
Software

Software

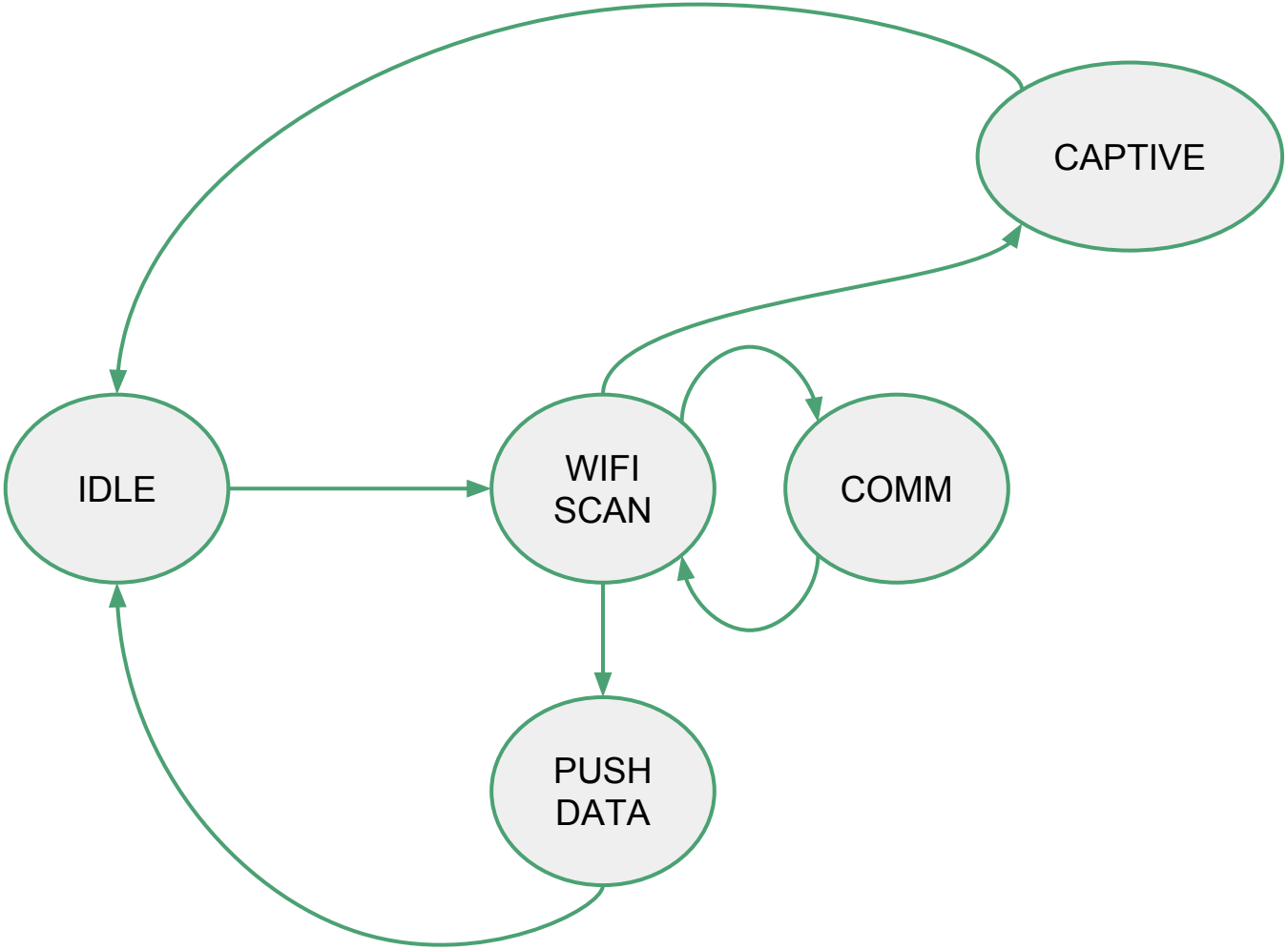
Basic Needs

- **Reprogram hardware**
- **Store data**
- **Retrieve data**
- **Modular/plugineable attacks**

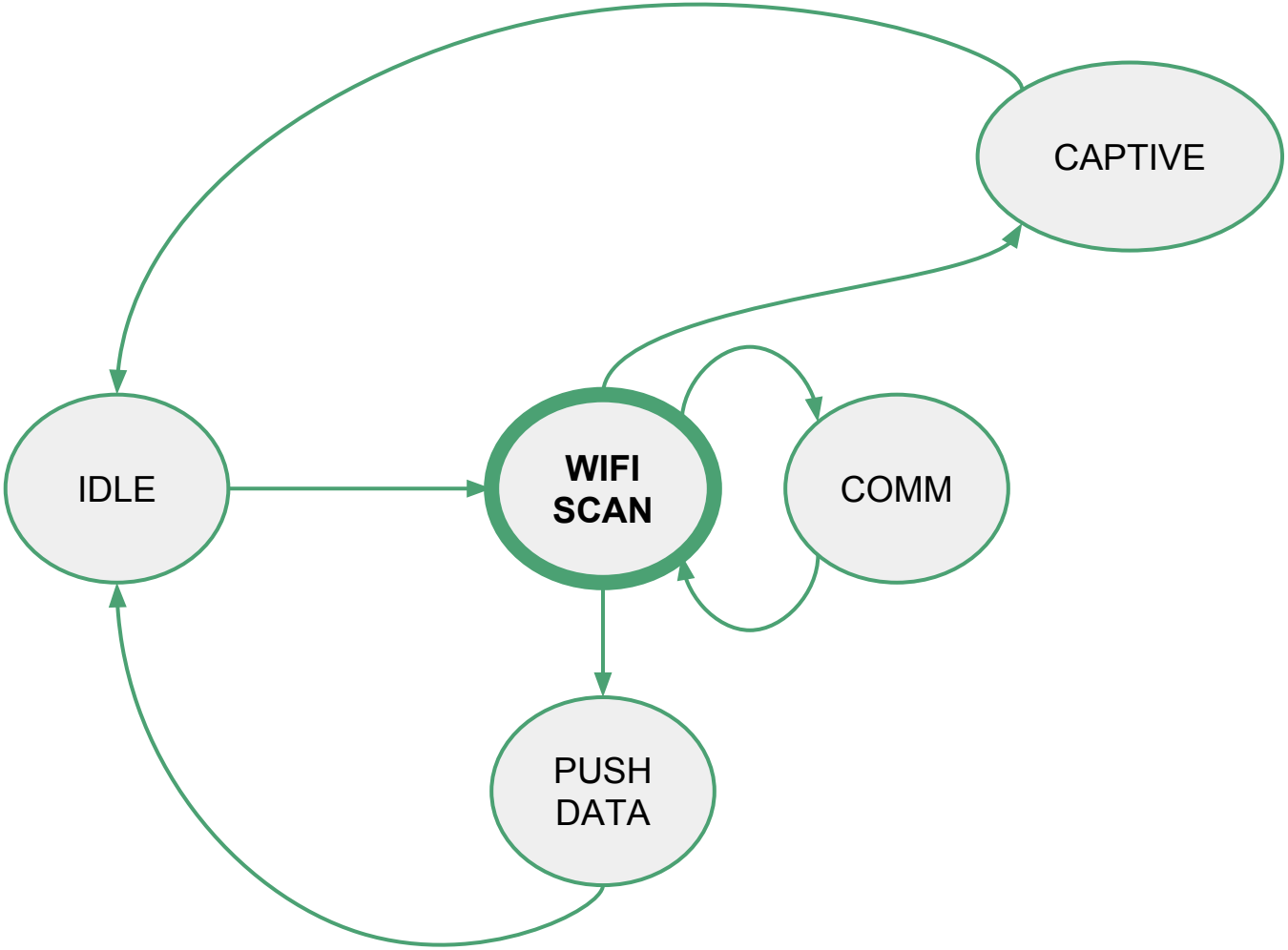
Software: Designing a general Wifi Attack



Software: Designing an attack for our Hacking Token



Software: Designing an attack for our Hacking Token



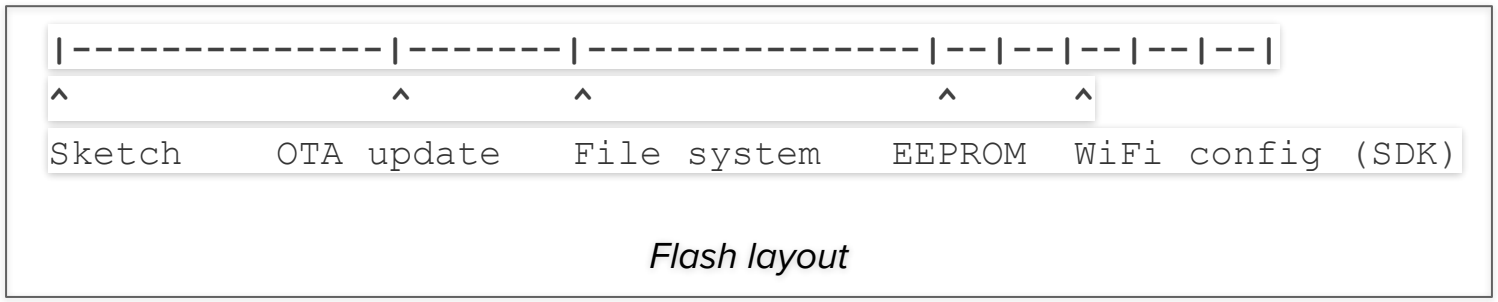
Loop state

Wifi Scan

- **Hacking Token as wifi client**
- **Scan for available wifi**
- **Will get ESSID, BSSID and PWR**
- **Use SPIFFS to store data**

SPIFFS

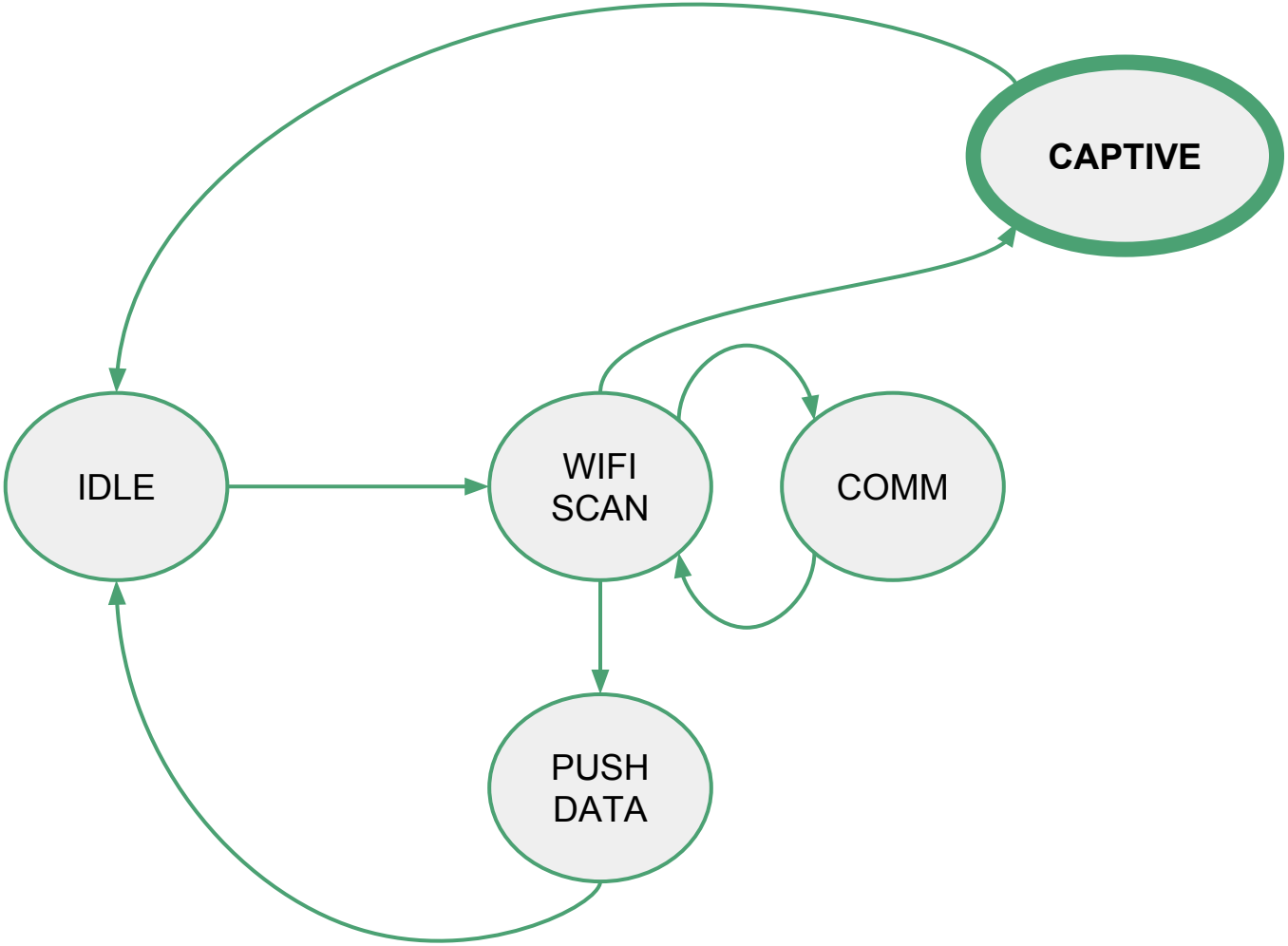
- File system stored on the same flash as the program
- Store sketch data, config files, web server content...
- FS size depends on the flash chip size
- Uploading a new sketch does not modify FS
- Same access modes as fopen in C: r, r+, w, w+, a, a+
- Some limitations: 31 chrs per file path, mandatory /data folder...



Flash layout

https://github.com/esp8266/Arduino/blob/master/doc/filesystem.rst

Software: Designing an attack for our Hacking Token



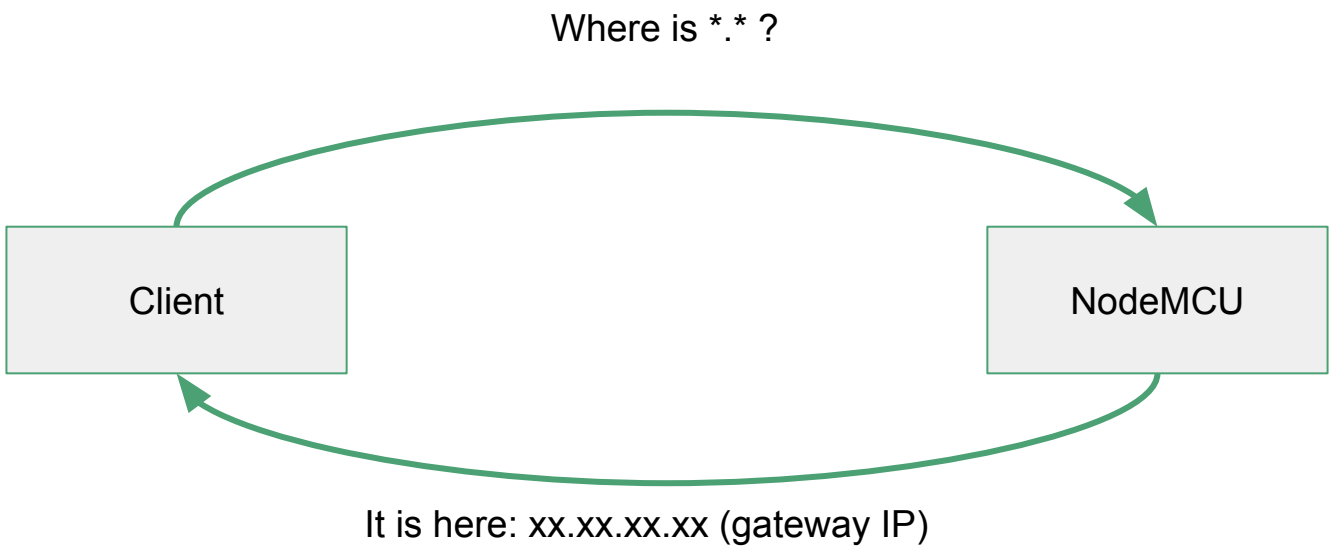
Attack module

Captive

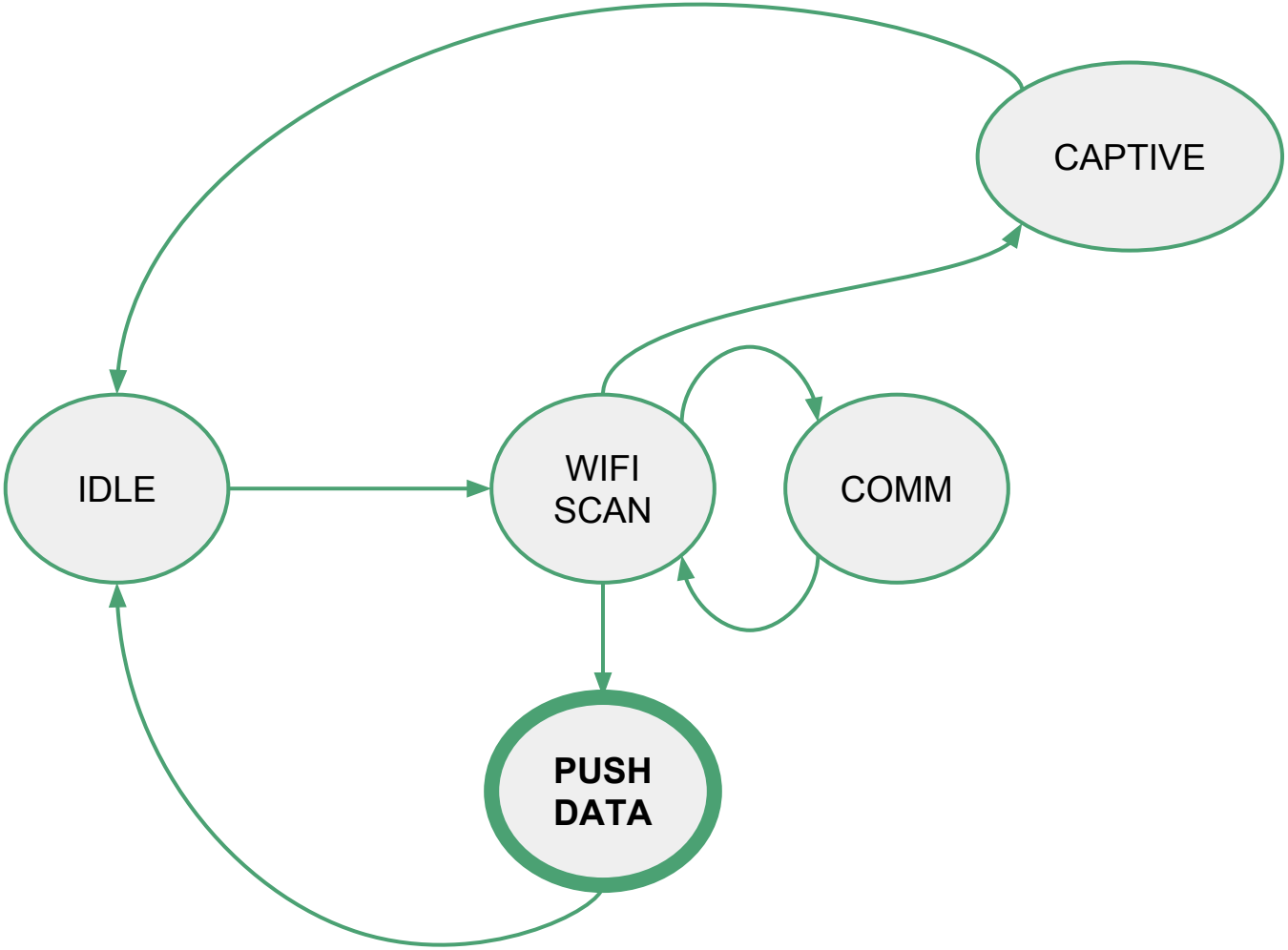
- **Hacking Token as AP**
- **Captive files on SPIFFS**
- **DNS server**

DNS server

- Serve fake captive files on AP’s gateway IP
- Resolve all requests to gateway
- WiFi sign in notification appears
- Captive portal handlers don’t care about HTTPS



Software: Designing an attack for our Hacking Token



Retrieve Data

Push Data

- **Hacking Token as client**
- **Connect to a reliable AP**
- **Send stored file**
- **Empty log file**

-

- **Server overview:**
  - **Built over python's BaseHTTPRequestHandler**
  - **Encrypted traffic**
  - **Unique id. with BasicAuth**
  - **Creds hased with PBKDF2**

Fork us!

@HackingTokens

PlatformIO

- **PlatformIO core (CLI utility)**
- **Official IDEs over Atom and VS**
- **Serial port monitor**
- **Library management system**
- **Multi-project**
- **Theme support**
- **Cross-platform support**
- **CI & Remote unit testing**

“An Open Source ecosystem for IoT development”

Results

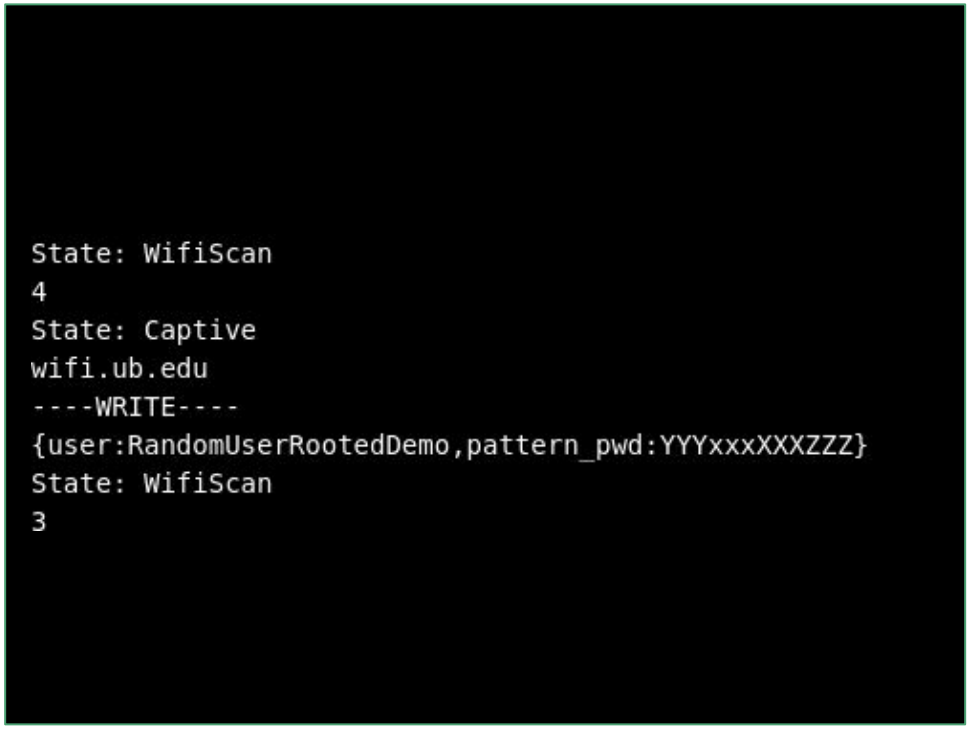
Results

Evil twin (fake captive portal)

- **Fake UB’s captive portal**
- **Able to capture and log credentials data**
- **No real users data has been stored**

Results: Evil twin (fake captive portal)

Results: Evil twin (fake captive portal)

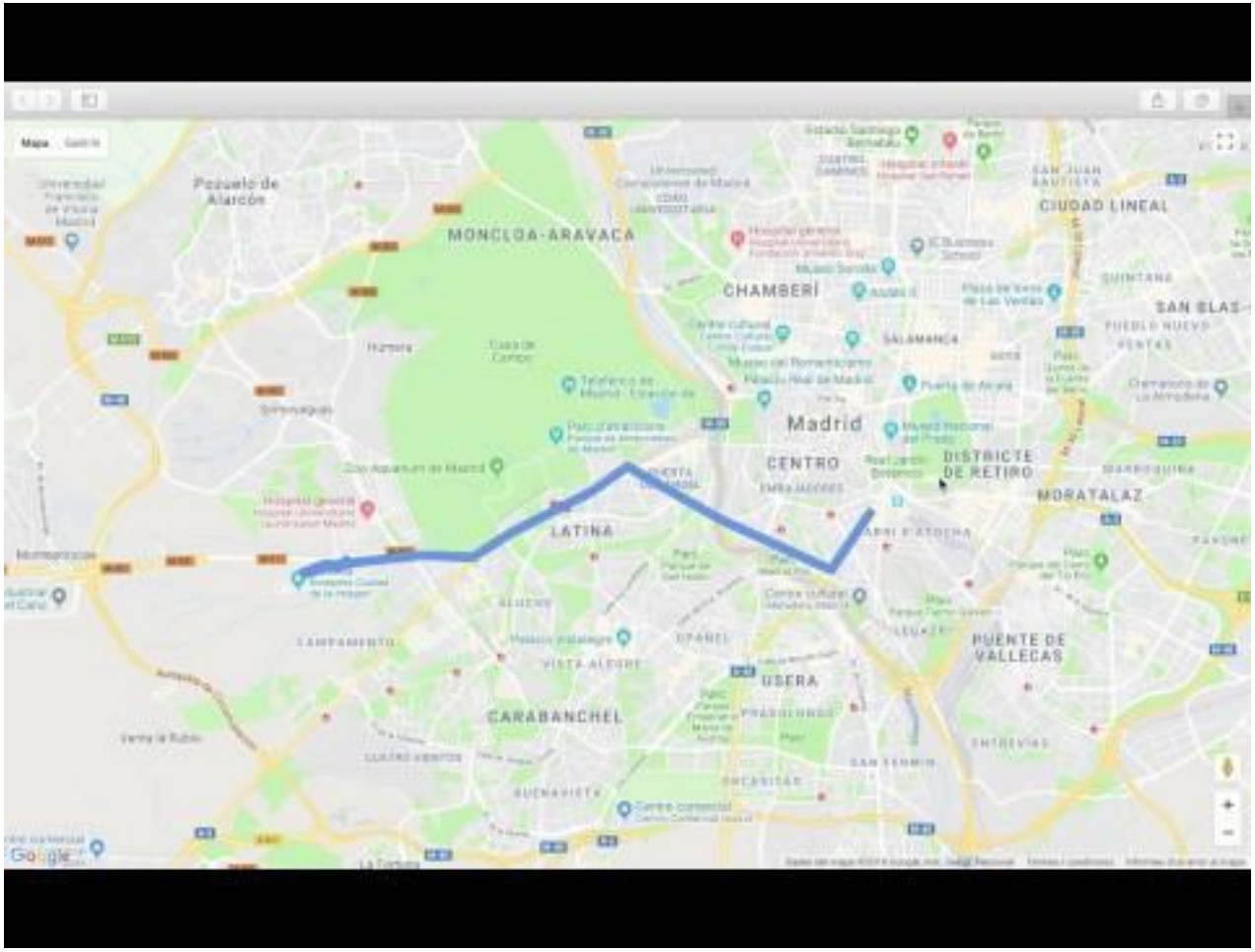


Results

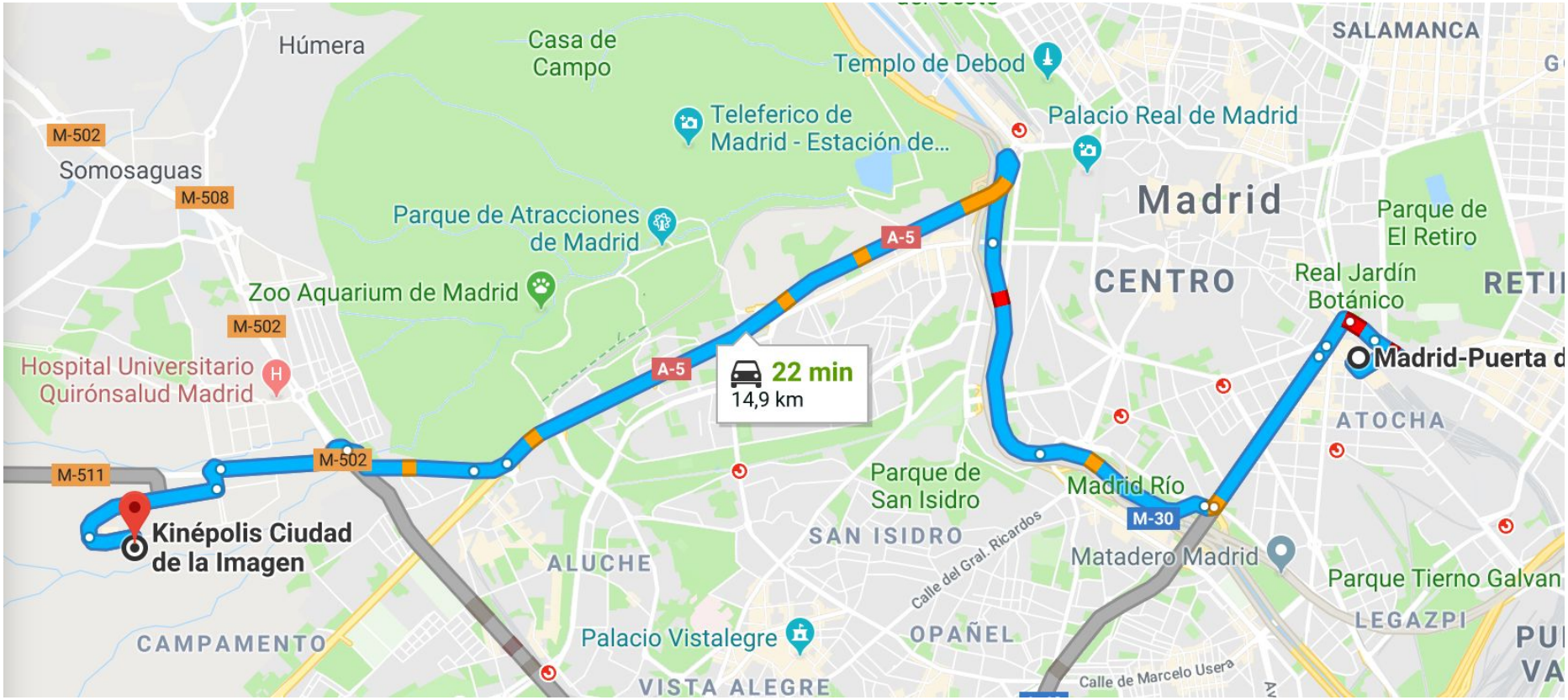
Geolocation

- **Google API**
- **Trace route based on WiFi APs**
- **Compare with real routes**

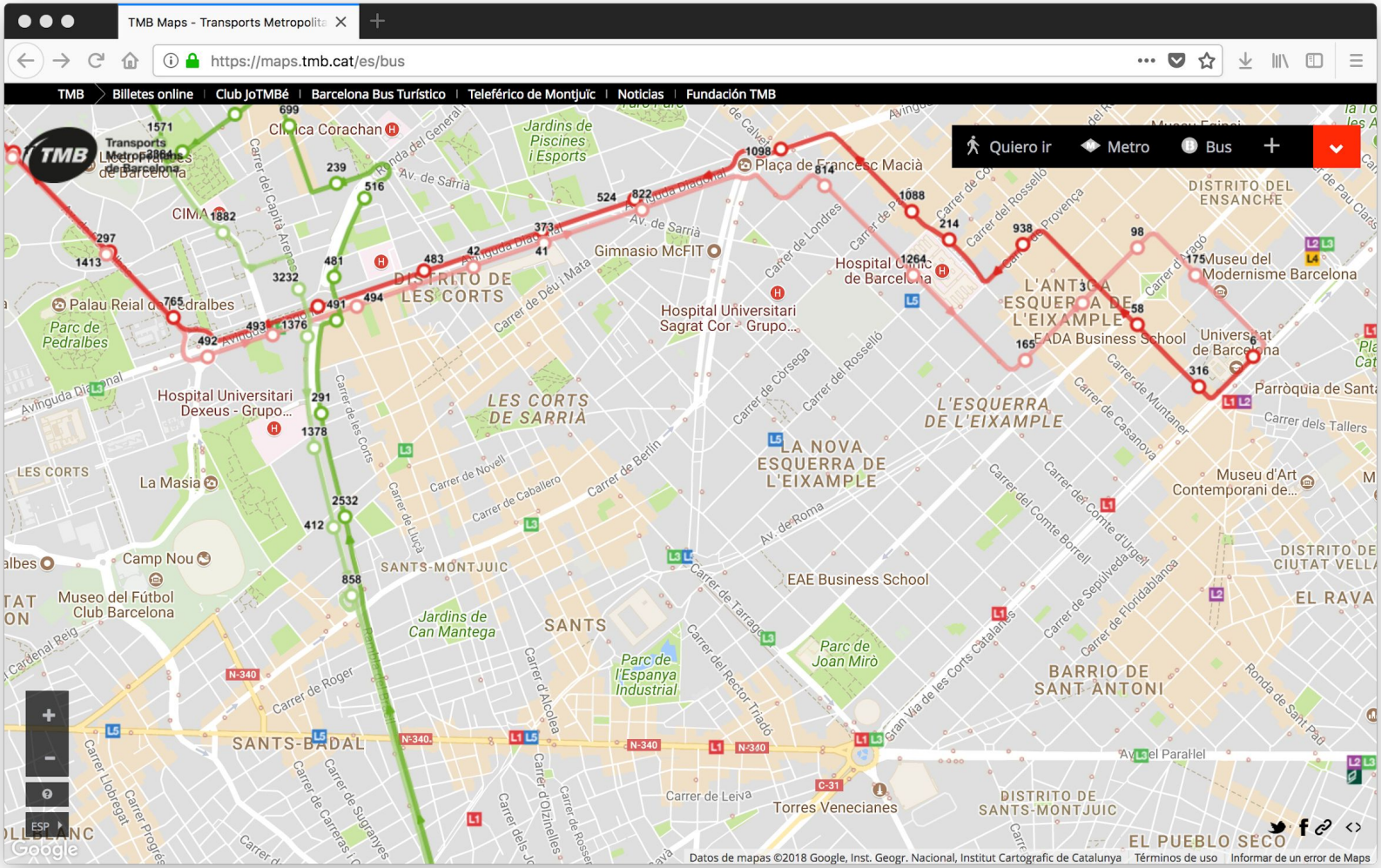
Results: Geolocation



Results: Geolocation



Results: Geolocation



Results

Bonus: Open AP (BadUSB)

- **Simple BadUSB**
- **Focused on Android devices**
- **Some limitations/requirements**
- **Funny AP**

Bonus: Open AP (BadUSB)

Conclusions

Conclusions

- **Successful PoC study**
- **Hardware viability**
- **Dedicated and isolated vector attacks**
- **Two direct attacks proved**
- **One post-processed attack**

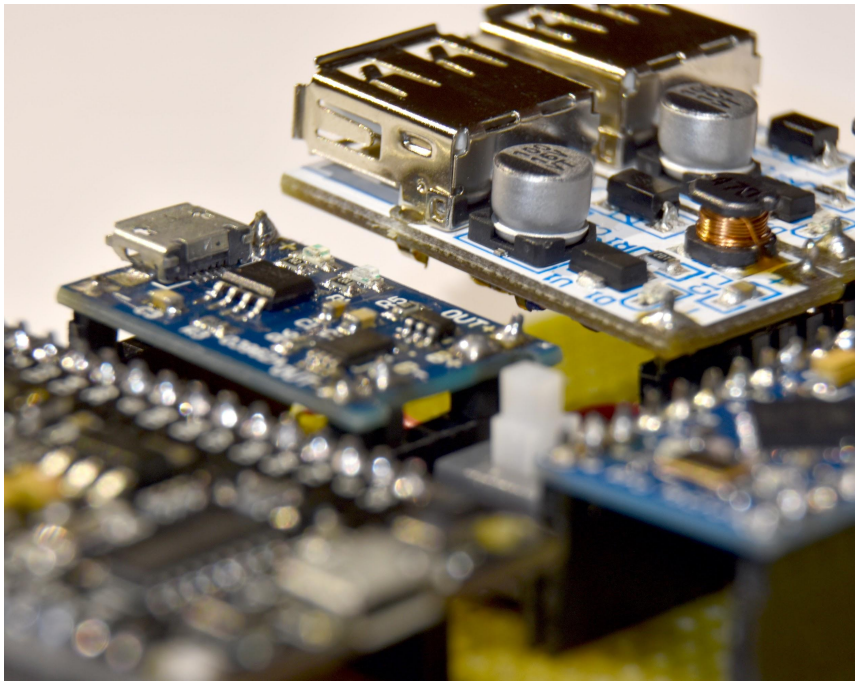
TODO

- Atmega32u4 @ 3.3V 8MHz
- Better current sensing
- Internal SPI/I2C protocol
- LED/LCD/TFT output

-

- OTA Firmware updates
- Wi-Fi Monitor mode
- USB Host (MAX3421E)
- Bluetooth (ESP32)

Acknowledgments



- **Paul Charbonneau** | PCB design
- **Alejandro Codina** | IT support
- **Gerard Finol** | WifiScan module and data processing
- **Enric Florit** | Server development and management
- **Isaac Godoy** | Hardware development and integration
- **David Martínez** | Modules integration and project refactor

-

- **Universitat de Barcelona** | Subsidized some of the materials and allowed us to perform PoCs on its network

Questions

Thank you!

@ismansiete

ibenito@el.ub.edu

isman7

@arnaugamez

arnau@hackinglliure.org

arnaugamez

Hacking Tokens: A Massive PoC

Ismael Benito | Arnau Gàmez

UNIVERSITAT DE BARCELONA

Fisitrónica

HACKING LLIURE

/RootedCON