

00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 9c 1f da	00001160	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	l0.A(. . .seabi.
00001170	5e 83 e8 1b 3c cc d2 86	79 13 07 1e 4b f4 63 c7	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	[.5TE.
00001180	99 b1 90 b5 9e 46 89 d0	33 4f 0d 0c 1b aa 0e 85	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	[trtab.interp.h
00001190	61 08 a1 9e 99 5e d9 19	f c 81 ba 54 55 05 92 8d	00001180	74 72 74 61 62 00 2e 69	6a 74 65 72 70 00 2e 68	[trtab.interp.h
000011a0	fb 21 24 c2 9b 26 0d 02	22 9a 8a aa 76 2e 1c 8f	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	[ash.dynsym.dyn
000011b0	b4 03 1d 7d 12 3f 0f 6e	54 37 57 c6 4b 76 36 cf	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 20 2e 74 65	[str.rel.plt.tel
000011c0	8d 45 94 9f 42 47 be da	55 c7 63 c0 99 ce a5 77	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	[xt.rodata.preli
000011d0	43 98 ff 2e 50 89 c0 92	1 f 2e a4 af af 96 44 af	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	[nit_array.init.
000011e0	49 36 c2 61 61 66 c6 40	e8 fe 6a 44 2c 54 88 67 d8	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	[annay.fini.Annay
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 19 53 0c 06 0f	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	[c.ctors.dynami
00001200	c f b4 d0 33 46 8e da 73	49 e0 05 ef 9d 9e fc 0c	000011f0	63 00 2e 67 67 74 00 2e	62 73 73 00 2e 63 6f 69	[.got.bss.com
00001210	a3 93 e5 b5 38 79 95 f0	22 43 7f 5c f8 da 12 b6	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	[ment.ARM.attrib
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 86 03 20 01 1e	00001210	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	[utes.ARM.attrib
*			00001220	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001240	76 29 32 26 e6 ee 85 32	02 11 35 44 a4 1f 3a 78				
00001250	36 42 f1 5a 24 86 1f 9e	33 e5 af 82 b3 06 d5 2e	00001240	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 1e 00	
00001260	ea b6 fe 20 c4 b2 44 8d	1f 90 c0 f4 a8 d2 2f 7f	00001250	84 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00	
00001270	16 89 92 ef c5 25 70 ff	9d 06 fb 4b a9 58 ca b2	00001260	01 00 00 00 00 00 00 00	13 2a 00 00 05 00 00 00	
00001280	d3 27 d1 a5 8f 57 d3 70	b2 88 d5 9e 5e 00 39 b4	00001270	02 00 00 00 e8 80 00 00	e8 00 00 00 cc 00 00 00	
00001290	f4 57 33 13 6d 1f 9c	b2 34 e2 a8 5e 93 91	00001280	8f 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	
000012a0	df 9e 38 84 04 9c 1e	88 34 e2 a8 5e 93 91	00001290	8f 00 00 00 00 00 00 00	04 00 00 00 04 81 00 00	
000012b0	f5 0a 83 b4 3a b5 01 83	88 34 e2 a8 5e 93 91	000012a0	8f 00 00 00 00 00 00 00	04 00 00 00 04 81 00 00	
000012c0	c0 24 e7 68 23 75 83 83	1e 8a e2 ad c5 17 ac 56	000012b0	04 00 00 00 10 00 00 00	00 00 00 00 03 00 00 00	
000012d0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	000012c0	02 00 00 00 b4 83 00 00	b4 03 00 00 05 01 00 00	
000012e0	f1 e9 f9 c9 fb e6 2e a5	66 97 71 99 f4 6e c3 88	000012d0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
000012f0	8b 3a b4 33 88 07 9a 84	af ab f8 14 56 1d 40 82	000012e0	29 00 00 00 09 00 00 00	02 00 00 00 bc 84 00 00	
00001300	ef 28 b7 3c 8d c1 a0 08	b7 be 8b fd a2 86 96 73	000012f0	bc 04 00 00 98 00 00 00	03 00 00 00 06 00 00 00	
00001310	e2 c3 87 58 67 9a 9c 81	07 f9 4a b5 94 92 26 67	00001300	04 00 00 00 08 00 00 00	20 00 00 00 01 00 00 00	
00001320	04 b7 46 ea ef 9a 17 04	4d 79 ed 97 d5 95 1e cf	00001310	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00	
00001330	e2 74 73 f4 0a 33 ca c2	4e 10 65 bd b2 09 d2 25	00001320	00 00 00 00 00 00 00 04	04 00 00 00 04 00 00 00	
00001340	64 1b ec dd b8 ab 1e 12	54 79 67 57 67 67 67 67	00001330	00 00 00 00 00 00 00 00	00 00 00 00 50 86 00 00	
00001350	8f 59 1b 80 4a c7 d8 69	e2 84 cc b9 1e 7d 91 de	00001340	10 00 00 00 00 00 00 00	38 00 00 00 01 00 00 00	
00001360	85 a7 31 c2 55 24 de d1	89 64 21 61 62 16 d6 d6	00001350	32 00 00 00 38 89 00 00	38 09 00 00 00 02 00 00	
00001370	a5 55 9f 5e 0b 9a c8 3e	32 15 2b 09 42 c5 53 91	00001360	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00	
00001380	df 6f cf 51 ee 1d 9b c8	35 f9 e6 6f 18 7d 20 29	00001370	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	
00001390	01 09 2a c2 9e 1e 89 93	54 aa a3 84 91 45 f7 95	00001380	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
000013a0	4b 06 11 d8 cb f2 7f 66	54 aa a3 84 91 45 f7 95	00001390	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	
000013b0	5e 1f 5a fa f6 fc bd 05 60	fd d5 6f 1f 6e bc 1a fe	000013a0	01 00 00 00 08 00 00 00	08 10 00 00 08 00 00 00	
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	000013b0	03 00 00 00 08 90 00 00	03 00 00 00 00 00 00 00	
000013d0	93 e2 77 ca 55 ed d0 ba	6e 40 58 08 bf 09 77 8b	000013c0	00 00 00 00 0f 00 00 00	01 00 00 00 00 00 00 00	
000013e0	ex 1d dd 66 67 77 27 1e	2e 4f 4c b5 66 95 79 b6	000013d0	5b 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	
000013f0	0e 3a 48 71 28 81 d6 11	74 48 5e a1 f3 a4 9a 27	000013e0	10 10 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001400	6d 8e 44 52 ea bb c4 42	a5 ba 9e c7 68 1e 1e 1e	000013f0	00 00 00 00 00 00 00 00	07 00 00 00 01 00 00 00	
00001410	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	00001400	00 00 00 00 00 00 00 00	18 10 00 00 08 00 00 00	
00001420	ff c9 33 80 c5 3b 30 33	ca 2e cc cc 0c c7 da 4c	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
00001430	da 21 47 c7 af 03 de e0	8e 2b 8c 91 70 6d db da	00001420	00 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	
00001440	48 f9 9e 18 d8 e8 26 b9	f7 aa 0e 47 01 5c d2 43	00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	
00001450	fd 57 0f ca ee cc c3 df	b2 59 95 15 31 55 d0 51	00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	
00001460	04 b7 46 ea ef ab 9a 17	d4 79 ed 97 d5 95 1e c2	00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	
00001470	4c 8d 75 fc 6c 36 f7	69 66 a5 ad 66 8b e1 8d	00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	
00001480	a5 70 93 47 03 7b 04 98	05 28 8b 0b b7 8b c6 b6	00001470	7e 00 00 00 08 00 00 00	03 00 00 00 40 01 00 00	

Fitness Tracker: Hack In Progress

Axelle Apvrille - FortiGuard Labs, Fortinet

Hack in Paris, June 2015





Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

Reverse engineering

Fun with the tracker

Conclusion



Smart watch

Wearables



Smart watch



Wearable camera

Wearables



Smart watch



Wearable camera



wristbands

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector



Drowsing detector

Don't drowse during my talk !!!

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector

Music beany



Drowsing detector
Don't drowse during my talk !!!

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector



Connected T-shirt



Drowsing detector
Don't drowse during my talk !!!



Music beany

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector



Connected T-shirt



Drowsing detector
Don't drowse during my talk !!!



Augmented reality glasses



Music beany

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector



Connected T-shirt



Drowsing detector
Don't drowse during my talk !!!



Augmented reality glasses



Music beany



Connected shoes

Wearables



Smart watch



Wearable camera



wristbands



Skin exposure detector



Connected T-shirt

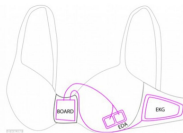
**And many others: smart helmets, smart pants
smart socks**



**Drowsing detector
Don't drowse during my talk !!!**



Augmented reality glasses



Smart bra



Music beany



Connected shoes



Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

Reverse engineering

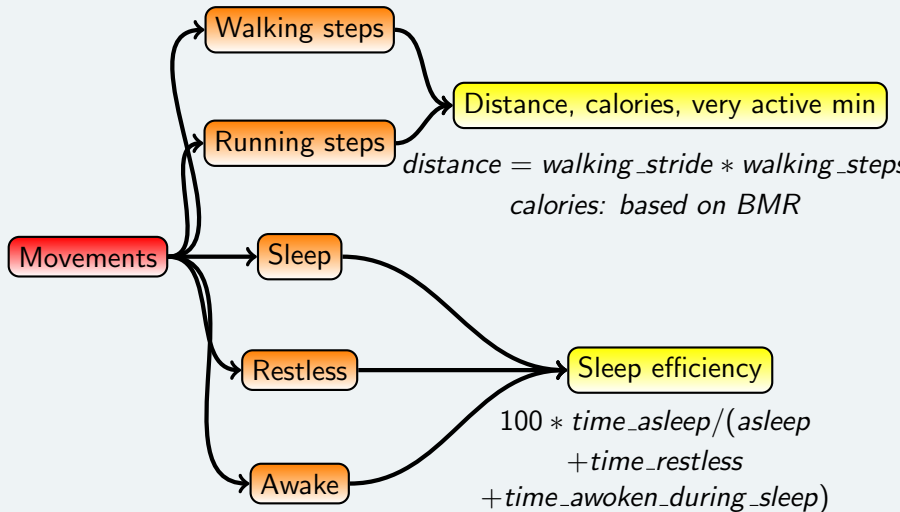
Fun with the tracker

Conclusion



- ▶ ST Microelectronics [32L151C6](#)
- ▶ Nordic Semiconductor [nRF8001](#) for **Bluetooth Low Energy** v4.0
- ▶ ST Microelectronics [LIS2DH](#) tri-axial **accelerometer**
- ▶ TI [BQ24040](#) **battery** Li-Pol charger
- ▶ **No altimeter, no GPS** on Flex. Only on Charge or Surge.

How does it work? (reverse engineered)



Prior issues: default privacy settings of user profiles

Google

"sexual activity" site:fitbit.com

About 199 results (0.05 seconds) Advanced search

Everything **Fitbit Profile**

www.fitbit.com/user/22DP9H/activities - Cached
Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 1:00 am. N/A 45 minutes 70 ...

Activities - Fitbit Profile

www.fitbit.com/user/22B6GD/activities/date/2010-11-14 - Cached
Nov 14, 2010 - Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 12:00 am. N/A 30 minutes 37 ...

Fitbit Profile

www.fitbit.com/user/222ZN6 - Cached
May 31, 2011 - **Sexual Activity**. General, moderate effort. started at 10:45 pm. N/A 20 minutes 36. Total N/A 20 minutes 36 ...

Activity Records Sat Jun 18 10:10:00 UTC 2011 See ... - Fitbit Profile

www.fitbit.com/user/223C7F - Cached
Jun 20, 2011 - **Sexual Activity**. Active, vigorous effort. started at 11:30 pm. N/A 1 hour 30 minutes 191. Total N/A 1 hour 30 minutes 191 ...

Activities - Fitbit Profile

www.fitbit.com/user/227QSS/activities
Feb 2, 2011 - **Sexual Activity**. Passive, light effort, kissing, hugging. N/A 10 minutes 9 ...
Sexual Activity. Active, vigorous effort. N/A 15 minutes 21 ...

Overall - Fitbit Profile

www.fitbit.com/user/22C10E - Cached

Wait, how can the Fitbit Flex track sexual activity?!



There's only an accelerometer!
How does it the tracker know what I'm doing?
It does not. You enter it manually on the website.

List of activities

Sexual activity - vigorous effort - 105 calories per hour

Cooking Indian bread on an outside stove - 211 calories per hour

Vacuuming - 246 calories per hour

Horse grooming - 422 calories

Those precise categories *no longer exist* (add manually)

The issue is fixed

1 result (0.28 seconds)

Activity Directory - Fitbit

www.fitbit.com/fitness/directory/s ▼

Sexual Activity. This is a fake description of the activity which is quite long so it does not fit into the box and the excess is cut off. This is a fake description of the ...

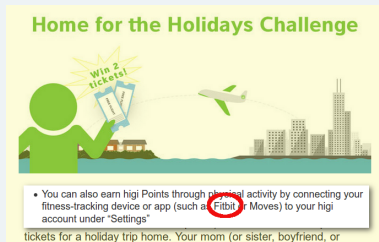
Quick fix the next day

Prevent access to user profiles by search engines
+ erased from Google, Yahoo and Bing

Other prior issues:

- ▶ **Clear text login information.** In HTTP POST data.
- ▶ **No consistency check, no authentication, no encryption in sync protocol.**

Set dummy values on tracker or account - yours or someone's else. Earn undeserved awards and profit.

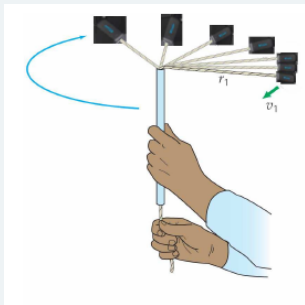


See *Rahman et al. Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device, 2013.*

Good news

No longer work - *I've checked ;)*

Known (but not so nasty) issues that still work



Images courtesy of Rahman et al. *Fit and Vulnerable* - 2013

- ▶ **Abusing physical sensors.** Shaking firmly towards the ground. Or attach to a rope. Or to a car wheel.

Still works

I tested: 50 spins is approx 40 steps.

Bluetooth tracking:

- ▶ LightBlue on iOS, Bluetooth Finder on Android.
- ▶ [Blueberry sniffer](#) (Raspberry Pi based).

Used to find lost devices

Found my FitBit ★★★★★

by OMG — it works!

Had my Fitbit for only 2 days. Not yet top of mind to remember where I put it. Searched for 3 hours in my house. I knew it was at home because my iPhone was syncing with it in various parts of the house. Could not narrow it down enough until I used this app. It was in my walk-in closet, but where? Looked through laundry basket, shoes, the clothes I wore last. It was attached to the

[...More](#)

Hack your tracker: why?

New Fitbit trackers have been significantly **locked up**:

- ▶ If Fitbit servers are down... your trackers are *useless*
 - ▶ You can't read your own walking or running steps
 - ▶ You can't set an alarm
 - ▶ You can't sync...
- ▶ No support besides **Mac** and **Windows**
- ▶ What are the trackers transmitting *about us*?
- ▶ Should we become concerned by the possibility of trackers getting *infected*?





Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

Reverse engineering

Fun with the tracker

Conclusion

Proprietary!

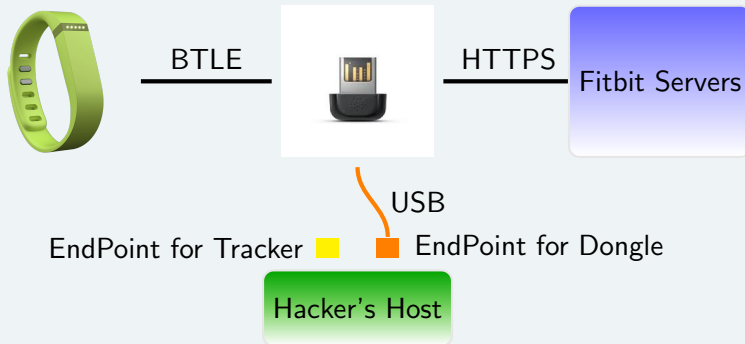
No technical user/ developer/ contributor documentation

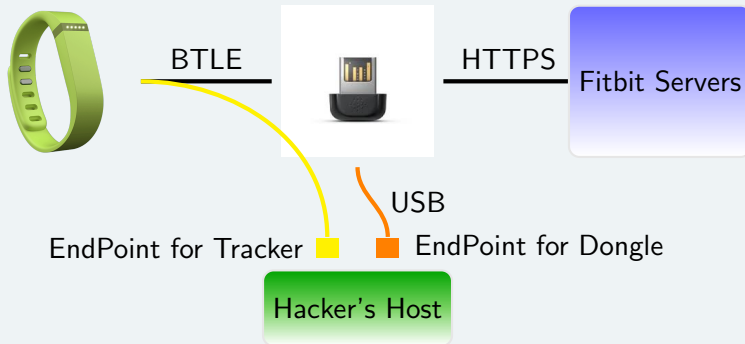
Everything has to be reverse engineered

What do we have to start with?

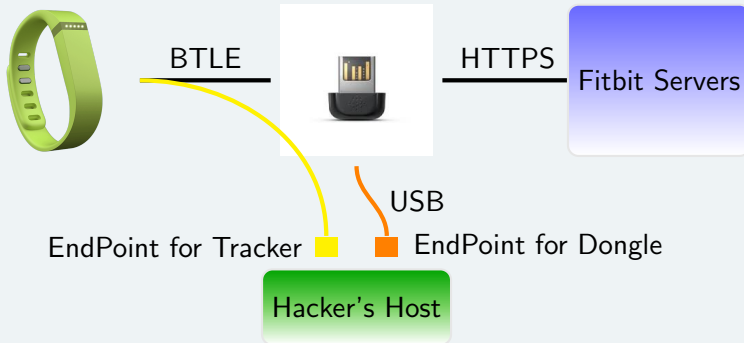
- ▶ **Product Manual**: high level user manual
- ▶ **Ben Allard's** Python utility to sync Flex ([Galileo](#))
- ▶ A few (incomplete) notes: [Sam Marshall](#), [RAThomas](#)
- ▶ My choice: **software** analysis only - "black box analysis"

**This is "hack in progress": still much work to do.
Feel free to join.**

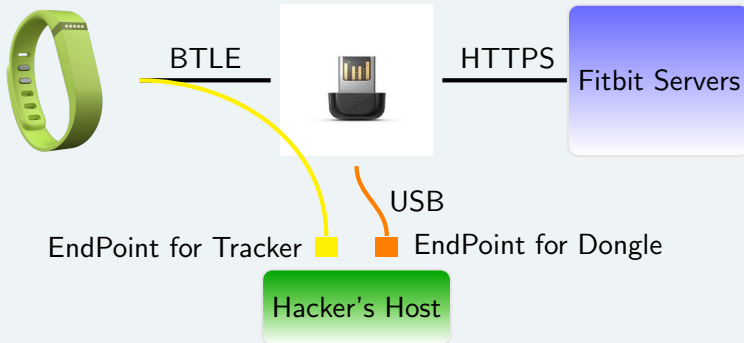




Data



Encrypted Data



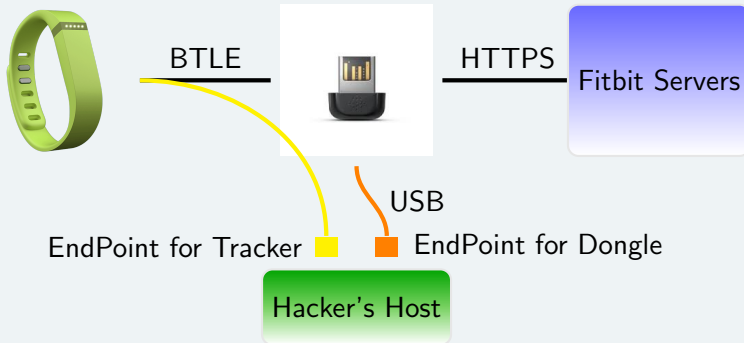
Encryption

Data is encrypted on the **tracker**

Decrypted on Fitbit Servers

Dongle does not encrypt/decrypt

Encrypted Data → Encapsulated in XML



Encryption

Data is encrypted on the **tracker**

Decrypted on Fitbit Servers

Dongle does not encrypt/decrypt

Encrypted Data → Encapsulated in XML → Decrypted Data



BTLE



HTTPS



Fitbit Servers

USB

EndPoint for Tracker



EndPoint for Dongle

Hacker's Host

Encryption

Data is encrypted on the **tracker**

Decrypted on Fitbit Servers

Dongle does not encrypt/decrypt



Reversed

- ▶ 16 dongle messages
- ▶ 24 tracker messages
- ▶ XML communication between client and server

Reversed

- ▶ 16 dongle messages
- ▶ 24 tracker messages
- ▶ XML communication between client and server

What we don't have

Encryption algorithm used between tracker and server



Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

Reverse engineering

Fun with the tracker

Conclusion



- ▶ USB HID claims the dongle (lsusb)
- ▶ You need to **unclaim** it:

```
import usb.core
import usb.util
import sys

idVendor=0x2687
idProduct=0xfb01
dev = usb.core.find(idVendor=idVendor, idProduct=idProduct)
for interface in range(0,2):
    usb.util.release_interface(dev, interface)
```

<https://bitbucket.org/benallard/galileo>

Python utility to synchronize the tracker

```
./run --no-upload --dump --force --no-https-only -d
```

Small interactive mode

```
./run interactive  
> c ; d ; l ; tx 1 ; al; => c0 10 03;  
<=
```

Linux tools: Wireshark + usbmon

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
8	7.193858000	3.0	host	USB	65	GET_CONFIGURATION Response
9	7.193950000	host	3.0	USB	64	SET_CONFIGURATION Request
10	7.194482000	3.0	host	USB	64	SET_CONFIGURATION Response
11	7.194763000	host	3.2	USB	66	URB_INTERRUPT out
12	7.195995000	3.2	host	USB	64	URB_INTERRUPT out
13	7.196206000	host	3.2	USB	64	URB_INTERRUPT in
14	7.198981000	3.2	host	USB	96	URB_INTERRUPT in
15	7.199094000	host	3.2	USB	64	URB_INTERRUPT in
16	7.202985000	3.2	host	USB	96	URB_INTERRUPT in
17	7.203089000	host	3.2	USB	64	URB_INTERRUPT in
18	9.206205000	3.2	host	USB	64	URB_INTERRUPT in
19	9.206406000	host	3.2	USB	66	URB_INTERRUPT out

USB_URB

- USB id: 0xffff8b01917fd5c0
- USB type: URB_COMPLETE ('C')
- USB transfer type: URB_INTERRUPT (0x01)
- Endpoint: 0x82, Direction: IN
- Device: 3
- USB bus id: 1
- Device setup request: not relevant ('')
- Data: present (0)
- URB sec: 1403614508
- URB usec: 888193
- URB status: Success (0)
- URB length [bytes]: 32
- Data length [bytes]: 32
- [request in: 13]
- [Time from request: 0.002775000 seconds]
- [InterfaceClass: Unknown (0xffff)]

Leftover Capture Data: 200143016e63056c446979636f76657279000000000000...

```
0000 c0 05 7f 91 01 88 ff ff 43 01 82 03 01 00 2d 00 ..... C.....
0010 2c 75 a9 53 00 00 00 00 81 8d 0d 00 00 00 00 00 ..U.S.....
0020 20 00 00 00 20 00 00 00 60 00 00 00 00 00 00 00
0030 02 00 00 00 00 00 00 00 00 02 00 00 00 00 00
0040 20 01 43 61 6e 63 05 6c 44 69 73 63 6f 76 05 72 ..Cancel Discover
0050 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Padding added by the USB capture ... Profile: Default

```
tshark -r file.pcap -T fields -e usb.capdata
```



- ▶ **Connect device.**

```
device = usb.core.find(idVendor=0x2687, \  
                        idProduct=0xfb01)
```

- ▶ **Send data** to tracker/dongle.

```
device.write(endpoint, data, timeout)
```

- ▶ **Read responses** from tracker/dongle. 32 bytes at most.

```
response = device.read(endpoint, length, timeout)
```

- ▶ **Exhaust in pipe:** loop on read until USB error occurs (must not be timeout error)

- ▶ **Be patient:** some requests are slow. Set correct timeouts.

- ▶ **Handle exceptions/errors:** e.g `usb.core.USBError`

Reverse engineering and fuzzing

- ▶ Fuzz all possible **command identifiers** with dummy payload length 0-30
- ▶ **Invalid messages** like get bad dump type, or bad toggle pipe

What did we find?

- ▶ Many details on packets' format: command identifier on 7 bits only, error code...
- ▶ Unknown commands
- ▶ Vulnerabilities (Responsible Disclosure)



Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

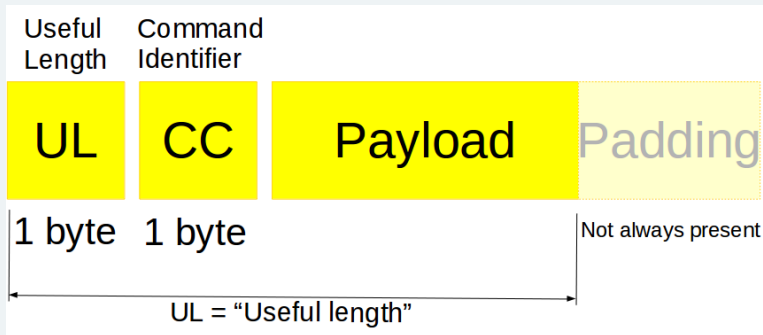
Reverse engineering

Fun with the tracker

Conclusion

Dongle messages

- ▶ Endpoints 0x02 (incoming for dongle), 0x82 (outgoing)
- ▶ Variable length



- ▶ Padding with zeros may or may not be present.
- ▶ Useful Length (UL) does not consider padding.

Known dongle requests (EP 0x02)

02 01	Get Dongle Information Request
02 02	Disconnect
1a 04 PP ..	Start Discovery
02 05	Cancel Discovery Request
0b 06 PP ..	Establish Link Request
02 07	Terminate AirLink Request
03 08 PP	Toggle Tx Pipe Request
11 12 PP ..	Establish Link Ex

Known dongle responses (EP 0x82)

Format	Padded?	Description
20 01 PP ..	✓	Information message
03 02 PP	✓	Finished Discovering Trackers
13 03 PP ..	✓	Tracker Discovered
03 04 PP ..		Establish Link Response
03 05 PP ..		Link Terminated Response
08 06 PP ..	✓	Test Air Link Response
02 07		(Establish Link?) Confirmed
15 08 PP ..	✓	Dongle Information Response

We won't detail all of them ;)



Drowsing detected ;)

Example of dongle message flow

Host

Dongle

Get Dongle Info Req

02 01

02 = Length of message

01 = Command Id for Get Dongle Info

15 08 MAJ MIN...

Get Dongle Info Resp

15 08 MAJ MIN dd dd dd dd

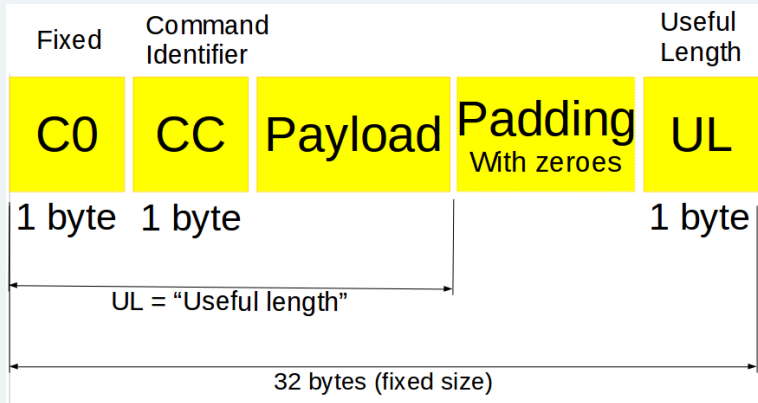
dd dd 74 04 00 02 00 00

ff e7 01 00 02 Zeroes

- ▶ Major (1 byte)
- ▶ Minor (1 byte)
- ▶ Dongle MAC address (6 bytes)
- ▶ Remaining seems to be fixed?

Tracker messages

- ▶ Endpoints 0x01 (received from tracker), 0x81 (sent to tracker)
- ▶ Fixed length
- ▶ Padded with zeroes up to 32 bytes



Messages sent to tracker (EP 0x01)

C0 01 -- ... 02	Reset Link
C0 04 PP ... 03	Handle secret (clear or display)
C0 05 -- ... 02	Alert user request
C0 06 -- ... 02	Display code (on the tracker)
C0 09 PP ... UL	Echo Request
C0 0a PP ... 0c	Initialize Air Link
C0 10 PP ... 03	Get Dump Request
C0 24 PP ... 09	Start Transmission
C0 50 PP ... 0a	Client Challenge
C0 52 PP ... 0a	Authentication Response

Messages received from tracker (EP 0x81)

C0 01 -- ... 02	Reset Link Response
C0 02 -- ... 02	Ack Response
C0 03 PP ... 04	Error Code Response
C0 05 -- ... 02	Alert user response
C0 08 -- ... 02	User Activity
C0 09 PP ... UL	Echo Response
C0 0b -- ... 02	Toggle Pipe Response
C0 12 PP ... 05	First Ack Block Response
C0 13 PP ... 05	Ack Block Response
C0 14 PP ... 0c	Air Link Initialized Response
C0 40 PP ... UL	Single block packet response
C0 41 PP ... 03	Start of Dump
C0 42 PP ... 09	End of Dump
C0 51 PP ... 0e	Tracker Challenge

We'll detail every each of them



We'll detail every each of them

No - I'm joking :)

Let's only have a look at how to sync (Get Dump)

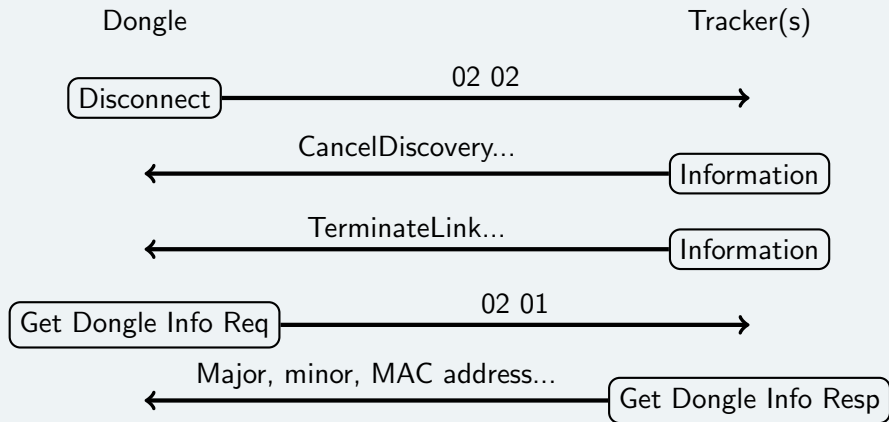


I'm watching those who drowse ;)

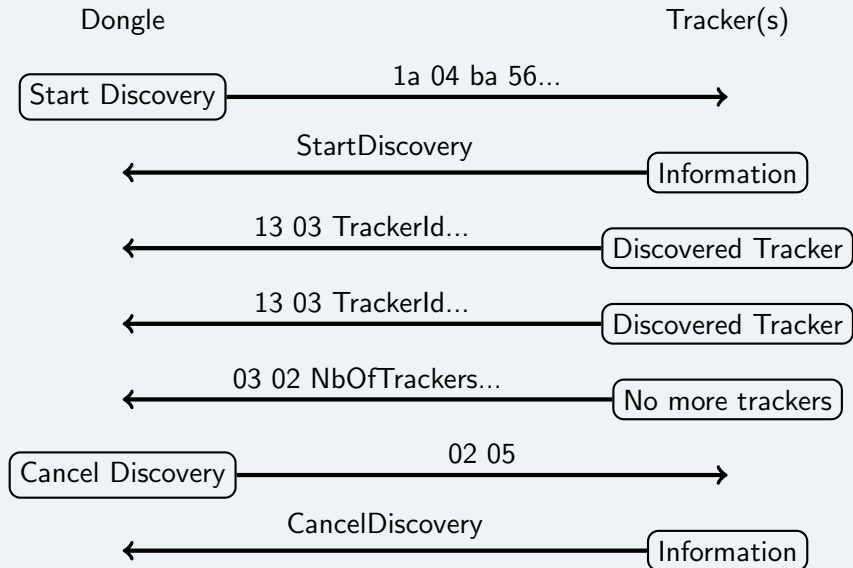
Setting up communication with tracker 1/4



- ▶ Disconnect. Clean up current state
- ▶ What's my dongle? Get Dongle Information



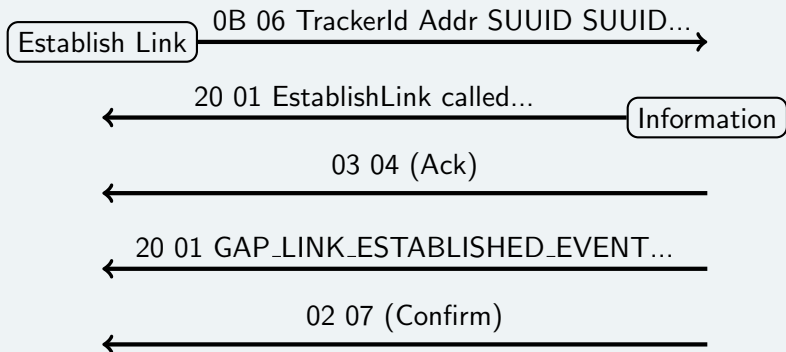
Communication setup 2/4: discovery



Communication setup 3/4: establish link

Dongle

Tracker(s)

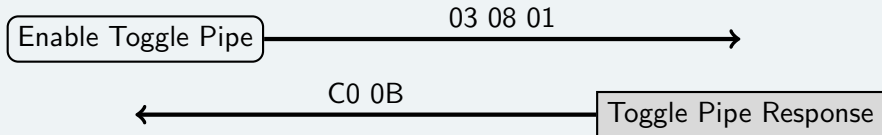


Communication setup 4/4: switch to tracker

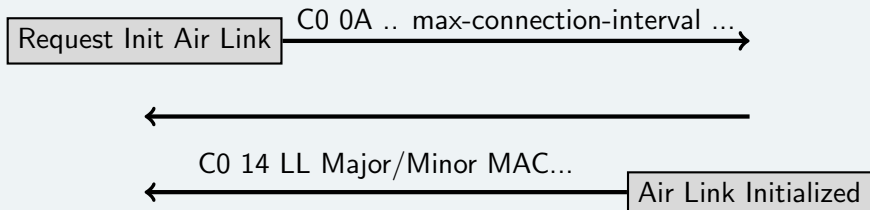
Enable (01) Pipe:

Dongle

Tracker(s)

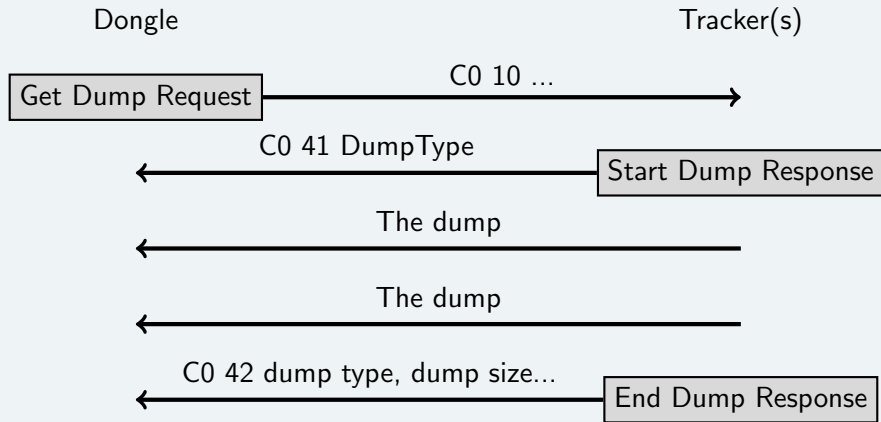


Init Air Link:





- ▶ **Disconnect** - to clean up.
- ▶ What's my dongle? get dongle info.
- ▶ **Discover** trackers.
- ▶ **Establish link** with a given tracker.
- ▶ **Switch** to communication with tracker
- ▶ Initialize **air link** with tracker
- ▶ Optional: authentication handshake



If dump holds in a single packet, c0 40 DumpType Dump ... UL

Different messages

- ▶ Megadump (0xd): tracker data sync
- ▶ Microdump (0x3): e.g requesting an update, pairing
- ▶ Megadump responses (0x4) (sent by server) e.g alarms sync
- ▶ Microdump responses (0x1) (sent by server) e.g updates

Megadump format

TT 02 00 00 01 00 SS SS SS SS MM MM MM MM MM MM

Encrypted ...

- ▶ **Device type.** Flex 0x28, 0xf4 is Zip, 0x26 is One
- ▶ **Sequence counter.** 4 bytes. Little Endian.
- ▶ **Model identifier** 6 bytes. Flex: D2 C0 56 2E 15 07 or C9 9B F8 2D 15 07 One: 7B 2E 9F 2B 2D 05 or 7B 16 E4 2A 2A 05 (old).
- ▶ Encrypted blob starts at offset 17 (0x11)

Example of megadump

```
28 02 00 00 01 00 7B 11 00 00 D2 C0 56 2E 15 07 08 5E E7 FC
93 83 83 D1 AE 8C 4D E7 D8 F6 B0 32 F5 41 29 EC D5 26 D5 A9
27 F1 A2 17 26 BC 51 4B 66 FA 08 39 6A 7B 07 60 02 5B CC 05
5D E7 3B F8 8B 33 28 6A EA 3B C7 9E C8 22 D5 A7 EA E4 4D A4
68 AB 09 8E D0 AE A7 04 6D CB 42 CC 8C 73 D1 05 47 C8 CD D3
11 01 E6 A3 EA EC 0F F8 44 43 0A 29 E3 24 4F B7 6A 14 BC 0E
33 DD B5 7C 7D F4 6F 49 84 CC BE B2 DE B6 B6 AA 99 8F F5 26
4A 5B 5C 74 65 16 B0 78 87 2A BA 4E 13 FD 75 C4 3B 8A D2 E5
90 60 67 2D 46 07 7A 4F EE 7E 19 56 29 91 D0 98 B8 FF 2A 5A
88 16 4D 9F 79 56 72 BE CD AC CE F0 B1 D0 46 06 24 CD 82 EB
88 AC D6 2A 3A 72 E1 BE 05 E3 A6 5A C8 E8 85 F6 F1 43 55 A5
A7 13 98 E7 F9 4E B3 87 FF 61 9E 94 94 A3 00 4A AE A9 0D D9
87 3D B2 D8 A4 7C 08 35 D7 50 17 9A 9A F4 4F D4 AD D2 09 5C
51 05 36 AE 61 DB 4A FB 60 9E 1E D9 6D 90 65 D5 1D 79 85 A1
02 B4 91 A2 ED E2 B0 60 60 1A 12 9F EC 91 FD CC 21 AE 80 A9
02 C7 C8 18 E8 3F 8C F7 DC 90 99 32 14 01 00
C0 42 0D B9 03 3B 01 00 00
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<galileo-client version="2.0">
...
  <tracker tracker-id="DEADBEEF0000" type="megadump">
    <data>
      Base 64 dump ...
    </data>
  </tracker>
</galileo-client>
```

What algorithm???
(and what key...)

- ▶ Megadump size different at each sync (1836 bytes, 1859(+23), 1877(+18), 1900(+23), 1915(+15)...)
- ▶ Differential cryptanalysis: ciphertext-only attack
- ▶ Hardware inspection? JTAG?
- ▶ Any other idea?

Guessing the algorithm

- ▶ STM32L151 does not support AES, only STM32L162...
- ▶ Yet, AES (or other) can be used and not accelerated by hardware
- ▶ Authenticity: XTEA-CMAC or AES-CMAC (Surge)
- ▶ Encryption: XTEA?



Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

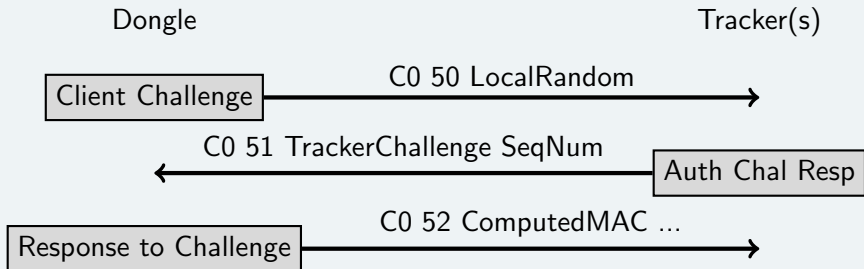
Reverse engineering

Fun with the tracker

Conclusion

Fitbit tracker as source of entropy?

Use authentication packets:



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

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
...
```

- ▶ Entropy 7.72: ok
- ▶ Source code: <https://github.com/cryptax/fittools>



Background on Wearables

Background on Fitbit Flex

Architecture

Hacking Tools

Reverse engineering

Fun with the tracker

Conclusion

Thanks for your attention!



Contact info

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

More fun

There's still lots to do:

- ▶ Control the LEDs on the tracker
- ▶ Make the tracker vibrate
- ▶ Fuzz the dongle, fuzz the server
- ▶ Algorithm for dumps?