Breaking the Internet of Vibrating Things

What we learned reverse-engineering Bluetooth- and internet- enabled adult toys

g0ldfisk & follower

DEF CON 2016

Content Advisory

Our intent is to create an inclusive & safe environment for everyone to learn about a topic that relates to sexuality and technology.

There are no sexually explicit descriptions or images in this talk. We briefly mention legal aspects related to sexual assault.

Our focus is on the technology aspect of this subject.

When you talk with people about this talk, ensure you have their consent before discussing any sexual aspect of this talk. Ensuring consent means making sure the person is comfortable talking about this topic with you.

Bluetooth devices are everywhere...

...now even adult toys are connected.

What could go wrong?

“Security, more like SEX-curity, amirite?”

What’s actually at stake?

“...We-Vibe®, the world’s number #1
vibrator for couples.
Used by over 2 million people...”

— standardinnovation.com

What's at stake:

Control

“Turning a sex toy on is not really a serious issue…”

— hackread.com/internet-connected-sex-toys-can-be-hacked/

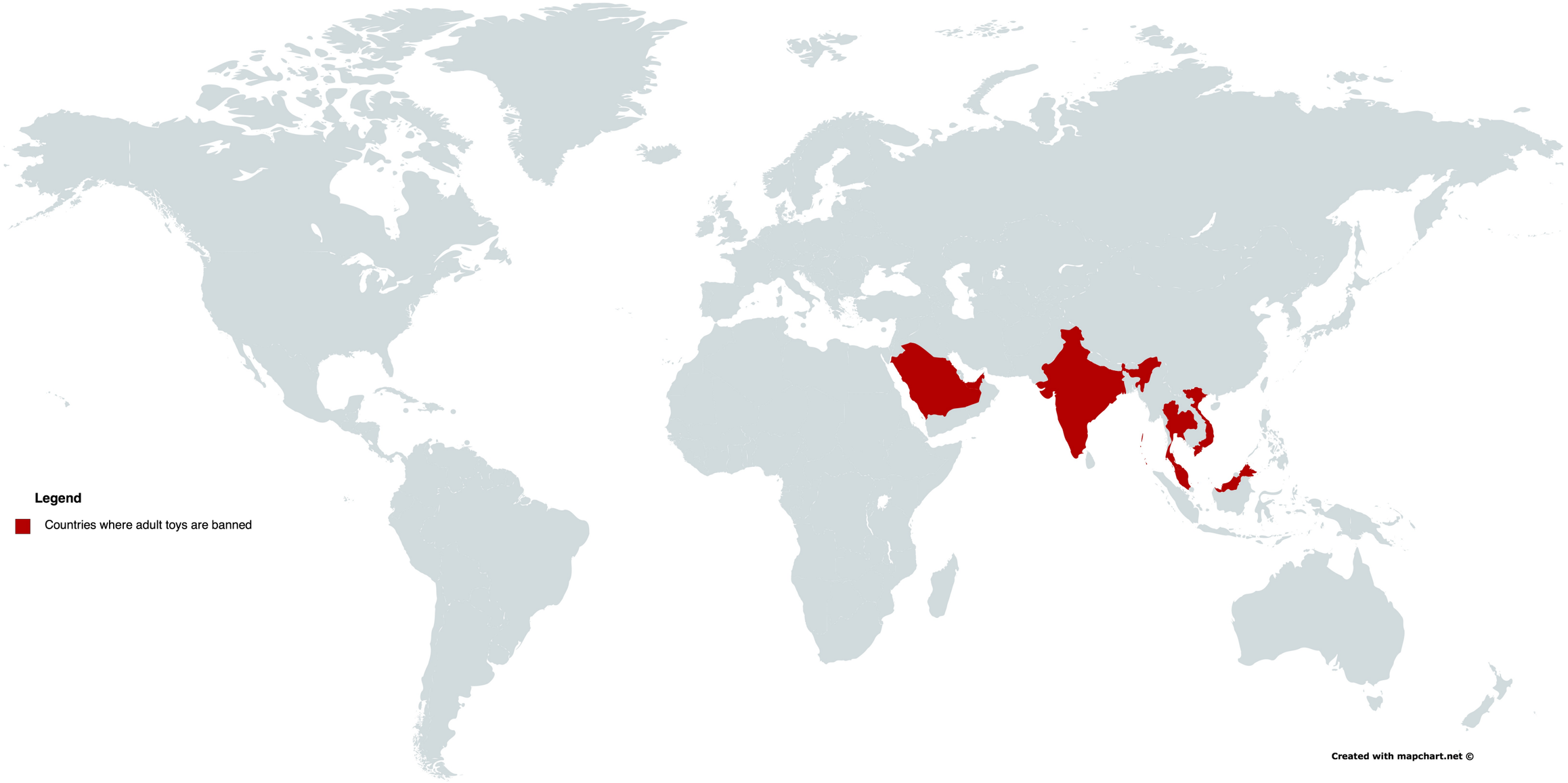
“If I hack a vibrator it’s just fun, but if I can get to the back-end, I can blackmail the manufacturer.”

— Trend Micro CTO reuters.com/article/us-germany-cyber-idUSKCN0WH1YU

Light bulb --> Vibrator --> Pacemaker

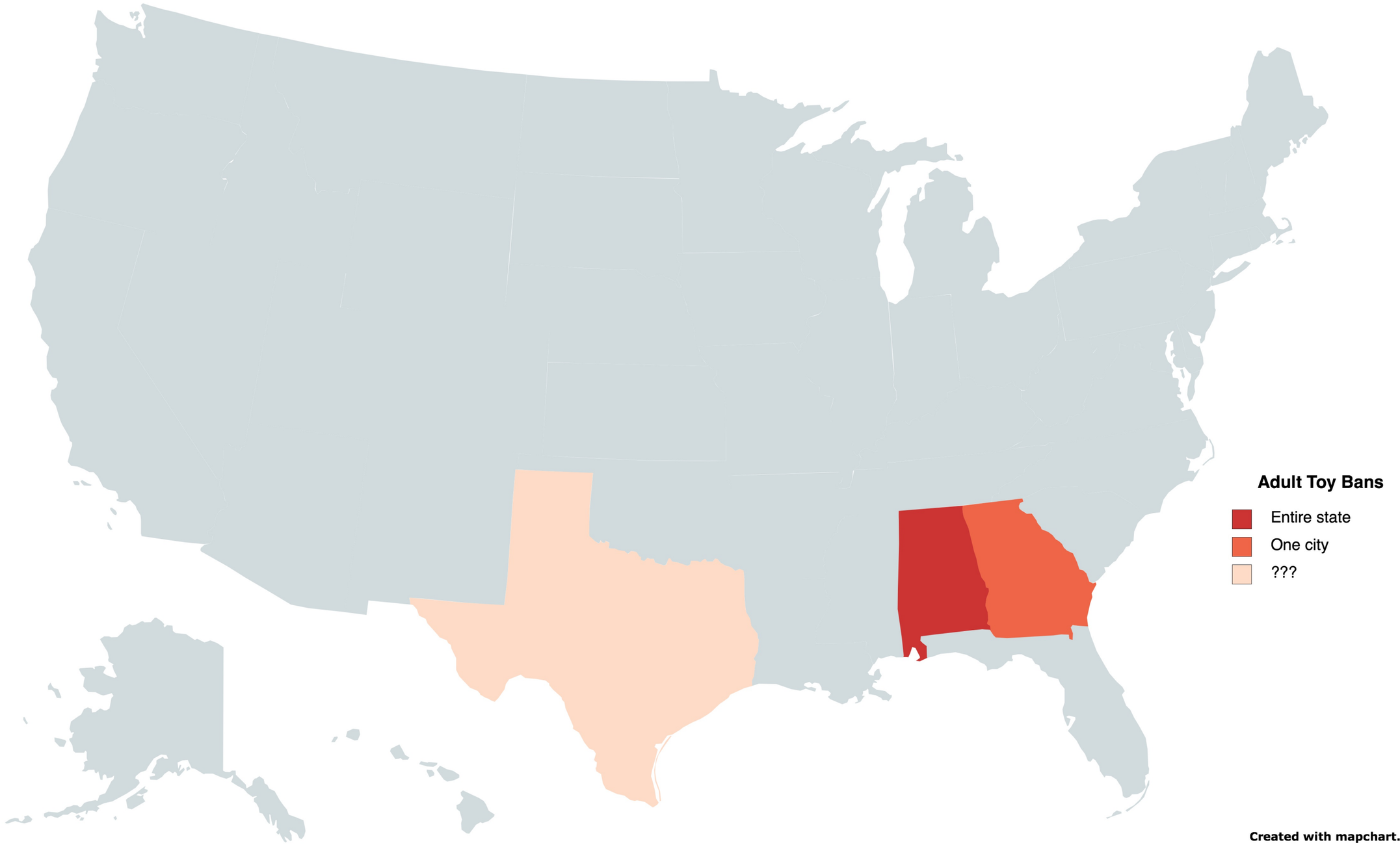
What's at stake:

Tracking/Detection


Legend
Countries where adult toys are banned
Created with mapchart.net ©

“A lesbian couple in Malaysia
was arrested for homosexual conduct
after a vibrator was uncovered in their hotel room.”

— sheswanderful.com/2015/04/16/getting-sex-toys-security-6-things-consider-traveling-birth-control-sex-toys/


Adult Toy Bans
Entire state
One city
???
Created with mapchart.net ©

Privacy

Who can get their hands on information about you?

Who is the bigger risk?

“…dedicated itself to transforming the lives of couples in committed relationships…”

— standardinnovation.com

“We reserve the right to disclose your personally identifiable information if required to by law.”

— standardinnovation.com

We Vibe 4 Plus

JSON Temperature data

```
{
    "batteryPercentage": "59",
     "deviceTemperature": "58",
    "eventTime": "2016-07-20T17:09:46+1200",
    "index": 0
}
```

(once per minute)

POST
https://<domain>/rest/users/profiles/<id>/usersessions/<id>/devicesessions/<id>/sessioninfo

JSON mode/intensity data

```
{
    "eventTime": "2016-07-20T17:13:04+1200",
    "index": 0,
     "intensity": 707,
     "vibrationMode": 3
}

{
    "eventTime": "2016-07-20T17:15:19+1200",
    "index": 0,
     "intensity": 703,
    "vibrationMode": 3
}
```

(real time, per event)

`POST https://<domain>/rest/users/profiles/<id>/usersessions/<id>/modechanged`

How can you avoid this information disclosure?

Use your We Vibe as a “dumb vibe”

How can you avoid this information disclosure?

Use your We Vibe as a “dumb vibe”

Only use the remote control

How can you avoid this information disclosure?

Use your We Vibe as a “dumb vibe”

Only use the remote control

Use the app in airplane mode

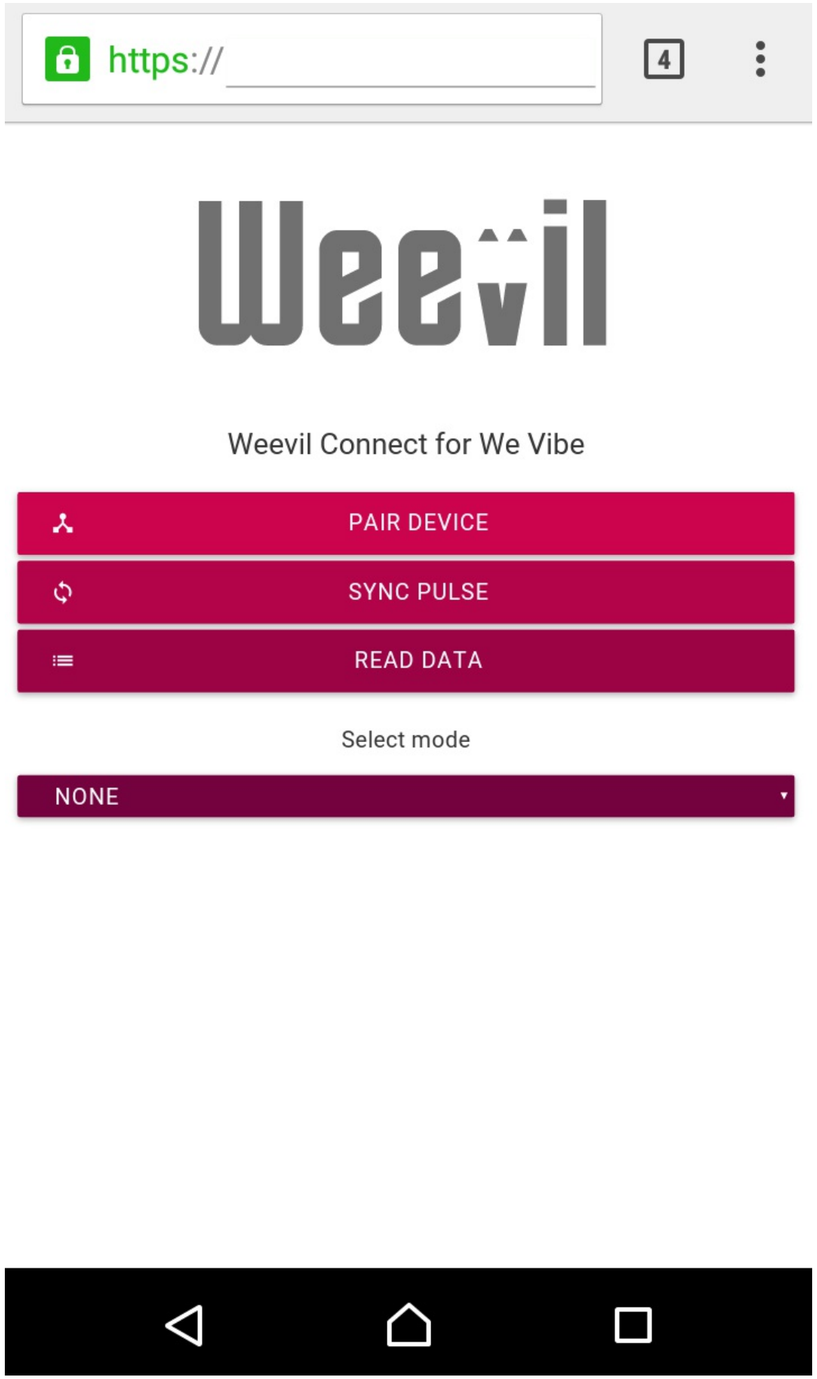
How can you avoid this information disclosure?

Use your We Vibe as a “dumb vibe”

Only use the remote control

Use the app in airplane mode

Block access to `wvdata.sic-apps.net` via firewall/DNS



Or... use Weevil Connect!

Implemented using Web Bluetooth

Part of our Weevil suite of tools

Announcing: The Private Play Accord

Goal: Protect people's privacy

Promote transparency of manufacturer data collection

Enable manufacturers to signal the steps they take to protect privacy

www.privateplayaccord.com

Private Play Accord: Starting the conversation

Contacted 8 manufacturers, retailers & reviewers.

Private Play Accord: Draft product rating system

★★★ – No usage data is collected, stored, transmitted or used.

★★☆ – People can explicitly opt-in to collection of limited data.

★☆☆ – People can explicitly opt-out of collection of limited data and clearly informed of this.

☆☆☆ – Usage data is collected, stored, transmitted and/or used with no ability to opt-out.

Private Play Accord: How you can help

Research other products to find out what data they are recording and transmitting.

Here’s what we did

And some tools we used.

And some tools we created for you!

We start with three questions

What does the product (i.e. device + app) do?

We start with three questions

What does the product (i.e. device + app) do?

And how does it do it?

We start with three questions

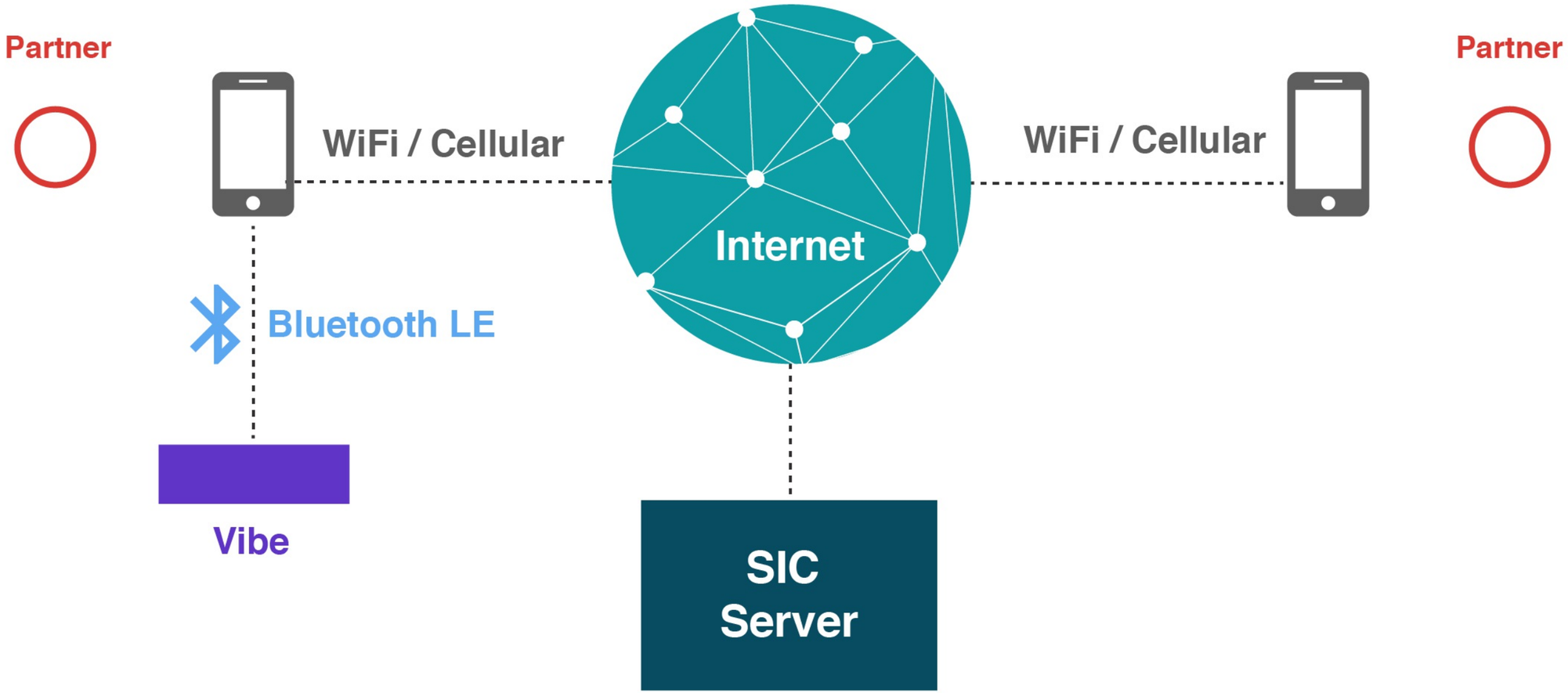
What does the product (i.e. device + app) do?

And how does it do it?

(And how can we get control of it?)

Hardware: the We Vibe 4 Plus

Software:
The We-Connect app


Partner
WiFi / Cellular
Internet
WiFi / Cellular
Partner
Bluetooth LE
Vibe
SIC
Server

HTTP

mitmproxy

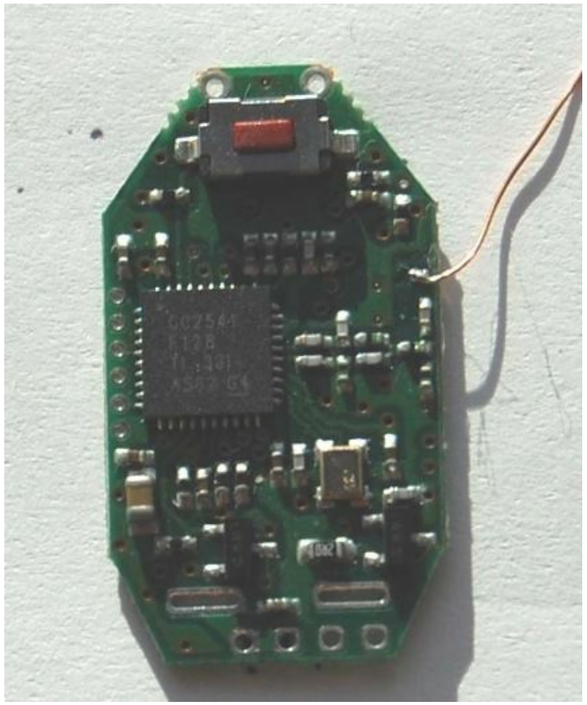
Certificate pinning

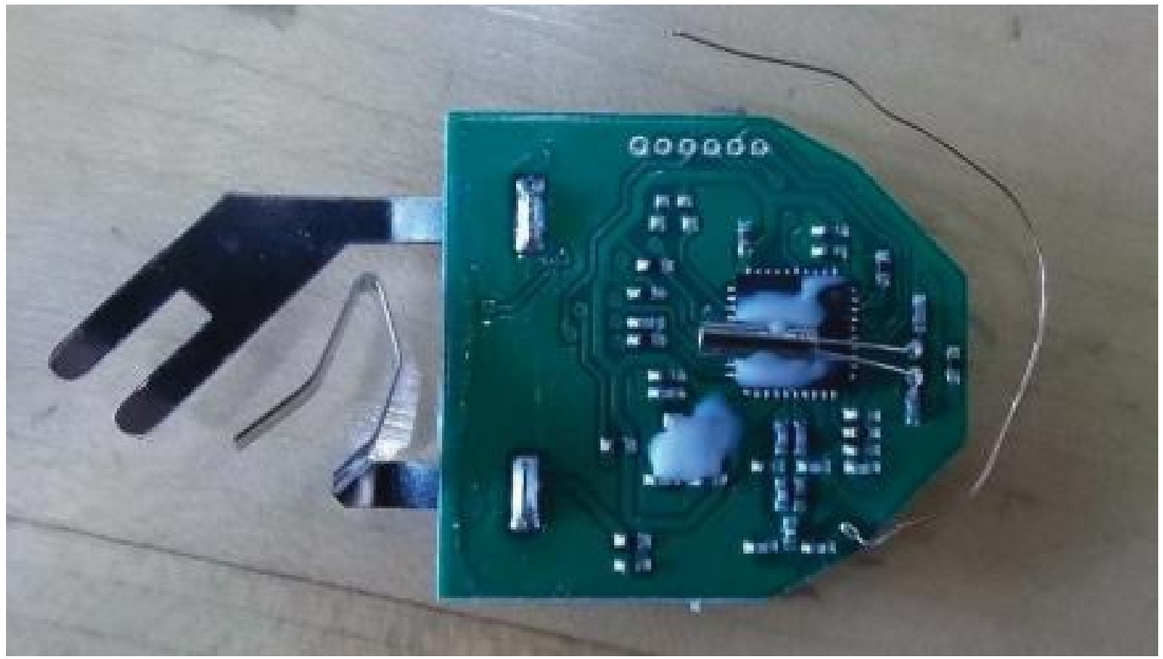
Hardware

FCC

Information required for certification.

Includes internal photos!





What's inside?

Texas Instruments CC2541 - 2.4GHz Bluetooth Smart/Low Energy

(IAR Compiler $3,000)

Confidential

FCC doesn't show everything of course.

FCC ID: ZUE1000

Product Name: We-Vibe Universal PCBA

Request for Confidentiality

Pursuant to Sections 0.457 and 0.459 of the commission's rules, we hereby request that the following documents be held confidential:

- Schematics
- Block diagram
- Bill of Materials
- Operational Description

These materials contain trade secrets and proprietary information and are not customarily released to the public. The public disclosure of this information might be harmful to the company and provide unjustified benefits to our competitors.

Mistakes were made

OET Exhibits List

14 Matches found for FCC ID ZUE1000

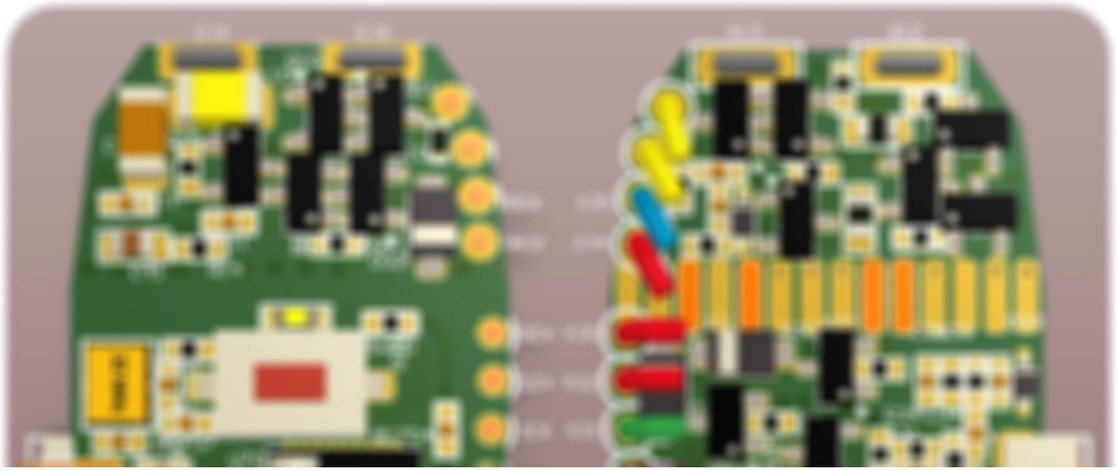
View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Cover Letters	Cover Letter(s)	02/25/2016	pdf	02/25/2016
Cover Letters	Cover Letter(s)	02/25/2016	pdf	02/25/2016
Cover Letters	Cover Letter(s)	02/25/2016	pdf	02/25/2016
External Photos	External Photos	02/25/2016	pdf	02/25/2016
Label and Label Location info	ID Label/Location Info	02/25/2016	pdf	02/25/2016
Internal Photos	Internal Photos	02/25/2016	pdf	02/25/2016
Operational Description	Operational Description	02/25/2016	pdf	02/25/2016
RF Exposure info	RF Exposure Info	02/25/2016	pdf	02/25/2016
Test Report	Test Report	02/25/2016	pdf	02/25/2016
Test Setup Photos	Test Setup Photos	02/25/2016	pdf	02/25/2016
Users Manual	Users Manual	02/25/2016	pdf	02/25/2016
Users Manual	Users Manual	02/25/2016	pdf	02/25/2016
Users Manual	Users Manual	02/25/2016	pdf	02/25/2016
Users Manual	Users Manual	02/25/2016	pdf	02/25/2016

Whoops...

WeVibe 5: HW/FW Platform PCB

Design Document

Revision: 18
(In Progress)

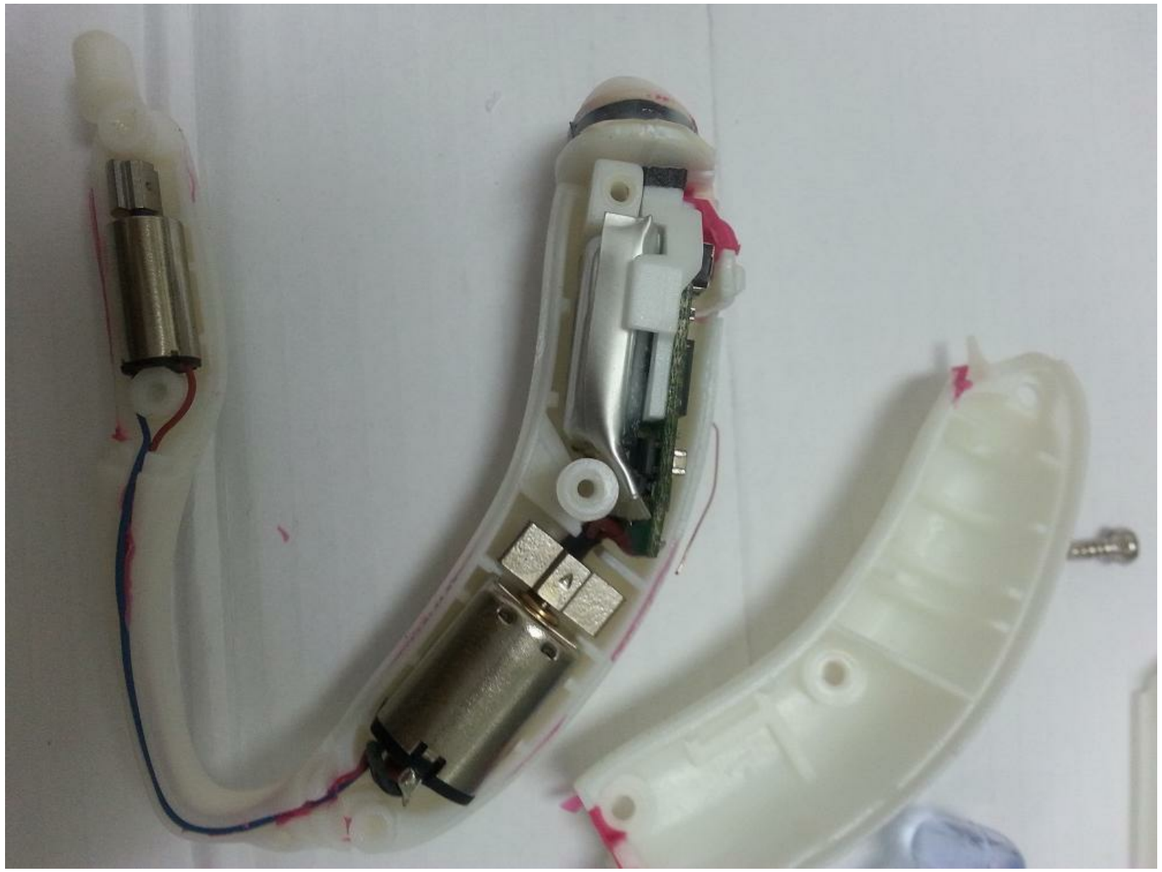


Don’t do drugs, kids.

In signing this letter, Applicant certifies that neither the applicant nor any party to the application is not subject to a denial of Federal benefits, that include FCC benefits, pursuant to Section 5301 of the Anti-Drug Abuse Act of 1988, 21 U.S.C. § 862 because of a conviction for possession or distribution of a controlled substance.
See 47 CFR 1.2002(b) for the definition of a "party" for these purposes.

Other options

e.g. Existing tear downs



The Remote

How can we control the device?

We know it uses Bluetooth LE

What is Bluetooth LE?

a.k.a. Bluetooth Smart (marketing, yay!)

What is Bluetooth LE?

a.k.a. Bluetooth Smart (marketing, yay!)

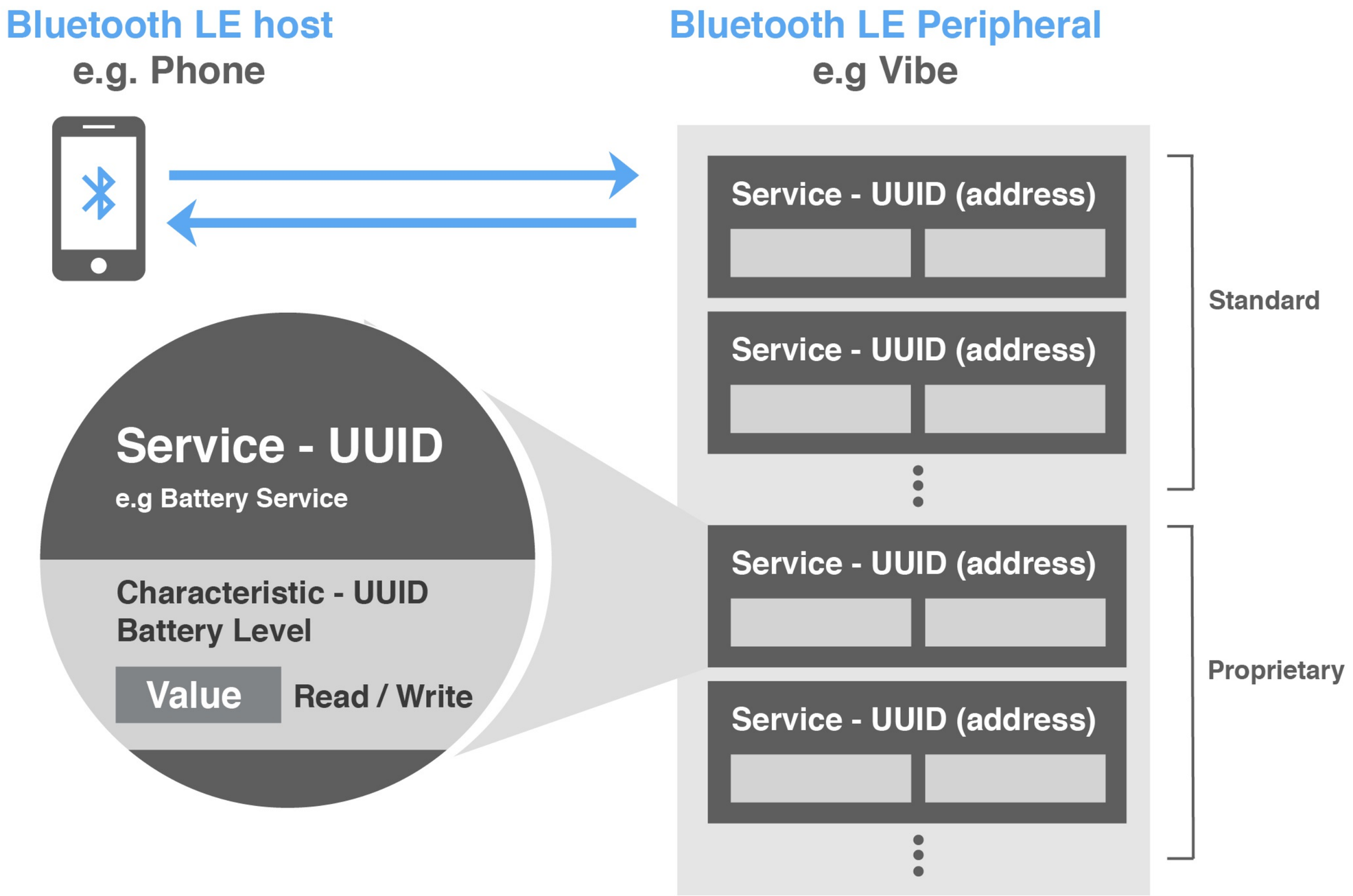
Central vs. Peripheral

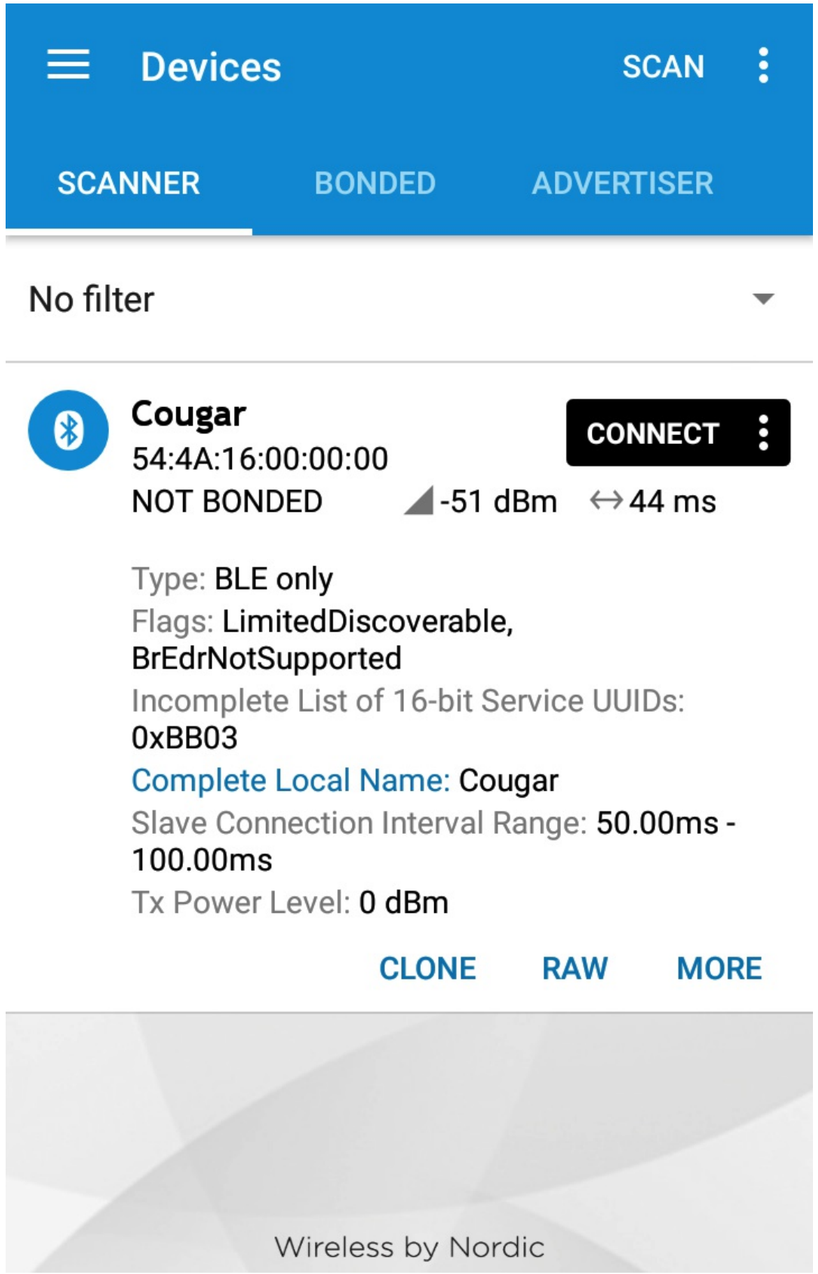
What is Bluetooth LE?

a.k.a. Bluetooth Smart (marketing, yay!)

Central vs. Peripheral

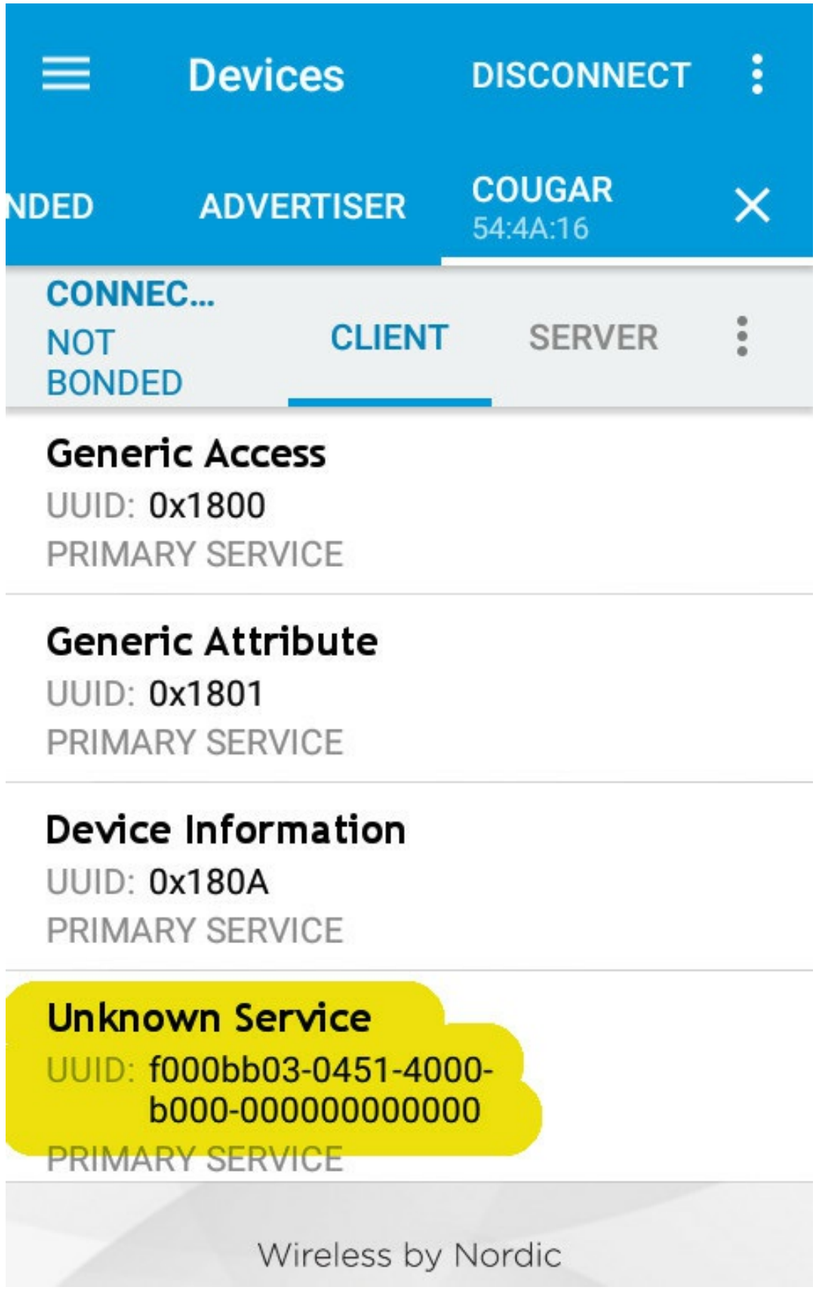
UUIDs, Services, Characteristics

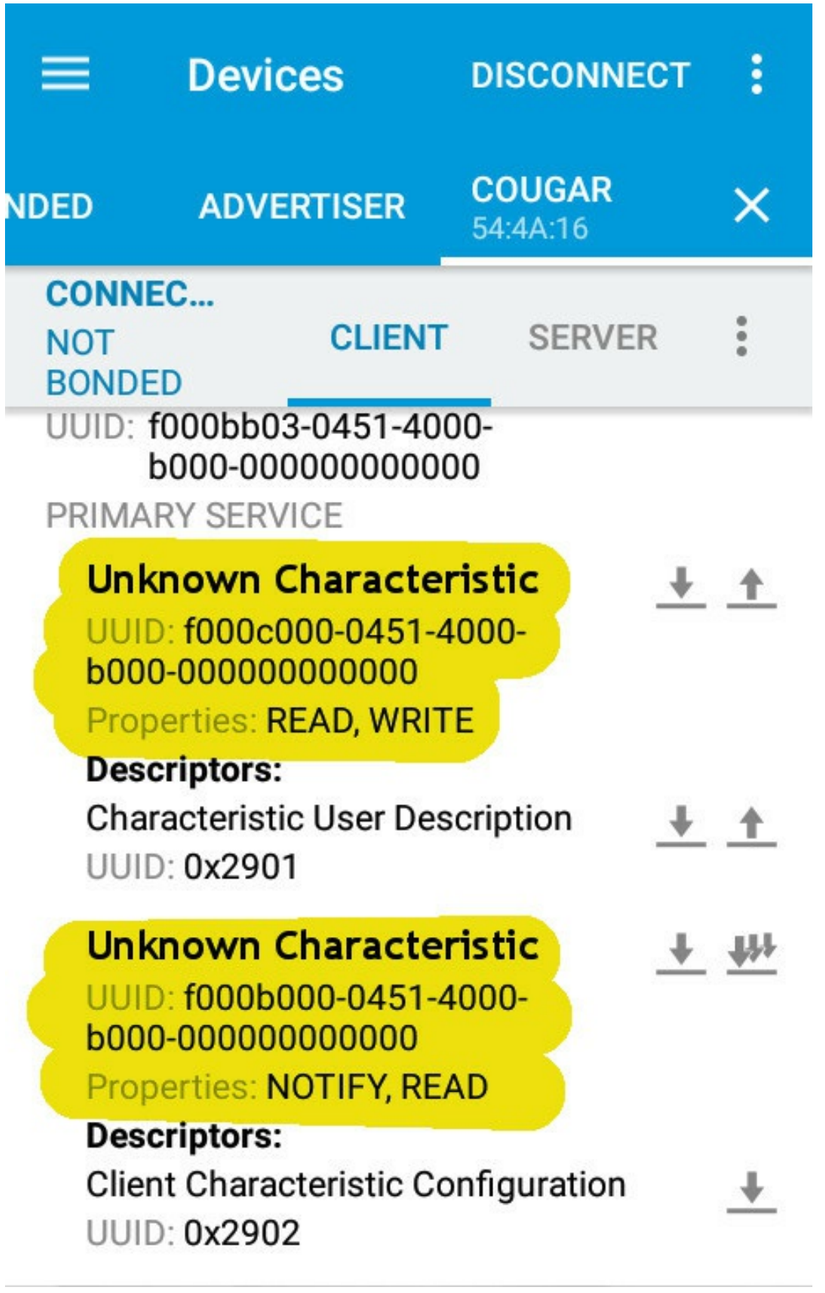

Bluetooth LE host
e.g. Phone
Bluetooth LE Peripheral
e.g Vibe
Service - UUID (address)
Service - UUID (address)
Service - UUID (address)
Service - UUID (address)
Standard
Proprietary
Service - UUID
e.g Battery Service
Characteristic - UUID
Battery Level
Value
Read / Write



Nordic nRF Connect for mobile

(a.k.a nRF Master Control Panel)


Devices
DISCONNECT
NDED
ADVERTISER
COUGAR
54:4A:16
CONNEC...
NOT BONDED
CLIENT
SERVER
Generic Access
UUID: 0x1800
PRIMARY SERVICE
Generic Attribute
UUID: 0x1801
PRIMARY SERVICE
Device Information
UUID: 0x180A
PRIMARY SERVICE
Unknown Service
UUID: f000bb03-0451-4000-b000-000000000000
PRIMARY SERVICE
Wireless by Nordic


Devices
DISCONNECT
NDED
ADVERTISER
COUGAR
54:4A:16
CONNEC...
NOT BONDED
CLIENT
SERVER
UUID: f000bb03-0451-4000-b000-000000000000
PRIMARY SERVICE
Unknown Characteristic
UUID: f000c000-0451-4000-b000-000000000000
Properties: READ, WRITE
Descriptors:
Characteristic User Description
UUID: 0x2901
Unknown Characteristic
UUID: f000b000-0451-4000-b000-000000000000
Properties: NOTIFY, READ
Descriptors:
Client Characteristic Configuration
UUID: 0x2902

Unpacking the APK

APK file is how Android apps are distributed
(. `zip` format archive of many different files)

Unpacking the APK

APK file is how Android apps are distributed
(. `zip` format archive of many different files)

Acquire the .apk via apkpure.com

Unpacking the APK

APK file is how Android apps are distributed
(. `zip` format archive of many different files)

Acquire the .apk via apkpure.com

Decompile the .apk via javadecompilers.com/apk

What we found

com/standardinnovation/mobile/bluetooth/device/bluetooth/command/SyncPulseCommand.java

```
public class SyncPulseCommand extends SimpleWriteListener implements Command {
    public List<int[]> getData(StdiDeviceModel model) {
        List<int[]> data = new ArrayList();
         data.add(new int[]{30, 32, 45, 0, 0, 0, 0, 0});
        return data;
    }
}
```

State of cross-platform Bluetooth LE support

Python — Linux / OS X (Various)

Node.js — Linux / OS X / Windows (`noble` & `bleno`)

noble & bleno

Node.js libraries for controlling or simulating a BLE device

github.com/sandeepmistry/noble (central)

github.com/sandeepmistry/bleno (peripheral)

noble for controlling the device

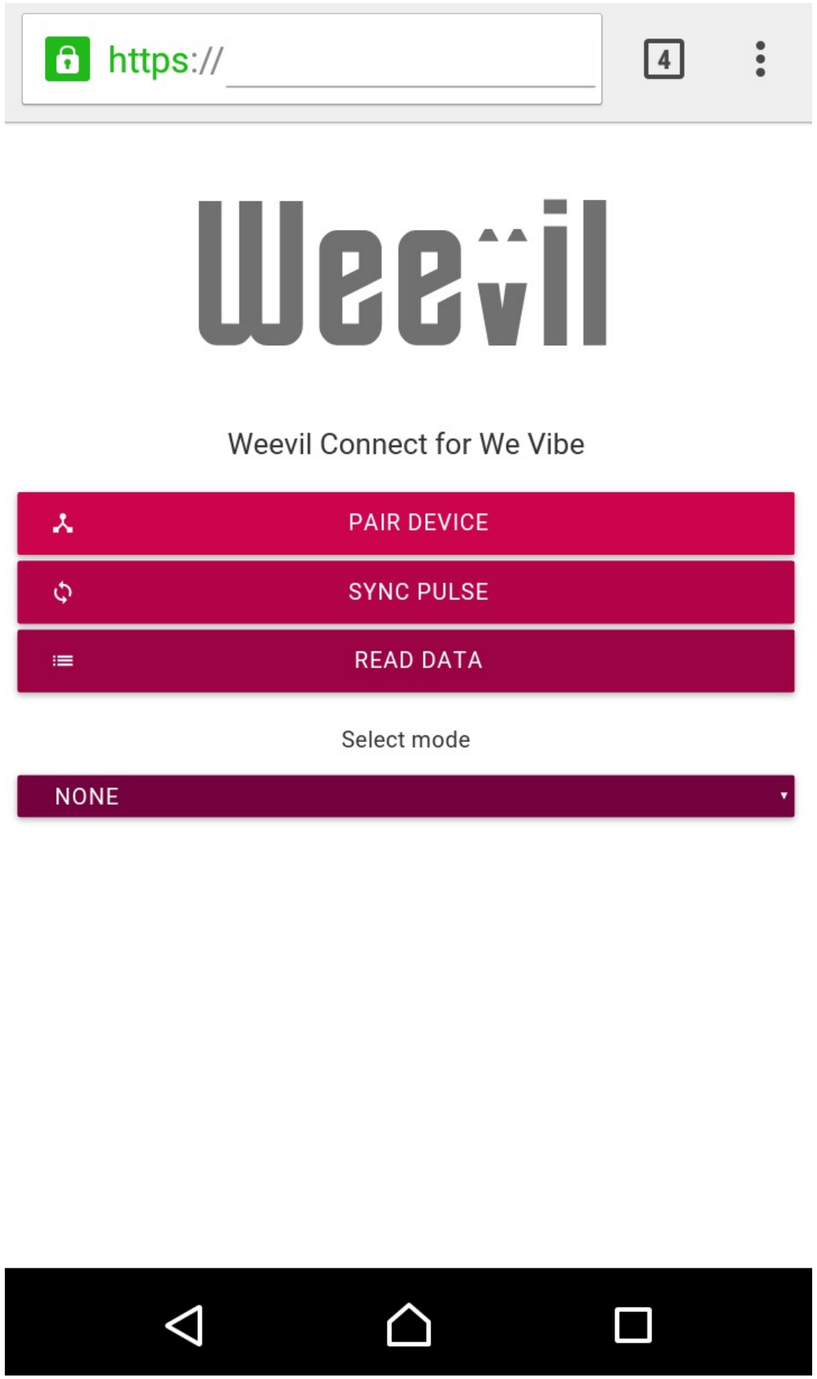
Set patterns & intensities

Getting extra info e.g. temperature, battery

bleno for impersonating device

Recognised by mobile app

Not yet recognised by remote

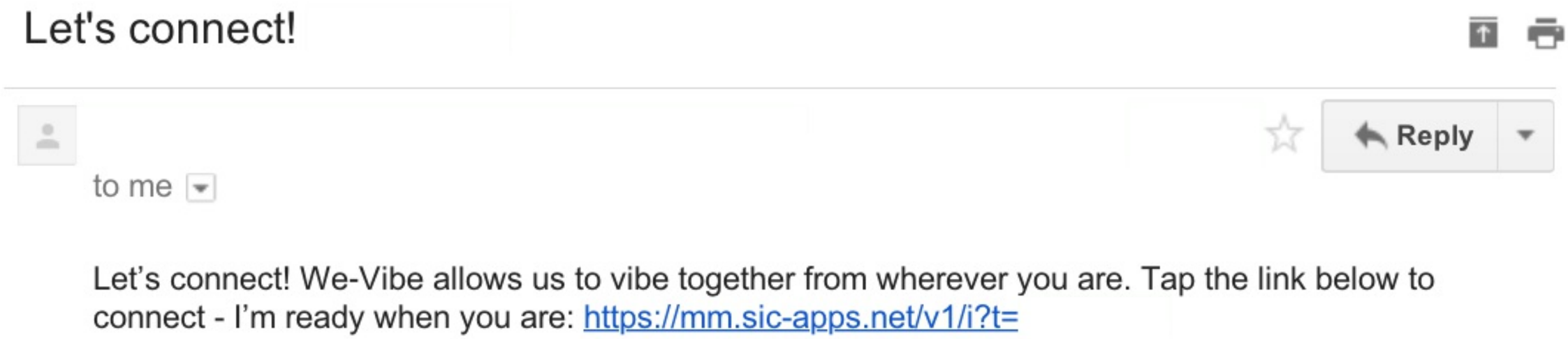


Weevil Connect (Web Bluetooth)

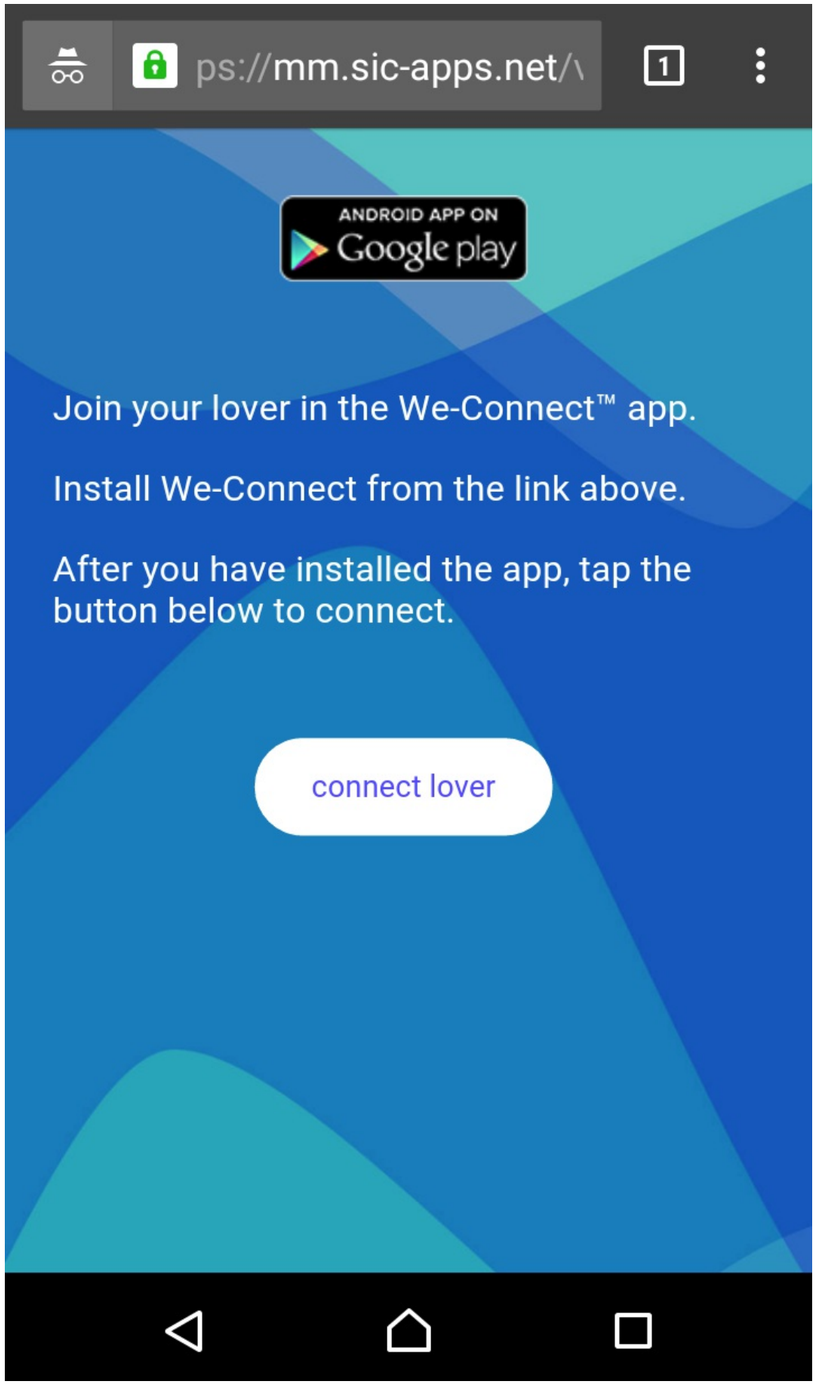
Chromium / Chrome

What we learned: Incorrect invitation expiry

Connect Invitation Process



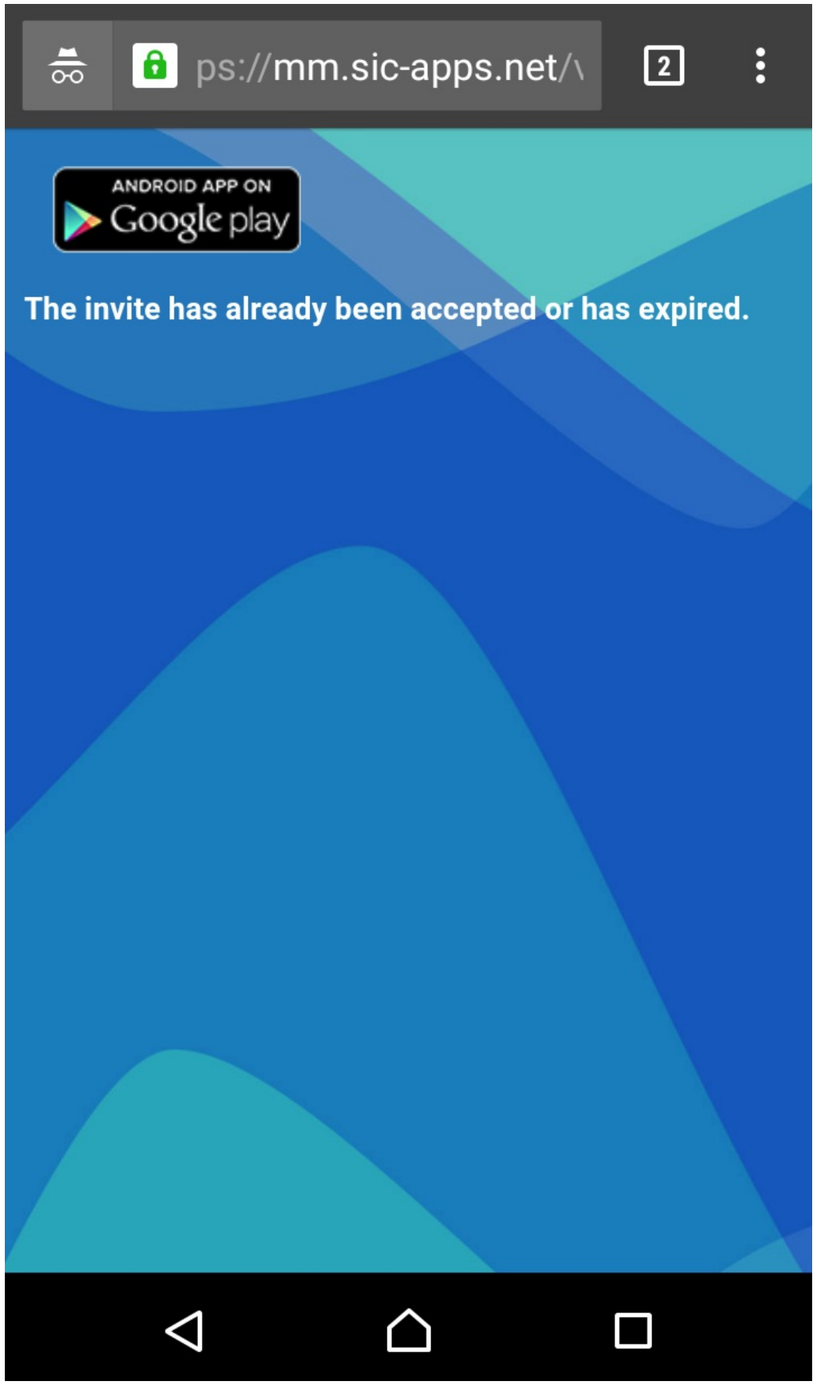
(Also via Facebook and SMS)



App installation page

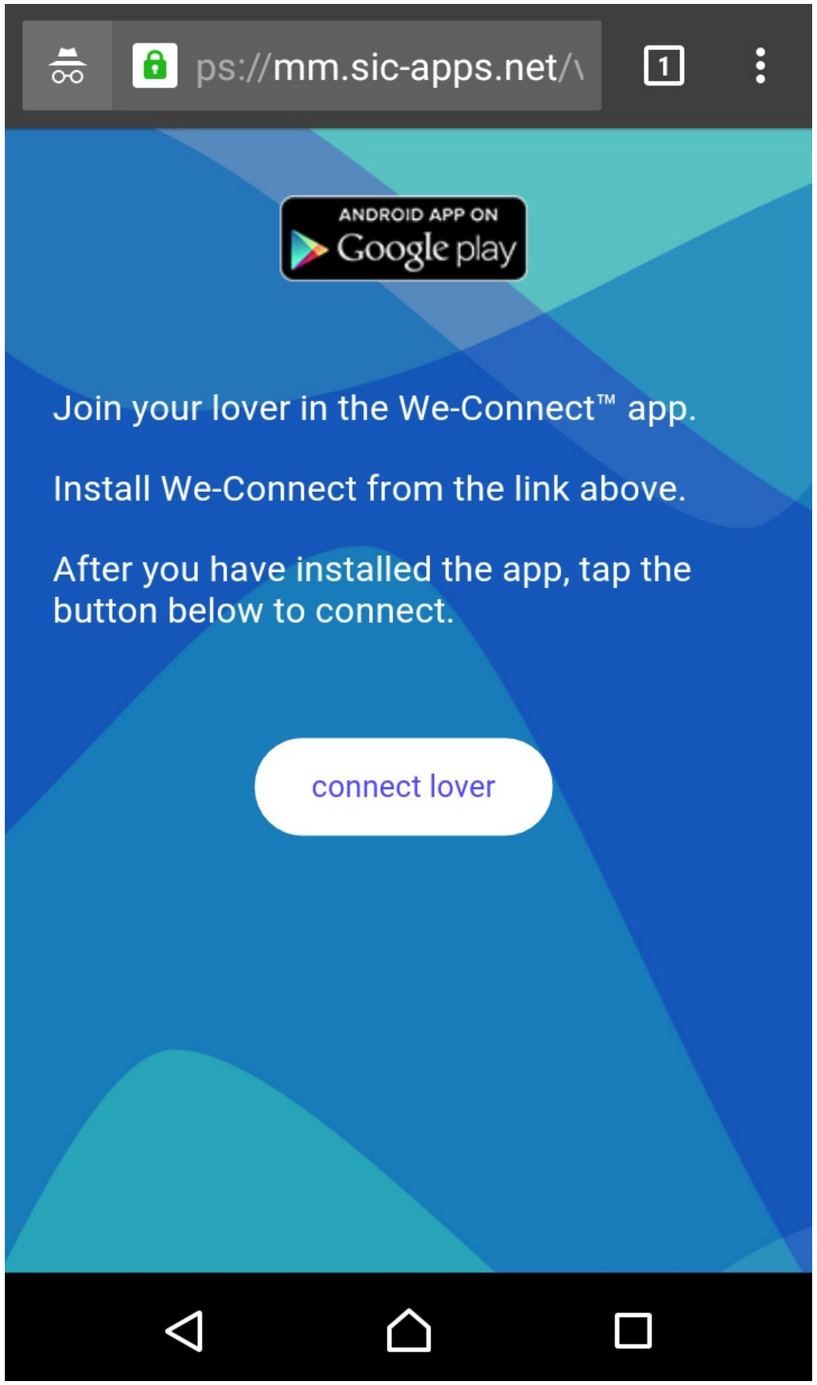
The "connect lover" link is of form:

`wevibe://connect?invite=<token>`



Invitation Links Expire

`https://mm.sic-apps.net/v1/i?t=<token>`



Invitation Links Expire?

...unless accessed via the long form URL:

```
https://mm.sic-apps.net/v1/invite?inviteToken=<token>&lang=en
```

XMPP / HTTP

XMPP / HTTP / JSON

Protocols & tools

XMPP Control Tool/library

XMPP research tool

XMPPPeek

Weevil release

weevil ˈwiːv(ə)l,ˈwiːvɪl/

Origin: Old English wifel ‘beetle’, from a Germanic base meaning ‘move briskly’.

Further/other work

- libjingle / webrtc etc etc
- Other products
- Other researcher's work:
  - PenTest Partners
- Other projects in adult toy domain / existing documentation:
  - metafetish Buttplug framework

Summary

Privacy is important

Summary

Privacy is important

Internet connected adult toys can and do collect intimate personal data

Summary

Privacy is important

Internet connected adult toys can and do collect intimate personal data

Adult toy research contributes to privacy encroachment awareness

What can you do

You now have knowledge of IoT reverse engineering tools and processes

Apply them to products you use and own to learn about their data collection

...and control your own devices in new private and fun ways.

www.privateplayaccord.com

@PrivatePlayNow @rancidbacon @goldfisk

Thanks & greetz to:

kellective, SecBarbie, Nikita, defcon, kiwicon