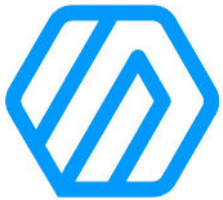
Cracking **Fun** with **Frida** & **Radare**

Mobile App & IoT Edition

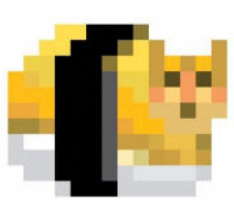
NowSecure

Who Are We and What We Do?

- **Sergi Alvarez** aka pancake
  - Author of radare2 and r2frida
- **Ole André** also known as oleavr
  - Author of Frida



Free Software enthusiasts working as Mobile Security Researchers at NowSecure.



- Saving the world from unsafe mobile apps

NowSecure

Agenda - Inspecting an IoT app

- Pick an app and take a look
- Instrumenting the interface and the APIs
- Checking and reducing the resources used
- Detecting and blocking data leaks
- Flashing lights when using the microphone

NowSecure

Selecting and Inspecting the App

- **Target:** iOS app to control RGB LEDs via Bluetooth
- App name: “LED BLE” available on the App Store
  - Last update was in 2018
  - No auth is required to use the LEDs
- Tooling used: **r2, frida** and **r2frida**

Privacy and Security

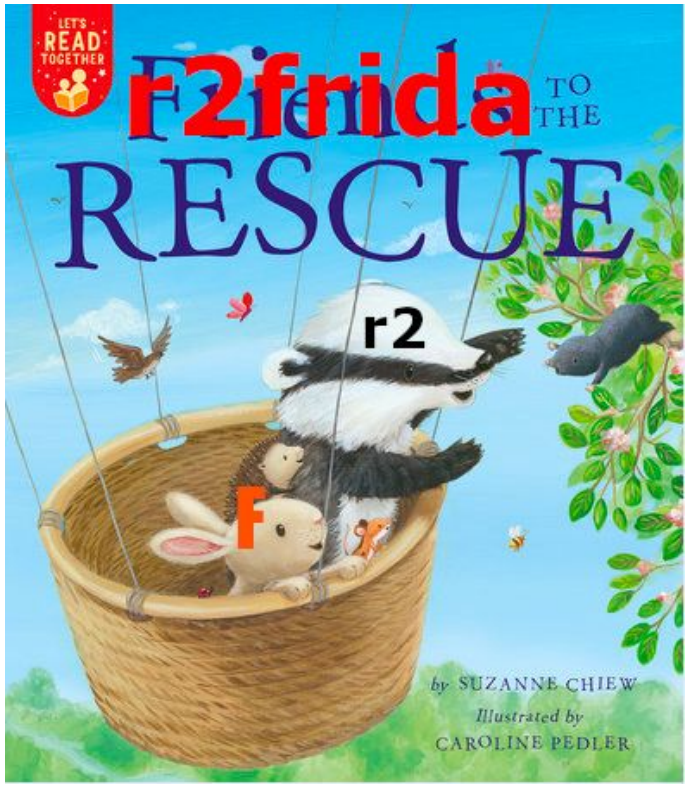
NowSecure

Early Instrumentation

- Manipulate process memory and code before executing the app.
- Catch startup and bg activity.
- r2frida commands start with:

```
$ r2pm -ci r2frida
$ r2 frida://launch/usb//LED BLE
```

- launch
- spawn
- attach



NowSecure

Fetching Resources

- Install app from the App Store
- Use `.:init` to setup r2 for the frida targe
- Use `ms` to mount the remote fs
- See :i app home, bundle and tmpdir
- Retrieve the Info.plist and main binary
- Dump decrypted region to patch in disk

```
[0x00000000]> .:init
Mounted io on /r2f at 0x0
Cannot seek to unknown address 'er
[0x00000000]> ms
[/]> cd /r2f
[/r2f]> ls
d AppHome
d AppBundle
d Device
[/r2f]> cd AppBundle
[/r2f/AppBundle]> get Info.plist
[/r2f/AppBundle]> !vim Info.plist
```

NowSecure

Entitlements, Info.Plist and Strings

- The app is requesting no special entitlements
- But have access to geolocation, pictures, microphone…
- Several plain http:// URLs can be spotted
- The https:// ones are just for tracking the user.

```
# rabin2 -OC LED\ BLE
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.c
<plist version="1.0">
<dict>
        <key>aps-environment</key>
        <string>production</string>
        <key>com.apple.developer.team-identifier</key>
        <string>89WUL7J5PK</string>
        <key>application-identifier</key>
        <string>89WUL7J5PK.com.huyajun.LedBle</string>
</dict>
</plist>
```

NowSecure

Inspecting App's Classes

- In static r2 list the classes with ic.
- For r2frida use :icw LED
- Analysis mainly recommended in static, for r2frida use asm.slow=false
- Analyze with aao;aac;aaef;aa
- Use V_ to filter out the symbols of interest and follow xrefs with x

Instances of classes

The `icw` command find where the classes are defined.

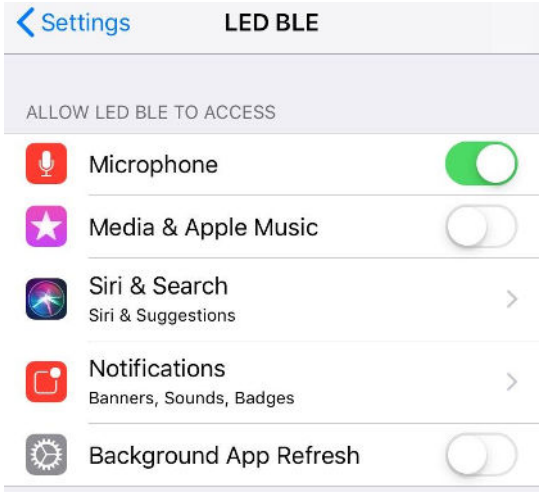
```
[0x00000000]> :icw LED~0x > a
...connect to the lights using th
[0x00000000]> :icw LED~0x > b
```

Check for changes to find out if there's any new instance:

```
[0x00000000]> !diff -u a b
--- a   2021-07-02 18:19:59.00000
+++ b   2021-07-02 18:20:13.00000
-JKBLEServicAndCharacter #
+JKBLEServicAndCharacter # 0x282
-JKBLEManager #
+JKBLEManager # 0x2825ba3c0
-SVProgressHUD #
+SVProgressHUD # 0x101044210
[0x00000000]>
```

Microphone, Music and Photos

- Audio can be blocked in Settings
- But there's no way to block gallery access or backgrounds code calls
- Let's block all those with r2frida!




```
:e hook.usecmd=:?E Wooops
:dif0 objc:AVAudioSession.sharedInstance
:dif0 objc:UIImagePickerController.isSourceTypeAvailable:
```

NowSecure

Network Instrumentation

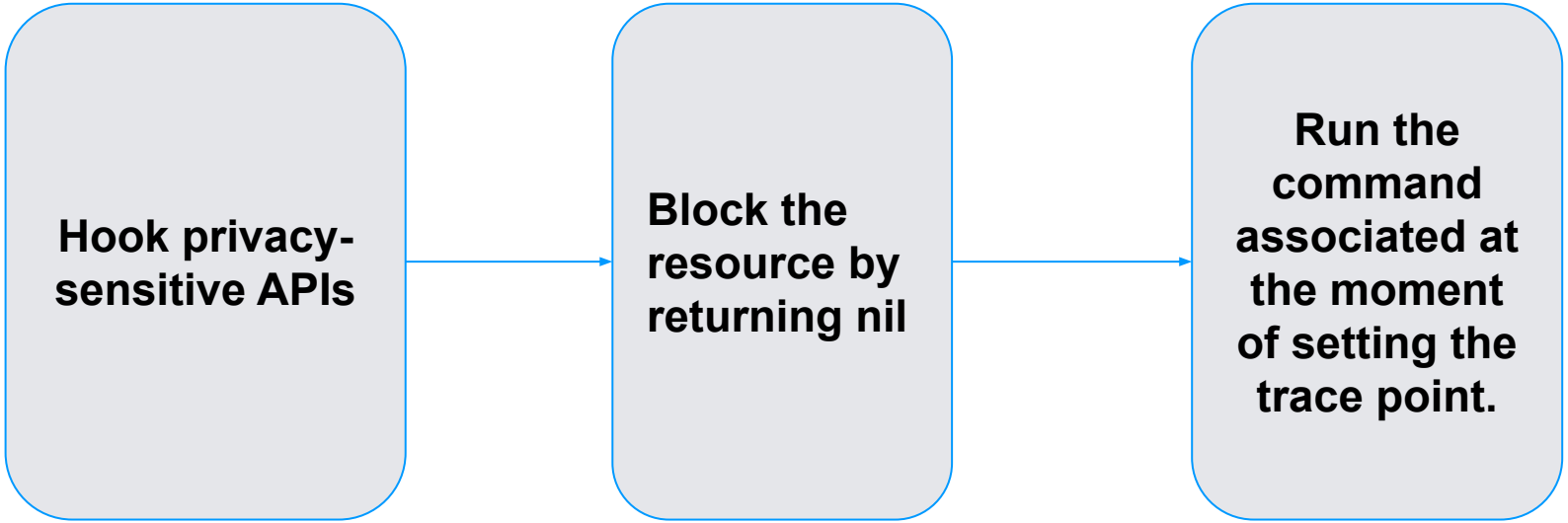
- Enable `:ws trace-crypto probe`
- Or use `dtf/dif0` wisely to trace URLs, POSTs and crypto calls
- Data is sent in POST and it's encrypted using `b64(aes(json))`.
- Keys and URLs can be easily retrieved with Workstation r2frida plugins

```
:dtf objc:NSURLSession.sharedSession OOO
:dtf objc:NSMutableURLRequest.setHTTPBody: OOO
```

```
{"scope":"CommonCrypto","name":"CCCryptorGetOutputLength","args":{}}
{"scope":"CommonCrypto","name":"CCCryptorUpdate","args":{}}
{"scope":"CommonCrypto","name":"CCCryptorFinal","args":{}}
{"scope":"CommonCrypto","name":"CCCryptorRelease","args":{}}
[trace-crypto] - [AES] Operation: Decrypt
[trace-crypto] - [AES] Mode: CBC
[trace-crypto] - [AES] Key: 383365353563643636646335356533 38
[trace-crypto] - [AES] IV: 0A010B05040F070917030106080C0D5B
[trace-crypto] - [AES] - Input:
133dc2e00  58 ec f2 f0 4b d4 f0 22 29 e9 ec 87 ad 7f 1e 76  X...K..").....v
133dc2e10  69 0e 52 e2 03 43 70 b9 02 72 9f 1b 8b 8e c3 b7  i.R..Cp..r......
133dc2e20  c2 4b 61 99 68 11 cd 00 06 de 82 70 64 eb 34 95  .Ka.h......pd.4.
133dc2e30  e0 9d 77 19 6d 8c a3 30 99 08 82 c4 88 b7 cb db  ..w.m..0........
133dc2e40  ad d5 75 d0 63 f0 60 f9 34 3f 8c b4 64 9a cb 6c  ..u.c.`.4?..d..l
....
[trace-crypto] - [AES] - Output:
133dce890  5b 7b 22 64 75 72 61 74 69 6f 6e 22 3a 35 34 30  [{"duration":540
133dce8a0  38 2c 22 70 61 67 65 5f 6e 61 6d 65 22 3a 22 4d  8,"page_name":"M
133dce8b0  75 73 69 63 56 69 65 77 43 6f 6e 74 72 6f 6c 6c  usicViewControll
133dce8c0  65 72 22 7d 2c 7b 22 64 75 72 61 74 69 6f 6e 22  er"},{"duration"
133dce8d0  3a 35 32 31 2c 22 70 61 67 65 5f 6e 61 6d 65 22  :521,"page_name"
133dce8e0  3a 22 54 69 6d 65 56 69 65 77 43 6f 6e 74 72 6f  :"TimeViewContro
133dce8f0  6c 6c 65 72 22 7d 2c 7b 22 64 75 72 61 74 69 6f  ller"},{"duratio
133dce900  6e 22 3a 37 35 32 2c 22 70 61 67 65 5f 6e 61 6d  n":752,"page_nam
133dce910  65 22 3a 22 4d 75 73 69 63 56 69 65 77 43 6f 6e  e":"MusicViewCon
133dce920  74 72 6f 6c 6c 65 72 22 7d 2c 7b 22 64 75 72 61  troller"},{"dura
133dce930  74 69 6f 6e 22 3a 37 32 33 2c 22 70 61 67 65 5f  tion":723,"page_
133dce940  6e 61 6d 65 22 3a 22 4d 75 73 69 63 56 69 65 77  name":"MusicView
133dce950  43 6f 6e 74 72 6f 6c 6c 65 72 22 7d 2c 7b 22 64  Controller"},{"d
133dce960  75 72 61 74 69 6f 6e 22 3a 33 34 37 37 32 37 2c  uration":347727,
133dce970  22 70 61 67 65 5f 6e 61 6d 65 22 3a 22 52 6f 6f  "page_name":"Roo
133dce980  74 56 69 65 77 43 6f 6e 74 72 6f 6c 6c 65 72 22  tViewController"
133dce990  7d 2c 7b 22 64 75 72 61 74 69 6f 6e 22 3a 33 34  },{"duration":34
133dce9a0  37 37 37 31 2c 22 70 61 67 65 5f 6e 61 6d 65 22  7771,"page_name"
133dce9b0  3a 22 55 49 4e 61 76 69 67 61 74 69 6f 6e 43 6f  :"UINavigationCo
```

NowSecure

Building Our Toy



NowSecure

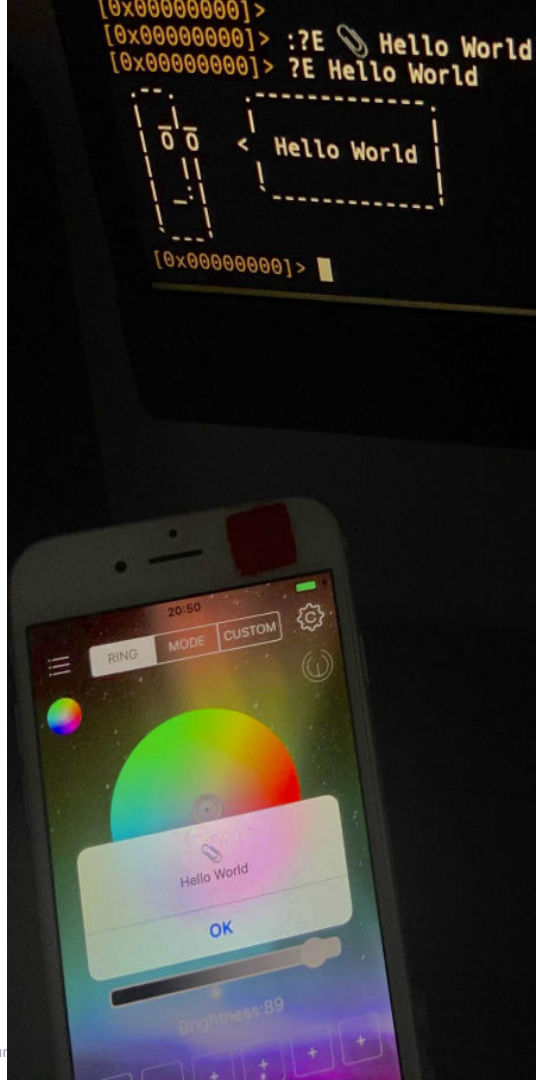
Running The Script

```
> cat flash-red.r2
"$bright=:dxo MulticolorViewController sendDataBright: "
"$flash=$bright 100;!sleep 0.3;$bright 1;!sleep 0.3"
"$rgb :dxo MulticolorViewController sendDataRGBWithRed_green_blue_ "
?E we dont want the microphone

# ensure we are using the right panel
:dxo MulticolorViewController viewWillDisappear: 0
:dxo MulticolorViewController viewWillAppear: 0
sleep 1

# light stuff
$rgb 255 0 0
5$flash
$rgb 1 1 1

> :e hook.usecmd=. flash-red.r2
> :dif0 objc:AVAudioSession.sharedInstance
> &w
```



NowSecure

To Learn More

If you want to understand in more detail all the topics explained in this presentation, please follow the link below:

- https://bit.ly/ns-r2-led

NowSecure

Thanks For Watching

NowSecure