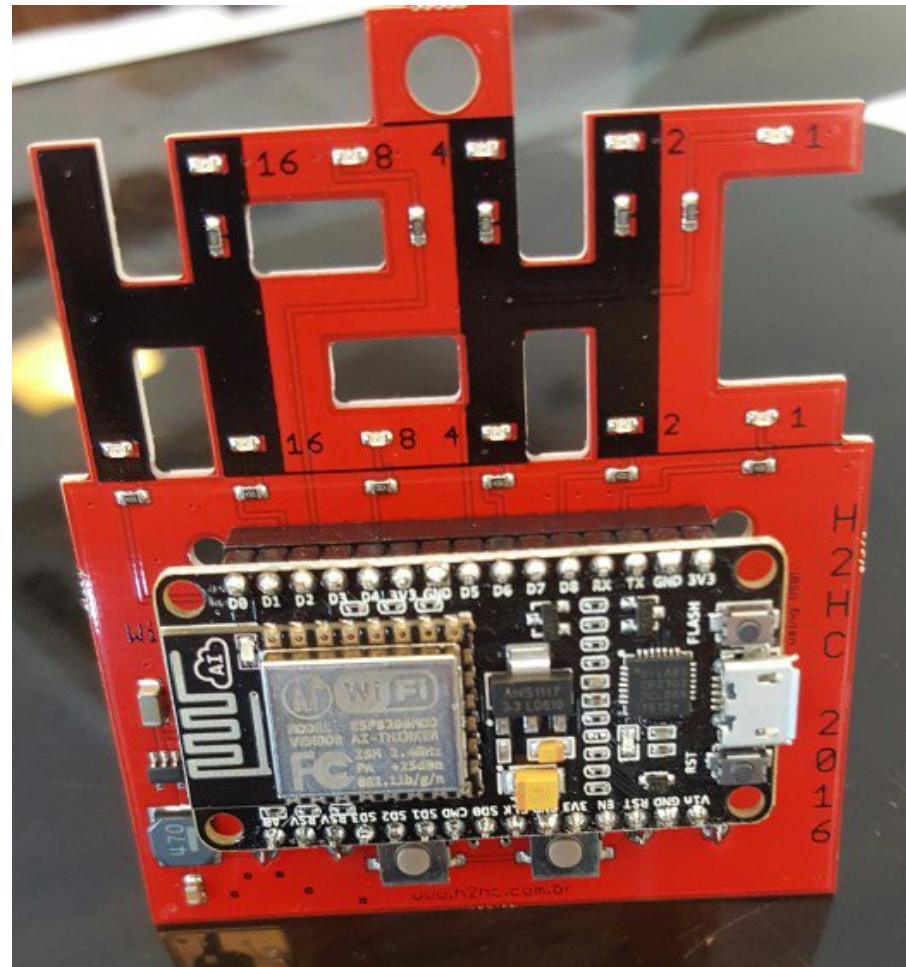


Badge H2HC 2016



Inspiração



Conhecer as limitações do esp8266 para explorar falhas em implementações alheias, através de uma POC que explore os limites do hardware.

Inspiração



Insegurança na Era da Internet das Coisas

Palestrante:

Christiane Borges Santos

14º Congresso Latino-americano de Software Livre e Tecnologias Abertas

Insegurança na Era da Internet das Coisas



≡ MENU | **techtudo** VIDA DIGITAL
INTERNET

20/01/2014 15h43 - Atualizado em 20/01/2014 15h50

Botnet envia spam na web com ajuda de Smart TVs e geladeira conectada

A empresa de segurança virtual Proofpoint identificou um grande ataque de botnets que vitimizou cerca de 100 mil aparelhos 'smart' entre os dias 23 de dezembro e 6 de janeiro de 2014.



Insegurança na Era da Internet das Coisas

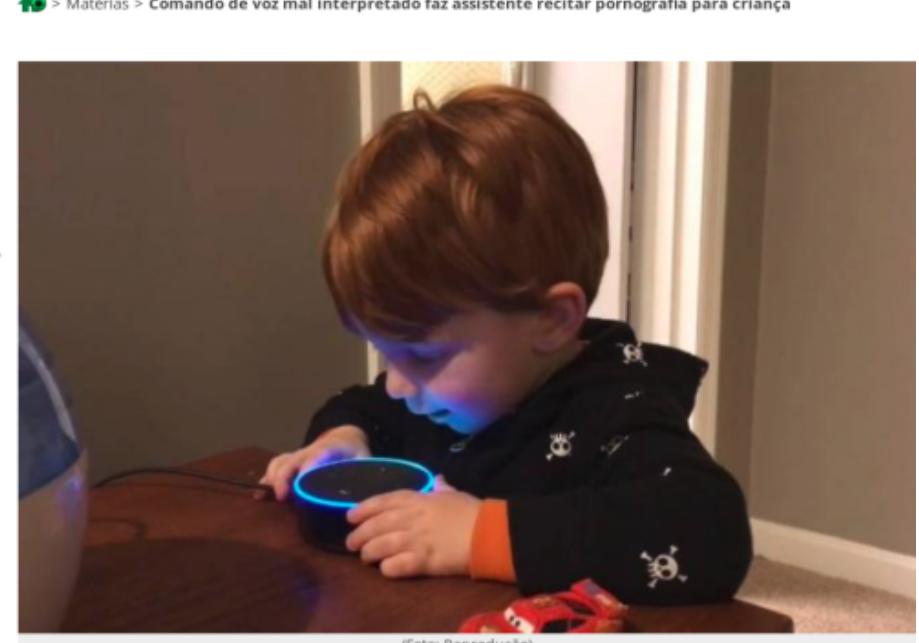


<https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud>

A screenshot of a Guardian news article. The title is "Goodbye privacy, hello 'Alexa': Amazon Echo, the home robot who hears it all". Below the title is a sub-headline: "We had **Rory Carroll** invite 'Alexa' aka the Echo into his home. There was helpful cooking assistance, endless facts and figures, an amusing misunderstanding - and concerns over what exactly Amazon does with all that interaction data". On the left, there's a sidebar with social sharing icons (Facebook, Twitter, Email) and a photo of Rory Carroll. The main content area shows a black Amazon Echo device. At the bottom, there's a caption: "Amazon Echo: 'I followed my instinct - which was to placate the machine.' Photograph: AP".

Is Alexa working for the CIA? Video shows owner asking Amazon's smart assistant if it is connected to the intelligence agency - causing it to shut down repeatedly

<https://goo.gl/Vx5hQh>



Comando de voz mal interpretado faz assistente recitar pornografia para criança

Insegurança na Era da Internet das Coisas



É só um brinquedo...

CloudPets

tecnoblog CURTIR

Segurança

Brinquedo conectado à internet vaza dados de crianças

By [Jean Prado](#)

3 de março de 2017

BBC Menu Q

BRASIL Seções

Autoridades alemãs fazem alerta contra boneca que pode ser hackeada para espionar crianças

17 fevereiro 2017



GETTY IMAGES

Segundo especialistas, é possível hackear a boneca My Friend Cayla

Insegurança na Era da Internet das Coisas



≡ MENU

techtudo

ELETRÔNICOS

10/07/2014 07h30 - Atualizado em 10/07/2014 07h30

Lâmpadas inteligentes são hackeadas para furto de senhas de Wi-Fi

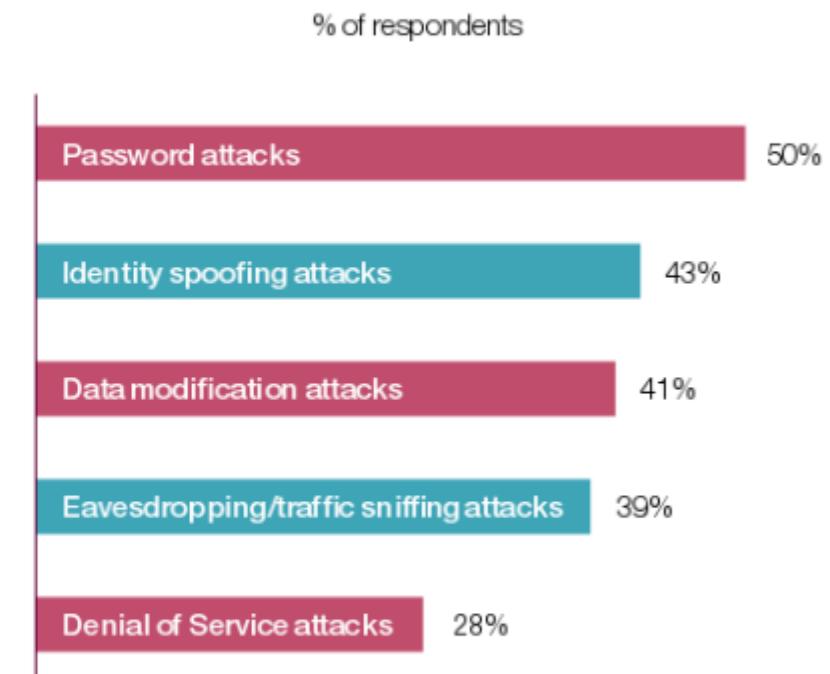


Lâmpadas inteligentes tem vulnerabilidade grave (Foto: Divulgação/LIFX)

Insegurança na Era da Internet das Coisas



Top Security Threats to IoT Products



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014

Ação

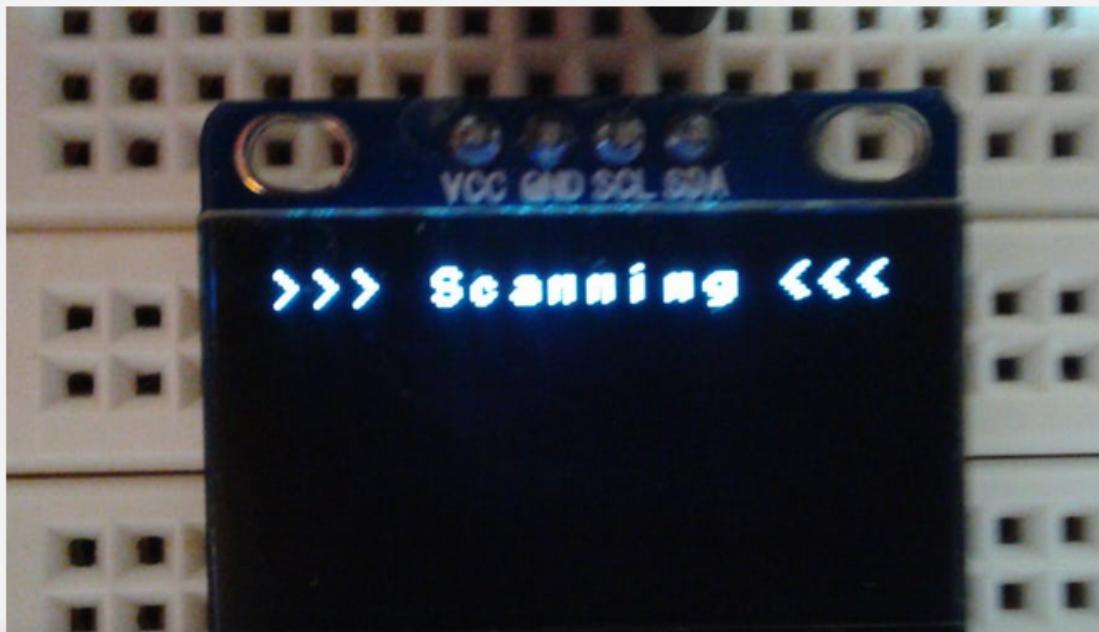


Conhecer as limitações do esp8266 para explorar falhas

<https://www.hackster.io/rayburne/warwalking-a9c021>

Warwalking with the ESP8266

Made by [Ray Burnette](#) - Published in [Everything ESP](#)



ABOUT THIS PROJECT

Warwalking is the pedestrian version of wardriving but in this case we are using an ESP8266+OLED powered by a single lithium 3.2V AA cell.

► arduino ► oled ► wardriving

PROJECT INFO

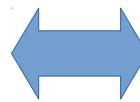
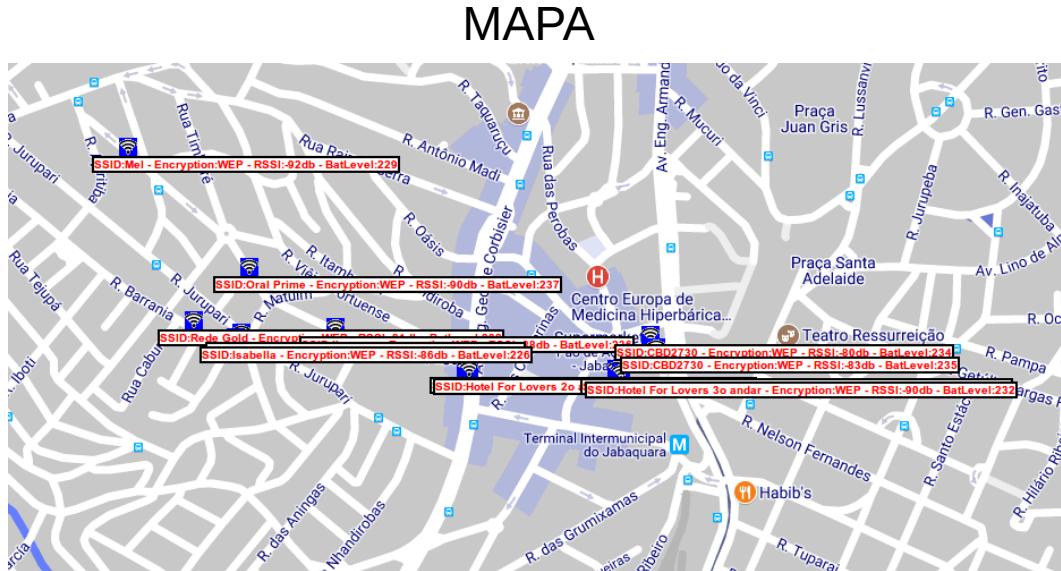
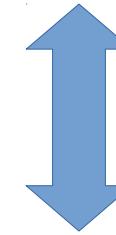
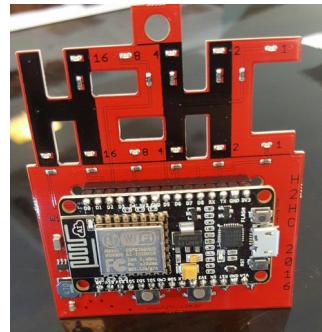
| | |
|------------|------------------------------|
| Type | ► Full instructions provided |
| Difficulty | Intermediate |
| Published | July 19, 2015 |
| License | CC BY |

Proof of concept

Modelo prático que possa provar o conceito (teórico) estabelecido por uma pesquisa.

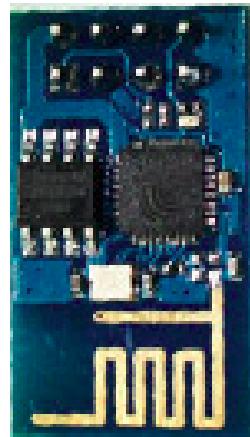
- Investigar limites do hardware, com foco na seg.
- Criar um scanner de redes wi-fi com data log
- Permitir geo-localização dos dados
- Backend com ferramentas de extração

Diagrama



BACKEND

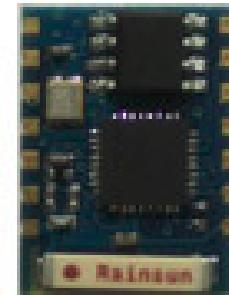
ESP8266



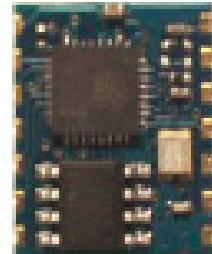
ESP-01



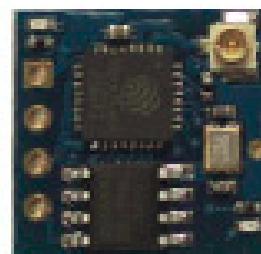
ESP-02



ESP-03



ESP-04



ESP-05



ESP-06



ESP-07



ESP-08



ESP-09



ESP-10



ESP-11

NODE MCU



Eletrônica e Mods - 3D



Base_GPS.scad — OpenSCAD

Editor

```
1
2
3 base size = 32.5;
4 base apoio = 1.5;
5 h base = 1;
6 h apoio = 5;
7
8 cube([base size, base size,
       h base]);
9
10 translate([0,0,h base])
      difference(){
11
12   cube([base size,
13         base size, h apoio]);
14
15   translate([base apoio,
16             base apoio,0])
17     cube([base size - (
```

Console

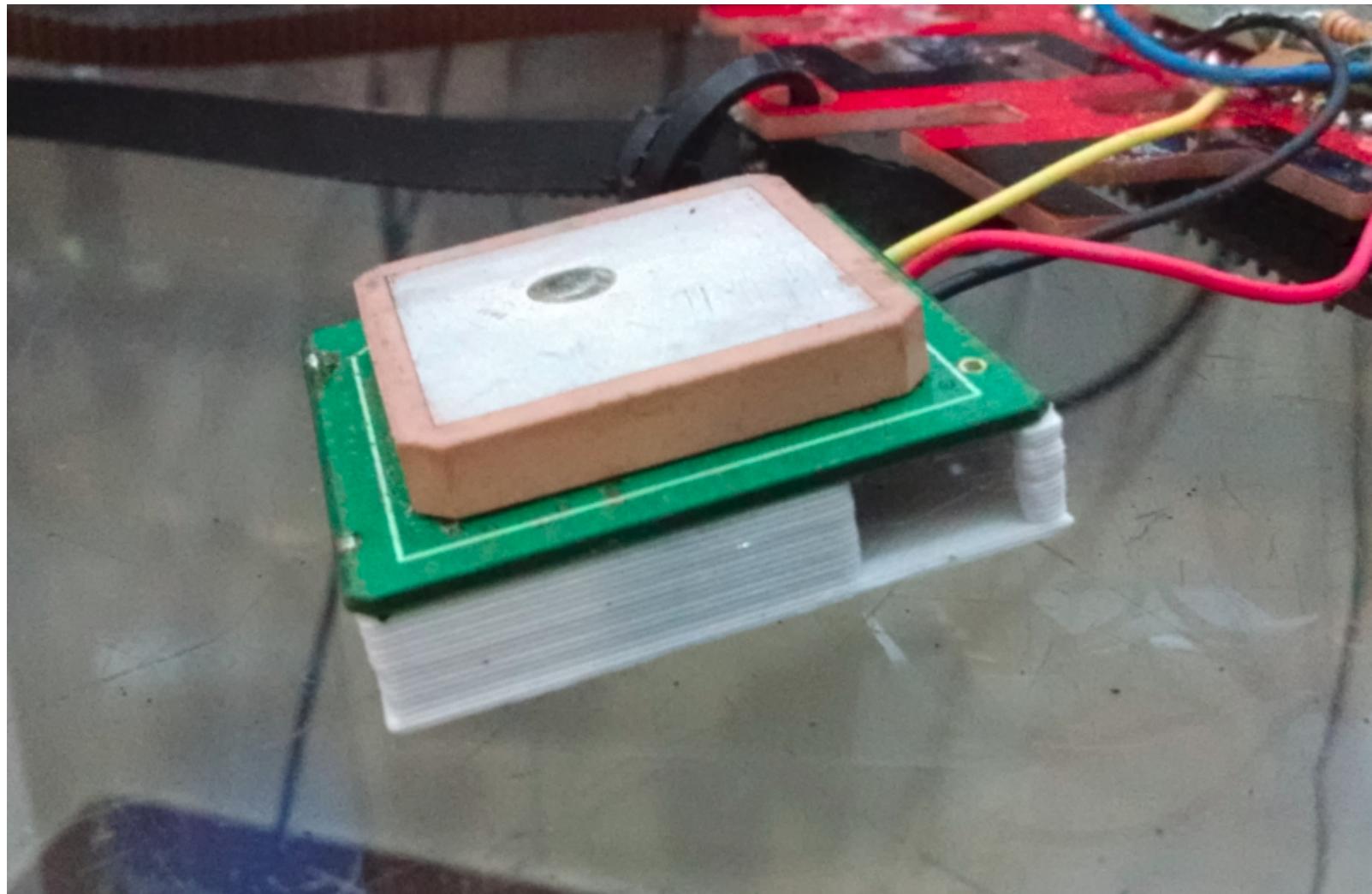
```
Geometry cache size in bytes: 5824
CGAL Polyhedrons in cache: 3
CGAL cache size in bytes: 131792
Total rendering time: 0 hours, 0 minutes, 0 seconds
Top level object is a 3D object:
Simple: yes
Vertices: 32
Halfedges: 96
Edges: 48
Halffacets: 36
Facets: 18
Volumes: 2
Rendering finished.
```

Viewport: translate = [11.84 38.73 -5.37], rotate = [55.00 0.00 34.80], distance = 192.04

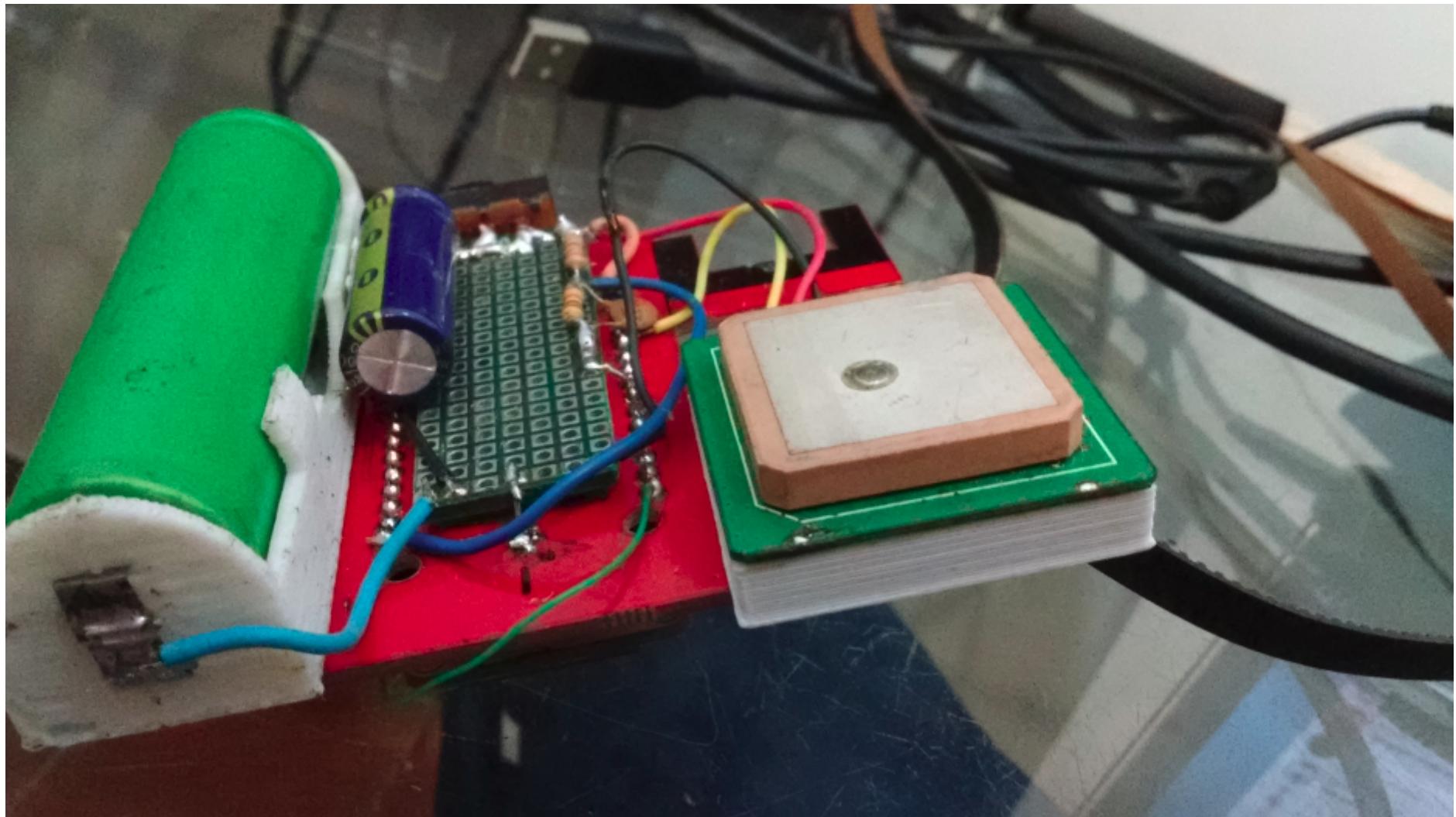
OpenSCAD 2015.03

14 / 27

Eletrônica e Mods - GPS



Eletrônica e Mods - Supply



FIRMWARE - Arduino



FIRMWARE - Considerações



|

```
const char *softAP_ssid = "HACKUDO_CUIDADO";
const char *softAP_password = "12345678";

/* hostname for mDNS. Should work at least on windows. Try http://esp8266.local */
const char *myHostname = "esp8266.local";

/* Don't set this wifi credentials. They are configurated at runtime and stored on EEPROM */
char ssid[32] = "";
char password[32] = "";

// DNS server
const byte DNS_PORT = 53;
DNSServer dnsServer;
```

Arquivo de dados

SSID – RSSI – Lat – Lng – Battery level

Rodrigo|Auto|-72|-23.64202000|-46.64996500|235|
dobmoto|Auto|-72|-23.64202000|-46.64996500|235|
JMS-JOMASI|WPA2|-84|-23.64202000|-46.64996500|235|
CBD2730|WEP|-80|-23.64490333|-46.64160000|234|
dobm_spare|Auto|-92|-23.64202000|-46.64996500|235|
RedeDaSilva2|Auto|-91|-23.64202000|-46.64996500|235|
lkreuser|WEP|-88|-23.64475500|-46.64756500|236|
Oral Prime|WEP|-90|-23.64371000|-46.64920167|237|
dobmoto_porteira|WPA2|-48|-23.64202000|-46.64996500|235|
Rodrigo|Auto|-77|-23.64198833|-46.64997500|229|
dobmoto|Auto|-76|-23.64198833|-46.64997500|229|
kawakubo2|WPA|-90|-23.64198833|-46.64997500|229|
Hotel For Lovers 2o andar|WEP|-92|-23.64549500|-46.64504167|235|
JMS-JOMASI|WPA2|-82|-23.64198833|-46.64997500|229|
dobm_spare|Auto|-88|-23.64198833|-46.64997500|229|
dobmoto_porteira|WPA2|-50|-23.64198833|-46.64997500|229|
NANA63|Auto|-89|-23.64198833|-46.64997500|229|

Backend



| | | | |
|---|----------------------------------|-----|--------------------------|
| - | h2hc_badge | 280 | if |
| | ▶ JavaScript Resources | 281 | |
| | ▶ PHP Language Library [PHP 7.1] | 282 | |
| | ▶ PHP Include Path | 283 | |
| | ▶ CSS | 284 | var customMapTy |
| | ▶ fonts | 285 | var customMapTy |
| | ▶ imagens | 286 | map.mapTypes.s |
| | ▶ include | 287 | map.mapTypes.s |
| | ▶ config.php | 288 | |
| | ▶ database.php | 289 | <i>// Create the DI</i> |
| | ▶ js | 290 | <i>// passing in thi</i> |
| | ▶ ole | 291 | var homeControl |
| | ▶ utilidades | 292 | var homeControl |
| | ▶ index.js | 293 | |
| | ▶ index.php | 294 | homeControlDiv. |
| | ▶ mapa.php | 295 | map.controls[go |
| | | 296 | |
| | | 297 | var diaNoiteCont |

Banco de dados e analise



File Edit View Query Database Server Tools Scripting Help

Management Schemas | MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Sets

Query 2 | pedido_status | consultor | SQL File 3* | SQL File 4* | log_badge - Table | Administration - Users and Privileges

Limit to 50000 rows

```
11     lng decimal(15,9),
12     auth varchar(128),
13     bat int
14 );
15
16 • select * from log_badge;
```

Result Grid Filter Rows:

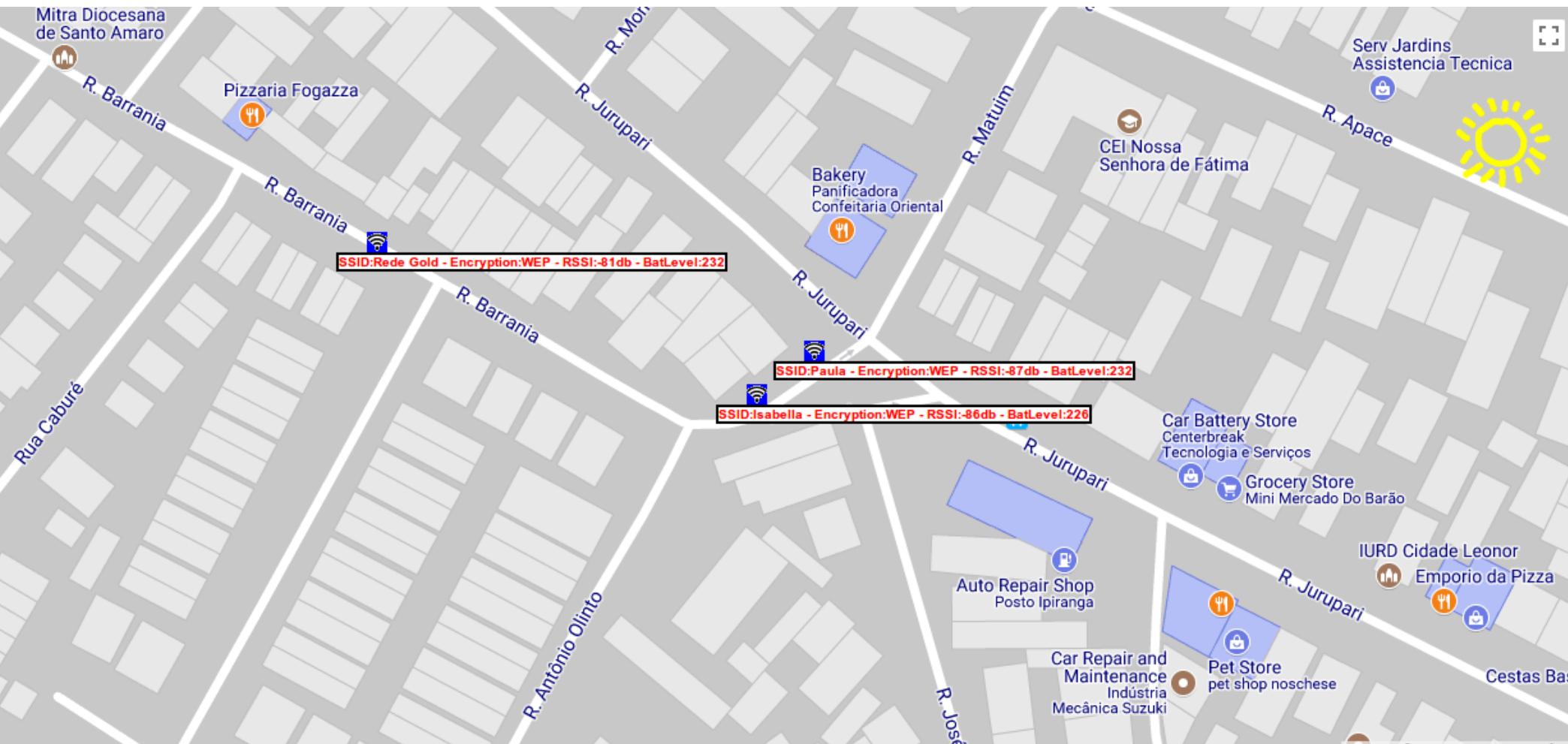
| # | id | ssid | rssi | lat | lng | auth | bat |
|----|----|--------------------|------|---------------|---------------|------|-----|
| 25 | 25 | Sabrina | -90 | -23.642246670 | -46.649976670 | Auto | 230 |
| 26 | 26 | Rodrigo | -92 | -23.642246670 | -46.649976670 | Auto | 230 |
| 27 | 27 | kawakubo2 | -87 | -23.642246670 | -46.649976670 | WPA | 230 |
| 28 | 28 | Sem Sinal | -88 | -23.642246670 | -46.649976670 | WPA2 | 230 |
| 29 | 29 | DIRECT-AP[TV][...] | -89 | -23.642246670 | -46.649976670 | WPA2 | 230 |
| 30 | 30 | antonio davi | -80 | -23.642246670 | -46.649976670 | WPA2 | 230 |
| 31 | 31 | Vivo-Internet-5778 | -88 | -23.642246670 | -46.649976670 | Auto | 230 |
| 32 | 32 | Kawakubo | -66 | -23.642405000 | -46.649921670 | Auto | 233 |
| 33 | 33 | DIRECT-AP[TV][...] | -65 | -23.642405000 | -46.649921670 | WPA2 | 233 |

log_badge 2

Action Output

| # | Time | Action | Message | Duration |
|---|----------|--|----------------------|-----------|
| 5 | 12:11:44 | select * from log_badge LIMIT 0, 50000 | 0 row(s) returned | 0,00082 |
| 6 | 12:14:56 | select * from log_badge LIMIT 0, 50000 | 3207 row(s) returned | 0,0013 se |

Geoposicionamiento de dados



Conclusão



Além do warwalking, percebe-se que todo contexto de desenvolvimento de código do ESP8266 pode ser explorado em busca de leaks, pois o foco dos exemplos é na facilidade de implementação e não na segurança.

Conclusão



Explorar as limitações do hardware permite saber mais sobre como hackea-lo

Conhecendo os limites de cada ferramenta, é possível utilizar um hardware extremamente barato para coleta de dados, Armazenamento e posterior análise

Perguntas?



Ano que vem tem mais!



Obrigado!!

Daniel Basconcello Filho
daniel@robotizando.com.br



Christiane Borges Santos
christiane.santos@ifg.edu.br



Bibliografias:

Warwalking with ESP8266 - <https://www.hackster.io/rayburne/warwalking-a9c021>

Wikipedia Proof of concept: https://en.wikipedia.org/wiki/Proof_of_concept

Node MCU: http://www.nodemcu.com/index_en.html

Arduino Board for ESP8266: http://arduino.esp8266.com/stable/package_esp8266com_index.json

Google maps API for DEVS: <https://developers.google.com/maps/?hl=pt-br>

OpenSCAD: <http://www.openscad.org/>

Projeto REPRAP: www.reprap.org