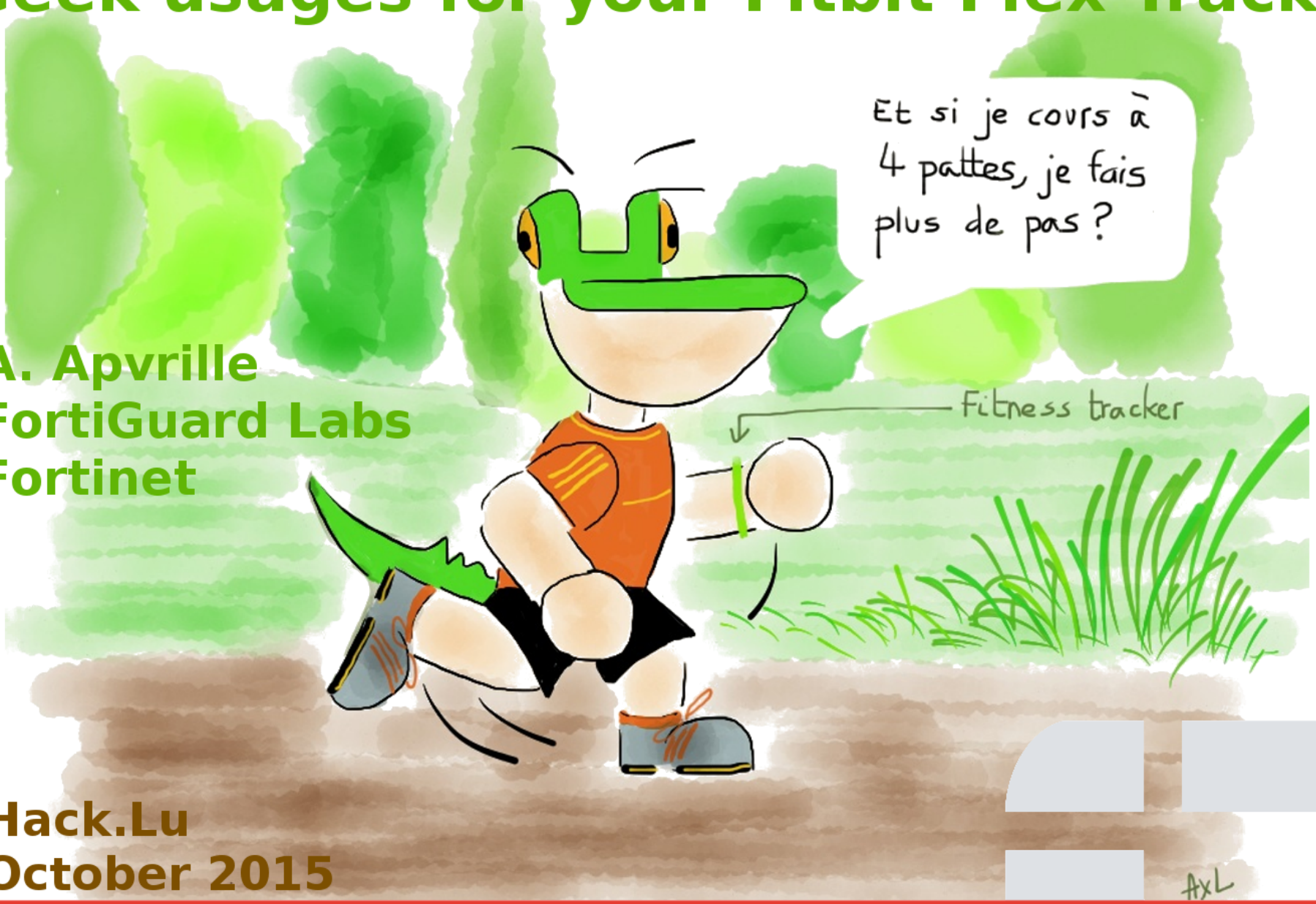
Geek usages for your Fitbit Flex Tracker



A. Apvrille
FortiGuard Labs
Fortinet

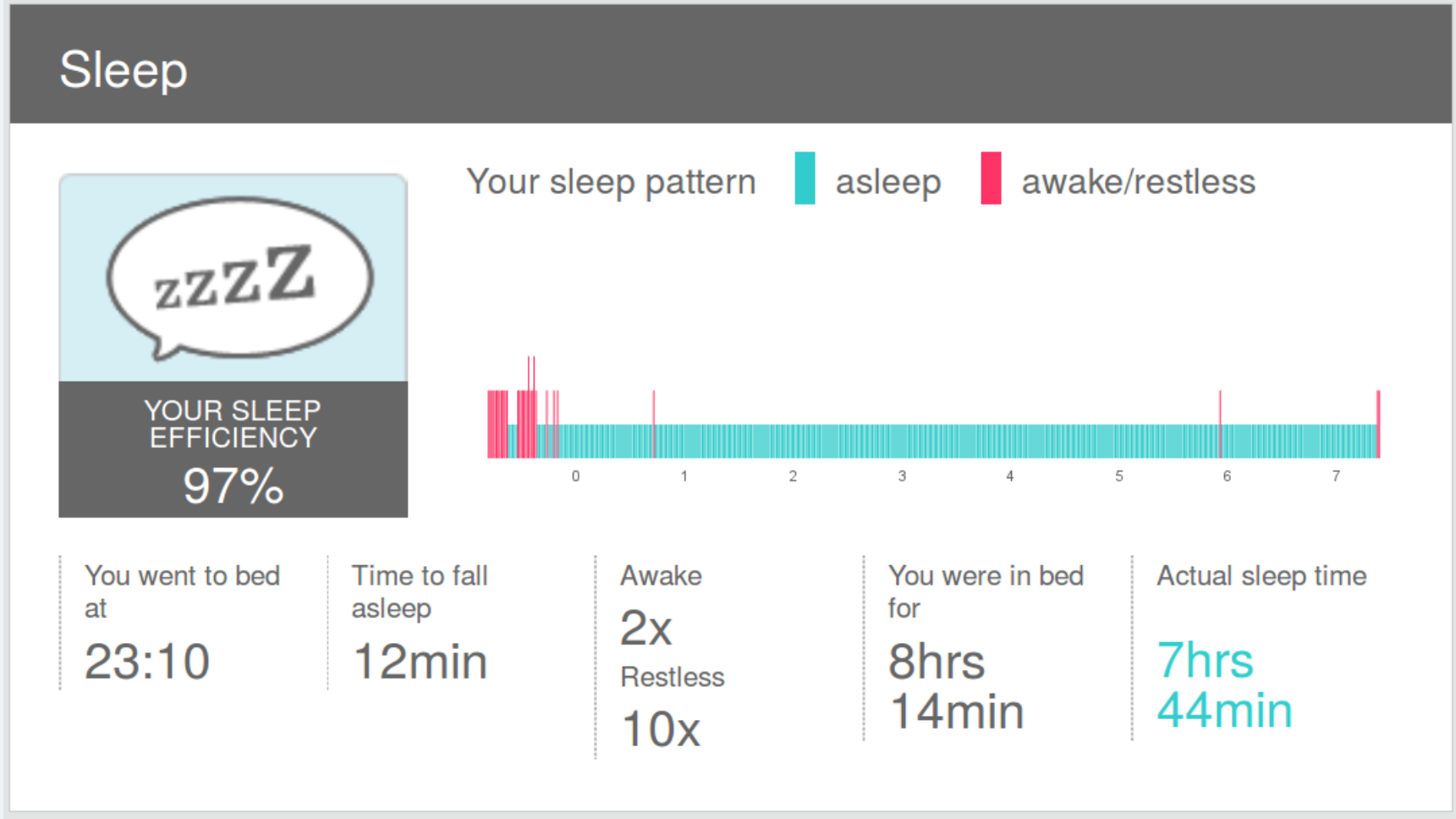
Hack.Lu
October 2015

FORTINET

Meet Fitbit Flex

- Wireless activity wristband
- Track steps, distance, calories, active minutes
- Display progress with 5 LEDs
- **No altimeter, no GPS** on Flex. Only on Charge or Surge.

It's also a "sleep wristband"



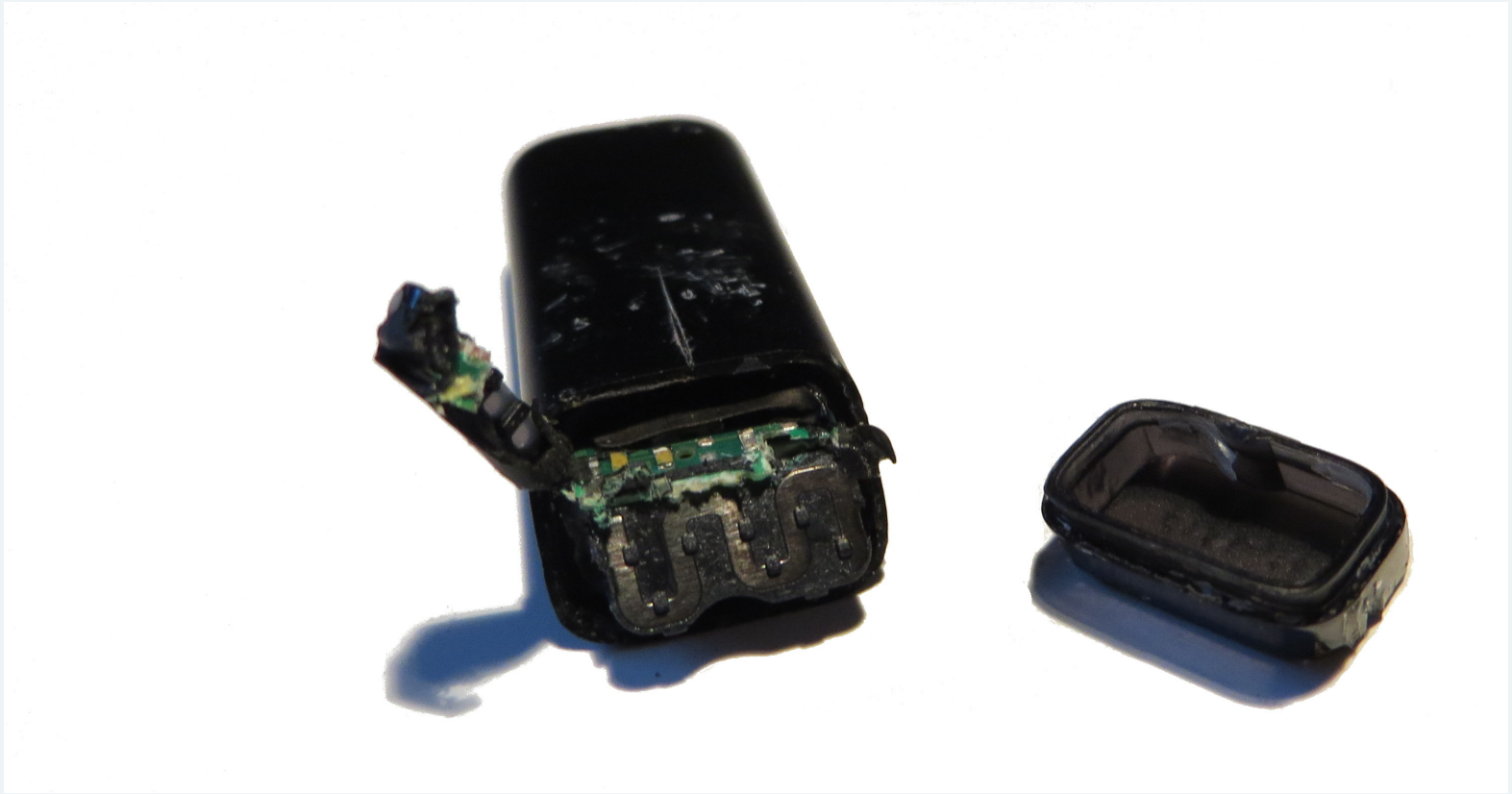
I slept well, thanks :)

Opening the tracker

Opening the tracker

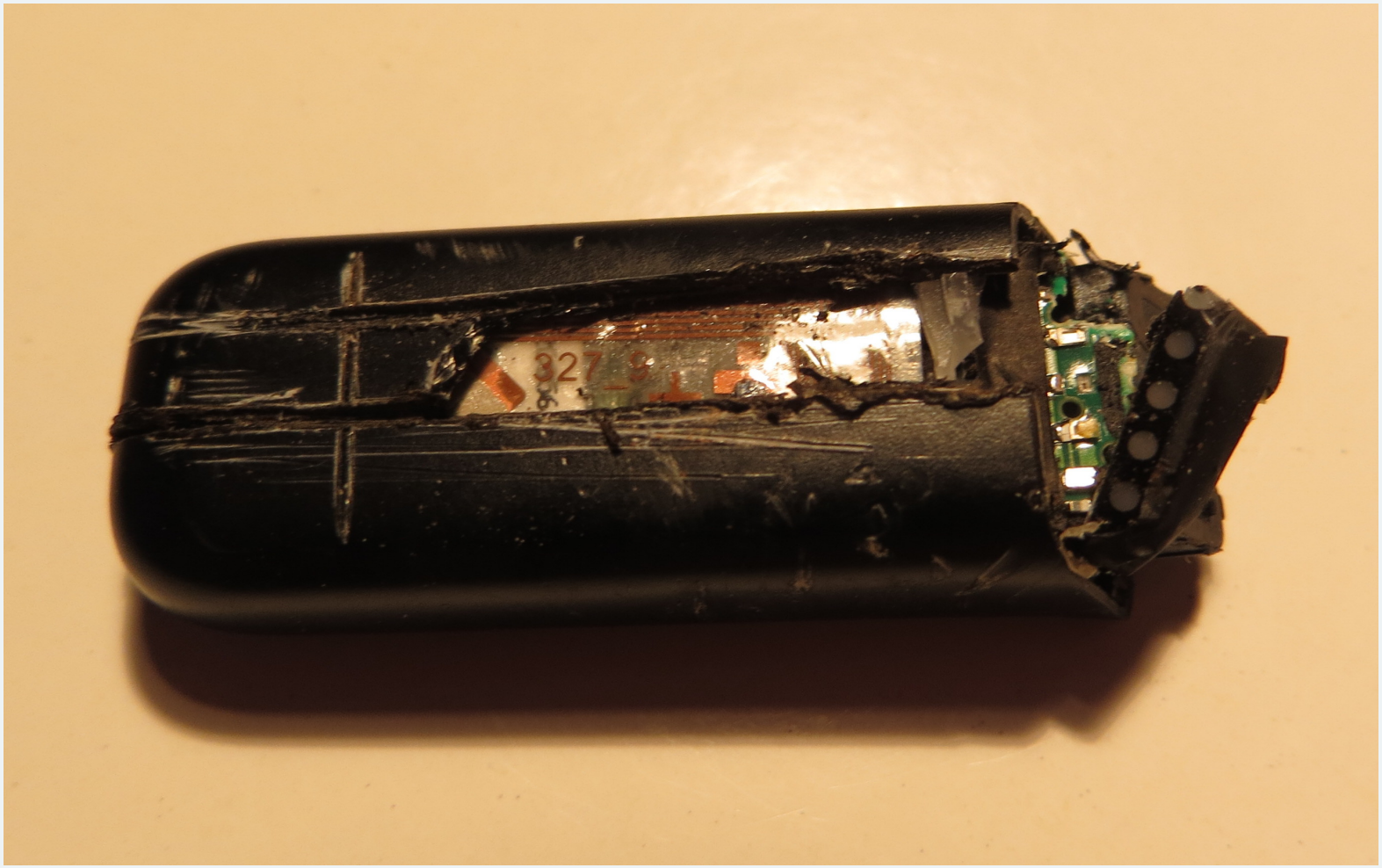
Thanks to my husband, Ludovic :)

Opening the tracker



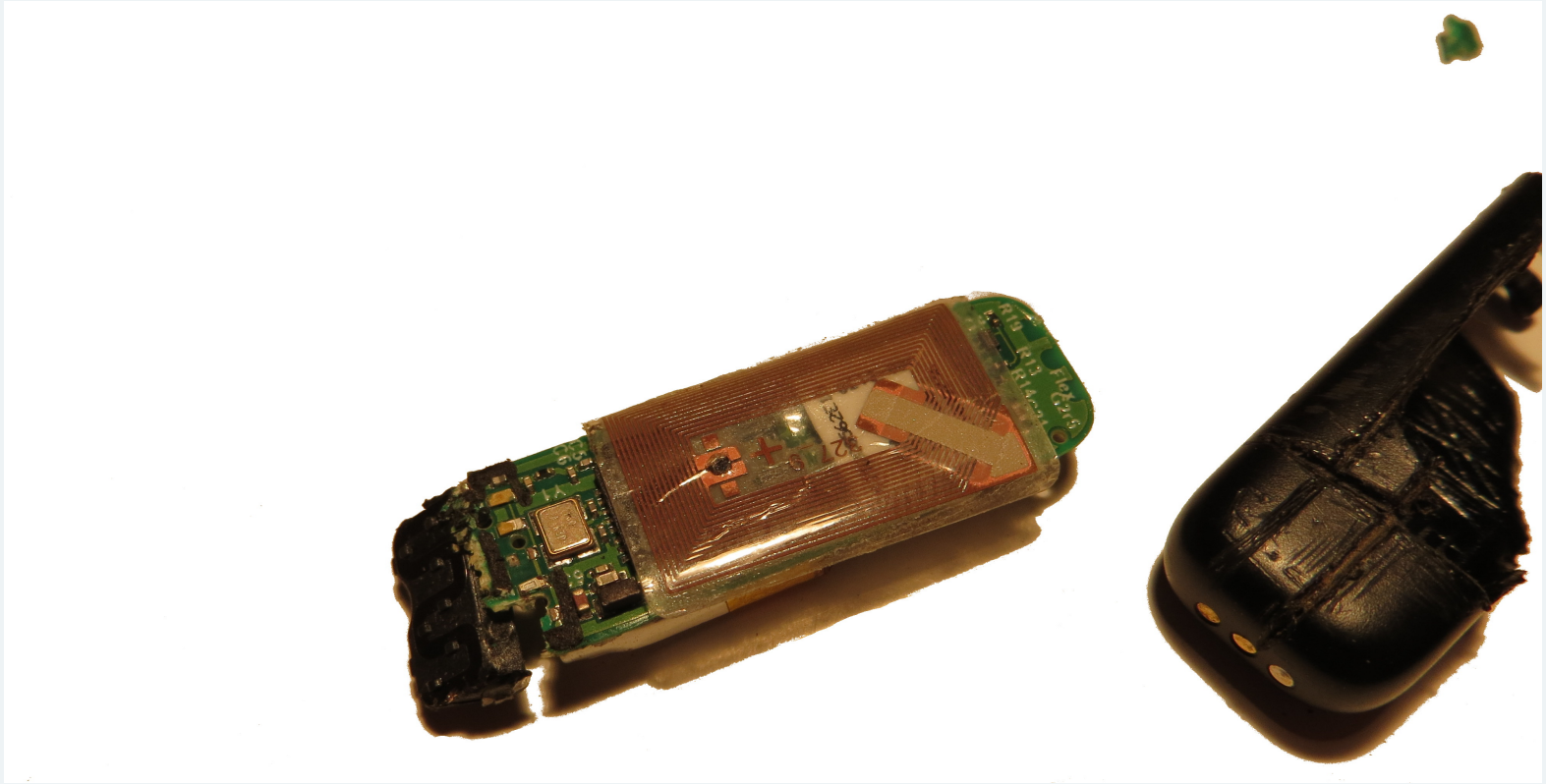
Thanks to my husband, Ludovic :)

Opening the tracker



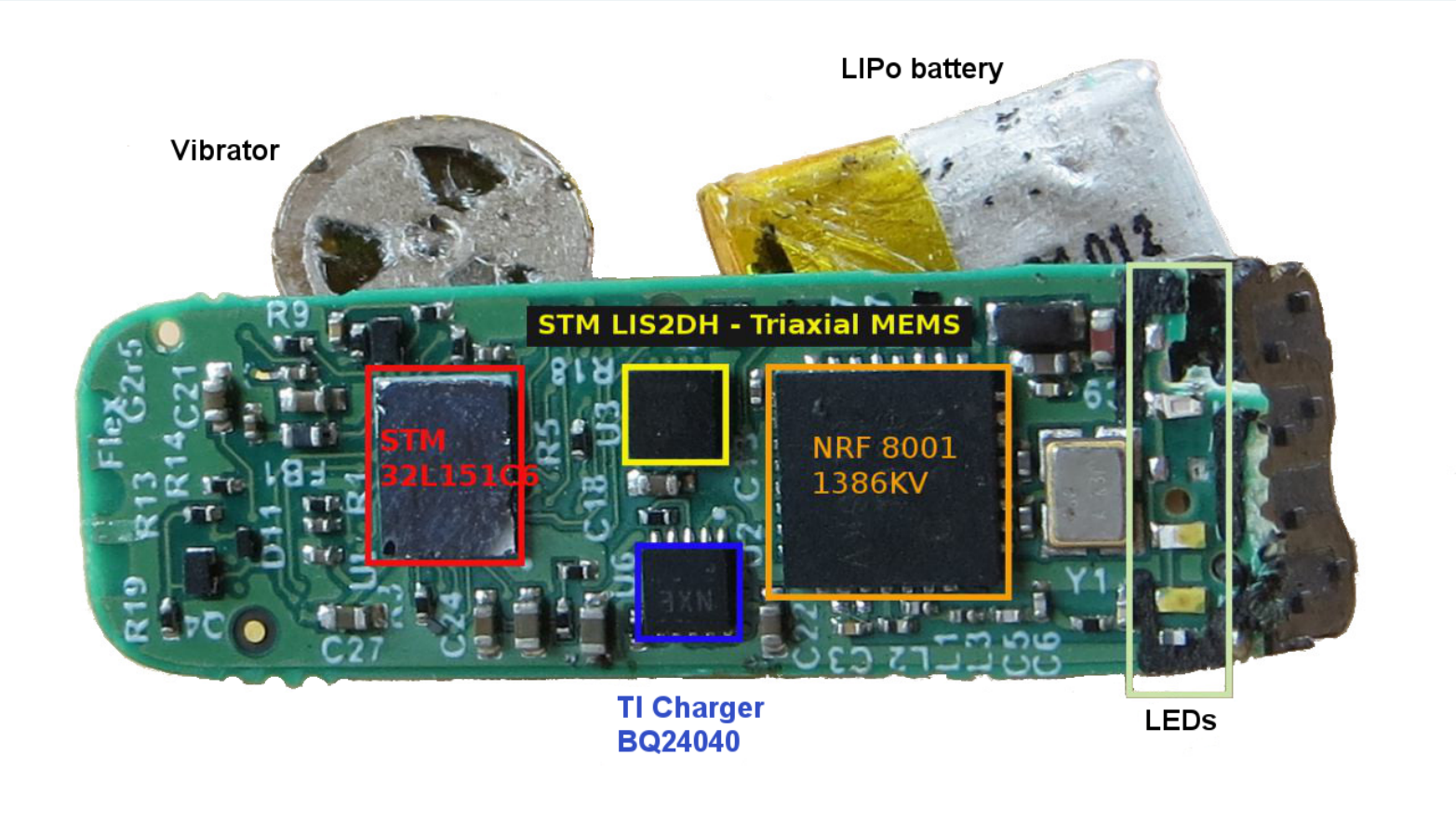
Thanks to my husband, Ludovic :)

Opening the tracker



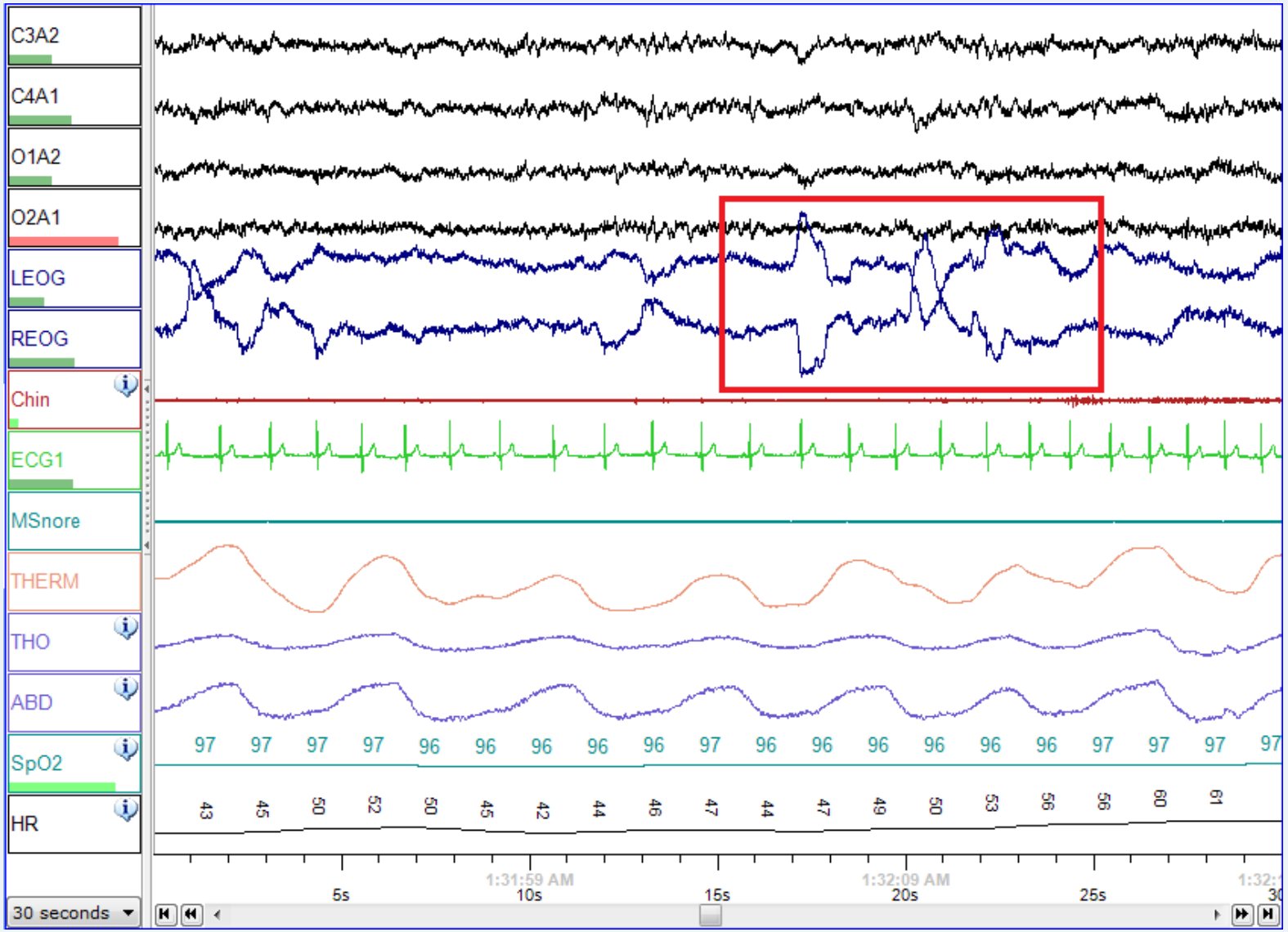
Thanks to my husband, Ludovic :)

Opening the tracker



Thanks to my husband, Ludovic :)

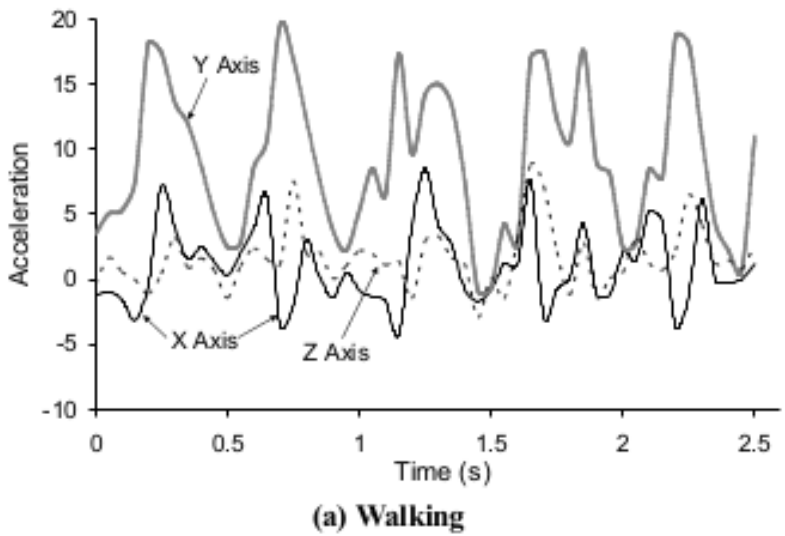
Sleep stage: polysomnography (PSG)



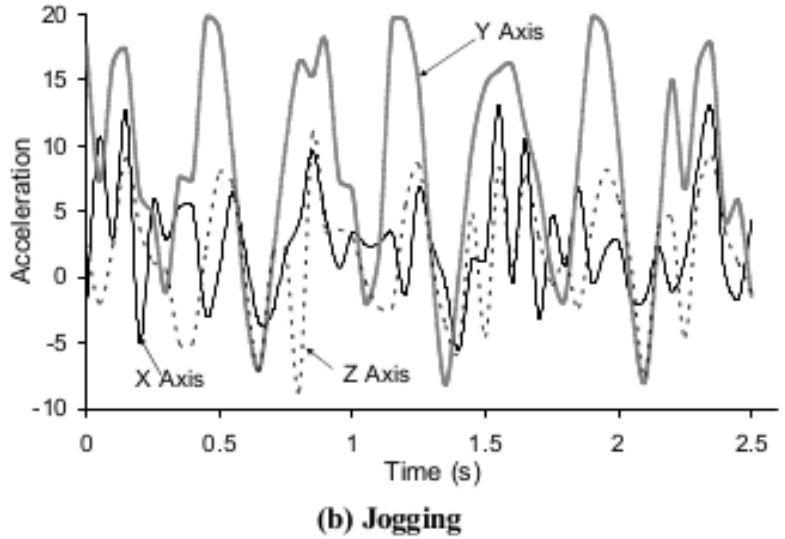
Credits: NascarEd

Tracking activity with an accelerometer

Acceleration on (x), (y) and (z) for **walking** and **jogging**



(a) Walking

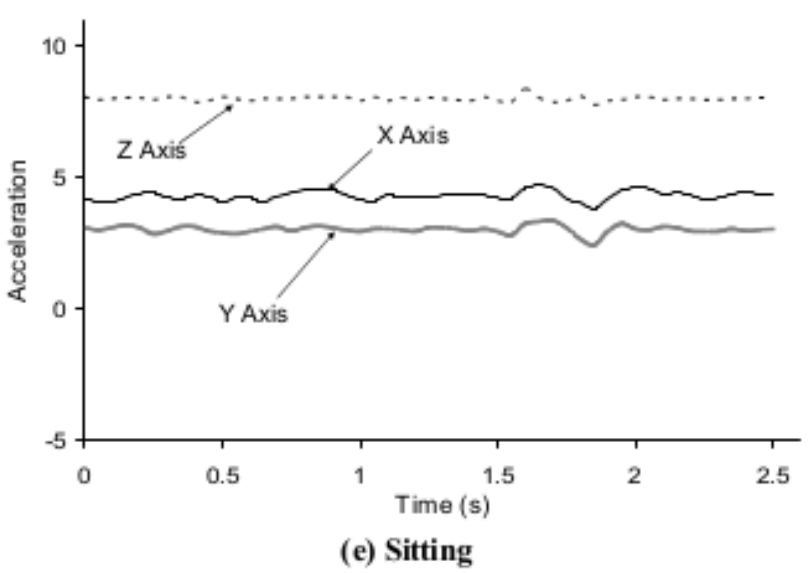


(b) Jogging

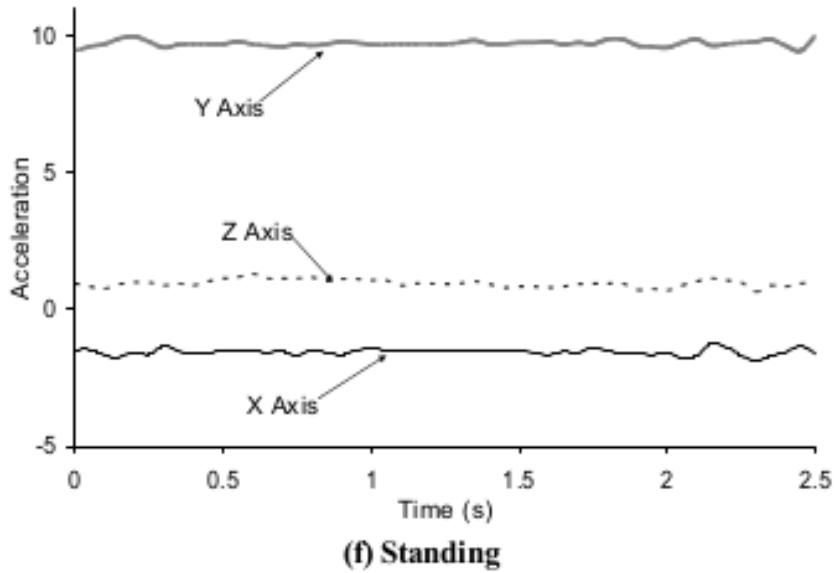
From Kwapisz, Weiss and Moore,
"Activity Recognition using Cell Phone Accelerometers",
SIGKDD 2011

Tracking activity with an accelerometer

Acceleration on (x), (y) and (z) for **sitting** and **standing**



(e) Sitting



(f) Standing

From Kwapisz, Weiss and Moore,
"Activity Recognition using Cell Phone Accelerometers",
SIGKDD 2011

Spying with an accelerometer

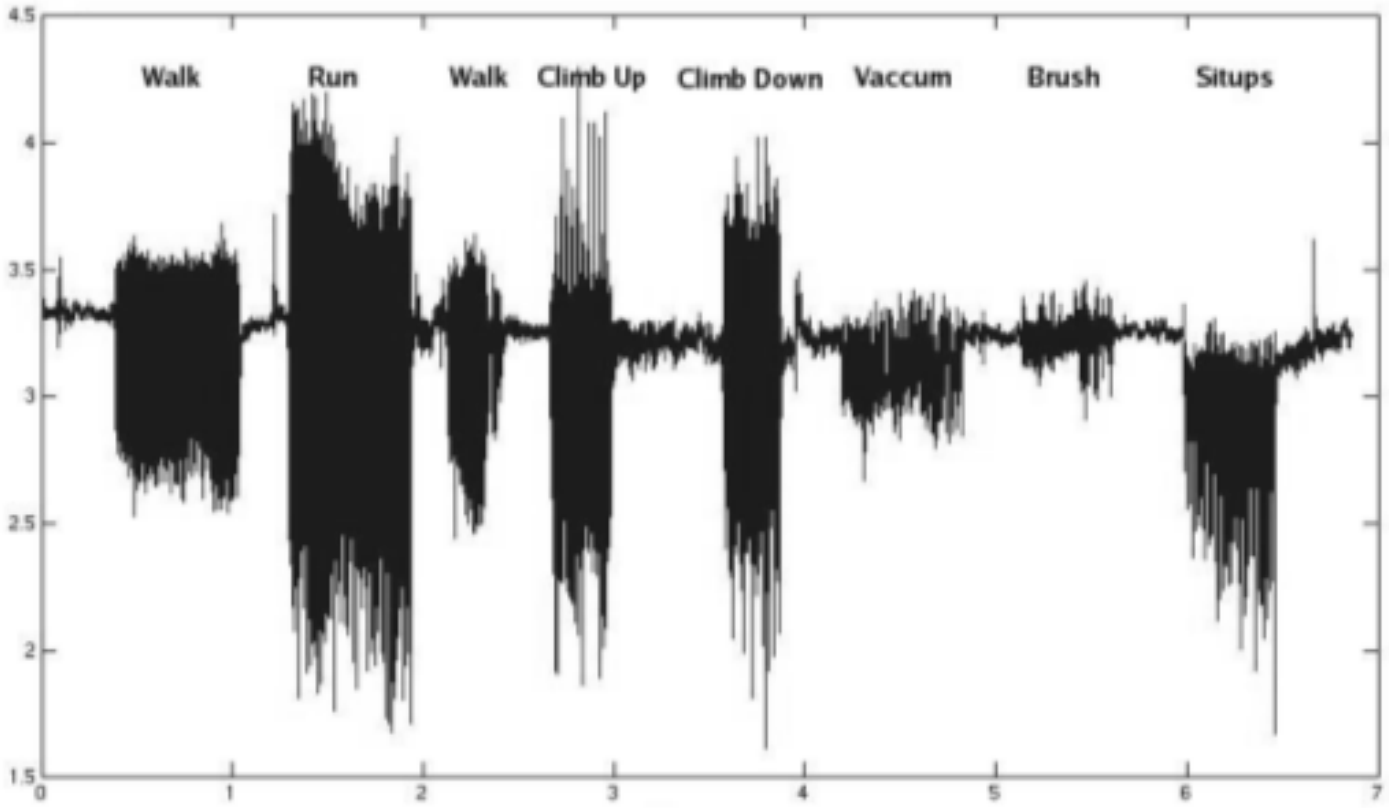
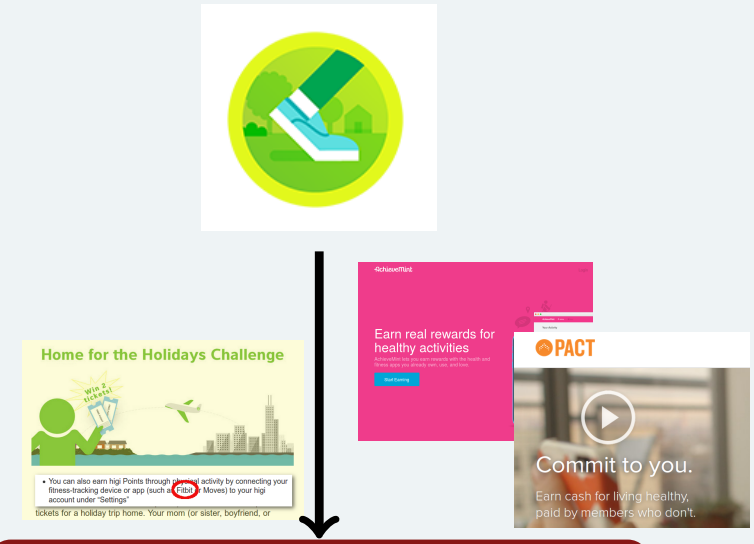


Figure 3: X-axis readings for different activities

From Ravi, Dandekar, Mysore and Littman,
"Activity Recognition from Accelerometer Data", IAAI'05

Where fitness data goes to



Various reward programs

Mavens Consulting

Sales forces, insurances, sponsors...

"Higi announced [..] the launching of its industry-leading, privacy-protected and secure API" - Source: PR News

"AchieveMint previously partnered with the Brooklyn Nets basketball team to encourage users in Brooklyn and 75 miles around it to earn special rewards, such as VIP tickets to the draft or signed merchandise." - Source: Mashable

Other Examples

Nest (thermostat) and Beam (toothbrushes) are sharing with *insurances*

Alternate usages to your tracker

What can you do with your (beloved) fitness tracker *without* sending anything to Fitbit (or other) servers?

Four alternate geek usages

"This can of green pees?
I'm going to turn it into caviar!"

1. Impress young kids with magician talent
2. Impress a scientist with a RNG
3. Impress a hacker friend with a screen saver
4. Impress security researchers with a scary attack

Geek no.1: Impress (very) young kids with magician talent

Proprietary!

No technical user/ developer/ contributor documentation

Everything has to be reverse engineered

Display Code

```
c0 06 00 .. 00 02
```

- **c0**: control packet, for the tracker
- **06**: command id - Display Code
- **02**: useful length for packet

Blinking LEDs

Endpoint 0x01

Blinking LEDs

Endpoint 0x01 `C0 06 00 ... 02`

Geek no.2 Impress a scientist with a RNG

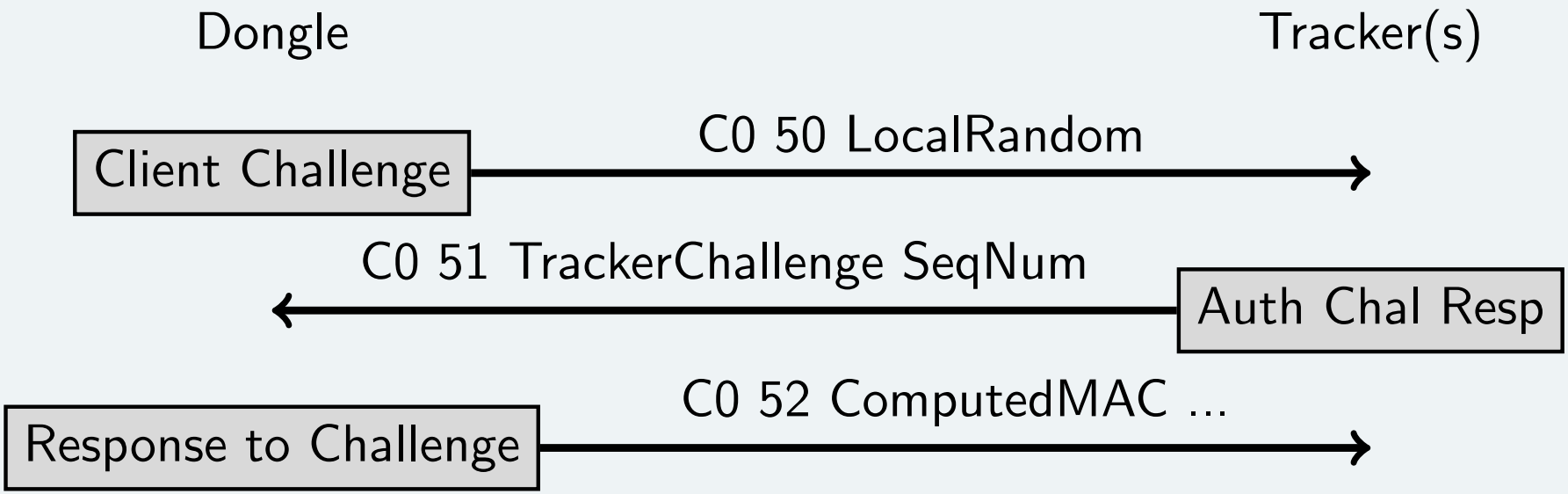
We always lack sources of entropy, don't we?
Use authentication packets

Funny!

Flex supports **authentication** messages, but it's a **passthru**

```
if ( !isencrypted ||
     (TrackerAuthUtils.checkMac(...)) {
  if (!isencrypted) {
    MySystemLog.log("TrackerAuthCommand",
    "Tracker is not encrypted,
    we just assume it\'s authed");
  }
  ...
```

Flex authentication



Implement a Flex-based RNG

- Send a dummy local random (C0 50)
- Wait for tracker's response: 8-byte challenge
- Never send last message (C0 52)

Is it (really) random???

Description	Entropy	Chi-square	Mean	Monte-Carlo Pi error	Dieharder failed tests
Target	**8**	**10-90%**	**127.5**	**0%**	**0**
Victor Hugo	4.6	0.01%	99	27%	2 weak
Linux PRNG /dev/urandom	8	75%	127	0.57%	0
AES ciphertext	8	50%	128	0.50%	
Fitbit tracker	**8**	**75%**	**127**	**0.36%**	**3 weak**
Radioactive decay events		41%		0.06%	

Tracker RNG: conclusion

I would not use it for crypto

It does not look notably worse than Linux's standard RNG

Geek no.3 Impress a hacker friend with a screen saver

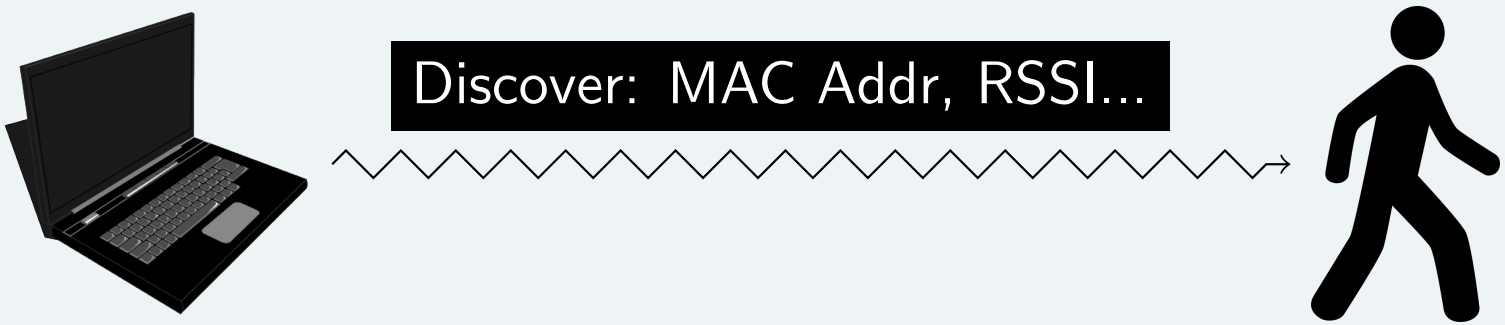
How to keep your laptop secure from curious eyes?

Screen lock

- See Matias Katz, "Backdooring X11 with much class and no privilege"
- Use the Fitbit USB dongle!
- Rely on udev

DEMO

Better: lock with the tracker



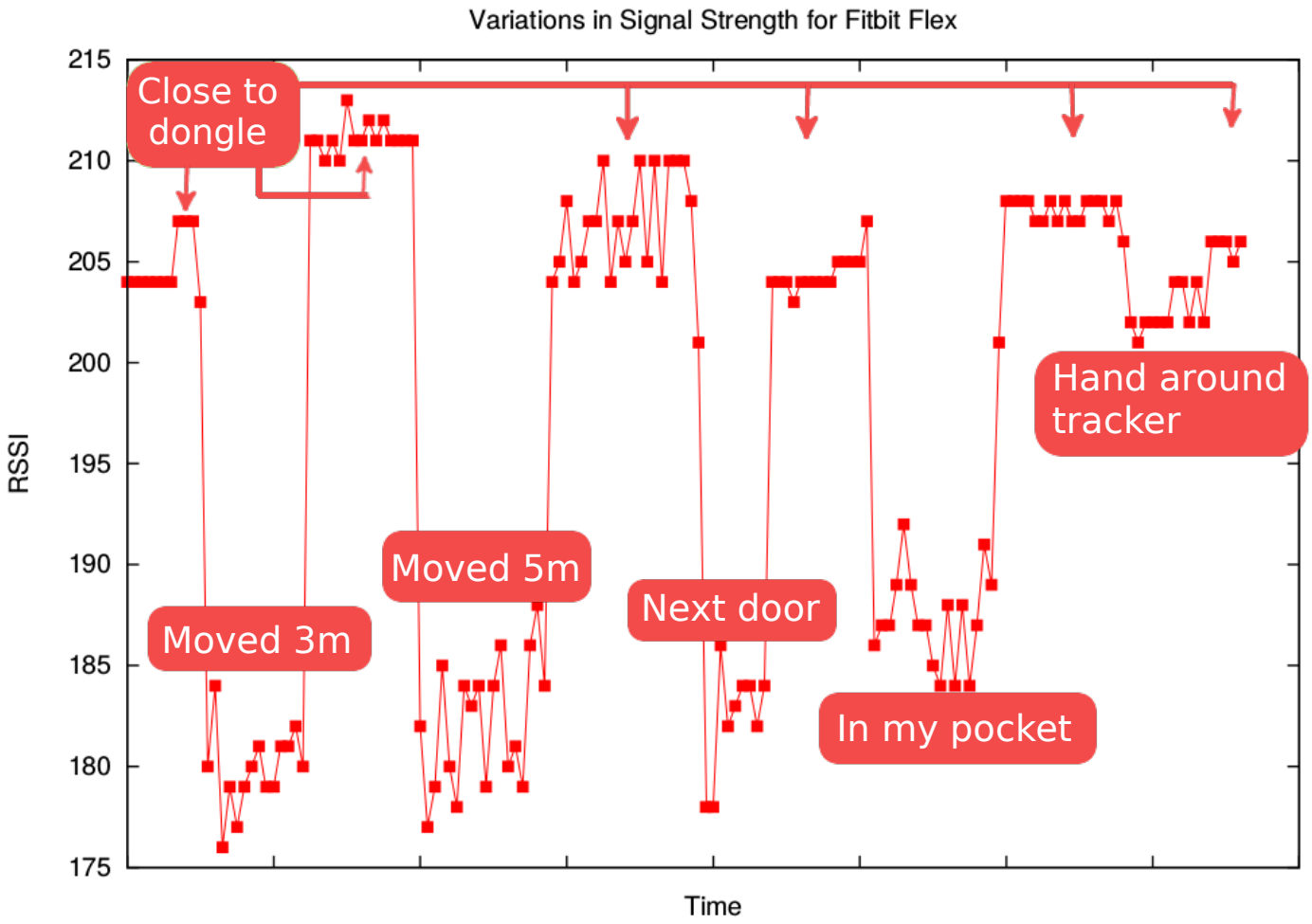
Lock the screen when you move
away from your laptop

How?

Discovery responses:

1. the tracker's ID - this is its Bluetooth MAC address
2. and the Received Signal Strength Indication

Plotting RSSI



Trackerlock demo

Trackerlock

```
$ python trackerlock.py --delay 1 --movement 15
Getting list of available trackers...
1- TrackerId: 09 73 78 63 f7 f3  AddrType: 1
   RSSI: 190 Attr: 02 07  SUUID: 00 fb
Select tracker's num: 1
Tracker has moved away!!! (RSSI=186)
```

Demo

Geeky no.4: Scare a Security Researcher

For Good .. or for Bad

Good: Digital Tatoo

Geeky no.4: Scare a Security Researcher

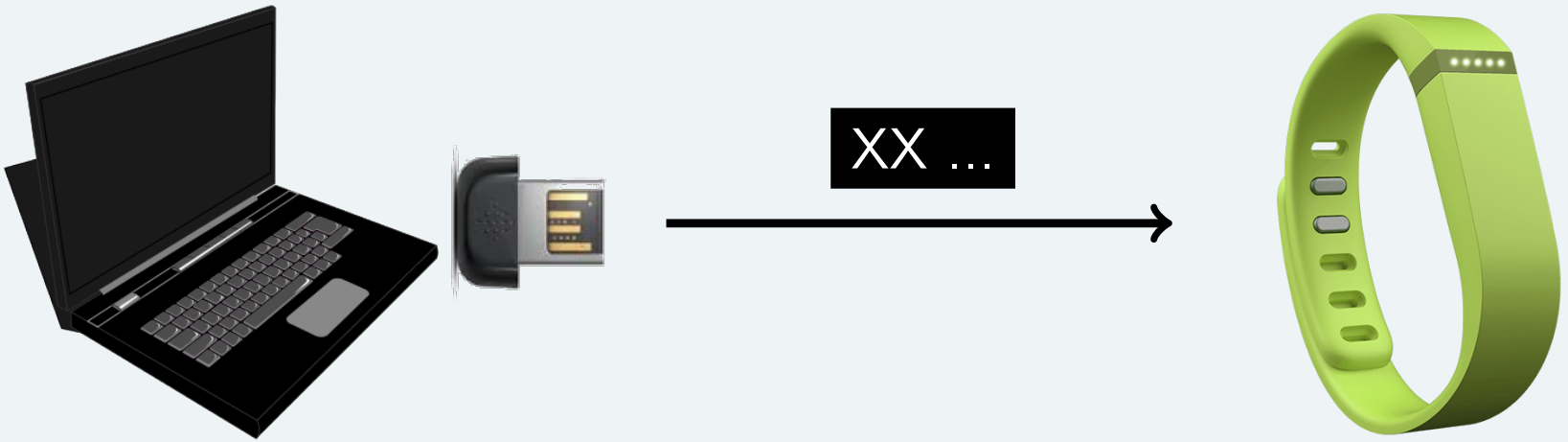
For Good .. or for Bad

Good: Digital Tatoo

Geeky no.4: Scare a Security Researcher

For Good .. or for Bad

Good: Digital Tatoo



Geeky no.4: Scare a Security Researcher

For Good .. or for Bad

Good: Digital Tatoo

...I LOVE YOU !

Tatoo response

Danger: What if Tatoo is Malicious Code?

Attacker

Victim's laptop

Danger: What if Tatoo is Malicious Code?

Attacker

Victim's laptop

INJECTED MALICIOUS CODE

Tracker
is infected

Danger: What if Tatoo is Malicious Code?

Attacker

Victim's laptop

INJECTED MALICIOUS CODE

DISCOVERY

Tracker
is infected

Danger: What if Tatoo is Malicious Code?

Attacker

INJECTED MALICIOUS CODE

Tracker
is infected

DISCOVERY

MALICIOUS CODE

Victim's laptop

Danger: What if Tatoo is Malicious Code?

Attacker

INJECTED MALICIOUS CODE

Tracker
is infected

DISCOVERY

MALICIOUS CODE

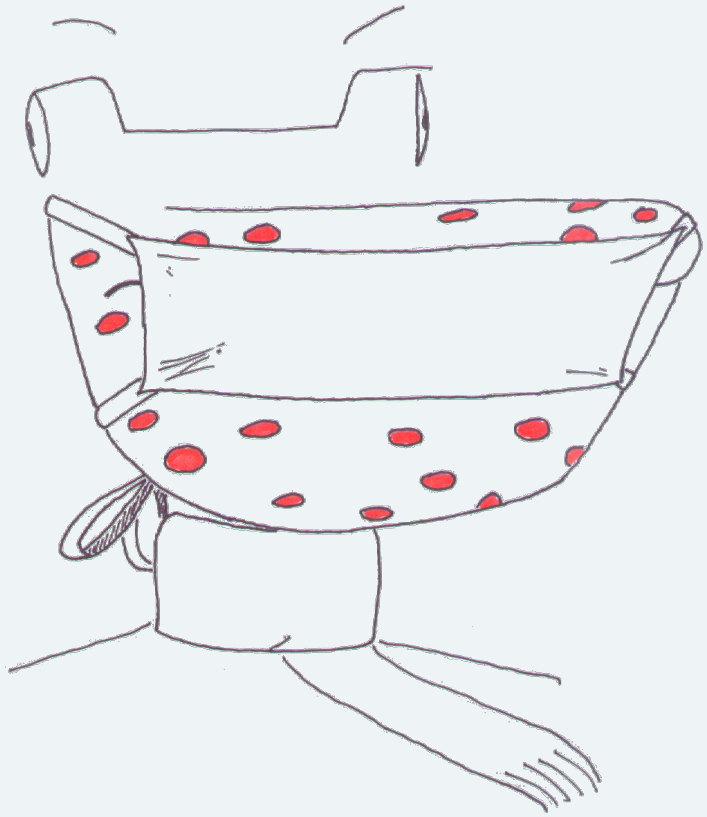
Victim's laptop

Deliver malicious payload: crash, propagate...

Video

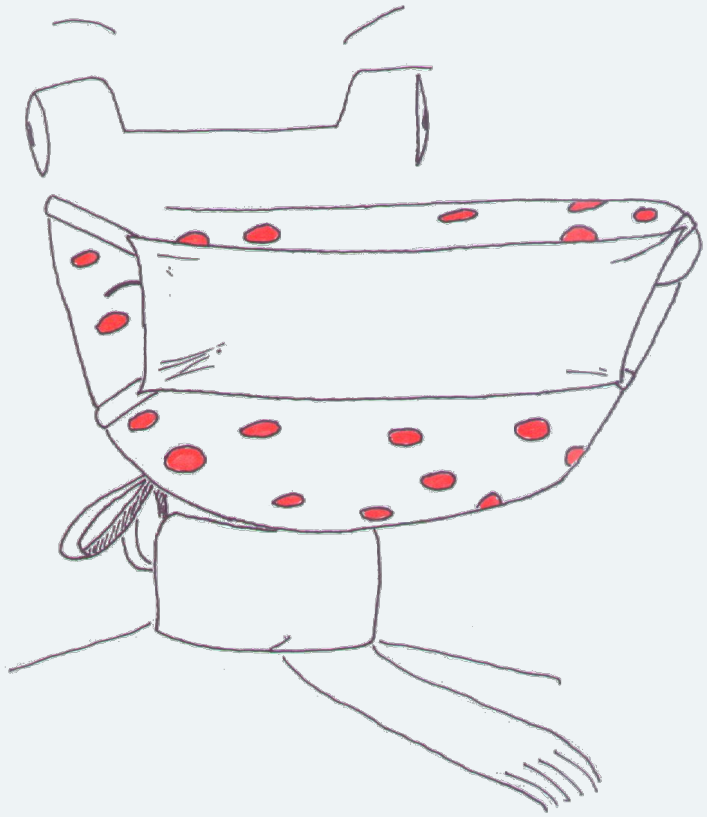
Digital Tatoo / Infection: Limitations

1. Max 17 bytes. Is that enough?
   Yes: Crash Pentium Trojan (2004): 4 bytes



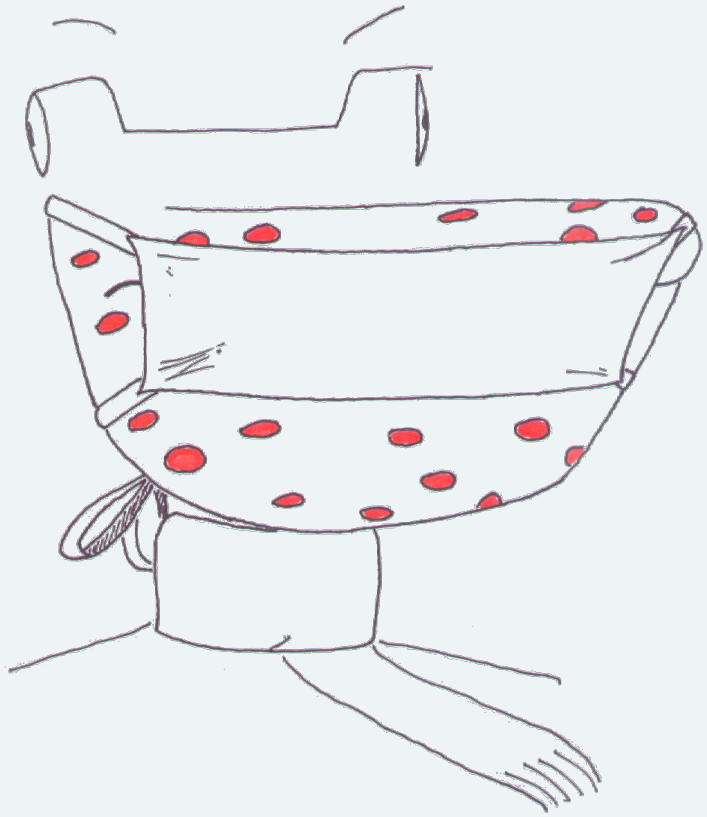
Digital Tatoo / Infection: Limitations

1. Max 17 bytes. Is that enough?
   Yes: Crash Pentium Trojan (2004): 4 bytes
2. Execute/Deliver code on target: we did not handle this!



Digital Tatoo / Infection: Limitations

1. Max 17 bytes. Is that enough?
   Yes: Crash Pentium Trojan (2004): 4 bytes
2. Execute/Deliver code on target: we did not handle this!
3. Fitbit patches



Interesting links

- Galileo - https://bitbucket.org/benallard/galileo
- Rahman et al. Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device, CoRR, 2013.
- Fitbit Flex Teardown. http://ifixit.org/blog/5042/fitbit-flex-teardown/
- Matias Katz - Backdooring X11 with much class and no privileges, Hack in Paris 2015
- My my Fitbit tools repository on GitHub
- My presentation at Hack in Paris 2015
- My own humoristic drawings Pico le croco
- Link to satisfaction form: http://bit.ly/1KUkjaB

Thanks for your attention!

Contact info

@cryptax or `aapvrille` (at) `fortinet` (dot) `com`

http://bit.ly/1KUkjaB

Thanks to
Ludovic Apvrille, Aurélien Francillon and Matias Katz