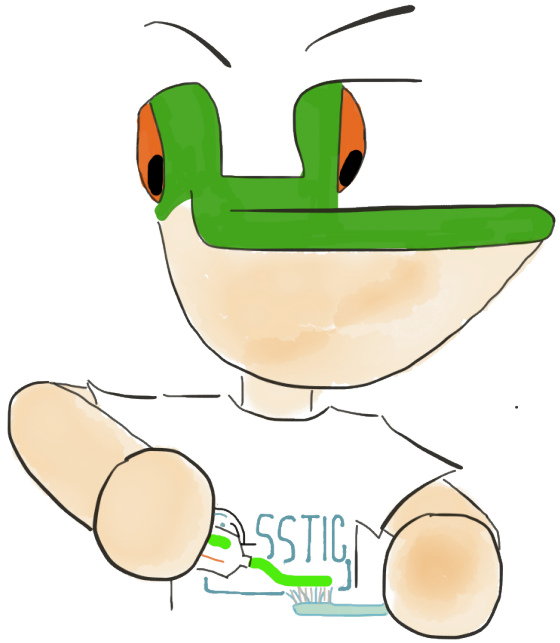
Ingénierie inverse d'une brosse à dents connectée

Axelle Apvrille - Fortinet
aapvrille@fortinet.com

SSTIC, Juin 2017

Outline



Qui suis-je ?

Chercheur anti-virus chez **Fortinet**
smart phone,
smart *things*

Salut ! Moi, je suis **Pico**, un crocodile
qui la ramène beaucoup - @picolecroco

Pourquoi étudier une brosse à dents ?

1. Parce que c'est **rigolo**

Pourquoi étudier une brosse à dents ?

1. Parce que c'est **rigolo**
2. Parce que c'est **difficile**

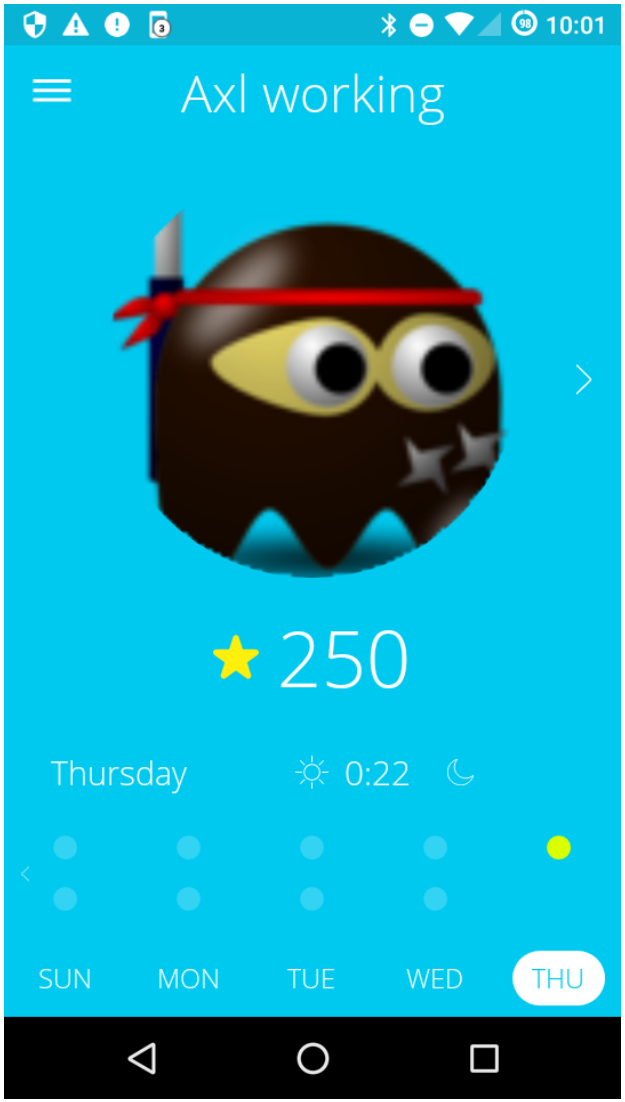
Pourquoi étudier une brosse à dents ?

1. Parce que c'est **rigolo**
2. Parce que c'est **difficile**
3. Si même une brosse à dents pose des problèmes, alors qu'en sera-t-il des systèmes plus complexes et plus critiques ? !

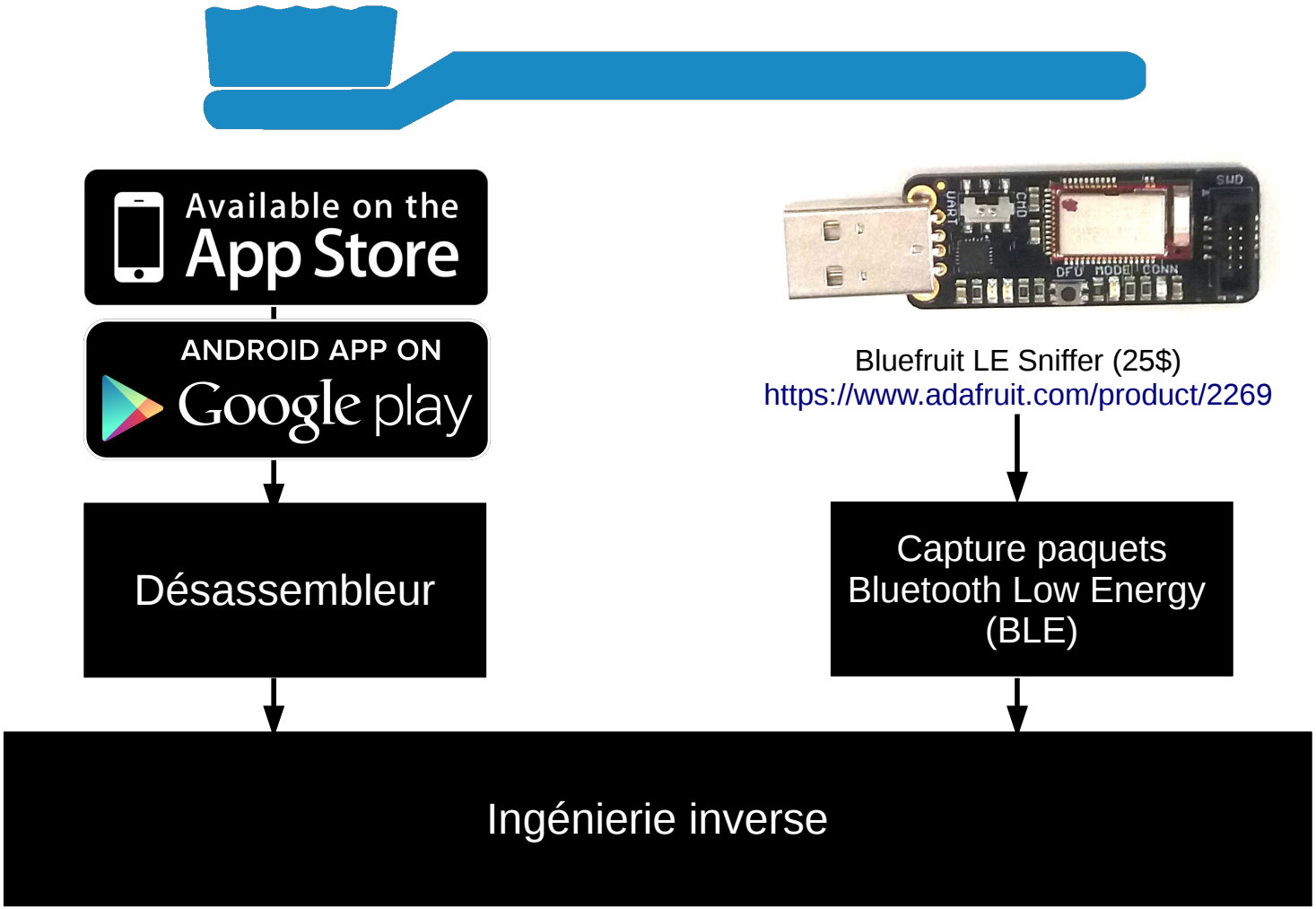
Présentation de la brosse à dents

Commercialisée par une *assurance dentaire* américaine

Application mobile



Rétro ingénierie de type boite noire

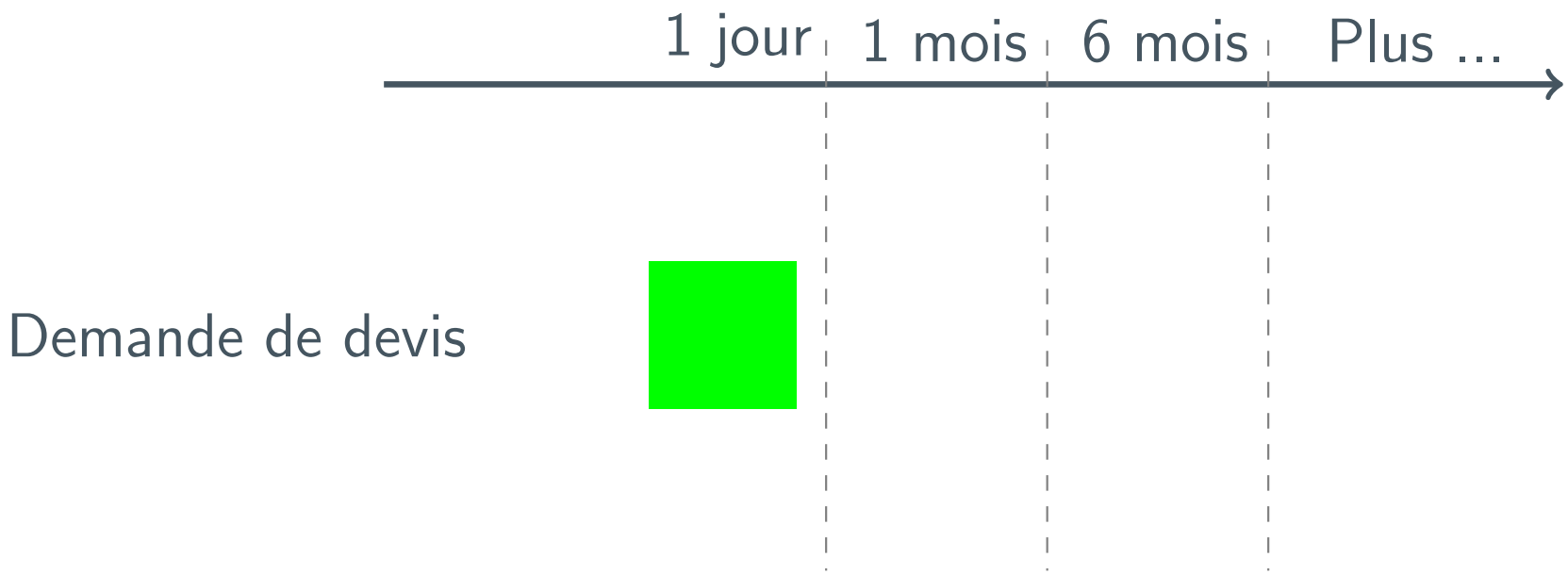


Temps de traitement des vulnérabilités

Quizz : combien de temps pour *répondre* à ...

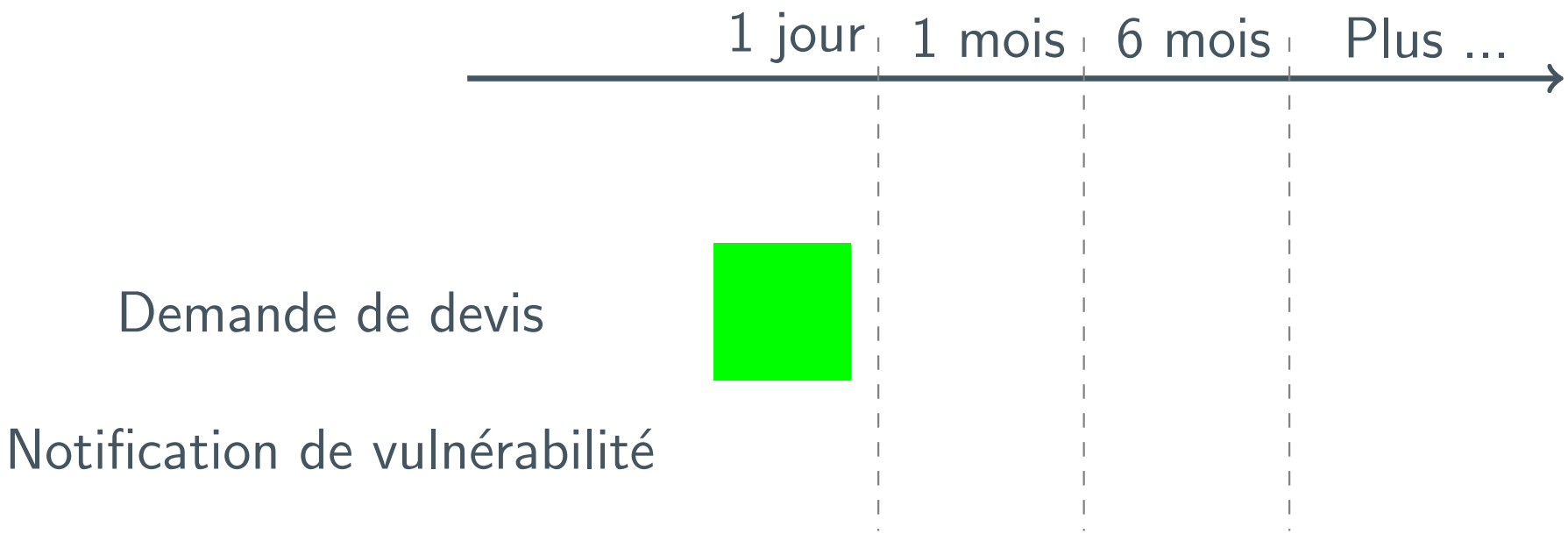
Temps de traitement des vulnérabilités

Quizz : combien de temps pour *répondre* à ...



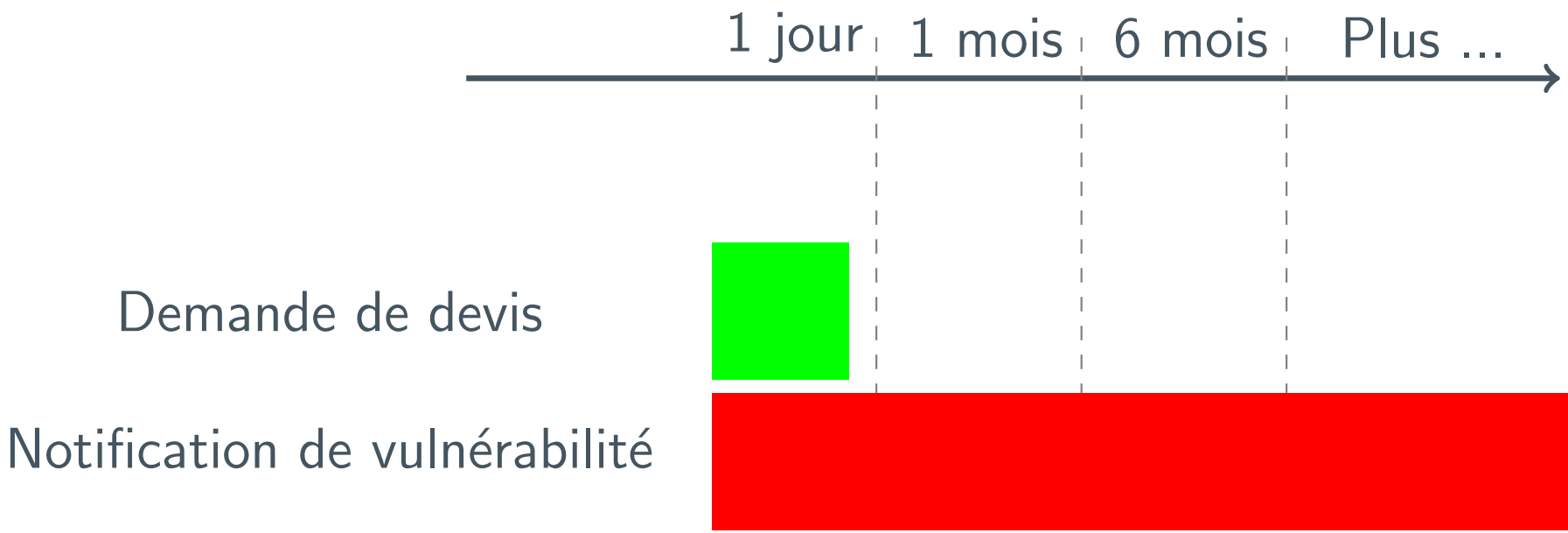
Temps de traitement des vulnérabilités

Quizz : combien de temps pour *répondre* à ...



Temps de traitement des vulnérabilités

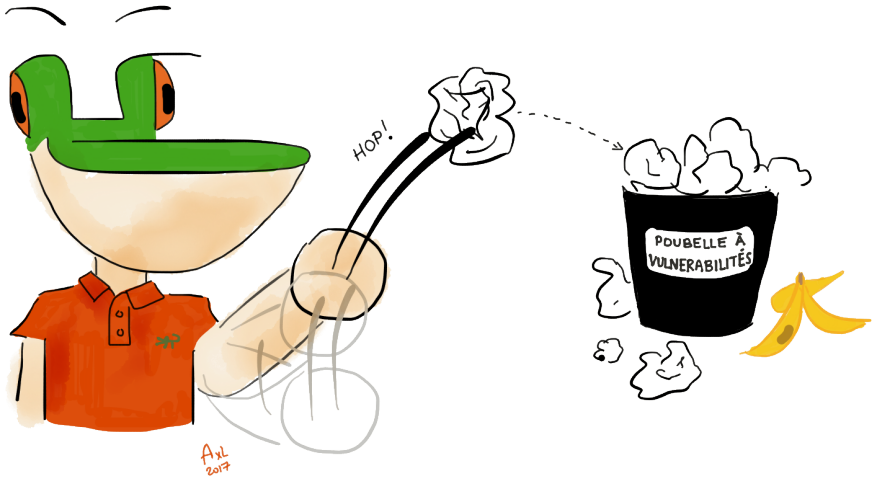
Quizz : combien de temps pour *répondre* à ...



Pourquoi ? Black list !

Solution

A la première notification de vulnérabilité, bannir l'email du chercheur...



Submit a request

Your email address *

[redacted]@fortinet.com

Requester [redacted] is suspended.

Subject *

Test

Description *

Test

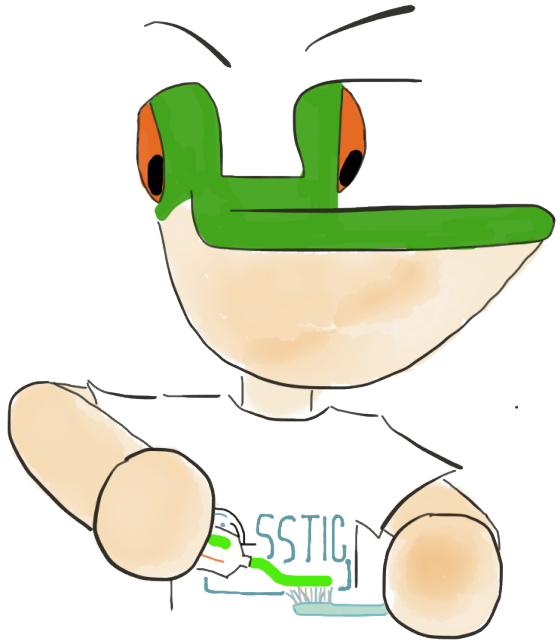
Please enter the details of your request. A member of our support staff will respond as soon as possible.

Attachments

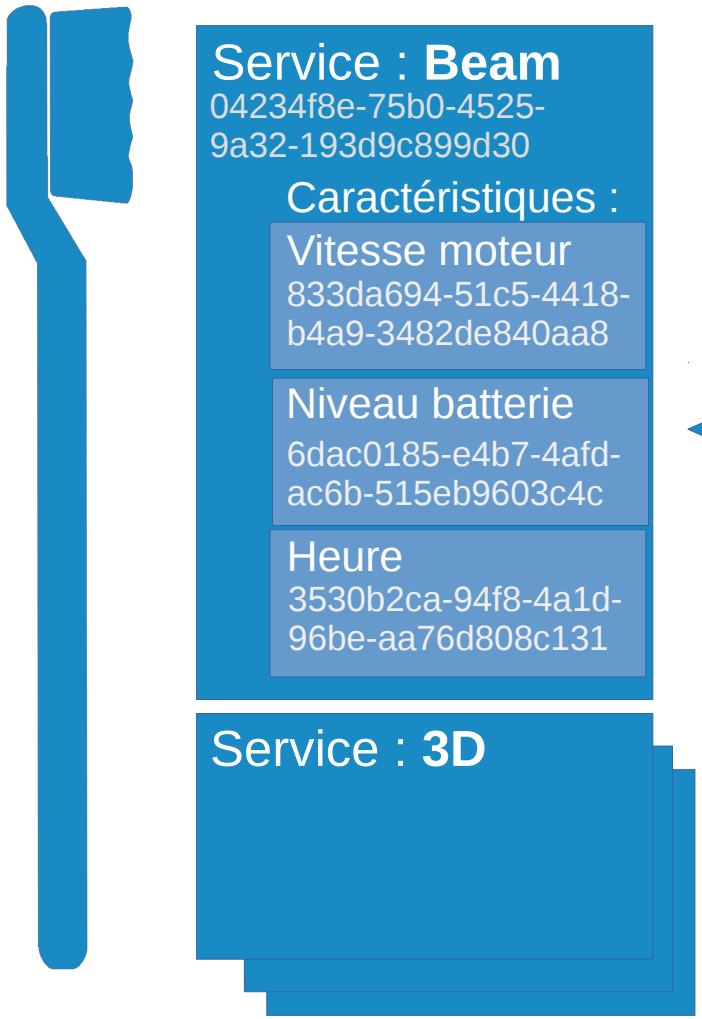
Add file or drop files here

Black-list de mon @ email

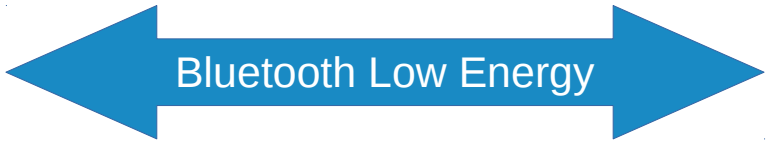
Outline



Un équipement **B**luetooth **L**ow **E**nergy



Pas d'appairage
Basse consommation
Portée 150m **max**



Etape 1 : à qui envoyer le paquet

Adresse MAC de la brosse à dents

```
$ sudo hcitool lescan
xx:xx:xx:xx:xx:xx Beam Brush
```

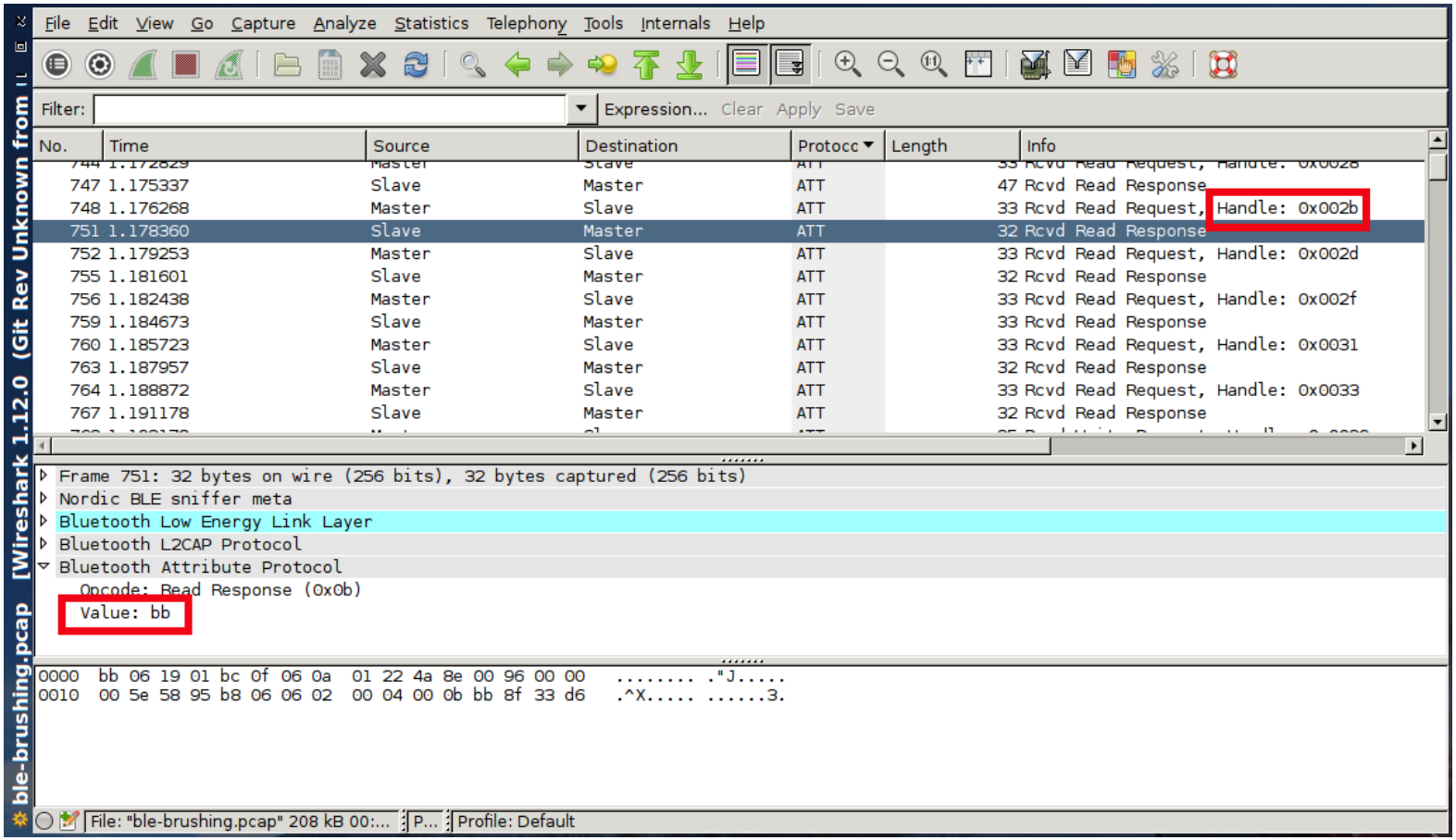
Identifiant du service (ex : Device Information)

```
$ sudo gatttool -b xx:xx:xx:xx:xx:xx -I
[   ][xx:xx:xx:xx:xx:xx][LE]> connect
[CON][xx:xx:xx:xx:xx:xx][LE]> primary
attr handle: 0x0001, end grp handle: 0x0005 uuid: 00001800-0000-1000-8000-
...
```

Identifiant ou *handle* de la caractéristique à contrôler

```
[CON][xx:xx:xx:xx:xx:xx][LE]> characteristics
handle: 0x0002, char properties: 0x02, char value handle: 0x0003, uuid: 00
handle: 0x0004, char properties: 0x02, char value handle: 0x0005, uuid: 00
...
```

Etape 2 : trouver quoi envoyer



La caractéristique de vitesse de moteur répond `0xbb`.
Ca veut dire quoi ?

Exemple : lire le niveau de la batterie

```
public static float getBatteryLevel(BluetoothGattCharacteristic charac){
  return ByteSerialize.somemax(ByteSerialize.a(1.1f,
    1.5f,
    (((float)(ByteSerialize.getUint16(charac, 0) >> 4))) * 0.001221f ,
    0f,
    1f));
}

private static float a(float arg2, float arg3, float arg4,
  float arg5, float arg6) {
  return (arg4 - arg2) / (arg3 - arg2) * (arg6 - arg5) + arg5;
}
```

Lire 16 bits, ôter 4 bits inutiles = 12 bits

Convertisseur analogique - digital sur 12 bits :
$0.001221 = 5V/2^{12}$

Talk2brush

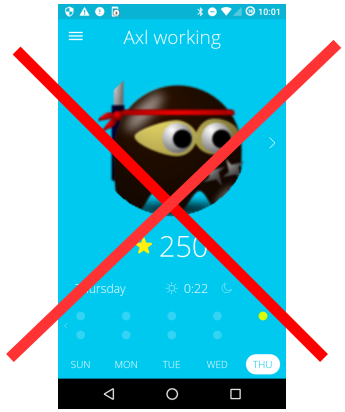
```
$ python talk2brush.py
=== talk2brush - a Beam Brush Linux utility tool ===
 0- Buzz
 1- Enable accelerometer data notifications
 2- Enable button state notifications
 3- Enable gyroscope data notifications
 4- Play morse
 5- Read actively brushing indicator
 6- Read all information
 7- Read appearance
 8- Read auto off and quadrant buzzer settings
 9- Read battery level
 ...
```

https://github.com/cryptax/beamtools

Résumé de la situation

Bluetooth Low Energy

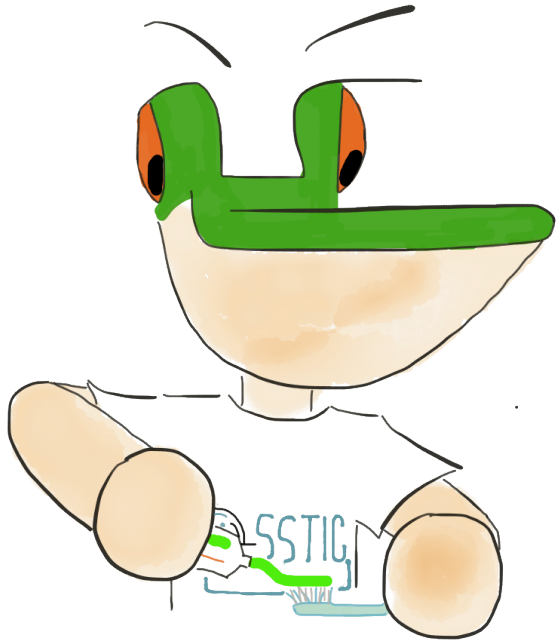
Application mobile officielle



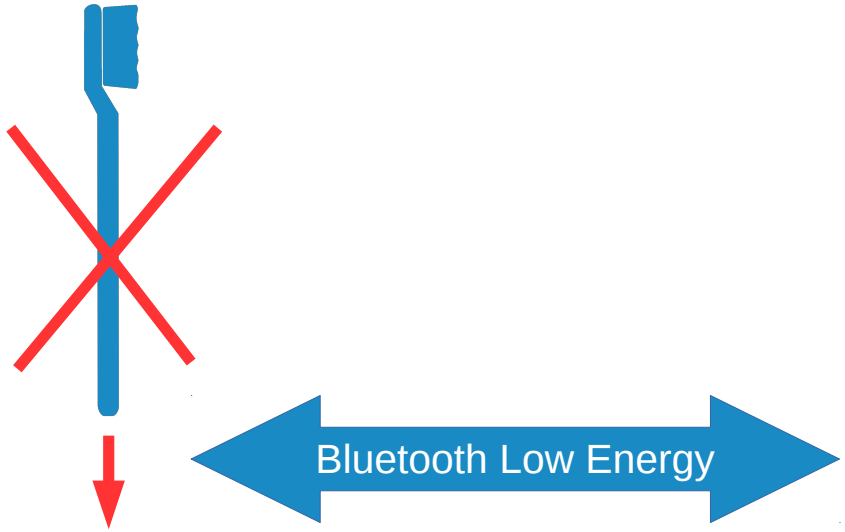
talk2brush

```
[!954]$ python talk2brush.py
=== 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- Play morse
 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 date
14- Read device name
15- Read firmware revision string
16- Read hardware revision
17- Read manufacturer name
18- Read model number
19- Read motor speed
20- Read motor state
21- Read serial number
22- Update firmware
23- Write auto off and quadrant buzzer settings
24- Write motor speed
Any other value will quit.
Your choice?
```

Outline

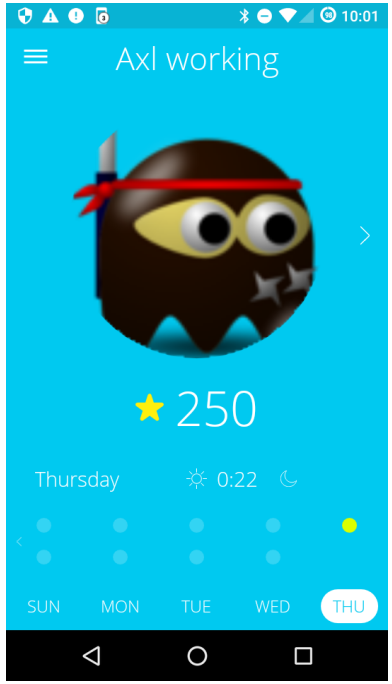


Se faire passer pour une brosse à dents ?




```
^Croot@alligator:~# node main.js
Fake Toothbrush BLE device
[+] Start advertising as Beam Service
[+] setServices: success
Accepted connection from address: 73:00
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:~#
```

Fausse brosse à dents



Application mobile officielle

Brosse à dents virtuelle : c'est possible !

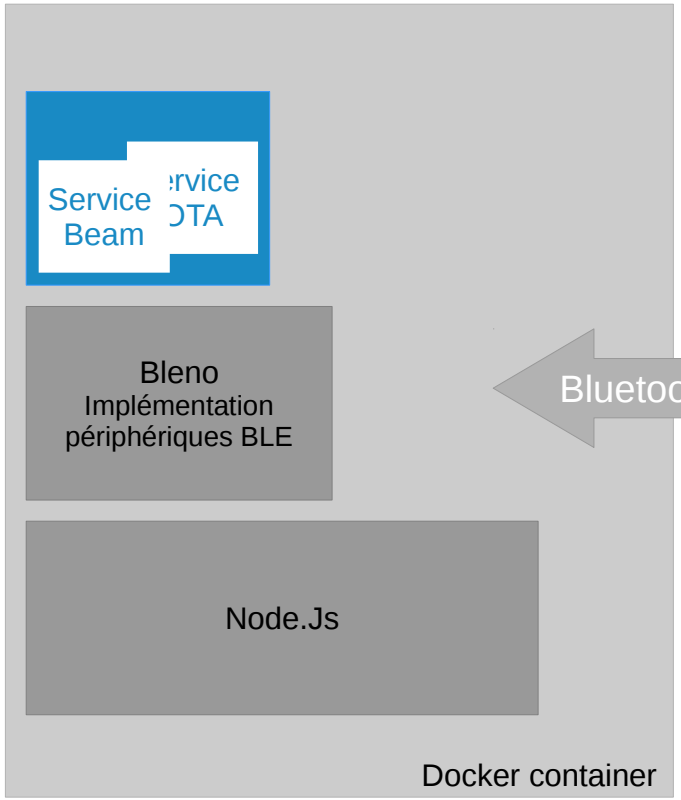
Je vous présente une brosse à dents

rose

König Micro Bluetooth Dongle v4.0 (13 euros)

Si, si, l'application officielle dit bien qu'elle est rose :)

Implémentation d'une fausse brosse à dents



Bluetooth Low Energy

Fausse brosse à dents

Application mobile officielle

Disponible sur https://github.com/cryptax/beamtools

Résumé : quels sont les problèmes ?

1. **Pas d'authentification**.

Résumé : quels sont les problèmes ?

1. **Pas d'authentification**.
2. **Pas de chiffrement** : paquets en clair. Ah pardon. Sauf dans les Brush Events. Qui utilise AES. Hum... AES **ECB** et clé codée en dur...

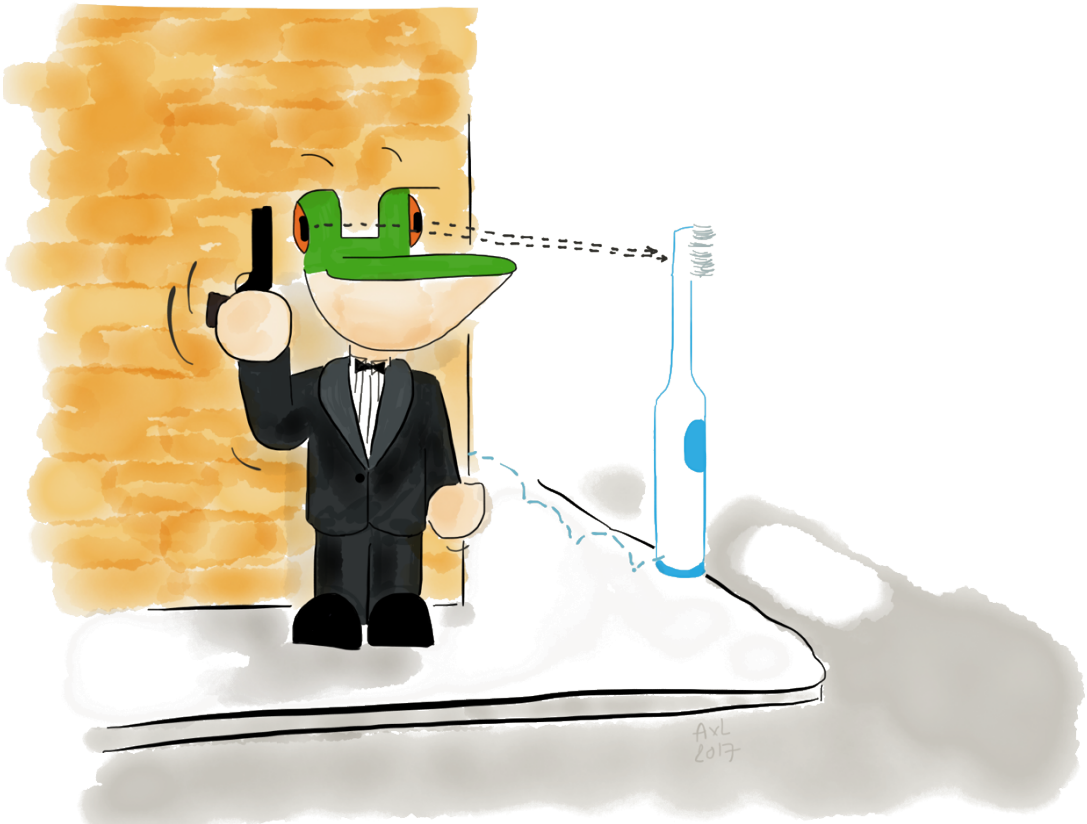
Résumé : quels sont les problèmes ?

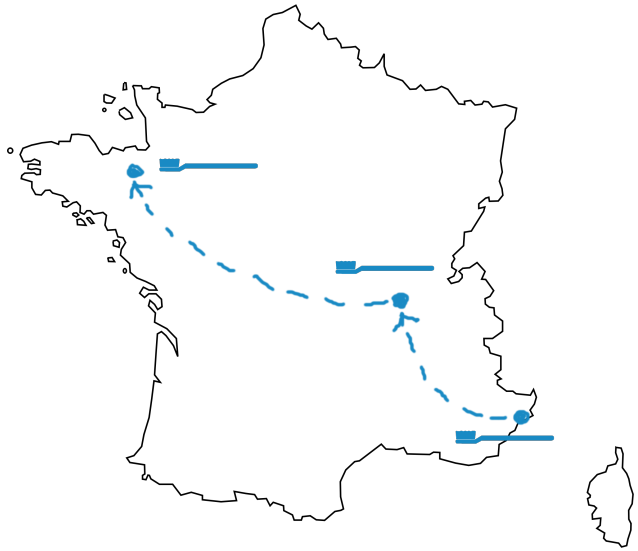
1. **Pas d'authentification**.
2. **Pas de chiffrement** : paquets en clair. Ah pardon. Sauf dans les Brush Events. Qui utilise AES. Hum... AES **ECB** et clé codée en dur...
3. Bref : **pas de sécurité**.

Dispositif de suivi peu onéreux, merci !

L'adresse MAC de la brosse à dents est toujours la même.

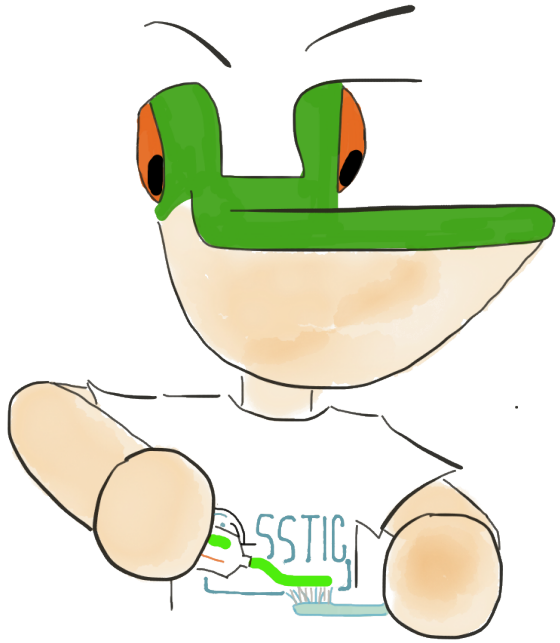
Même éteinte, elle émet ! Il faut enlever les piles !



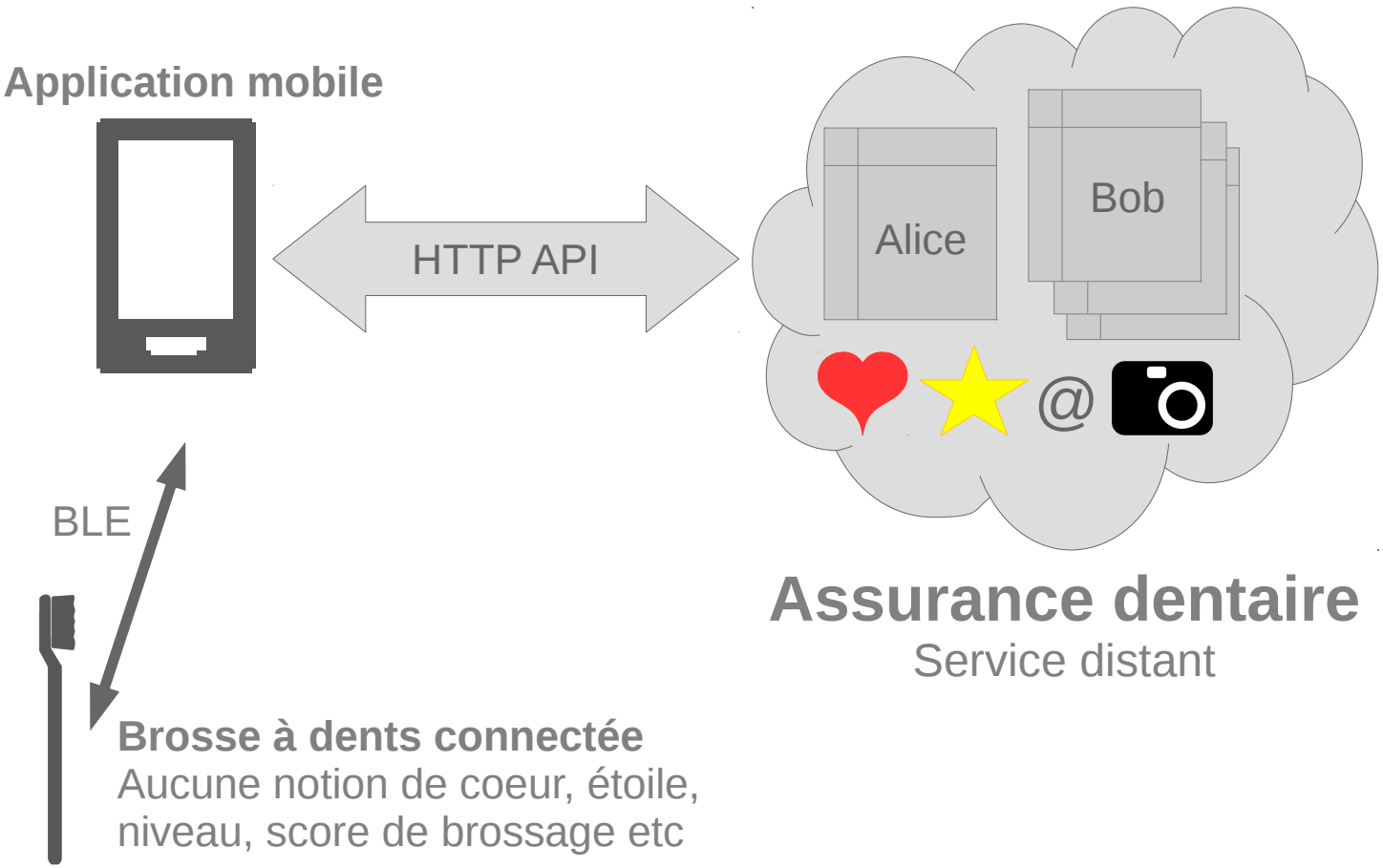


Le trajet de ma brosse à dents pour venir à SSTIC :)

Outline



Service distant : accès par HTTP API



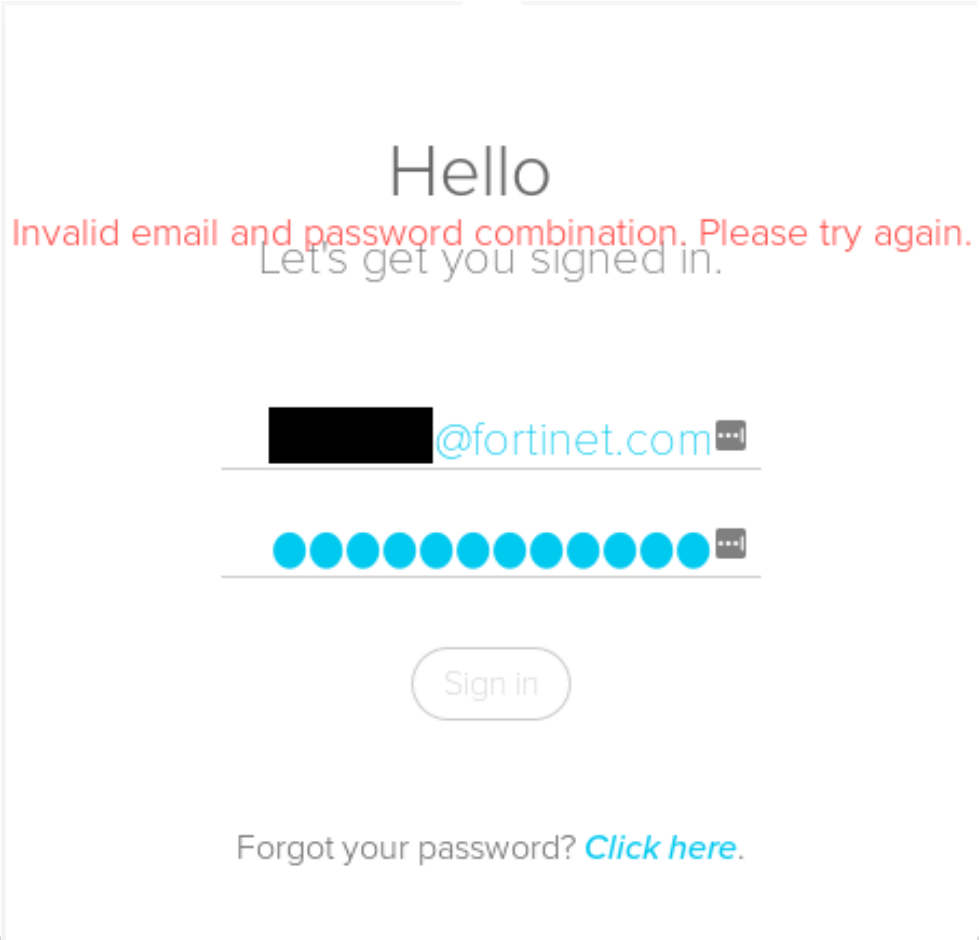
Comment une entreprise corrige-t-elle une vulnérabilité ?

Réponse :

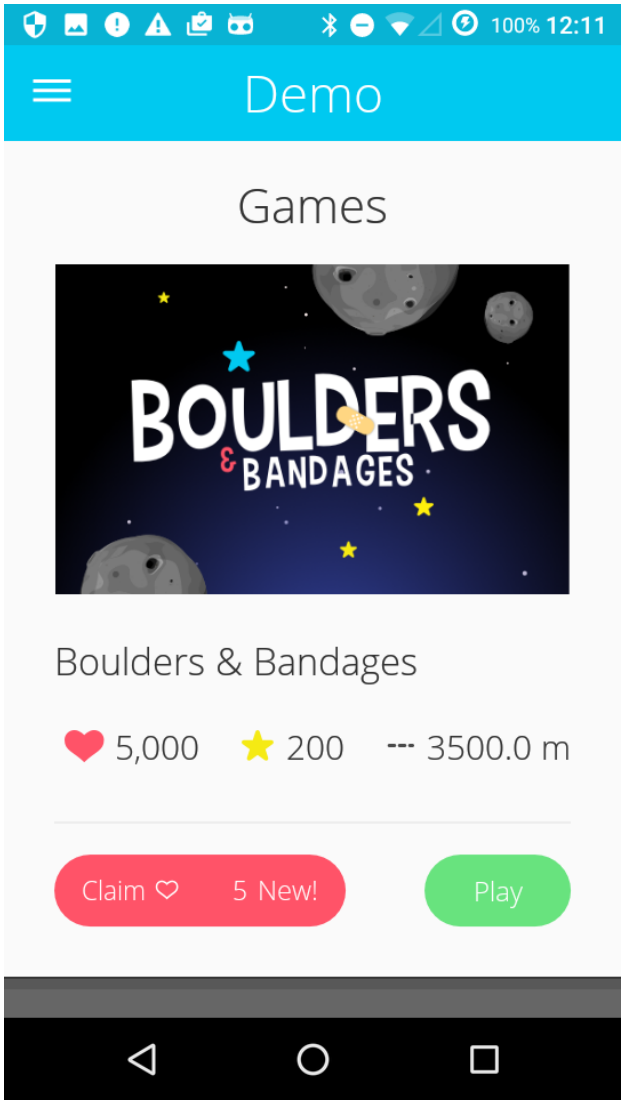
Comment une entreprise corrige-t-elle une vulnérabilité ?

Réponse :

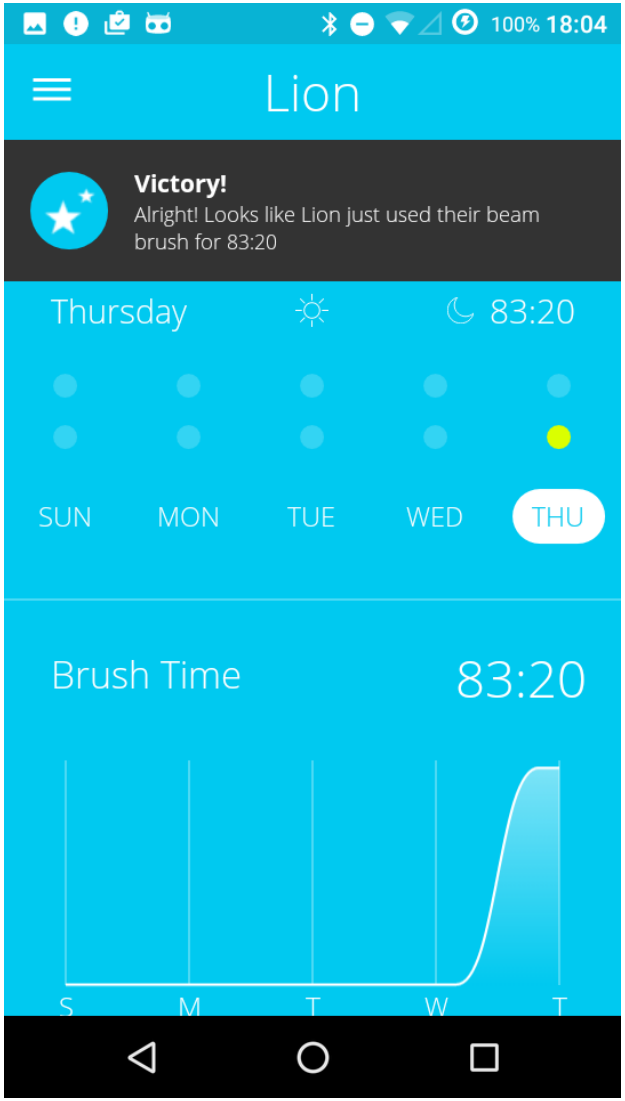
Elle **ferme le compte** de test du **chercheur**



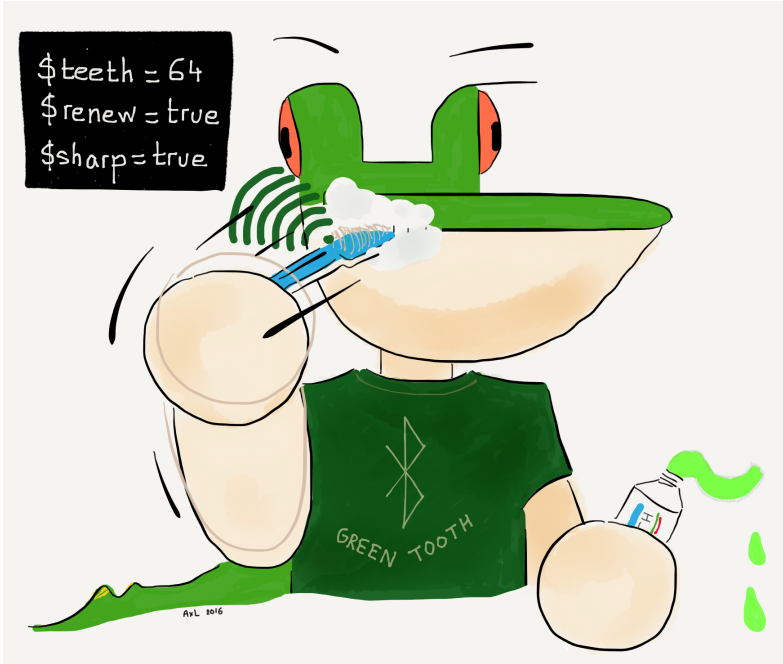
Modifier le nombre de coeurs, étoiles, distance



Se brosser les dents virtuellement



Je me suis brossé les dents pendant **83 minutes 20 secondes** = 5000 secondes ! :)



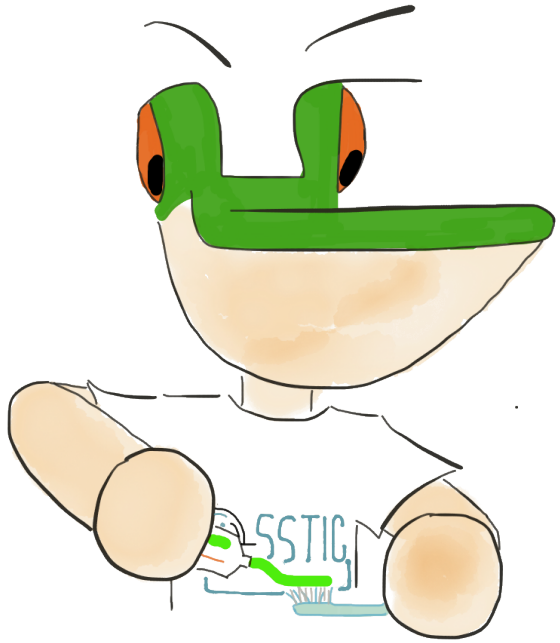
Quel intérêt ? Fraude à l'assurance !

Capture d'écran mai 2017

Accès à la base de données des clients

CENSORED - Leak of kid photos, emails, names...

Outline



Impacts d'une mauvaise sécurité

La brosse à dents, un objet sans intérêt pour un attaquant ?

Erreur !

Vous sous-estimez leur créativité ;)

1. Monétisation des coeurs, étoiles virtuels

Impacts d'une mauvaise sécurité

La brosse à dents, un objet sans intérêt pour un attaquant ?

Erreur !

Vous sous-estimez leur créativité ;)

1. Monétisation des coeurs, étoiles virtuels
2. Fraude à l'assurance

Impacts d'une mauvaise sécurité

La brosse à dents, un objet sans intérêt pour un attaquant ?

Erreur !

Vous sous-estimez leur créativité ;)

1. Monétisation des coeurs, étoiles virtuels
2. Fraude à l'assurance
3. Dispositif de suivi

Impacts d'une mauvaise sécurité

La brosse à dents, un objet sans intérêt pour un attaquant ?

Erreur !

Vous sous-estimez leur créativité ;)

1. Monétisation des coeurs, étoiles virtuels
2. Fraude à l'assurance
3. Dispositif de suivi
4. Récupération de photos d'enfants, emails, noms...

Que retenir ?

Chercheurs

Pas besoin de sortir le fer à souder ou la scie !

Vendeurs

Formation à la sécurité, embauches, pentests...

Utilisateurs

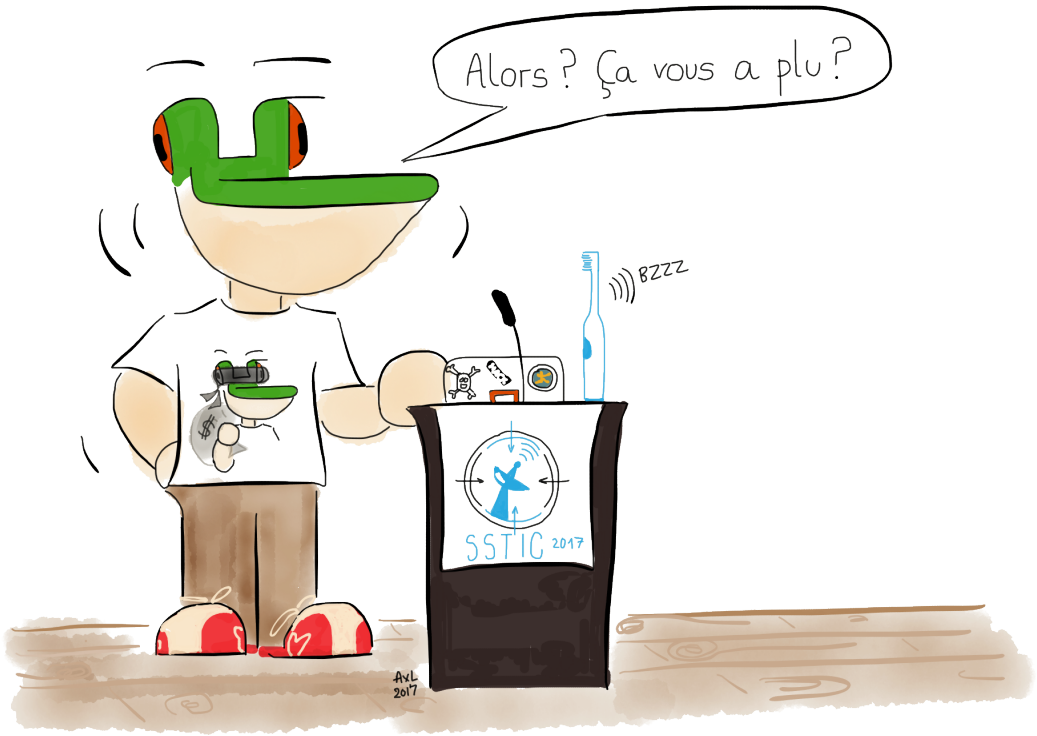
Stop aux idées préconçues

"Il n'y a aucun intérêt à attaquer l'objet"

"Ces données ne sont pas privées"

Merci de m'avoir écoutée !

eSAME **Ph0wn : CTF IoT**
30 novembre 2017 à **Sophia Antipolis**



aapvrille (at) fortinet (dot) com - @cryptax
http://github.com/cryptax/beamtools