

# 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.**

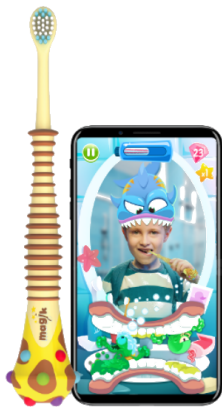
# Smart toothbrushes?

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

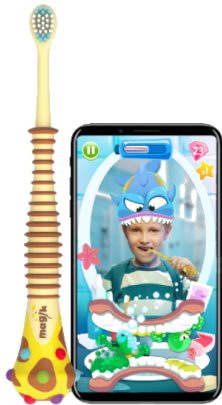
# Smart toothbrushes?

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

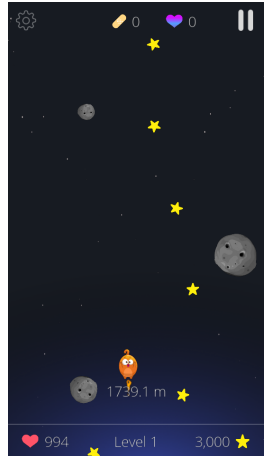
Photo credits: Kolibree



For this talk

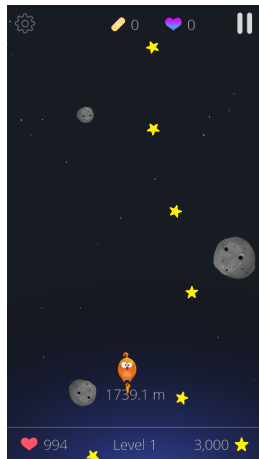
# What for?

- 1 Motivate and educate kids



# What for?

- 1 Motivate and educate kids
- 2 And adults



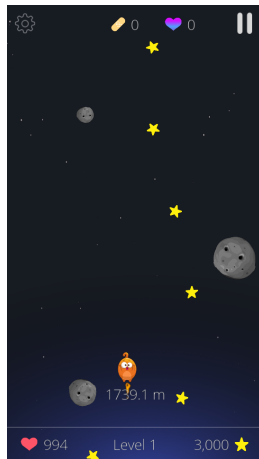
## Health improvements?

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**





Introduction

How it works

Virtual toothbrush

Smart Toothbrush Cloud

Conclusion

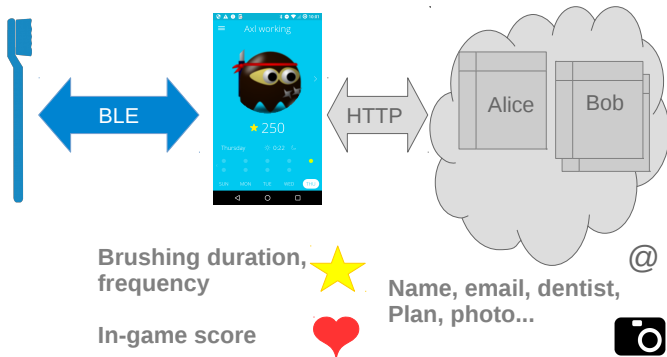


# Connecting the toothbrush

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

...

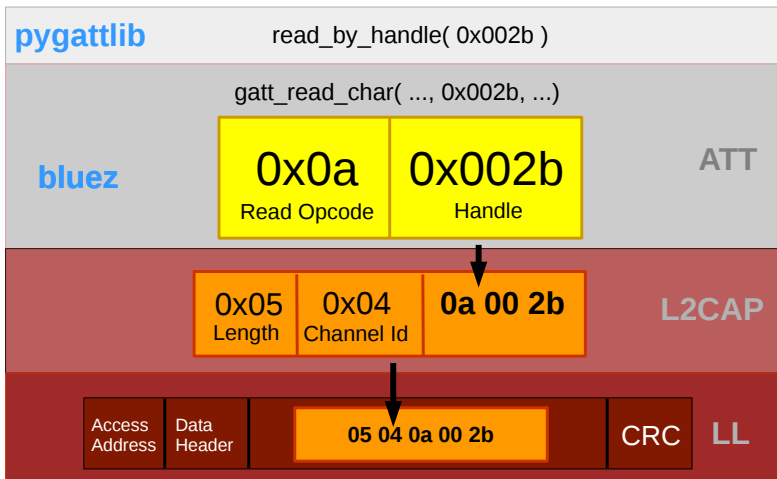
An attribute consists of:

- **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...



# How to capture BLE

Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
2982	2.791757	Master	Slave	ATT	34	Rcvd Read Request, Handle: 0x0010
2988	2.790367	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
2990	2.791766	Slave	Master	ATT	35	Rcvd Read Response
3077	2.853965	Master	Slave	ATT	34	Rcvd Write Request, Handle: 0x002b
3080	2.856068	Slave	Master	ATT	31	Rcvd Write Response
3171	2.921471	Master	Slave	ATT	33	Rcvd Read Request, Handle: 0x001d
3174	2.923848	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3176	2.925272	Slave	Master	ATT	35	Rcvd Read Response
3228	2.963022	Master	Slave	ATT	34	Rcvd Write Request, Handle: 0x002d
3231	2.965297	Slave	Master	ATT	31	Rcvd Write Response
3354	3.053512	Master	Slave	ATT	33	Rcvd Read Request, Handle: 0x001d
3357	3.055684	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3359	3.057389	Slave	Master	ATT	35	Rcvd Read Response
3535	3.183798	Master	Slave	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3538	3.186147	Slave	Master	ATT	35	Rcvd Read Response
3540	3.187499	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3709	3.308494	Master	Slave	ATT	33	Rcvd Read Request, Handle: 0x001d
3712	3.310994	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3714	3.312271	Slave	Master	ATT	35	Rcvd Read Response
3890	3.435569	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3891	3.436556	Master	Slave	ATT	33	Rcvd Read Request, Handle: 0x001d
3906	3.447568	Slave	Master	ATT	34	Rcvd Handle Value Notification, Handle: 0x0020
3908	3.449074	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
3910	3.450472	Slave	Master	ATT	35	Rcvd Read Response
3996	3.511180	Slave	Master	ATT	34	Rcvd Handle Value Notification, Handle: 0x003e
3998	3.513025	Slave	Master	ATT	37	Rcvd Handle Value Notification, Handle: 0x001d
4000	3.514538	Slave	Master	ATT	34	Rcvd Handle Value Notification, Handle: 0x0020
4006	3.519250	Slave	Master	ATT	34	Rcvd Handle Value Notification, Handle: 0x003e

Filter:  Expression... Clear Apply Save

Frame 3077: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on interface 0

Ethernet II, Src: Realtek USB (80:00:00:02:00:00), Dst: Realtek USB (80:00:00:02:00:00)

Nordic BLE sniffer meta

Bluetooth Low Energy Link Layer

Access Address: 0xb895505e

Data Header: 0x0802

CRC: 0x0f564e

Bluetooth L2CAP Protocol

Length: 4

CID: Attribute Protocol (0x0004)

Bluetooth Attribute Protocol


Opcode: Write Request (0x12)

Handle: 0x002b

Value: d0

Write Request on handle 0x2b with value 0xd0

Bluefruit LE Sniffer



0000 bb 06 1b 01 d2 18 06 0a 03 1d 42 a1 05 38 bd 00 .....B..B..

0010 00 5e 58 95 b8 02 08 04 00 04 00 12 2b 00 d0 f0 ..X.....L..

0020 6a 72 jr

# BLE Tools

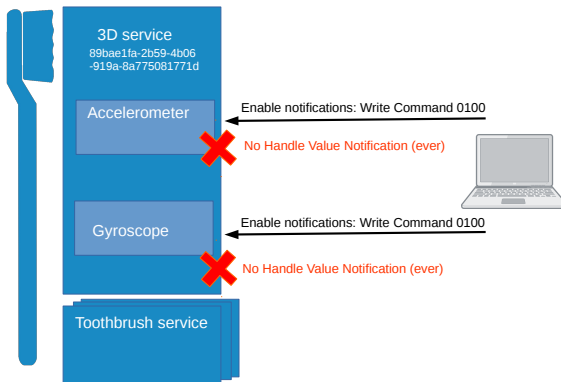
- Adafruit Bluefruit sniffer  
<https://www.adafruit.com/product/2269> (25\$),  
Ubertooth  
<https://github.com/greatscottgadgets/ubertooth>
- Adafruit Python BLE Sniffer [https://github.com/adafruit/Adafruit\\_BLESniffer\\_Python](https://github.com/adafruit/Adafruit_BLESniffer_Python)
- Bluez <http://www.bluez.org/>: 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

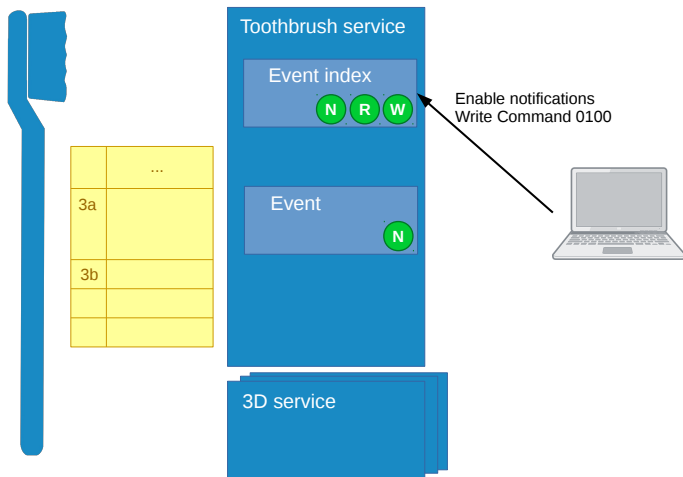
# Quadrant buzz is ... a timer



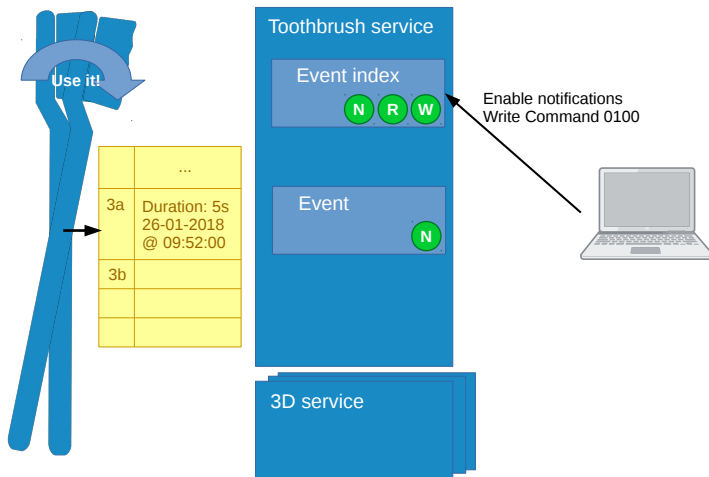
**Gyroscope and accelerometer are not used** in this version  
The toothbrush cannot know which teeth we brush



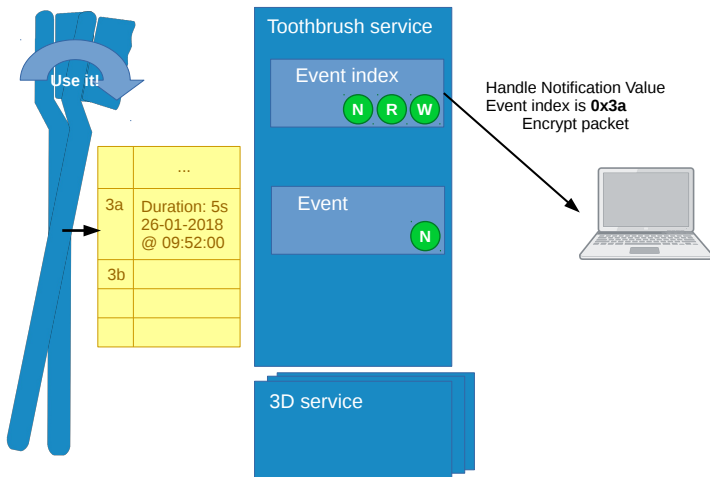
# Hardware events



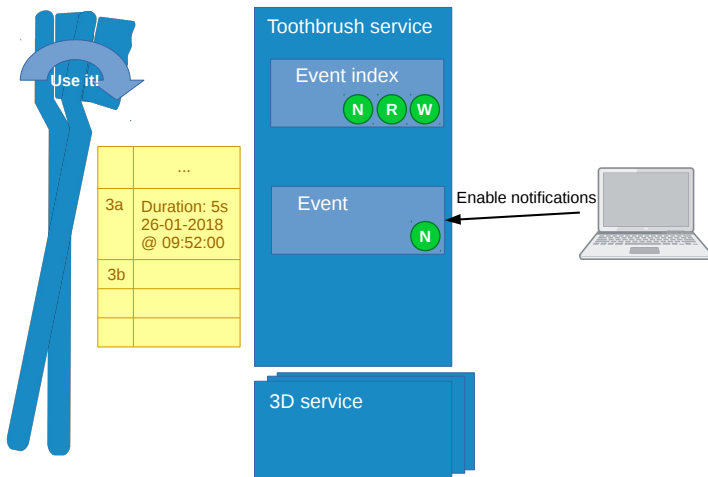
# Hardware events



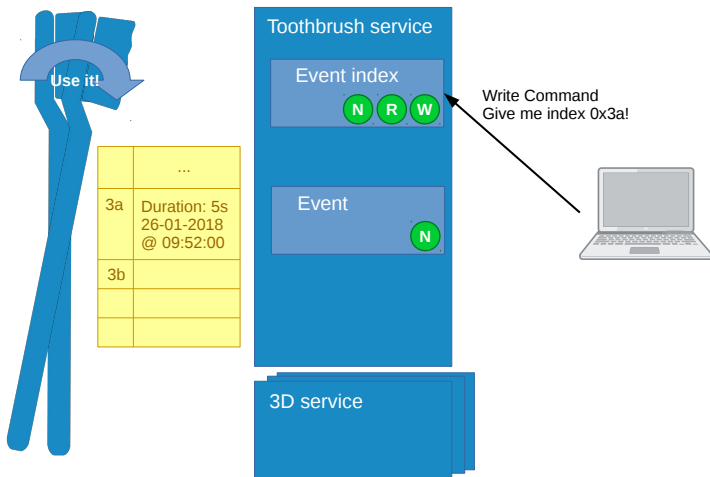
# Hardware events



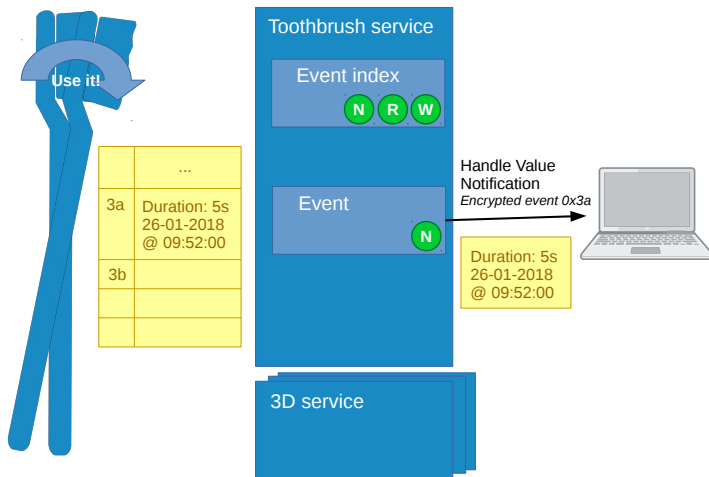
# Hardware events



# Hardware events



# Hardware events

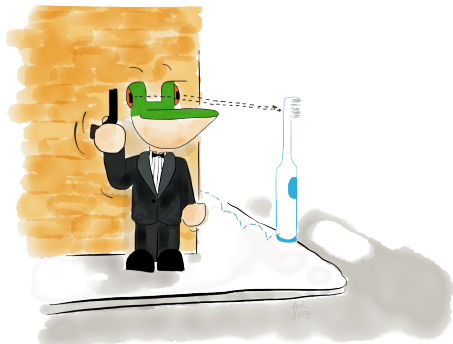


# DEMO

- 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?

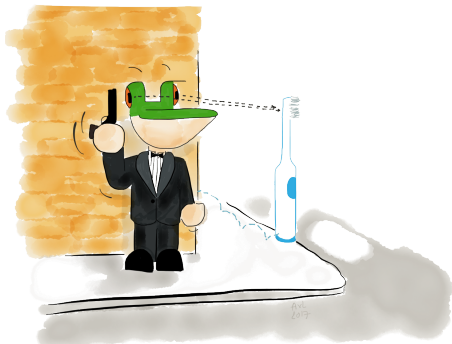
- Not many at this point. (But lots of fun).





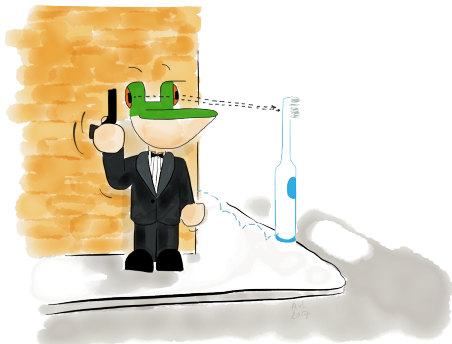
# Interesting attacks for cyber-criminals?

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



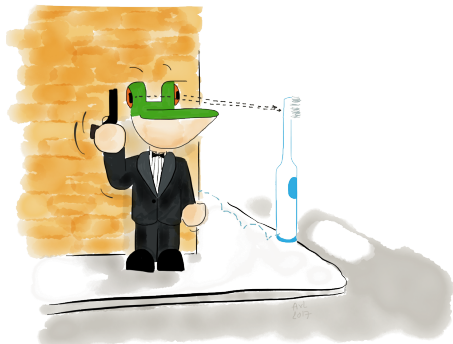
# Interesting attacks for cyber-criminals?

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



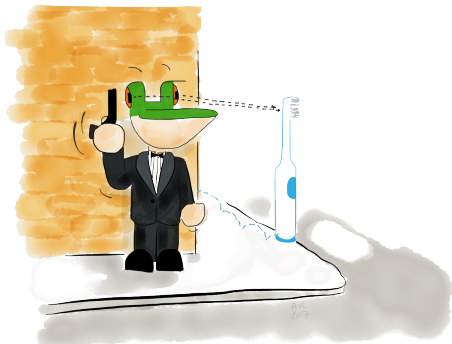
# Interesting attacks for cyber-criminals?

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



# Interesting attacks for cyber-criminals?

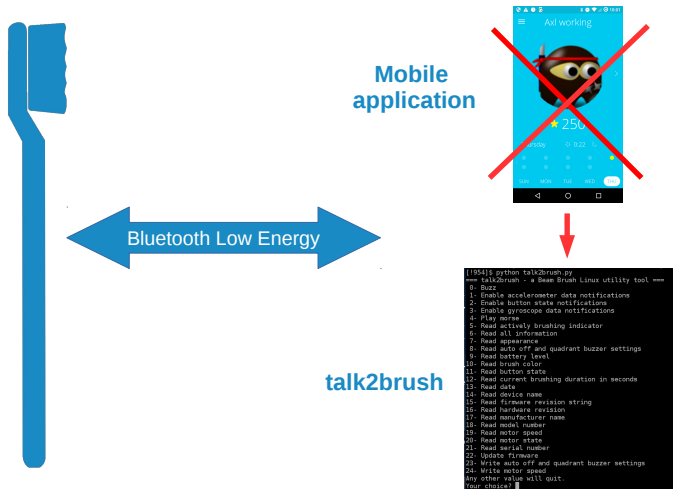
- Not many at this point. (But lots of fun).
- Damage victim's teeth and gums with high **motor speed**? Hmm.
- Remote **kill** of toothbrush. Okaaaay.
- Do you mind if we **track** you? Toothbrush MAC address is fixed (despite specs say how to do it)
- But we'll see bad design leads to worse later.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



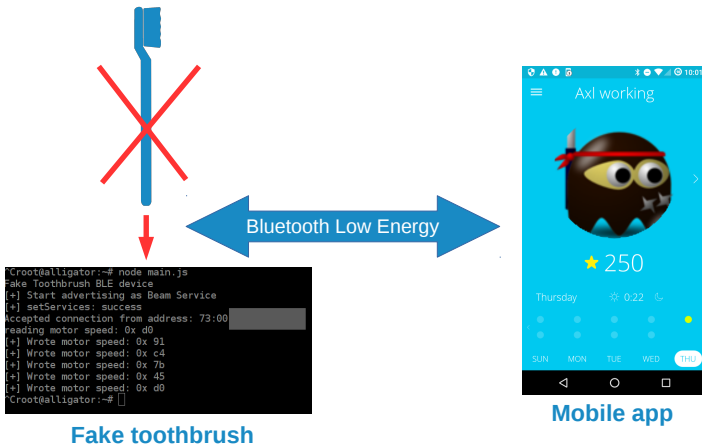
Introduction  
How it works  
Virtual toothbrush  
Smart Toothbrush Cloud  
Conclusion



# Summary / Achievements



# Can we create a fake toothbrush?

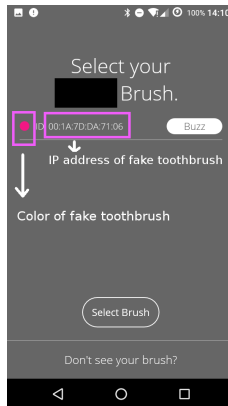


Yes, we can!

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', 'utf8'))
}
```

# A Fake Toothbrush: Is that useful?

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

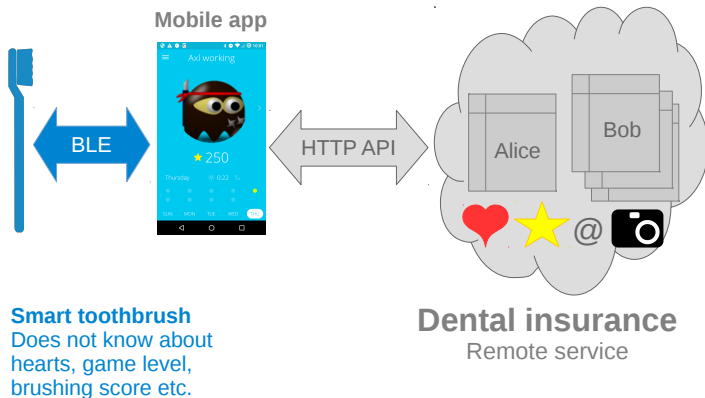
# A Fake Toothbrush: Is that useful?

- 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

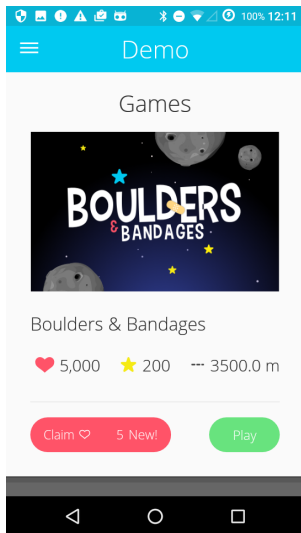


# Security Issues

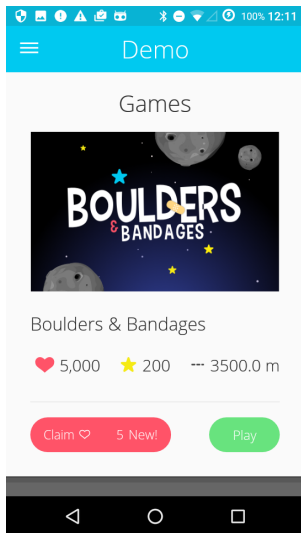
- ① Monetize virtual rewards - or fool your parents
- ② Insurance fraud
- ③ Massive privacy leak

No live demo, sorry

# Hack hearts, stars and game distance



# Hack hearts, stars and game distance



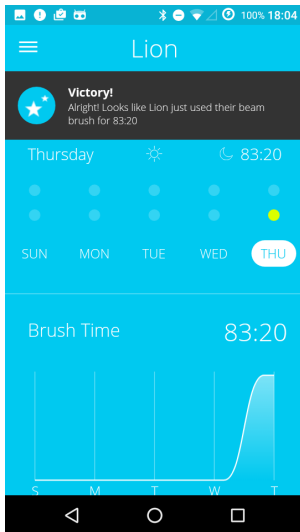
## Monetizing history (video games, fitness etc)

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

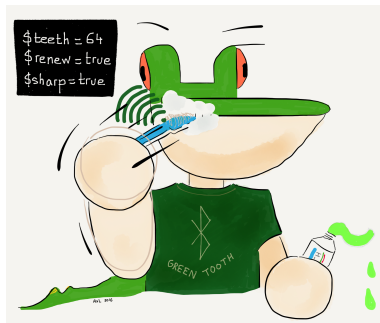
*"Developers should be aware that, depending on the features they include, an in-app virtual currency may be regulated in the same way as bitcoin under interpretations of U.S. anti-money laundering laws first announced in 2013 by the Financial Crimes Enforcement Network (FinCEN)."* [see article](#)



# I brushed my teeth for 5000 seconds



That's **83 minutes 20 seconds**  
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



**Ph0wn smart devices CTF**

December 14, 2018

<https://ph0wn.org>