Geek usages for your Fitbit Flex Tracker

A. Apvrille
FortiGuard Labs
Fortinet

Et si je cours à
4 pattes, je fais
plus de pas?

Fitness tracker

Hack.Lu
October 2015
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

Thanks to my husband, Ludovic :)

Tu vas adorer, mon p’tit ! C’est GEANT

il est zentil mais je préfère mes zéux à moi
Opening the tracker

Thanks to my husband, Ludovic :)
Opening the tracker

Thanks to my husband, Ludovic :)

Fortinet

Hack.lu 2015 - A. Apvrille
Opening the tracker

Thanks to my husband, Ludovic :)
Opening the tracker

Thanks to my husband, Ludovic :)
Opening the tracker

Thanks to my husband, Ludovic :)

STM LIS2DH - Triaxial MEMS
STM 32L151CB
NRF 8001 1386KV
TII Charger
BQ24040
LIPo battery
Vibrator
LEDs
Sleep stage: polysomnography (PSG)

Credits: NascarEd
Tracking activity with an accelerometer

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

From Kwapisz, Weiss and Moore, “Activity Recognition using Cell Phone Accelerometers”, SIGKDD 2011
Spying with an accelerometer

From Ravi, Dandekar, Mysore and Littman, “Activity Recognition from Accelerometer Data”, IAAI’05
“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...
What can you do with your (beloved) fitness tracker *without* sending anything to Fitbit (or other) servers?
Four alternate geek usages

“Cette boîte de petits pois ?
Je vais la transformer en 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

“This can of green peas? I’m going to turn it into caviar!”
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

\texttt{c0 06 00 .. 00 02}

\begin{itemize}
\item \texttt{c0}: control packet, for the tracker
\item \texttt{06}: command id - Display Code
\item \texttt{02}: useful length for packet
\end{itemize}
Blinking LEDs

Endpoint 0x01
Blinking LEDs

Endpoint 0x01

C0 06 00 ... 02

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

Funny!

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

```java
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???

<table>
<thead>
<tr>
<th>Description</th>
<th>Entropy</th>
<th>Chi-square</th>
<th>Mean</th>
<th>Monte-Carlo Pi error</th>
<th>Dieharder failed tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>8</td>
<td>10-90%</td>
<td>127.5</td>
<td>0%</td>
<td>0</td>
</tr>
<tr>
<td>Victor Hugo</td>
<td>4.6</td>
<td>0.01%</td>
<td>99</td>
<td>27%</td>
<td>2 weak</td>
</tr>
<tr>
<td>Linux PRNG /dev/urandom</td>
<td>8</td>
<td>75%</td>
<td>127</td>
<td>0.57%</td>
<td>0</td>
</tr>
<tr>
<td>AES ciphertext</td>
<td>8</td>
<td>50%</td>
<td>128</td>
<td>0.50%</td>
<td>3 weak</td>
</tr>
<tr>
<td>Fitbit tracker</td>
<td>8</td>
<td>75%</td>
<td>127</td>
<td>0.36%</td>
<td></td>
</tr>
<tr>
<td>Radioactive decay events</td>
<td></td>
<td>41%</td>
<td></td>
<td>0.06%</td>
<td></td>
</tr>
</tbody>
</table>
I would not use it for crypto

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

Variations in Signal Strength for Fitbit Flex

- Close to dongle
- Moved 3m
- Moved 5m
- Next door
- In my pocket
- Hand around tracker
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

I LOVE YOU!

Tatoo
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

Tracker is infected

INJECTED MALICIOUS CODE
Danger: What if Tatoo is Malicious Code?

Attacker

Victim’s laptop

Tracker is infected

Injecting Malicious Code

Discovery
Danger: What if Tatoo is Malicious Code?

Attacker

Victim’s laptop

Tracker is infected

INJECTED MALICIOUS CODE

DISCOVERY

MALICIOUS CODE
Danger: What if Tatoo is Malicious Code?

Attacker

Victim’s laptop

Tracker is infected

Deliver malicious payload: crash, propagate...

INJECTED MALICIOUS CODE

DISCOVERY

MALICIOUS CODE
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!
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
- 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
Thanks for your attention!

Contact info
@cryptax or aapvrille (at) fortinet (dot) com

Thanks to
Ludovic Apvrille, Aurélien Francillon and Matias Katz