



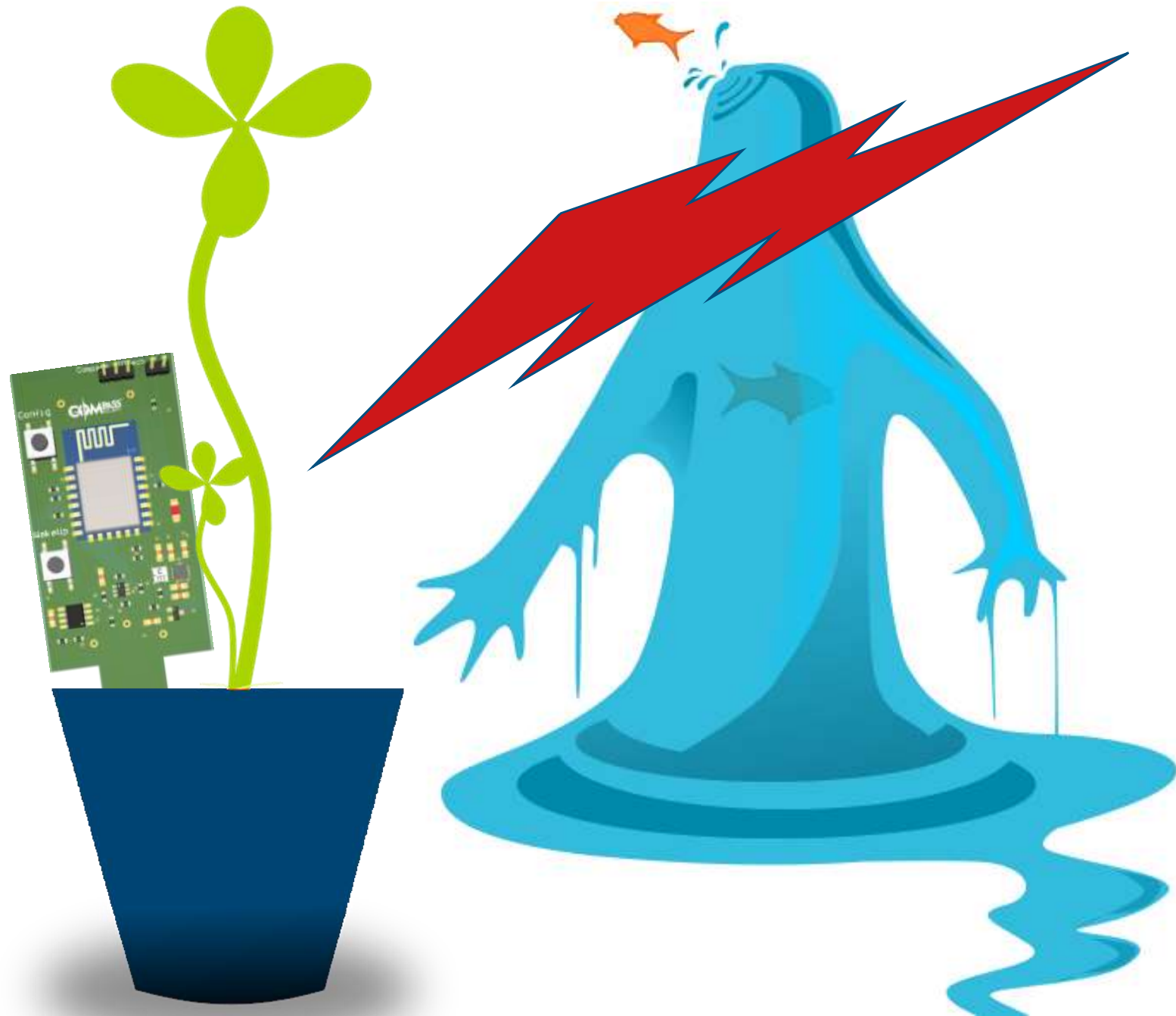
Hacking blOTech

Get your hands on IoT

October 18th 2017, Swiss Cyber Storm, Lucern KKL, cyrill.brunschwiler@compass-security.com

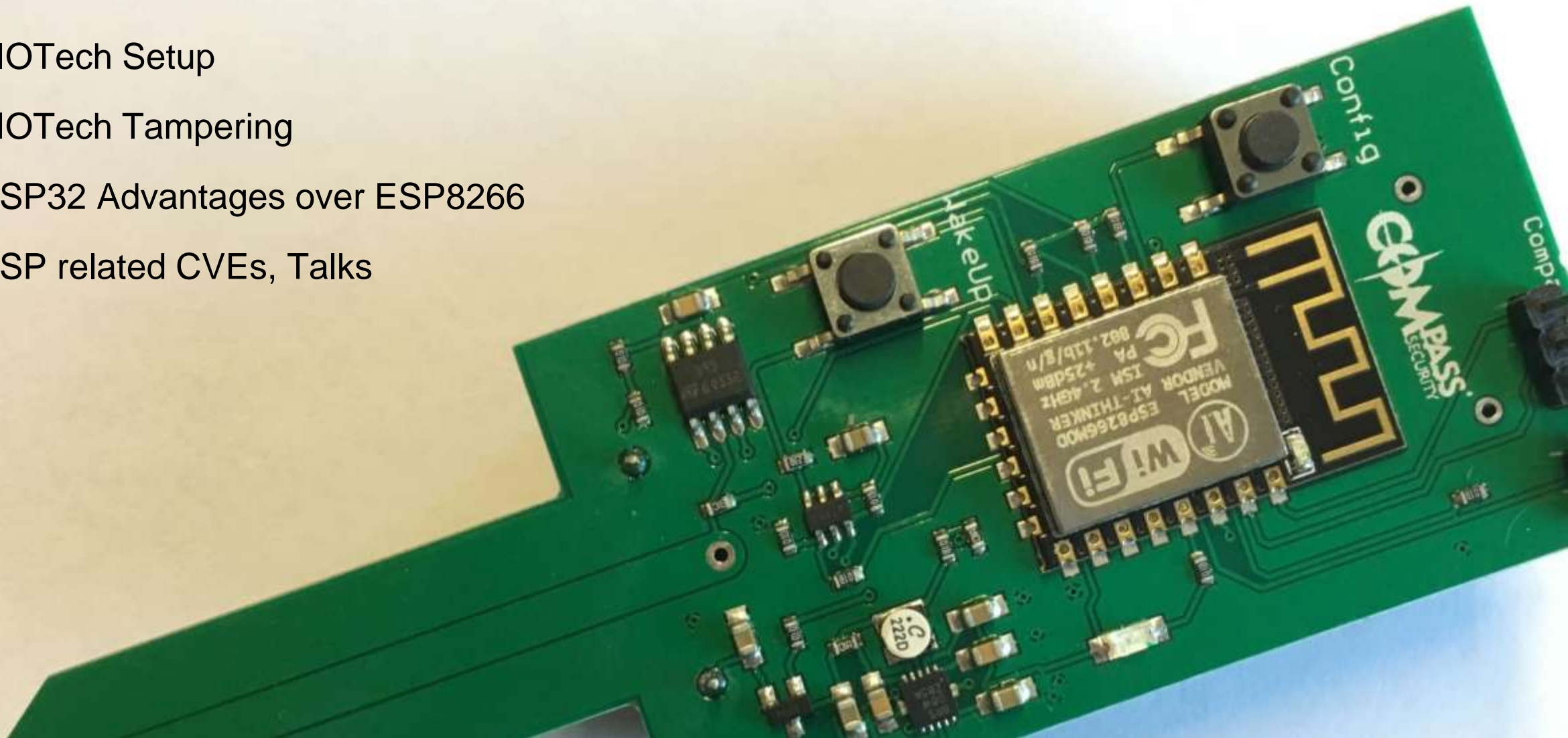
bioTech Intro

> biotech --help



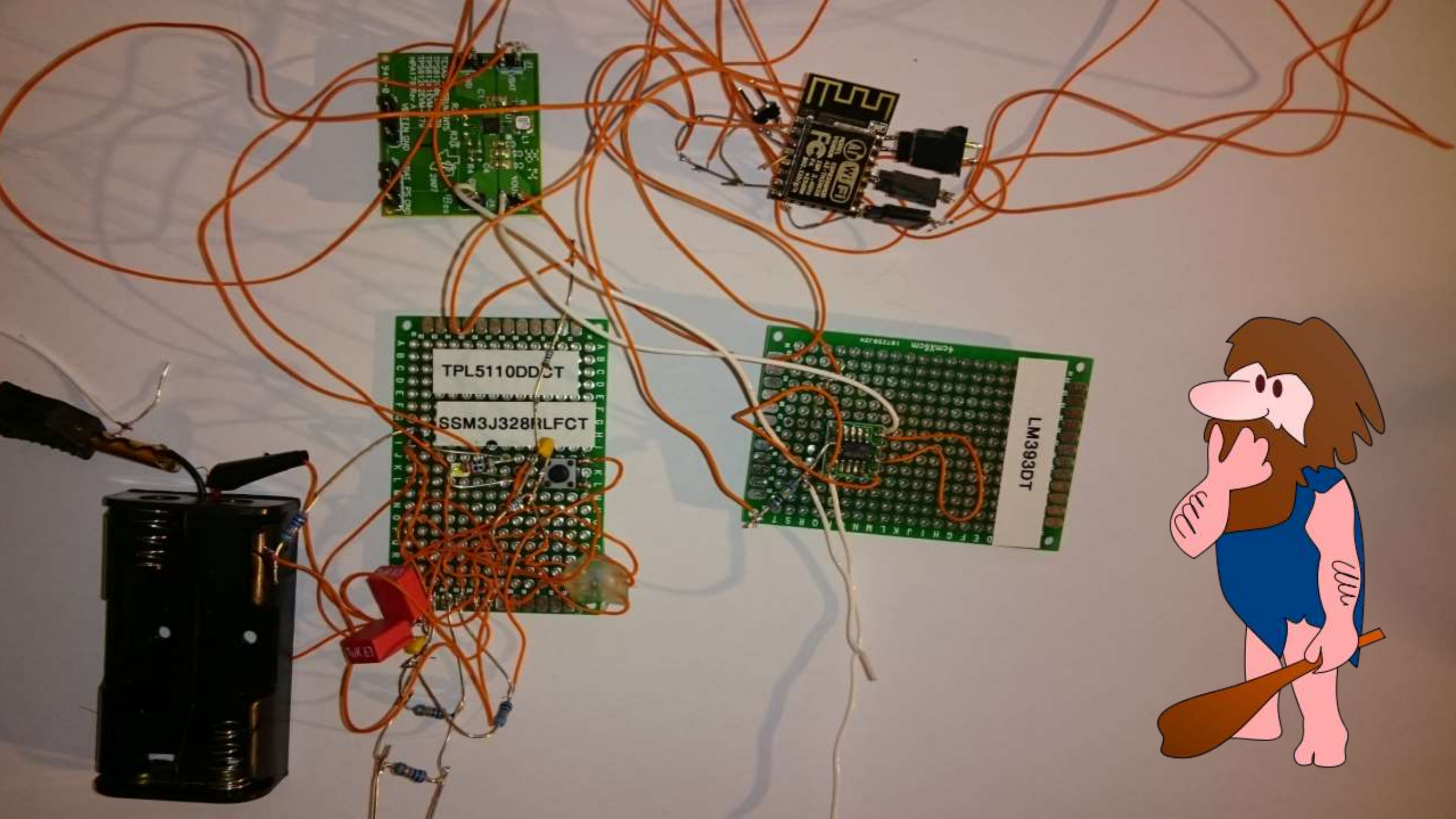
Agenda

- bIOTech Intro
- bIOTech Setup
- bIOTech Tampering
- ESP32 Advantages over ESP8266
- ESP related CVEs, Talks



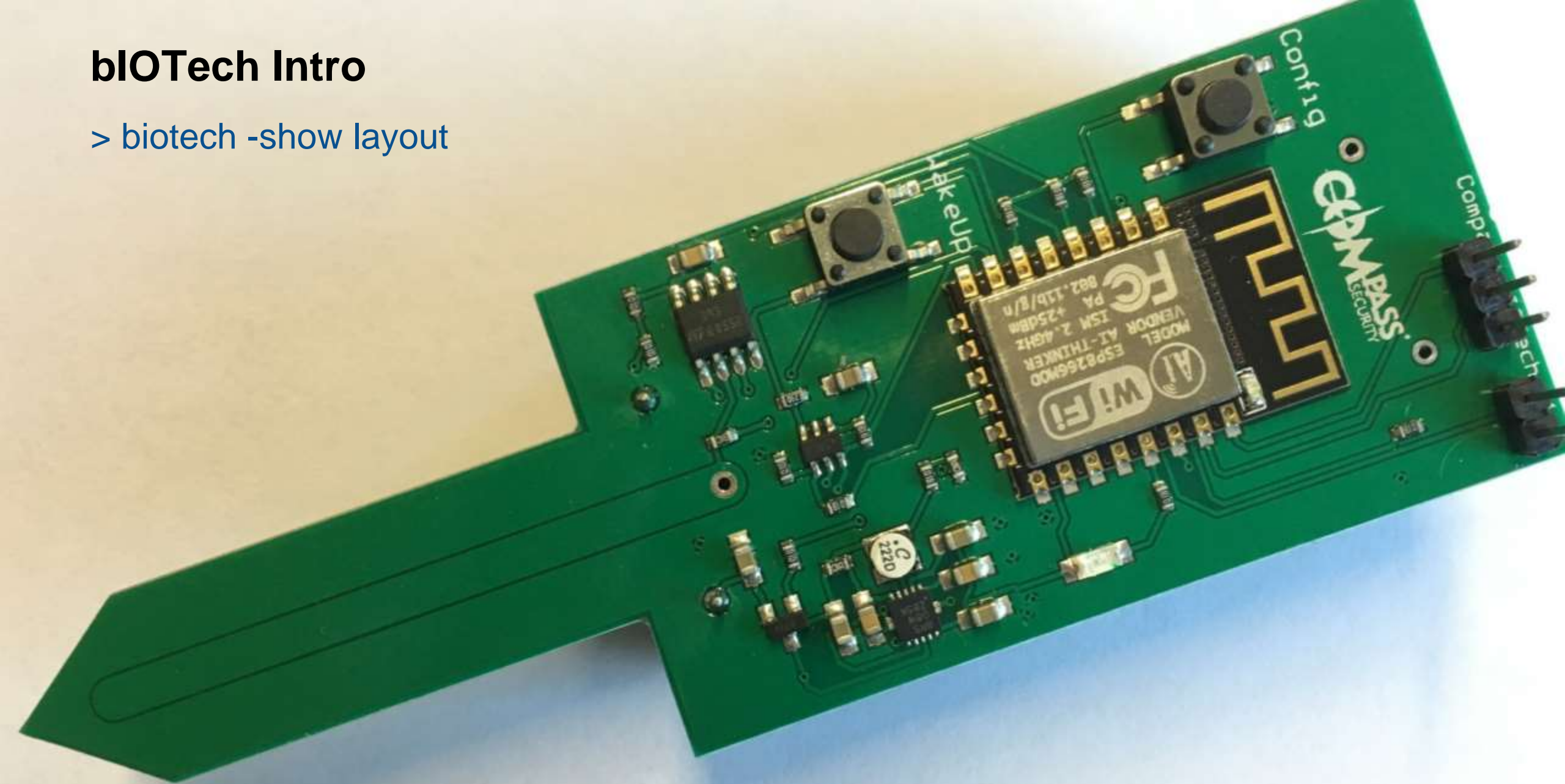
**“The S in IoT stands
for security.”**

Tim Kadlec ([@tkadlec](#))



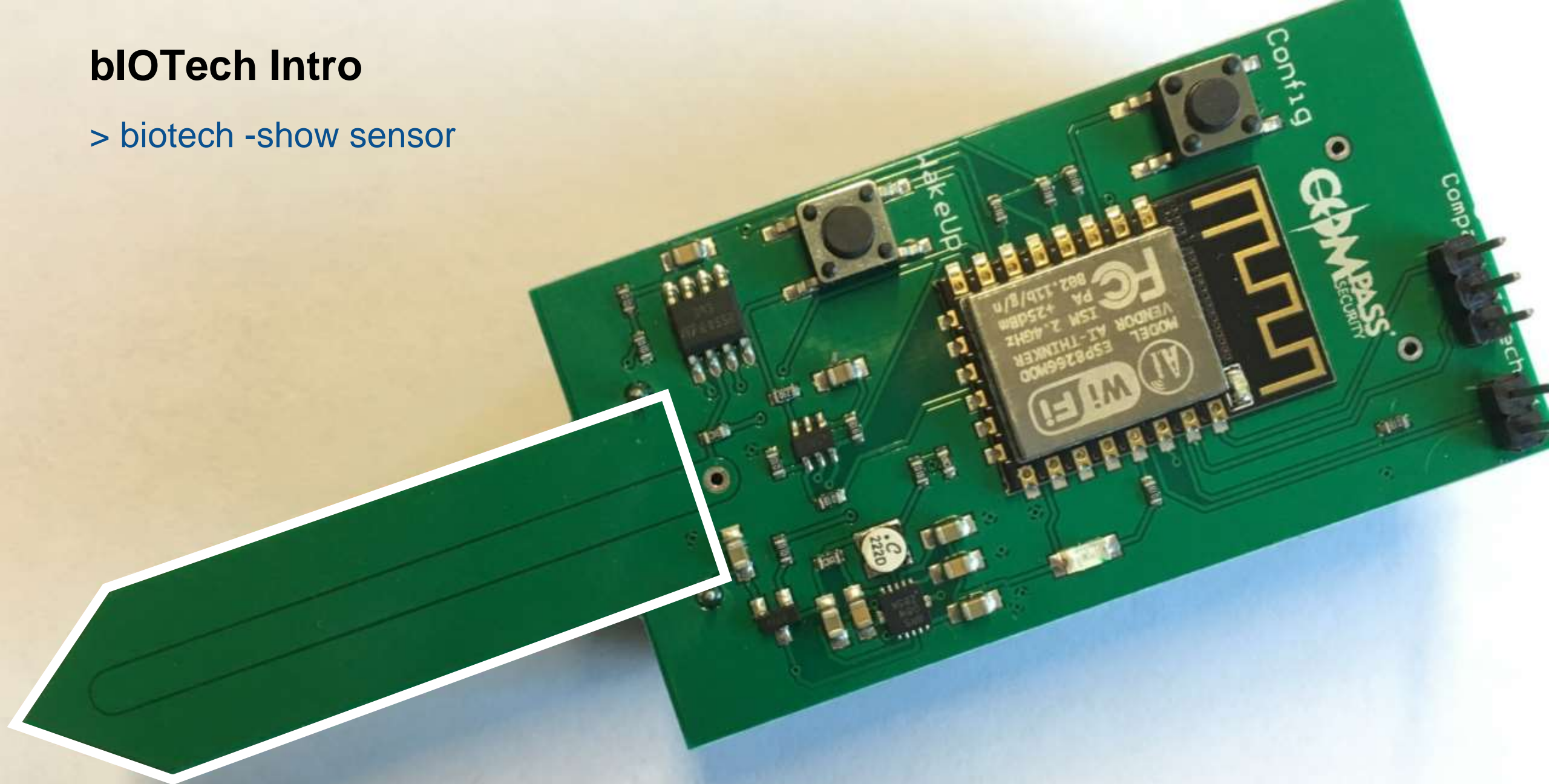
blOTech Intro

> biotech -show layout



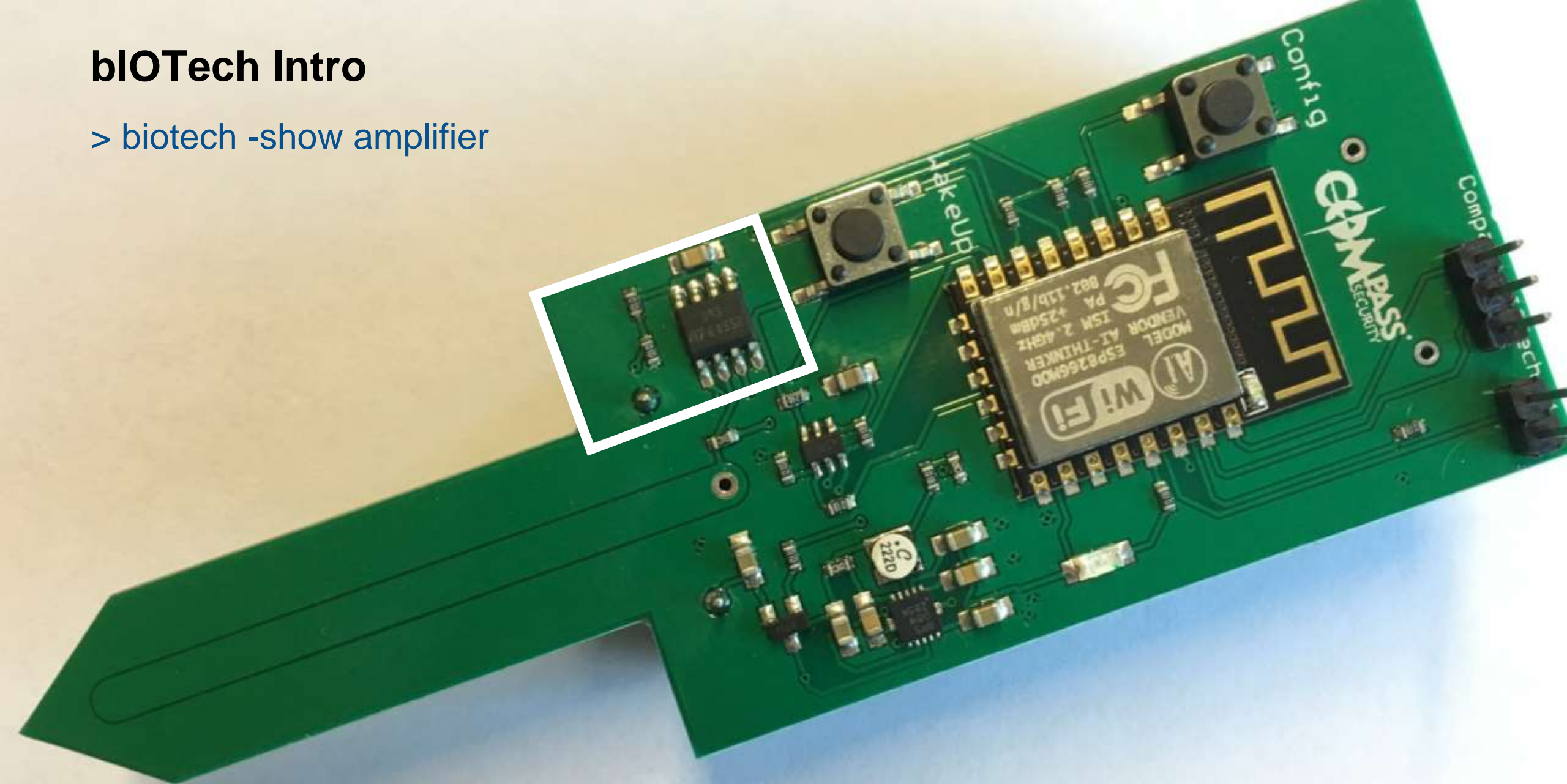
blOTech Intro

> biotech -show sensor



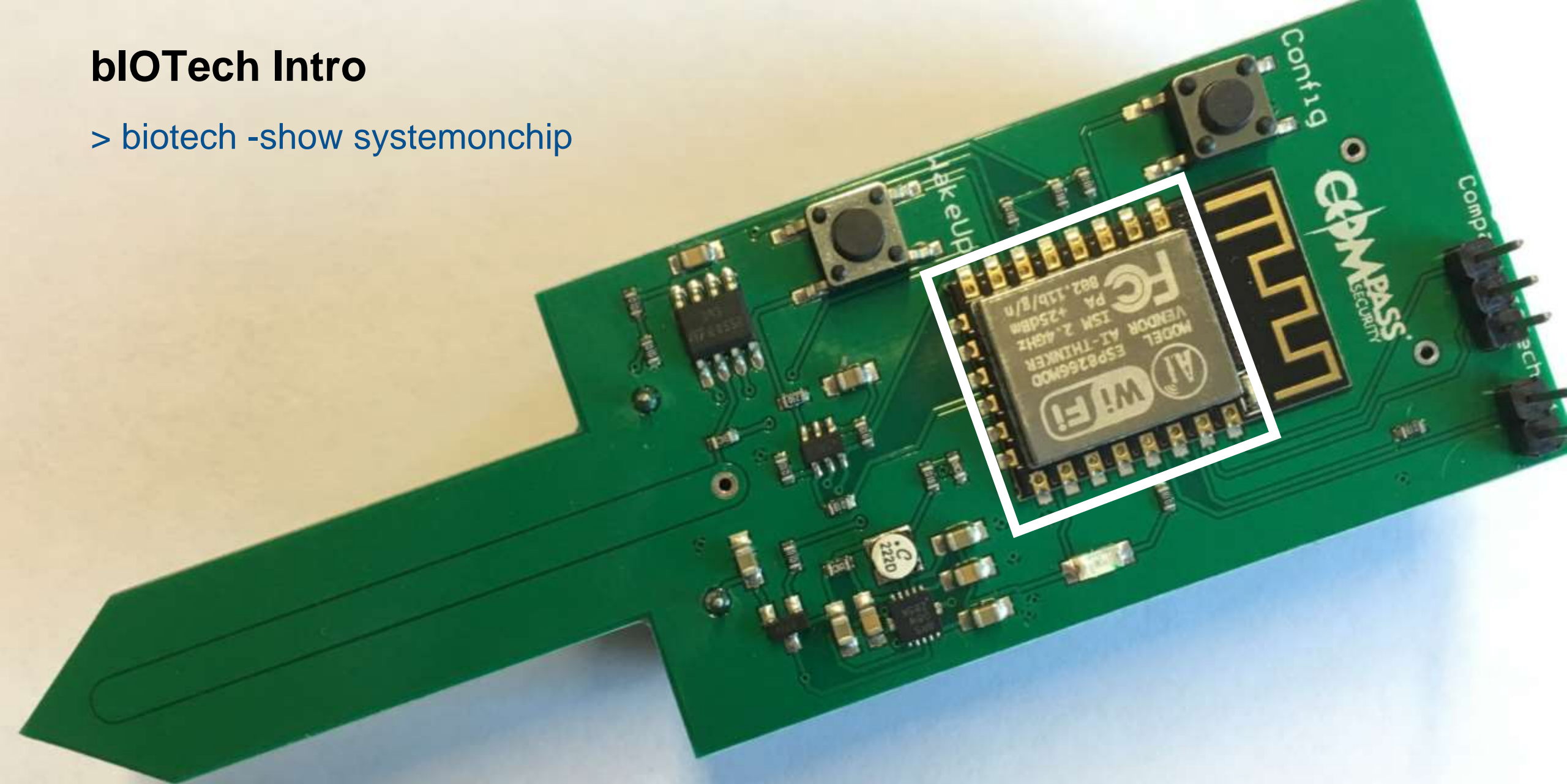
blOTech Intro

> biotech -show amplifier



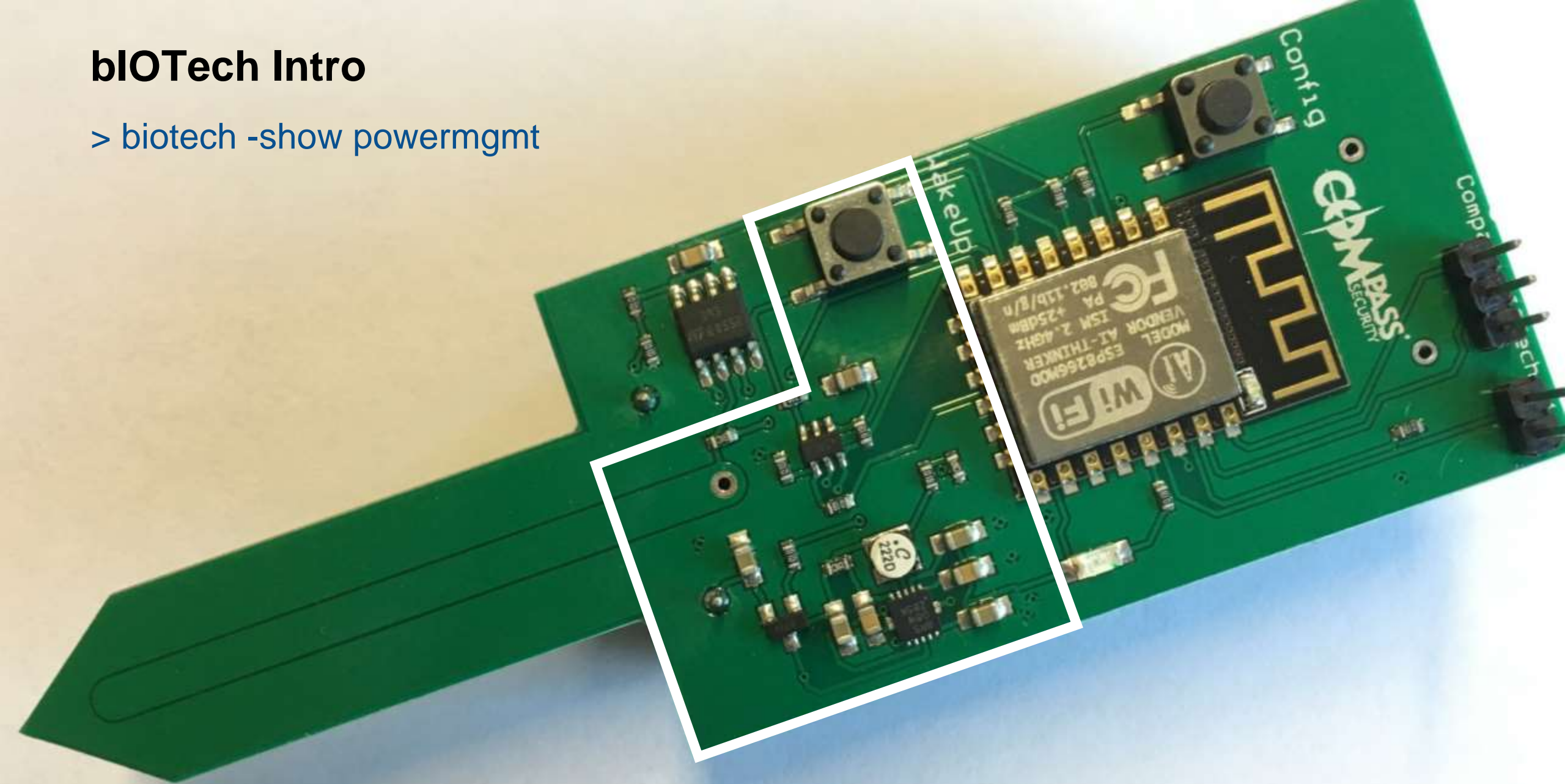
blOTech Intro

> biotech -show systemonchip



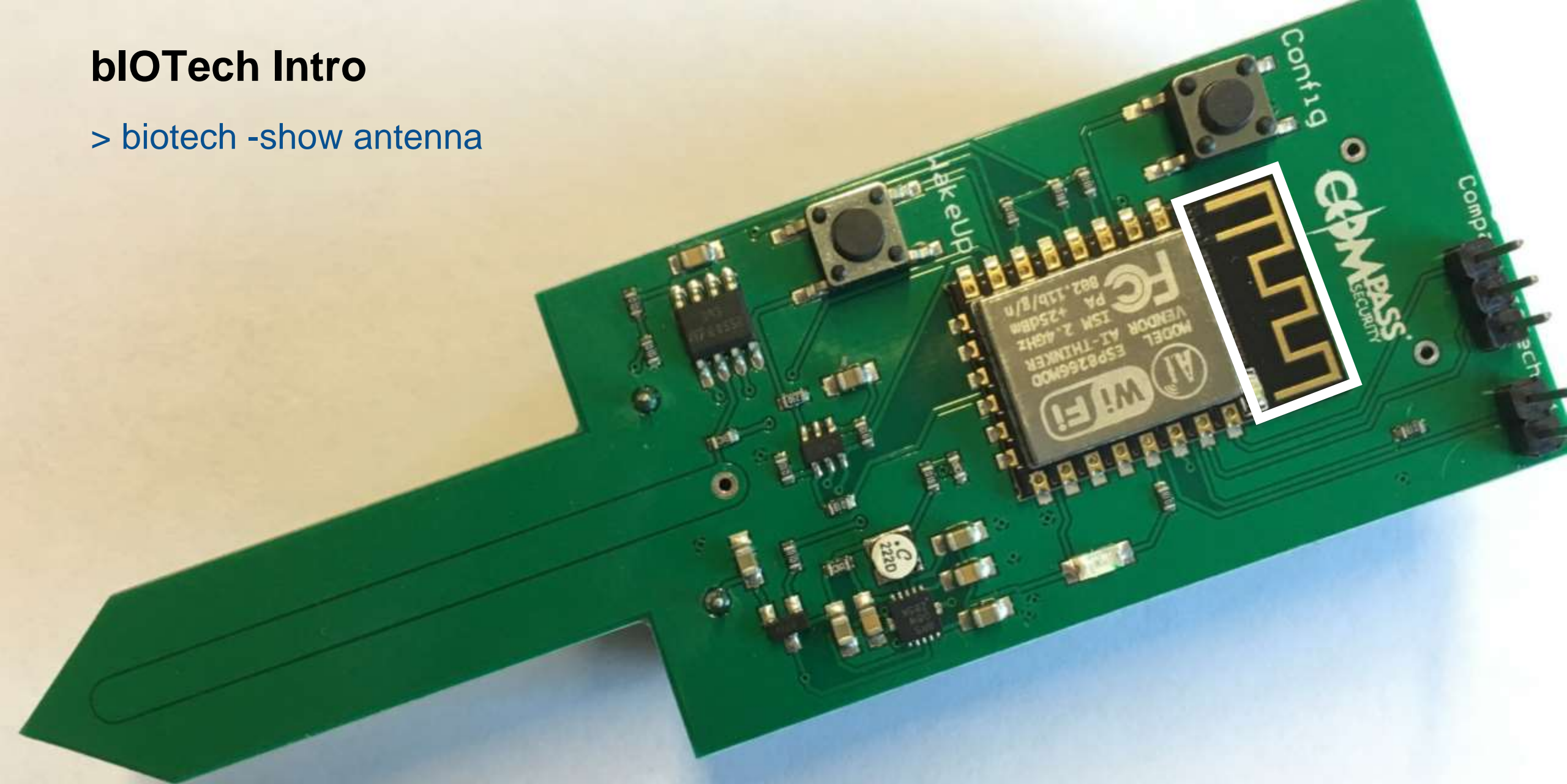
blOTech Intro

> biotech -show powermgmt



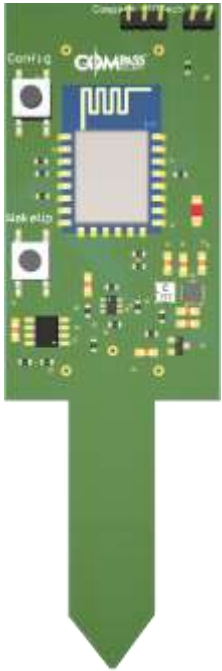
bioTech Intro

> biotech -show antenna



biOTech Intro

> biotech -net show



HACKING-LAB®

57336 62

IoT Devices

If you are the lucky owner of one of our IoT devices, you can register it here. For more information read this [PDF](#) about biOTech devices.

[Register New Device](#)

Token	Last Check	Battery	Humidity/Limit
ikUQLbIwqSvkJmzAC39Ys2z7AYw74R1E	2017-10-10 14:21	2.76	1218 / 10000

blOTech Setup

> biotech -show opmodes

Configuration Mode (**red** LED on)

- Device is a Wifi AP and DHCP service
- Provides Web GUI for configuration



Measurement Mode (**blue** LED only on)

- Device connects to the configured WLAN SSID
- Submits moisture level, battery level and firmware version



Switch to Configuration Mode

- Wait until the **blue** LED is off, press and hold the Config button
- Press and release the WakeUp button, wait 2 seconds
- Release Config button

biOTech Setup

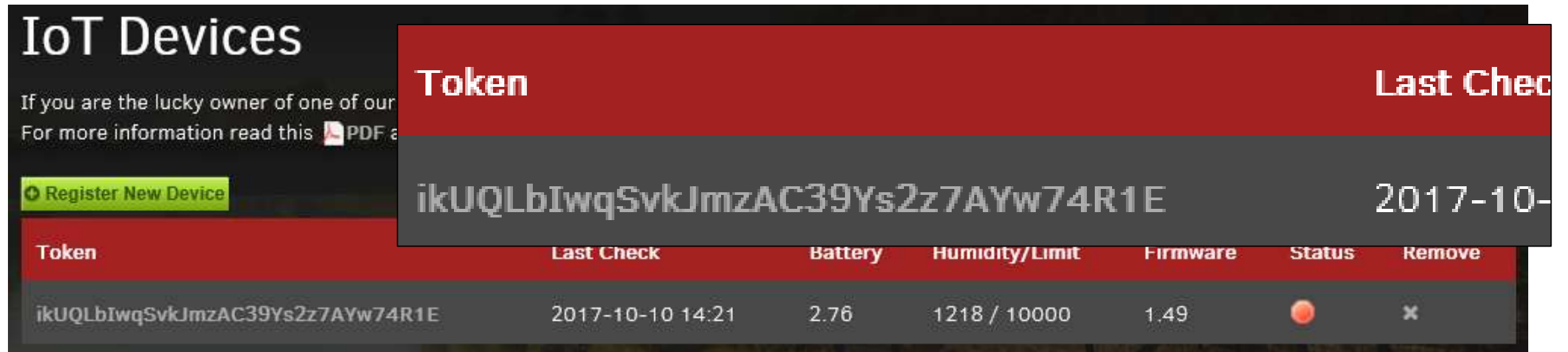
> biotech --get-token

1. Login with your credentials to the HACKING-LAB webpage, or create a new account:

<https://www.hacking-lab.com>

2. Open the IoT devices page and “Register New Device”

<https://www.hacking-lab.com/user/myprofile/iotdevice.html>



The screenshot shows the 'IoT Devices' page with a table of devices. A modal window is open, displaying a token. The table has columns: Token, Last Check, Battery, Humidity/Limit, Firmware, Status, and Remove. The modal window shows the token: ikUQLbIwqSvkJmzAC39Ys2z7AYw74R1E and the last check date: 2017-10-10.

Token	Last Check	Battery	Humidity/Limit	Firmware	Status	Remove
ikUQLbIwqSvkJmzAC39Ys2z7AYw74R1E	2017-10-10 14:21	2.76	1218 / 10000	1.49		

3. Copy the Token (e.g. ikUQLbIwqSvkJmzAC39Ys2z7AYw74R1E) to the clipboard

blOTech Setup

> `biotech --set-speaking-id name`

4. Click on the device entry to label it with a human readable text

A screenshot of a web interface titled "IoT Devices". The interface has a dark background with a light-colored header bar. In the top left of the header is a "Send" button with an upward arrow icon. In the top right is a "back" link with a left arrow icon. Below the header, there are three input fields. The first is labeled "Token" and contains the text "ikUQLblwqSvkJmzAC39Ys2z7AYw74R1E". The second is labeled "Name" and is empty. The third is labeled "Humidity (lower limit)" and contains the text "10000".

IoT Devices

[Send](#) [back](#)

Token: ikUQLblwqSvkJmzAC39Ys2z7AYw74R1E

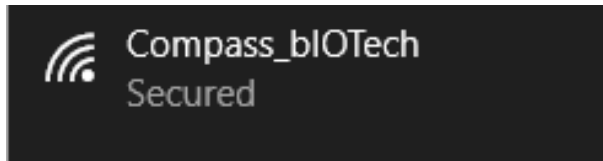
Name:

Humidity (lower limit): 10000

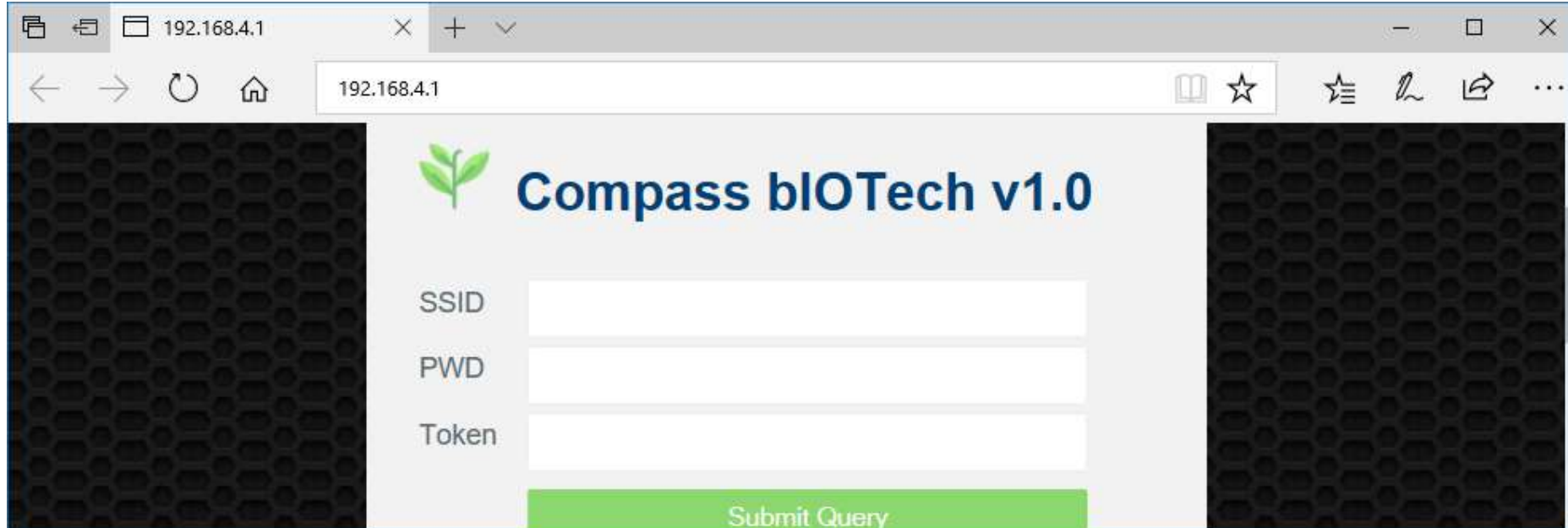
blOTech Setup

> biotech -mode config

1. Insert battery and check config mode (red LED on)
2. Connect to the Compass_bIOTech WLAN (Pass: BonsaiBonsai)



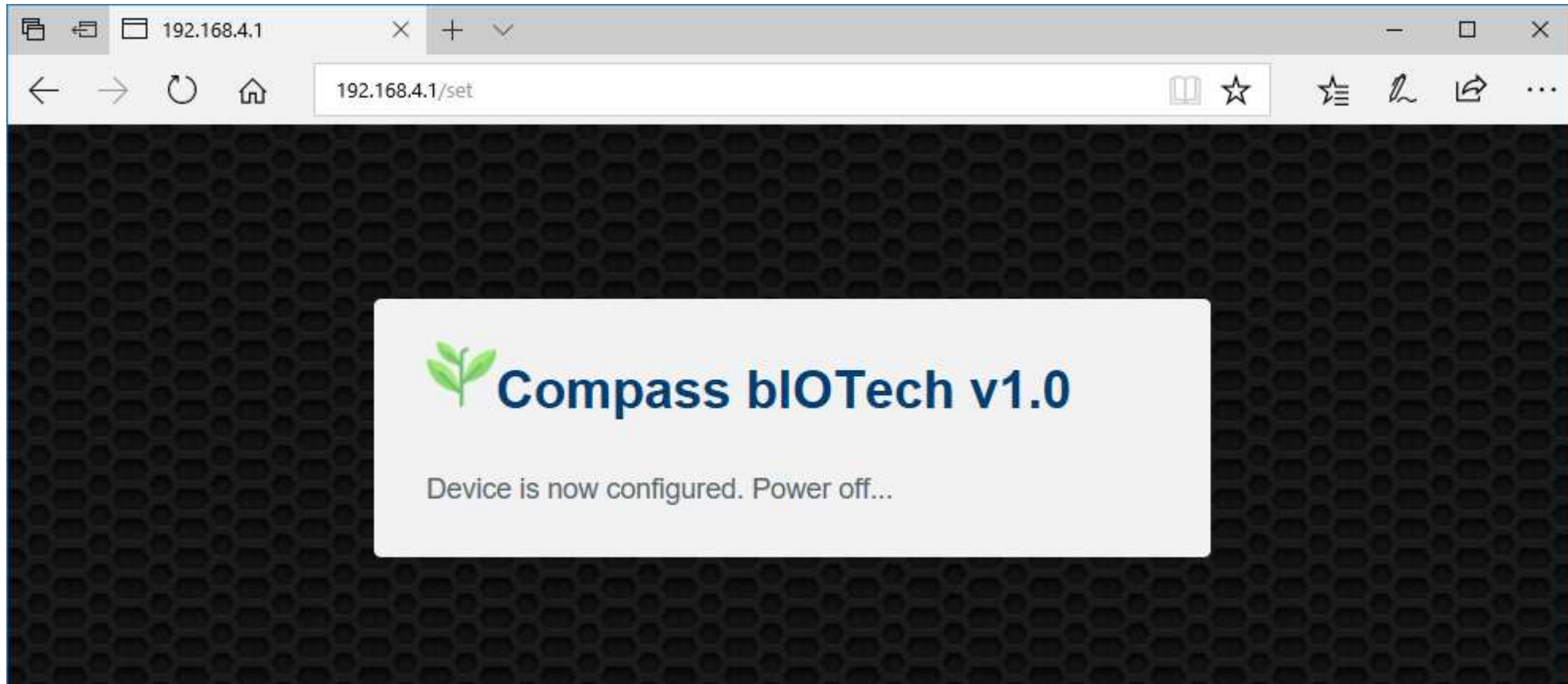
3. Browse to the Web UI – <http://192.168.4.1/> and enter your own SSID/Password/Token



blOTech Setup

> biotech -mode config

4. Device will store config and turn-off




bIOTech Setup



> biotech -status

5. Status happily turns green on success

IoT Devices

If you are the lucky owner of one of our IoT devices, you can register it here.
For more information read this  PDF about bIOTech devices.

[+ Register New Device](#)

Token	Last Check	Battery	Humidity/Limit	Firmware	Status	Rem
My Device	2017-10-17 17:49	2.54	1227 / 10000	1.49		

bioTech Tampering

> biotech --do-evil

What could go wrong?

- Access Controls Deficiencies
- Network Connectivity Fails
- Web Interfaces Issues
- Firmware Bugs
- Physical Security
- ...

... we encourage you to do your own threat modelling.

Maybe with OWASPs ideas on IoT at hand

https://www.owasp.org/index.php/IoT_Security_Guidance



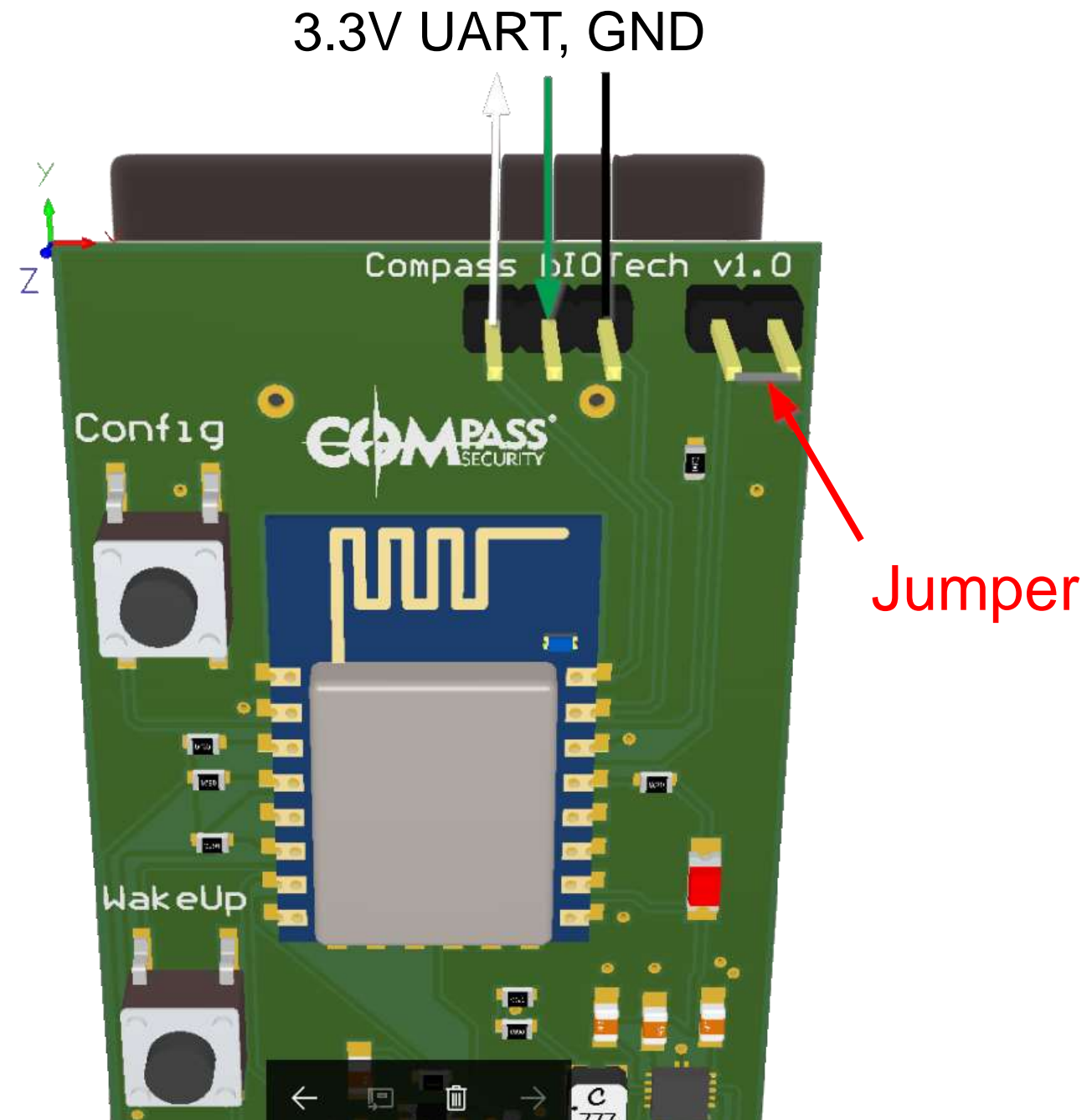
blOTech Tampering

> biotech --connect /dev/ttyUSB0

UART (3.3V !!!) access to the SoC can be enabled by setting a **jumper**

Various ways of programming and dumping are provided by either Espressif's toolchain or third-parties.

Kickstart at
<https://github.com/espressif/esptool>



blOTech Tampering

> biotech --dump-flash

```
Terminal - root@HLKali: /opt/esptool
File Edit View Terminal Tabs Help
root@HLKali:/opt/esptool# ./esptool.py --port /dev/ttyUSB0 --baud 115200 read_flash 0x0 0x100000 dump.bin
esptool.py v2.2-dev
Connecting....
Detecting chip type... ESP8266
Chip is ESP8266EX
Uploading stub...
Running stub...
Stub running...
1048576 (100 %)
1048576 (100 %)
Read 1048576 bytes at 0x0 in 96.3 seconds (87.1 kbit/s)...
Hard resetting...
root@HLKali:/opt/esptool#
```

biOTech Tampering

> biotech --grep-flash

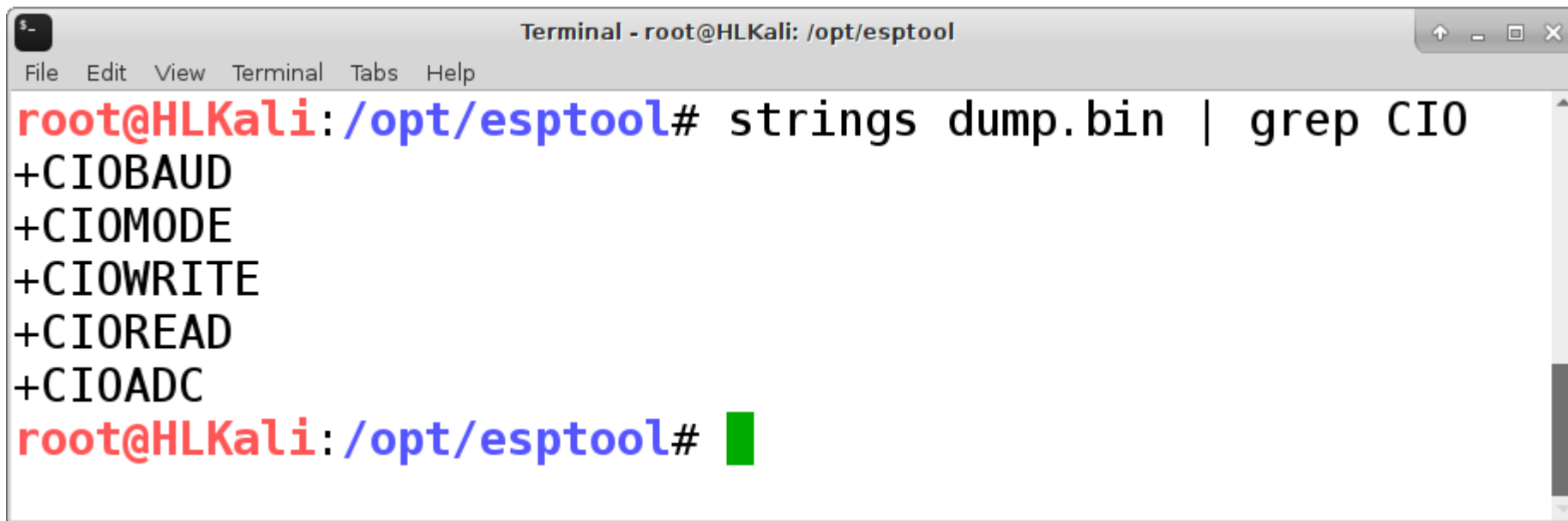
Scrape memory for strings. E.g. the WLAN SSID and password

```
Terminal - root@HLKali: /opt/esptool
File Edit View Terminal Tabs Help
?m~ @
0$;f
Compass_bIOTech
?BonsaiBonsai
P#@*
Dungeon
blabliblu
?m~ @
0$;f
RNJD@8
RNJD@8
|8|9|:|;|<|=|x|y|z|{|||}|
AI-THINKER_C883BB
AI-THINKER_C883BB
root@HLKali: /opt/esptool#
```

blOTech Tampering

> biotech --talk-to-cio

It seems like the blOTech does talk and understand the CIO language. It can even adopt to the baud rate ;)



```
Terminal - root@HLKali: /opt/esptool
File Edit View Terminal Tabs Help
root@HLKali:/opt/esptool# strings dump.bin | grep CIO
+CIOBAUD
+CIOMODE
+CIOWRITE
+CIOREAD
+CIOADC
root@HLKali:/opt/esptool#
```


blOTech Tampering

```
/* Dumper written in C based on Arduino IDE package
 * http://arduino.esp8266.com/stable/package\_esp8266com\_index.json
 */

// read wlan ssid (location 1 to \0)
if ((i < 32) and esid_stop == false) {
    if ((EEPROM.read(i) != '\0')) {
        ...
    }
// read wlan pass (location 32 to \0)
if ((i >= 32) and (i < 96) and epass_stop == false) {
    if ((EEPROM.read(i) != '\0')) {
        ...
    }
// read webservice token (location 96 to 128)
if ((i >= 96) and (i < 128)) {
    token += char(EEPROM.read(i));
}
}
```

biOTech Tampering

> biotech --connect /dev/ttyUSB0

How about the Hacking-lab device ID token?

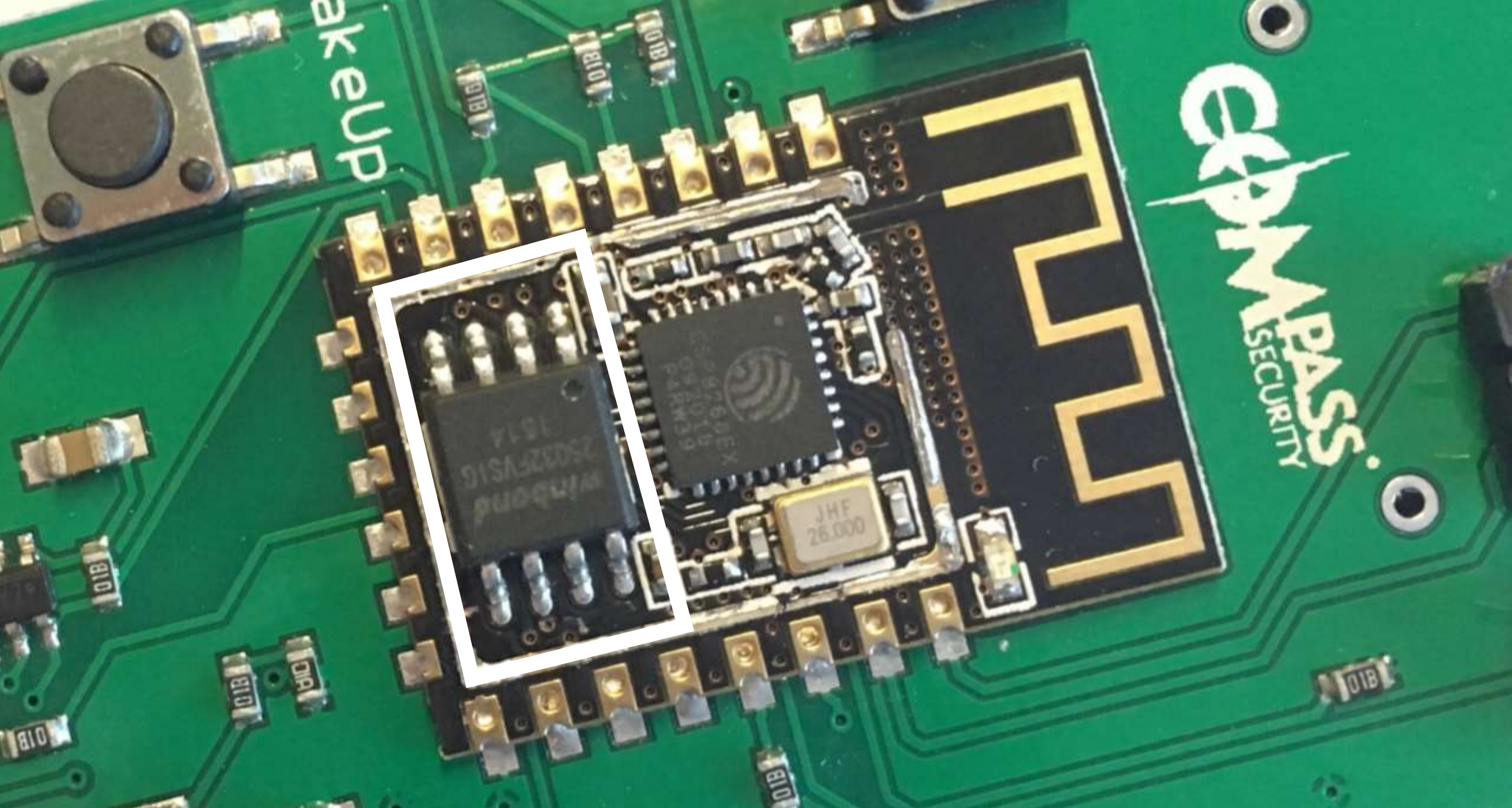
```
Compass biOTech EEPROM dumper V0.1...
```

```
44 75 6e 67 65 6f 6e 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
62 6c 61 62 6c 69 62 6c 75 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
69 6b 55 51 4c 62 49 77 71 53 76 6b 4a 6d 7a 41 43 33 39 59 73 32 7a 37 41 59 77 37 34 5
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
```

```
...

*****
SSID:   Dungeon
PASS:   blabliblu
Token:  ikUQLbIwqSvkJmzAC39Ys2z7AYw74R1E
*****
```

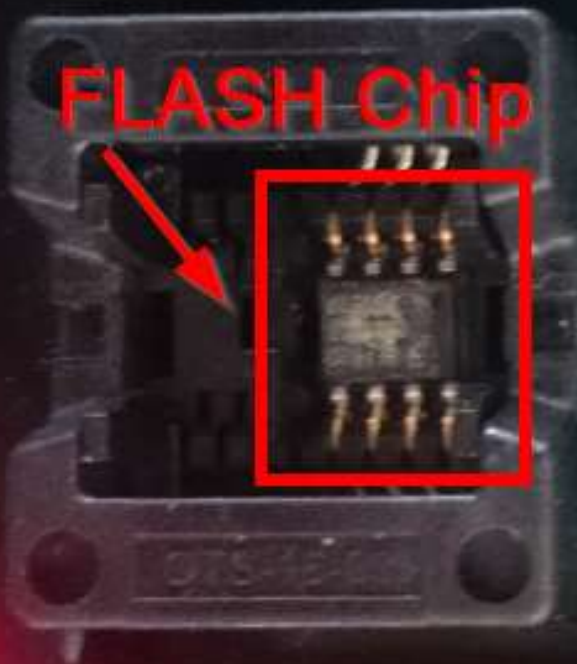
```
Put device to sleep... zzzZZzzzzZZzzzzz!
```





REVELPROG IS

FLASH Chip



POWER
BUSY

X	7	5	3	1
X	8	6	4	2





	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
000E3940	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E3950	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E3960	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E3970	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E3980	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E3990	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E39A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E39B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E39C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E39D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E39E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E39F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000E3A00	0F	00	00	00	FC	7B	0A	20	20	22	77	69	66	69	22	3A
000E3A10	20	7B	0A	20	20	20	20	22	73	74	61	22	3A	20	7B	0A
000E3A20	20	20	20	20	20	20	22	65	6E	61	62	6C	65	22	3A	20
000E3A30	74	72	75	65	2C	0A	20	20	20	20	20	22	73	73	69	
000E3A40	64	22	3A	20	22	48	35	22	2C	0A	20	20	20	20	20	20
000E3A50	22	70	61	73	73	22	3A	20	22	52	65	74	6F	73	54	65
000E3A60	73	74	41	50	22	0A	20	20	20	20	7D	2C	0A	20	20	20
000E3A70	20	22	61	70	22	3A	20	7B	0A	20	20	20	20	20	20	22

```
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
YYYYYYYYYYYYYYYYYY
....ü{.  "wifi":
{.  "sta": {.
  "enable":
true,.  "ssi
d": "H5",.
"pass": "RetosTe
stAP".  },.
```


Conclusion

ESP8266 has NO physical security features.

ESP32 could provide

- Flash Encryption
- Secure Boot
- E-Fuses to lock-down JTAG, MAC-Address etc.

However, this is by no means comparable to tamper-resistance of TPMs and SmartCards

More on ESP8266 and ESP32

- CVE-2017-7185 Mongoose Web Server, **Use After Free and DoS**
- CVE-unassigned Mongoose Web Server, **Stack Based Overflow**
- Want to hear more on ESP32, ESP8266 and Mongoose OS?
 - Join us for our next Beertalks in Jona and Berne
 - Listen to us at DefCamp 2017 in Bucharest
 - Visit our IoT Security Training (30% discount today)
 - Stay tuned @compasssecurity

Thanks... don't forget your device

