

# Is my toothbrush really smart?

Axelle Apvrille

Troopers, March 2018



## Introduction

How it works

Virtual toothbrush

Smart Toothbrush Cloud

Conclusion



# Who am I?



Anti-virus researcher with **Fortinet**  
smart phone, smart *things*

# Why hack a smart toothbrush?

- ① Because it's **fun**. You're going to *brush your teeth with a Bluetooth dongle*, you're warned :)

# Why hack a smart toothbrush?

- ① Because it's **fun**. You're going to *brush your teeth with a Bluetooth dongle*, you're warned :)
- ② Because it's **difficult**. Yes, it's harder than hacking an **IP camera**. Everybody knows how to *telnet* on a Linux, huh ;P

# Why hack a smart toothbrush?

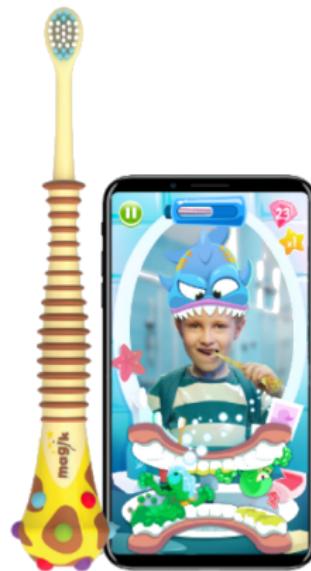
- ① Because it's **fun**. You're going to *brush your teeth with a Bluetooth dongle*, you're warned :)
- ② Because it's **difficult**. Yes, it's harder than hacking an **IP camera**. Everybody knows how to *telnet* on a Linux, huh ;P
- ③ I want to **turn down the myth “nobody cares, there's nothing to secure in a toothbrush”**. **All connected devices need some level of security.**

# Smart toothbrushes?

Braun Oral B, Grush Smart toothbrush, Shenzhen Tita, Ningbo  
Seago SG 976, Kolibree Magik, Ara...



Oral B Pro 5000  
Photo credits: Oral B



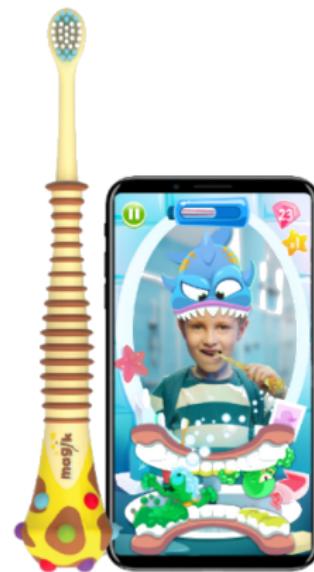
Kolibree Magik  
Photo credits: Kolibree

# Smart toothbrushes?

Braun Oral B, Grush Smart toothbrush, Shenzhen Tita, Ningbo Seago SG 976, Kolibree Magik, Ara...



Oral B Pro 5000  
Photo credits: Oral B



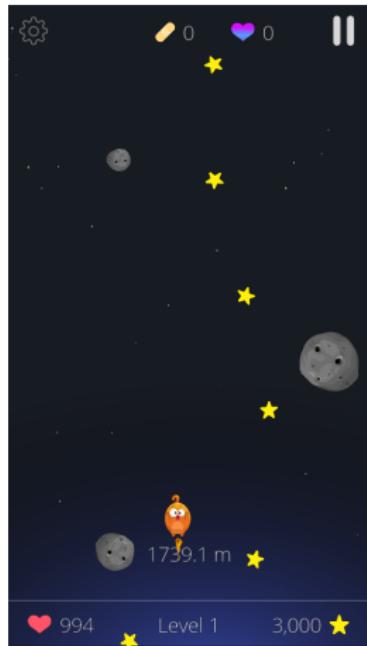
Kolibree Magik  
Photo credits: Kolibree



For this talk

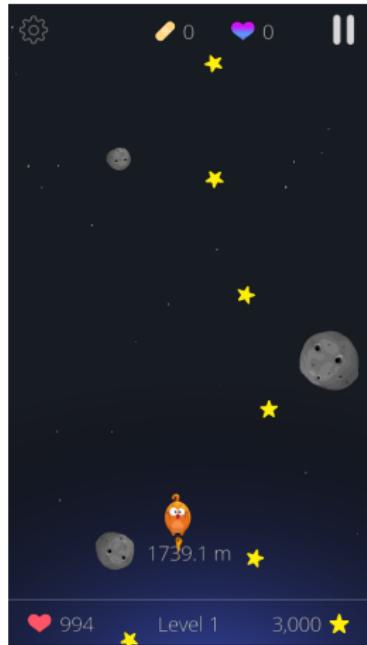
# What for?

- ① Motivate and educate kids



# What for?

- ① Motivate and educate kids
- ② And adults



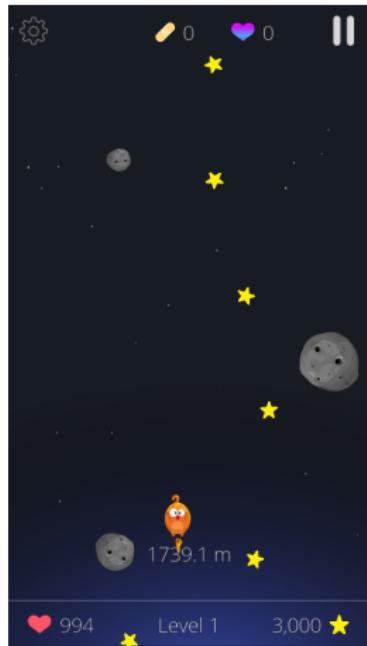
## Health improvements?

Average for brushing teeth is **once for 45 to 70 seconds**

Vendor say their users' average is **twice for 110 seconds**

# What for?

- ① Motivate and educate kids
- ② And adults
- ③ Do business, make money ;P



## Health improvements?

Average for brushing teeth is **once for 45 to 70 seconds**

Vendor say their users' average is **twice for 110 seconds**

# Dental insurance



- Commercialized in the **USA**
- Employer-based **dental insurance**
- You subscribe to a dental plan and receive a smart toothbrush, replacement heads, toothpaste & floss.
- **Impossible to purchase the toothbrush alone.**

Introduction

How it works

Virtual toothbrush

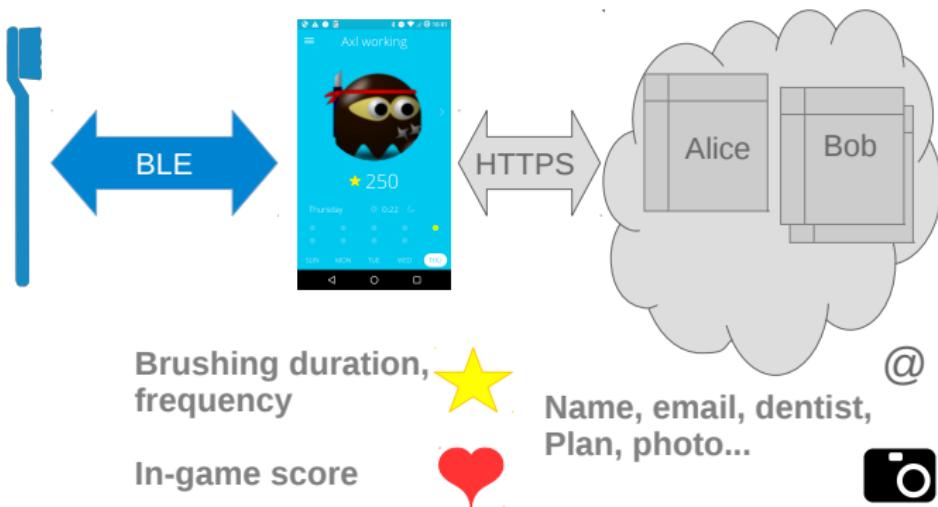
Smart Toothbrush Cloud

Conclusion



# Connecting the toothbrush

Smart toothbrush      Mobile app      Dental insurance



# A Bluetooth Low Energy device



## Toothbrush Service

04234f8e-75b0-4525-9a32-193d9c899d30

- **Motor Speed.** UUID: 833da694-51c5-4418-..., Value: 0xd0, Read, Write
- **Battery Level.** UUID: 6dac0185-e4b7-4a..., Value: 584c, Read.
- ...

## 3D Service

...

An attribute consists of:

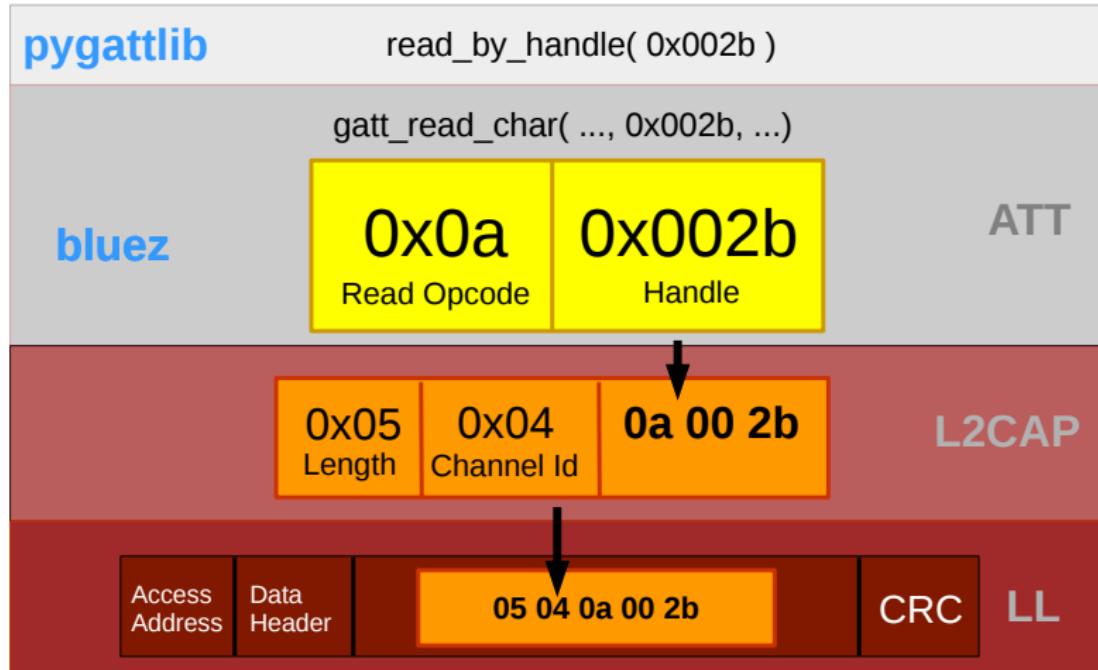
- UUID: it is a **type** e.g. Device Name type
- **Value** e.g. “My smart toothbrush”
- Permissions to access the attribute

Accessed by a **handle**

We can search for attributes, read, write, get notifications.

# How to Speak BLE

Read Motor Speed UUID = 833da694-51c...





# BLE Tools

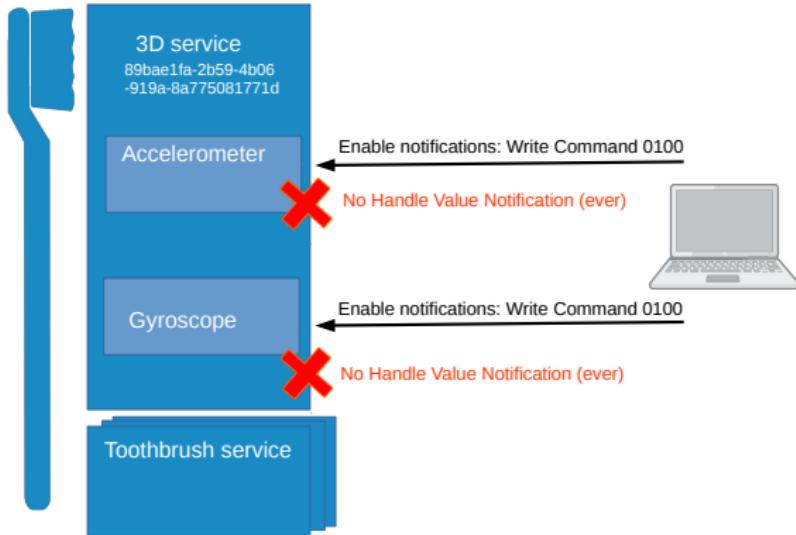
- Adafruit Bluefruit sniffer  
<https://www.adafruit.com/product/2269> (25\$),  
Ubertooth  
<https://github.com/greatscottgadgets/ubertooth>
- Adafruit Python BLE Sniffer [https://github.com/adafruit/Adafruit\\_BLESniffer\\_Python](https://github.com/adafruit/Adafruit_BLESniffer_Python)
- Bluez <http://www.bluez.org/>: Linux Bluetooth protocol stack (see hcitool, gatttool)
- Python interface to BLE: Bluepy  
<https://github.com/IanHarvey/bluepy>, Python interface to GATT: pygattlib  
<https://bitbucket.org/OscarAcena/pygattlib>
- Bleah <https://github.com/evilsocket/bleah>: BLE scan/read/write
- Mobile apps: BLE Scanner (BluePixel), nRF Connect (Nordic Semi.) ...

# Controlling the toothbrush remotely

## Demo

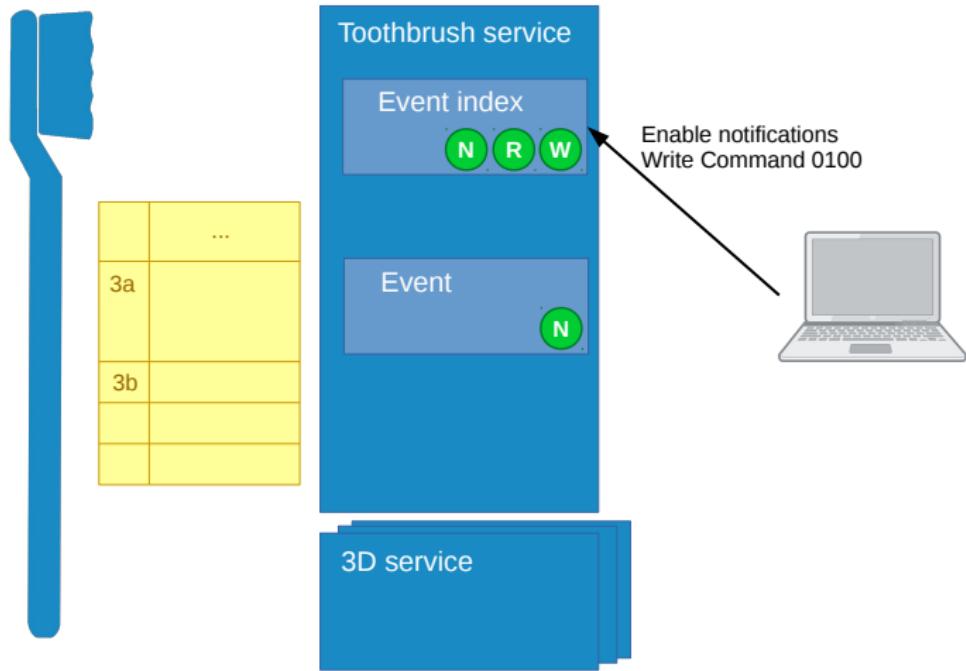
- ① For **Fun**
- ② To gain *independance* - DIY

# Quadrant buzz is ... a timer

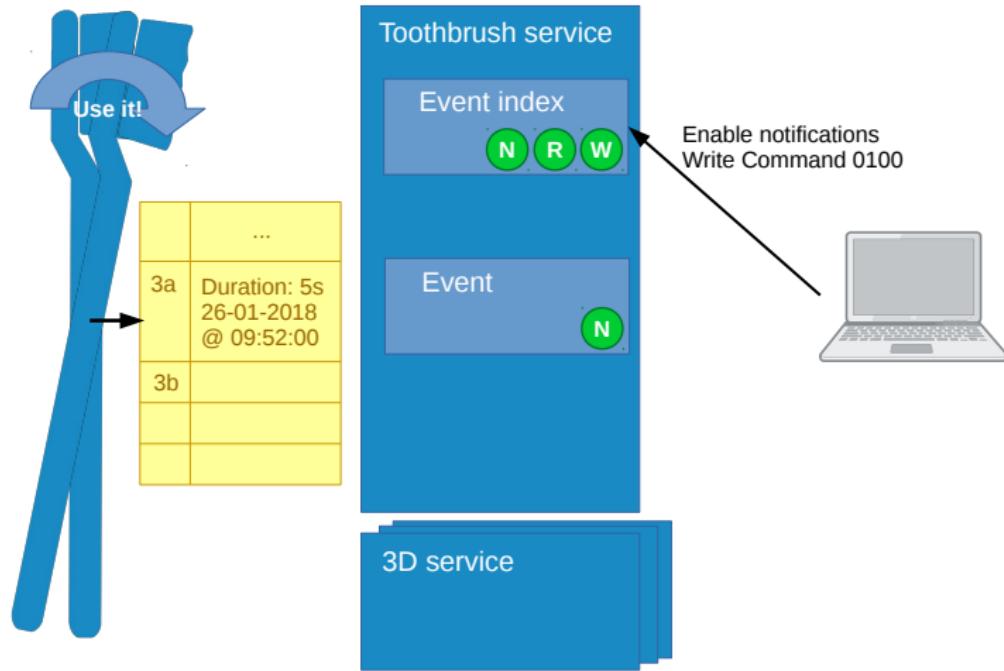


**Gyroscope and accelerometer are not used** in this version  
The toothbrush cannot know which teeth we brush

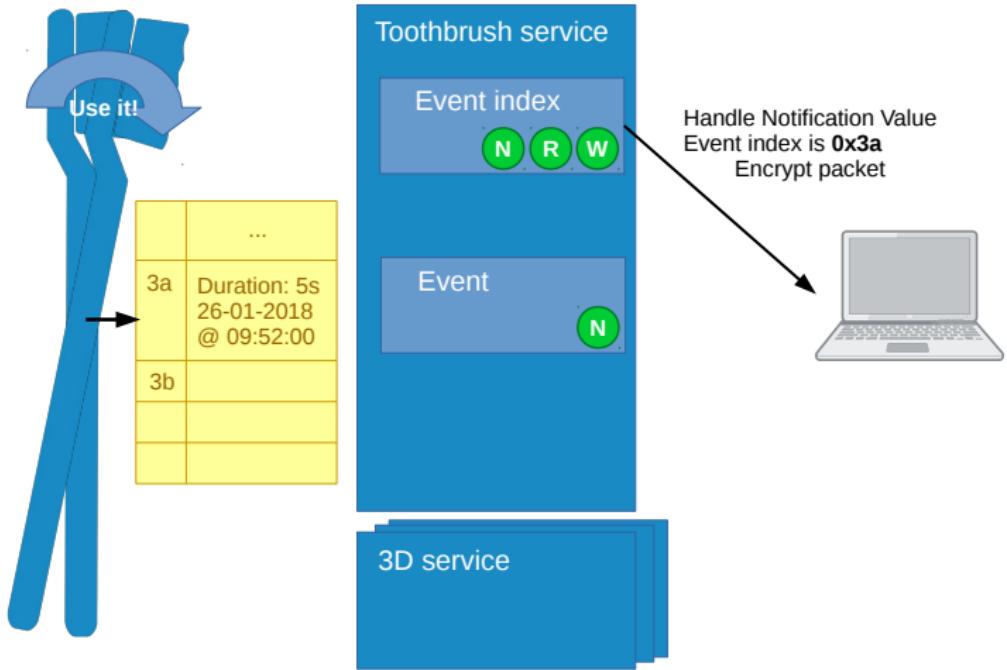
# Hardware events



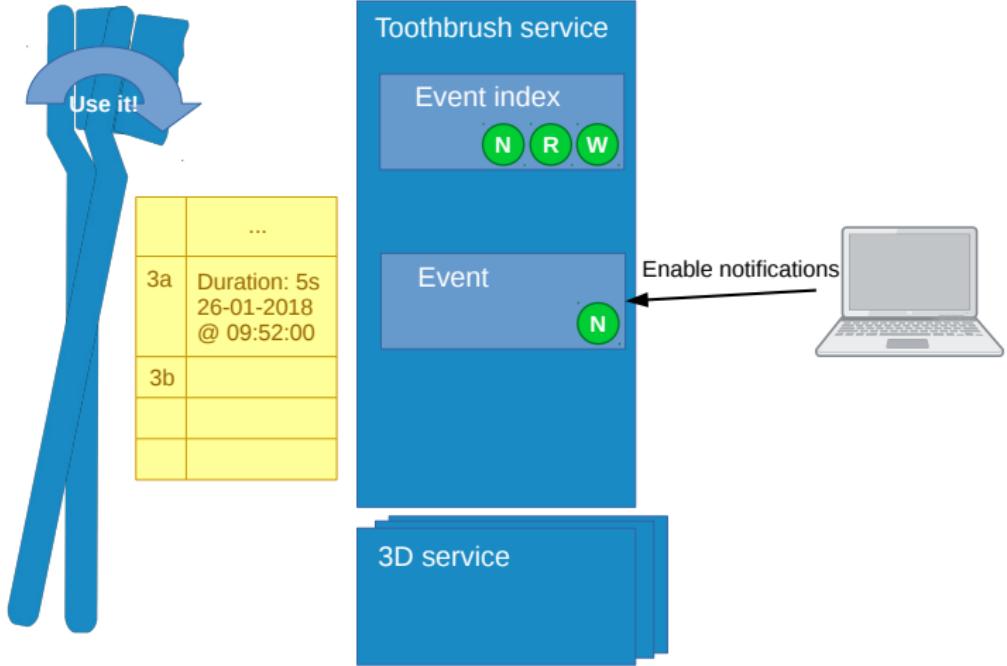
# Hardware events



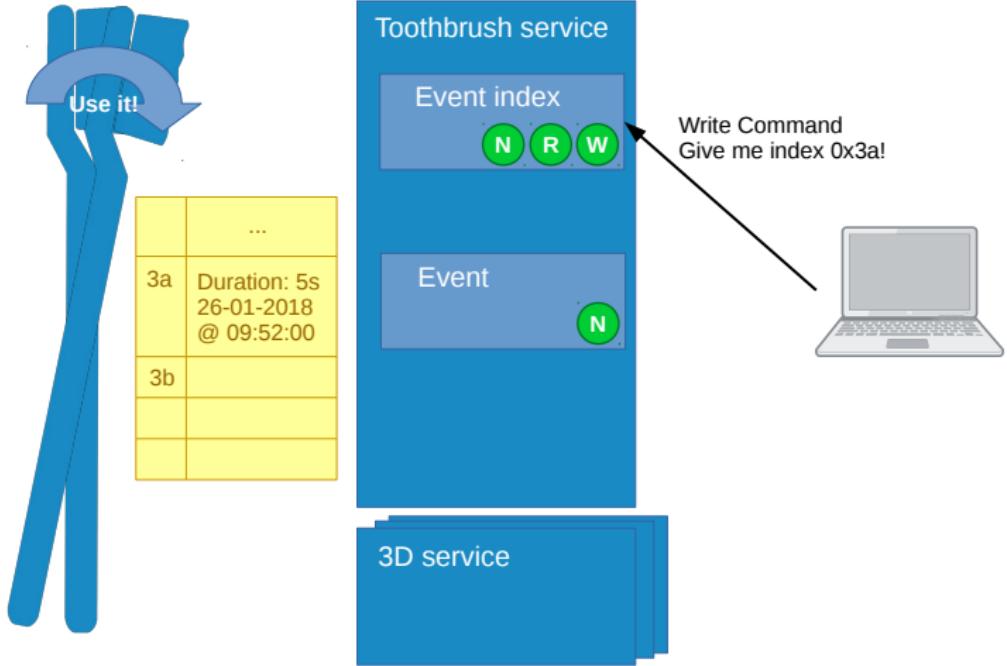
# Hardware events



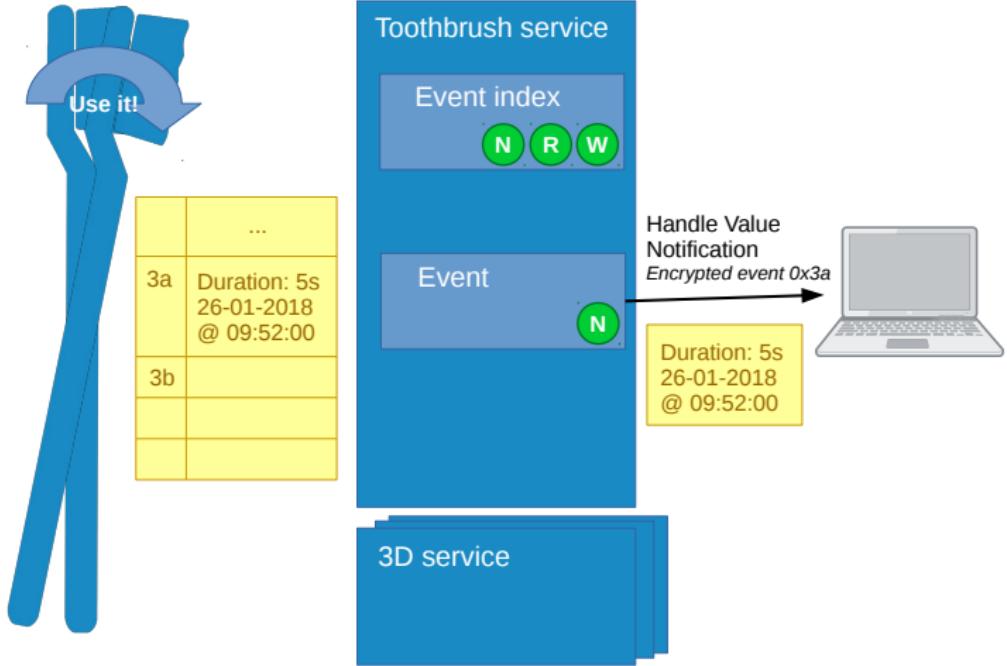
# Hardware events



# Hardware events



# Hardware events

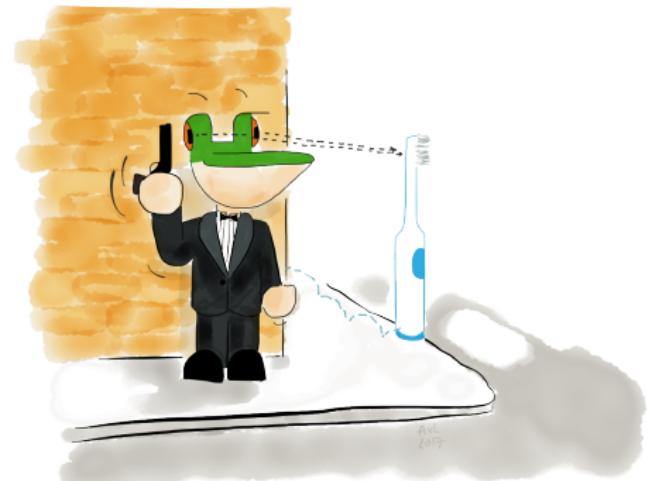


# DEMO

- ① Enable event index notification
- ② Move toothbrush
- ③ Decrypt event index notification
- ④ Enable event notification
- ⑤ Query event index
- ⑥ Decrypt event notification

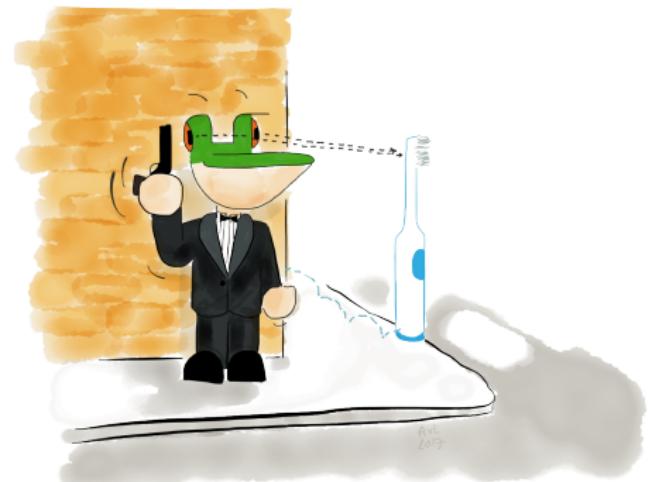
# Interesting attacks for cyber-criminals?

- Not many at this point. (But lots of fun).



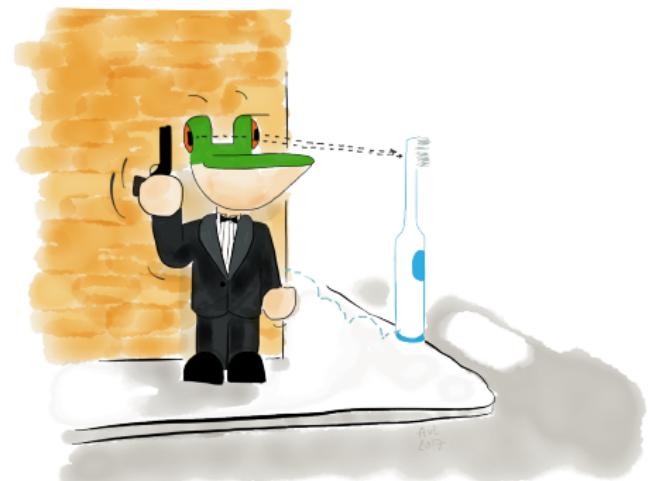
# Interesting attacks for cyber-criminals?

- Not many at this point. (But lots of fun).
- Damage victim's teeth and gums with high **motor speed**?  
Hmmm.



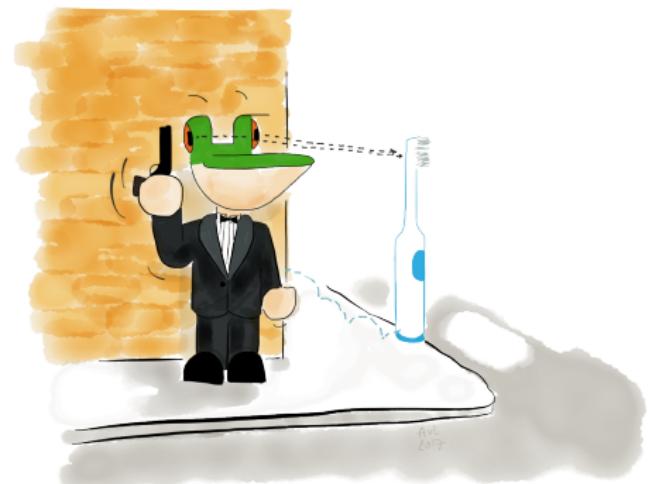
# Interesting attacks for cyber-criminals?

- Not many at this point. (But lots of fun).
- Damage victim's teeth and gums with high **motor speed**?  
Hmmm.
- Remote **kill** of toothbrush.  
Okaaaay.



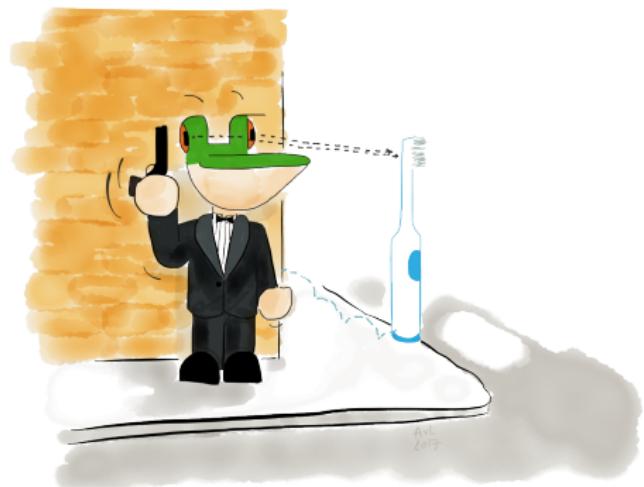
# Interesting attacks for cyber-criminals?

- Not many at this point. (But lots of fun).
- Damage victim's teeth and gums with high **motor speed**?  
Hmmm.
- Remote **kill** of toothbrush.  
Okaaaaay.
- Do you mind if we **track** you?  
Toothbrush MAC address is fixed (despite specs say how to do it)



# Interesting attacks for cyber-criminals?

- Not many at this point. (But lots of fun).
- Damage victim's teeth and gums with high **motor speed**?  
Hmmm.
- Remote **kill** of toothbrush.  
Okaaaaay.
- Do you mind if we **track** you?  
Toothbrush MAC address is fixed (despite specs say how to do it)
- But we'll see bad design leads to worse later. (Suspens).



Introduction  
How it works  
**Virtual toothbrush**  
Smart Toothbrush Cloud  
Conclusion

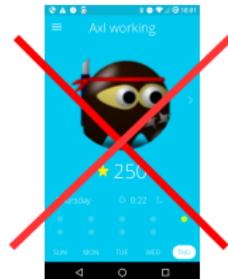


# Summary / Achievements



Bluetooth Low Energy

Mobile application



talk2brush

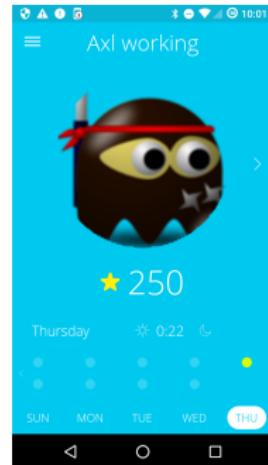
```
| 19:54|$ python talk2brush.py
| 19:54|$ talk2brush - a Beam Brush Linux utility tool ===
0- Buzz
1- Enable accelerometer data notifications
2- Enable button state notifications
3- Enable gyroscope data notifications
4- Enable light sensor notifications
5- Read actively brushing indicator
6- Read all information
7- Read appearance
8- Read auto off and quadrant buzzer settings
9- Read battery level
10- Read brush color
11- Read button state
12- Read current brushing duration in seconds
13- Read gyroscope
14- Read device name
15- Read firmware revision string
16- Read hardware revision
17- Read manufacturer name
18- Read motor number
19- Read motor speed
20- Read motor state
21- Read serial number
22- Read temperature
23- Write auto off and quadrant buzzer settings
24- Write motor speed
Any other value will quit.
Your choice? |
```

# Can we create a fake toothbrush?



```
[Croot@alligator:~# node main.js
Fake Toothbrush BLE device
[+] Start advertising as Beam Service
[+] setServices: success
[+] accepted connection from address: 73:00 [REDACTED]
reading motor speed: 0x d0
[+] Wrote motor speed: 0x 91
[+] Wrote motor speed: 0x c4
[+] Wrote motor speed: 0x 7b
[+] Wrote motor speed: 0x 45
[+] Wrote motor speed: 0x d0
'Croot@alligator:~# ]
```

Fake toothbrush



Mobile app

Yes, we can!

This is a pink smart toothbrush



König Micro Bluetooth Dongle v4.0 (13 euros)



Official mobile app says  
it is pink :)

# How do we do that?

JavaScript

Bleno

Node JS



```
var bleno = require('bleno');
var BlenoPrimaryService = bleno.PrimaryService;

function ToothbrushService() {
  ToothbrushService.super_.call(this, {
    uuid: '04234f8e75b045259a32193d9c899d30',
    characteristics: [ new bleno.Characteristic({
      uuid: '0971ed14e92949f9925f81f638952193',
      properties: ['read'],
      value : colorRead,
    }),
    function colorRead(offset, callback) {
      // 02 = pink
      console.log('reading toothbrush color');
      callback(this.RESULT_SUCCESS, new Buffer('02', 'hex'));
    }
  });
}
```

# A Fake Toothbrush: Is that useful?

- To brush your teeth? **No** ;-)

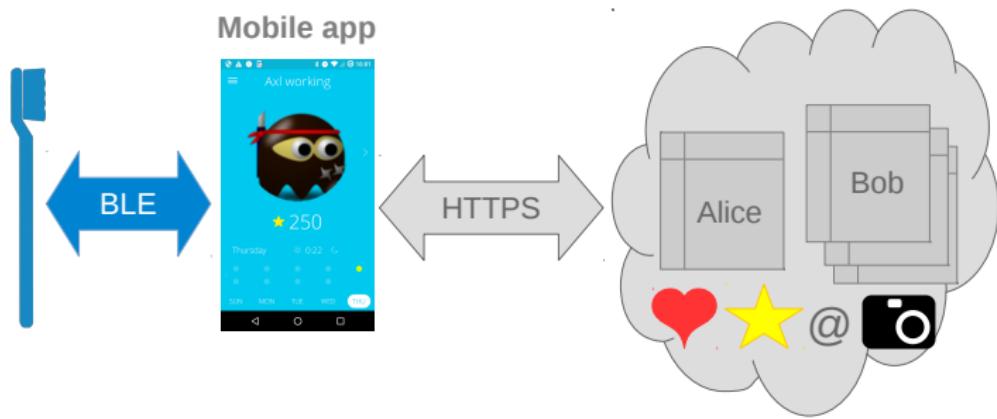
# A Fake Toothbrush: Is that useful?

- To brush your teeth? **No** ;-)
- To test / understand / fuzz the **cloud**, **Yes** ;-)

Introduction  
How it works  
Virtual toothbrush  
**Smart Toothbrush Cloud**  
Conclusion



# Smart Toothbrush Cloud



**Smart toothbrush**  
Does not know about  
hearts, game level,  
brushing score etc.

**Dental insurance**  
Remote service

# Security Issues

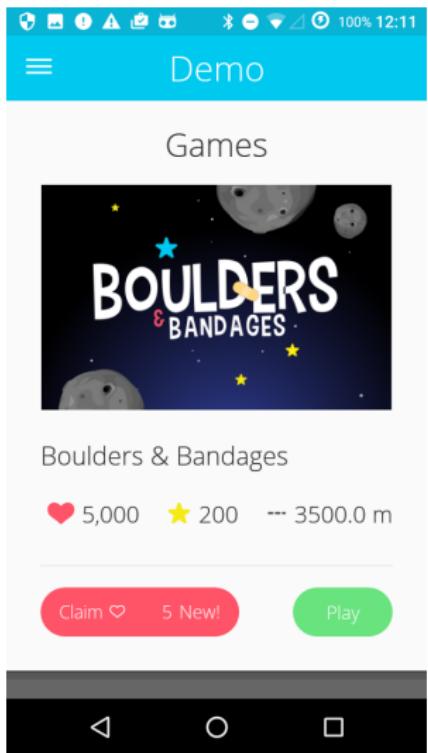
- ① Monetize virtual rewards - or fool your parents
- ② Insurance fraud
- ③ Massive privacy leak

No live demo, sorry

# Hack hearts, stars and game distance



# Hack hearts, stars and game distance

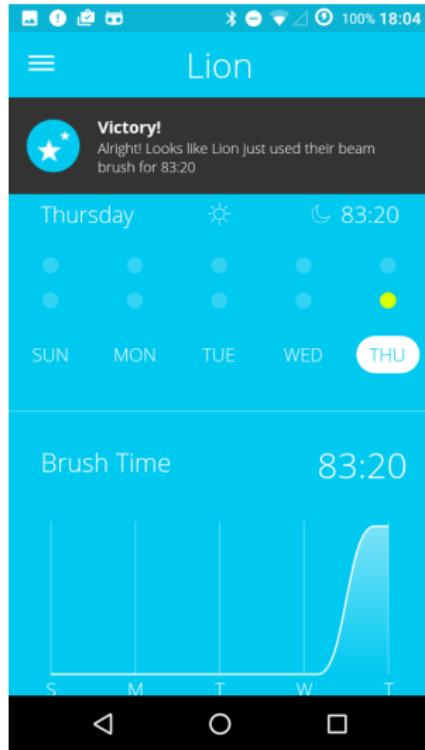


Monetizing history (video games, fitness etc)

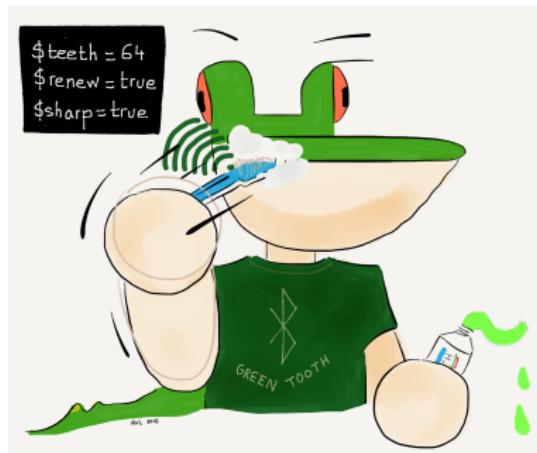
*"Reports show that users are quick to shell out money for VIP status, virtual items..." see source*

*"Developers should be aware that, depending on the features they include, an in-app virtual currency may be regulated in the same way as bitcoin under interpretations of U.S. anti-money laundering laws first announced in 2013 by the Financial Crimes Enforcement Network (FinCEN). " see article*

# I brushed my teeth for 5000 seconds



That's **83 minutes 20 secondes**  
No, I did not. But cloud does not know.



# What for? Insurance fraud!

It's easy — the better you brush  
the less you pay

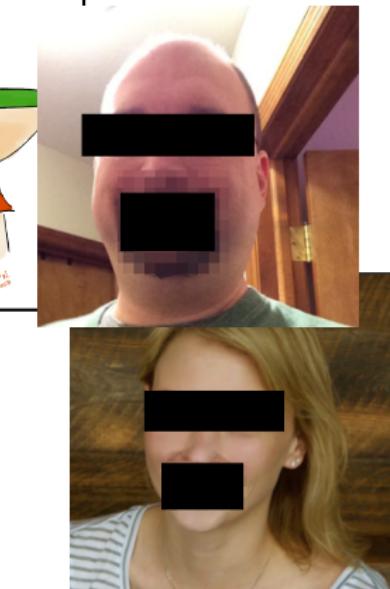


Screenshot of January 2018

# Full public access to customer database

Let's respect their privacy

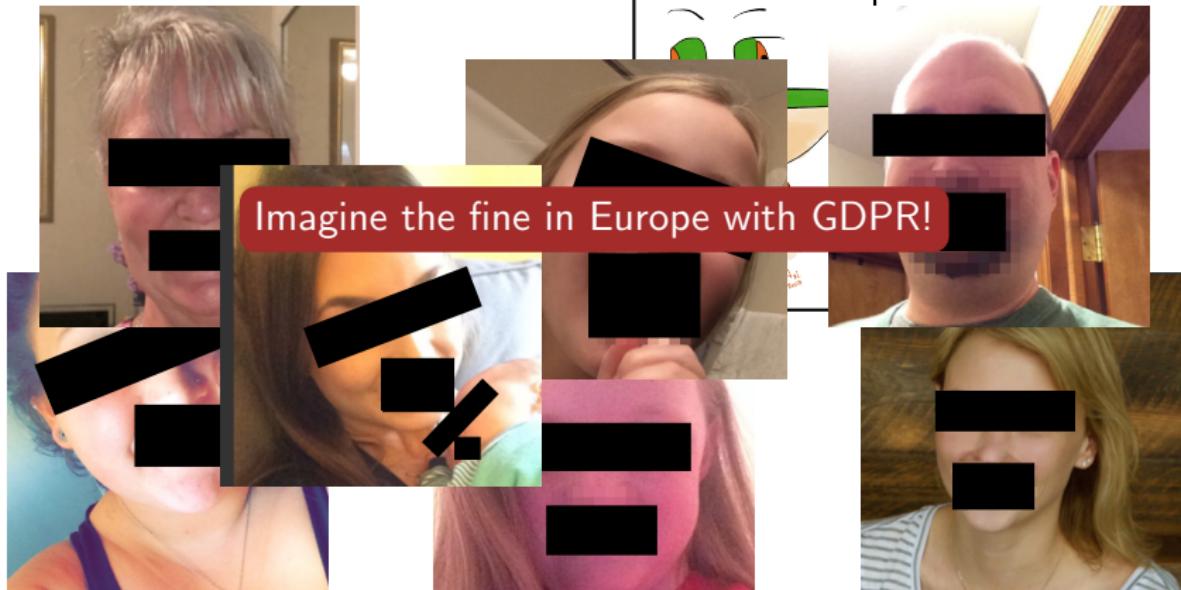
**No picture, no tweet (etc) PLEASE!**



# Full public access to customer database

Let's respect their privacy

**No picture, no tweet (etc) PLEASE!**



# Full public access to customer database

Let's respect their privacy

**No picture, no tweet (etc) PLEASE!**



## Introduction

## How it works

## Virtual toothbrush

## Smart Toothbrush Cloud

## Conclusion



# Conclusion

- ① Gained **independance** from mobile app and cloud

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**
- ⑤ **Monetize rewards**

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**
- ⑤ **Monetize rewards**
- ⑥ **Track** you during your travels (you take your toothbrush with you, don't you?)

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**
- ⑤ **Monetize rewards**
- ⑥ **Track** you during your travels (you take your toothbrush with you, don't you?)
- ⑦ Get **full profile** data of customers, including kids

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**
- ⑤ **Monetize rewards**
- ⑥ **Track** you during your travels (you take your toothbrush with you, don't you?)
- ⑦ Get **full profile** data of customers, including kids
- ⑧ IoT vulnerability reporting is absolutely **immature**

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**
- ⑤ **Monetize rewards**
- ⑥ **Track** you during your travels (you take your toothbrush with you, don't you?)
- ⑦ Get **full profile** data of customers, including kids
- ⑧ IoT vulnerability reporting is absolutely **immature**

With a **toothbrush!**

# Conclusion

- ① Gained **independance** from mobile app and cloud
- ② Had lots of **fun**
- ③ Fool mom and dad with **fake brushing score**
- ④ Insurance **fraud**
- ⑤ **Monetize rewards**
- ⑥ **Track** you during your travels (you take your toothbrush with you, don't you?)
- ⑦ Get **full profile** data of customers, including kids
- ⑧ IoT vulnerability reporting is absolutely **immature**

With a **toothbrush!**

**All connected devices need to be secured**

*Do not under-estimate creativity of attackers!*

Questions?

# Thanks

aapvrille (at) fortinet (dot) com - @cryptax



**PhOwn smart devices CTF**

December 14, 2018

<https://phOwn.org>