Backdooring the Front Door

About me

- Software Engineer by trade
- Hacker by passion
- Lock picker for fun
- The best puzzles are not meant to be solved
- All opinions are my own, and may not reflect those of my past, present, or future employers
- Twitter: @jmaxxz



Internet of things

August smart lock


PRODUCTS
HOW IT WORKS
SUPPORT
STORE
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.

"Unlike physical keys which can be duplicated and distributed without your knowledge"

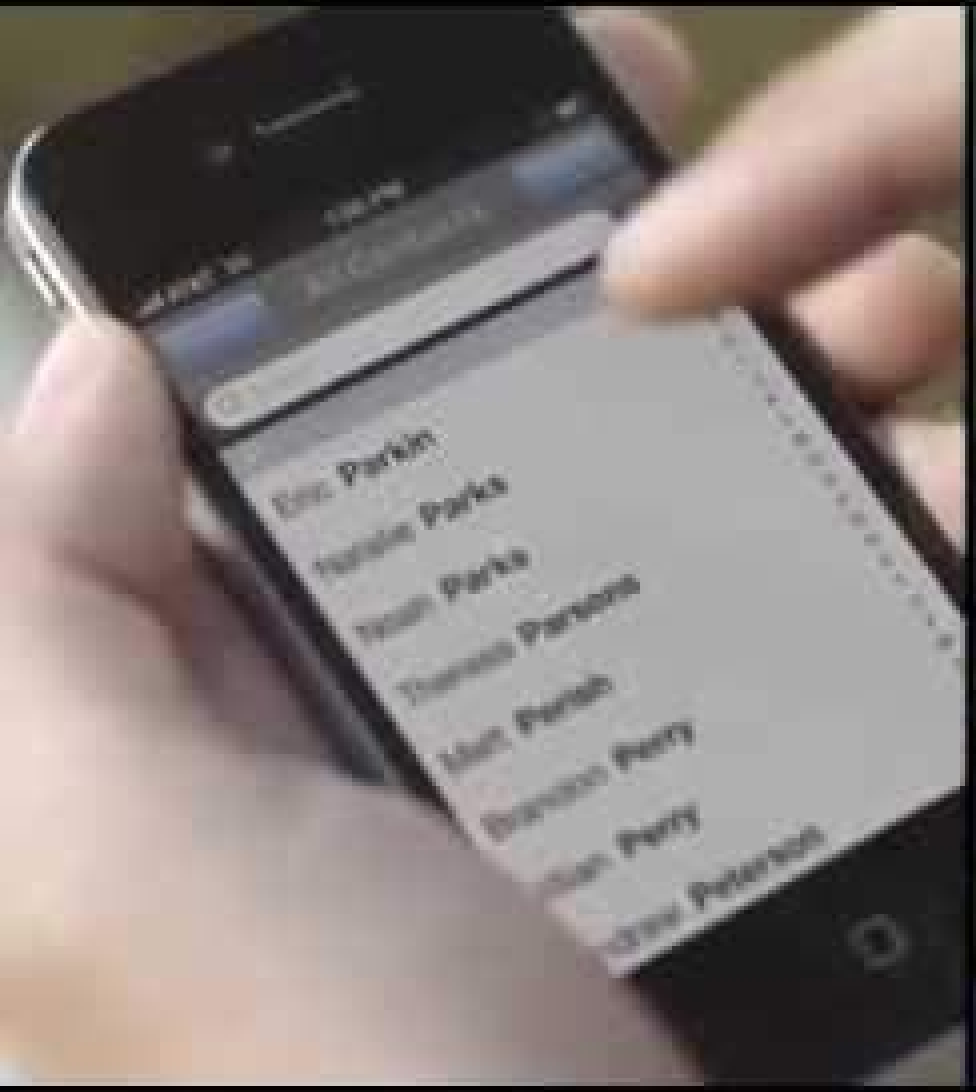
Source: august.com (August 17th, 2015)

Keyless

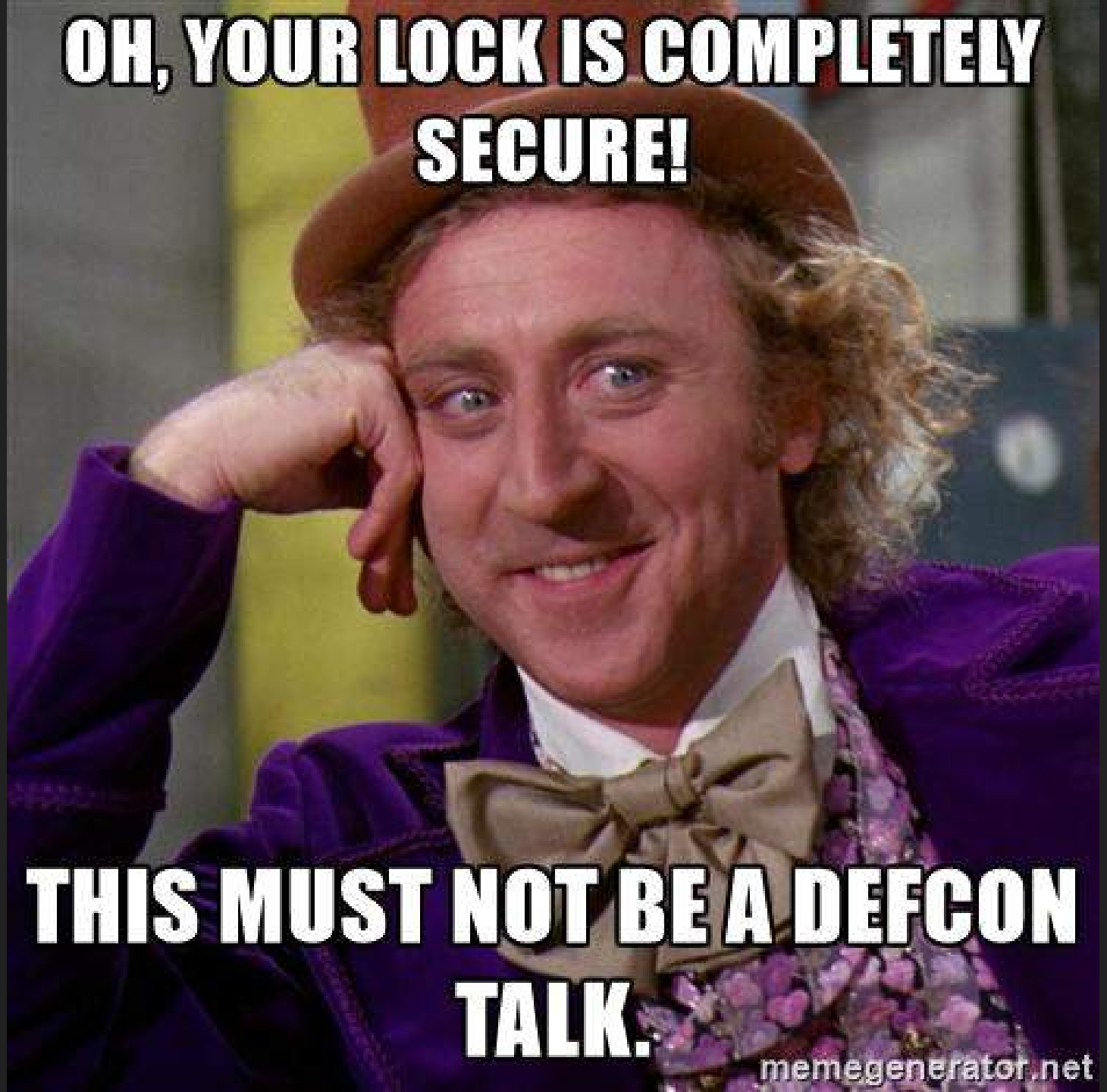
August's encrypted locking technology is safer than keys that can get lost and codes that can be copied.

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

"Safer than … codes that can be copied."


Parkin
Parks
Parks
Parsons
Perry
Perry
Peterson




OH, YOUR LOCK IS COMPLETELY SECURE!
THIS MUST NOT BE A DEFCON TALK.
memegenerator.net

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
- Track who enters and exits your home

Mapping out the API



WiFi | HTTPS



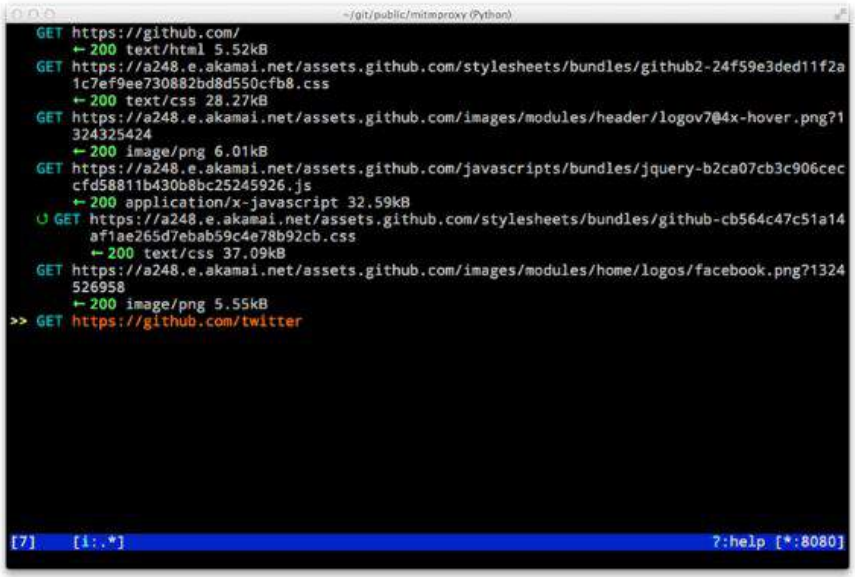
BLE



MitM proxy

https://mitmproxy.org

mitmproxy home docs forums about

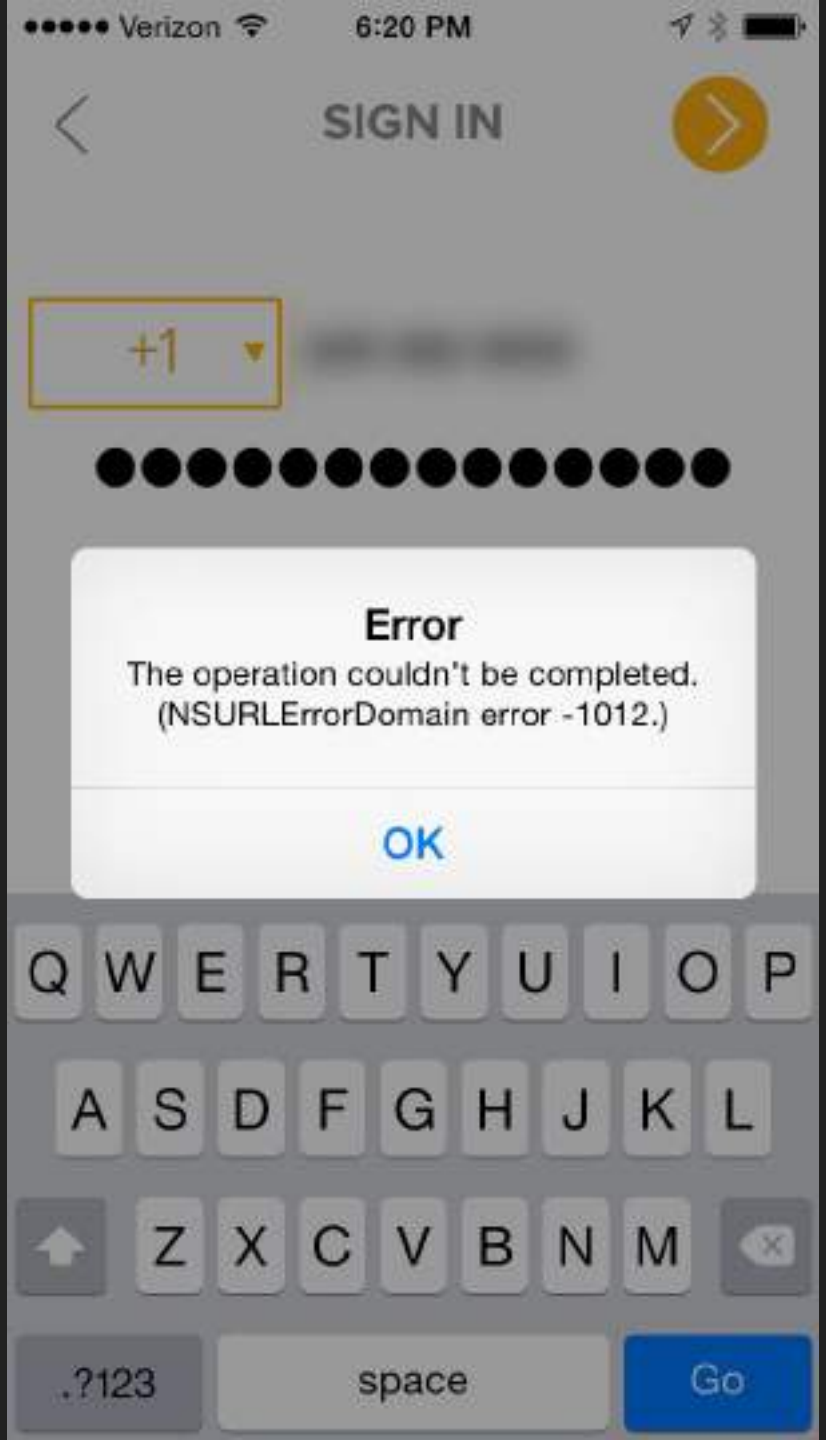


mitmproxy

An interactive console program that allows traffic flows to

mitmdump

Think tcpdump for HTTP - the same functionality as


Verizon
6:20 PM
SIGN IN
+1
Error
The operation couldn't be completed.
(NSURLErrorDomain error -1012.)
OK
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
Go

Certificate pinning …crap...

Solution:
iOS Kill Switch 2

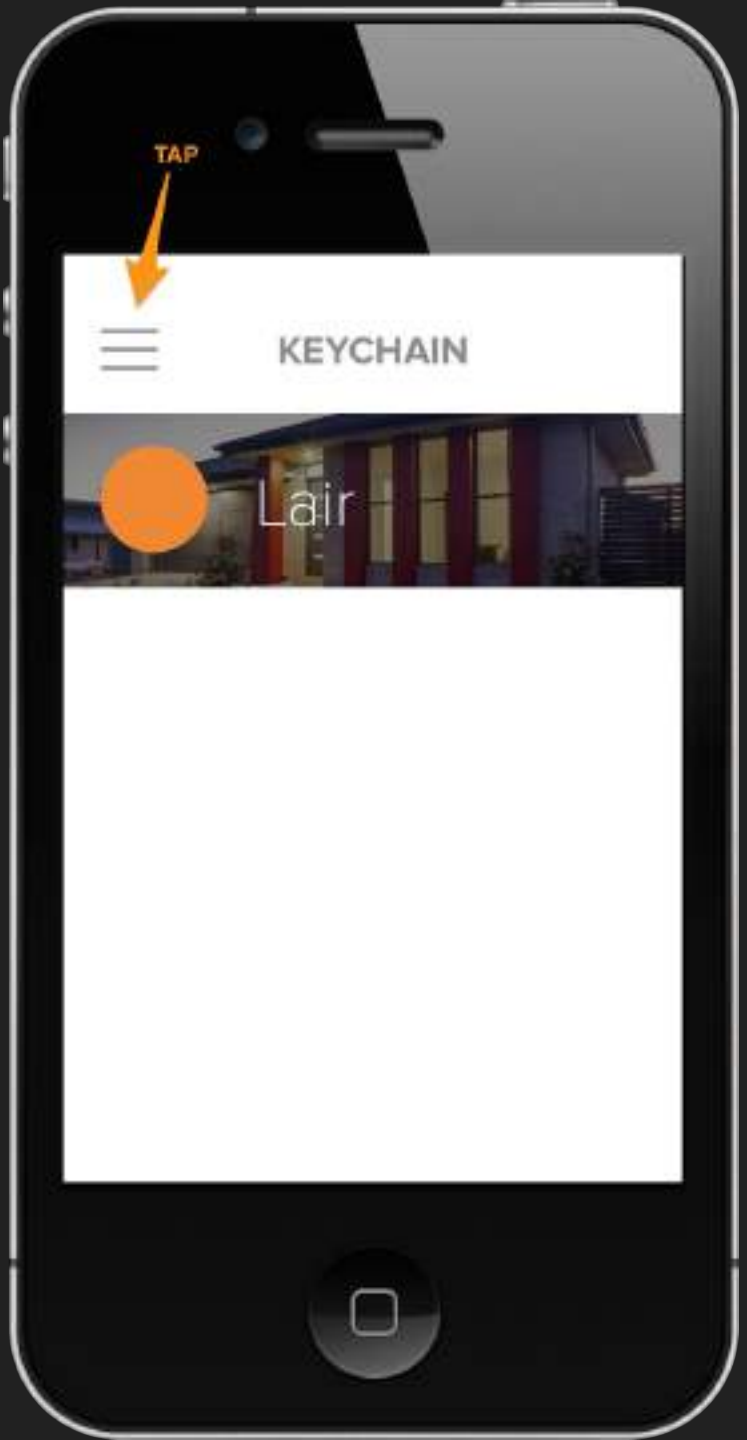
(https://github.com/nabla-c0d3/ssl-kill-switch2)

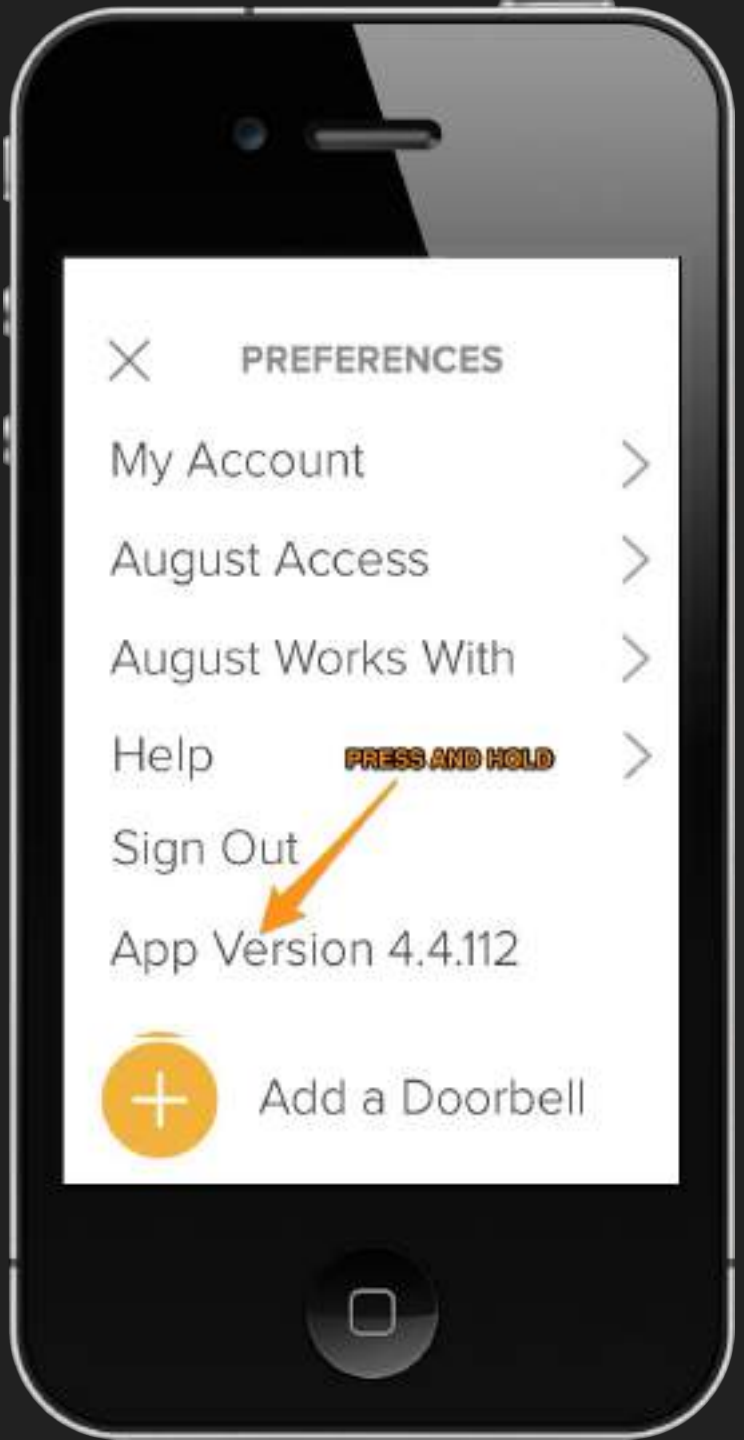


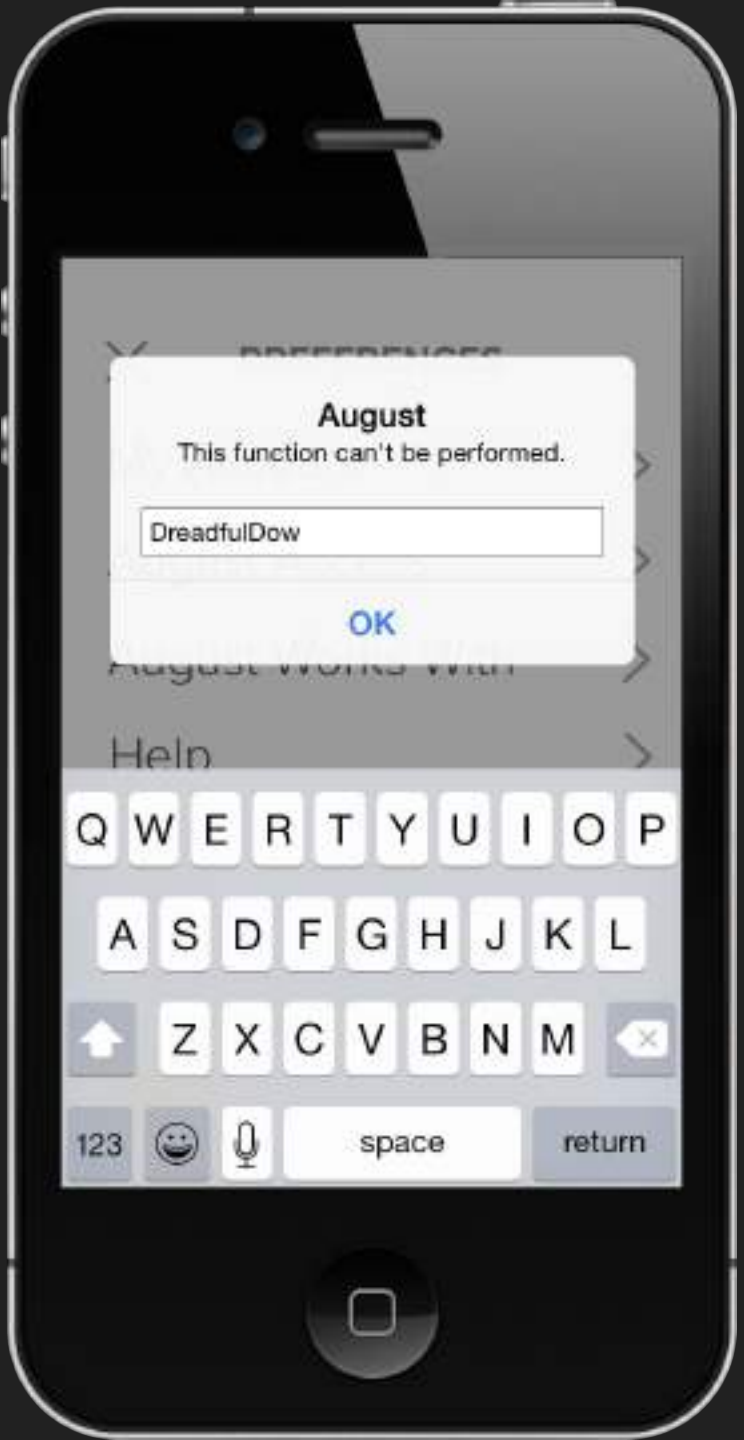
Disabling SSL/TLS system wide at Defcon?

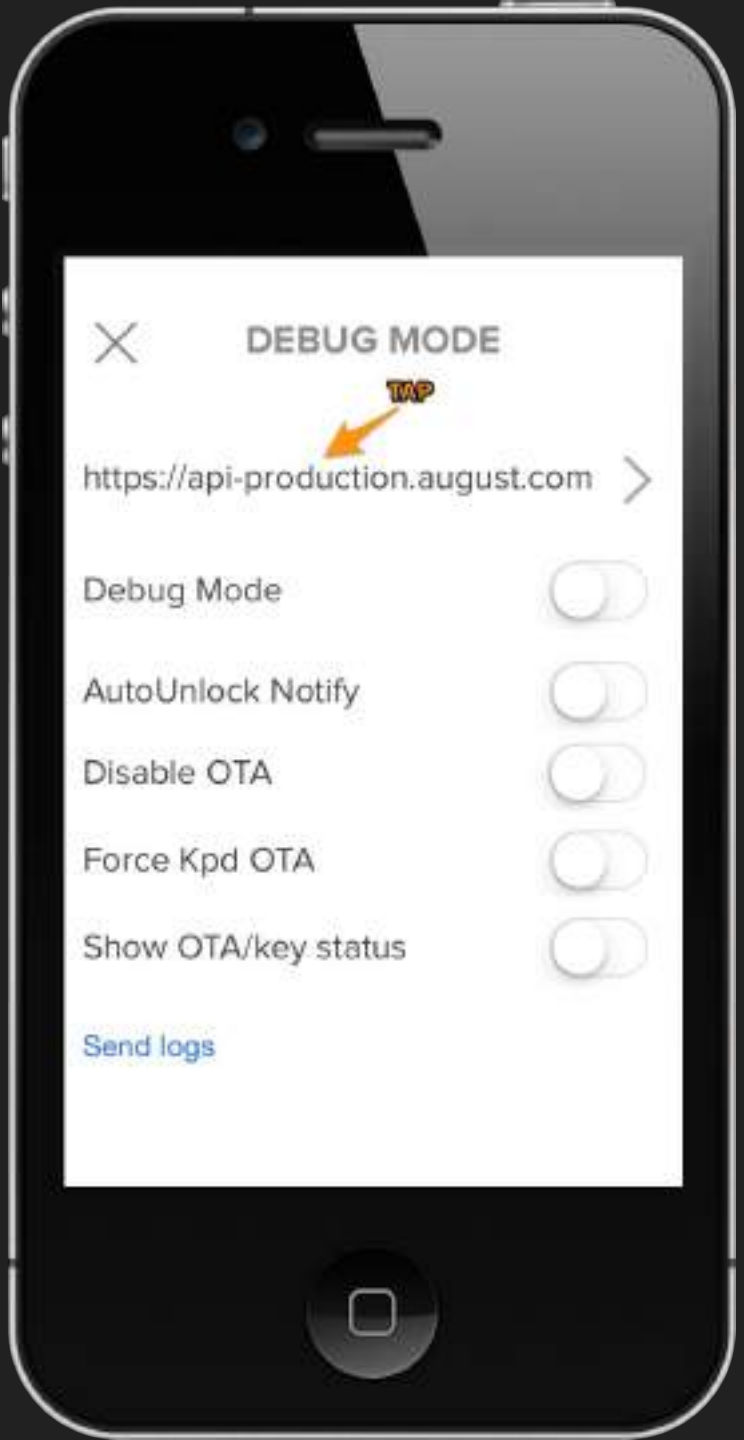

ITS A BAD IDEA
MKAY
WORK
MENTS
DIYLOL.COM

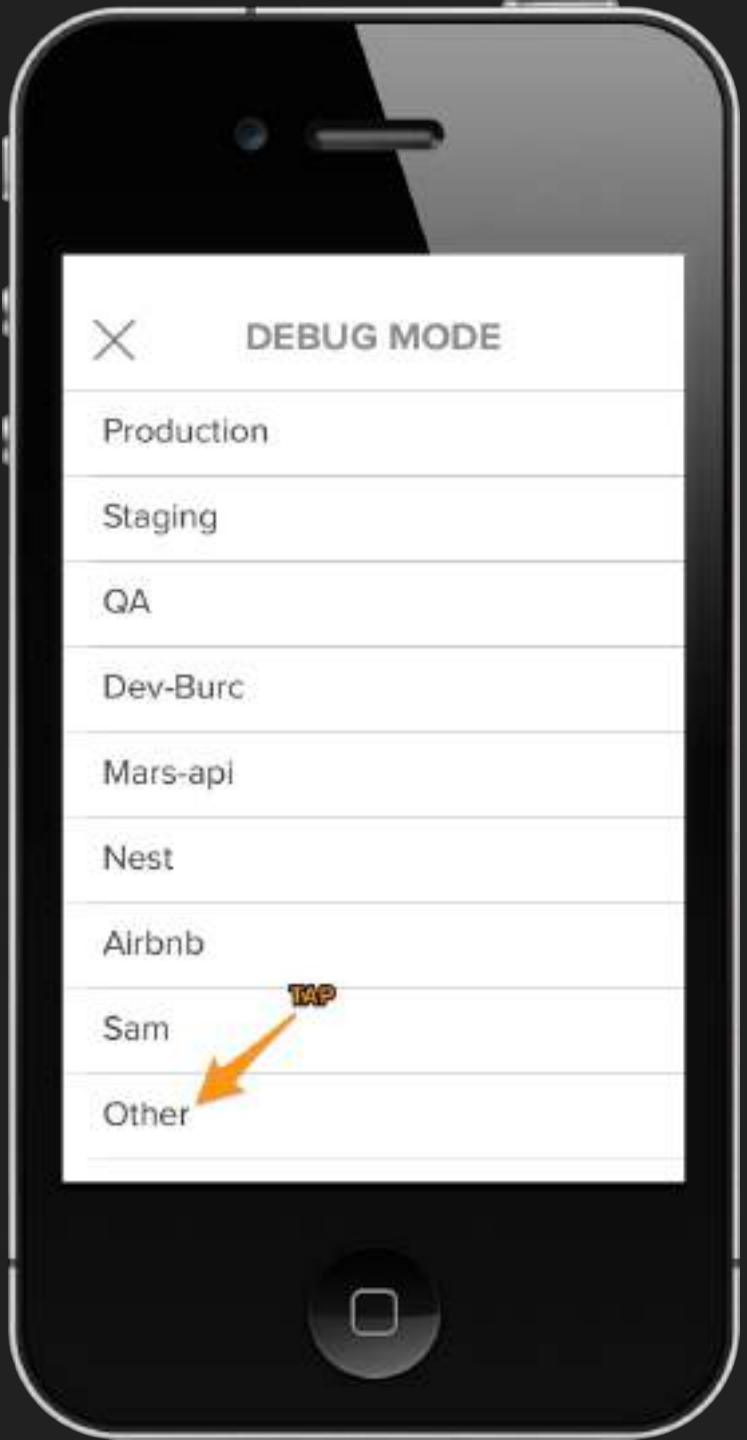
Better solution


TAP
KEYCHAIN
Lair

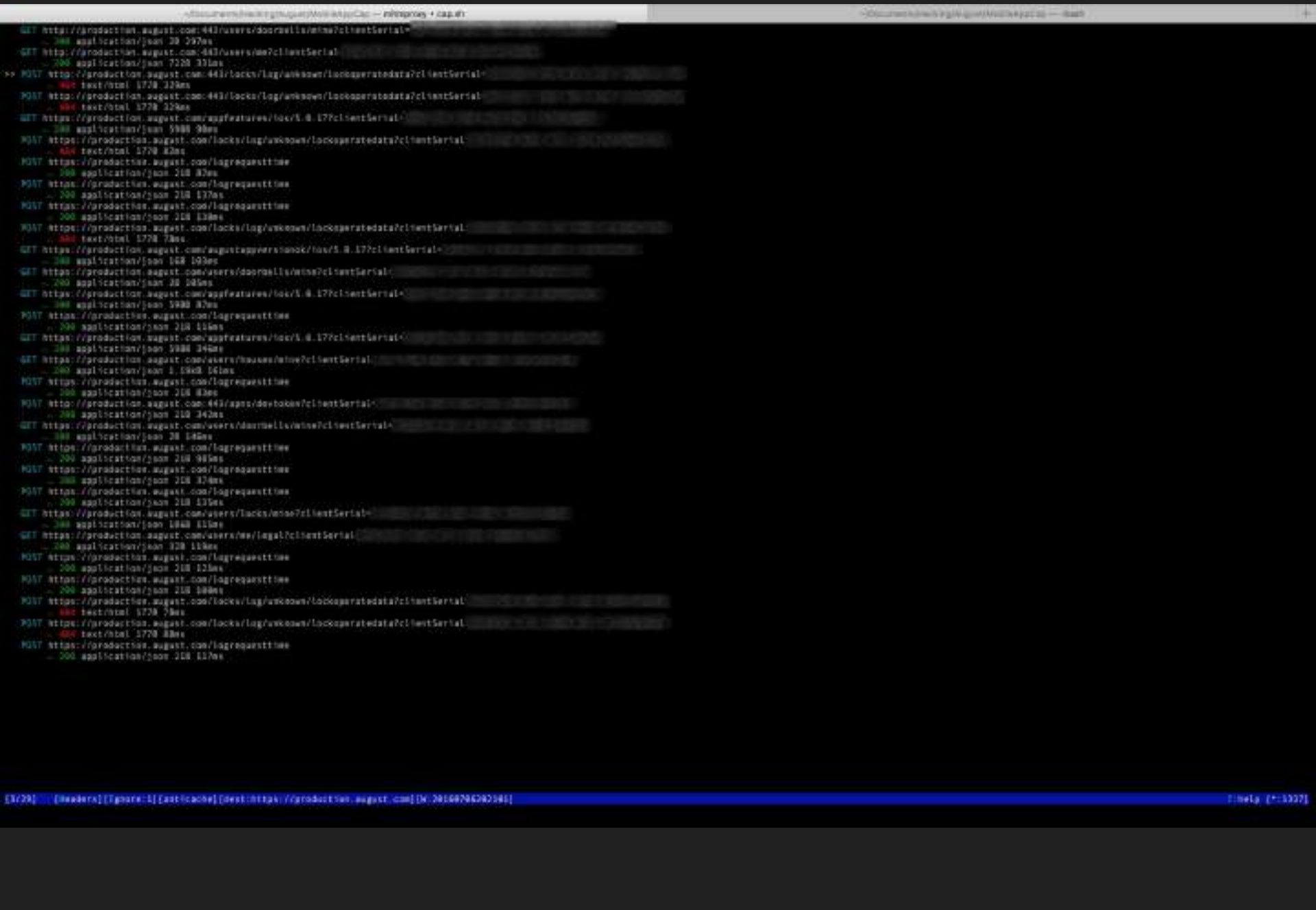

PREFERENCES
My Account
August Access
August Works With
Help
PRESS AND HOLD
Sign Out
App Version 4.4.112
Add a Doorbell


August
This function can't be performed.
DreadfulDow
OK
Help
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


DEBUG MODE
TAP
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
TAP
Sam
Other


Custom server
Server full address (https://www.example.com)
https://mitmrelay.jmaxxz.com
Cancel
Custom
1 2 3 4 5 6 7 8 9 0
- / : ; ( ) $ & @ "
#+= . , ? ! '
ABC
space
return


GET http://production.august.com:443/users/doorbells/mine?clientSerial=
200 application/json 20 297ms
GET http://production.august.com:443/users/me?clientSerial
200 application/json 7220 331ms
>> POST http://production.august.com:443/locks/log/unknown/lockoperatedata?clientSerial=
404 text/html 1770 329ms
POST http://production.august.com:443/locks/log/unknown/lockoperatedata?clientSerial
404 text/html 1770 329ms
GET https://production.august.com/appfeatures/ios/5.0.17?clientSerial=
200 application/json 5900 90ms
POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial
404 text/html 1770 82ms
POST https://production.august.com/logrequesttime
200 application/json 210 87ms
POST https://production.august.com/logrequesttime
200 application/json 210 137ms
POST https://production.august.com/logrequesttime
200 application/json 210 130ms
POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial
404 text/html 1770 78ms
GET https://production.august.com/augustappversionok/ios/5.0.17?clientSerial=
200 application/json 160 103ms
GET https://production.august.com/users/doorbells/mine?clientSerial=
200 application/json 20 105ms
GET https://production.august.com/appfeatures/ios/5.0.17?clientSerial=
200 application/json 5900 87ms
POST https://production.august.com/logrequesttime
200 application/json 210 116ms
GET https://production.august.com/appfeatures/ios/5.0.17?clientSerial=
200 application/json 5900 346ms
GET https://production.august.com/users/houses/mine?clientSerial
200 application/json 1.19kB 161ms
POST https://production.august.com/logrequesttime
200 application/json 210 83ms
POST http://production.august.com:443/apns/devtoken?clientSerial=
200 application/json 210 342ms
GET https://production.august.com/users/doorbells/mine?clientSerial=
200 application/json 20 146ms
POST https://production.august.com/logrequesttime
200 application/json 210 985ms
POST https://production.august.com/logrequesttime
200 application/json 210 370ms
POST https://production.august.com/logrequesttime
200 application/json 210 135ms
GET https://production.august.com/users/locks/mine?clientSerial=
200 application/json 1060 115ms
GET https://production.august.com/users/me/legal?clientSerial
200 application/json 320 119ms
POST https://production.august.com/logrequesttime
200 application/json 210 125ms
POST https://production.august.com/logrequesttime
200 application/json 210 100ms
POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial
404 text/html 1770 70ms
POST https://production.august.com/locks/log/unknown/lockoperatedata?clientSerial
404 text/html 1770 80ms
POST https://production.august.com/logrequesttime
200 application/json 210 117ms
[3/29] [Headers][Ignore:1][anticache][dest:https://production.august.com][W:20160706202101]
?:help [*:1337]

No Jailbreak

Certificate Pinned!!!

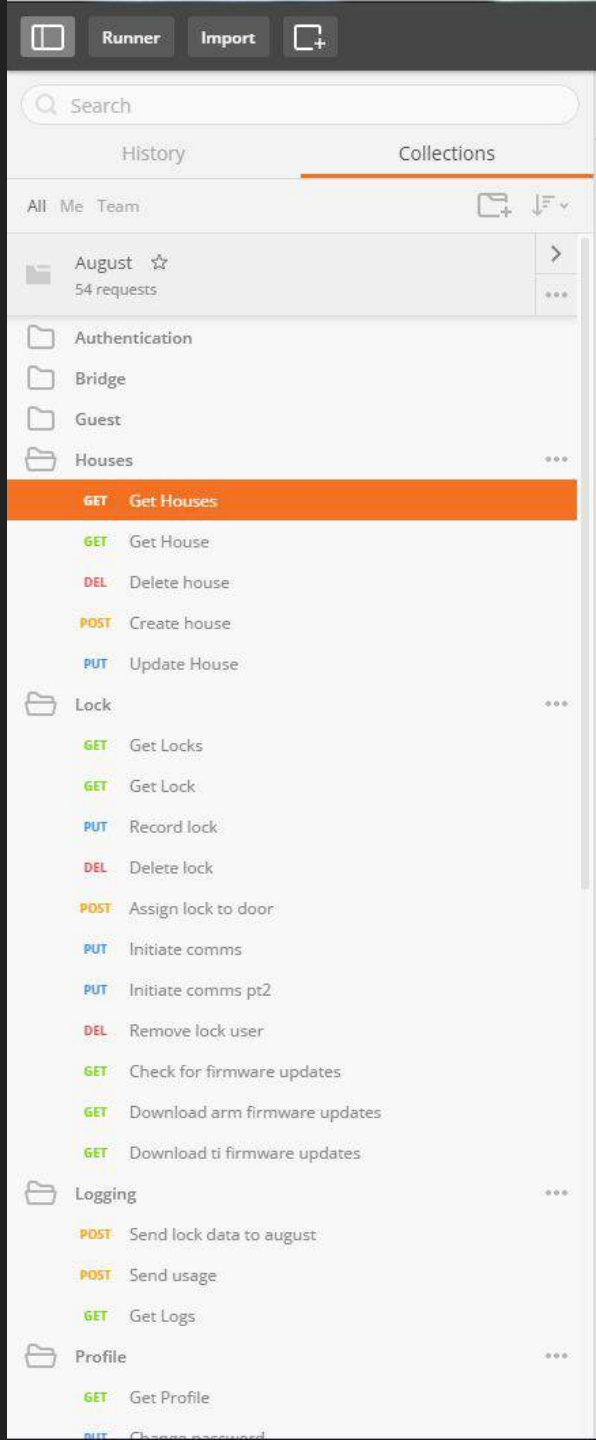


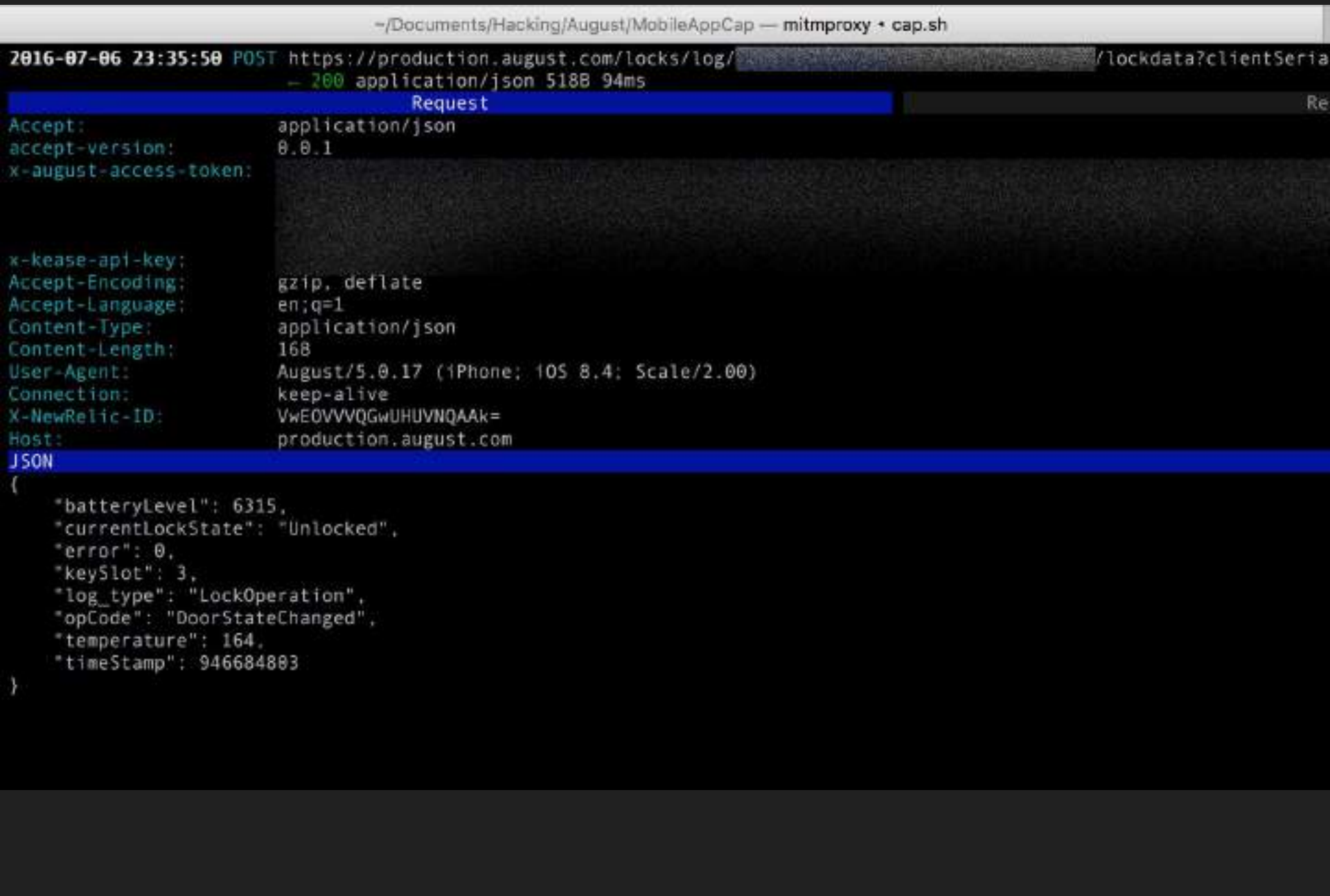
Security claims

- ~~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
- Track who enters and exits your home

After mapping out api

Postman collection created (see [github repo]())




~/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:
x-kease-api-key:
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


August
DON'T MIND US
memegenerator.net

Creepy

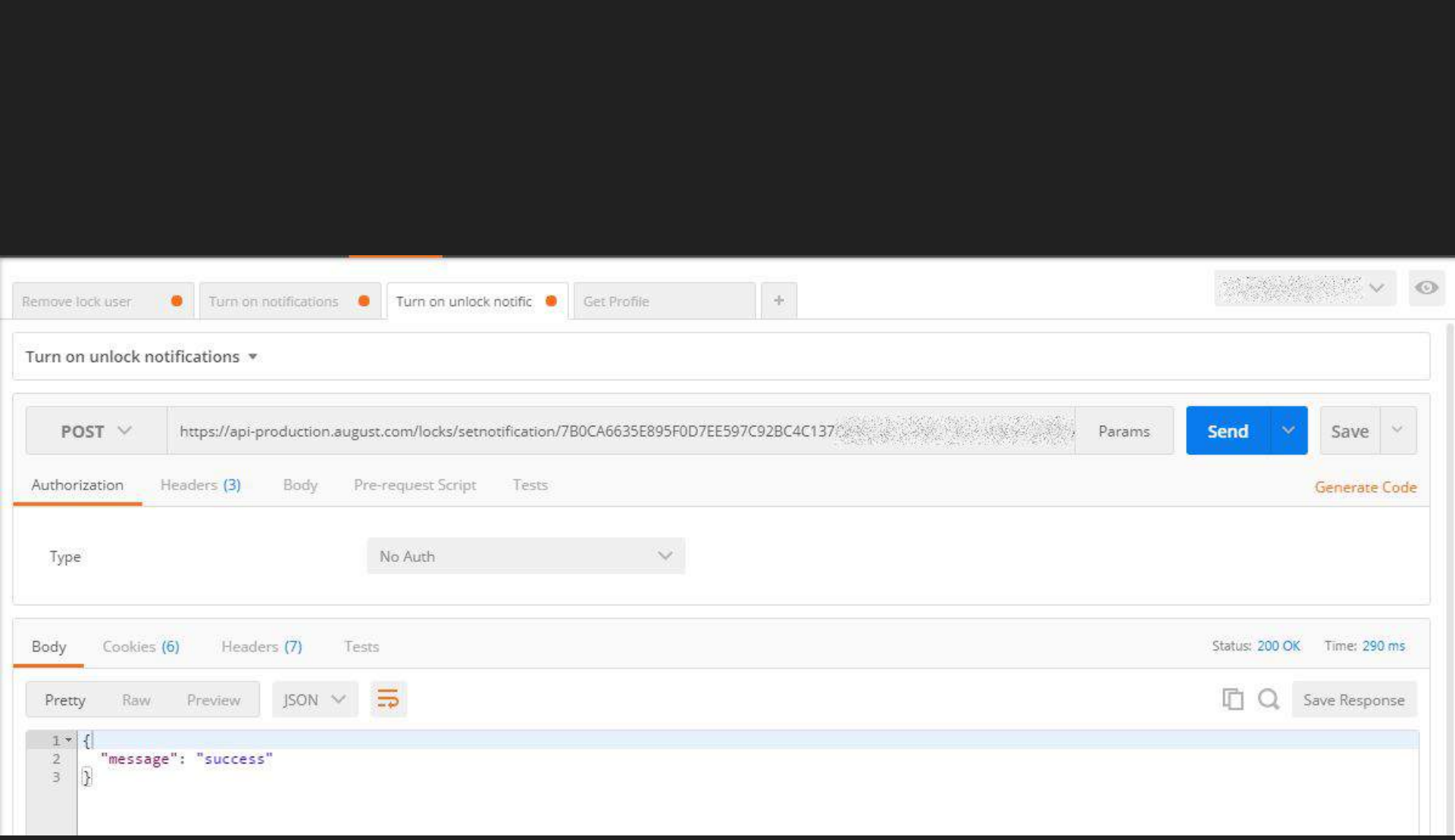
Let's fix this

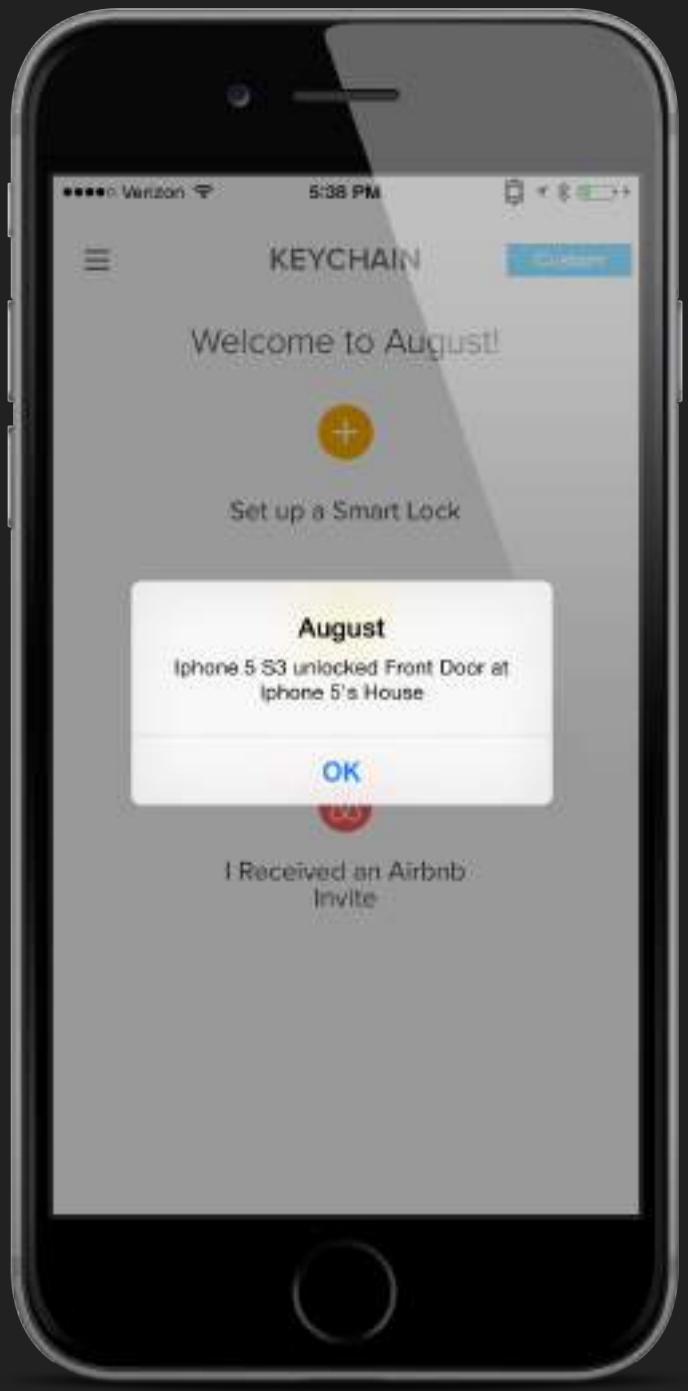
MiTM can modify traffic

Fix

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

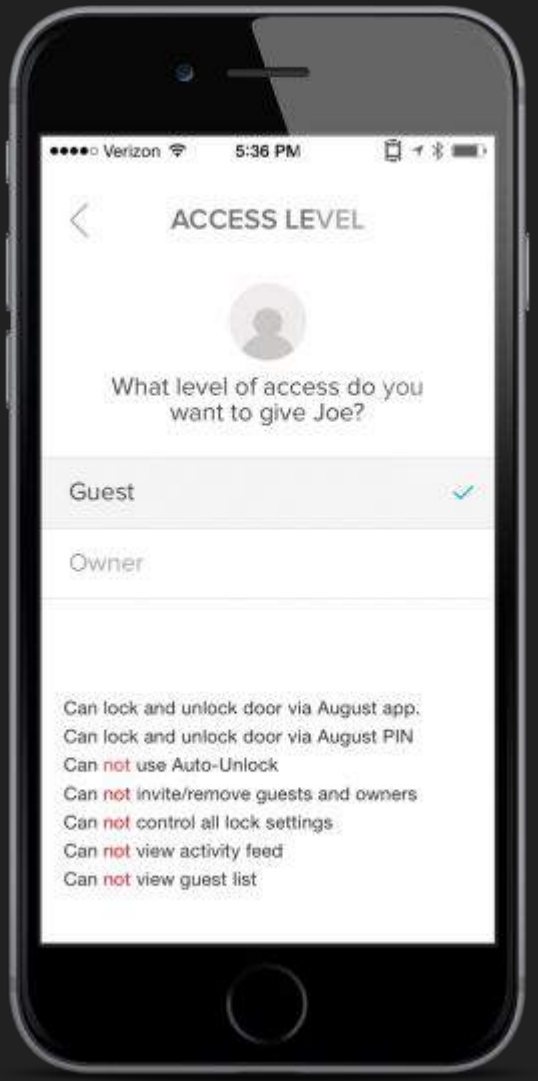



Remove lock user
Turn on notifications
Turn on unlock notific
Get Profile
Turn on unlock notifications
POST
https://api-production.august.com/locks/setnotification/7B0CA6635E895F0D7EE597C92BC4C137
Params
Send
Save
Authorization
Headers (3)
Body
Pre-request Script
Tests
Generate Code
Type
No Auth
Body
Cookies (6)
Headers (7)
Tests
Status: 200 OK
Time: 290 ms
Pretty
Raw
Preview
JSON
Save Response
1 {
2 "message": "success"
3 }

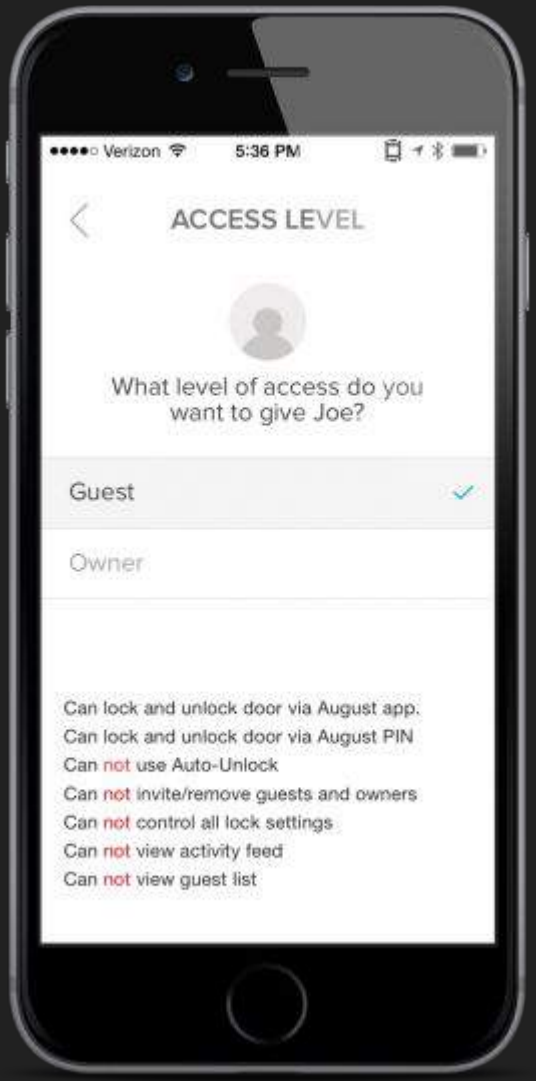

Verizon
5:38 PM
KEYCHAIN
Welcome to August!
Set up a Smart Lock
August
Iphone 5 S3 unlocked Front Door at Iphone 5's House
OK
I Received an Airbnb Invite

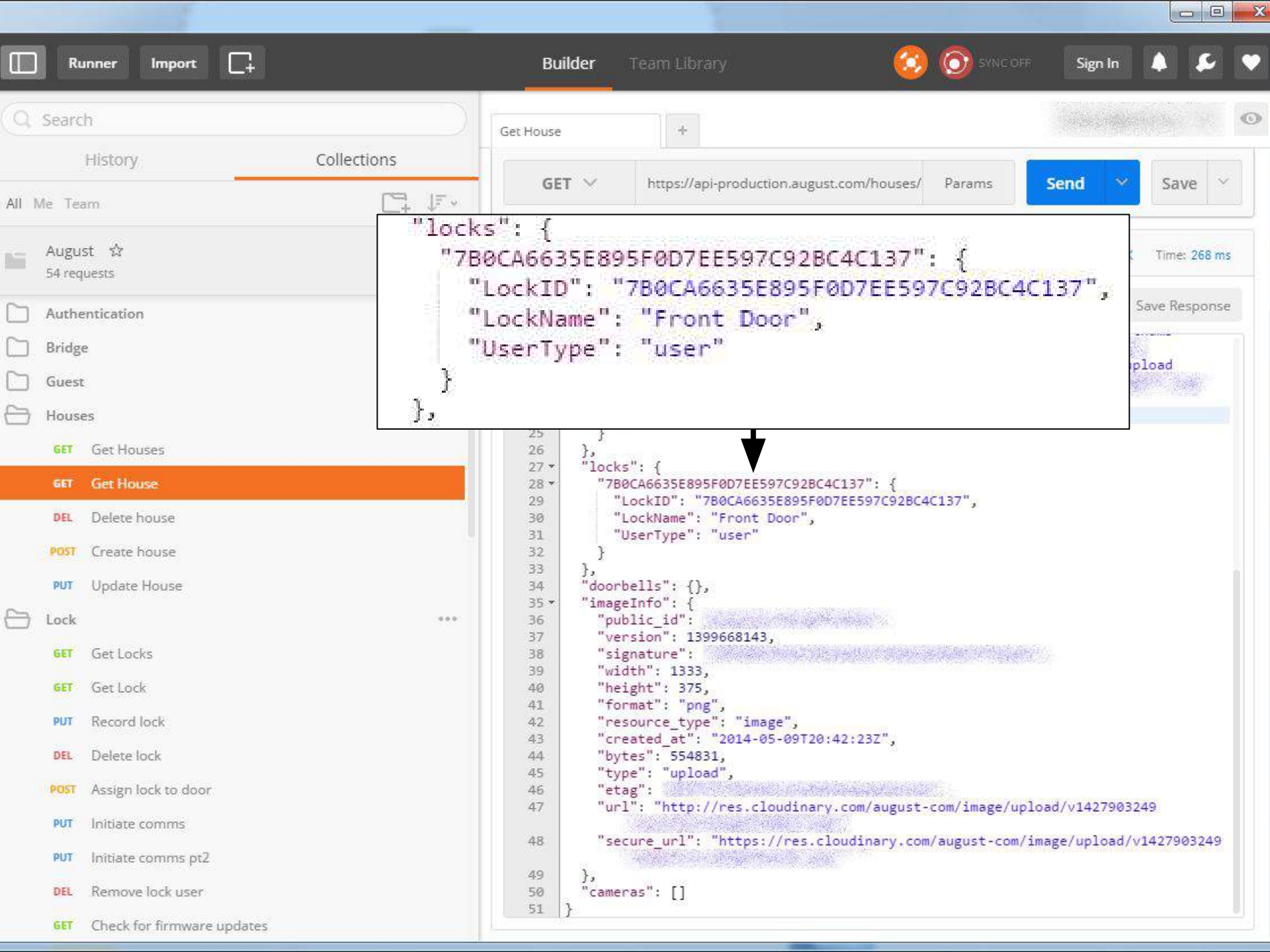
What else can we do?

Guest to admin?

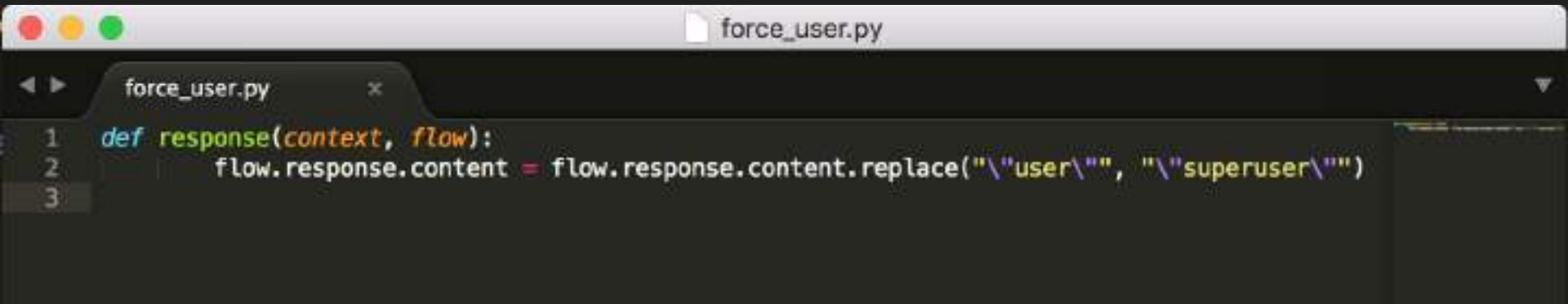


Guests can not use Auto-Unlock
Guests can not control lock settings

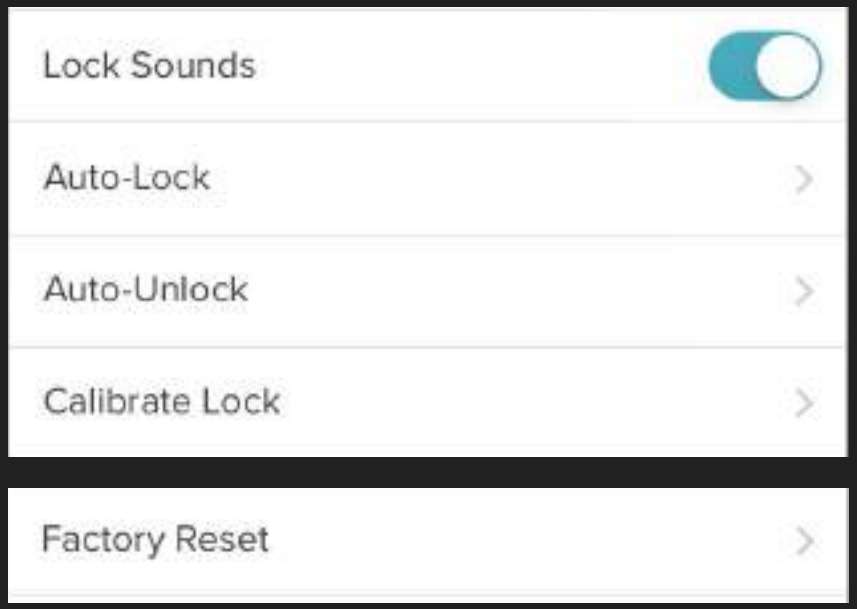


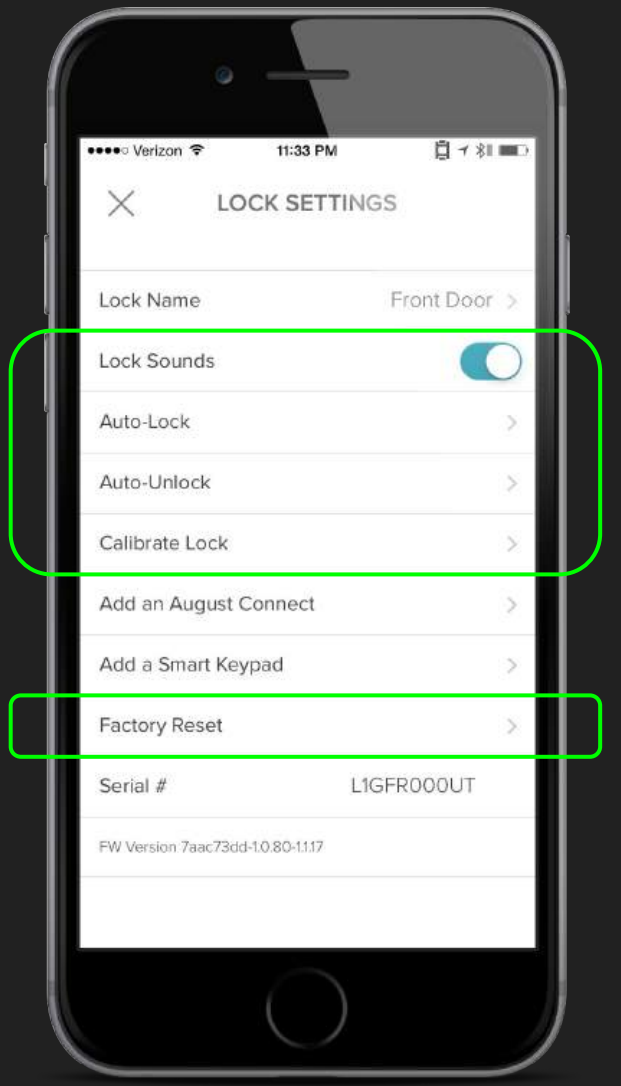

Runner
Import
Builder
Team Library
SYNC OFF
Sign In
Search
History
Collections
All Me Team
August
54 requests
Authentication
Bridge
Guest
Houses
GET Get Houses
GET Get House
DEL Delete house
POST Create house
PUT Update House
Lock
GET Get Locks
GET Get Lock
PUT Record lock
DEL Delete lock
POST Assign lock to door
PUT Initiate comms
PUT Initiate comms pt2
DEL Remove lock user
GET Check for firmware updates
Get House
GET
https://api-production.august.com/houses/
Params
Send
Save
Time: 268 ms
Save Response
"locks": {
"7B0CA6635E895F0D7EE597C92BC4C137": {
"LockID": "7B0CA6635E895F0D7EE597C92BC4C137",
"LockName": "Front Door",
"UserType": "user"
}
},
"doorbells": {},
"imageInfo": {
"public_id":
"version": 1399668143,
"signature":
"width": 1333,
"height": 375,
"format": "png",
"resource_type": "image",
"created_at": "2014-05-09T20:42:23Z",
"bytes": 554831,
"type": "upload",
"etag":
"url": "http://res.cloudinary.com/august-com/image/upload/v1427903249
"secure_url": "https://res.cloudinary.com/august-com/image/upload/v1427903249
"cameras": []

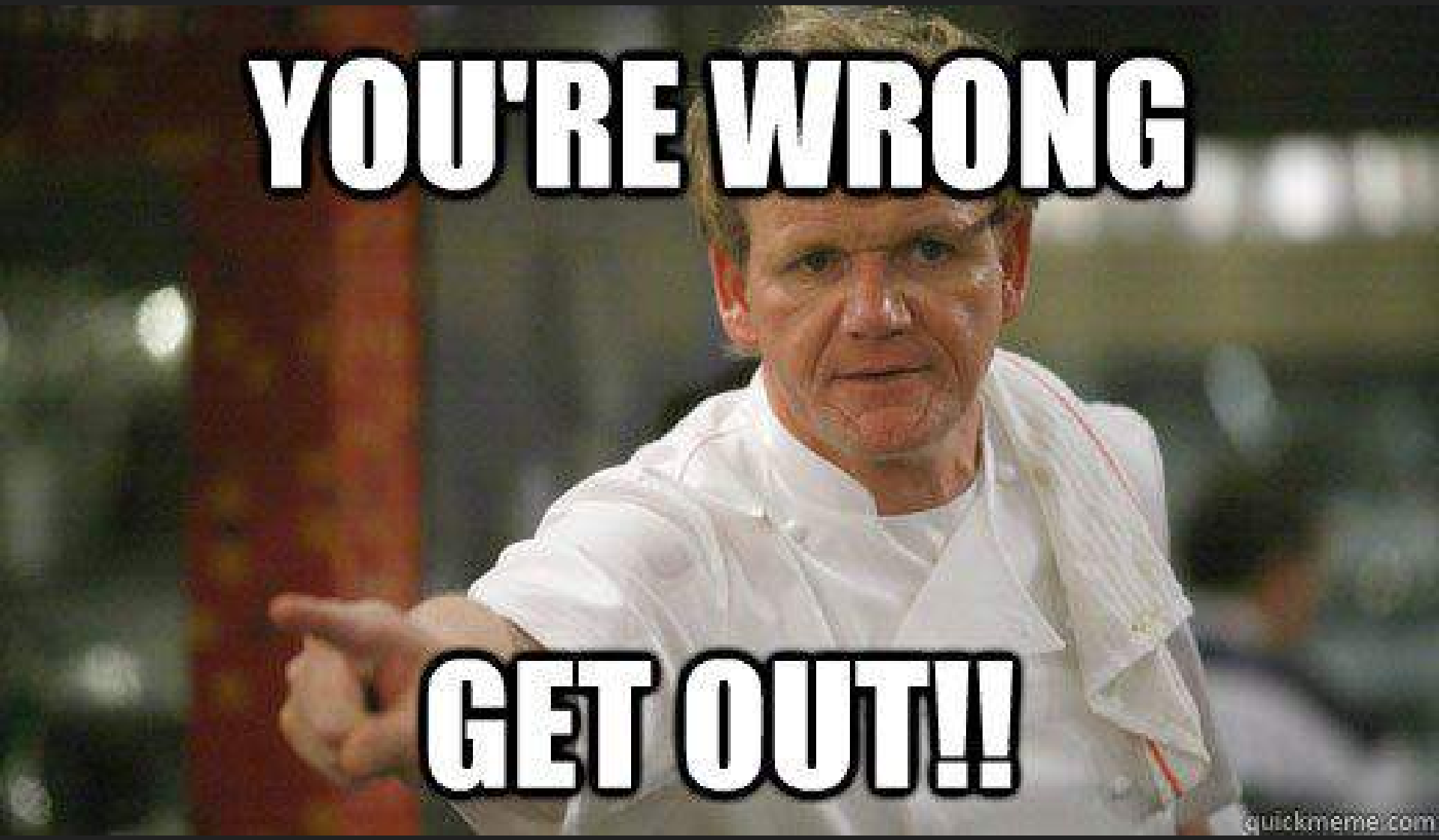
Replace "user" with "superuser"



Guests can change lock settings!



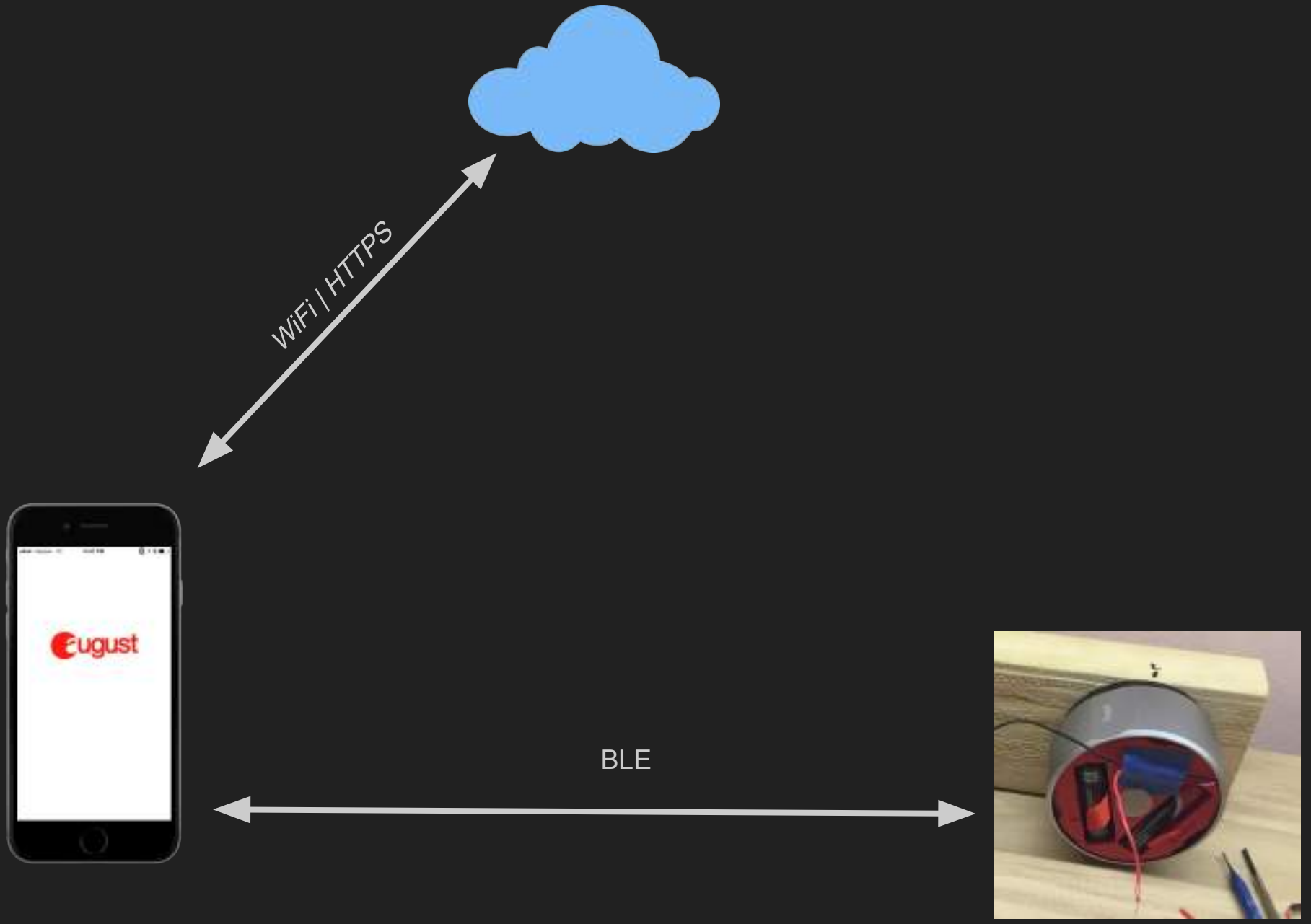



YOU'RE WRONG
GET OUT!!
quickmeme.com

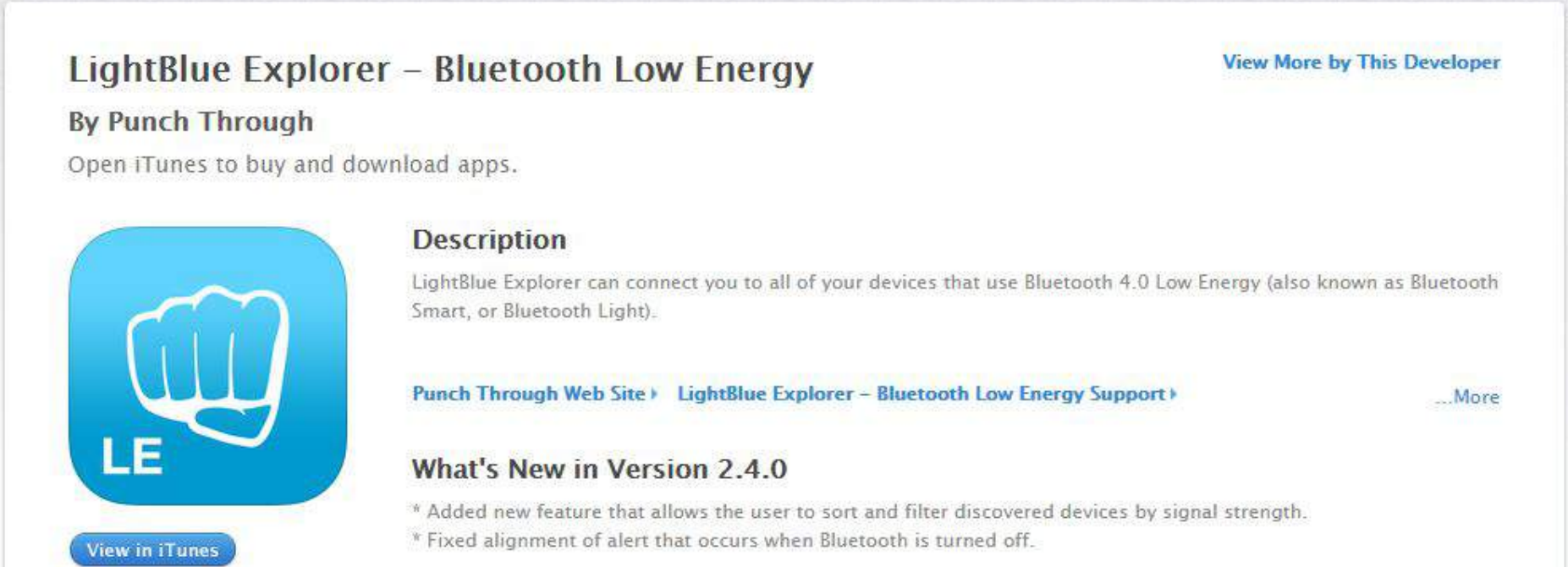
Security claims

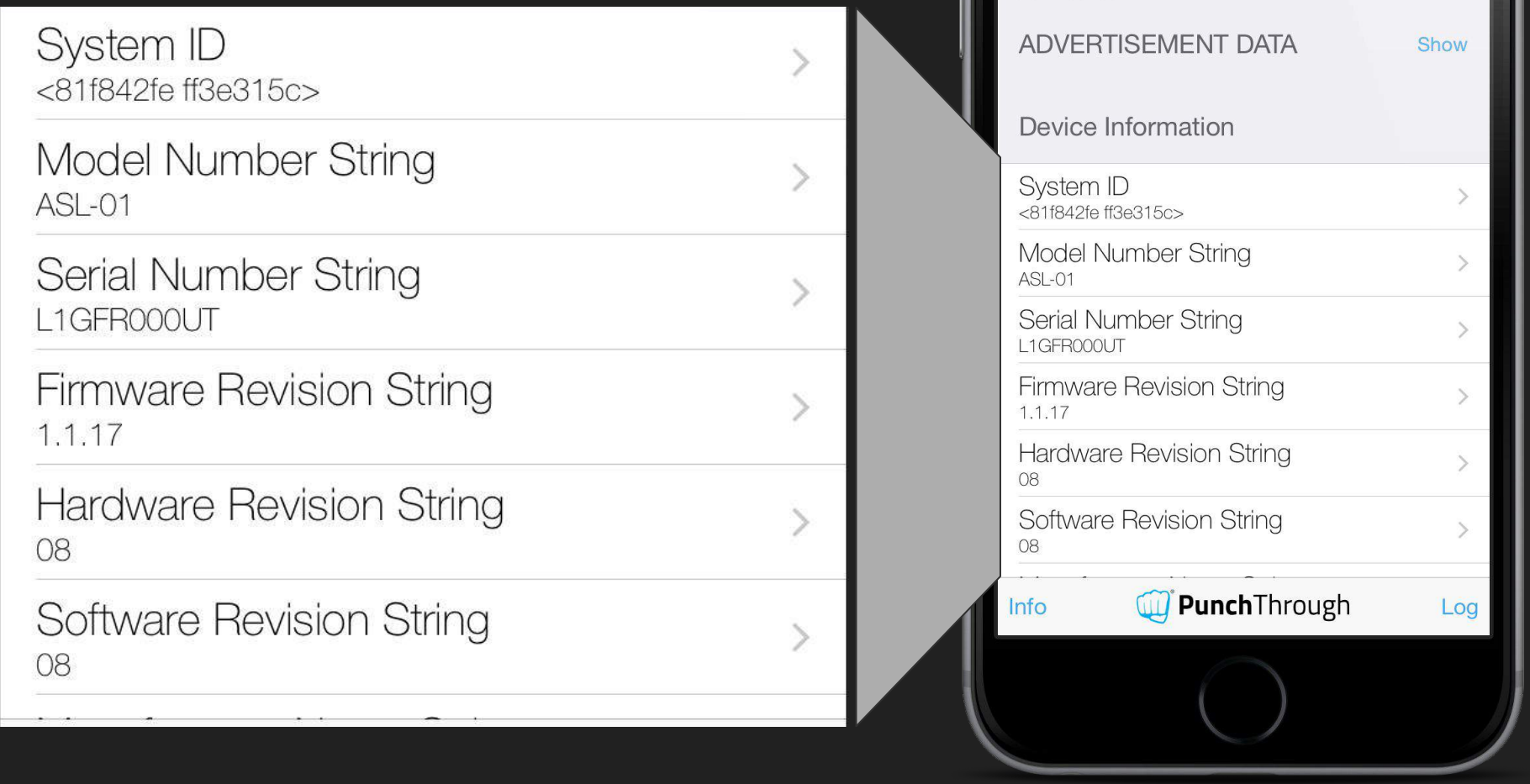
- ~~Perfectly secure~~
- Guest access can be revoked at any time
- Guest permission can be limited to a schedule
- Guest can not
  - ~~Use auto unlock~~
  - Invite or remove guests or owners
  - ~~View activity feed~~
  - View Guest List
  - ~~Change lock settings~~
- Keys can not be duplicated or distributed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

Mapping out the BLE API


WiFi | HTTPS
August
BLE

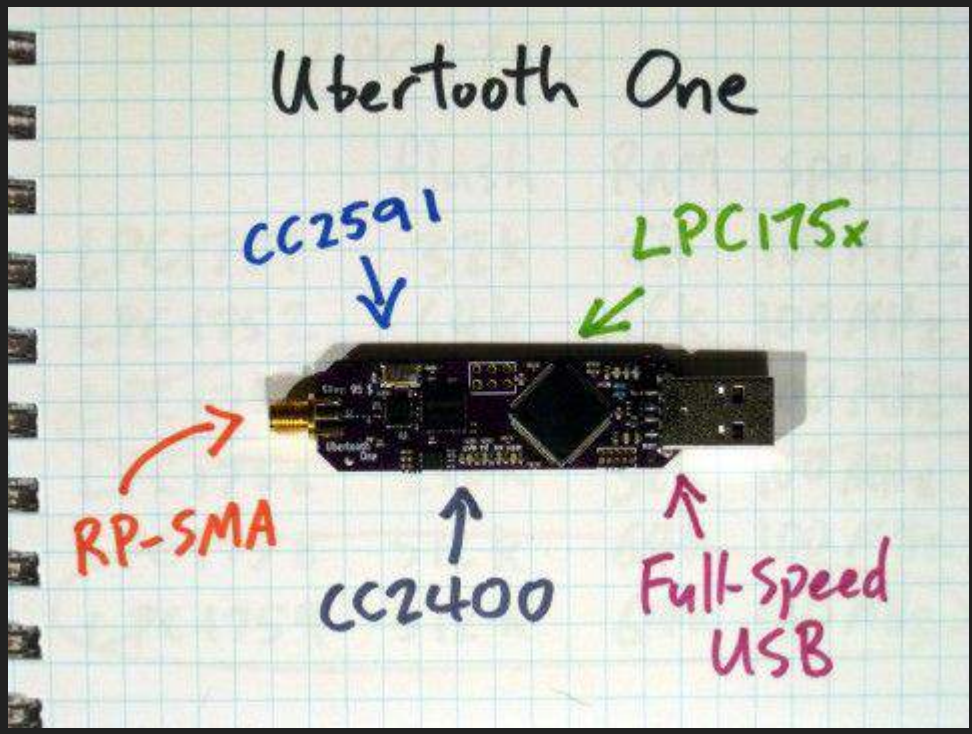
Enumerate BLE services




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
Verizon
9:33 AM
Back
Peripheral
Clone
August81
UUID: 42915464-4408-5438-77A4-0F0A35B8E5F7
Connected
ADVERTISEMENT DATA
Show
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
Info
PunchThrough
Log

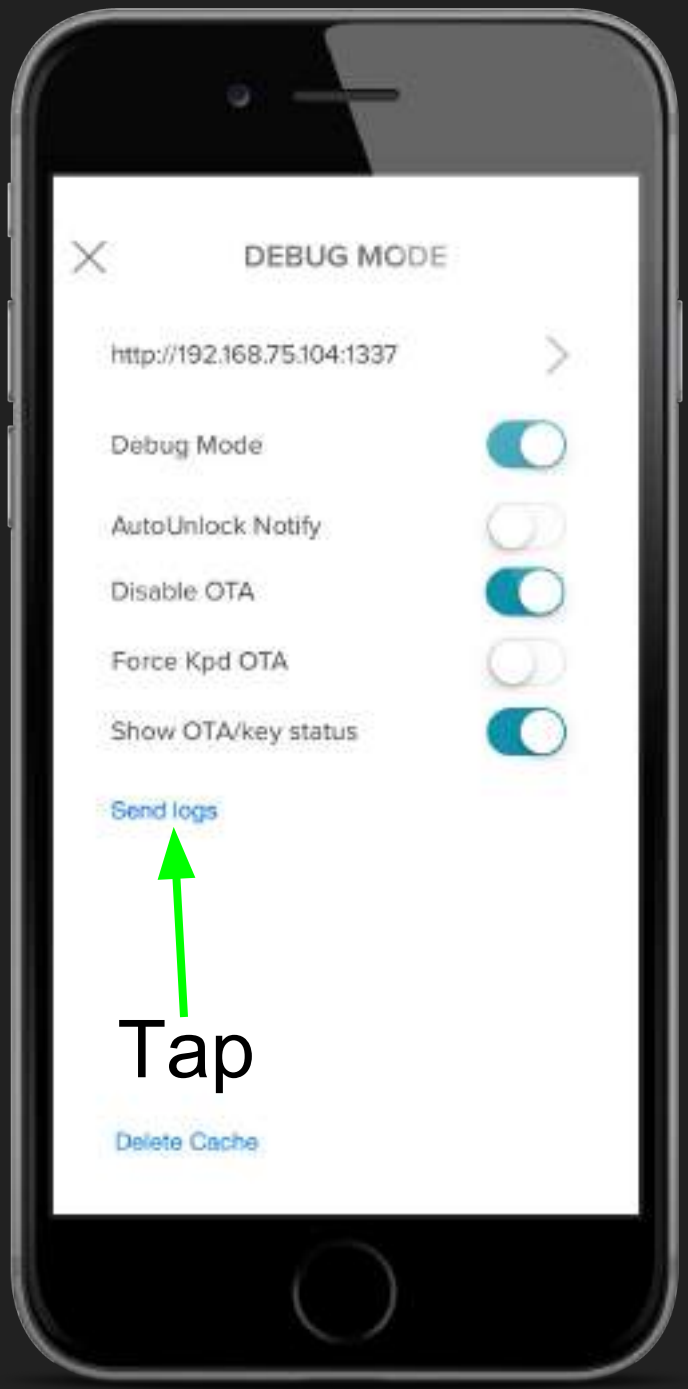
Intercepting BLE

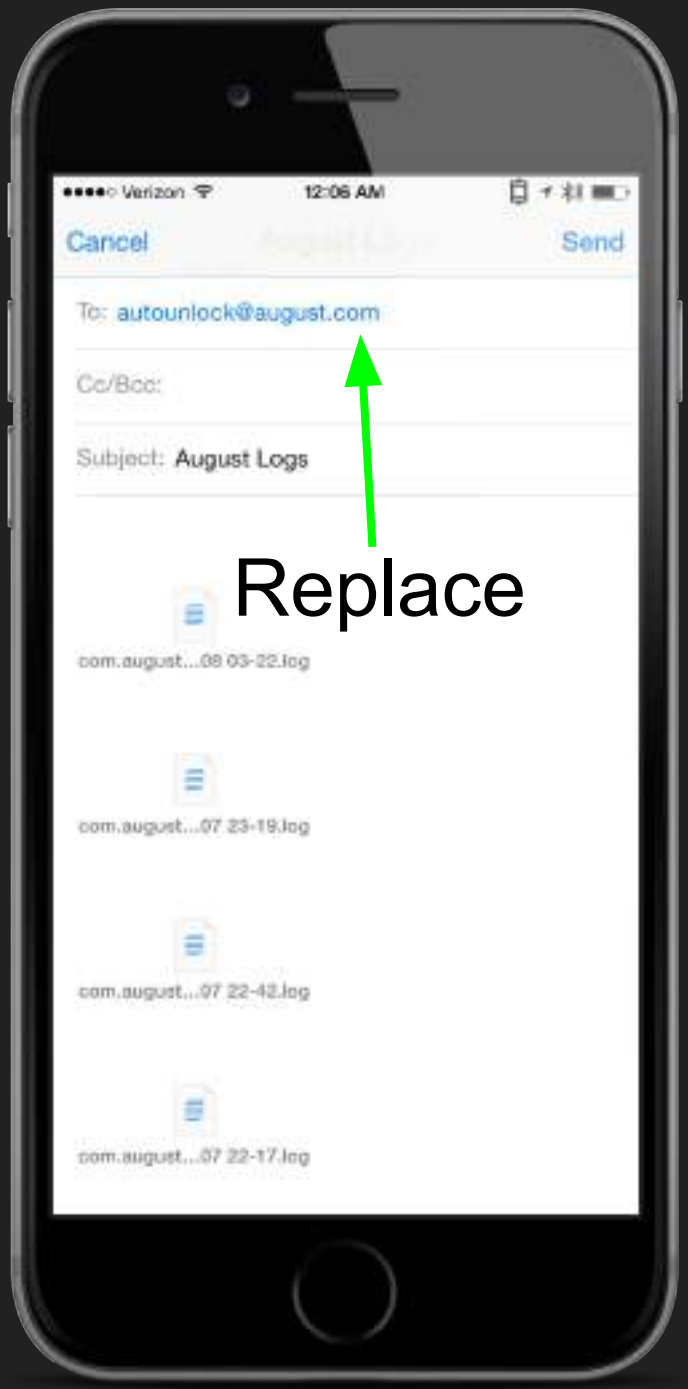
Solution: Ubertooth




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

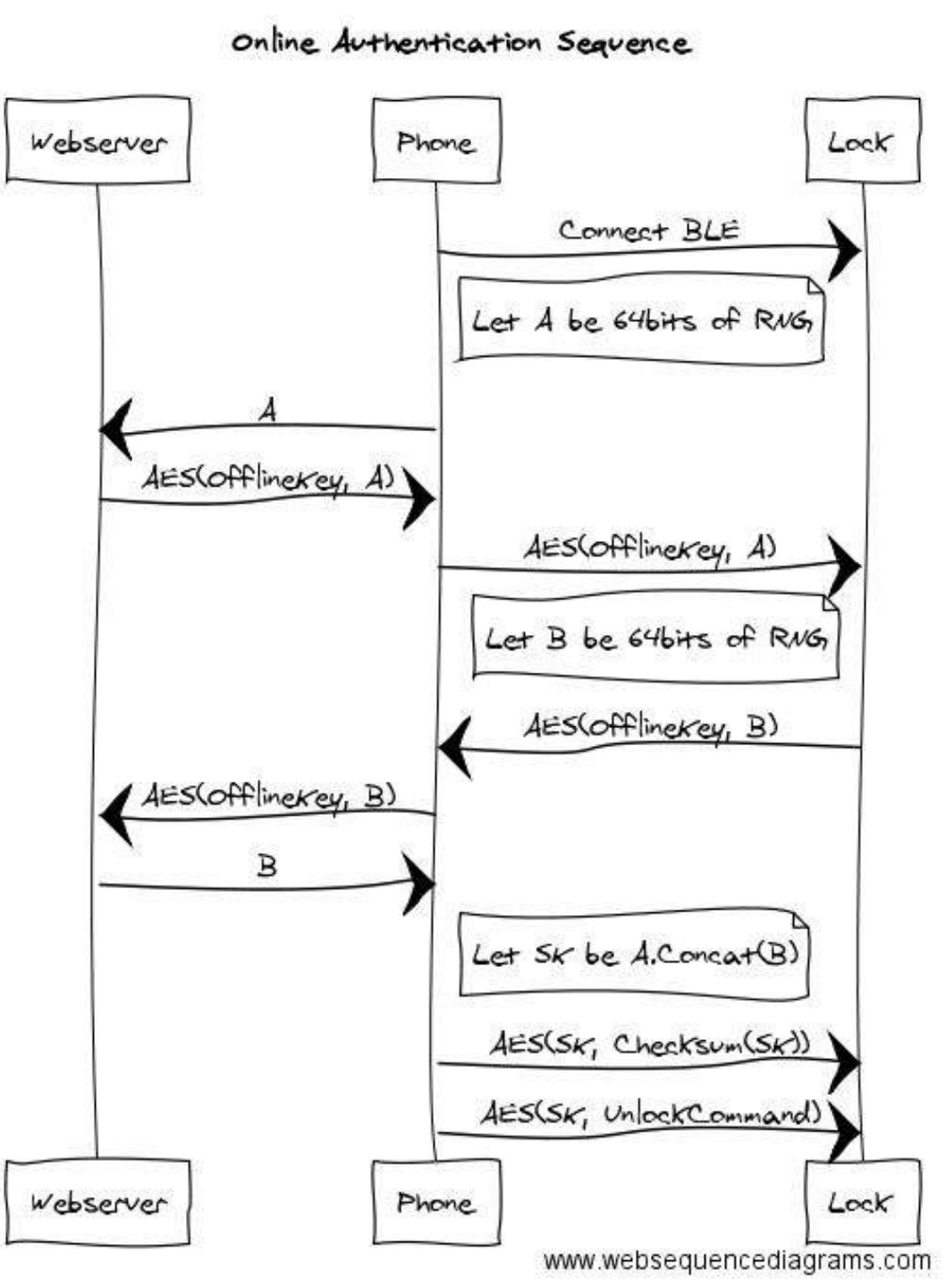

Verizon
12:06 AM
Cancel
Send
To: autounlock@august.com
Cc/Bcc:
Subject: August Logs
Replace
com.august...08 03-22.log
com.august...07 23-19.log
com.august...07 22-42.log
com.august...07 22-17.log

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>,
```

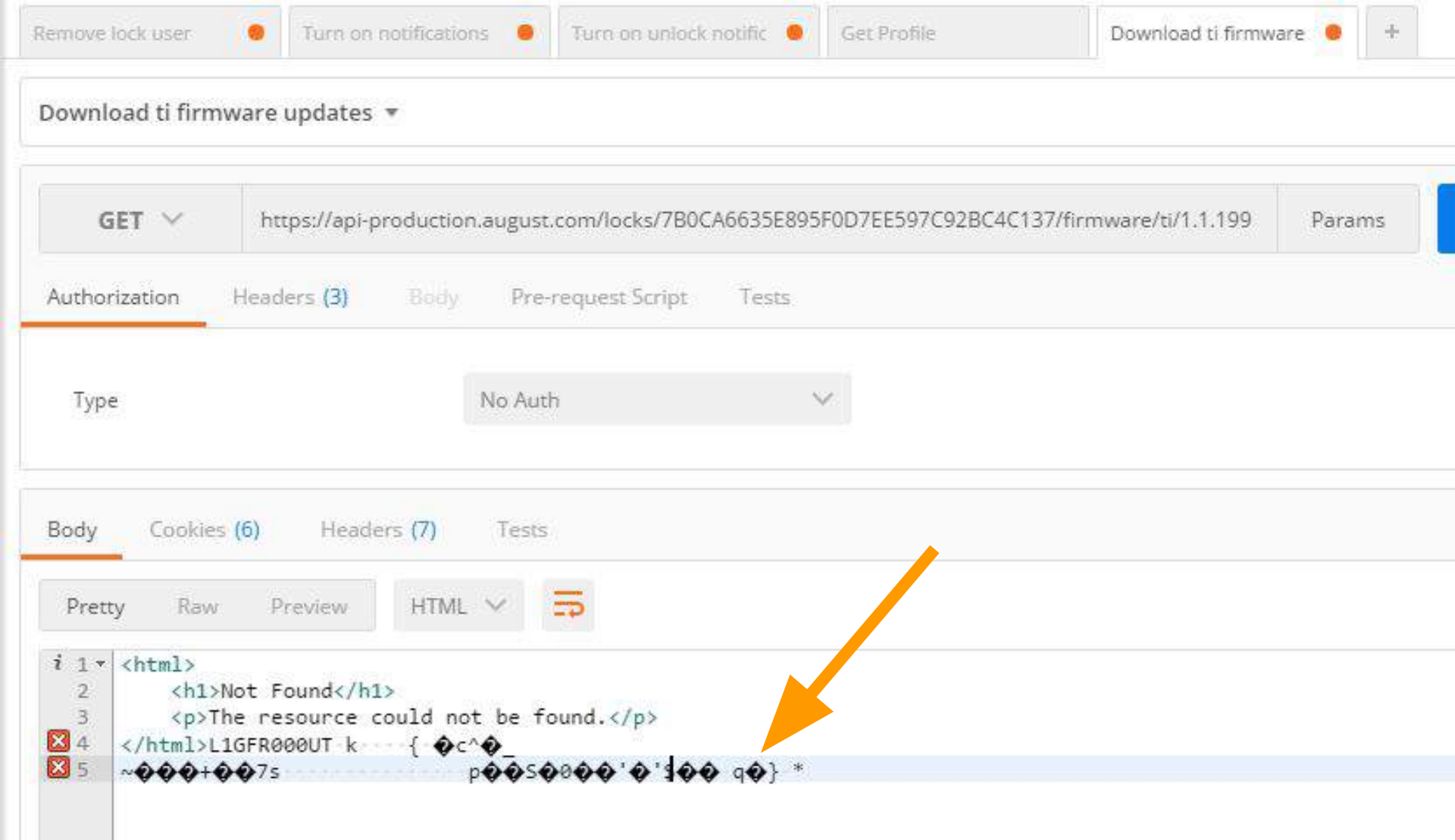
No Jailbreak

How August's authentication works


Online Authentication Sequence
Webserver
Phone
Lock
Connect BLE
Let A be 64bits of RNG
A
AES(offlinekey, A)
AES(offlinekey, A)
Let B be 64bits of RNG
AES(offlinekey, B)
AES(offlinekey, B)
B
Let Sk be A.Concat(B)
AES(Sk, Checksum(Sk))
AES(Sk, UnlockCommand)
Webserver
Phone
Lock
www.websequencediagrams.com

Requesting firmware as a guest

This is weird



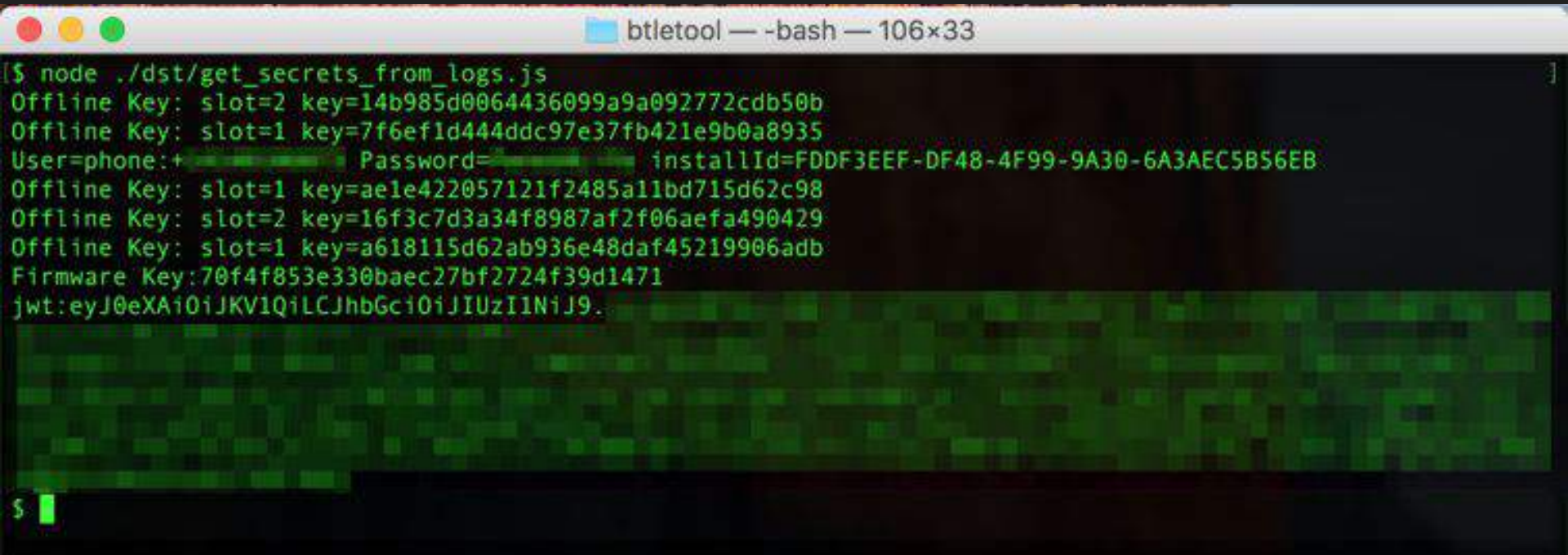
```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

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"}.*
```

"Safer than … codes that can be copied."

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

70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471
70F4F853E330BAEC27BF2724F39D1471

Key material in logs



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~~
- ~~Track who enters and exits your home~~

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

Code on
github
github.com/jmaxxz/keymaker



Demo

Mistakes made

- Mobile app logs include sensitive information
- Lock does not differentiate between guest and owner
- Firmware not signed
- No apparent way for average users to discover backdoor keys
- Guest users can download key material
- System relies on guests self reporting unlock/lock events
- Vendor claims two factor auth when really two step auth
- ~~No rate limiting of password reset attempts~~ (fixed)
- Mobile app includes bypass for certificate pinning
- ~~Secure random not used for nonce or session key generation~~ (fixed)
- Key material not stored on iOS keychain

What was done correctly

- August has been very responsive
- Mobile apps attempt to use certificate pinning
- Protocol makes use of nonces CBC
- 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 proof can be dismissed without proof.