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
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..."
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
MitM proxy

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)
Disabling SSL/TLS system wide at Defcon?
IT'S A BAD IDEA

MKAY
Better solution
August
This function can't be performed.
DreadfulDow
OK
Help
space
August Works With
123
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)
POST https://production.august.com/locks/log/

---

**Request**

```plaintext
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: VwEOVvVQwUHVNoQAk=
Host: production.august.com
```

**JSON**

```json
{
  "batteryLevel": 6315,
  "currentState": "Unlocked",
  "error": 0,
  "keySlot": 3,
  "log_type": "LockOperation",
  "opCode": "DoorStateChanged",
  "temperature": 164,
  "timeStamp": 946684883
}
```
Not anonymized
DON'T MIND US
Creepy
Let's fix this
MiTM can modify traffic
Fix

Don't forward log data to August, and tell app logs were received
What else can we do?
Guest to admin?
"locks": {
    "7B0CA6635E895F0D7EE597C92BC4C137": {
        "LockID": "7B0CA6635E895F0D7EE597C92BC4C137",
        "LockName": "Front Door",
        "UserType": "user"
    }
},
"locks": {
    "7B0CA6635E895F0D7EE597C92BC4C137": {
        "LockID": "7B0CA6635E895F0D7EE597C92BC4C137",
        "LockName": "Front Door",
        "UserType": "user"
    }
},
"doorbells": {},
"imageinfo": {
    "public_id": "",
    "version": 1399688143,
    "signature": "",
    "width": 1933,
    "height": 375,
    "format": "png",
    "resource_type": "image",
    "created_at": "2014-05-08T20:42:23Z",
    "bytes": 552431,
    "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": []
}
User Types

Guest = user
Owner = superuser
Replace "user" with "superuser"
Guests can change lock settings!
Guests can not use Auto-Unock
Guests can not control lock settings
YOU'RE WRONG
GET OUT!!
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
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

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

Connected

ADVERTISEMENT DATA

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

Punch Through

Log
<16000215 7b0ca663 5e895f0d 7ee597c9 2bc4c137
Manufacturer Data
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
Better solution
Replace
Plaintext BLE traffic in log files!

cipherText: <3e6c47ac 367d8735 f06bd842 3d86a0d7 0200> clearText: <ee0400e4 28000000 00000000 00000000 00000000 0200>,
cipherText: <a1cf80d2 a22d6eab8 b66e63071 0062ae50 0200> clearText: <ee0300e5 28000000 00000000 00000000 00000000 0200>,
cipherText: <7fba14da 82b2cdac aac6698d 43609ff0b 0200> clearText: <ee02000b 03000000 00000000 00000000 00000000 0200>,
cipherText: <09db706 5c7a0ba4 6a5efe7c c8df1150 0200> clearText: <ee02000b 03000000 00000000 00000000 00000000 0200>,
cipherText: <fb8305b3 50843c7d 497d685e c423f03e 0200> clearText: <ee0300eb 20000000 02000000 00000000 00000000 0200>,
cipherText: <c7269071 e1f0f51f 6264c5c8 a5526e1d 0200> clearText: <ee030018 18000000 b7260000 02000000 00000000 0200>,
cipherText: <60e0d03f6 0a535481 c1931212 92c2a1a49 0200> clearText: <ee030002 1a000000 cf220000 00000000 0200>,
cipherText: <2e281ce5 2ef77237 a6320935 83771a05 0200> clearText: <ee030014 19000000 ed5ff000 00000000 0200>,
cipherText: <ae74bc1f b793a32 32621cf6 da44c010 0200> clearText: <ee030026 1b000000 d5f9ff00 00000000 0200>,
cipherText: <9f3010a6 2b180d2b 33cb0260 b3183e1b 0200> clearText: <ee0300d4 38000000 01000000 00000000 00000000 0200>,
cipherText: <586d289b 9bc9502f 45ecc03c 14ad460a 0200> clearText: <ee0300e5 28000000 00000000 00000000 00000000 0200>,
cipherText: <6004d424 88e840bc 9f8fbc40 34bd1054 0200> clearText: <ee0200c0 02000000 00000000 00000000 00000000 0200>,
cipherText: <c516758e 2723bbba 600eb93e 3ea4ddde 0200> clearText: <ee0b0005 00000000 00000000 00000000 00000000 0200>,
cipherText: <193bb7f8 05f9e80e a4b46d0b e3da1910 0200> clearText: <ee02000c 02000000 00000000 00000000 00000000 0200>,
cipherText: <2edd4fbd 56b41f94 86f50ba4 67841005 0200> clearText: <ee02000e 28000000 00000000 00000000 00000000 0200>,
cipherText: <e5c2be83ff83cd4c 692e3a2c 5a5a043f 0200> clearText: <ee0200e5 29000000 00000000 00000000 00000000 0200>,
cipherText: <d4d1a991 d7b52f47 cc0fe9915 d938c2b2 0200> clearText: <ee0200e2 2c000000 00000000 00000000 00000000 0200>,
cipherText: <de640518 69ba8698 f0840840 98d30438 0200> clearText: <ee020005 02000000 00000000 00000000 00000000 0200>,
No Jailbreak
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
<html><h1>Not Found</h1><p>The resource could not be found.</p></html>
Firmware key 'can not' be changed
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
POST  
https://api-production.august.com/locks/setnotification/7B0CA6635E895F0D7EE597C92BC4C137? 

Authorization: No Auth

Body:
```
{
    "message": "success"
}
```
Welcome to August!

Set up a Smart Lock

August
Iphone 5 S3 unlocked Front Door at Iphone 5’s House

I Received an Airbnb Invite
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.