Fitness Tracker: Hack In Progress

Axelle Apvrille - FortiGuard Labs, Fortinet

Hacktivity, October 2015
Meet Fitbit Flex

- Wireless activity + Sleep wristband
- Track steps, distance, calories
- Display progress with 5 LEDs
- Monitor how well you sleep
- Wake up alarm
- No altimeter, no GPS on Flex. Only on Charge or Surge.
How to open the wristband
Lightweight option :)  

Thanks to my husband, Ludovic :)
Thanks to my husband, Ludovic :)
Thanks to my husband, Ludovic :)

NFC antenna

Thanks to my husband, Ludovic :)

Hacktivity 2015 - A. Apvrille
Thanks to my husband, Ludovic :)

STM LIS2DH - Triaxial MEMS
STM 32L151CG
NRF 8001 1386KV
TI Charger BQ24040
LIPo battery
Vibrator
LEDs
How many fitness trackers sold in 2014?

- 10 million
- 40 million
- 70 million
How many fitness trackers sold in 2014?

- 10 million
- 40 million
- **70 million**
“If I run on all fours, does this count for more steps?”
Fitness for the Lazy
Other lazy alternatives to fitness

Images courtesy of Rahman et al. *Fit and Vulnerable* - 2013
We can abuse **steps**
Recap’

- We can abuse **steps**
- We can abuse **distance**
Recap’

- We can abuse **steps**
- We can abuse **distance**
- We can abuse calories, very active minutes...
And running?

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

From Kwapisz, Weiss and Moore,
“Activity Recognition using Cell Phone Accelerometers”, SIGKDD 2011
Sitting and standing patterns

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
Why hack steps?

Earn undeserved badges
Why hack steps?

- Earn undeserved badges
  - Affiliation points
- Gift cards
- Discounts
- Pact - Bet
Why hack steps?

- Earn undeserved badges
- Affiliation points
- Gift cards
Why hack steps?

- Earn undeserved badges
- Affiliation points
- Gift cards
- Discounts

Hacktivity 2015 - A. Apvrille
Why hack steps?

- Earn undeserved badges
- Affiliation points
- Gift cards
- Discounts
- Pact - Bet

Hacktivity 2015 - A. Apvrille
“April 13, 2015, Chicago, IL - higi, a leading cloud-based consumer engagement platform that provides trusted partners with ways to more fully engage with their communities around health and wellness, announced today the launching of its industry-leading, privacy-protected and secure API.

...The API will allow higi’s trusted partners, on a user opt-in basis only, to receive health outcomes and activity data from participating users with a higi account.”

Source: Higi Blog - Press Releases
1. We can hack steps, distance etc without opening/compromising
   the tracker
1. We can hack steps, distance etc without opening/compromising the tracker

2. An accelerometer trace provides more information on your activities than you’d think
Recap’

1. We can hack steps, distance etc without opening/compromising the tracker
2. An accelerometer trace provides more information on your activities than you’d think
3. Your fitness data is worth money for you, attackers and the industry
1. We can hack steps, distance etc without opening/compromising the tracker
2. An accelerometer trace provides more information on your activities than you’d think
3. Your fitness data is worth money for you, attackers and the industry

Cyber-criminality fact: Money means Threats
Flex: Communication Protocols

Bluetooth Low Energy
Flex: Communication Protocols

- Bluetooth Low Energy
- HTTP(S)
Talking to the Flex

Hello World!

Two USB interfaces
1. For the dongle
2. For the tracker

Demo
Wrote a Python utility to communicate with the dongle and the tracker
Reverse engineering

Proprietary!

No technical user/developer/contributor documentation

Everything has to be reverse engineered
Reverse engineering

Proprietary!
No technical user/ developer/ contributor documentation
Everything has to be reverse engineered

Achievements

▶ 20 different commands for the dongle:
Get dongle information, disconnect, start discovery, cancel discovery, establish link, toggle pipe...

▶ 24 different commands for the tracker:
Echo, start transmission, display code, handle secret, alert user...

▶ XML communication with the remote servers
How does it work?

Example: Get Dump

Dongle

Get Dump Request

Tracker(s)

C0 10 ...

C0 41 DumpType

Start Dump Response

The dump

The dump

C0 42 dump type, dump size...

End Dump Response

https://github.com/cryptax/fittools
Recap’ - Achievements

1. Get information, status from the dongle
2. Discover trackers nearby
3. Get data to synchronize from the tracker
4. Light LEDs of the tracker

Anything better?
Satisfaction form

http://ftnt.net/1iKyoNn
Can the tracker get infected?

Can it propagate infection to other devices?
Scenario: Fitness Tracker as an Infection Vector

Attacker

Victim’s laptop
Scenario: Fitness Tracker as an Infection Vector

Attacker

INJECTED MALICIOUS CODE

Victim’s laptop

Tracker is infected

Deliver malicious payload: crash, propagate...
Scenario: Fitness Tracker as an Infection Vector

INJECTED MALICIOUS CODE

Victim’s laptop

Tracker is infected

Attacker
Scenario: Fitness Tracker as an Infection Vector

Attacker

INJECTED MALICIOUS CODE

Tracker

is infected

Victim’s laptop

DISCOVERY

MALICIOUS CODE

Deliver malicious payload: crash, propagate...
Scenario: Fitness Tracker as an Infection Vector

INJECTED MALICIOUS CODE

Tracker is infected

DISCOVERY

MALICIOUS CODE

Deliver malicious payload: crash, propagate...

Attacker

Victim’s laptop
Code inject and infect video
1. It’s a PoC: no malicious payload!
Tracker Infection: Limitations

1. It’s a PoC: no malicious payload!

2. Max 17 bytes. Is that enough?
   ▶ Yes. Crash Pentium Trojan (2004): 4 bytes
   ▶ Mini DOS virus (1991): 13 bytes
   ▶ Not enough for an advanced botnet though ;)

Hacktivity 2015 - A. Apvrille
1. It’s a PoC: no malicious payload!

2. Max 17 bytes. Is that enough?
   ▶ Yes. Crash Pentium Trojan (2004): 4 bytes
   ▶ Mini DOS virus (1991): 13 bytes
   ▶ Not enough for an advanced botnet though ;)

3. Execute/Deliver code on target: we did not handle this!
Tracker Infection: Limitations

1. It’s a PoC: no malicious payload!

2. Max 17 bytes. Is that enough?
   - Yes. Crash Pentium Trojan (2004): 4 bytes
   - Mini DOS virus (1991): 13 bytes
   - Not enough for an advanced botnet though ;)

3. Execute/Deliver code on target: we did not handle this!

4. Fitbit patches
Let’s have fun with our tracker

We always lack sources of entropy, don’t we?
Implementing a Tracker RNG

Dongle

Client Challenge

C0 50 LocalRandom

C0 51 TrackerChallenge SeqNum

Auth Chal Resp

Response to Challenge

C0 52 ComputedMAC ...

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

Getting random bytes

$ python rndflex.py -b 256
e3 57 5a d0 00 14 4a b2
25 d3 91 0b 21 5b c1 e4
fd 9e c9 8d e8 c4 9e 90
76 ba 01 1f ba 56 95 19
...
<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><strong>Target</strong></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>
That’s all folks!

Keep it in mind

- It’s easy to fool step & distance count
That’s all folks!

Keep it in mind

- It’s easy to fool step & distance count
- Display Code makes the flex LEDs blink
That's all folks!

Keep it in mind

- It’s easy to fool step & distance count
- Display Code makes the flex LEDs blink
- Sync data is encrypted on the tracker
That’s all folks!

Keep it in mind

- It’s easy to fool step & distance count
- Display Code makes the flex LEDs blink
- Sync data is encrypted on the tracker
- Inject 17 bytes on the tracker
That’s all folks!

Keep it in mind

- It’s easy to fool step & distance count
- Display Code makes the flex LEDs blink
- Sync data is encrypted on the tracker
- Inject 17 bytes on the tracker
- Use your tracker as a hardware RNG
Thanks for your attention!

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

Interesting links
- Galileo - https://bitbucket.org/benallard/galileo
- Fitbit Flex Teardown.
  http://ifixit.org/blog/5042/fitbit-flex-teardown/
- My Fitbit tools repository on GitHub
- Link to satisfaction form: http://ftnt.net/1iKyoNn