Hacking BLE Bicycle Locks for Fun & A Small Profit

Vincent Tan
• 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 use this sensor from world-renowned manufacturers, used in high-end smartphones and has excellent consistency.

**Bluetooth:** TappLock uses AES 128-bit encryption to protect documents with confidential and personal information.

**Firmware:** TappLock is equipped with an anti-jamming function to prevent unauthorized attempts to compromise the lock.

**Anti-shim/Anti-Theft:** A very popular technique used by lock pickers to create a false profile latch is designed to eliminate any risk of unauthorized access.

**Durable, secure body:** The TappLock body is made of high-quality materials to ensure a secure design. The lock body consists of five aluminum alloy casings and a seam. Each casing is a single-piece and cannot be opened.

---

Hackers built hotel rooms

New research shows how hackers can compromise hotel rooms.

By Zack Whittaker for Zero Day | April 25, 2018 -- 15:00 GMT (21:00 BST) | Topic: Security

---

Picking Bluetooth Low Energy Smart Locks

Ramsey

AERCLITE SECURITY

Slawomir Jasek
slawomir.jasek@securing.pl
slawomir.jasek@smartlockpicking.com
@slaweja

Blue picking – hacking Bluetooth Smart Locks

HackInTheBox Amsterdam, 14.03.2017

---

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

---
Major Players

- ofo - Ride Sharing Platform
  - BikeLock Technology CO., Ltd.
  - Rating: 4.4
  - Reviews: 11,293

- Mobike - Smart Bike Sharing
  - Beijing Mobike Technology Co., Ltd.
  - Rating: 4.4
  - Reviews: 15,735

- oBike - Bike Sharing
  - OBike Asia PTE. LTD.
  - Rating: 4.4
  - Reviews: 383

iPhone

- ofo
  - Unlock every corner of the world!

- Mobike
  - Easy and Fun Riding Experience

- oBike
  - The Future of Transportation

- Find a bike nearby

- Easy to find a bike next

- Share your location

- Offers Apple Watch App
# Major Players

<table>
<thead>
<tr>
<th>Country</th>
<th>China</th>
<th>China</th>
<th>Singapore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Founded</td>
<td>2014</td>
<td>2015</td>
<td>2017</td>
</tr>
<tr>
<td>Operations</td>
<td>20 Countries</td>
<td>16 Countries</td>
<td>22 Countries</td>
</tr>
<tr>
<td>Valuation</td>
<td>$2 Billion</td>
<td>$2.7 Billion</td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td>SGD$0.50/30min</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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
原价 ￥159.00 优惠促销
优惠 高端优惠券 30元店铺优惠券，满1099元可用
高端优惠券 15元店铺优惠券，满999元可用

配送 广东深圳 全国 快递 ￥12.00

颜色分类

数量 1

立即购买 加入购物车

描述 4.8 服务 4.8 物流 4.8

7天无理由退换货 运费险

¥180.00 ¥199.00
Major Components
Lock Decomposition
Logic Controller / BLE

Motor to release lock
Notch

Spring Mechanism

Notch

Pin

Notch
Picking Bluetooth Low Energy Locks from a Quarter Mile Away

Anthony Rose & Ben Ramsey
# Ubertooth One – Wireshark Capture

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>758</td>
<td>65.667491400</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>759</td>
<td>65.717492200</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>760</td>
<td>65.767716700</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>761</td>
<td>65.792493900</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>762</td>
<td>65.882653700</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>ATT</td>
<td>56</td>
<td>Unknown Direction Write Request, Handle: 0x0107 (Unknown: Unknown)</td>
</tr>
<tr>
<td>763</td>
<td>65.892980400</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>764</td>
<td>65.917493900</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>765</td>
<td>65.917685200</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>ATT</td>
<td>56</td>
<td>Unknown Direction Handle Value Notification, Handle: 0x0109 (Unknown: Unknown)</td>
</tr>
<tr>
<td>766</td>
<td>65.918140000</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>767</td>
<td>65.918483800</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>ATT</td>
<td>38</td>
<td>Unknown Direction Write Response, Handle: 0x0107 (Unknown: Unknown)</td>
</tr>
<tr>
<td>768</td>
<td>65.918642500</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
<tr>
<td>769</td>
<td>65.918873200</td>
<td>Unknown_6xaf9a82eb</td>
<td>Unknown_6xaf9a82eb</td>
<td>LE LL</td>
<td>33</td>
<td>Empty PDU</td>
</tr>
</tbody>
</table>

[Slave Address: d1:bf:36:28:b8:08 (d1:bf:36:20:b8:08)]

- Data Header: 0x170a
  - [L2CAP Index: 39]
- CRC: 0xfc0963
- Bluetooth L2CAP Protocol
  - Length: 19
- CID: Attribute Protocol (0xe004)
- Bluetooth Attribute Protocol
  - Opcode: Write Request (0x12)
  - Handle: 0x0107 (Unknown: Unknown)
  - Value: 86f491c203792565c5415e6c4a193176
    - [Response in Frame: 767]

The hexadecimal data frames are as follows:

| 0000 | 00 00 18 06 93 00 00 00 36 75 0c 09 00 00 09 01 |
| 0010 | 87 b0 95 45 24 00 00 00 eb 82 9a af 9a 17 13 00 |
| 0020 | 04 00 12 87 01 86 f4 91 c2 83 70 25 65 c5 41 5e |
| 0030 | 6c 4a 19 31 76 3f 99 c6 | 1.1.1v?... |
What do I need?

1. Communication Endpoints
2. Understanding the Data
BLEAH - Services and Characteristics

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

- d1:bf:36:20:b8:08 (-51 dBm)
  Vendor
  Allows Connections
  Address Type
  Complete Local Name
  Complete 16b Services
  Manufacturer

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

<table>
<thead>
<tr>
<th>Handles</th>
<th>Service &gt; Characteristics</th>
<th>Properties</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001 -&gt; 0005</td>
<td>Generic Access (00001800-0000-1000-0000-00805f9b34fb)</td>
<td>READ</td>
<td>u'NoKeLock'</td>
</tr>
<tr>
<td>0003</td>
<td>Device Name (00002a00-0000-1000-0000-0805f9b34fb)</td>
<td>READ</td>
<td>Unknown</td>
</tr>
<tr>
<td>0005</td>
<td>Appearance (00002a01-0000-1000-0000-0805f9b34fb)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0006 -&gt; 0008</td>
<td>Generic Attribute (00001801-0000-1000-0000-00805f9b34fb)</td>
<td>INDICATE</td>
<td></td>
</tr>
<tr>
<td>0008</td>
<td>Service Changed (00002a05-0000-1000-0000-00805f9b34fb)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0100 -&gt; 0104</td>
<td>1Aa (000018a0-0000-1000-8000-00805f9b34fb)</td>
<td>READ INDICATE</td>
<td></td>
</tr>
<tr>
<td>0102</td>
<td>Magnetic Flux Density - 2D (00002a0a-0000-1000-0000-00805f9b34fb)</td>
<td>WRITE</td>
<td></td>
</tr>
<tr>
<td>0104</td>
<td>Magnetic Flux Density - 3D (00002a0a1-0000-1000-0000-00805f9b34fb)</td>
<td>WRITE</td>
<td></td>
</tr>
<tr>
<td>0105 -&gt; 0110</td>
<td>fee7 (0000fee7-0000-1000-8000-00805f9b34fb)</td>
<td>WRITE</td>
<td>Error from Bluetooth stack (comerr)</td>
</tr>
<tr>
<td>0107</td>
<td>3Ef6 (00003Ef6-0000-1000-0000-00805f9b34fb)</td>
<td>NOTIFY READ</td>
<td></td>
</tr>
<tr>
<td>0109</td>
<td>fec7 (0000fec7-0000-1000-0000-00805f9b34fb)</td>
<td>WRITE</td>
<td></td>
</tr>
<tr>
<td>010d</td>
<td>fec8 (0000fecd-0000-1000-0000-00805f9b34fb)</td>
<td>READ INDICATE</td>
<td></td>
</tr>
<tr>
<td>0110</td>
<td>fec9 (0000fec9-0000-1000-0000-00805f9b34fb)</td>
<td>READ</td>
<td></td>
</tr>
</tbody>
</table>

root in ~/Desktop
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...

1. Scan QR Code
2. Get Lock Key From Server
3. Server Responds with Lock Key
4. Request Encrypted Token
5. Gets Encrypted Token
6. Decrypt Token & Unlock!
<table>
<thead>
<tr>
<th>Request</th>
<th>Payload</th>
<th>Status</th>
<th>Error</th>
<th>Timeout</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>656</td>
<td>0120</td>
<td>200</td>
<td></td>
<td></td>
<td>525</td>
</tr>
<tr>
<td>1009</td>
<td>0999</td>
<td>200</td>
<td></td>
<td></td>
<td>518</td>
</tr>
<tr>
<td>1014</td>
<td>0114</td>
<td>200</td>
<td></td>
<td></td>
<td>517</td>
</tr>
<tr>
<td>893</td>
<td>0998</td>
<td>200</td>
<td></td>
<td></td>
<td>516</td>
</tr>
<tr>
<td>352</td>
<td>0004</td>
<td>200</td>
<td></td>
<td></td>
<td>515</td>
</tr>
<tr>
<td>613</td>
<td>0072</td>
<td>200</td>
<td></td>
<td></td>
<td>515</td>
</tr>
<tr>
<td>370</td>
<td>0119</td>
<td>200</td>
<td></td>
<td></td>
<td>513</td>
</tr>
<tr>
<td>221</td>
<td>0206</td>
<td>200</td>
<td></td>
<td></td>
<td>512</td>
</tr>
<tr>
<td>339</td>
<td>0212</td>
<td>200</td>
<td></td>
<td></td>
<td>512</td>
</tr>
<tr>
<td>31</td>
<td>0095</td>
<td>200</td>
<td></td>
<td></td>
<td>510</td>
</tr>
<tr>
<td>206</td>
<td>0115</td>
<td>200</td>
<td></td>
<td></td>
<td>510</td>
</tr>
<tr>
<td>663</td>
<td>0024</td>
<td>200</td>
<td></td>
<td></td>
<td>510</td>
</tr>
<tr>
<td>962</td>
<td>0103</td>
<td>200</td>
<td></td>
<td></td>
<td>510</td>
</tr>
<tr>
<td>405</td>
<td>0084</td>
<td>200</td>
<td></td>
<td></td>
<td>509</td>
</tr>
<tr>
<td>1043</td>
<td>0209</td>
<td>200</td>
<td></td>
<td></td>
<td>509</td>
</tr>
<tr>
<td>590</td>
<td>0082</td>
<td>200</td>
<td></td>
<td></td>
<td>508</td>
</tr>
<tr>
<td>751</td>
<td>0040</td>
<td>200</td>
<td></td>
<td></td>
<td>508</td>
</tr>
</tbody>
</table>

```
<table>
<thead>
<tr>
<th>lockKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;80,33.22,72,21,17,80,15,32,99,68,86,66,45,99,87&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;91,83,64,74,53,3,73,90,50,14,83,95,76,57,17&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;78,16,78,50,27,5,1,67,7,47,92,22,19,12,26,87&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;7,58,61,45,27,79,72,40,95,70,72,11,13,39,78,42&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;32,87,47,92,54,75,63,71,48,80,65,88,17,99,45,43&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;64,81,43,24,15,53,12,40,92,53,87,5,1,83,14,62&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;33,42,37,88,43,24,51,74,45,23,37,61,94,80,46&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;32,46,84,15,25,58,6,53,63,80,40,88,59,78,39,23&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;57,11,67,24,46,63,13,84,04,34,71,25,65,40,64,65&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;20,12,72,3,60,99,23,2,93,37,85,16,10,33,2&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;29,79,89,50,6,21,19,13,78,73,78,37,25,29,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;92,87,52,64,31,72,86,91,51,28,35,9,67,57,90&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;51,76,27,65,25,95,38,1,11,83,89,28,49,61,65,73&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;38,60,98,30,94,80,47,77,12,57,38,41,59,41,97,69&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;33,79,59,17,9,44,97,33,56,83,46,95,76,26&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;25,79,12,2,20,46,90,71,31,19,35,59,63,24,78,56&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
<tr>
<td>&quot;32,87,47,92,54,75,63,71,48,80,65,88,17,99,45,43&quot;,&quot;lockPwd&quot;:000000</td>
</tr>
</tbody>
</table>
```

**POST /newNckelock/lock/getDeviceInfo HTTP/1.1**
Host: 120.24.3.146:8000
phoneModel: iPhone 6
Accept: */*
appVersion: 3.0.0
Accept-Language: en-SG;q=1
Accept-Encoding: gzip, deflate
token: sfe6667t2324a3ab2ehlce0e40714
Content-Type: application/json
Content-Length: 64
clientType: iOS
Language: en-SG
User-Agent: nckelock/3.0.0 (iPhone; iOS 10.1.1; Scale/2.00)
Connection: close
osVersion: 10.1.1

("barcode":"http://www.nckelock.com/app.html?id=MCAl100008885")
oBike
oBike Lock

oBike lock teardown and rebuild, dockless share bike rescue: https://youtu.be/VI3Gl8w8n-Q
01. http://www.o.bike/download/app.html?m=065002064

02. App Checks Lock Status. Uploads Coordinates.

03. Server Responds with Lock Status

04. App Requests Key Source

05. App Gets Key Source

06. Request Unlock Key

07. Server Responds with Unlock Key

08. Unlock Bike Lock
http://www.o.bike/download/app.html?m=065002064

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>]

16519 ms | [OBikeBluetoothManager BLEDidNotify]

16519 ms | [CBPeripheral writeValue: 0x17483f980 forCharacteristic: 0x1704ae100 type: 0x1]

writeValue -> _NSInlineData forCharacteristic -> CBCharacteristic

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF gt...
App Gets Key Source

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]
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}
Unlock Bike Lock

19106 ms: `[OBikeBluetoothManager openLock:0xb4 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`
## Unlock Algorithm

### Message 1

<table>
<thead>
<tr>
<th>Key Index</th>
<th>Message Length</th>
<th>Command</th>
<th>Index:</th>
</tr>
</thead>
<tbody>
<tr>
<td>b4</td>
<td>18</td>
<td>82</td>
<td>0xb4</td>
</tr>
</tbody>
</table>

**Key:** 8be1be17d41e8fdff1ae1c82e4500fec

### Date Time

<table>
<thead>
<tr>
<th>00 00 02 79 40 48</th>
</tr>
</thead>
</table>

### Message 2

**AES Key (Truncated):**

| 8b e1 be 17 d4 1e 8f df f1 ae 1c 82 |

**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":"68693cfa10579681d81837350843342d99f0ba4373f9926c53c1f1c88576304d0b936e7003888288fe949e73eb1d3267b713d2b261829ee0498523423d6965db28e8b99854bf2adf592e51fb9da3b77068f647b29caa5f22473ad01ec1011270a9d3a73100292b0fdf331b17b37564556df790a58489d8cad3f4dd276d5ae68a95fc7effefc998de151eeb0983ddc7216345e7682df8cf2de0d2cbf3a8b7e7c1c8f8604016c377b0195b0ab9e83c604d"}

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

{"value":"aa47e49f01cc740fdaa87973966799f94bf02ced7416b15f1cc7f63bf52f50f928e76c5d7f911a054188751f7243d68daef4b69b22432ec2166dc823f29de811e21f4adbfdb826748b9e2573912422b0a51f6a07a5c7be2bf7d41b56d69945c3ecf3ec94444db5abb26b8c771fe8eba91cb1a5d336cc2130bde9bcb25350250bb92c5aa880b2e6c0b3c0004c11ab0f14eb1182b78fb3dc5eb68e61205ae5048"}
HTTP Message Encryption - AES

9386 ms | | +[OBikeEncrypt aesEncryptString: {"deviceId":"1521828969000-8035385","dateTime":"1521984609867.631836","longitude":103.8331503422035,"latitude":1.38163138647611}&58bc93f4ac249b829174520a5afe733503f371f8]

9388 ms | | | | +[OBikeEncrypt aesEncryptData:<7b226465 76696365 4964223a 22313532313839363930 30302d38 303335333835222c 22646174 6554696d 65223a22 31353231393834603836372e363331383362e363239313734353230613561666537333530336337316638> 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"
}&oBi0SX4buhBMG

+ 324
08 Unlock Bike Lock
09 Lock Status & Start Timer
10 Lock Status & End Timer
11 You have been billed $$$
oBike Demo
MoBike
@ Scanning for 5s [-128 dBm of sensitivity] ...

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe:91:4a:dc:fc:d4</td>
<td>-54 dBm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Allows Connections</th>
<th>Address Type</th>
<th>Flags</th>
<th>Manufacturer</th>
<th>Complete Local Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td></td>
<td></td>
<td></td>
<td>'b3040101fe91adcfcd4a000003913000000'</td>
<td>mobike</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Handles</th>
<th>Service &gt; Characteristics</th>
<th>Properties</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001 -&gt; 0007</td>
<td><strong>Generic Access</strong> (00001000-0000-1000-8000-0080f9b34fb)</td>
<td>READ WRITE</td>
<td>u'mobike'</td>
</tr>
<tr>
<td>0003</td>
<td><strong>Device Name</strong> (00002a00-0000-1000-8000-0080f9b34fb)</td>
<td>READ</td>
<td>Unknown</td>
</tr>
<tr>
<td>0005</td>
<td><strong>Appearance</strong> (0004a0-0000-1000-8000-0080f9b34fb)</td>
<td>READ</td>
<td>Connection Interval: 8 -&gt; 80</td>
</tr>
<tr>
<td>0007</td>
<td><strong>Peripheral Preferred Connection Parameters</strong> (0002a04-0000-1000-8000-0080f9b34fb)</td>
<td>READ</td>
<td>Slave Latency: 0</td>
</tr>
<tr>
<td>0009 -&gt; ffff</td>
<td><strong>a000faa0-0047-005a-0052-6d6f2696b65</strong></td>
<td>NOTIFY</td>
<td>Connection Supervision Timeout Multiplier: 600</td>
</tr>
<tr>
<td>000b</td>
<td><strong>a000fe1-0047-005a-0052-6d6f2696b65</strong></td>
<td>WRITE</td>
<td></td>
</tr>
<tr>
<td>000e</td>
<td><strong>a000fe0-0047-005a-0052-6d6f2696b65</strong></td>
<td>WRITE</td>
<td></td>
</tr>
</tbody>
</table>
01. Visit the website: http://www.mobike.com/download/app.html?b=A1234567

02. App checks lock status and uploads coordinates.

03. Server responds with lock status.

04. Server responds with unlock key.

05. Unlock bike lock.
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: XXXXXXXXXXXXXXXX
platform: 0
Content-Type: application/x-www-form-urlencoded
Connection: close
Content-Length: 445

accesstoken=XXXXXXXXXXXXXXXXX&bikencode=A0000XXXXX&biketype=0&btEnabled=1&channel=1&client_id=ios&epdata=Es7dCTkXiZ1IV3H6z%2BS9R%2BYzRjFby0T4ADUNKh0aXm6wfZzfJtQEQ5IC%2By5lZYGKFVy8I9vP6wwvkKCEqxNSMMCM3WespduyU8Svj7qyadFV4pN/nbC1behZa7ew3V0G8ofy6udhTkjbWlcjWeWvioJwrELB24aALccUKxCoMds%3D&latitude=1.3XXX&longitude=103.8XXX&mobileNo=+6512345678&time=1530100847000&timestamp=1530100847.123456&userid=XXXXXXXXXX
HTTP Message Encryption

30714 ms | +[RSA encryptString:XXXXXXXXXXXuseridXXXXXXX#1530031691.737942
publicKey:MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCi/VezJp6KaJNXZCHpQ4YmKxlWrcreddowSpHDX3vHe
iUqdOoJZJoBpUvFuFd1WEqP7itWNcPnuYAqRwXkh6xWD1oM4MrK4eH8/AzdGIgrcgq+pbB3DymgEujkHBhrXqFiUS2
OjfebKwU0xJTPQM/KcxjqGDZxzswOxFJDxyKcwIDAQAB]

enter mbk_lowercaseMd5 ->
accesstoken=XXXXXXX&biketoken=A0000XXXXX&biketype=0&btEnabled=1&channel=1&client_id=ios&eb
pdate=Es7dCTkXiZ1IV3H6z+S9R+YzRjFby0T4ADUNKh0aXm6wfZzfJtQEQ5IC+y51ZYGKFVy8I9vP6wwvkKCEqxNSM
MC3WespduyU8Svj7qyadFV4pN/nbC1behZa7ew3V0G8ofy6udhTkjbWLcjWeWvioJwrELB24aALccUKxComds=&lati
tude=1.381585998461937&longitude=103.8330852148159&mobileNo=+65XXXXXX&time=1530031691000
&timestamp=1530031691.737942&userid=XXXXXXXXX@iossecret

leave mbk_lowercaseMd5 -> b9441790c2e3c42a57b439b51995f546
POST /api/v2/rentmgr/unlockBike.do?sign=9623f419340536f95c314d81c4c2b548 HTTP/1.1

bikecode=A0000XXXXX&biketype=0&btEnabled=1&channel=1&client_id=ios&epdata=ML1G%2BNjHnhzQPMoRZwtBx5k3c0y0BpBFZKePvb3WsR0%2BWbvtT7saxcwIwbI6JAkG27HGjWKMGeCwUyvw1z0gOA17Lybmbv30tFBwUkeFmpgklpG2YMEgFEEdCjYxhskfMtoLKWCz3WFBriiZ5S6yHnH5aT1yKe/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": "AXXXXXX",
    ...
    "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
{
    "authkey": "",
    "data": "001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A23235201",
    "orderid": "MBKA0000000000X",
    ...
}
Unlock Bike Lock

32484 ms - [MBKUnlockBikeData `setData`: `001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A23235201`]
32489 ms - [MBKUnlockBikeData `setMacaddress`: `XX:XX:XX:XX:XX:XX`]
32494 ms - [MBKUnlockBikeData `setAuthkey`: `001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A23235201`]
32498 ms - [MBKUnlockBikeData `setBikeid`: `A0XXXXXXXX`]
32501 ms - [MBKUnlockBikeData `setOrderid`: `MBKA000XXXXXXXXX`]

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`]
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]
Unlock Algorithm

32484 ms - [MBKUnlockBikeData setData:001BB441CB88B4034565E1C7BE448CD4B3D9F5CAA8452A23235201]

<table>
<thead>
<tr>
<th>Message 1</th>
<th>Index</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>33 30</td>
<td>001BB441CB88B40345</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message 2</th>
<th>Index</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>33 31</td>
<td>65E1C7BE448CD4B3D9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message 3</th>
<th>Index</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>33 32</td>
<td>F5CAA8452A23235201</td>
</tr>
</tbody>
</table>
MoBike Demo
In Summary...
2 Types of Lock Schemes

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

Frida
Thank you for listening!

@Vincent_tky