The Most Interesting Bits From Sniffing Bluetooth the Last 3 Years

Xeno Kovah
OpenSecurityTraining2 &
Dark Mentor LLC

About Me

- 75% of my time is spent making free (as in beer), open access, and *open source* (CreativeCommons licensed) classes for a non-profit I started, **OpenSecurityTraining2 (ost2.fyi)**

About Me

- 75% of my time is spent making free (as in beer), open access, and *open source* (CreativeCommons licensed) classes for a non-profit I started, **OpenSecurityTraining2 (ost2.fyi)**

- 25% of my time doing consulting and research for **Dark Mentor LLC**
  - The research is for fun, but is *also a trojan horse* to get me into conferences to tell you about OST2 ;)

OST2 Crew

In order of appearance

Xeno Kovah

Arch1001 ~28 hours, Arch2001 ~27 hours
Arch4001 ~14 hours, HW1101 ~6 hours
Vulns1001 ~15 hours, Vulns1002 ~23 hours

Piotr Król

Arch4021 ~6 hours
Arch4031 ~6 hours

Michał Żygowski

Arch4021 ~6 hours

Thaís Moreira Hamasaki

RE3201 ~6 hours

Gal Zaban

RE3011 ~6 hours

Kc Udonsi

Vulns1001 ~15 hours

Cedric Halbronn

Dbg3011 ~6 hours
Arch2821 ~5 hours
Exp4011 ~33(!) hours

Sina Karvandi

Dbg3301 ~16 hours

What I Want To Know:

What Bluetooth Chip Is Inside Any Device

nest

TEXAS INSTRUMENTS

BROADCOM®

SILICON LABS®

?

Why I Want To Know It:

So I Know If It's Vulnerable To A Firmware-Level Exploit

Texas Instruments

Silicon Labs

Broadcom

ARMIS®

TEXAS INSTRUMENTS

SILICON LABS®

BROADCOM®

ARMIS®

TEXAS INSTRUMENTS

SEMO
SECURE MOBILE NETWORKING

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

SEMO

SECURE MOBILE NETWORKING

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

SEMO

SECURE MOBILE NETWORKING

BROADCOM®

DARK MENTOR

SILICON LABS®

How Am I Going To Figure It Out?

1) Know That I Know Nothing 😏
2) Do A Bunch Of Naive BT Data Collection
3) Find Out What I Don't Know

Hardware

By price & capability

Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT

Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT

- Raspberry Pi 4 Model B - $35/$45/$55
  - 1/2/4GB RAM, 1.5GHz 64-bit quad-core ARM Cortex-A72 CPU (BCM2711) + CYW 43455 BT/WiFi

Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT

- Raspberry Pi 4 Model B - $35/$45/$55
  - 1/2/4GB RAM, 1.5GHz 64-bit quad-core ARM Cortex-A72 CPU (BCM2711) + CYW 43455 BT/WiFi
- BeagleBone Black Wireless - $72 (when I got it. Now $111 but out of stock)
  - .5GB RAM, 1GHz ARM Cortex-A8 + TI WL1385
  - **Antenna connector!**

Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT

- Raspberry Pi 4 Model B - $35/$45/$55
  - 1/2/4GB RAM, 1.5GHz 64-bit quad-core ARM Cortex-A72 CPU (BCM2711) + CYW 43455 BT/WiFi
- BeagleBone Black Wireless - $72 (when I got it. Now $111 but out of stock)
  - .5GB RAM, 1GHz ARM Cortex-A8 + TI WL1385
  - **Antenna connector!**

Hardware

What collects more?

vs.

- Test 1: Pi Zero & Pi 4b in parallel
  - Pi0 = **113**, Pi4b = 65 *named devices*

vs.

- Test 2: Pi 4b & Beagle Bone Black Wireless in parallel
  - Pi4b == BBBW == 422 *named devices*

Hardware

What collects

vs.

- Test 1: Pi Zero & Pi 4b in parallel
  - Pi0 = **113**, Pi4b = 65 *named devices*

vs.

- Test 2: Pi 4b & Beagle Bone Black Wireless in parallel
  - Pi4b == BBBW == 422 *named devices*

Run-time on Battery

Model	Runtime	RAM
rPi Zero W .5GB	90h 2m	.5 GB
BeagleBone Black W .5GB	55h 16m	.5GB
rPi 4B 1GB	21h 51m	1GB
rPi 4B 4GB	21h 21m	4GB

Run-time on Battery

Model	Runtime	RAM
rPi Zero W .5GB	90h 2m	.5 GB
BeagleBone Black W .5GB	55h 16m	.5GB
rPi 4B 1GB	21h 51m	1GB
rPi 4B 4GB	21h 21m	4GB

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

https://github.com/darkmentorllc/naiveBTsniffing

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

- v.0001 - Bash scripts around Linux CLI tools!

https://github.com/darkmentorllc/naiveBTsniffing

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

- v.0001 - Bash scripts around Linux CLI tools!
  - 99% of my data - Python scripts to analyze!

https://github.com/darkmentorllc/naiveBTsniffing

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

- v.0001 - Bash scripts around Linux CLI tools!
  - 99% of my data - Python scripts to analyze!
- v.001 - C-based BlueZ DBus-based API + MySQL DB
  - Only made this around Feb 2023, captures incomplete data compared to bash scripts! I basically don't even use this anymore, so I didn't release it. Someday I will make it good enough to be my primary mechanism... 🤔

https://github.com/darkmentorllc/naiveBTsniffing

Background - *BT Device Address (BDADDR)*

BT Classic Addresses

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

BT Classic Addresses

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

BT Classic Addresses

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

BT Classic Addresses

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

BT Classic Addresses

00:1f:ff:5f:0d:5a

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

BT Classic Addresses

00:1f:ff:5f:0d:5a
(00:1f:ff): Respironics, Inc.

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT De*

Random Static Addresses can be used in one of two ways:

- It can be assigned and fixed for the lifetime of the device
- It can be changed at bootup

However, it **cannot** be changed during runtime.

The format of Random Static Addresses looks like this:

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Minimally Trackable *(in principle)*
(Possibly trackable using device-specific data (e.g. names))

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *E*

A Resolvable Random Private address is made up of the following fields:

Random Private Resolvable Address format (little-endian format)

- 0 and 1 are fixed in the most significant bits (MSB)
- The next 22 bits are randomly generated
- The **prand** constitutes of these most significant 24 bits
- The lower 24 bits represent a hash value which is generated using the **prand** and the **IRK**

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Minimally Trackable *(in principle)*
(Possibly trackable using device-specific data (e.g. names))

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Minimally Trackable *(in principle)*
(Possibly trackable using device-specific data (e.g. names))

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

Minimally Trackable *(in principle)*
(Possibly trackable using device-specific data (e.g. names))

Minimally Trackable *(in principle)*
(Have to use device-specific data)

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT D*

The format of Non-Resolvable Random Private Addresses is as follows:

Random	0	0
46 bits		

Random Private Non-Resolvable Address format (little-endian format)

- 0 and 0 are fixed in the most significant bits (MSB)
- The remaining 46 bits are chosen at random

Minimally Trackable *(in principle)*
(Possibly trackable using device-specific data (e.g. names))

Minimally Trackable *(in principle)*
(Have to use device-specific data)

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

```
> HCI Event: LE Meta Event (0x3e) plen 37
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Public (0x00)
      Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
      Data length: 25
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      Name (complete): Triones-FFFFEA003484
      RSSI: -83 dBm (0xad)
```

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

```
> HCI Event: LE Meta Event (0x3e) plen 37
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connecta[illegible]ected - ADV_IND (0x00)
      Address type: Public
      Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
      Data length: 25
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      Name (complete): Triones-FFFFEA003484
      RSSI: -83 dBm (0xad)
```

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

```
> HCI Event: LE Meta Event (0x3e) plen 37
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Public (0x00)
      Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
      Data length: 25
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      Name (complete): Triones-FFFFEA003484
      RSSI: -83 dBm (0xad)
```

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

```
> HCI Event: LE Meta Event (0x3e) plen 37
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Public (0x00)
      Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
      Data length: 25
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      Name (complete): Triones-FFFFEA003484
      RSSI: -83 dBm (0xad)
```

Congrats! Your car can now be tracked by its headlights!

TellMeEverything.py

- If you see output like the below in this presentation, it's from my script I've written for analyzing my analyzing log data once it’s inserted into mysql

```
DeviceName: AP 000722ED 0E96AAC1000E09F2
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
```

TellMeEverything.py

- If you see output like the below in this presentation, it's from my script I've written for analyzing my analyzing log data once it’s inserted into mysql

```
DeviceName: AP 000722ED 0E96AAC1000E09F2
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
```

TellMeEverything.py

- If you see output like the below in this presentation, it's from my script I've written for analyzing my analyzing log data once it’s inserted into mysql

```
DeviceName: AP 000722ED 0E96AAC1000E09F2
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
```

Congrats! You can now be tracked by your diabetes-management device

WiGLE

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

WiGLE

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

Discovered + : 21,443
Seen **Networks:** 52,109
this month / last month with : 103 / 653

Discovered + : 380
Seen : 877
Discovered + : 706187
Seen : 764234

WiGLE

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

Discovered + : 21,443
Seen Networks: 52,109
this month / last month with : 103 / 653

Order of magnitude more BT than WiFi!

Discovered + : 380
Seen : 877
Discovered + : 706187
Seen : 764234

WiGLE

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

Discovered + : 21,443
Seen **Networks:** 52,109
this month / last month with : 103 / 653

Order of magnitude more BT than WiFi!

Discovered + : 380
Seen : 877
Discovered + : 706187
Seen : 764234

"Currently, the actual number of Bluetooth radios in use is four times higher than the number of Wi-Fi radios deployed." - Herfurt & Mulliner, "Blueprinting" 2004

Begin - Anecdotes - Locations

Across the USA - Pandemic Cannonball Run!

Across the USA - Pandemic Cannonball Run!

Las Vegas

RingZer0.Training & DEF CON 2023

Las Vegas

RingZer0.Training &

Las Vegas

RingZer0.Training &

Las Vegas

RingZer0.Training &

Las Vegas

RingZer0.Training 2023 @ Palms

- Regex: ^PayRange$ but also ^BlueRadios[A-F0-9]{6}$ but also ^BluKeyPayRange$
  - Semantically: the [A-F0-9]{6} are the last 6 digits of the BDADDR
- Device would advertise as PayRange but send back e.g. BlueRadios169B67 when asked what its name is. Some would also reply "BluKeyPayRange"

https://shop.payrange.com/industries/vending/

Background

Passive Scanning

Active Scanning

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Background

Passive Scanning

Sometimes the name will be here

Active Scanning

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Background

Passive Scanning

Sometimes the name will be here

Active Scanning

Other times you need to ask for it, and it comes back in the SCAN_RSP

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Las Vegas

RingZer0.Training 2023 @ Palms

- Regex: ^PayRange$ but also ^BlueRadios[A-F0-9]{6}$ but also ^BluKeyPayRange$
  - Semantically: the [A-F0-9]{6} are the last 6 digits of the BDADDR
- Device would advertise as PayRange but send back e.g. BlueRadios169B67 when asked what its name is. Some would also reply "BluKeyPayRange"

https://shop.payrange.com/industries/vending/

Las Vegas

RingZer0.Training 2023 @ Palms

- Regex: ^PayRange$ but also ^BlueRadios[A-F0-9]{6}$ but also ^BluKeyPayRange$
  - Semantically: the [A-F0-9]{6} are the last 6 digits of the BDADDR
- Device would advertise as PayRange but send back e.g. BlueRadios169B67 when asked what its name is. Some would also reply "BluKeyPayRange"

https://shop.payrange.com/industries/vending/

How It Works

ayRange$

67 when asked what

uKey for
ending

LIMITED TIME OFFER!
OFFER ENDS AUGUST 31

~~9.00~~ $49.95

ble options:

uct Assurance Plan – $4.99

selection

$54.94

Las Vegas

RingZer0.Training 2023 @ Palms

- Uses "BlueRadios, Inc." *bluetooth module* based on its (public) BDADDR and manufacturer-specific data
  - Which is actually just a Nordic NRF52840 chip

```
For bdaddr = ec:fe:7e:16:5d:f1:
        Company Name by IEEE OUI (ec:fe:7e): BlueRadios, Inc

        No BTC Extended Inquiry Result Device info.

        DeviceName: PayRange
                In BT LE Data (LE_bdaddr_to_name), bdaddr_ranc
                        NamePrint: match found for ^PayRange$:
                This was found in an event of type 19 which cc

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0085  BlueRadios, Inc ) -
```

https://www.blueradios.com/nBlue%20BR-LE5.0-S1A%20Summary%20Datasheet.pdf

Las

RingZ

- Uses
  manu
  - Wh

```
For bdaddr = ec:fe
        Company Na

        No BTC Ext

        DeviceName
                In

                Th

        No UUID16s

        No transmi

        No Appeara

        Manufactur
                De
```

https://www.blueradios.

*n*Blue BR-LE5.0-S1A Module Summary Datasheet
Copyright © 2002-2021 BlueRadios, Inc.
v1.3

BT5.0 Low Energy Single Mode Class 1 SoC Module

*n*Blue™ BR-LE5.0-S1A (nRF52840)

- ***AT HOME. AT WORK. ON THE ROAD.*** ***USING BT5.0 LOW ENERGY WIRELESS TECHNOLOGY MEANS TOTAL FREEDOM FROM THE CONSTRAINTS AND CLUTTER OF WIRES IN YOUR LIFE.***
- **FCC, IC, CE, RoHS, and BT5.0 Certified ISM 2.4GHz module supporting BT5.0 high speed mode, long range mode and advertising extensions. Can also support BT5.0 Mesh, 802.15.4 for Thread and Zigbee, ANT or proprietary 2.4Ghz.**
- **Utilizes the Nordic nRF52840 SoC. 64Mhz ARM® Cortex™ M4F 32-bit processor with FPU, 1MB Flash, 256K RAM, built in DC-DC converter and ARM CryptoCell cryptographic accelerator.**
- **Programmable output power from -40dBm to +8dBm for short to long range applications.**
- **Over 1000 meter line of site distance with integrated antenna. External antenna can be connected to RF_OUT pad or through optional u.FL connector (requires moving RF path resistor).**
- **Can be externally controlled via simple ASCII AT commands over UART, USB and BT5.0, or programmed with custom applications embedded in the module.**

FCC CE -Certified- RoHS

Las

RingZ

- Uses
  manu
  - Wh

```
For bdaddr = ec:fe
        Company Na

        No BTC Ext

        DeviceName
                In

                Th

        No UUID16s

        No transmi

        No Appeara

        Manufactur
                De
```

https://www.blueradios.

*n*Blue BR-LE5.0-S1A Module Summary Datasheet
Copyright © 2002-2021 BlueRadios, Inc.
v1.3

BT5.0 Low Energy Single Mode Class 1 SoC Module

*n*Blue™ BR-LE5.0-S1A (nRF52840)

- *AT HOME. AT WORK. ON THE ROAD. USING BT5.0 LOW ENERGY WIRELESS TECHNOLOGY MEANS TOTAL FREEDOM FROM THE CONSTRAINTS AND CLUTTER OF WIRES IN YOUR LIFE.*
- FCC, IC, CE, RoHS, and BT5.0 Certified ISM 2.4GHz module supporting BT5.0 high speed mode, long range mode and advertising extensions. Can also support BT5.0 Mesh, 802.15.4 for Thread and Zigbee, ANT or proprietary 2.4Ghz.
- Utilizes the Nordic nRF52840 SoC 64Mhz ARM® Cortex™ M4F 32-bit processor with FPU, 1MB Flash, 256K RAM, built in DC-DC converter and ARM CryptoCell cryptographic accelerator.
- Programmable output power from -40dBm to +8dBm for short to long range applications.
- Over 1000 meter line of site distance with integrated antenna. External antenna can be connected to RF_OUT pad or through optional u.FL connector (requires moving RF path resistor).
- Can be externally controlled via simple ASCII AT commands over UART, USB and BT5.0, or programmed with custom applications embedded in the module.

FCC CE RoHS
-Certified-

Mini-Takeaway

Chip identification

- Identification of a BT module-maker can give you a *set* of possible chips that they use in their modules
  - And which chip a device is using, is one of the things I want to know!

Las Vegas
DEF CON 2023

- When walking around, I would often have basic BT scanning phone apps open, so that if I saw anything with an interesting new name I hadn't seen before, I could stop and give my scanner an opportunity to potentially collect more data about it

- When I wandered into the Wynn casino area, all of a sudden my phone app lit up with all sorts of ^IGT Card Reader$ entries!

Las Vegas
DEF CON 2023

- When walking arou ing phone apps open, so that if I sa ne I hadn't seen before, I could sto o potentially collect more data a

- When I wandered en my phone app lit up with all sorts

Las Vegas
DEF CON 2023

- When walking arou ing phone apps open, so that if I sa ne I hadn't seen before, I could sto o potentially collect more data a
- When I wandered en my phone app lit up with all sorts

Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gaming machine hardware maker!

https://store.igt.com/32916691

Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gaming machine hardware maker!

https://www.igt.com/products-and-services/gaming/systems/-/media/248ae3be76cc4cd8a60cd213357e9e0e.ashx

Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gami

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https://www.igt.com/products-and-services/

Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gami

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https://www.igt.com/products-and-services/

IGT Card Reader

UUID: ED5A634B-1779-445B-371(

Disconnected. Data is Stale.

ADVERTISEMENT DATA

Yes
Device Is Connectable

IGT Card Reader
Local Name

129
kCBAdvDataRxPrimaryPHY

0
kCBAdvDataRxSecondaryPHY

{
Service Data

E079C6A0-AA8B-11E3-A903-0002A5D5C5…en
Service UUIDs

713458723.6085089
kCBAdvDataTimestamp

-72
Tx Power Level

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https

IGT Card Reader

UUID: ED5A634B-1779-445B-371(

Disconnected. Data is Stale.

ADVERTISEMENT DATA

Yes
Device Is Connectable

IGT Card Reader
Local Name

129
kCBAdvDataRxPrimaryPHY

0
kCBAdvDataRxSecondaryPHY

{
Service Data

E079C6A0-AA8B-11E3-A903-0002A5D5C5…en
Service UUIDs

713458723.6085089
kCBAdvDataTimestamp

-72
Tx Power Level

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https

Las Vegas
DEF CON 2023

- Where else besides Wynn are there "IGT Card Reader" devices advertising?

Las Vegas
DEF CON 2023

- Where else besid dvertising?

Las Vegas
DEF CON 2023

- Where else besid dvertising?

Las Vegas
DEF CON 2023

- Where else besid dvertising?

Las Vegas
DEF CON 2023

- Where else besid dvertising?

Las Vegas
DEF CON 2023

- Where else besid dvertising?

Remember, that's just where WiGLE users had a GPS signal! Which is uncommon in the middle of mega-casinos!

Las Vegas
DEF CON 2023

- Are they *supposed* to be advertising or are they misconfigured?
- ¯_(ツ)_/¯

South Korea - All

So

Namyangju
남양주
Hongcheon
홍천
Pyeongchang
평창
Donghae
동해
Incheon
인천
GYEONGGI-DO
Samcheok
삼척
Taebaek
태백
Suwon
Yongin
용인
Wonju
원주
Jecheon
제천
Chungju
충주
Yeongju
영주
Seosan
서산
Uljin
울진
Mungyeong
문경
Hongseong
홍성
Andong
안동
Yeongdeok
영덕
Sangju
상주
Gumi
구미
Pohang
포항
Iksan
익산
Gimcheon
김천
Daegu
대구
Gyeongju
경주
Gunsan
군산
Jeonju
전주
Geochang
거창
Gyeongsan
경산
JEOLLABUK-DO
Ulsan
울산
Jeongeup
정읍
Namwon
남원
Yangsan
양산
Gwangju
광주
Jinju
진주
Gimhae
김해
Suncheon
순천
Changwon
창원
Muan
무안
Naju
나주
Gwangyang
광양
Tongyeong
통영
Geoje
거제
Sinan
Mokpo
목포
Yeosu
여수
Haenam
해남
Goheung
고흥
Wando
완도
Tsushima
対馬
Ojika
For development purposes only

So

Namyangju
남양주
Hongcheon
홍천
Pyeongchang
평창
Donghae
동해
Incheon
인천
GYEONGGI-DO
Samcheok
삼척
Taebaek
태백
Suwon
Yongin
용인
Wonju
원주
Jecheon
제천
Chungju
충주
Yeongju
영주
Seosan
서산
Uljin
울진
Mungyeong
문경
Hongseong
홍성
Andong
안동
Yeongdeok
영덕
Sangju
상주
Gumi
구미
Pohang
포항
Iksan
익산
Gimcheon
김천
Daegu
대구
Gyeongju
경주
Gunsan
군산
Jeonju
전주
Geochang
거창
Gyeongsan
경산
JEOLLABUK-DO
Ulsan
울산
Jeongeup
정읍
Namwon
남원
Yangsan
양산
Gwangju
광주
Jinju
진주
Gimhae
김해
Muan
무안
Naju
나주
Suncheon
순천
Changwon
창원
Gwangyang
광양
Sinan
Mokpo
목포
Tongyeong
통영
Geoje
거제
Yeosu
여수
Haenam
해남
Goheung
고흥
Wando
완도
Tsushima
対馬
For development purposes only

Seoul
서울
GANGWON-DO
Incheon
인천
GYEONGGI-DO
Donghae
동해
CHUNGCHEONGBUK-DO
CHUNGCHEONGNAM-DO
WIGLE.NET
Daejeon
대전
Pohang
포항
Daegu
대구
Jeonju
전주
JEOLLABUK-DO
GYEONGSANGNAM-DO
Gwangju
광주
Changwon
창원
Busan
부산
JEOLLANAM-DO
JEJU-DO
Seogwipo

South Korea - Seoul

- Yes, I ran around Gangnam with the sniffer...

South Korea - Seoul

Scooters

- Regex: ^KICKGOING$
- Not just a country-specific, but *city*-specific devices!

```
Company Name by IEEE OUI (10:52:1c): Espressif Inc.

No BTC Extended Inquiry Result Device info.

DeviceName: KICKGOING
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

South Korea - Seoul

Scooters

- Regex: ^KICKGOING$
- Not just a country-specific, but *city*-specific devices!

```
Company Name by IEEE OUI (10:52:1c): Espressif Inc.

No BTC Extended Inquiry Result Device info.

DeviceName: KICKGOING
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

South Korea - Seoul

Scooters

- Regex: ^KICKGOING$
- Not just a country-specific, but *city*-specific devices!

```
Company Name by IEEE OUI (10:52:1c): Espressif Inc.

No BTC Extended Inquiry Result Device info.

DeviceName: KICKGOING
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

Mini-Takeaway

Chip identification

- *Sometimes* devices which are using BT Classic, or BLE *Public* BDADDRs have an OUI which is from a *chip-maker*
- This can give a pretty strong signal of which chip a device is using
  - And which chip a device is using, is one of the things I want to know!

South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB 👀
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd 👀

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB 👀
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

BCM-L101-A

v4.1/CSR1010
17 X 12 X 2

BCM-L102-A

v4.1 / CSR1012
18.7 X 10 X 2.3

BCM-L101-A

v4.1 / CSR1010
17 X 12 X 2

```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810

```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810

```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810

```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810

```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810

```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810

FCC ID: 2APDI-BCM-LN300-AS

Main Board Front

Main Board Front

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5693550

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5693550

Mini-Takeaway

Chip identification

- FCC "Internal Photos" pictures can be used to identify chips for devices *in some cases*
  - And which chip a device is using, is one of the things I want to know!

Canada - Toronto

QoS: **0** type: **BLE**
00:02:3c:7f:d8:c1 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:07:80:a6:3a:6a ? 2023-10-24 - 2023-10-24

PIX0lnl QoS: **0** type: **BLE**
00:07:ce:d0:89:c8 ? 2023-10-24 - 2023-10-24

PIX5iyE QoS: **0** type: **BLE**
00:07:ce:e6:2c:84 ? 2023-10-24 - 2023-10-24

LE_ATH-M50xBT2 QoS: **0** type: **BLE**
00:0a:45:23:b5:89 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:0c:8a:63:ec:9f ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:0d:e2:2d:6e:55 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:0e:db:97:48:b6 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:10:68:9c:88:fc ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:10:7f:9a:10:e1 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:10:7f:9a:15:d7 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:12:14:bf:81:89 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:14:fa:1b:59:61 ? 2023-10-24 - 2023-10-24

Cubinote-BFF2 QoS: **0** type: **BT**
00:15:83:0d:bf:f2 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:1b:66:0d:79:33 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:1b:66:0f:38:ee ? 2023-10-24 - 2023-10-24

CX Plus True Wireless QoS: **0** type: **BLE**
00:1b:66:13:f8:a5 ? 2023-10-24 - 2023-10-24

Canada - Toronto

- Regex: ^MERO$

Canada - Toronto

- Regex: ^MERO$

MERO	QoS: 0	type: BLE	
ef:90:d6:fe:30:34	2022-12-29 - 2022-12-31		
MERO	QoS: 0	type: BLE	
f0:3e:26:ae:52:93	2023-03-01 - 2023-03-01		
MERO	QoS: 0	type: BLE	
f0:98:8f:3f:3a:32	2022-12-29 - 2022-12-31		
MERO	QoS: 0	type: BLE	
f2:9a:04:48:25:a5	2023-02-20 - 2023-02-21		
MERO	QoS: 0	type: BLE	
f2:a1:31:fe:8e:d5	2023-10-24 - 2023-10-24		
MERO	QoS: 0	type: BLE	
f3:bb:9b:33:b4:4b	2022-08-14 - 2022-08-14		
MERO	QoS: 0	type: BLE	
f4:a3:7b:6e:49:28	2022-09-12 - 2022-09-12		
MERO	QoS: 0	type: BLE	
f4:f1:8f:c3:af:e7	2023-10-24 - 2023-10-24		
MERO	QoS: 0	type: BLE	
f5:0a:5d:25:1c:f8	2023-03-01 - 2023-03-01		
MERO	QoS: 0	type: BLE	
f5:18:fc:44:46:97	2022-12-29 - 2022-12-31		

The visibility and insights you need deliver stellar cleaning results

Understand what's happening across your sites, pinpoint problem areas, get recommendations on how to maximize productivity, and put them into action – all from one platform.

SEE IT IN ACTION

From https://mero.co

Meró

How it Works | Solutions | Customers | Resources | Pricing | Log In | BOOK A DEMO

276 Queen St W Unit 200
Toronto, ON
M5V 2A1

The visibility and insights you need deliver stellar cleaning results

Understand what's happening across your sites, pinpoint problem areas, get recommendations on how to maximize productivity, and put them into action – all from one platform.

SEE IT IN ACTION

From https://mero.co

Canada - Toronto

```
For bdaddr = cb:9c:77:d7:9b:7c:
        Company Name by IEEE OUI: Not Applicable because this is a Random Static address

        No BTC Extended Inquiry Result Device info.

        DeviceName: MERO
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0059 (Nordic Semiconductor ASA) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x5900 (No Match)
                Raw Data: 0502be77723d0000000000000005
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)
```

Canada - Toronto

```
For bdaddr = cb:9c:77:d7:9b:7c:
        Company Name by IEEE OUI: Not Applicable because this is a Random Static address

        No BTC Extended Inquiry Result Device info.

        DeviceName: MERO
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0059 (Nordic Semiconductor ASA) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x5900 (No Match)
                Raw Data: 0502be77723d0000000000000005
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)
```

Canada - Toronto

```
For bdaddr = cb:9c:77:d7:9b:7c:
        Company Name by IEEE OUI: Not Applicable because this is a Random Static address

        No BTC Extended Inquiry Result Device info.

        DeviceName: MERO
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0059 (Nordic Semiconductor ASA) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x5900 (No Match)
                Raw Data: 0502be77723d0000000000000005
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)
```

```
Raw Data: 0502028bad820000000000000005
```

```
Raw Data: 010210ee146b011f000000000005
```

Different devices broadcast different data

End - Anecdotes - Locations

Begin - Anecdotes - Devices

Teslas

- "Random static" BDADDR (that has never changed on my Model 3)
- Non-randomized advertised name
  - Regex: ^S[0-9a-f]{16}C$ e.g. S83952932d49bc8aeC

  - Semantically: the [0-9a-f]{16} is *part of the SHA hash of the VIN*
    - https://trifinite.org/Downloads/20220916_tempa_presentation_sec-t_public.pdf
- https://teslaradar.com/ to crowdsource Tesla tracking
  - But don't use that, use WiGLE instead!

Teslas

Synacktiv
@Synacktiv

After having finished their exploit in an hotel room, @_p0ly_ and @vdehors successfully compromised the Tesla Model 3 infotainment through bluetooth and elevated their privileges to root!
Combined with the previous entry, this could have been a full chain to take over the car!

https://twitter.com/Synacktiv/status/1638996681260781574

Teslas

Synacktiv
@Synacktiv

After having finished their exploit in an hotel room, @_p0ly_ and @vdehors successfully compromised the Tesla Model 3 infotainment through bluetooth and elevated their privileges to root!
Combined with the previous entry, this could have been a full chain to take over the car!

https://twitter.com/Synacktiv/status/1638996681260781574

Lexus

2020-03-30

Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars

by Tencent Keen Security Lab

Since 2017, Lexus has equipped several models (including Lexus NX, LS and ES series) with a new generation infotainment, which is also known as AVN (Audio, Visual and Navigation) unit. Compared to some Intelligent connected infotainment units, like Tesla IVI and BMW ConnectedDrive system, the new Lexus AVN unit seems to be a bit more traditional. From a security perspective, it may highly reduce the possibility of being attacked by potential cybersecurity issues. But a new system is always introducing new security risks. After conducting an ethical hacking research on a 2017 Lexus NX300, Keen Security Lab [1] has discovered several security findings in Bluetooth and vehicular diagnosis functions on the car, which would compromise AVN unit, internal CAN network and related ECUs. By

https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

Address type: **Public** (0x00)
Address: AC:4D:16:FD:40:93 (OUI AC-4D-16)
Name (complete): Rivian Sensor 3

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

Address type: **Public** (0x00)
Address: AC:4D:16:FD:40:93 (OUI AC-4D-16) ← Actually Texas Instruments btmon just didn't have it in its vendor database
Name (complete): Rivian Sensor 3

```
For bdaddr = AC:4D:16:FD:40:93:
        Company Name by IEEE OUI (AC:4D:16): Texas Instruments

        No BTC Extended Inquiry Result Device info.

        DeviceName: Rivian Sensor 3
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

E Tu

- Rege
- Rege
- Rege

Address
Address
Name (c

```
For bdaddr = A
        Compan

        No BTC

        Device
```

https://apps.fcc.gov/e

E Tu

- Rege
- Rege
- Rege

Address
Address
Name (c

```
For bdaddr = A
        Compan

        No BTC

        Device
```

https://apps.fcc.gov/e

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

Address type: **Public** (0x00)
Address: AC:4D:16:FD:40:93 (OUI AC-4D-16) ← Actually Texas Instruments btmon just didn't have it in its vendor database
Name (complete): Rivian Sensor 3

```
For bdaddr = AC:4D:16:FD:40:93:
        Company Name by IEEE OUI (AC:4D:16): Texas Instruments

        No BTC Extended Inquiry Result Device info.

        DeviceName: Rivian Sensor 3
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

Rivian Key Fob

Other Car Things

- Regex: "^Tesla Model S.*", "^Tesla Model X.*" e.g. "Tesla Model S IDRISS"
- Regex: "^TOYOTA 4Runner$", "^TOYOTA Camry$", "^TOYOTA Corolla$", "^TOYOTA Highlander$", "^TOYOTA Rav 4$", "^TOYOTA RAV4$", "^TOYOTA SIENNA$"
- Regex: "^GM_PEPS_VKM$", "^GM_PEPS_VKM[1234]$"
- Regex: "^Audi_MMI_[0-9]{4}$", "^Audi MMI [0-9]{4}$"
- Regex: "^VW BT [0-9]{4}$"
- Regex: "^Porsche BT [0-9]{4}$"
- Regex: "^Polestar2$"

Other Car Things

- Regex: "^Tesla Model S.*", "^Tesla Model X.*" e.g. "Tesla Model S IDRISS"
- Regex: "^TOYOTA 4Runner$", "^TOYOTA Camry$", "^TOYOTA Corolla$", "^TOYOTA Highlander$", "^TOYOTA Rav 4$", "^TOYOTA RAV4$", "^TOYOTA SIENNA$"
- Regex: "^GM_PEPS_VKM$", "^GM_PEPS_VKM[1234]$"
- Regex: "^Audi_MMI_[0-9]{4}$", "^Audi MMI [0-9]{4}$"
- Regex: "^VW BT [0-9]{4}$"
- Regex: "^Porsche BT [0-9]{4}$"
- Regex: "^Polestar2$"

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num reports: 1
Event type: Connectable undirected - ADV_IND (0x00)
Address type: *Random* (0x01)
Address: 42:39:35:69:EC:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N0037**
RSSI: -90 dBm (0xa6)

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num reports: 1
Event type: Connectable undirected - ADV_IND (0x00)
Address type: *Random* (0x01)
Address: 78:4E:57:0D:C4:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N6ANS**
RSSI: -93 dBm (0xa3)

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Where in the world is Nest 0001?

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num Reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

WiGLE data ->


```
"trilat": 44.85729218,
"trilong": -93.43252563,
"ssid": "N0001",
"qos": 0,
"transid": "20190615-00000",
"firsttime": "2019-06-15T17:00:00.000Z",
"lasttime": "2019-06-15T16:00:00.000Z",
"lastupdt": "2019-06-15T16:00:00.000Z",
"netid": "6c:06:d0:eb:7d:4d",
"type": "BLE",
"capabilities": [
  "Uncategorized"
],
"userfound": false,
"device": 7936,
"name": "N0001",
"country": "US",
"region": "MN",
"road": "Singletree Lane",
"city": "Eden Prairie",
"housenumber": "12300",
"postalcode": "55344"
```


Where in the world is Nest 0001?

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num Reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

WiGLE data ->


```
"trilat": 35.68451691,
"trilong": 139.74157715,
"ssid": "N0001",
"qos": 0,
"transid": "20230223-00000",
"firsttime": "2023-02-23T16:00:00.000Z",
"lasttime": "2023-02-23T06:00:00.000Z",
"lastupdt": "2023-02-23T06:00:00.000Z",
"netid": "69:e3:a2:9a:1e:81",
"type": "BLE",
"capabilities": [
  "Misc"
],
"userfound": false,
"device": 0,
"name": "N0001",
"country": "JP",
"region": "麹町一丁目",
"road": "麹町学園通り",
"city": "千代田区",
"housenumber": null,
"postalcode": "102-0083"
```


Where in the world is Nest 0001?

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num[redacted] 1
Eve[redacted]onnectable undirected - ADV_IND (0x00)
Addr[redacted] *Random* (0x01)
Address: 42:39:35:69:EC:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N0037**
RSSI: -90 dBm (0xa6)

WiGLE data ->


```
"trilat": 52.28806686,
"trilong": -1.58548605,
"ssid": "N0001",
"qos": 0,
"transid": "20190505-00000",
"firsttime": "2019-05-05T15:00:00.000Z",
"lasttime": "2019-05-05T07:00:00.000Z",
"lastupdt": "2023-03-08T14:00:00.000Z",
"netid": "68:ad:8f:18:f0:d3",
"type": "BLE",
"capabilities": [
  "Misc"
],
"userfound": false,
"device": 0,
"name": "N0001",
"country": "GB",
"region": "England",
"road": "Wathen Road",
"city": "Warwick",
"housenumber": null,
"postalcode": "CV34 5BG"
```


Where in the world is Nest 0001?

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num Reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial) 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

WiGLE data ->


```
"trilat": 52.28806686,
"trilong": -1.58548605,
"ssid": "N0001",
"qos": 0,
"transid": "20190505-00000",
"firsttime": "2019-05-05T15:00:00.000Z",
"lasttime": "2019-05-05T07:00:00.000Z",
"lastupdt": "2023-03-08T14:00:00.000Z",
"netid": "68:ad:8f:18:f0:d3",
"type": "BLE",
"capabilities": [
  "Misc"
],
"userfound": false,
"device": 0,
"name": "N0001",
"country": "GB",
"region": "England",
"road": "Wathen Road",
"city": "Warwick",
"housenumber": null,
"postalcode": "CV34 5BG"
```


Where in the world is Nest 0001?

Mini-Takeaway

Vendor identification

- 16 bit service UUIDs are useful
  - *to associate products with vendors*
  - to differentiate between different products with similar names
- Filed tickets with WiGLE to request they be added

https://github.com/wiglenet/wigle-wifi-wardriving/issues/614
https://github.com/wiglenet/wigle-wifi-wardriving/issues/615
https://github.com/wiglenet/wigle-wifi-wardriving/issues/616

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

  TX Power: 0 dBm max

  RX Sensitivity: -96 dBm

  Data rate: 2 Mbps

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

  TX Power: 0 dBm max

  RX Sensitivity: -96 dBm

  Data rate: 2 Mbps

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-
- Flippers beaconing to finc
- **Bluetooth LE 5.0**

Data rate: 2 Mbps

Estimated Range

15 to 21 meters

https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/#estimator

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

  TX Power: 0 dBm max

  RX Sensitivity: -96 dBm

  Data rate: 2 Mbps

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

TX Power: 0 dBm max

RX Sensitivity: -96 dBm

Data rate: 2 Mbps

This low transmit power diminishes the long-term utility as a BT active-scanning/ attack tool

https://flipperzero.one/

- Flipper Ectruv
- **Flipper Eironeoo**
- Flipper Emiperda
- Flipper Eota
- Flipper Ew1csed4
- Flipper Himuti
- Flipper Hl4ken
- Flipper Iludaow
- Flipper Inudy
- Flipper Itey
- Flipper Jaalmo
- Flipper Kiteko
- Flipper L4spil
- Flipper Leotar
- Flipper Luneor
- Flipper Noda
- Flipper Nyn4k4
- Flipper Ogoty
- Flipper Opot
- Flipper Orable
- Flipper Ost4rder
- Flipper Otaro
- Flipper R4g0
- Flipper R4u0
- Flipper Roswigd
- Flipper Tuna
- Flipper Un1l0
- Flipper Ylepjl0d

Flipper Eironeoo

- WiGLE data saw it near a *Panera Bread* in Peachtree Corners, GA (outside Atlanta GA)
- I saw at Hardwear.io 2022 in The Hague

Change Dolphin Name?

Cwruidth Jun '22

This is almost certainly answered somewhere, but i've been searching around and couldn't find a topic for it:
Is it possible to change the unique dolphin name, or should i just reserve my effort for learning to love the goofy name mine was supplied by the factory?

created	last reply	12	8.5k	10	6	1
Jun '22	16d	replies	views	users	likes	link

Astra Support Jun '22

The Dolphin name is written into the OTP (one-time programmable) memory, so changing it is not possible.
However, you can edit the firmware to read the name from a string instead.

https://forum.flipper.net/t/change-dolphin-name/3670

Change Dolphin Name?

Cwruidth Jun '22

This is almost certainly answered somewhere, but i've been searching around and couldn't find a topic for it:
Is it possible to change the unique dolphin name, or should i just reserve my effort for learning to love the goofy name mine was supplied by the factory?

Address type: **Public** (0x00)
Address: **80:E1:26**:6A:4A:E6 (OUI 80-E1-26)
Data length: 28
Flags: 0x06
LE General Discoverable Mode
BR/EDR Not Supported
Name (complete): **Flipper Eironeoo**

8.5k views 10 users 6 likes 1 link

Astra Support Jun '22

The Dolphin name is written into the OTP (one-time programmable) memory, so changing it is not possible.
However, you can edit the firmware to read the name from a string instead.

https://forum.flipper.net/t/change-dolphin-name/3670

Change Dolphin Name?

Cwruidth Jun '22

This is almost certainly answered somewhere, but i've been searching around and couldn't find a topic for it:
Is it possible to change the unique dolphin name, or should i just reserve my effort for learning to love the goofy name mine was supplied by the factory?

Even if the name is changed, the BDADDR is not randomized...

Address type: **Public** (0x00)
Address: **80:E1:26**:6A:4A:E6 (OUI 80-E1-26)
Data length: 28
Flags: 0x06
  LE General Discoverable Mode
  BR/EDR Not Supported
Name (complete): **Flipper Eironeoo**

8.5k views 10 users 6 likes 1 link

Astra Support Jun '22

The Dolphin name is written into the OTP (one-time programmable) memory, so changing it is not possible.
However, you can edit the firmware to read the name from a string instead.

https://forum.flipper.net/t/change-dolphin-name/3670

Maybe they will change it

Someday

- https://github.com/flipperdevices/flipperzero-firmware/issues/2031
  - Filed November 2022, last post April 2023
  - Still open as of today
- Until then, if you've got a Flipper 👁️🌊👊

Maybe they will change it

Someday

- https://github.com/flipperdevices/flipperzero-firmware/issues/2031
  - Filed November 2022, last post April 2023
  - Still open as of today
- Until then, if you've got a Flipper 👁️🌊👊

Hotels

- Regex: ^[0-9]{8}\.[0-9]{8}$
  - E.g. 46351777.00007702
- At the time I saw no obvious semantic association between the first portion of the name and either the BDADDR or room number
- Saw 17 instances from my room

Hotels

- Door physically looked like this:

Unity
United Technologies

HT RFID Lock with DirectKey™ Module

Features

- On-board DirectKey module provides secure wireless communication of credentials from a user's smartphone to a locking device via Bluetooth® Smart communications
- Reading technology: contactless RFID (ISO14443A, 14443B part 4, NFC)
- Multiple opening devices available: keycards, wristbands, keychains, etc.
- Average battery life: approximately 2 years
- Non-volatile memory records the last 500 lock openings – including date, time and card used
- Programmable to customer needs (meeting rooms, offices, housekeeping, etc.)
- LEDs to indicate lock status including a low battery warning
- MIFARE® compatibility - no need for proprietary keycards
- Corrosion-treated for normal atmospheric conditions

https://fccid.io/R32-HT34RFIDBT/User-Manual/user-manual-3020324

Hotels

- Company Name by IEEE OUI (00:17:55): *GE Security*
- UUID16 0xfea7 (Company ID: *UTC Fire and Security*)
- What's WiGLE say if we search for that OUI?

Hotels - GE Security OUI 00:17:55

Hotels - GE Security OUI 00:17:55

Hotels - GE Security OUI 00:17:55

WiFi | Cell | BT

Lat: 35.1879 **to:** 35.1889

Lon: -80.9156 **to:** -80.9145

Last Updated: 20010925174546

BSSID/MAC: 00:17:55

Network Name (wildcards[1]: % and _):

foorbar or foobar%

☐ **Only Nets I Was the First to See**

Query

[1]'%': 0-or-more characters, '_': a single character.

44039037.00008208 QoS: 1 type: BLE
00:17:55:a3:f2:61 ? 2022-02-08 - 2022-02-11

44084700.00008208 QoS: 1 type: BLE
00:17:55:a4:a4:c0 ? 2022-02-08 - 2022-02-11

44084714.00008208 QoS: 1 type: BLE
00:17:55:a4:a4:ce ? 2022-02-08 - 2022-02-11

44084738.00008208 QoS: 1 type: BLE
00:17:55:a4:a4:e6 ? 2021-11-15 - 2022-02-11

44084798.00008208 QoS: 1 type: BLE
00:17:55:a4:a5:22 ? 2022-02-08 - 2022-02-11

44084906.00008208 QoS: 1 type: BLE
00:17:55:a4:a5:8e ? 2022-02-08 - 2022-02-11

44084915.00008208 QoS: 1 type: BLE
00:17:55:a4:a5:97 ? 2022-02-08 - 2022-02-11

44085226.00008208 QoS: 1 type: BLE
00:17:55:a4:a6:ce ? 2022-02-08 - 2022-02-11

44085241.00008208 QoS: 1 type: BLE
00:17:55:a4:a6:dd ? 2022-02-08 - 2022-02-11

44085256.00008208 QoS: 1 type: BLE

Hotels - GE Security OUI 00:17:55 @ Hilton

black hat USA 2019

AUGUST 3–8, 2019

MANDALAY BAY / LAS VEGAS

Moving from Hacking IoT Gadgets to Breaking into One of Europe's Highest Hotel Suites

by Ray & mh

µc³

SPORTSFREUNDE DER SPERRTECHNIK - DEUTSCHLAND E.V.

https://i.blackhat.com/USA-19/Thursday/us-19-Ray-Moving-From-Hacking-IoT-Gadgets-To-Breaking-Into-One-Of-Europes-Highest-Hotel-Suites.pdf

Reminder Why Hotel Room Security Matters...

2010 assassination of Hamas leader by Mossad, in Dubai hotel

- https://www.wired.com/2010/02/alleged-assassins-caught-on-tape/
- https://www.youtube.com/watch?v=bJujlwtdk8w

Possible ways of gaining entry:

- Entry by reprogramming the lock on the door to room 230, as the system shows an attempt to do this during this time.

- Kevin or Gail could have knocked on the victim's door posing as hotel staff.

gntv
Play (k)
SUBSCRIBE
22:40 / 27:26

Possible ways of gaining entry:

- Entry by reprogramming the lock on the door to room 230, as the system shows an attempt to do this during this time.

- Kevin or Gail could have knocked on the victim's door posing as hotel staff.

gntv

VingCard

Locklink transfer lock events

Readout for lock: 230
Number of events: 100

Read-out date: 03/02/2010 08:05
Lock mode: Normal

Event	Date & Time / User ID	Event description / Name (Room)	Event Details / User group	Keycard type
1	18/01/2010 20:00 Operation failed Clock	Locklink	Write	
2	18/01/2010 19:05 15258 Override on start time	Opened/closed, New card LAUNDRY, LAUNDRY	Deadbolt not overridden LAUNDRY	LAUNDRY
3	18/01/2010 19:00 14426	Opened/closed, Valid card SUPERVISOR6, FLOOR2	Deadbolt not overridden FLOOR 2	HK MAID
4	18/01/2010 15:25 3239 Override on start time	Opened/closed, New card Hassan Mr., Mahmoud (230)	Deadbolt not overridden GUEST	GUEST ROOM
5	18/01/2010 14:10 12267	Opened/closed, Valid card MARSHALL, MARSHALL	Deadbolt not overridden MINI BAR	MINIBAR
6	18/01/2010 13:35 12852	Opened/closed, Valid card SUPERVISOR1, FLOOR2	Deadbolt not overridden FLOOR 2	HK MAID
7	18/01/2010 12:45 12710	Opened/closed, Valid card FLOOR2, KEY2	Deadbolt not overridden FLOOR 2	HK MAID
8	18/01/2010 23:05 3069 Override on start time	Opened/closed, New card Kolemaire Ms., Julia (230)	Deadbolt not overridden GUEST	GUEST ROOM
[illegible]	18/01/2010 18:35 [illegible]	Opened/closed, Valid card	Deadbolt not overridden	

Play (k)

22:40 / 27:26

VingCard

Locklink transfer lock events

Readout for lock: 230
Number of events: 100

Read-out date: 03/02/2010 08:05
Lock mode: Normal

Event	Date & Time User ID	Event description Name (Room) Status = Checked out or retrieved cardholders set of the point time	Event Details User group	Keycard type
1	19/01/2010 20:00 Operation failed Clock	Locklink	Write	
2	19/01/2010 19:05 15258 Override on start time	Opened/closed, New card LAUNDRY, LAUNDRY	Deadbolt not overridden LAUNDRY	LAUNDRY
3	19/01/2010 19:00 14426	Opened/closed, Valid card SUPERVISOR5, FLOOR2	Deadbolt not overridden FLOOR 2	HK MAID
4	19/01/2010 15:25 3239 Override on start time	Opened/closed, New card *Hassan Mr., Mahmoud (230)*	Deadbolt not overridden GUEST	GUEST ROOM
5	19/01/2010 14:10 12267	Opened/closed, Valid card MARSHALL, MARSHALL	Deadbolt not overridden MINI BAR	MINIBAR
6	19/01/2010 13:35 12852	Opened/closed, Valid card SUPERVISOR1, FLOOR2	Deadbolt not overridden FLOOR 2	HK MAID
7	19/01/2010 12:45 12710	Opened/closed, Valid card FLOOR2, KEY2	Deadbolt not overridden FLOOR 2	HK MAID
8	18/01/2010 23:05 3069 Override on start time	Opened/closed, New card *Kolomiets Ms., Iuliia (230)*	Deadbolt not overridden GUEST	GUEST ROOM

Random - "^Pokemon GO Plus$"

- Regex: ^Pokemon GO Plus$
- "The Pokémon GO Plus is a small device that lets you enjoy Pokémon GO while you're on the move and not looking at your smartphone
- The device connects to a smartphone via Bluetooth low energy and notifies you about events in the game, such as the appearance of a Pokémon nearby using an LED and vibration
- The Pokémon GO Plus will begin to blink and vibrate whenever you're within range of a PokéStop; Press the Pokémon GO Plus button to search the PokéStop for items; If you find any items, they'll immediately be added to your inventory"

Fitness (*People?*) Trackers / Watches

Fitbit

- Regex: ^Versa(| 2| 3| 4| Lite)$ e.g. Versa 2
- Regex: ^Inspire(| HR| 2| 3)$ e.g. Inspire HR
- Regex: ^Alta(| HR)$ e.g. Alta HR
- Regex: ^Ionic$
- Regex: ^Flex(| 2)$ e.g. Flex 2
- Regex: ^One$ e.g. One

Fitness (*People?*) Trackers / Watches

Fitbit

- Regex: ^Versa(| 2| 3| 4| Lite)$ e.g. Versa 2
- Regex: ^Inspire(| HR| 2| 3)$ e.g. Inspire HR
- Regex: ^Alta(| HR)$ e.g. Alta HR
- Regex: ^Ionic$
- Regex: ^Flex(| 2)$ e.g. Flex 2
- Regex: ^One$ e.g. One

Address type: Random (0x01)
Address: ED:BD:7C:77:18:EC (**Static**)

Address type: Random (0x01)
Address: D8:D0:87:BB:3A:6C (**Static**)

Address type: Random (0x01)
Address: DF:22:47:91:6D:B7 (**Static**)

Address type: Random (0x01)
Address: CA:C3:40:DB:BC:64 (**Static**)

Address type: Random (0x01)
Address: CA:C3:40:DB:BC:64 (**Static**)

Address type: Random (0x01)
Address: F2:0A:E8:4C:4D:4B (**Static**)

Vendor-specific 128-bit UUIDs

- *abba*ff00-e56a-484c-b832-8b17cf6cbfe8
  - Versa (|2|Lite), Ionic
- *adab*fb00-**6e7d-4601-bda2-bffaa68956ba**
  - Inspire HR, Flex 2
- *adab*0d57-**6e7d-4601-bda2-bffaa68956ba**
- *adab*6552-**6e7d-4601-bda2-bffaa68956ba**
  - One
- *adab*5b8c-**6e7d-4601-bda2-bffaa68956ba**
  - Flex

Vendor-specific 128-bit UUIDs

- *abba*ff00-e56a-484c-b832-8b17cf6cbfe8
  - Versa (|2|Lite), Ionic
- *adab*fb00-**6e7d-4601-bda2-bffaa68956ba**
  - Inspire HR, Flex 2
- *adab*0d57-**6e7d-4601-bda2-bffaa68956ba**
- *adab*6552-**6e7d-4601-bda2-bffaa68956ba**
  - One
- *adab*5b8c-**6e7d-4601-bda2-bffaa68956ba**
  - Flex

```
> HCI Event: LE Meta Event (0x3e) plen 42
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: F5:6E:B2:C3:73:D2 (Static)
      Data length: 30
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      128-bit Service UUIDs (partial): 1 entry
        Vendor specific (abbaff00-e56a-484c-b832-8b17cf6cbfe8)
      Service Data (UUID 0x180a): 2604329303
      RSSI: -93 dBm (0xa3)
```

Vendor-specific 128-bit UUIDs

- *abba*ff00-e56a-484c-b832-8b17cf6cbfe8
  - Versa (|2|Lite), Ionic
- *adab*fb00-**6e7d-4601-bda2-bffaa68956ba**
  - Inspire HR, Flex 2
- *adab*0d57-**6e7d-4601-bda2-bffaa68956ba**
- *adab*6552-**6e7d-4601-bda2-bffaa68956ba**
  - One
- *adab*5b8c-**6e7d-4601-bda2-bffaa68956ba**
  - Flex

```
> HCI Event: LE Meta Event (0x3e) plen 42
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: F5:6E:B2:C3:73:D2 (Static)
      Data length: 30
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      128-bit Service UUIDs (partial): 1 entry
        Vendor specific (abbaff00-e56a-484c-b832-8b17cf6cbfe8)
      Service Data (UUID 0x180a): 2604329303
      RSSI: -93 dBm (0xa3)
```

Background

Passive Scanning

Active Scanning

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Background

Passive Scanning

Sometimes the name will be here

Active Scanning

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Background

Passive Scanning

Sometimes the name will be here

Active Scanning

Other times you need to ask for it, and it comes back in the SCAN_RSP

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Find New Devices

I hadn't previously sorted any of the devices in bold as being fitbits

I suppose I should have looked at https://en.wikipedia.org/wiki/List_of_Fitbit_products, but I didn't care that much

btmon -T -r logs/btmon/2023-02-07-05-51-24_pi1.bin | grep -A 3 **bffaa68956ba** | grep Name | sort | uniq

Name (complete): **Ace 2**

Name (complete): **Ace 3**

Name (complete): Alta HR

Name (complete): **Blaze**

Name (complete): **Charge 2**

Name (complete): **Charge 3**

Name (complete): Flex 2

Name (complete): Inspire 2

Name (complete): Inspire HR

Name (complete): Versa Lite

Name (complete): **Zip**

btmon -T -r logs/btmon/2023-02-07-05-51-24_pi1.bin | grep -A 3 **8b17cf6cbfe8** | grep Name | sort | uniq

Name (complete): **Charge 4**

Name (complete): **Charge 5**

Name (complete): Inspire 3

Name (complete): **Luxe**

Name (complete): **Sense**

Name (complete): Versa

Name (complete): Versa 2

Name (complete): Versa 3

Mini-Takeaway

Vendor & model identification

- 128 bit service UUIDs are useful
  - *to associate products with vendors*, even without human-readable names
    - and even within a *completely passive* scanner
  - to determine how similar one generation of product is to the next
  - to find similarities across product lines

In the Car

ODBII-to-BT

- ^FIXD$: ("ISSC Technologies Corp." or "SHENZHEN XIN FEI JIA ELECTRONIC CO. LTD." or "SST Taiwan Ltd." or no match OUI)
  - I connected to one of these with their app, and it didn't seem to have auth? (But couldn't get meaningful data since car was turned off)
- ^OBDBLE$ and ^Zus$: ("NO NDA Inc" OUI)
- ^OBDeleven 2$: Voltas IT https://obdeleven.com/ ("Teltonika" OUI)
- ^OBDLink CX$: OBD Solutions, LLC. ("Dialog Semiconductor Hellas SA" OUI)
- ^OBDII$: Unknown brand (could be white-label), but highly likely ODBII-to-BT car monitor

Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT

Haohuang Wen[1], Qi Alfred Chen[2], Zhiqiang Lin[1]

[1]Ohio State University
[2]University of California, Irvine

USENIX Security 2020

From https://www.usenix.org/system/files/sec20_slides_wen.pdf

A Quick Word About Threat Models

BT sniffers vs. automated license plate readers (ALPRs)

- It is starting to become common to surreptitiously install automated license plate scanners in public places [1][2]
- Thus far I've only seen BT tracking discussed in the context of advertisement [3], not forensically placing criminals at a given location based on BT data
- For any device that is *not* adequately randomizing its identity, bluetooth scanners can serve a similar function as ALPRs
    - I once spoke with a local county police officer who had brought this up without prompting

[1] https://www.eff.org/pages/automated-license-plate-readers-alpr
[2] https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/
[3] https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html

A Quick Word About Threat Models

Surveillance vs. Sousveillance

- The BT sword cuts both ways ⚔️: surveillance or sousveillance
  - "Sousveillance (/suːˈveɪləns/ soo-VAY-lənss) is the recording of an activity by a member of the public, rather than a person or organisation in authority, typically by way of small wearable or portable personal technologies."
    - https://en.wikipedia.org/wiki/Sousveillance
  - WiGLE can be used for sousveilance

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}
- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay

- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay

- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

```
> HCI Event: LE Meta Event (0x3
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable unc                _IND (0x00)
      Address type: Public (0x00)
      Address: BC:C3:42:54:63:AD (Panasonic Communications Co., Ltd.)
      Data length: 21
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      128-bit Service UUIDs (complete): 1 entry
```

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay

- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

Does this only broadcast if it's recording?
Or is it configurable?

```
> HCI Event: LE Meta Event (0x3
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable unc                _IND (0x00)
      Address type: Public (0x00)
      Address: BC:C3:42:54:63:AD (Panasonic Communications Co., Ltd.)
      Data length: 21
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      128-bit Service UUIDs (complete): 1 entry
```

https://media.defcon.org/DEF%20CON%2031/DEF%20CON%2031%20presentations/nullagent%20rekcahdam%20-%20Snoop%20on%20to%20them%20as%20they%20snoop%20on%20to%20us.pdf

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

```
For bdaddr = 00:1f:ff:5f:0d:5a:
        Company Name by IEEE OUI (00:1f:ff): Respironics, Inc.

        No BTC Extended Inquiry Result Device info.

        DeviceName: PR BT 5C0A
                In BT Classic Data (EIR_bdaddr_to_name)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
        DeviceName: PR BT 5C0A
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
                This was found in an event of type 0 which corresponds to Conn

        UUID16s found:
                UUID16 0x1101 (Service ID: SerialPort)
                         Found in BT Classic data (EIR_bdaddr_to_UUID16s)
```

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

```
For bdaddr = 00:1f:ff:5f:0d:5a:
        Company Name by IEEE OUI (00:1f:ff): Respironics, Inc.

        No BTC Extended Inquiry Result Device info.

        DeviceName: PR BT 5C0A
                In BT Classic Data (EIR_bdaddr_to_name)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
        DeviceName: PR BT 5C0A
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
                This was found in an event of type 0 which corresponds to Conn

        UUID16s found:
                UUID16 0x1101 (Service ID: SerialPort)
                         Found in BT Classic data (EIR_bdaddr_to_UUID16s)
```

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

```
For bdaddr = 00:1f:ff:5f:0d:5a:
        Company Name by IEEE OUI (00:1f:ff): Respironics, Inc.

        No BTC Extended Inquiry Res                ce info.

        DeviceName: PR BT 5C0A
                In BT Classic Data (EIR_bdaddr_to_name)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Phill
        DeviceName: PR BT 5C0A
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
                This was found in an event of type 0 which corresponds to Conn

        UUID16s found:
                UUID16 0x1101 (Service ID: SerialPort)
                         Found in BT Classic data (EIR_bdaddr_to_UUID16s)
```

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

```
For bdaddr = 00:1f:ff:5f:0d:5a:
        Company Name by IEEE OUI (00:1f:ff): Respironics, Inc.

        No BTC Extended Inquiry Res                ce info.

        DeviceName: PR BT 5C0A
                In BT Classic Data (EIR_bdaddr_to_name)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Phill
        DeviceName: PR BT 5C0A
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
                This was found in an event of type 0 which corresponds to Conn

        UUID16s found:
                UUID16 0x1101 (Service ID: SerialPort)
                        Found in BT Classic data (EIR_bdaddr_to_UUID16s)
```

Sleep Apnea <- Obesity <- Poverty

- "There is a linear correlation between obesity and OSA [sleep apnea]"[1]
- There is a link between poverty and obesity[2][3]
- Is a neighborhood with lots of sleep apnea machines likely to be a poorer neighborhood?
- *Or* can the people in poorer neighborhoods not afford bluetooth sleep apnea machines?

[1] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5836788/#:~:text=There%20is%20a%20linear%20correlation,ultimately%20resulting%20in%20sleep%20apnea.
[2] https://www.seacaa.org/post/the-link-between-poverty-and-obesity#:~:text=There%20tends%20to%20be%20fewer,major%20contributing%20factor%20to%20obesity.
[3] https://scholars.org/contribution/why-poverty-leads-obesity-and-life-long-problems

Rockville
95
Beltsville
270
Potomac
495
Bowie
College Park
Bethesda
Lanham
450
Hyattsville
267
McLean
50
Tysons
Washington
66
Capitol
Heights
214
301
Arlington
295
495
495
Fairfax
WIGLE.NET
395
495
Upper
Marlboro
4
Alexandria
Joint Base
Andrews
Burke
Springfield
495
633
301
382
123
Clinton
210

Income
0 - 32,000
32,000 - 40,000
40,000 - 46,000
46,000 - 52,000
52,000 - 58,000
58,000 - 65,000
65,000 - 74,000
74,000 - 87,000
87,000 - 109,000
109,000 - and more
Potomac
Bethesda
Chevy Chase
Silver Spring
Takoma Park
College Park
Greenbelt
Beltsville
Laurel
Bowie
Patuxent Research Refuge
Hyattsville
Riverdale Park
Landover
Greater Landover
Capitol Heights
Washington
DISTRICT OF COLUMBIA
MARYLAND
VIRGINIA
Arlington
Falls Church
McLean
Tysons
Vienna
Fairfax
Alexandria
Springfield
Burke
Joint Base Andrews
Clinton
Upper Marlboro
Great Falls Park
George Washington Memorial Parkway
Wolf Trap
Friendship Village
Rollins Park
Wheaton-Glenmont
Aspen Hill
Calverton
South Laurel
White Oak
Travilah
North Bethesda
Adelphi
Hillcrest Heights
Suitland-Silver Hill
Temple Hills
Oxon Hill
Bailey's Crossroads
Seven Corners
Annandale
Lincolnia
Franconia
West Springfield
South Run
Newington
Hybla Valley
Belle Haven
NATIONAL HARBOR
Rosaryville
Croom
Cheltenham
Queenland
Idylwood
Oakton
Merrifield
Kings Park West
Fairfax Station
George Mason
Friendly

Rockville
95
Beltsville
270
Potomac
495
Bowie
College Park
Bethesda
Lanham
450
Hyattsville
267
McLean
50
Tysons
Washington
66
Capitol
Heights
214
301
Arlington
295
495
495
Fairfax
WIGLE.NET
395
495
Upper
Marlboro
4
Alexandria
Joint Base
Andrews
Burke
Springfield
495
633
301
382
123
Clinton
210

Income
0 - 32,000
32,000 - 40,000
40,000 - 46,000
46,000 - 52,000
52,000 - 58,000
58,000 - 65,000
65,000 - 74,000
74,000 - 87,000
87,000 - 109,000
109,000 - and more
Potomac
Bethesda
Chevy Chase
Silver Spring
Takoma Park
College Park
Greenbelt
Beltsville
Laurel
Bowie
Patuxent Research Refuge
Hyattsville
Riverdale Park
Landover
Greater Landover
Capitol Heights
Washington
DISTRICT OF COLUMBIA
MARYLAND
VIRGINIA
Arlington
Falls Church
McLean
Tysons
Vienna
Fairfax
Alexandria
Springfield
Burke
Joint Base Andrews
Clinton
Upper Marlboro
Great Falls Park
George Washington Memorial Parkway
Wolf Trap
Friendship Village
Rollins Park
Wheaton-Glenmont
Aspen Hill
Calverton
South Laurel
White Oak
Travilah
North Bethesda
Adelphi
Hillcrest Heights
Suitland-Silver Hill
Temple Hills
Oxon Hill
Bailey's Crossroads
Seven Corners
Annandale
Lincolnia
Franconia
West Springfield
South Run
Newington
Hybla Valley
Belle Haven
NATIONAL HARBOR
Rosaryville
Croom
Cheltenham
Queenland
Idylwood
Oakton
Merrifield
Kings Park West
Fairfax Station
George Mason
Friendly

PR BT 2F1C QoS: **1** type: **BT**
00:1f:ff:36:6b:23 ? 2022-10-27 - 2022-10-29

PR BT DE6E QoS: **0** type: **BT**
00:1f:ff:36:9d:4a ? 2019-07-14 - 2019-07-14

PR BT F271 QoS: **0** type: **BT**
00:1f:ff:36:b9:f8 ? 2022-05-03 - 2022-05-14

PR BT 5EE5 QoS: **0** type: **BT**
00:1f:ff:36:bc:46 ? 2019-11-30 - 2019-11-30

PR BT 535F QoS: **2** type: **BT**
00:1f:ff:36:c3:ff ? 2001-12-31 - 2019-08-02

PR BT 6E37 QoS: **0** type: **BT**
00:1f:ff:36:c4:96 ? 2022-08-14 - 2023-02-07

PR BT E8F4 QoS: **0** type: **BT**
00:1f:ff:36:c5:c9 ? 2023-09-07 - 2023-09-07

PR BT 6A25 QoS: **0** type: **BT**
00:1f:ff:37:68:06 ? 2023-10-14 - 2023-10-13

PR BT 7853 QoS: **1** type: **BT**
00:1f:ff:38:c1:fc ? 2019-11-16 - 2019-12-08

PR BT C057 QoS: **0** type: **BT**
00:1f:ff:3a:49:f8 ? 2020-01-24 - 2020-01-24

PR BT 5645 QoS: **1** type: **BT**
00:1f:ff:3a:6d:1b ? 2019-11-11 - 2020-02-05

PR BT 747E QoS: **0** type: **BLE**
00:1f:ff:3b:7b:01 ? 2019-11-23 - 2019-11-23

PR BT CFDB QoS: **0** type: **BT**
00:1f:ff:3e:7d:91 ? 2023-07-09 - 2023-07-09

PR BT BE73 QoS: **6** type: **BLE**
00:1f:ff:3f:fc:7f ? 2019-07-14 - 2021-05-18

PR BT 2B35 QoS: **0** type: **BLE**
00:1f:ff:40:68:59 ? 2022-08-14 - 2023-02-07

PR BT 784A QoS: **0** type: **BT**
00:1f:ff:40:71:63 ? 2020-03-07 - 2020-03-07

PR BT 2459 QoS: **0** type: **BLE**
00:1f:ff:40:a9:6b ? 2018-12-05 - 2019-03-01

PR BT 4241 QoS: **0** type: **BLE**
00:1f:ff:41:8b:f8 ? 2019-05-24 - 2019-05-24

PR BT E13F QoS: **0** type: **BLE**
00:1f:ff:42:47:d6 ? 2001-12-31 - 2019-09-04

PR BT 196B QoS: **2** type: **BLE**
00:1f:ff:43:9d:f9 ? 2019-07-14 - 2023-09-07

Medical 😬

Continuous Glucose Monitoring System

- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"

```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

```
toring System (https://www.d
tising (ADV_IND)

toring System (https://www.d
```

Dexcom
Pairing
Please wait, transmitter and receiver pairing...
May take 30 minutes. Keep receiver within 6 meters of transmitter.

Medical 😬

Continuous Glucose Monitoring System

- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"

```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

Medical 😬

Continuous Glucose Monitoring System

- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"

```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

Medical 😬

Continuous Glucose Monitoring System

- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"

```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

Medical 😬

```
For bdaddr = c2:33:98:f6:fd:41:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (http   www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x00d0 (Dexcom, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0xd000 (No Match)
                Raw Data: 3703
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
                Device Company ID: 0x00d0 (Dexcom, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0xd000 (No Match)
                Raw Data: 3703
```

Medical 😬

```
For bdaddr = c2:33:98:t6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (http   www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x00d0 (Dexcom, Inc.) - take with a grain of salt, not all companies populate this accurately!
                        Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0xd000 (No Match)
                Raw Data: 3703
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
                Device Company ID: 0x00d0 (Dexcom, Inc.) - take with a grain of salt, not all companies populate this accurately!
                        Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0xd000 (No Match)
                Raw Data: 3703
```

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care) 👀
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        No Appearance data found.

        No Manufacturer-specific Data found.

        No Class of Device Data found.

        GATT Information:
                GATT Service: Begin Handle: 1   End Handle: 9           UUID128: 00001800-0000-1000-8000
                        GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
                        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
                        GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
                                GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name),
                                GATT Characteristic value read as b'tslim X2 ***611'
                        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
```

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        No Appearance data found.

        No Manufacturer-specific Data found.

        No Class of Device Data found.

        GATT Information:
                GATT Service: Begin Handle: 1   End Handle: 9           UUID128: 00001800-0000-1000-8000
                        GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
                        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
                        GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
                                GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name),
                                GATT Characteristic value read as b'tslim X2 ***611'
                        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
```

```
ice Data found.

n:
rvice: Begin Handle: 1   End Handle: 9          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
 GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
         GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name), Properties: 10 ('Readab
         GATT Characteristic value read as b'tslim X2 ***611'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
 GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
         GATT Characteristic: 00002a01-0000-1000-8000-00805f9b34fb (Appearance), Properties: 2 ('Readable
         GATT Characteristic value read as b'\x00\x00'
                 Appearance decodes as: Category (0): Unknown, Sub-Category (0): Generic
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002a04-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
         GATT Characteristic: 00002a04-0000-1000-8000-00805f9b34fb (Peripheral Preferred Connection Param
         GATT Characteristic value read as b'\x0c\x00\x18\x00\x1d\x00\x0f\x01'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
 GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
         GATT Characteristic: 00002aa6-0000-1000-8000-00805f9b34fb (Central Address Resolution), Properti
         GATT Characteristic value read as b'\x01'
rvice: Begin Handle: 10  End Handle: 13         UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
         GATT Characteristic: 00002a05-0000-1000-8000-00805f9b34fb (Service Changed), Properties: 32 ('In
 GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 13
rvice: Begin Handle: 14  End Handle: 22         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device In
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 14
rvice: Begin Handle: 23  End Handle: 65535      UUID128: 0000fdfb-0000-1000-8000-00805f9b34fb (This is a
```

```
ice Data found.

n:
rvice: Begin Handle: 1   End Handle: 9          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
 GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
         GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name), Properties: 10 ('Readab
         GATT Characteristic value read as b'tslim X2 ***611'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
 GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
         GATT Characteristic: 00002a01-0000-1000-8000-00805f9b34fb (Appearance), Properties: 2 ('Readable
         GATT Characteristic value read as b'\x00\x00'
                 Appearance decodes as: Category (0): Unknown, Sub-Category (0): Generic
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002a04-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
         GATT Characteristic: 00002a04-0000-1000-8000-00805f9b34fb (Peripheral Preferred Connection Param
         GATT Characteristic value read as b'\x0c\x00\x18\x00\x1d\x00\x0f\x01'👀
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
 GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
         GATT Characteristic: 00002aa6-0000-1000-8000-00805f9b34fb (Central Address Resolution), Properti
         GATT Characteristic value read as b'\x01'
rvice: Begin Handle: 10  End Handle: 13         UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
         GATT Characteristic: 00002a05-0000-1000-8000-00805f9b34fb (Service Changed), Properties: 32 ('In
 GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 13
rvice: Begin Handle: 14  End Handle: 22         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device In
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 14
rvice: Begin Handle: 23  End Handle: 65535      UUID128: 0000fdfb-0000-1000-8000-00805f9b34fb (This is a
```

```
ice Data found.

n:
rvice: Begin Handle: 1   End Handle: 9          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
 GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
         GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name), Properties: 10 ('Readab
         GATT Characteristic value read as b'tslim X2 ***611'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
 GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
         GATT Characteristic: 00002a01-0000-1000-8000-00805f9b34fb (Appearance), Properties: 2 ('Readable
         GATT Characteristic value read as b'\x00\x00'
                 Appearance decodes as: Category (0): Unknown, Sub-Category (0): Generic
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002a04-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
         GATT Characteristic: 00002a04-0000-1000-8000-00805f9b34fb (Peripheral Preferred Connection Param
         GATT Characteristic value read as b'\x0c\x00\x18\x00\x1d\x00\x0f\x01'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
 GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
         GATT Characteristic: 00002aa6-0000-1000-8000-00805f9b34fb (Central Address Resolution), Properti
         GATT Characteristic value read as b'\x01'
rvice: Begin Handle: 10  End Handle: 13         UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
         GATT Characteristic: 00002a05-0000-1000-8000-00805f9b34fb (Service Changed), Properties: 32 ('In
 GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 13
rvice: Begin Handle: 14  End Handle: 22         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device In
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 14
rvice: Begin Handle: 23  End Handle: 65535      UUID128: 0000fdfb-0000-1000-8000-00805f9b34fb (This is a
```

Heavy Machinery

- Regex: ^CATBTNT-0(4|7) [A-Z]{3}[0-9]{5}$ (3 char model, 5 serial?)
  - "CATBTNT-04 DKS02123"
  - "CATBTNT-04 LHW00220"
  - "CATBTNT-07 WCH10725"

https://fccid.io/PQMA5S4/User-Manual/Exhibit-D-Users-Manual-per-2-1033-b3-3137980.pdf

Heavy Machinery

- Regex: ^CATBTNT-0(4|7) [A-Z]{3}[0-9]{5}$ (3 char model,
  - "CATBTNT-04 DKS02123"
  - "CATBTNT-04 LHW00220"
  - "CATBTNT-07 WCH10725"

Cat Bluetooth Network Transceiver Overview

Illustration 1 g06087602

The Cat BTNT acts as a central hub for wireless Bluetooth devices on Cat machines. The Bluetooth network uses Bluetooth Low Energy technology. This technology enables the machine to read Cat key fobs and sensors wirelessly and convert the data to standard and proprietary J1939 messages. These messages are sent over the CAN datalink to a machine control ECM to enable operator identification or machine system security.

https://fccid.io/PQMA5S4/User-Manual/Exhibit-D-Users-Manual-per-2-1033-b3-3137980.pdf

Name of product: Cat® Bluetooth® Network
Make: Cat® Brand
Model: CATBTNT
(A5:S4)
Type: Wireless Device (Module for the reception-transmission of data from Bluetooth® Key Fob and sensors)
SMCS Code: 7008; 7600-ZM

The CATBTNT part number 504-4980 is the buy-level part that includes a radio equipment and a software tied to the machine integration. The radio equipment contained in the CATBTNT is 462-0441. Such radio equipment complies with the applicable regional product compliance requirements as demonstrated with the attached DoC. The software included in the buy-level part does not impact regulatory performance parameters.

Name of product: Cat® Bluetooth® FOB
Make: Cat® Brand
Model: CATBTFOB
(A1:S1)
Type: Wireless Device (Chip-key for operator identification with Bluetooth®)
SMCS Code: 7008; 7600-ZM

https://s7d2.scene7.com/is/content/Caterpillar/CM20201217-d18d8-0b502

INTRODUCE THE MAC ID KEY CODE
Key Code
5065
1 2 3 4 5
6 7 8 9 0
A B C
D E F
Close
OK
P/N: 487-3004-03
S/N: AK0W00DVA1
MAC ID: 5065837D1887
MODEL: CATBTFOB
CMIIT ID: 2016DJ9153
TA= 2016/2631
ASSEMBLED IN USA
TRA
REGISTERED No:
ER49295/16
DEALER No:
DA0130583/14
ictQATAR
Type Approval reg. No:
CRA/SA/2016/R-5775
This Telecommunications equipment conforms to NTC technical requirements
2:44 / 6:43

INTRODUCE THE MAC ID KEY CODE
Key Code
5065
1 2 3 4 5
6 7 8 9 0
A B C
D E F
Close
OK
Note: "50:65:83" is a Texas Instruments OUI (and all devices in my data use public TI BDADDRS)
P/N: 487-3004-03
S/N: AK0W00DVA1
MAC ID: 5065837D1887
MODEL: CATBTFOB
CMIIT ID: 2016DJ9153
TA= 2016/2631
ASSEMBLED IN USA
TRA REGISTERED No: ER49295/16 DEALER No: DA0130583/14
ictQATAR Type Approval reg. No: CRA/SA/2016/R-5775
This Telecommunications equipment conforms to NTC technical requirements
2:44 / 6:43

INTRODUCE THE MAC ID KEY CODE
Key Code
5065
1 2 3 4 5
6 7 8 9 0
A B C
D E F
Close
OK
P/N: 487-3004-03
S/N: AK0W00DVA1
MAC ID: 5065837D1887
MODEL: CATBTFOB
CMIIT ID: 2016DJ9153
TA= 2016/2631
CAT
SSEMBLED IN USA
TRA
REGISTERED No:
ER49295/16
DEALER No:
DA0130583/14
ictQATAR
Type Approval reg. No:
CRA/SA/2016/R-5775
This Telecommunications equipment conforms to NTC technical requirements
Note: "50:65:83" is a Texas Instruments OUI (and all devices in my data use public TI BDADDRS)
2:44 / 6:43

INTRODUCE THE MAC ID KEY CODE
Key Code
5065837D1
1 2 3 4 5
6 7 8 0
A B C
D E F
Close
OK
CMIIT ID: 2016DJ9153
MAC ID:
5065837D1887
2:49 / 6:43

https://fccid.io/PQMA1S1/Internal-Photos/Exhibit-C-Internal-Photographs-per-2-1033-b7-3154594.pdf

2.4-GHz *Bluetooth*™ low energy and Proprietary System-on-Chip

Check for Samples: CC2541

FEATURES

- RF
  - 2.4-GHz *Bluetooth* low energy Compliant and Proprietary RF System-on-Chip
  - Supports 250-kbps, 500-kbps, 1-Mbps, 2-Mbps Data Rates
  - Excellent Link Budget, Enabling Long-Range Applications Without External Front End
  - Programmable Output Power up to 0 dBm
  - Excellent Receiver Sensitivity (–94 dBm at 1 Mbps), Selectivity, and Blocking Performance
  - Suitable for Systems Targeting Compliance With Worldwide Radio Frequency Regulations: ETSI EN 300 328 and EN 300 440 Class 2 (Europe), FCC CFR47 Part 15 (US), and ARIB STD-T66 (Japan)
- Layout
  - Few External Components
  - Reference Design Provided
  - 6-mm × 6-mm QFN-40 Package
  - Pin-Compatible With CC2540 (When Not Using USB or I^2C)
- Low Power
  - Active-Mode RX Down to: 17.9 mA
  - Active-Mode TX (0 dBm): 18.2 mA
  - Power Mode 1 (4-μs Wake-Up): 270 μA
  - Power Mode 2 (Sleep Timer On): 1 μA
  - Power Mode 3 (External Interrupts): 0.5 μA
  - Wide Supply-Voltage Range (2 V–3.6 V)
- TPS62730 Compatible Low Power in Active Mode
  - RX Down to: 14.7 mA (3-V supply)
  - TX (0 dBm): 14.3 mA (3-V supply)
- Microcontroller
  - High-Performance and Low-Power 8051 Microcontroller Core With Code Prefetch
  - In-System-Programmable Flash, 128- or 256-KB
  - 8-KB RAM With Retention in All Power Modes
  - Hardware Debug Support
  - Extensive Baseband Automation, Including Auto-Acknowledgment and Address Decoding
  - Retention of All Relevant Registers in All Power Modes
- Peripherals
  - Powerful Five-Channel DMA
  - General-Purpose Timers (One 16-Bit, Two 8-Bit)
  - IR Generation Circuitry
  - 32-kHz Sleep Timer With Capture
  - Accurate Digital RSSI Support
  - Battery Monitor and Temperature Sensor
  - 12-Bit ADC With Eight Channels and Configurable Resolution
  - AES Security Coprocessor
  - Two Powerful USARTs With Support for Several Serial Protocols
  - 23 General-Purpose I/O Pins (21 × 4 mA, 2 × 20 mA)
  - I^2C interface
  - 2 I/O Pins Have LED Driving Capabilities
  - Watchdog Timer
  - Integrated High-Performance Comparator
- Development Tools
  - CC2541 Evaluation Module Kit (CC2541EMK)
  - CC2541 Mini Development Kit (CC2541DK-MINI)
  - SmartRF™ Software
  - IAR Embedded Workbench™ Available

Please be aware that an important notice concerning availability, standard warranty, and use in critical applications of Texas Instruments semiconductor products and disclaimers thereto appears at the end of this data sheet.

Bluetooth is a trademark of Bluetooth SIG, Inc..
ZigBee is a registered trademark of ZigBee Alliance.

PRODUCTION DATA information is current as of publication date. Products conform to specifications per the terms of the Texas Instruments standard warranty. Production processing does not necessarily include testing of all parameters.

Copyright © 2012–2013, Texas Instruments Incorporated

https://www.ti.com/lit/ds/symlink/cc2541.pdf?ts=1680851781995&ref_url=http%253A%252F%252Fwww.google.com

CC2541DK-MINI

CC2541 Mini Development Kit

Order now

Overview | Order & start development | Technical documentation | Related design resources | Support & training

Overview

Description & features Supported products

The CC2541DK-MINI development kit provides a working reference design for software development of single-mode *Bluetooth* low energy (BLE) applications based on the Texas Instruments CC2541. The included "keyfob" board operates as a BLE peripheral device, and contains modifiable software that can be tailored towards different applications. Using BTool (Windows PC application) along with the included CC2540 USB Dongle, the Texas Instruments BLE stack can be tested and verified while developing custom applications.

Features

The kit contains the following hardware components:

Shop by category

CATBTNT

All Categories

Price

$ Min to $ Max

See all

Buying Format

- All Listings
- Accepts Offers
- Auction
- Buy It Now

All Listings | Accepts Offers | Auction | Buy It Now | Condition | Shipping | Local

0 results for **CATBTNT** Save this search

Shipping to: 20705

No exact matches found

Save this search to receive email alerts and notifications when new items are available.

Save this search

Tell us what you think

CAT 5 Caterpillar Keys Loader Skidder Paver Tractor Excavator Compactor Dozer

Condition: **New**

Bulk savings:

Buy 1	Buy 2	Buy 3
$8.95/ea	$8.06/ea	$7.61/ea

4 or more for $7.16/ea

Quantity: 1 More than 10 available / **84 sold**

Price: **US $8.95/ea**

Buy It Now

Add to cart

♡ Add to Watchlist

Fast and reliable. Ships from United States.

This one's trending. 84 have already sold.

Caterpillar (CAT) Equipment Igniton / Door / Hood Key

Golden Color

Parts No: 5P8500 , 5P-8500

A package contains 5 keys

If you are fed up with heavy and thick keys, It will be your best choice

Compatible models

Wheel-Type Loader

901C 901C2 902 902C 902C2 903C 903C2 903D 904B 904H 906 906H 906H2 906K 906M 907H 907H2 907K 907M 908 908H 908H2 908K 908M 910 910E 910F 910K 910M 914G 914G2 914K 914M 916 918F 918M 920 920K 924F 924G 924GZ 924H 924HZ 924K 926 926E 926M 928F 928G 928H 928HZ 930 930G 930H 930K 930M 930R 930T 936 936E 936F 938F 938G 938G II 938H 938K 938M 950 950 GC 950B 950B/950E 950E 950F 950F II 950G 950G II 950H 950K 950L 950M 950M Z 960F 962 962G 962G II 962H 962K 962L 962M 962M Z 966 GC 966C 966D 966E 966F 966F II 966G 966G II 966H 966K 966K XE 966L 966M 966M XE 970F 972G 972G II 972H 972K 972L 972M 972M XE 980 980B 980C 980F 980F II 980G 980G II 980H 980K 980K HLG 980L 980M 980XE 982 982M 982XE 986H 986K 988 988B 988F 988F II 988G 988H 988K 988K XE 990 990 II 990H 990K 992C 992D 992G 992K 993K 994 994D 994F 994H 994K G910 G916 G926 G936

Challenger

35 45 55 65 65B 75

Engine - Generator Set

3406C 3512 3512B 3516 3516B 3516B GEN 3516C 3516E C13 C13GENSET C15 C175-16 C2.2 C32 C4.4 C6.6 C7.1 DG150 DG60 G3412C G3516H PM3412 PM3456 PM3508 PM3512 PM3516 PMG3516 XQC1200 XQC1600 XQG400

Wheel-Type Skidder

120C 508 515 518 518C 525 525B 525C 525D 528 528B 530B 535B 535C 535D 545 545C 545D 555D

Off-Highway Truck

69D 768C 769 769B 769C 769D 770 770G 770G OEM 771C 771D 772 772B 772G 772G OEM 773B 773D 773E 773F 773G 773G LRC 773G OEM 773GC 775B 775D 775E 775F 775G 775G LRC 775G OEM 776 776B 776C 776D 777 777B 777C 777D 777E 777F 777G 784B 784C 785 785B 785C 785D 785G 789 789B 789C 789D 789G 793 793B 793C 793D 793F 793F AC 793F CMD 793F OEM 793F XQ 794 AC 795F AC 795F XQ 796 AC 797 797B 797F 798 798 AC

Track-Type Loader

931 931B 931C 931C II 933 933C 935B 935C 935C II 939 939C 941 943 951 951B 951C 953 953B 953C 953D 953K 955 955L 963 963B 963C 963D 963K 973 973C 973D 973K 977 977L 983 983B

Engine - Industrial

3126B 3176C 3196 3306B 3406C 3406E 3408E 3412 3412C 3412E 3456 3508 3508B 3512 3512B 3512C 3516 3516B 3516C 3516E C-10 C-12 C-15 C-16 C-9 C11 C13 C13B C15 C15 I6 C175-16 C18 C18 I6 C27 C32 C4.4 C7 C9 C9 GEN SET C9.3 C9.3B DG100 DG125 DG60 DG80 G3508 G3512 G3512E G3512H G3516 G3516B G3516C G3516E G3516H G3520 G3520C G3520E G3520H PM3412

Articulated Dump Truck

725 725C 725C2 730 730C 730C2 730C2 EJ 735 735 OEM 735B 735C 740 740 GC 740B 740C 745 745C D20D D250B D250D D250E D250E II D25C D25D D300B D300D D300E D300E II D30C D30D D350C D350D D350E D350E II D35C D35HP D400 D400D D400E D400E II D40D

Mini Hydraulic Excavator

300.9D 301.4C 301.5 301.6 301.6C 301.7D 301.7D CR 301.8 301.8C 302.2D 302.4D 302.5 302.5C 302.7D 303 303.5 303.5C 303.5D 303.5E 303.5E2 303.5E2 CR 303E CR 304 304.5 304.5E2 304E 304E2 304E2 CR 305 305.5 305.5D 305.5E 305.5E2 305.5E2 CR 305C CR 305D CR 305E 305E2 305E2 CR 306 306.5 306E 306E2 307 307-A 307.5 307B 307D 307E 307E2 308 308.5 308D 308E 308E2 308E2 CR 309 310

Road Reclaimer

RM-250C RM-300 RM-350 RM-350B RM-500 RM400 RM500B RR-250 RR-250B SM-350 SS-250 SS-250B

Motor Grader

120 120G 120H 120H ES 120H NA 120K 120K 2 120M 120M 2 12F 12G 12H 12H ES 12H NA 12K 12M 12M 2 12M 3 12M 3 AWD 130G 135H 135H NA 14 140 140 GC 140G 140H 140H ES 140H NA 140K 140K 2 140M 140M 2 140M 3 140M 3 AWD 143H 14G 14H 14H NA 14L 14M 14M-3 14M3 150 16 160 160G 160H 160H ES 160H NA 160K 160M 160M 2 160M 3 160M 3 AWD 163H 163H NA 16G 16H 16H NA 16M 16M3 18 18M3 24 24H 24M 404F-22

Track-Type Skidder

120C 125C 4P 517 527 54H D4HTSK II D4HTSK III D5HTSK II

TELEHANDLER

RT100 RT50 RT50SA RT60 RT80 RTC60 TH103 TH210 TH215 TH220B TH255C TH306D TH314D TH330B TH336C TH337C TH340B TH350B TH3510D TH355B TH357D TH360B TH406C TH407C TH408D TH414C TH417C TH417D TH460B TH514C TH514D TH560B TH580B TH62 TH63 TH82 TH83 TL1055C TL1055D TL1255C TL1255D TL642C TL642D TL943C TL943D

Wheel Dozer

814 814B 814F 814F II 814K 824B 824C 824G 824G II 824H 824K 824S 834 834B 834G 834H 834K 834S 834U 844 844H 844K 854G 854K

Backhoe Loader

414E 415 415F2 415F2 IL 416 416B 416C 416D 416E 416F 416F2 420 420D 420E 420F 420F2 420XE 422E 422F 422F2 424B 424B HD 424B2 424D 426 F2 426B 426C 427F2 428 428B 428C 428D 428E 428F 428F2 430 430D 430E 430F 430F2 432 432D 432E 432F 432F2 434 434E 434F 434F2 436B 436C 438B 438C 438D 440 442D 442E 444 444E 444F 444F2 446B 446D 450 450E 450F

Skid Steer Loader

216 216B 216B3 226 226B 226B3 226D 226D3 232B 232D3 236 236B 236B3 236D 236D3 239D3 242B 242B3 242D 242D3 246 246B 246C 246D 246D3 247B 247B3 248B 249D 249D3 252 252B 252B3 256C 257B 257B3 257D 257D3 259B3 259D 259D3 262 262B 262C 262C2 262D 262D3 267 267B 268B 272C 272D 272D XHP 272D2 272D2 XHP 272D3 272D3 XE 277 277B 277C 277C2 277D 279C 279C2 279D 279D3 287 287B 287C 287C2 287D 289C 289C2 289D 289D3 297C 297D 297D XHP 297D2 297D2 XHP 299C 299D 299D XHP 299D2 299D2 XHP 299D3 299D3 XE

Asphalt Paver

10 FT 10-20B 10-20WB 10B 8 FT 8-16B AP-1000 AP-1000B AP-1000D AP-1000E AP-1000F AP-1050 AP-1050B AP-1055B AP-1055D AP-1055E AP-1055F AP-200 AP-200B AP-255E AP-300D AP-500E AP-555E AP-600D AP-650B AP-655C AP-655D AP-800 AP-800B AP-800C AP-800D AP-900B AP300F AP355F AP500F AP555F AP600F AP655F AP655F L AS2251 AS2252C AS2301 AS2302 AS2302C AS3251C AS3301C AS4252C BG-2255C BG-225C BG-230 BG-230D BG-240C BG-2455C BG-2455D BG-245C BG-260C BG-260D BG1000E BG1055E BG500E BG555E BG600D BG655D SE50 V SE50 VT SE60 V SE60 V XW SE60 VT XW SE60VT XW

Pipelayer

561D 561M 561N 571G 572G 572R 572R II 578 583K 583R 583T 587R 587T 589 594H PL61 PL72 PL83 PL87

Integrated Toolcarrier

IT12 IT12B IT14B IT14F IT14G IT14G2 IT18 IT18B IT18F IT24F IT28 IT28B IT28F IT28G IT38F IT38G IT38G II IT38H IT62G IT62G II IT62H

Marine Products

3126B 3412E 3508B 3512B 3516B C12 C30 C32 C7 C9

Expanded Mining Products

6015B 6020B MD5150C MD6200 MD6250 MD6310 MD6640

Track-Type Tractor

10 10C 10S 10SU 10U 11 11SU 11U 140 141 143 153 163 183B 3 3P 3S 4 4A 4P 4S 5 53 54 55 56 56H 57 57H 58 58L 59 59L 59N 5A 5A PAT 5P 5S 6 6A 6S 6SU 7 7A 7S 7S LGP 7SU 7U 8 8A 8D 8S 8SU 8U 9 9C 9S 9SU 9U D1 D10 D10N D10R D10T D10T2 D11 D11N D11R D11T D2 D3 D3B D3C D3C II D3C III D3G D3K LGP D3K XL D3K2 LGP D3K2 XL D4 D4B D4C D4C II D4C III D4D D4E D4E SR D4G D4H D4H III D4H XL D4K LGP D4K XL D4K2 LGP D4K2 XL D5 D5B D5C D5C III D5C PAT D5C PATLGP D5E D5G D5H D5H XL D5K LGP D5K XL D5K2 LGP D5K2 XL D5M D5N D5R2 D6 D6 XE D6C D6D D6D SR D6E D6E SR D6F SR D6G D6G SR D6G2 LGP D6G2 XL D6GC D6H D6H II D6H XL D6H XR D6K D6K LGP D6K XL D6K2 D6K2 LGP D6K2 XL D6M D6N D6N LGP D6N OEM D6N XL D6R D6R II D6R III D6R LGP D6R STD D6R XL D6T D6T LGP D6T LGPPAT D6T XL D6T XL PAT D6T XW D6T XW PAT D6XE D7E D7E LGP D7F D7G D7G2 D7H D7R D7R II D7R LGP D7R SERIES D7R XR D8H D8K D8L D8N D8R D8R II D8T D9G D9H D9L D9N D9R D9T

Load, Haul, Dump

R1300 R1300G R1300G II R1600 R1600G R1600H R1700 II R1700G R1700K R2900 R2900G R3000H

Utility Vehicle

CUV102D CUV105D CUV82 CUV85

Oem Solutions

CAT WDS

eBay

FCC

User Manual

Me: It's probably possible to steal expensive construction equipment with a Bluetooth exploit!

Me: It's probably possible to steal expensive construction equipment with a Bluetooth exploit!
Them: The physical security baseline for construction equipment is very low, and it's actually super easy to steal them with cheap universal physical keys...

Me: It's probably possible to steal expensive construction equipment with a Bluetooth exploit!
Them: The physical security baseline for construction equipment is very low, and it's actually super easy to steal them with cheap universal physical keys...
Me:

So...This is Actually A Security Win?!

- If my understanding is correct, and the prior state of physical security for these devices was that it only required a universal physical key to steal one of them[1]...
- Then clearly adding a BT proximity requirement is a ***net security improvement!***
- An important reminder to consider the *total threat model*

[1]https://www.quora.com/Is-it-true-that-you-can-operate-all-Caterpillar-machinery-with-one-key

End - Anecdotes - Devices

Final Takeaways 1

- *Bluetooth sniffing goals are different from WiFi goals*, and consequently the sniffing tech is under-developed to help with those goals
- When there's a BT FW bug, **no one knows what all it affects**

Final Takeaways 2

- There are lots of devices that are advertising names, but it's not clear what they are
  - I'm looking at you "***UGZZF_X[AB10]{4}***"
  - Somebody ought to start a database! Or at least a wiki?!
- There are lots of devices that do not have human-readable names, so it's not clear what they are
  - *Somebody (/me!)* ought to start learning to *toothprint* BT devices!

Call To Action!

Call To Action!

- WiGLE's Android app is open source! If you know Android development, it'd be great if you could help them get more Bluetooth info collected within WiGLE
- I'd like to crowdsource more information, but my web-fu is weak
  - I could use help creating a website that allows people to contribute as well as query this kind of information
- Go collect some information and then share what you find out
  - My data will be available to other researchers on a "share and share alike" basis - you need to collect some useful information that you share with me, and then I'll share my data back

https://github.com/darkmentorllc/naiveBTsniffing

Conclusion

What I now know I didn't know

- Basic Bluetooth sniffing can *sometimes* give me some of the information I'm looking for, in a roundabout way:
  - If the BDADDR is for a BT Classic device or BLE Public device, if OUI is a silicon vendor (like Texas Instruments), this provides a good indication of which chip they're likely using
    - The same holds true for two other 16-bit IDs that have assigned companies according to the BT assigned numbers document (Member UUID16 and BT Member Company ID)

Conclusion

What I now know I didn't know

- Some of the information mentioned in the BT spec that would help point at which BT chip a device uses, is not exposed
  - Therefore I need to collect it myself...

Conclusio

What I now kn

- Some of the inf
  which BT chip a
  - Therefore I ne

Conclusion

What I now know

Stay tuned (@XenoKovah) for the next research!

Conclusion

What I now know

Stay tuned (@XenoKovah) for the next research!

Fin

- BT research is cool
- But *OpenSecurityTraining2 (https://ost2.fyi, @OpenSecTraining) is cooler!*
  - We'll have BT classes eventually, but in the meantime there's so much other stuff to learn! Reverse Engineering, Vulnerabilities, Firmware, System Architecture!
- You should take a class, or *teach* a class!