black hat® EUROPE 2020

DECEMBER 9–10

BRIEFINGS

Manufacturing Hardware Implants from Idea to Mass Production

A Hacker’s Journey

Luca Bongiorni

Speaker’s Intro

- @LucaBongiorni
- Head of Offensive Security at Bentley Product Security
- After this presentation, you will know:
  - How challenging & painful is to mass-produce hacking devices
  - What to do if you have an idea and wanna bring it to life
  - What to avoid, in order to increase chances of success
  - A bit more about WHID Injector, WHID Elite and the upcoming POTAEbox

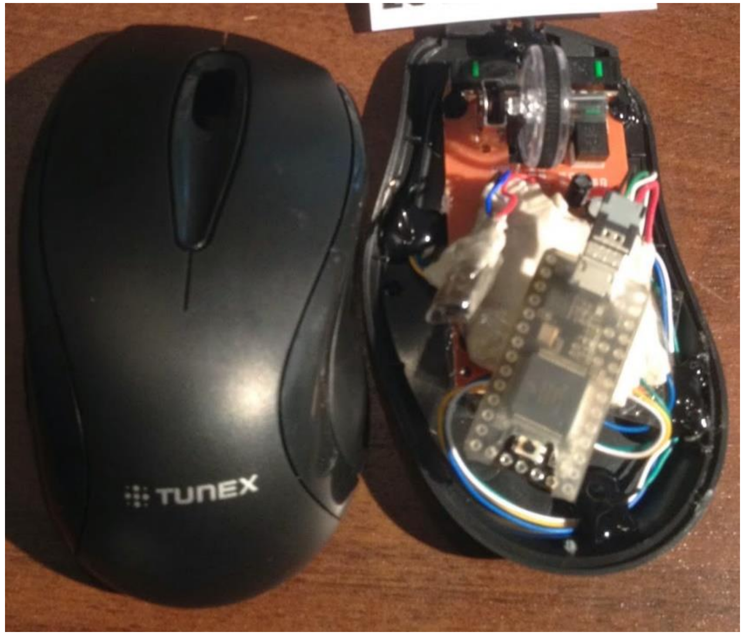
Once Upon a Time… Many Engagements Ago…

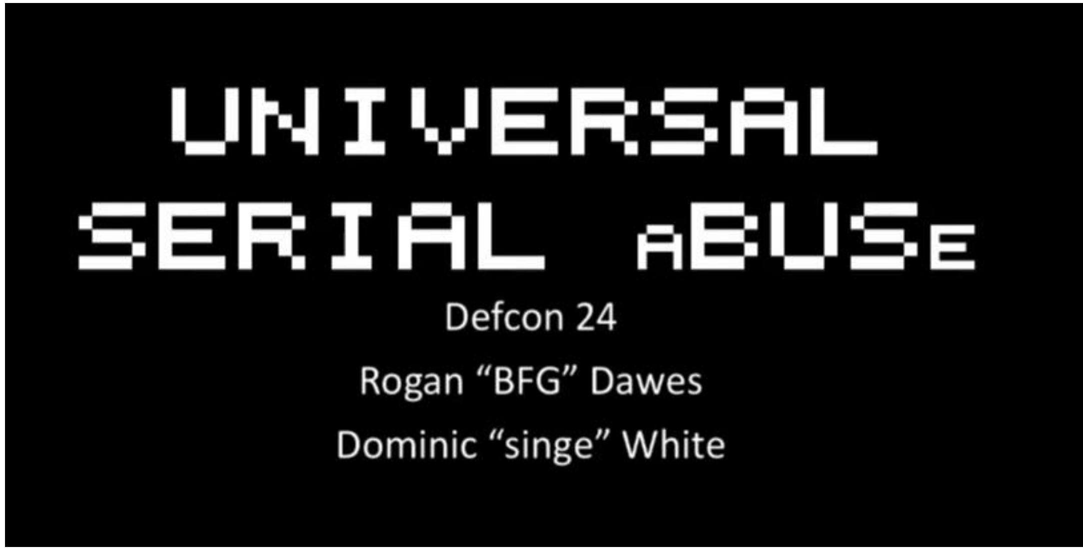
Back in 2010 I wanted to turn this weaponized Mouse into a remotely controlled one.

Sadly, I failed for many reasons:

- Lack of time for R&D
- Lack of a miniaturized RX module
- Not enough room inside the mouse

Eventually, the idea ended up in my never-ending TODO list. Until in 2016…




UNIVERSAL SERIAL aBUSe

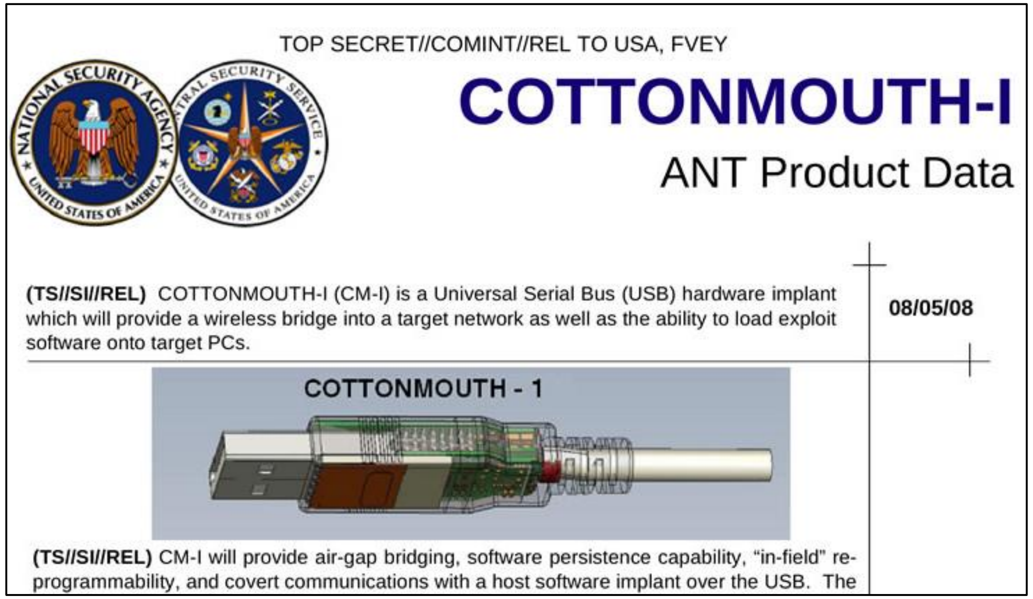
Defcon 24

Rogan “BFG” Dawes

Dominic “singe” White

UNIVERSAL SERIAL aBUSe

- Developed by **@RoganDawes** in 2016
- Bypass Windows Air-Gaps



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

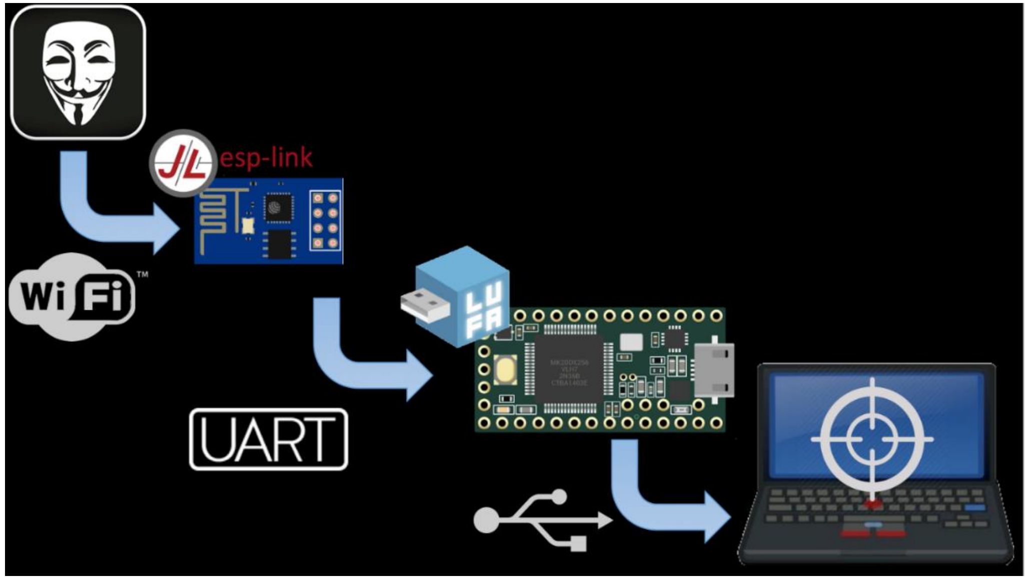
ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The



https://github.com/sensepost/USaBUSe

The Journey

Quarters

Weeks

Days

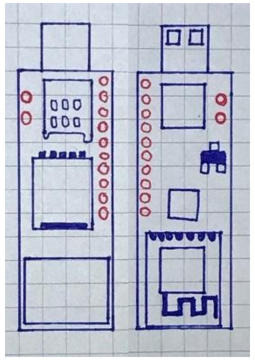
Hours

$$$

$$

$

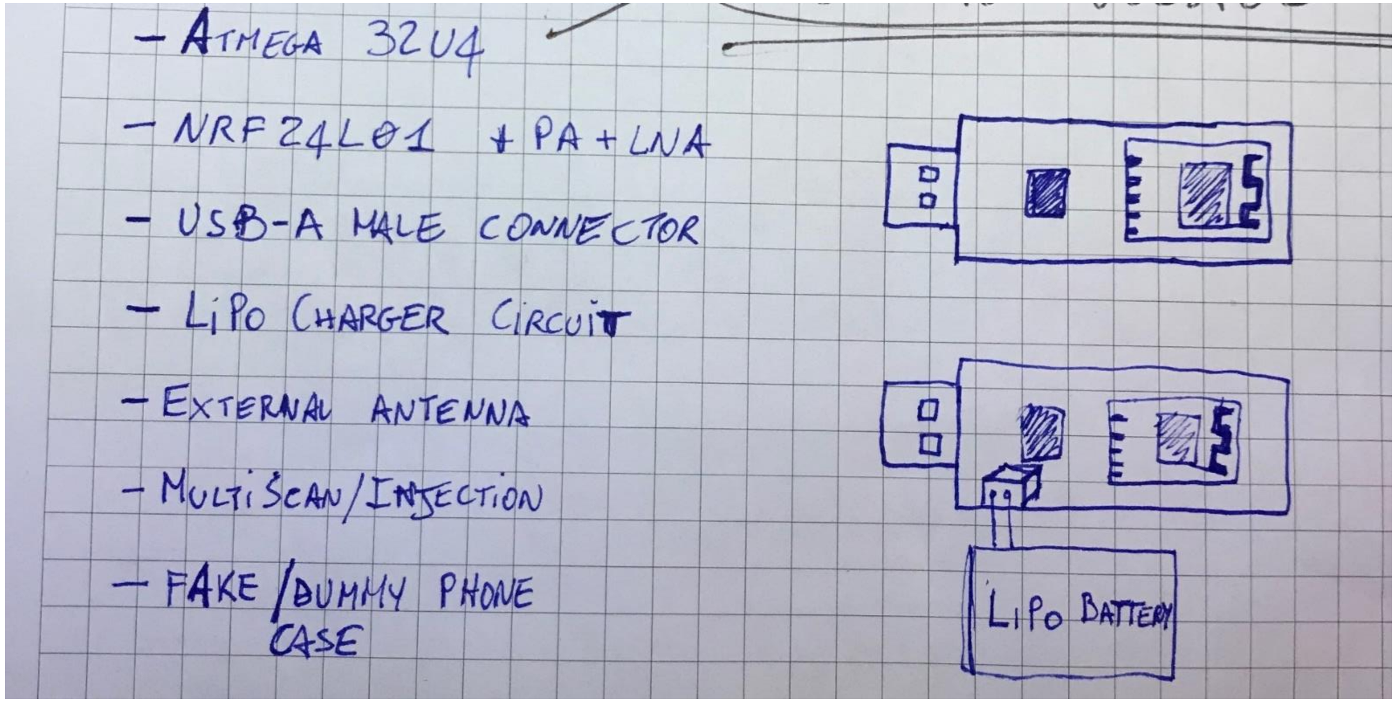
Free



Napkin Sketch

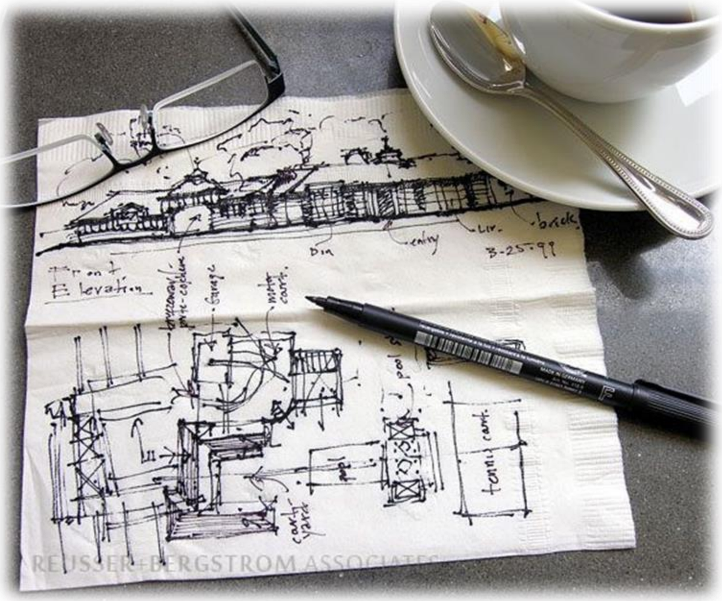
Napkin Sketch

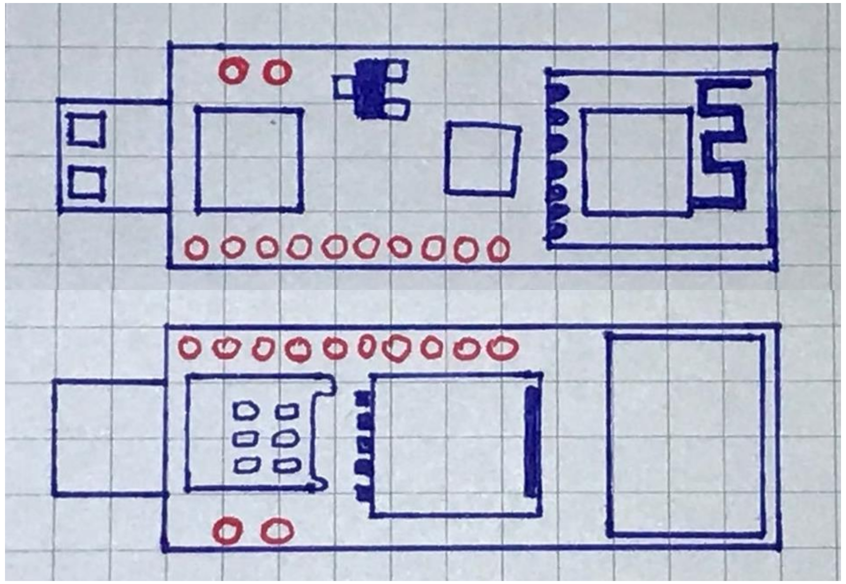
- Dirty Cheap
- Time Needed:
  - Couple of Hours



- ATMEGA 32U4
- NRF24L01 + PA + LNA
- USB-A MALE CONNECTOR
- LiPo CHARGER CIRCUIT
- EXTERNAL ANTENNA
- MULTISCAN/INJECTION
- FAKE/DUMMY PHONE CASE

LiPo BATTERY





The Journey

Quarters

Weeks

Days

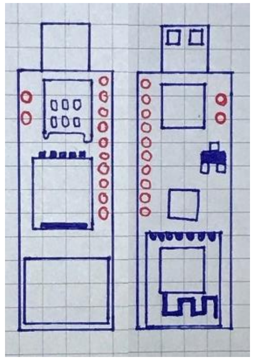
Hours

$$$

$$

$

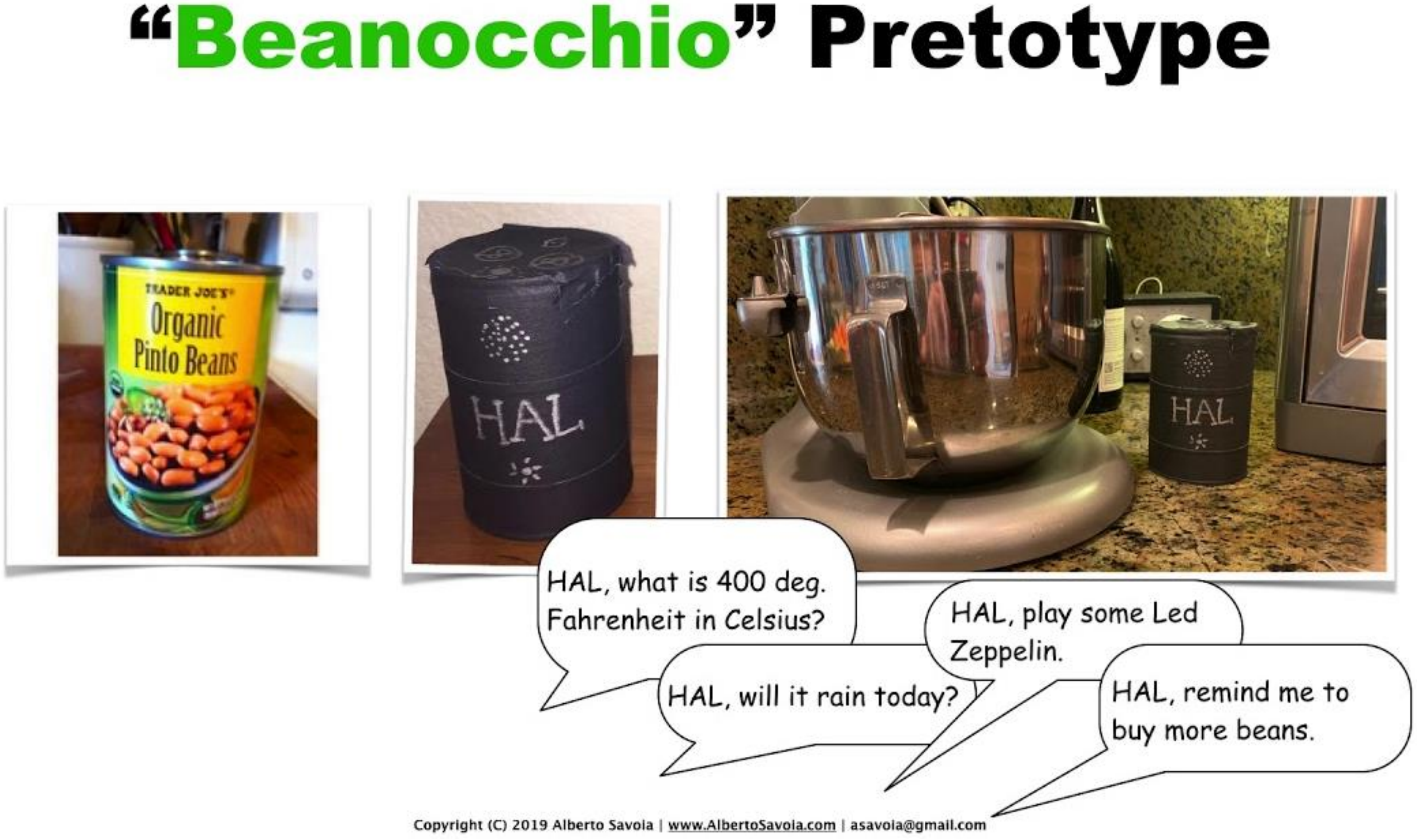
Free



Napkin Sketch

Pretotype

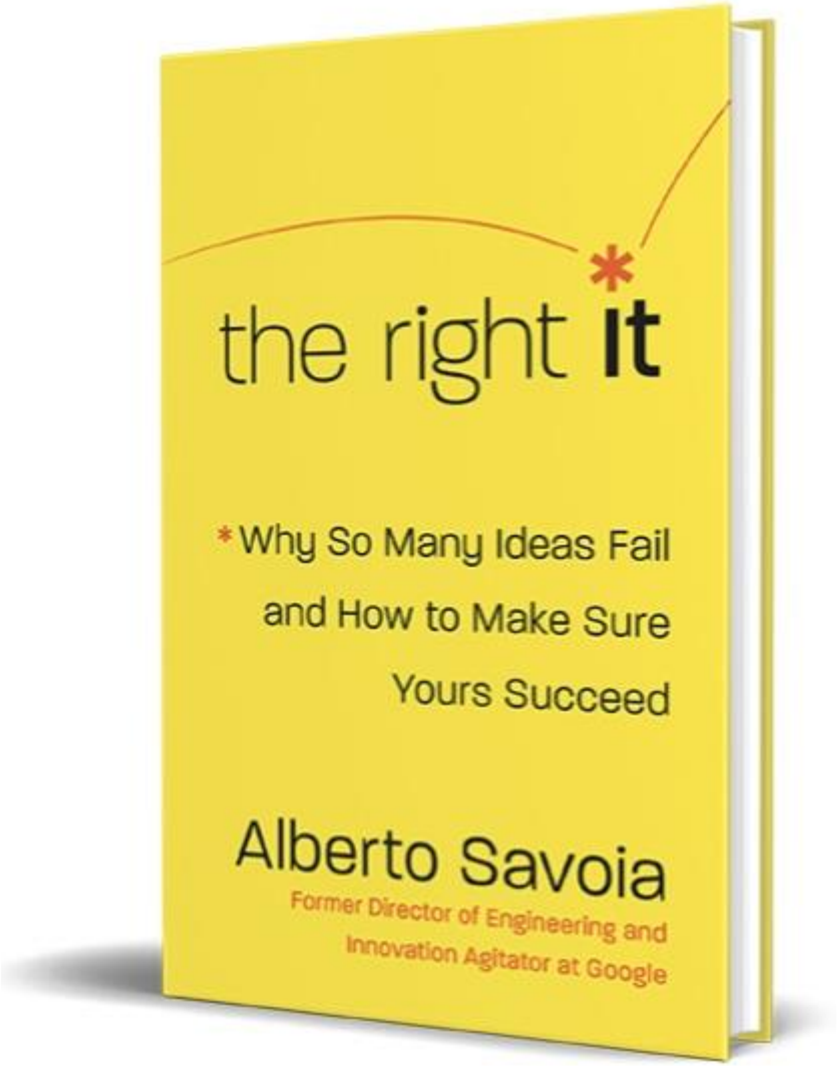
Pretotyping



“Beanocchio” Pretotype

TRADER JOE'S
Organic Pinto Beans
HAL
HAL
HAL, what is 400 deg. Fahrenheit in Celsius?
HAL, play some Led Zeppelin.
HAL, will it rain today?
HAL, remind me to buy more beans.

Copyright (C) 2019 Alberto Savoia | www.AlbertoSavoia.com | asavoia@gmail.com

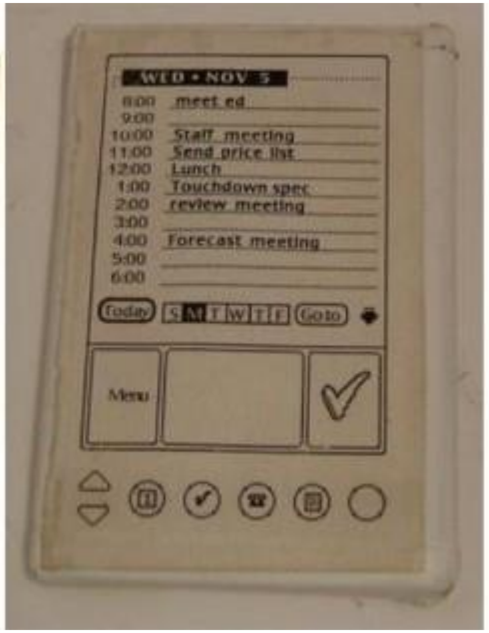


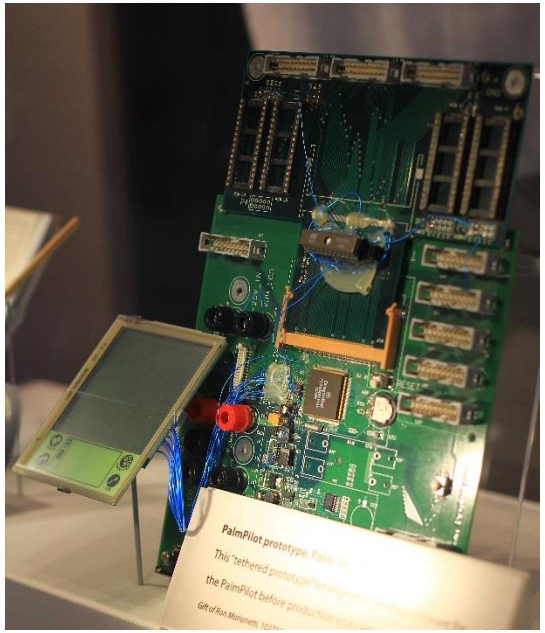
the right It*
*Why So Many Ideas Fail and How to Make Sure Yours Succeed
Alberto Savoia
Former Director of Engineering and Innovation Agitator at Google

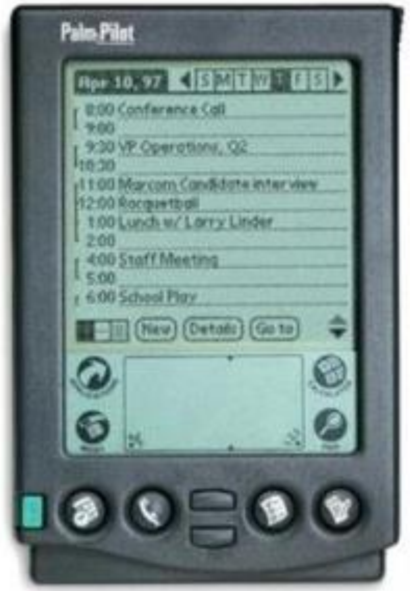
Case Study: The Palm Pilot

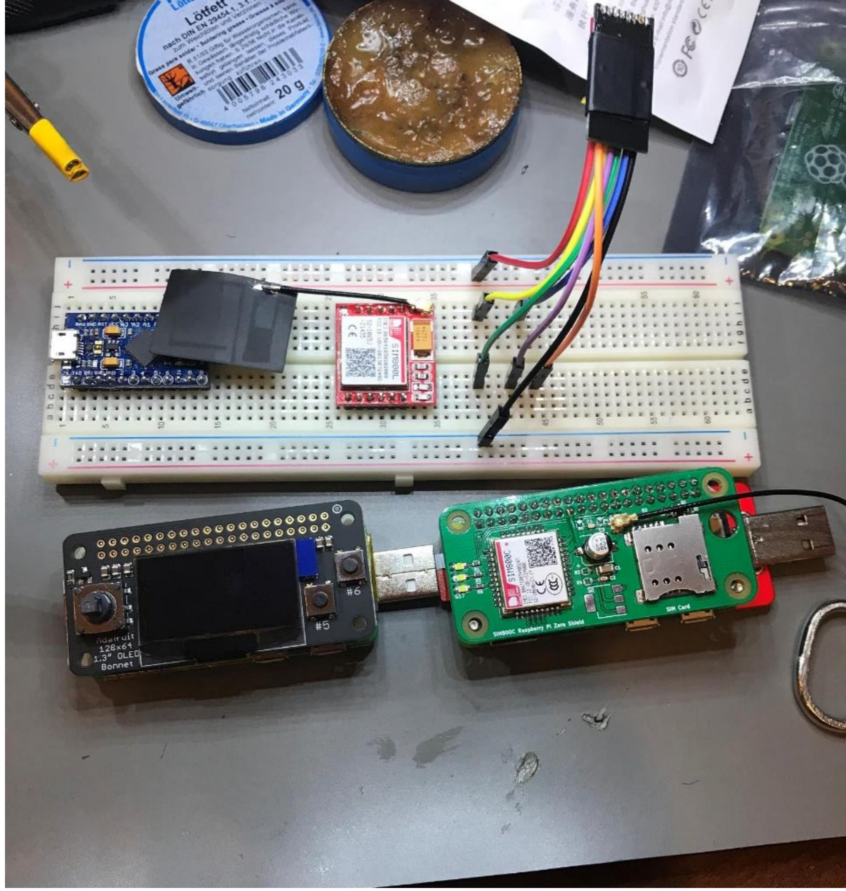
Jeff Hawkins, designed one of the first tablets in the market, the **GRiDPad**. It was an **engineering marvel but a market failure** because, it was still too big.

Determined to not make the mistake again, He decided to **change approach**.




PalmPilot prototype, Palm, Inc.
This "tethered prototype" let engineers
the PalmPilot before production units
Gift of Ron Marianetti





My Pretotypes

- **It must be cheap** (use what you have around)
- **It takes at least few days in order to get the feeling if worth pursuing the project**

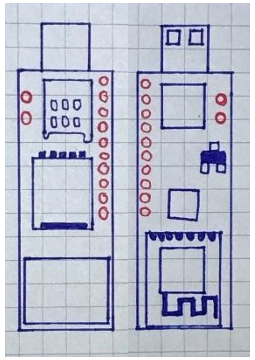
The Journey

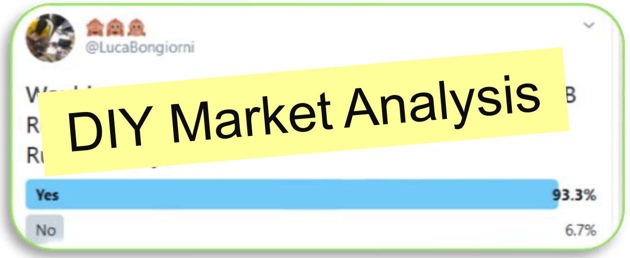
Quarters

Weeks

Days

Hours





@LucaBongiorni

DIY Market Analysis

Yes 93.3%

No 6.7%

Napkin Sketch

Pretotype

PoC/Prototype

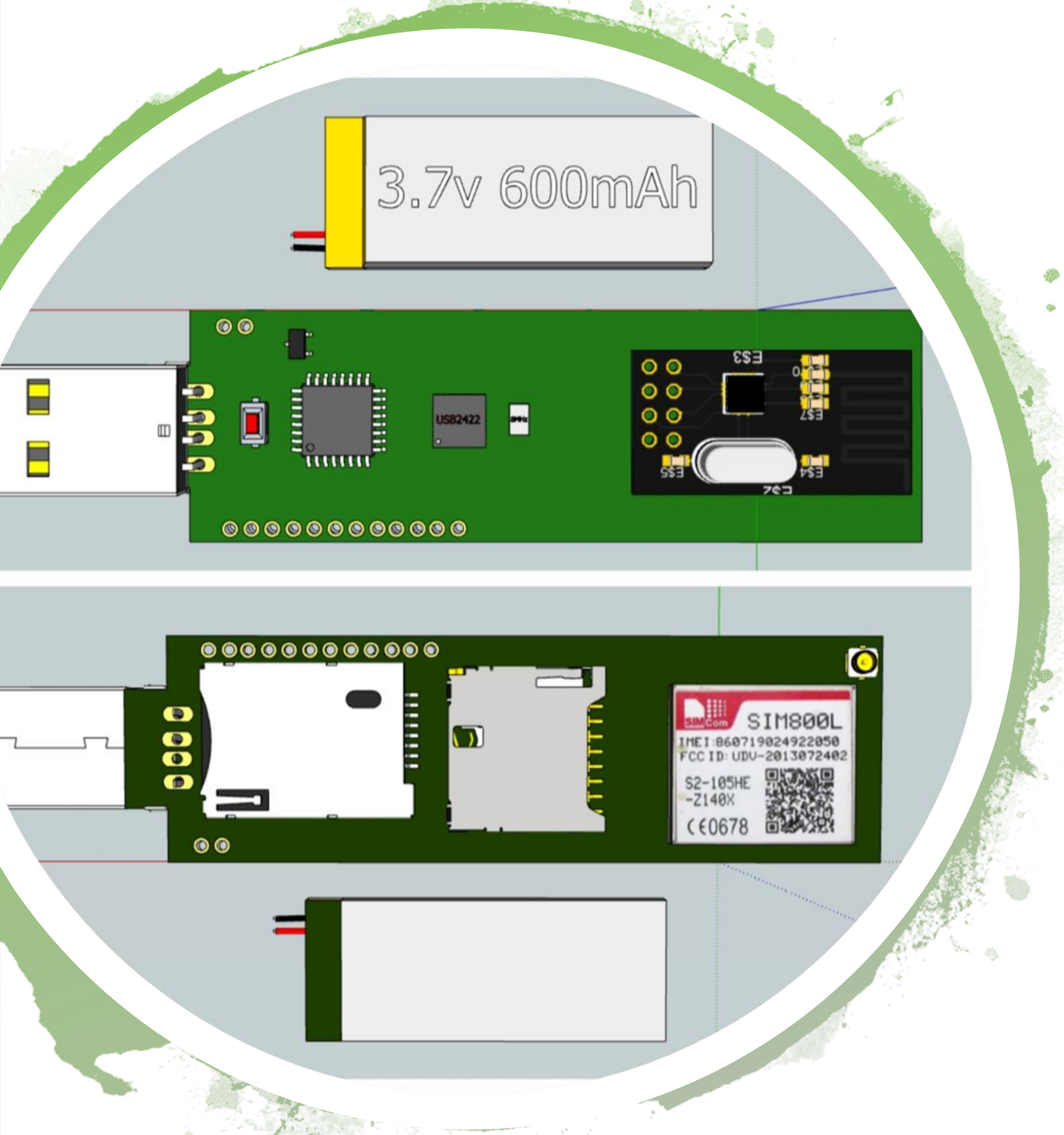
Final Product

$$$

$$

$

Free



3D Concept

- **Cheap** (Free CAD tools available)
- **Faster than designing the prototype with KiCAD**
- **Good enough to further validate the idea** and present to manufacturers/investors
- Time Needed:
  - **Couple of days** (included a basic training on SketchUp)

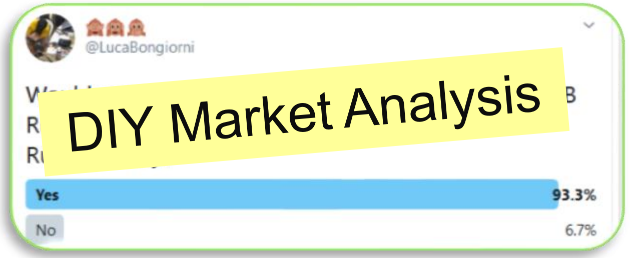
The Journey

Quarters

Weeks

Days

Hours

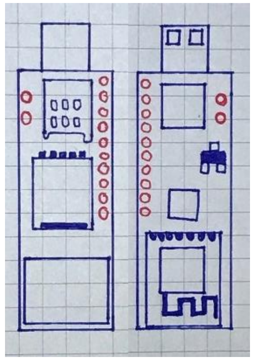


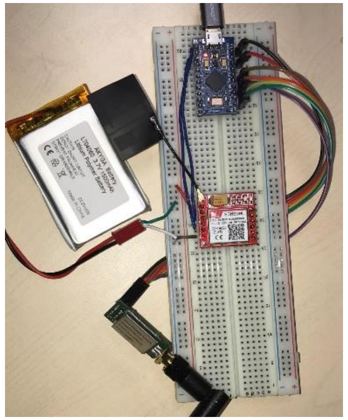
🙈🙉🙊
@LucaBongiorni

DIY Market Analysis

Yes 93.3%

No 6.7%





$$$

$$

$

Free

Napkin Sketch

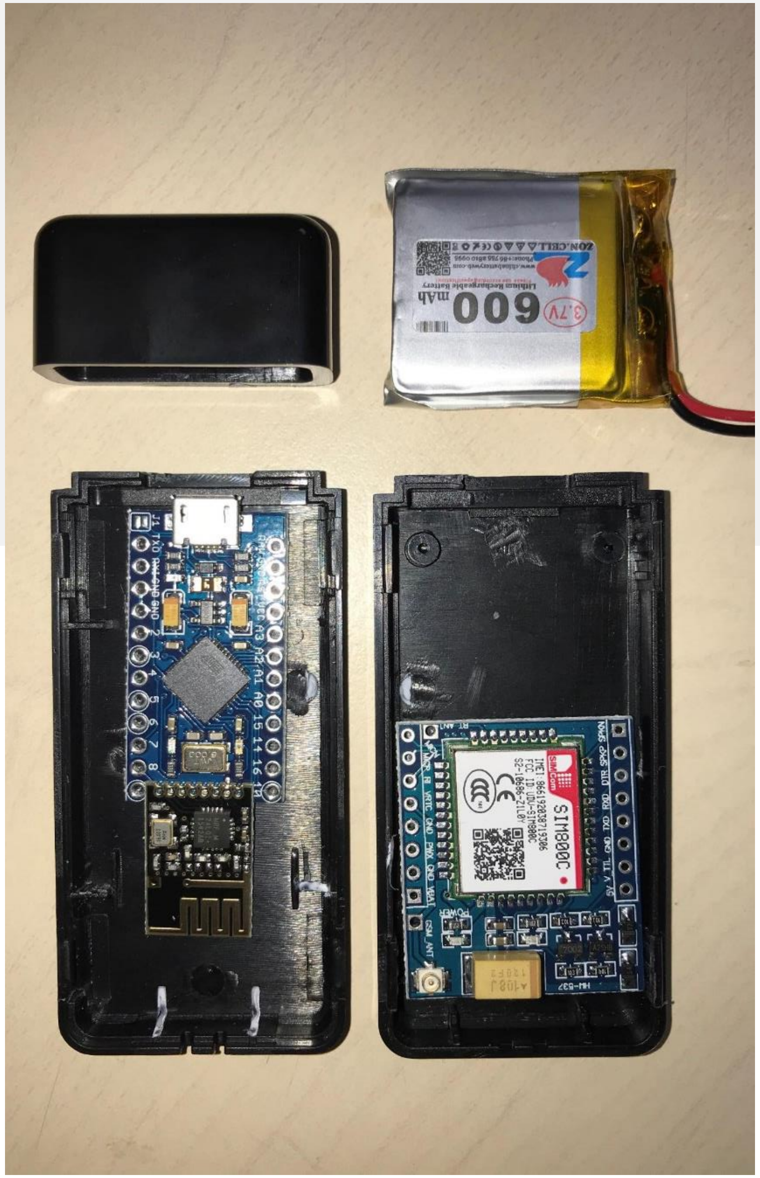
Pretotype

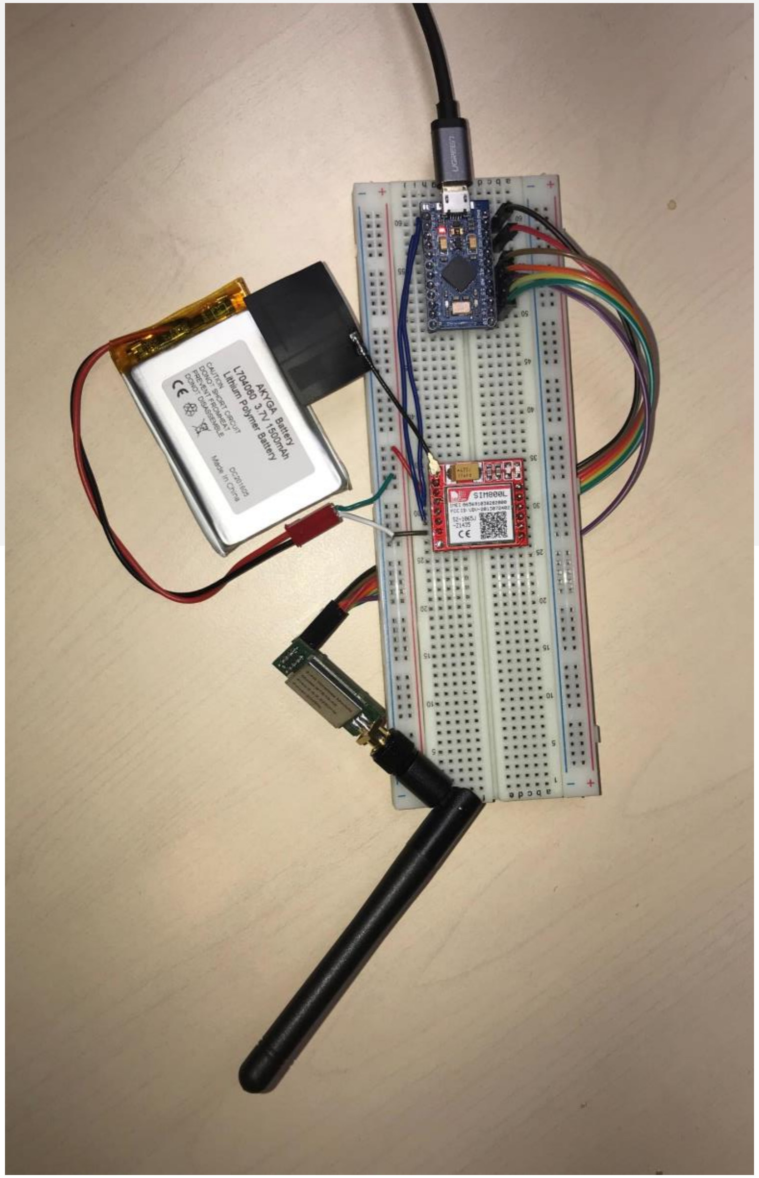
PoC/Prototype

Final Product

PoC/Prototype

- **Reasonable Costs** <100 EUR
- Time Needed:
  - **Aprox 15 days**
    - Reading Datasheets
    - Taking Measures
    - Coding/Testing main features





First Stable PoC: https://www.youtube.com/watch?v=tuoT-cPldMk

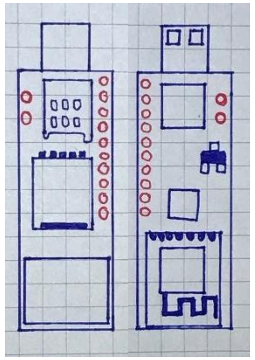
The Journey

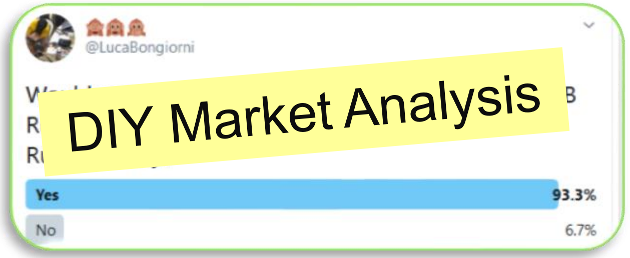
Quarters

Weeks

Days

Hours



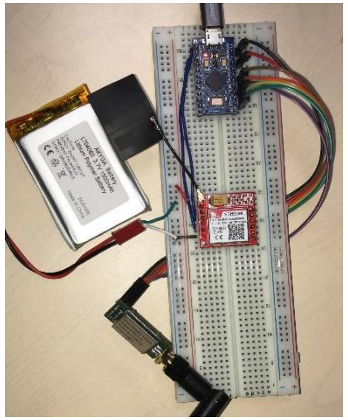


@LucaBongiorni

DIY Market Analysis

Yes 93.3%

No 6.7%



$$$

$$

$

Free

Napkin Sketch

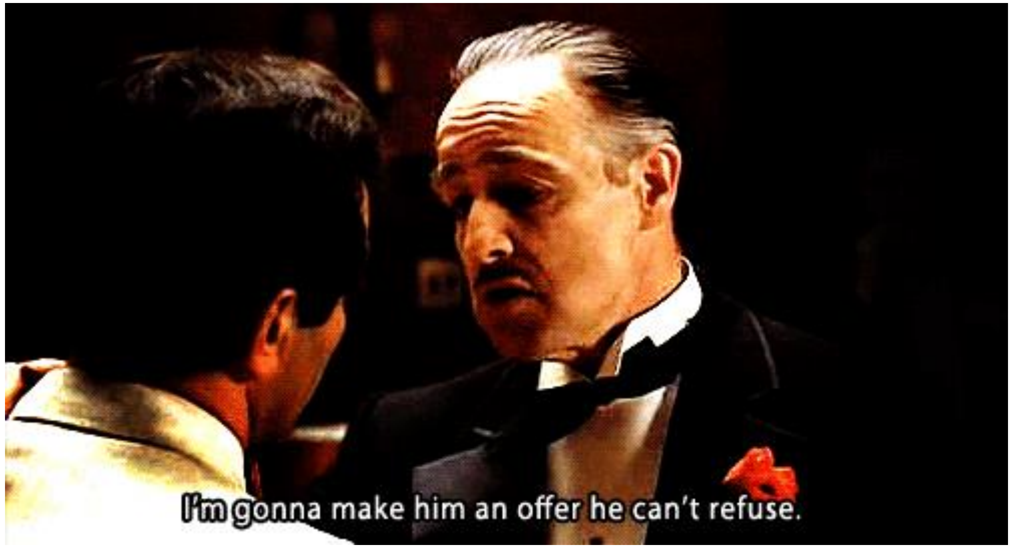
Pretotype

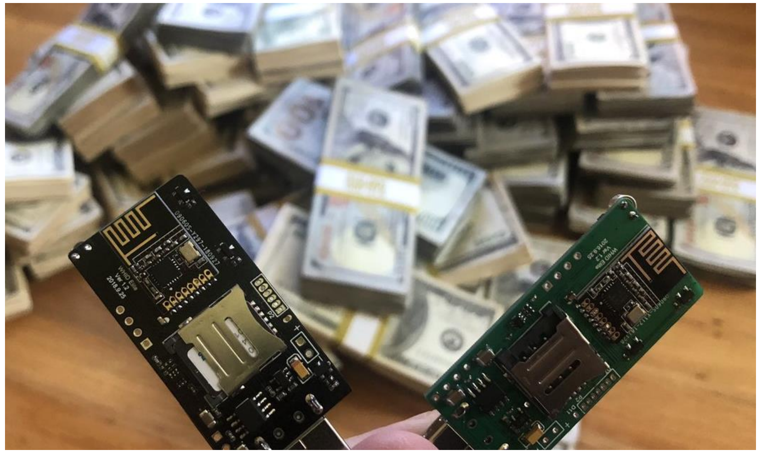
PoC/Prototype

Final Product

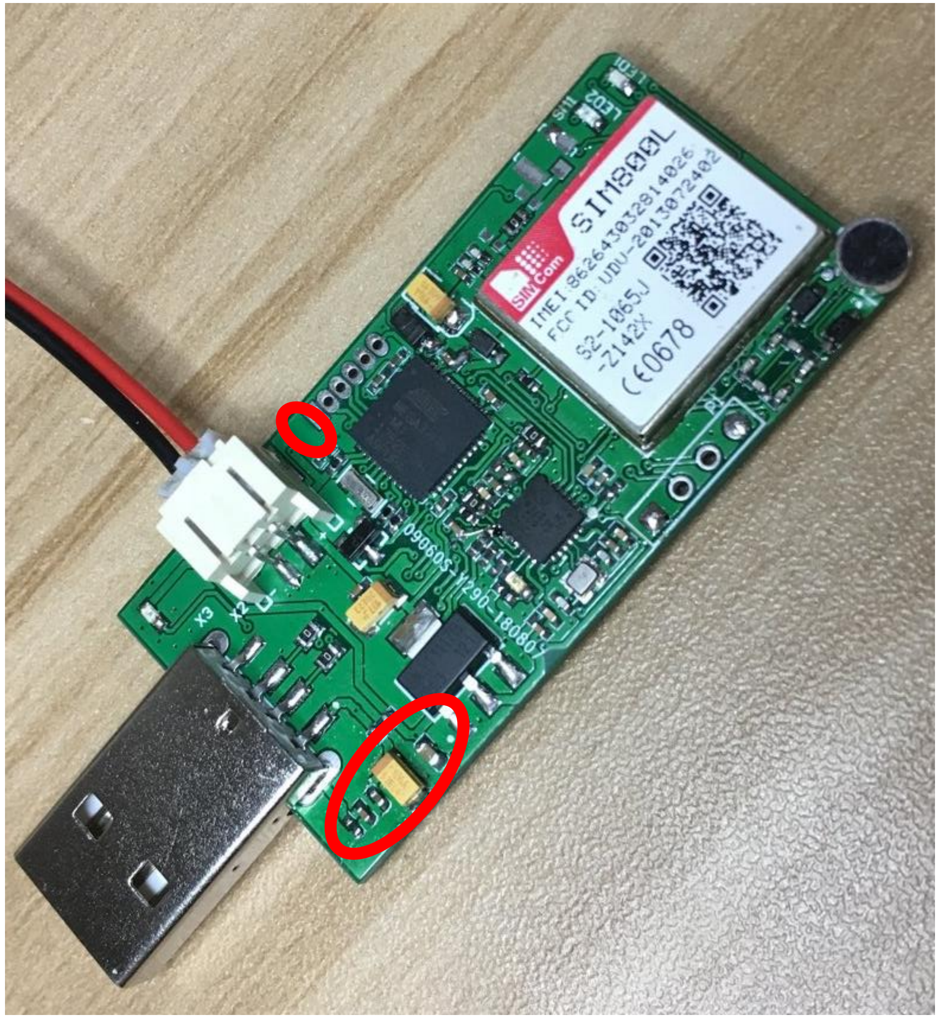
The Business Un-deal

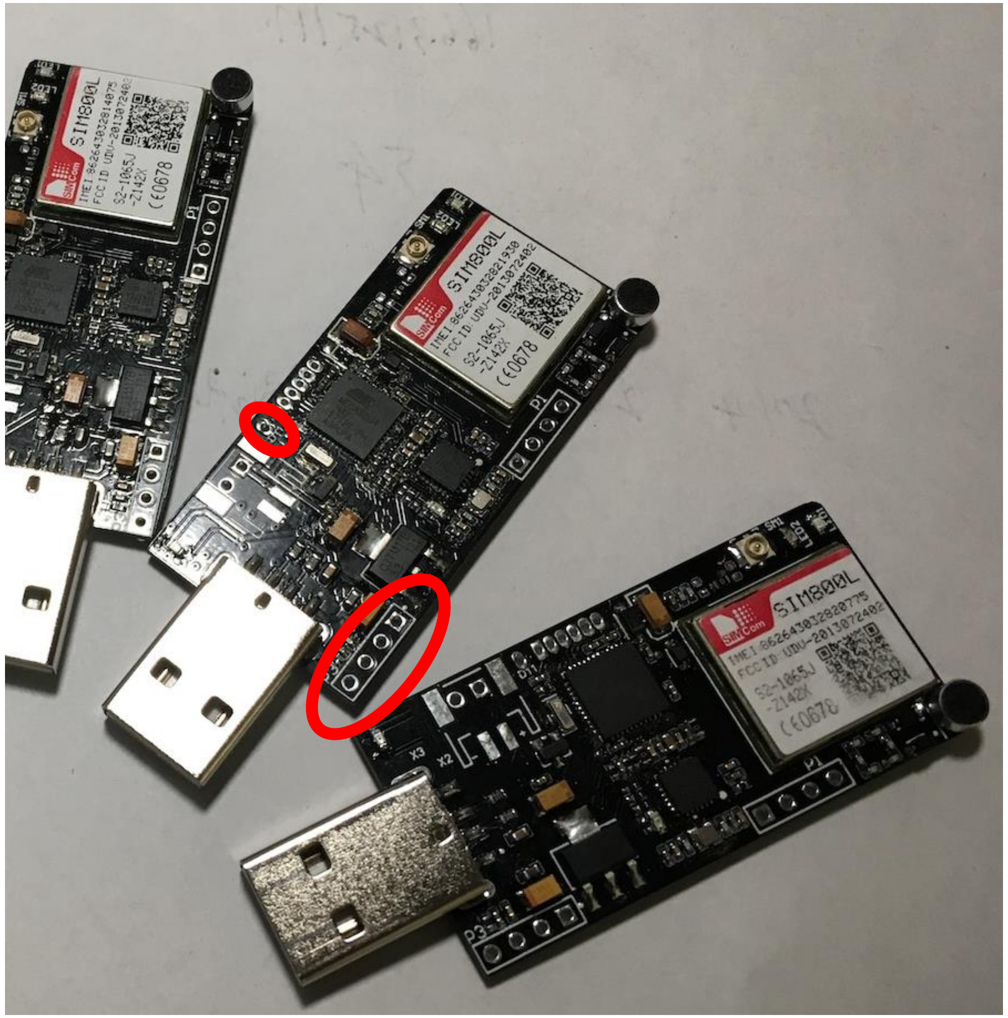
- **The Odyssey Starts**
  - Looking for Manufacturer
    - Alibaba, Twitter & Tindie are your friends
- **The Kickstart E-mail**
- **Unleash the Un-Deal**
  - I R&D it
  - I prototype it
  - I QA it
  - You make it
  - You sell it worldwide at an affordable price
  - You keep the profit
  - Everyone enjoys it!





From Alfa To Beta PCB

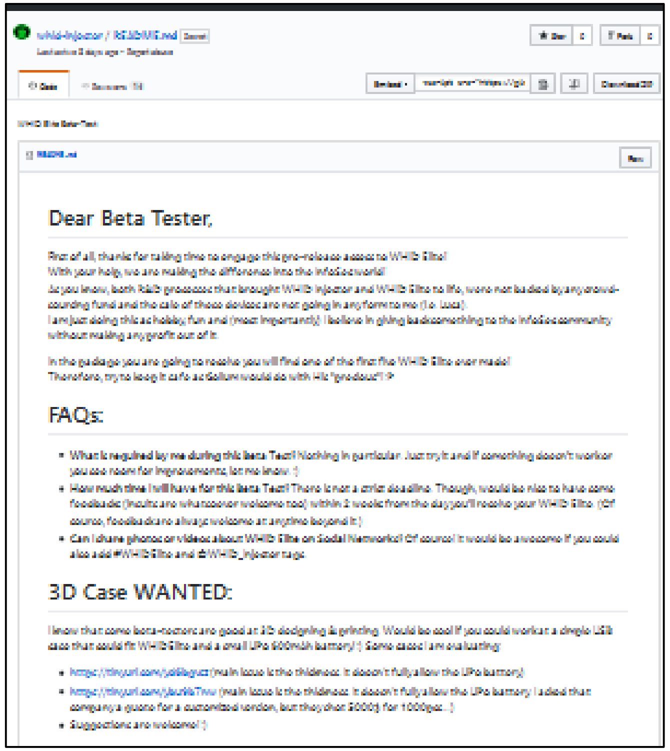




Time for Beta Test

BETA TESTING ★★★ BETA TESTING ★★★ BETA TESTING

- **Select Wisely Beta Testers**
- Do not have high expectations anyway (people are busy)
- Prepare easy-to-digest Documentation



Dear Beta Tester,

First of all, thanks for taking time to engage this pre-release access to WHID Elite!
With your help, we are making the difference into the InfoSec world!
As you know, both R&D processes that brought WHID Injector and WHID Elite to life, were not funded by any crowd-sourcing fund and the sale of these devices are not going in any form to me (i.e. Luca).
I am just doing this as hobby, fun and (most importantly) I believe in giving back something to the InfoSec community without making any profit out of it.

In the package you are going to receive you will find one of the first five WHID Elite ever made!
Therefore, try to keep it safe as Gollum would do with His "precious"! :P

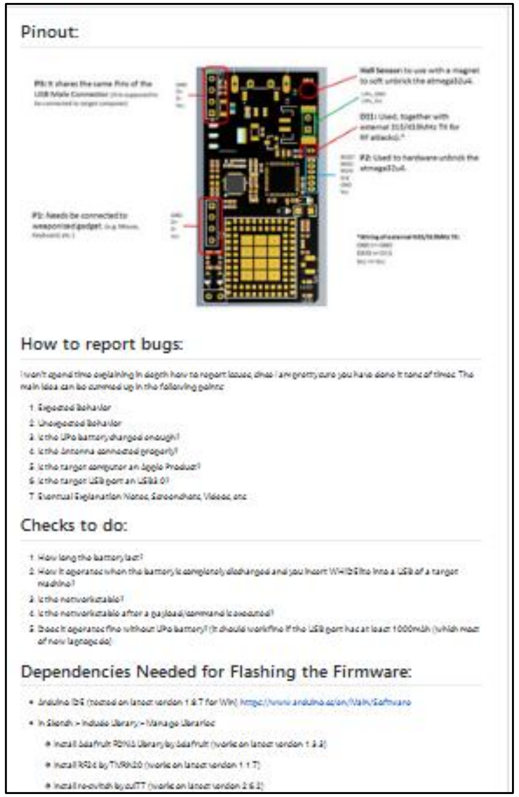
FAQs:

- What is required by me during this Beta Test? Nothing in particular. Just try it and if something doesn't work or you see room for improvements, let me know :)
- How much time I will have for this Beta Test? There is not a strict deadline. Though, would be nice to have some feedback (insults are whatsoever welcome too) within 2 weeks from the day you'll receive your WHID Elite. (Of course, feedbacks are always welcome at anytime beyond it.)
- Can I share photos or videos about WHID Elite on Social Networks? Of course! It would be awesome if you could also add #WHIDElite and #WHID_Injector tags.

3D Case WANTED:

I know that some beta-testers are good at 3D designing & printing. Would be cool if you could work at a simple USB case that could fit WHIDElite and a small LiPo 600mAh battery! :) Some cases I am evaluating:

- https://tinyurl.com/y68kgucz (main issue is the thickness. It doesn't fully allow the LiPo battery)
- https://tinyurl.com/yaurhkTww (main issue is the thickness. It doesn't fully allow the LiPo battery. I asked that company a quote for a customized version, but they shot 5000$ for 1000pcs...)
- Suggestions are welcome! :)



Pinout:

P5: It shares the same Pins of the USB Male Connector (it is supposed to be connected to target computer)
GND
D+
D-
Vcc
Hall Sensor: to use with a magnet to soft unbrick the atmega32u4.
D11: Used, together with external 315/433MHz TX for RF attacks(...).*
P2: Used to hardware unbrick the atmega32u4.
P1: Needs be connected to weaponized gadget (e.g. Mouse, Keyboard, etc.)
GND
D+
D-
Vcc
*Wiring of external 315/433MHz TX:
GND <-> GND
DATA <-> D11
Vcc <-> Vcc

How to report bugs:

I won't spend time explaining in depth how to report issues, since I am pretty sure you have done it tons of times. The main idea can be summed up in the following points:

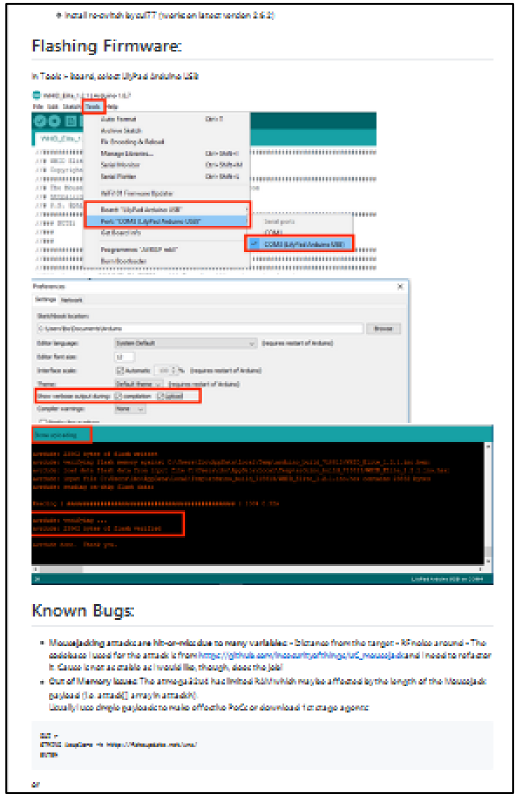
1. Expected Behavior
2. Unexpected Behavior
3. Is the LiPo battery charged enough?
4. Is the Antenna connected properly?
5. Is the target computer an Apple Product?
6. Is the target USB port an USB3.0?
7. Eventual Explanation Notes, Screenshots, Videos, etc.

Checks to do:

1. How long the battery last?
2. How it operates when the battery is completely discharged and you insert WHIDElite into a USB of a target machine?
3. Is the network stable?
4. Is the network stable after a payload/command is executed?
5. Does it operates fine without LiPo battery? (It should work fine if the USB port has at least 1000mAh (which most of new laptops do))

Dependencies Needed for Flashing the Firmware:

- Arduino IDE (tested on latest version 1.8.7 for Win) https://www.arduino.cc/en/Main/Software
- In Sketch -> Include Library -> Manage Libraries:
  - Install Adafruit PCNA Library by Adafruit (works on latest version 1.3.2)
  - Install RF24 by TMRh20 (works on latest version 1.1.7)
  - Install rc-switch by sui77 (works on latest version 2.6.2)



- Install rc-switch by sui77 (works on latest version 2.6.2)

Flashing Firmware:

In Tools -> Board, select LilyPad Arduino USB

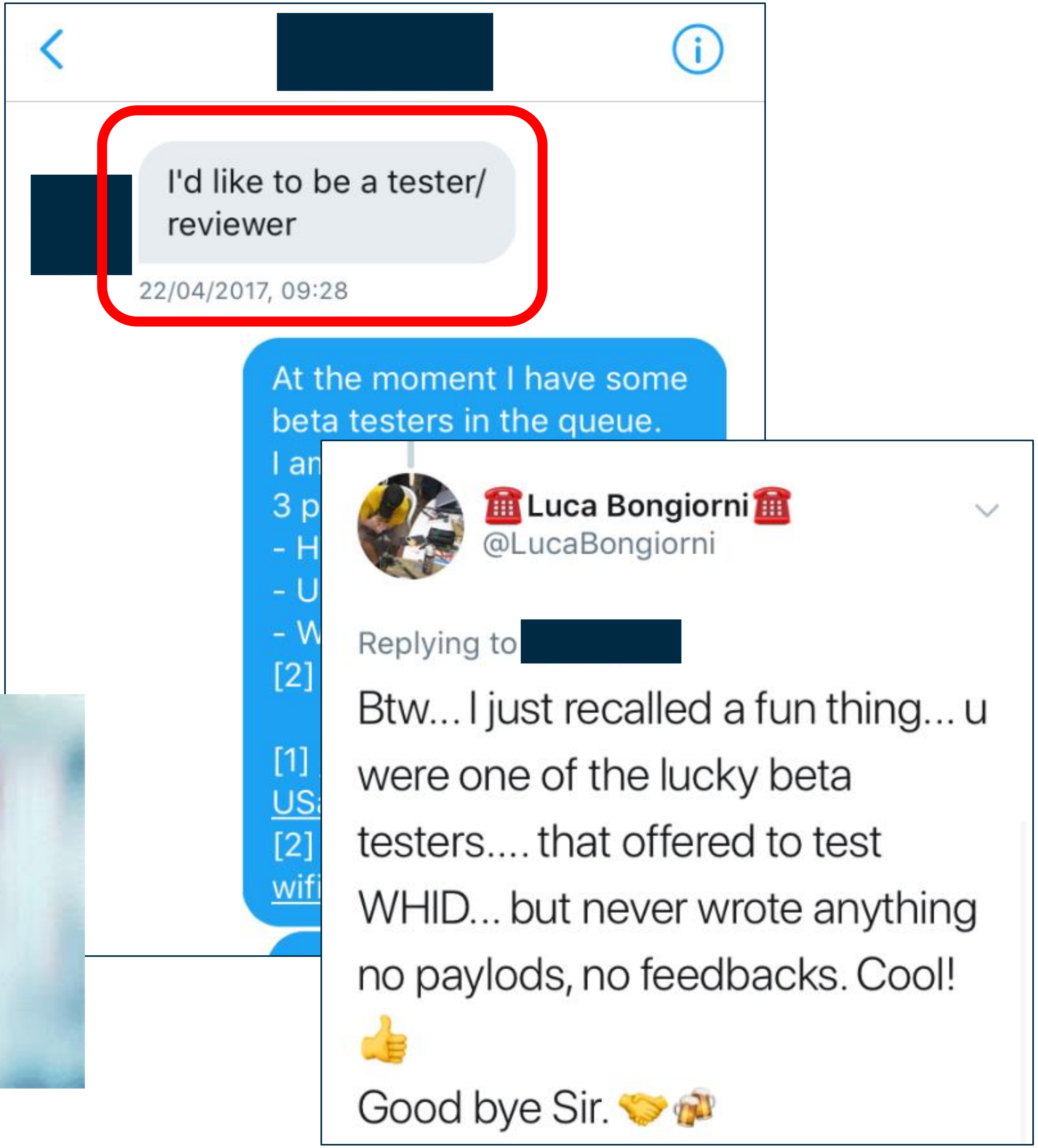
File Edit Sketch Tools Help
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Manage Libraries... Ctrl+Shift+I
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
WiFi101 Firmware Updater
Board: "LilyPad Arduino USB"
Port: "COM3 (LilyPad Arduino USB)"
Get Board Info
Programmer: "AVRISP mkII"
Burn Bootloader
Serial ports
COM1
COM3 (LilyPad Arduino USB)
Preferences
Settings Network
Sketchbook location:
Browse
Editor language: System Default (requires restart of Arduino)
Editor font size: 12
Interface scale: ☑ Automatic 100 % (requires restart of Arduino)
Theme: Default theme (requires restart of Arduino)
Show verbose output during: ☐ compilation ☑ upload
Compiler warnings: None
Done uploading.
avrdude done. Thank you.
LilyPad Arduino USB on COM4

Known Bugs:

- MouseJacking attacks are hit-or-miss due to many variables: - Distance from the target - RF noise around - The codebase I used for the attack is from https://github.com/insecurityofthings/uC_mousejack and I need to refactor it. Cause is not as stable as I would like, though, does the job!
- Out of Memory issues: The atmega32u4 has limited RAM which may be affected by the length of the MouseJack payload (i.e. attack[] array in attack.h).
  Usually I use simple payloads to make effective PoCs or download 1st stage agents:

```
GUI r
STRING [illegible] -> http://[illegible]
ENTER
```

- Most of them will say/promise everything just to get a free cool device!
- Then they’ll disappear like “tears in the rain”…



[redacted]

[redacted]

I'd like to be a tester/ reviewer

22/04/2017, 09:28

At the moment I have some beta testers in the queue.
I an
3 p
- H
- U
- W
[2]

[1]
US
[2]
wifi

☎Luca Bongiorni☎
@LucaBongiorni

Replying to [redacted]

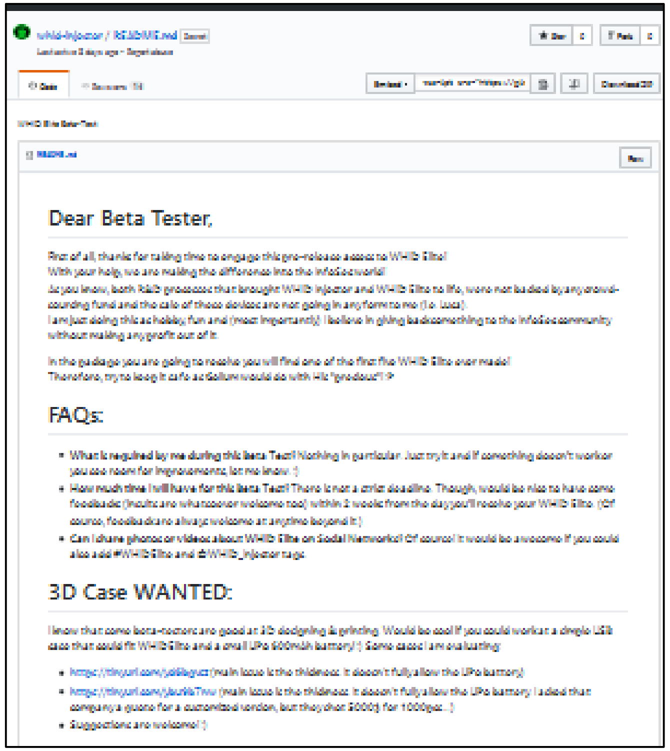
Btw... I just recalled a fun thing... u were one of the lucky beta testers.... that offered to test WHID... but never wrote anything no paylods, no feedbacks. Cool! 👍

Good bye Sir. 🤝🍻

Time for Beta Test

BETA TESTING
BETA TESTING
BETA TESTING

- Select Wisely Beta Testers
- **Do not have high expectations anyway (people are busy)**
- **Prepare easy-to-digest Documentation**



Last active 3 days ago · Report abuse

WHID Elite Beta-Test

Dear Beta Tester,

First of all, thanks for taking time to engage this pre-release access to WHID Elite!
With your help, we are making the difference into the InfoSec world!
As you know, both R&D processes that brought WHID Injector and WHID Elite to life, were not backed by any crowd-sourcing fund and the sale of these devices are not going in any form to me (i.e. Luca).
I am just doing this as hobby, fun and (most importantly) I believe in giving back something to the InfoSec community without making any profit out of it.

In the package you are going to receive you will find one of the first five WHID Elite ever made!
Therefore, try to keep it safe as Gollum would do with His "precious"!! :P

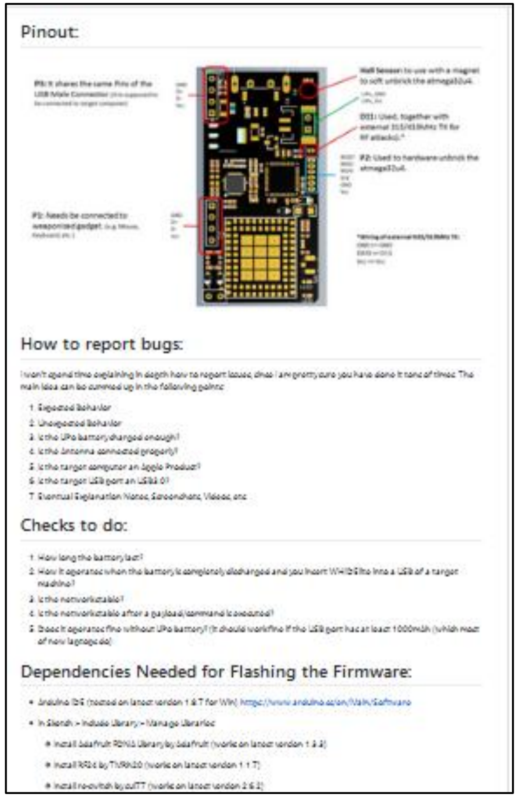
FAQs:

- What is required by me during this Beta Test? Nothing in particular. Just try it and if something doesn't work or you see room for improvements, let me know :)
- How much time I will have for this Beta Test? There is not a strict deadline. Though, would be nice to have some feedbacks (insults are whatsoever welcome too) within 2 weeks from the day you'll receive your WHID Elite. (Of course, feedbacks are always welcome at anytime beyond it.)
- Can I share photos or videos about WHID Elite on Social Networks? Of course! It would be awesome if you could also add #WHIDElite and #WHID_Injector tags.

3D Case WANTED:

I know that some beta-testers are good at 3D designing & printing. Would be cool if you could work at a single USB case that could fit WHIDElite and a small LiPo 600mAh battery! :) Some cases I am evaluating:

- https://tinyurl.com/[illegible] (main issue is the thickness. It doesn't fully allow the LiPo battery)
- https://tinyurl.com/[illegible] (main issue is the thickness. It doesn't fully allow the LiPo battery. I asked that company a quote for a customized version, but they shot 5000$ for 1000pcs...)
- Suggestions are welcome! :)



Pinout:

P3: It shares the same Pins of the USB Male Connector (it is supposed to be connected to target computer)
Hall Sensor: to use with a magnet to soft unbrick the atmega32u4.
D31: Used, together with external 315/433MHz TX for RF attack(s).*
P2: Used to hardware unbrick the atmega32u4.
P1: Needs be connected to weaponized gadget (e.g. Mouse, Keyboard, etc.)
*Wiring of external 315/433MHz TX:
GND <-> GND
DATA <-> D31
Vcc <-> Vcc

How to report bugs:

I won't spend time explaining in depth how to report issues, since I am pretty sure you have done it tons of times. The main idea can be summed up in the following points:

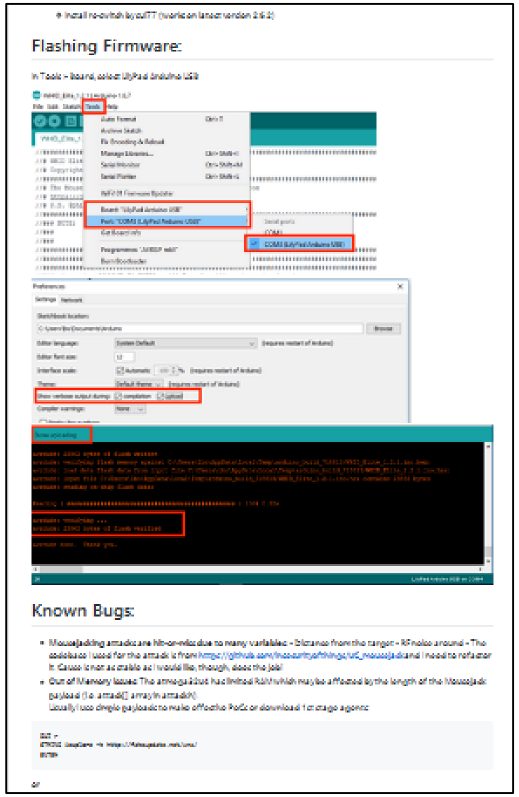
1. Expected Behavior
2. Unexpected Behavior
3. Is the LiPo battery charged enough?
4. Is the Antenna connected properly?
5. Is the target computer an Apple Product?
6. Is the target USB port an USB3.0?
7. Eventual Explanation Notes, Screenshots, Videos, etc.

Checks to do:

1. How long the battery last?
2. How it operates when the battery is completely discharged and you insert WHIDElite into a USB of a target machine?
3. Is the network stable?
4. Is the network stable after a payload/command is executed?
5. Does it operates fine without LiPo battery? (It should work fine if the USB port has at least 1000mAh (which most of new laptops do))

Dependencies Needed for Flashing the Firmware:

- Arduino IDE (tested on latest version 1.8.7 for Win) https://www.arduino.cc/en/Main/Software
- In Sketch > Include Library > Manage Libraries:
  - Install Adafruit FONA Library by Adafruit (works on latest version 1.3.2)
  - Install RF24 by TMRh20 (works on latest version 1.1.7)
  - Install rc-switch by sui77 (works on latest version 2.6.2)



- Install rc-switch by sui77 (works on latest version 2.6.2)

Flashing Firmware:

In Tools > Board, select LilyPad Arduino USB

Board: "LilyPad Arduino USB"
Port: "COM3 (LilyPad Arduino USB)"
Programmer: "AVRISP mkII"
☑ COM3 (LilyPad Arduino USB)

Sketchbook location: C:\Users\[illegible]\Documents\Arduino
Editor language: System Default (requires restart of Arduino)
Editor font size: 12
Interface scale: ☑ Automatic 100 % (requires restart of Arduino)
Theme: Default theme (requires restart of Arduino)
Show verbose output during: ☑ compilation ☑ upload
Compiler warnings: None

Done uploading.

```
avrdude: [illegible] bytes of flash written
avrdude: verifying flash memory against [illegible]
avrdude: load data flash data from input file [illegible]
avrdude: input file [illegible] contains [illegible] bytes
avrdude: reading on-chip flash data:

Reading | ################################################## | 100% [illegible]

avrdude: verifying ...
avrdude: 23942 bytes of flash verified

avrdude done.  Thank you.
```

LilyPad Arduino USB on COM4

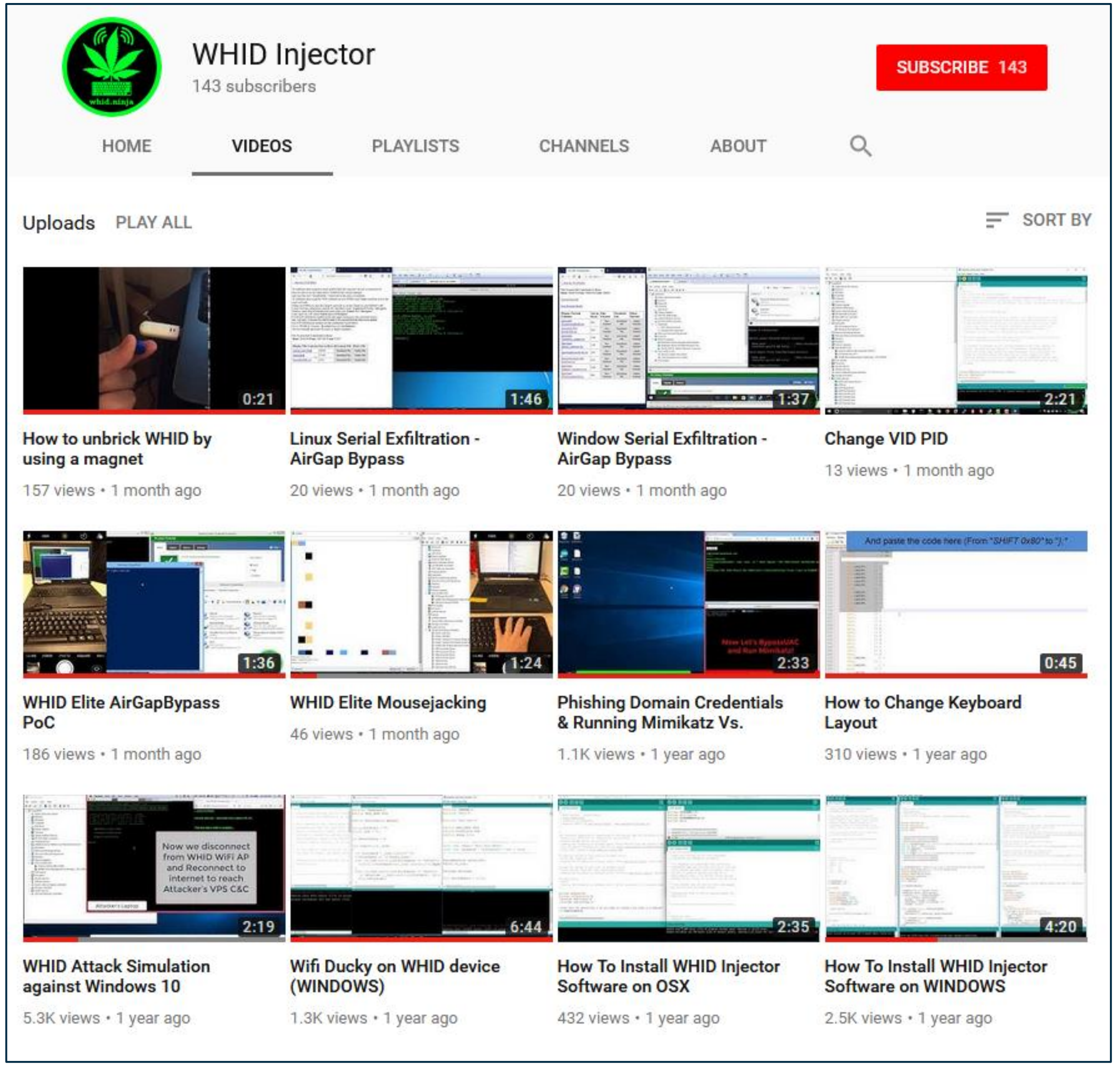
Known Bugs:

- MouseJacking attacks are hit-or-miss due to many variables: - Distance from the target - RF noise around - The codebase I used for the attack is from https://github.com/insecurityofthings/uC_mousejack and I need to refactor it. Cause is not as stable as I would like, though, does the job!
- Out of Memory issues: The atmega32u4 has limited RAM which may be affected by the length of the MouseJack payload (i.e. attack[] array in attack.h).
  Usually I use simple payloads to make effective PoCs or download 1st stage agents:

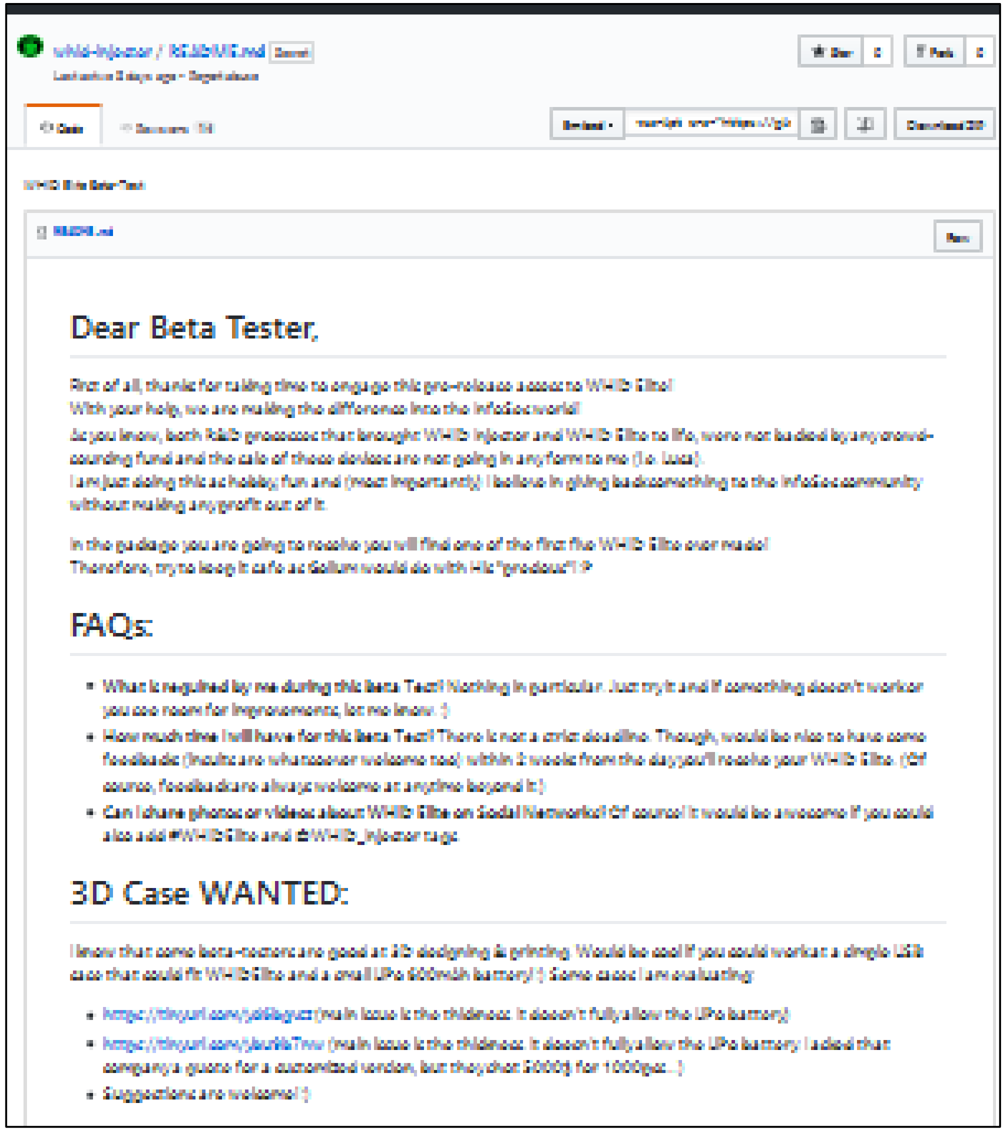
```
GUI r
STRING [illegible] -> https://[illegible]
ENTER
```

;P

The art of writing instructions for the dumbest person on Earth!



- 0:21 How to unbrick WHID by using a magnet — 157 views • 1 month ago
- 1:46 Linux Serial Exfiltration - AirGap Bypass — 20 views • 1 month ago
- 1:37 Window Serial Exfiltration - AirGap Bypass — 20 views • 1 month ago
- 2:21 Change VID PID — 13 views • 1 month ago
- 1:36 WHID Elite AirGapBypass PoC — 186 views • 1 month ago
- 1:24 WHID Elite Mousejacking — 46 views • 1 month ago
- 2:33 Phishing Domain Credentials & Running Mimikatz Vs. — 1.1K views • 1 year ago
- 0:45 How to Change Keyboard Layout — 310 views • 1 year ago
- 2:19 WHID Attack Simulation against Windows 10 — 5.3K views • 1 year ago
- 6:44 Wifi Ducky on WHID device (WINDOWS) — 1.3K views • 1 year ago
- 2:35 How To Install WHID Injector Software on OSX — 432 views • 1 year ago
- 4:20 How To Install WHID Injector Software on WINDOWS — 2.5K views • 1 year ago



WHID Elite Beta-Test

Dear Beta Tester,

First of all, thanks for taking time to engage this pre-release access to WHID Elite!
With your help, we are making the difference into the InfoSec world!
As you know, both R&D processes that brought WHID Injector and WHID Elite to life, were not backed by any crowd-founding fund and the sale of these devices are not going in any form to me (i.e. Luca).
I am just doing this as hobby, fun and (most importantly) I believe in giving back something to the InfoSec community without making any profit out of it.

In the package you are going to receive you will find one of the first five WHID Elite ever made!
Therefore, try to keep it safe as Gollum would do with His "precious"! :P

FAQs:

- What is required by me during this Beta Test? Nothing in particular. Just try it and if something doesn't work or you see room for improvements, let me know. :)
- How much time I will have for this Beta Test? There is not a strict deadline. Though, would be nice to have some feedbacks (insults are whatsoever welcome too) within 2 weeks from the day you'll receive your WHID Elite. (Of course, feedbacks are always welcome at anytime beyond it :)
- Can I share photos or videos about WHID Elite on Social Networks? Of course! It would be awesome if you could also add #WHIDElite and #WHID_Injector tags.

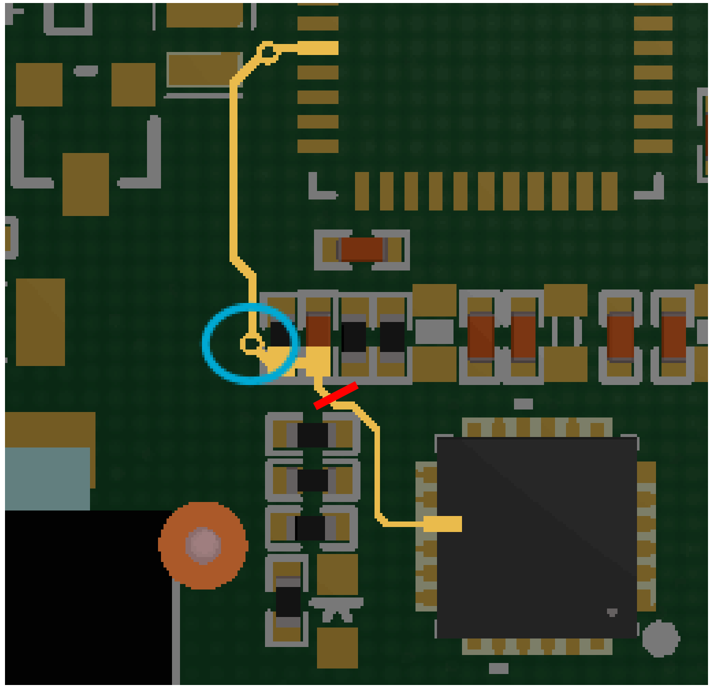
3D Case WANTED:

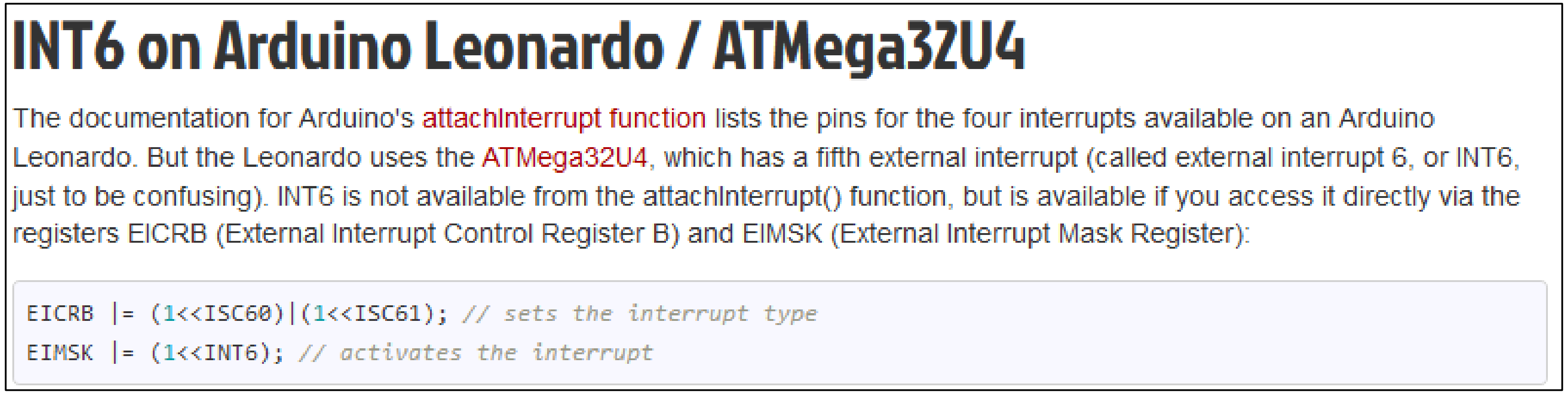
I know that some beta-testers are good at 3D designing & printing. Would be cool if you could work at a single USB case that could fit WHID Elite and a small LiPo 600mAh battery! :) Some cases I am evaluating:

- https://tinyurl.com/[illegible] (main issue is the thickness. It doesn't fully allow the LiPo battery)
- https://tinyurl.com/[illegible] (main issue is the thickness. It doesn't fully allow the LiPo battery. I asked that company a quote for a customized version, but they shot 5000$ for 1000pcs...)
- Suggestions are welcome! :)

Zen-Time: More Features ➡ More Bugs

- I needed an INT Pin for RXing ASK-OOK signals
- Used D7/INT6 because was close and free!
- Got new PCB Rev… and…
- It is the most painful INT of Atmega32u4…

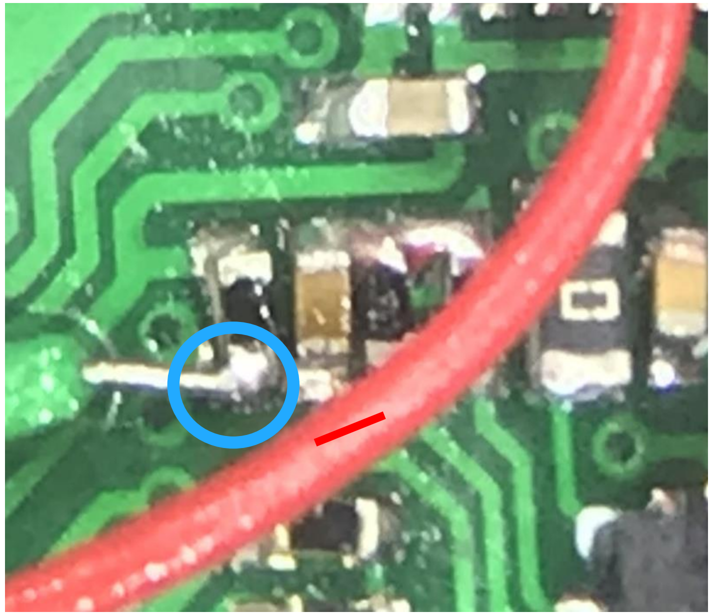




INT6 on Arduino Leonardo / ATMega32U4

The documentation for Arduino's attachInterrupt function lists the pins for the four interrupts available on an Arduino Leonardo. But the Leonardo uses the ATMega32U4, which has a fifth external interrupt (called external interrupt 6, or INT6, just to be confusing). INT6 is not available from the attachInterrupt() function, but is available if you access it directly via the registers EICRB (External Interrupt Control Register B) and EIMSK (External Interrupt Mask Register):

```
EICRB |= (1<<ISC60)|(1<<ISC61); // sets the interrupt type
EIMSK |= (1<<INT6); // activates the interrupt
```



- Re-Engineered the Board to use D3 instead

Release the Kraken!

Quarters

Weeks

Days

Hours

$$$

$$

$

Free

Napkin Sketch

Pretotype

PoC/Prototype

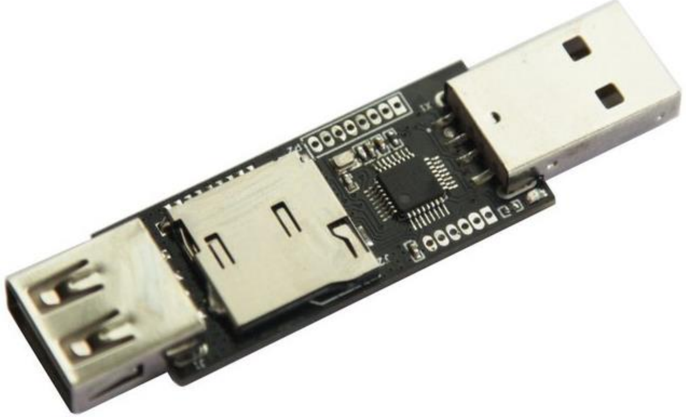
Final Product

~ 10.300 PCS

Number of units sold by the manufacturer until now

But do not tell my wife

~ 1150 PCS



EvilCrow Keylogger

RFID-Tool

EvilCrow Cable

Similar Success Stories

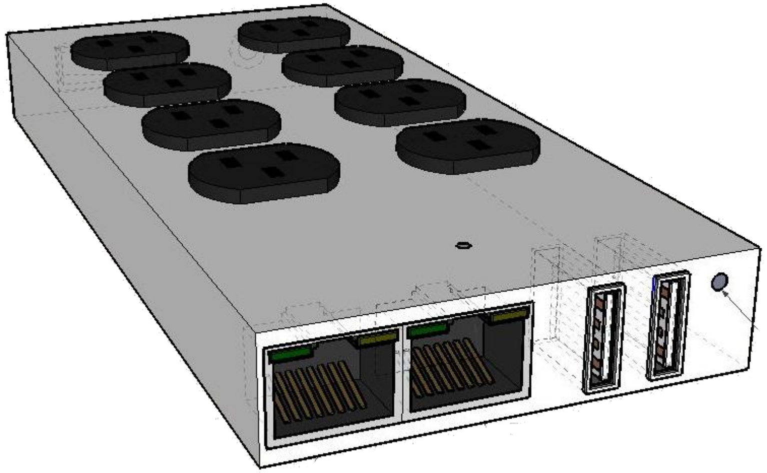
Lessons Learned

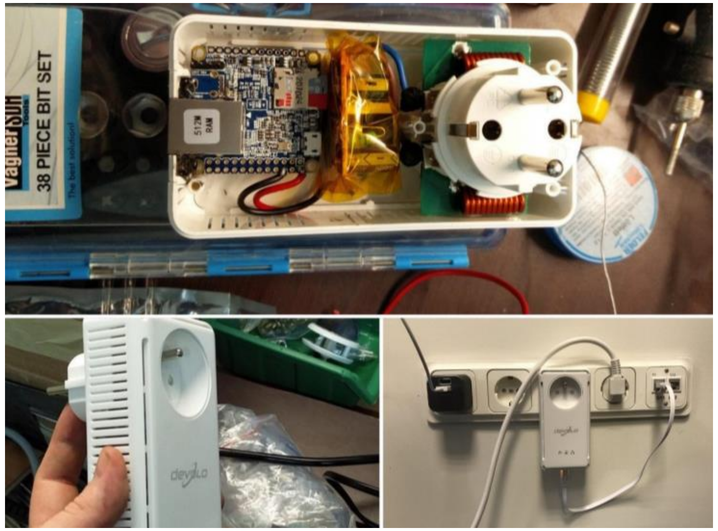
- Validating the idea is a prerogative (DIY Market Analysis & Pretotyping FTW)
- Don’t give up at the first manufacturer refusal!
- Documentation is vital
- Pick wisely beta testers
- Listen your users
  - Got plenty of improvements derived from this!
- Prioritize action items (divide-et-impera FTW)
- Finally… beware of some human beings. Copycats and IP thieves are always behind the corner… NDAs & OPSEC are your friends.

POTÆbox – Penetration Over The {Air, Ethernet} box

POTAEbox Purposes:

- Covert Security Operations (i.e. Pentests/RedTeam)
- Covert Surveillance
- Network Appliance (i.e. Firewall, IDS, Honeypot)
- Home Automation (i.e. Lights, Sensors)
- DIY Electronic Projects





Keep an eye at:

@potaebox

Fin

Special Thanks To:

_MG_, alphaomikron, dcuthbert, elkentaro, exploit_agency, jermainlaforce, JoelSernaMoreno, Mame82, MrGloglas, notameadow, PaulWebSec, PearCrew, Re4sonKernel, RoganDawes, saviolokiu, squiggly, SymbianSyMoh, TravisPooley and the rest of the folks out there that believed and keep believing in my crazy ideas.