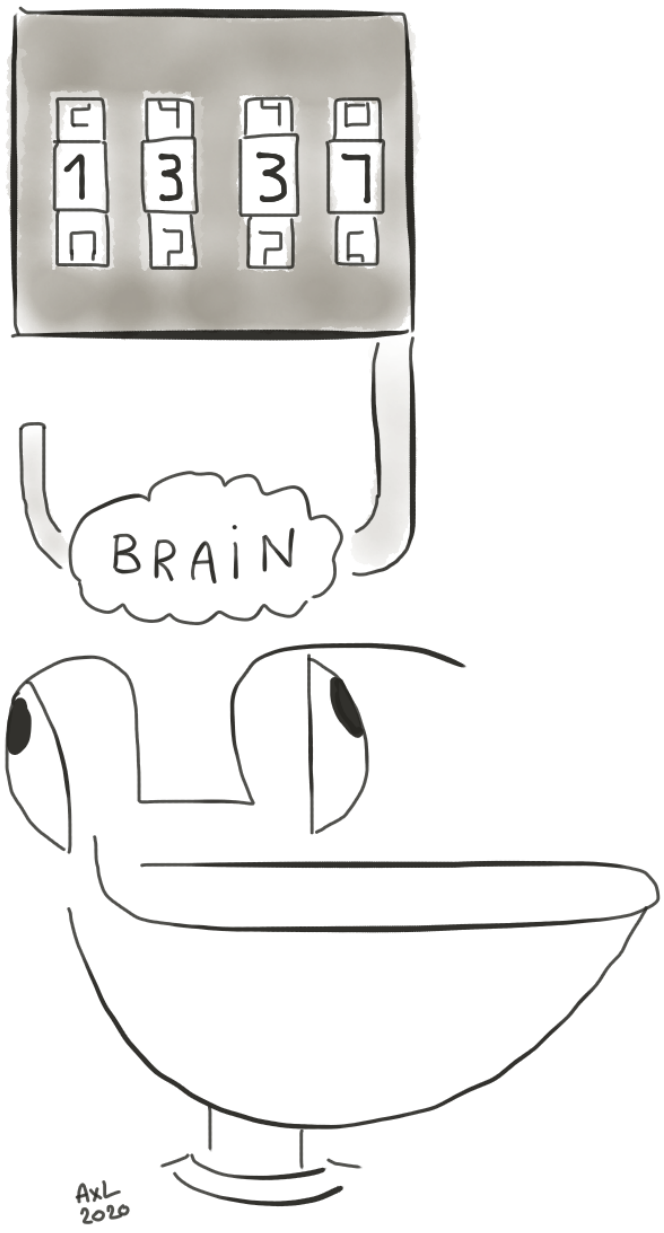


Hacking de capteur de glycémie connecté

Axelle Apvrille (Fortinet)
Travis Goodspeed

Unlock Your Brain
Harden Your System
UYBHYS

Novembre 2020

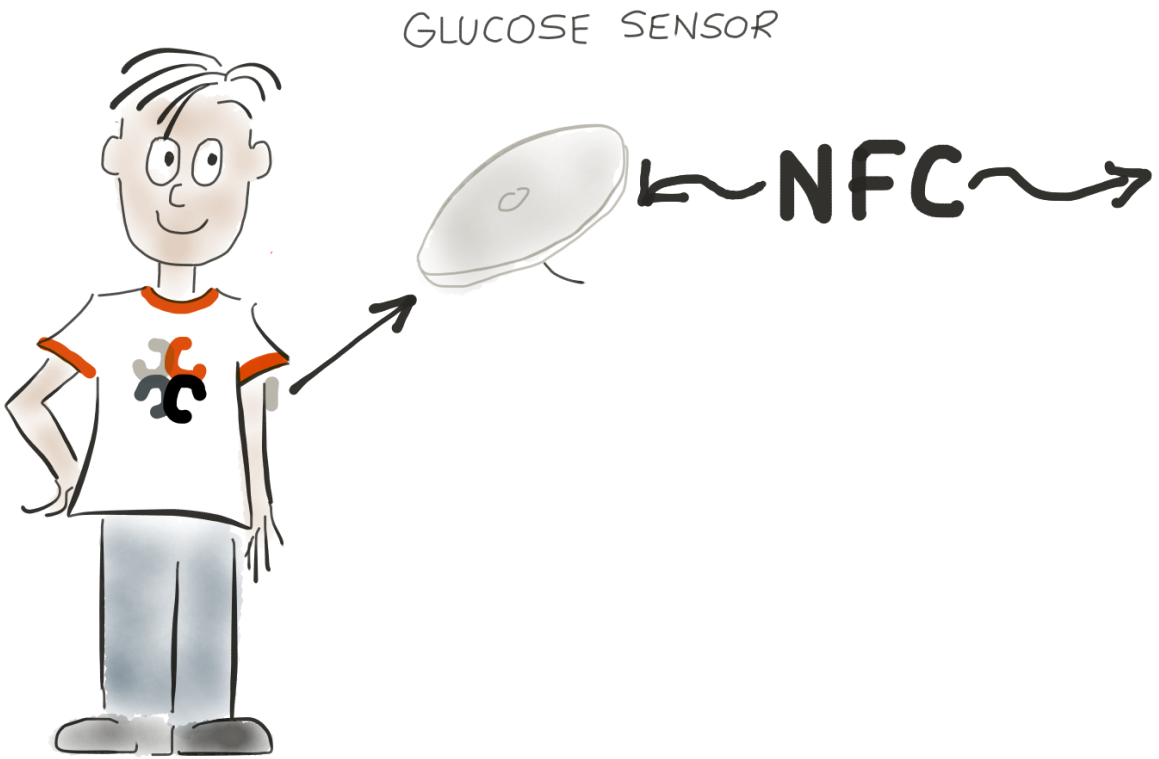
FORTINET®

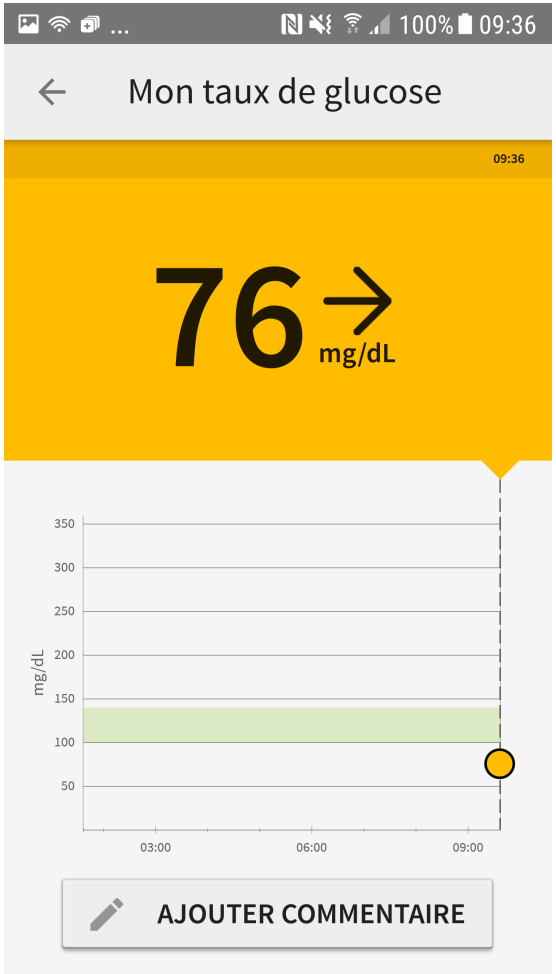
Bonjour !

Axelle Apvrille
Principal Security Researcher chez
Fortinet, @cryptax
Mobile malware, IoT, Ph0wn CTF

Travis Goodspeed
Digital watchmaker and Studebaker
enthusiast, @travisgoodspeed
GoodFET, GoodWatch, PoC||GTFO

FreeStyle Libre: c'est vraiment utile !



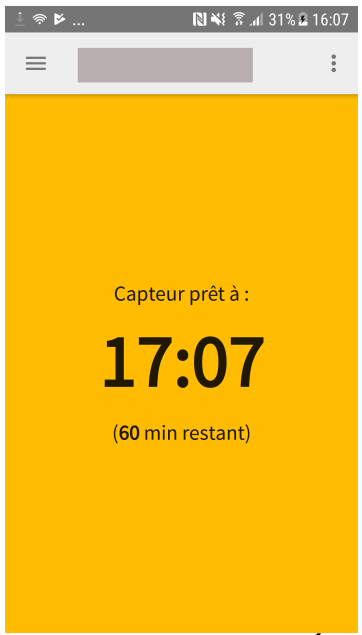


Evite de devoir se piquer trop souvent

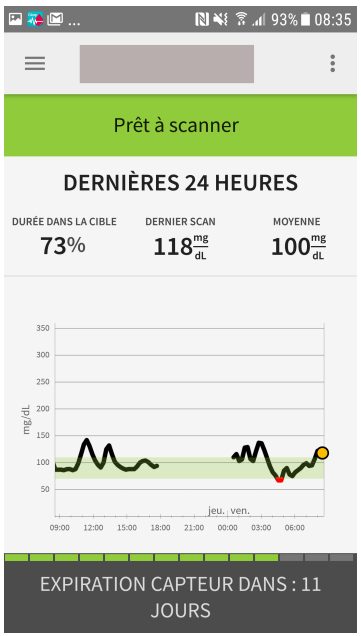
Cycle de vie d'un capteur

Monter le capteur

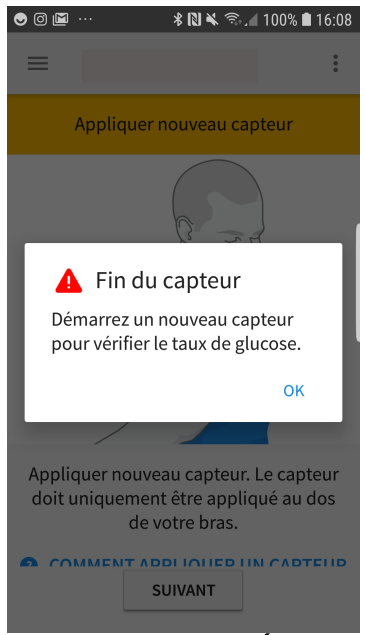
Appliquer le capteur



Délai d'activation (60 min)



On peut l'utiliser !



Expiration (14 j)

Hacking

1. Réinitialisation du capteur
2. Durée d'activation
3. Zonage du capteur
4. Longévité du capteur
5. Modifier les valeurs de glycémie

Ces hacks fonctionnent sur le **FreeStyle Libre**, mais n'ont pas été testés sur le tout **nouveau** **FreeStyle Libre 2***

* Disponibles en France seulement depuis Juin 2020, vendus en ligne, pas encore remboursés par la Sécu.

Avertissement d'usage !

Ces hacks fonctionnent d'un point de vue **technique**

Ils n'ont pas été testés d'un point de vue médical et peuvent être dangereux. Nous vous **déconseillons de "jouer" avec**.

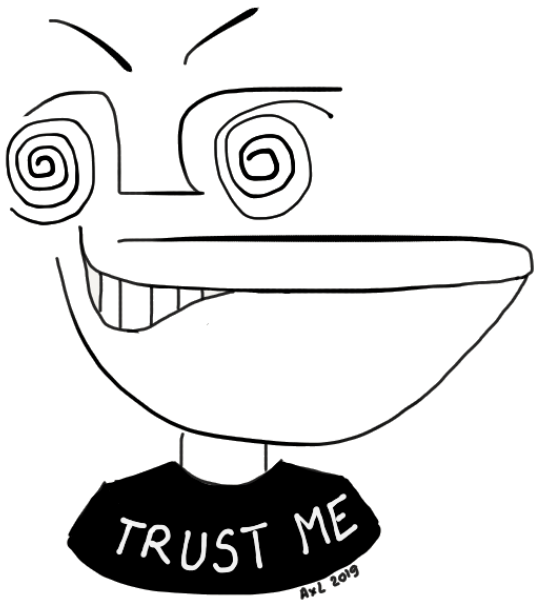
mais un attaquant pourrait le faire...

Démo: résurrection

Principe

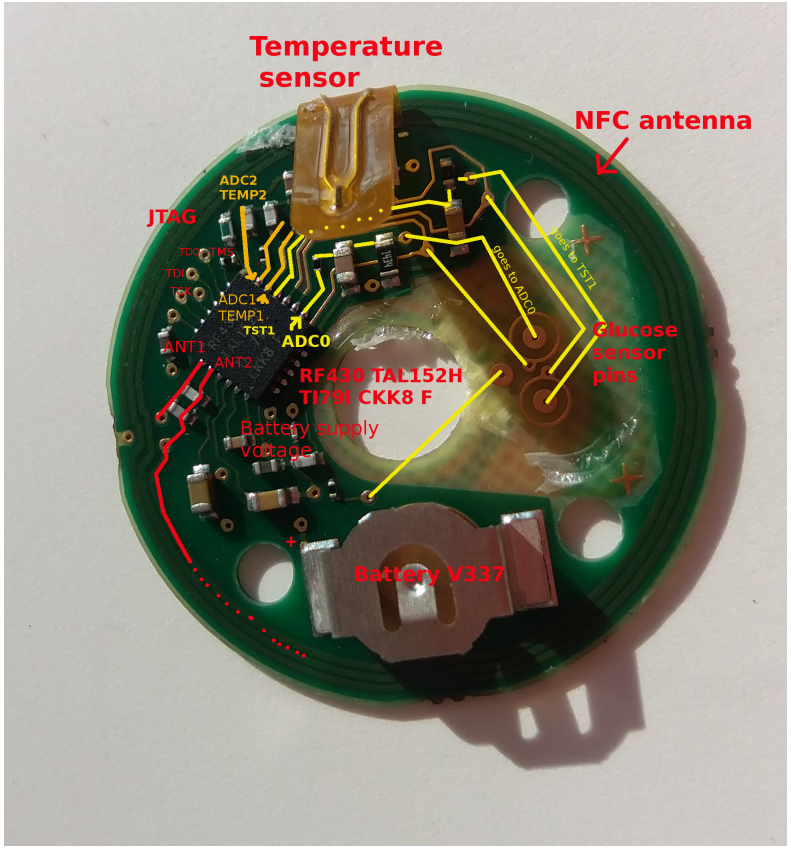
- Le capteur a expiré
- Magie* ! On le ramène à la vie !
- Il faut l'activer (comme un capteur neuf)
- Attendre le délai d'activation (comme un capteur neuf)
- Puis l'utiliser ! (euh, attention, il n'est pas vraiment neuf !)

* En fait, non, il n'y a rien de magique



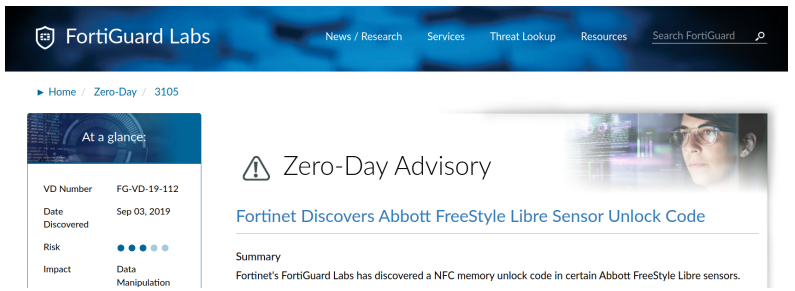
Les étapes de notre démarche

1. Démontage de l'objet: il y a une puce **TI RF 430 TAL**



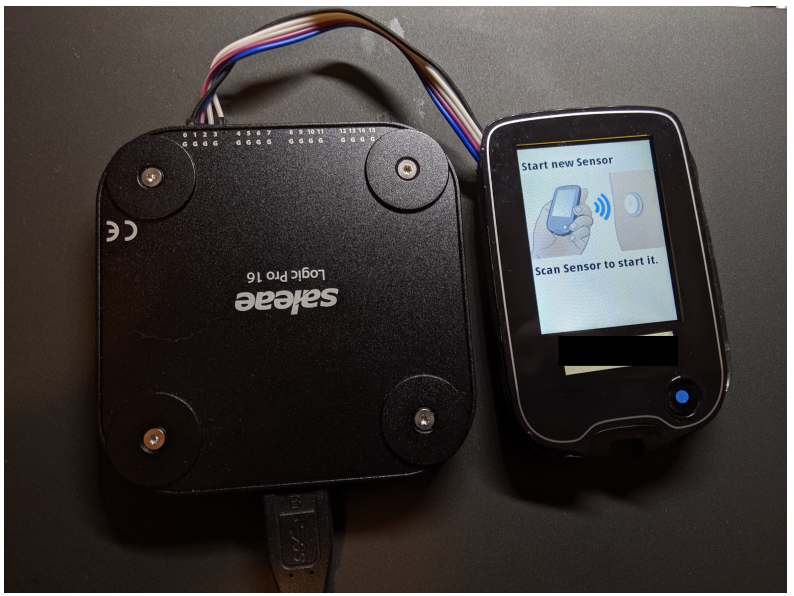
Les étapes de notre démarche

1. Démontage de l'objet: il y a une puce **TI RF 430 TAL**
2. Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)



Les étapes de notre démarche

1. Démontage de l'objet: il y a une puce **TI RF 430 TAL**
2. Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)
3. Dump du firmware, via NFC

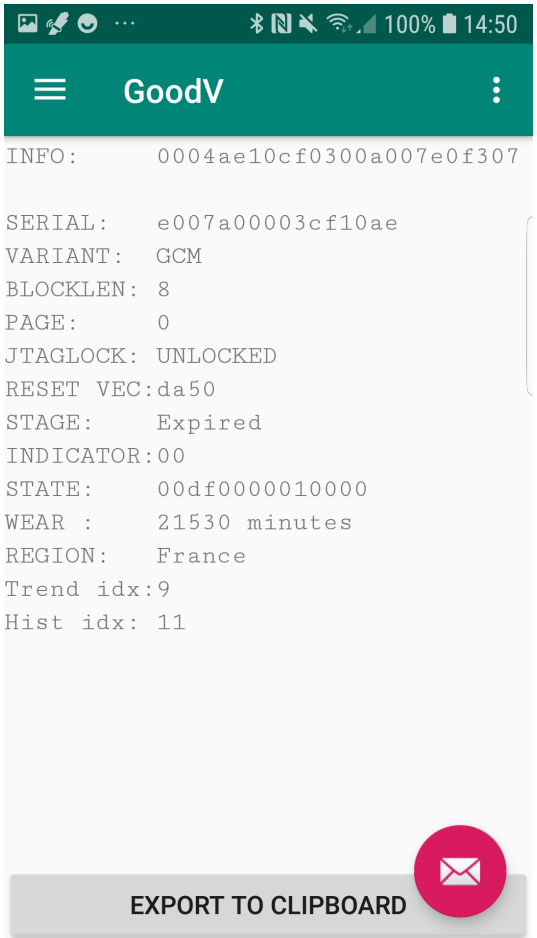


Les étapes de notre démarche

1. Démontage de l'objet: il y a une puce **TI RF 430 TAL**
2. Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)
3. Dump du firmware, via NFC
4. Reverse du firmware, identification d'une fonction désactivée (E0) pour le reset

Les étapes de notre démarche

1. Démontage de l'objet: il y a une puce **TI RF 430 TAL**
2. Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)
3. Dump du firmware, via NFC
4. Reverse du firmware, identification d'une fonction désactivée (E0) pour le reset
5. Implémentation d'une appli Android

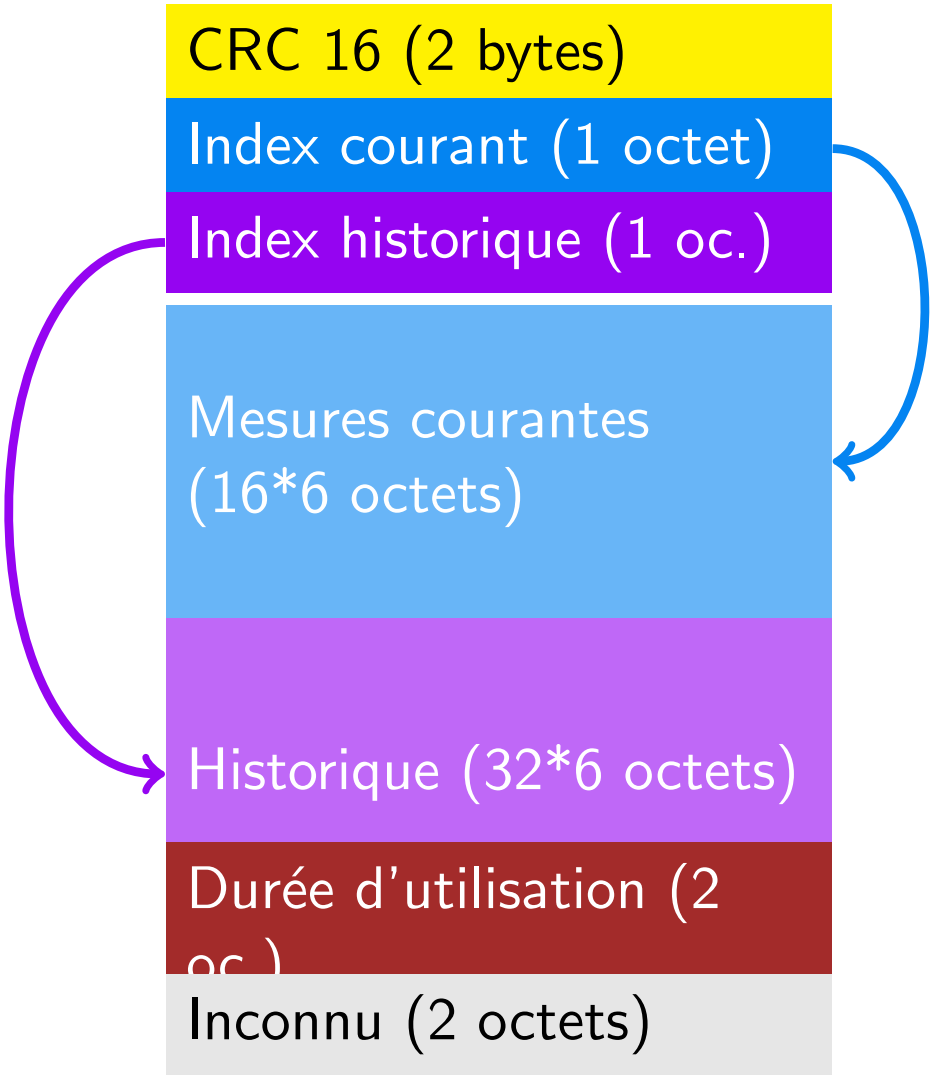


Sections du capteur et CRC

Section	Début	Fin
Blocs d'activation	F860	F877
Mesures de glycémie	F878	F99F
Capteur et région	F9A0	F9B7
Commandes	F9B8	FFCF
Suffixe	FFD0	FFF7

Adresses des sections applicatives sur le capteur

Infos complètes: rapport technique (38 pages)

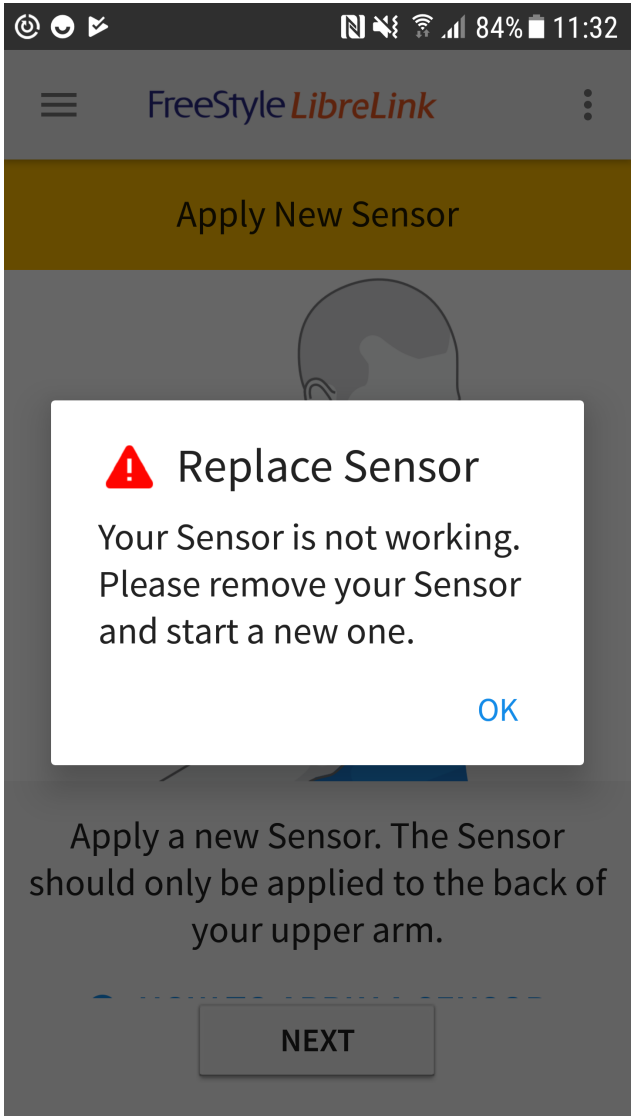


Exemple : section des mesures

Assassinat d'un capteur

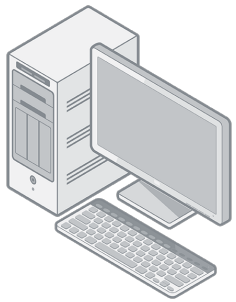
Deux façons de faire:

- Sale: corruption de la mémoire.
- Propre: modifier l'état du capteur vers "expiré".



Exemple : corruption mémoire

Démo: hack de l'activation avec Frida



Capteur

Hook (en JavaScript):
[*] Hack PatchTimeValues: we set warmup=2 weartime=6912000 minutes

App pour le capteur

Serveur Frida

Récapitulatif des hacks

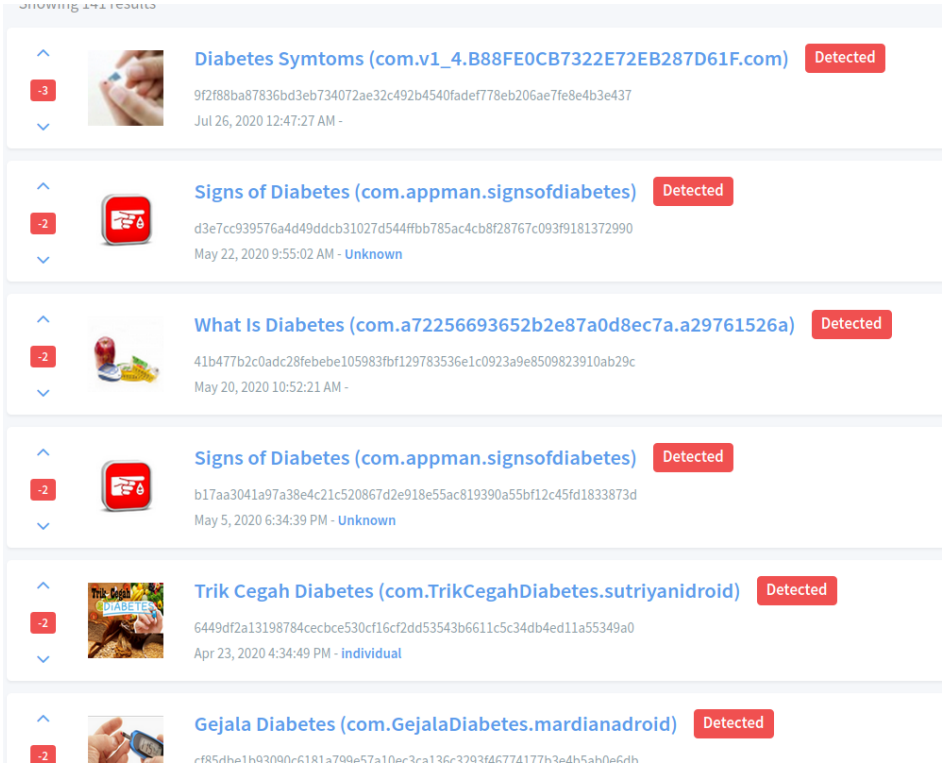
Hack	Conditions	Mise en place
Réssusciter	Proximité + secret	Facile
Assassinat	Proximité + secret	Très facile
Durée d'activation	Lab	Difficile
Longévité	Lab	Difficile
Niveau de glycémie	Lab	Difficile
Zone	Proximité + secret	Facile

Vulnérabilités remontées au fabriquant,
a priori ne sont plus présentes dans Libre 2.

Que ferait un attaquant ?

C'est bien plus facile d'infecter le téléphone avec un **rançongiciel** !

Les malwares "pour diabétiques", ça existe !



Et FreeStyle Libre 2 ?

La FRAM est chiffrée par un algorithme propriétaire:

- Génération d'une clé de bloc basée sur l'id du capteur, le modèle, magic, et le numéro du bloc
- XOR avec la clé

```
axelle@boostix ~/git/IoT/diabete/prog $ python3 readlibre2.py
Reading ../memory-dumps/libre2-E007A400011DDAC4.dump ------------
Status indicator    : Expired
Expiration indicator: Inactive
Trend index         : 9
Historic index      : 9
Trend Glucose level : 1.7 mg/dL
Historic Glucose lev: 220.7 mg/dL
Wear time           : 21498 minutes (i.e 14 days, 22:18:00 hours)
Sensor region       : Europe / UK
Header CRC          : read=c121 computed=c121 OK
Record CRC          : read=d0f0 computed=d0f0 OK
```

Demo

Références

- Rapport complet sur le capteur de glycémie
- GoodV Android application
- Outil pour la lecture du FreeStyle Libre
- NFC exploitation with RF430RFL152 and 'TAL152, PoC || GTFO, 20:03

Merci pour votre attention

Nous contacter :
@cryptax @travisgoodspeed

Merci particulièrement à

- Contacts diabétiques (je garde anonyme!)
- Et: @aamirlakhani @PagetPhil @TuxDePoinsisse @aurelsec @UYBHYS

Je serais bien venue déguster des galettes bretonnes... snif