ERNW
providing security.

AIROHA
達發科技股份有限公司

Headphone Jacking: A Key to Your Phone

Hacking Airoha-based Bluetooth Audio Devices

Troopers 2025 - Dennis Heinze & Frieder Steinmetz

ERNW
providing security.

Back in the old days...

ERNW
providing security.

Then vendors started to remove the headphone jack

ERNW
providing security.

Now these have become the new standard

ERNW
providing security.

Which means that Bluetooth headphones are everywhere

ERNW
providing security.

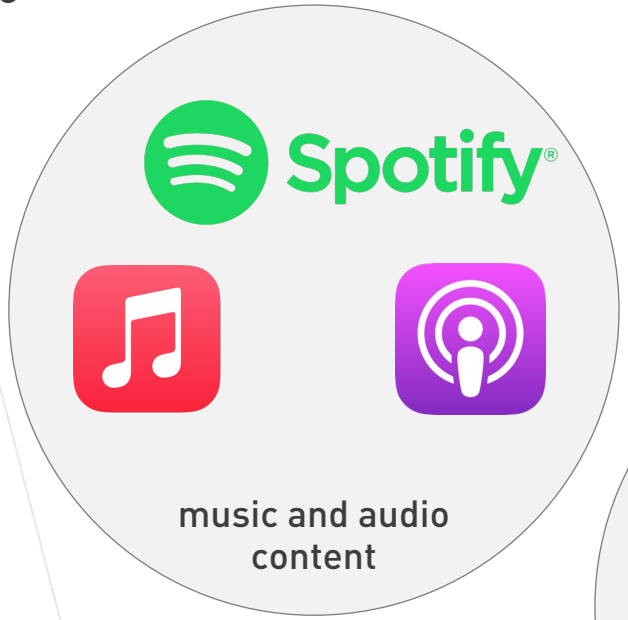
And at the center there's this love relationship

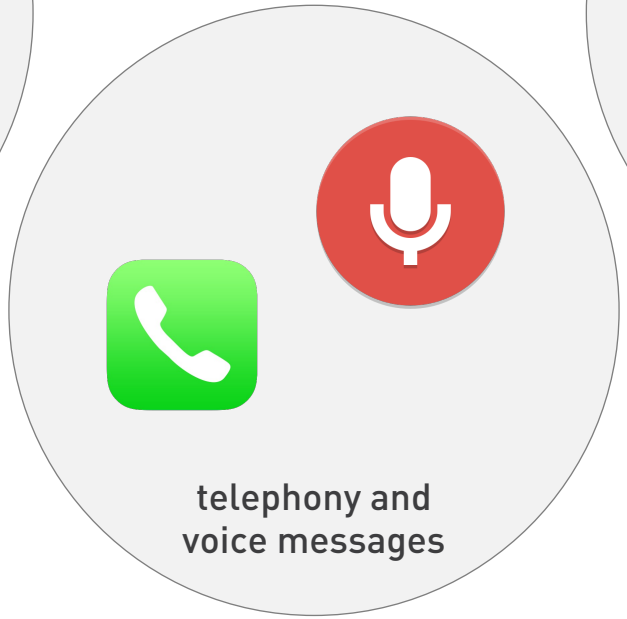
ERNW
providing security.

Or rather:
This cryptographic bond

ERNW
providing security.

What do people use headphones for?





ERNW
providing security.

Let‘s imagine an evil pair of headphones...

ERNW
providing security.

Listen to your calls

Call someone

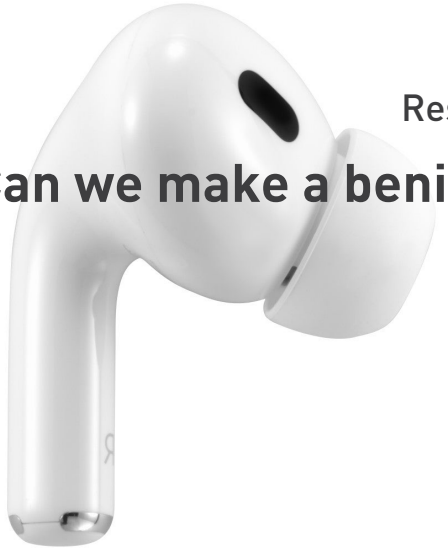
Listen to your microphone

Access your phonebook

Listen to your content (music, podcasts)

Act as input device?

This has been discussed before. Most OSes prevent this now.



Research idea:

Can we make a benign pair of headphones evil?

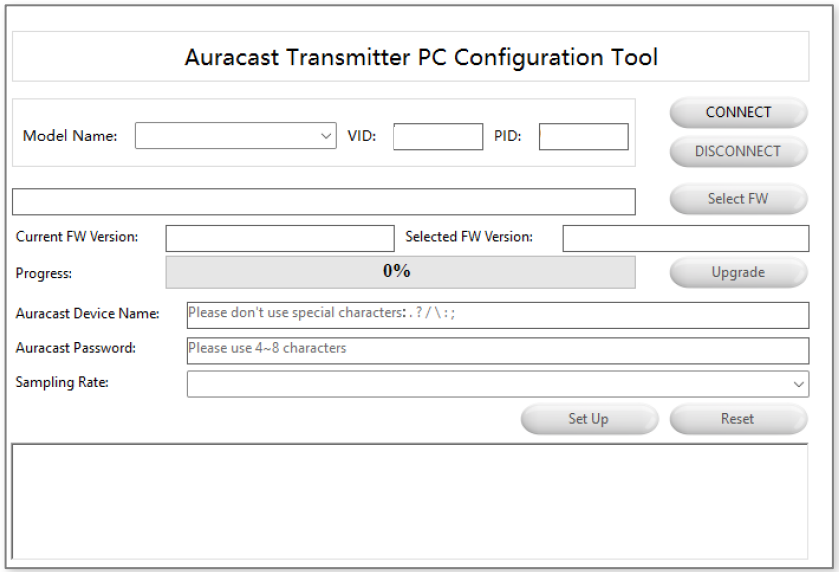
We still had some headphones from our previous Bluetooth Auracast research.

Starting research on an IoT project:

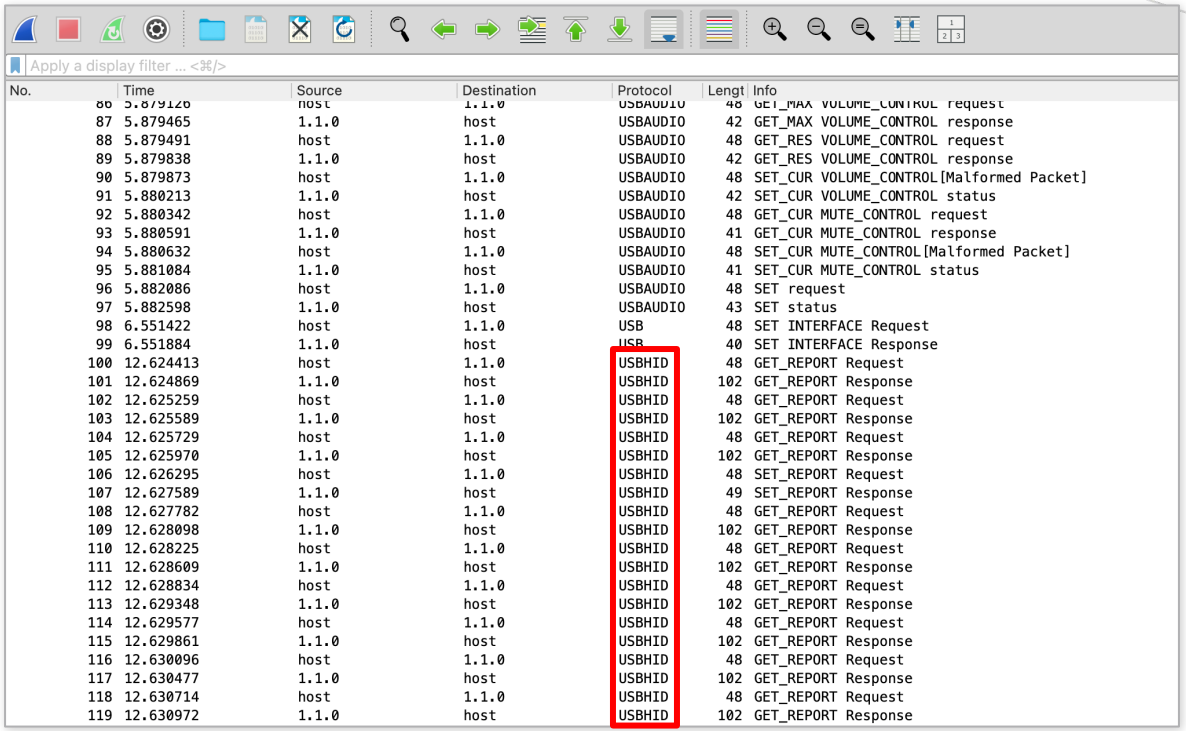
- Trying to obtain the device firmware
- Analyzing the firmware
- Identifying debugging interfaces

We have a firmware update file!

We also had the Auracast transmitter from our research.



The tool to configure and update the Auracast transmitter via USB.



Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Lengt	Info
86	5.879126	host	1.1.0	USBAUDIO	48	GET_MAX VOLUME_CONTROL request
87	5.879465	1.1.0	host	USBAUDIO	42	GET_MAX VOLUME_CONTROL response
88	5.879491	host	1.1.0	USBAUDIO	48	GET_RES VOLUME_CONTROL request
89	5.879838	1.1.0	host	USBAUDIO	42	GET_RES VOLUME_CONTROL response
90	5.879873	host	1.1.0	USBAUDIO	48	SET_CUR VOLUME_CONTROL[Malformed Packet]
91	5.880213	1.1.0	host	USBAUDIO	42	SET_CUR VOLUME_CONTROL status
92	5.880342	host	1.1.0	USBAUDIO	48	GET_CUR MUTE_CONTROL request
93	5.880591	1.1.0	host	USBAUDIO	41	GET_CUR MUTE_CONTROL response
94	5.880632	host	1.1.0	USBAUDIO	48	SET_CUR MUTE_CONTROL[Malformed Packet]
95	5.881084	1.1.0	host	USBAUDIO	41	SET_CUR MUTE_CONTROL status
96	5.882086	host	1.1.0	USBAUDIO	48	SET request
97	5.882598	1.1.0	host	USBAUDIO	43	SET status
98	6.551422	host	1.1.0	USB	48	SET INTERFACE Request
99	6.551884	1.1.0	host	USB	40	SET INTERFACE Response
100	12.624413	host	1.1.0	USBHID	48	GET_REPORT Request
101	12.624869	1.1.0	host	USBHID	102	GET_REPORT Response
102	12.625259	host	1.1.0	USBHID	48	GET_REPORT Request
103	12.625589	1.1.0	host	USBHID	102	GET_REPORT Response
104	12.625729	host	1.1.0	USBHID	48	GET_REPORT Request
105	12.625970	1.1.0	host	USBHID	102	GET_REPORT Response
106	12.626295	host	1.1.0	USBHID	48	SET_REPORT Request
107	12.627589	1.1.0	host	USBHID	49	SET_REPORT Response
108	12.627782	host	1.1.0	USBHID	48	GET_REPORT Request
109	12.628098	1.1.0	host	USBHID	102	GET_REPORT Response
110	12.628225	host	1.1.0	USBHID	48	GET_REPORT Request
111	12.628609	1.1.0	host	USBHID	102	GET_REPORT Response
112	12.628834	host	1.1.0	USBHID	48	GET_REPORT Request
113	12.629348	1.1.0	host	USBHID	102	GET_REPORT Response
114	12.629577	host	1.1.0	USBHID	48	GET_REPORT Request
115	12.629861	1.1.0	host	USBHID	102	GET_REPORT Response
116	12.630096	host	1.1.0	USBHID	48	GET_REPORT Request
117	12.630477	1.1.0	host	USBHID	102	GET_REPORT Response
118	12.630714	host	1.1.0	USBHID	48	GET_REPORT Request
119	12.630972	1.1.0	host	USBHID	102	GET_REPORT Response

Writing Data

USB HID Packets

???	CMD ID	80 08 52 f8 71 a4 2f 25 26 e5
???	CMD ID	88 08 2f 43 93 26 3e 58 c1 19
???	CMD ID	90 08 55 96 a7 ff ec c0 20 00
???	CMD ID	98 08 11 00 41 42 31 35 36 35
???	CMD ID	A0 08 5f 4c 45 41 5f 44 4f 4e
???	CMD ID	A8 08 47 4c 45 21 00 0c 00 64

Update File

00000180:	52 f8 71 a4 2f 25 26 e5	|R.q./%&.|
00000188:	2f 43 93 26 3e 58 c1 19	|/C.&>X..|
00000190:	55 96 a7 ff ec c0 20 00	|U..... .|
00000198:	11 00 41 42 31 35 36 35	|..AB1565|
000001a0:	5f 4c 45 41 5f 44 4f 4e	|_LEA_DON|
000001a8:	47 4c 45 21 00 0c 00 64	|GLE!...d.
...	...	...

Following the CMD_ID

```
switch(cmd_id) {
  case 0x100:
    pvVar3 = FUN_0838bad4(&inputMsg->hdr,length,transport_id);
    return pvVar3;
  case 0x102:
    pvVar3 = cmd_write_page(&inputMsg->hdr,length,transport_id);
    return pvVar3;
  case 0x103:
    pvVar3 = FUN_0838b920(&inputMsg->hdr,length,transport_id);
    return pvVar3;
  case 0x104:
    pvVar3 = FUN_0838b994(&inputMsg->hdr,length,transport_id);
    return pvVar3;
}
```

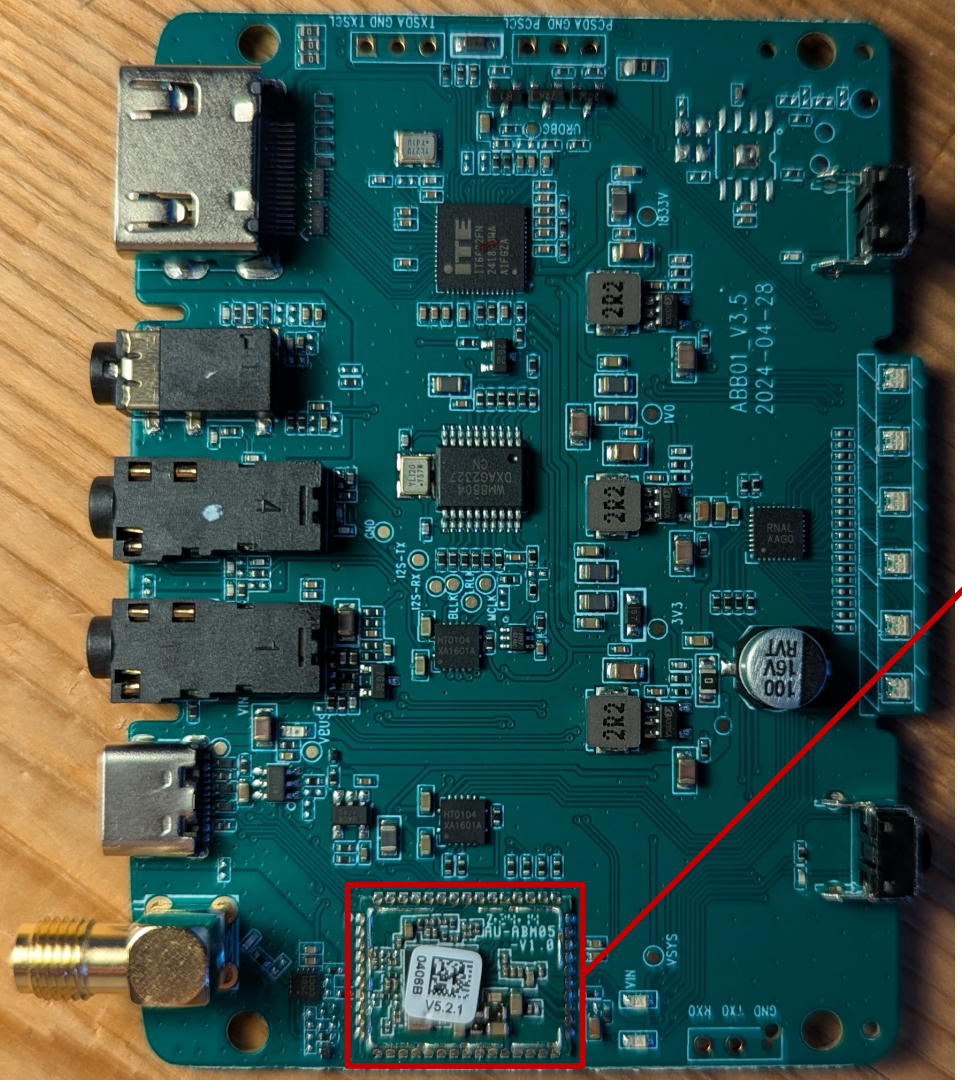
ERNW
providing security.

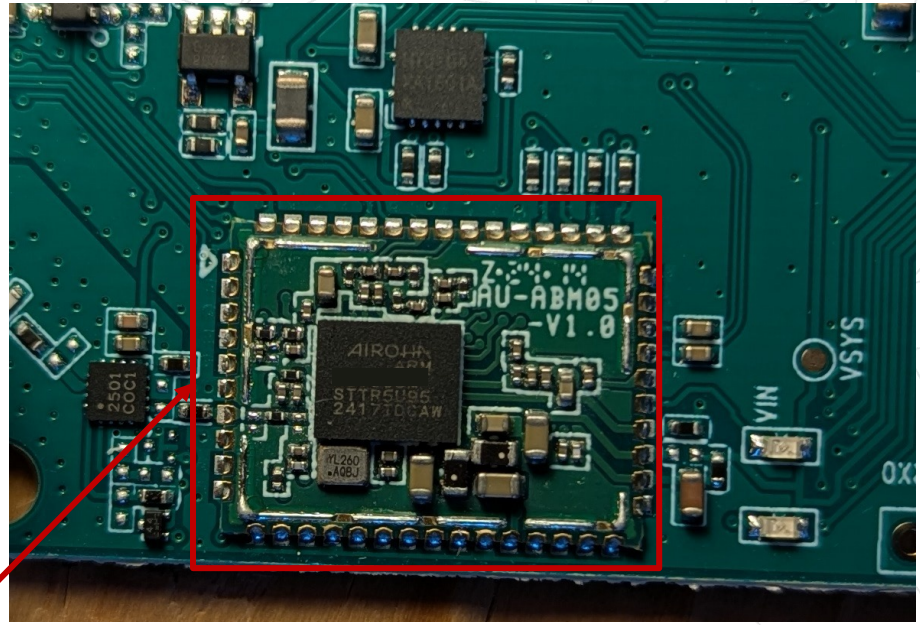
Found the Read Command

- We were able to dump flash via USB HID.
- And it worked for the headphones too!

Are there more prestigious affected devices?

No, not these $9.000 Bose diamond crusted earbuds...





What do the headphones and transmitter have in common?

AIROHA

達發科技股份有限公司

AB1565M

In fact, there are plenty of fancy flagship devices with Airoha Bluetooth chips.

So, we bought one.

No USB 😭

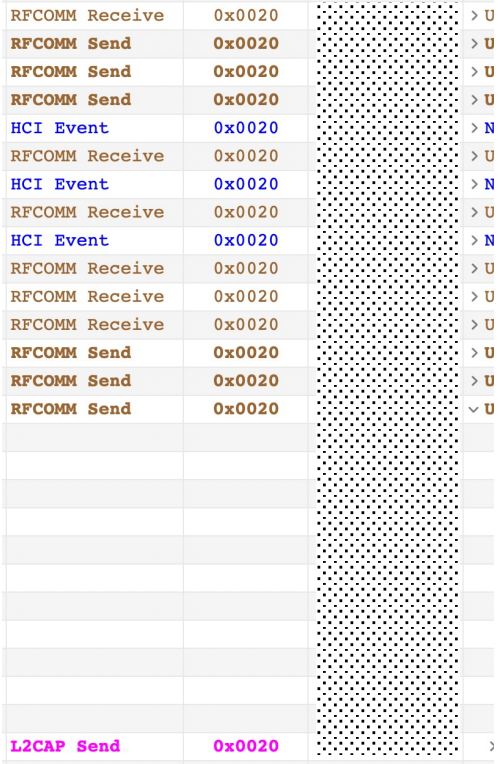
```
(.venv) frieder@fswork-ng ~/ERNW/research/le_audio/airoha sudo python hid_dump.py
Traceback (most recent call last):
  File "/home/frieder/ERNW/research/le_audio/airoha/hid_dump.py", line 158, in <module>
    device = find_hid_device(VID, PID)
  File "/home/frieder/ERNW/research/le_audio/airoha/hid_dump.py", line 13, in find_hid_device
    return hid.Device(vid, pid)
           ~~~~~~~~~~^^^^^^^^^^
  File "/home/frieder/ERNW/research/le_audio/.venv/lib/python3.13/site-packages/hid/__init__.py
", line 174, in __init__
    raise HIDException('unable to open device')
hid.HIDException: unable to open device
```

ERNW
providing security.

But how do you update the headphones?

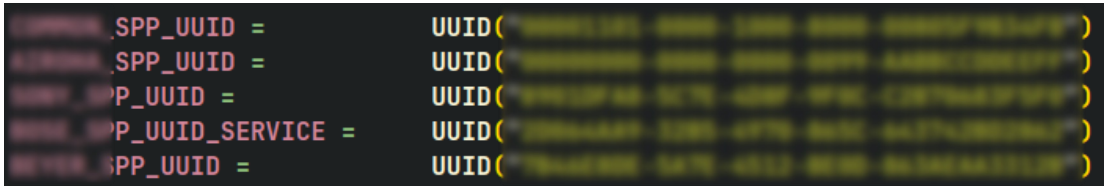
There‘s an app for that!

Firmware updates use RFCOMM!

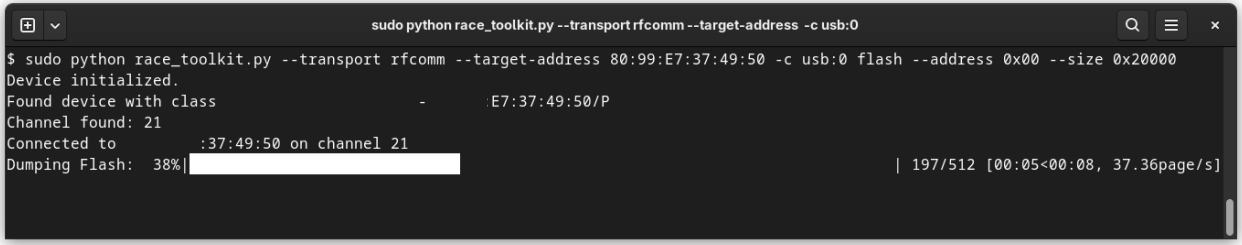


Bluetooth Classic as Transport

- **Our Protocol** uses the RFCOMM profile as transport
- **RFCOMM** has channels that are identified by their channel number (e.g., 21)
- **Channel numbers** can be discovered using the **SDP** protocol and a channel UUID
- **Channel UUIDs** for our protocol are vendor specific



Tool Time



- We built a tool that implements the Airoha protocol via RFCOMM.
- We feel most comfortable in Python, so we built it using Google's Bumble library.

ERNW
providing security.

Wait a minute, ...

- Bumble is a fully featured Bluetooth stack written in Python.
- Its entirely separated from your Host OS' Bluetooth stack.
- We never paired Bumble with the headphones.
- **Why the hell does this still work?**

ERNW
providing security.

OMG!

- Pairing is broken
- Anyone in Bluetooth range can dump our headphone's flash.
- Anyone in Bluetooth range can connect to our headphones!

ERNW
providing security.

Bluetooth Classic Caveats

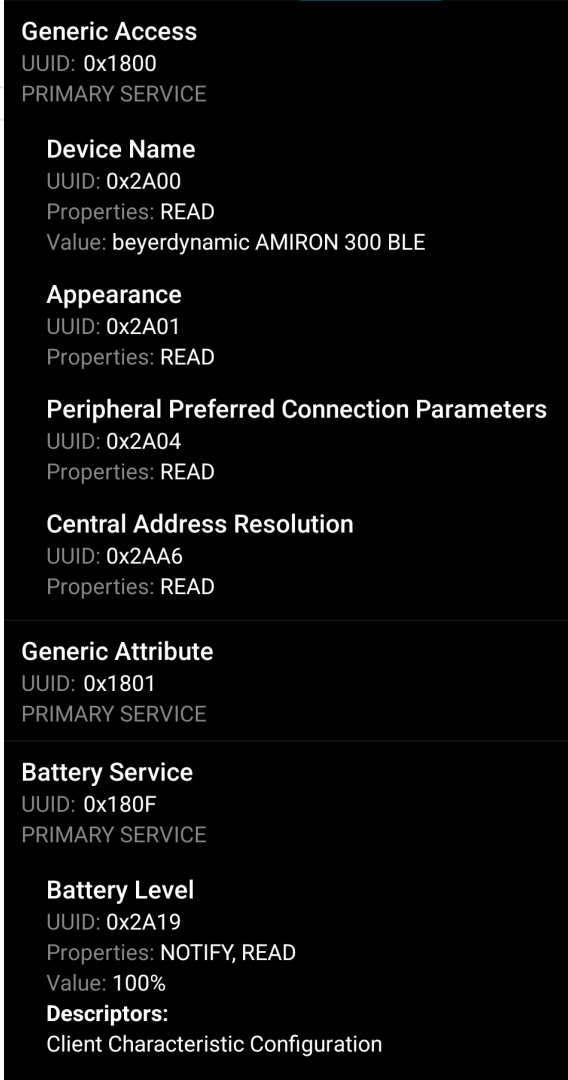
- To establish a Bluetooth Classic (BR/EDR) connection we typically need to know the device's address.
  - Address can be "discovered" with sniffing devices for ~$100 (Ubertooth One).
- Many devices will only accept one connection at a time.

→ We have to find the address and audio will drop when we attack.

ERNW
providing security.

The other kind of Bluetooth: BLE

- BLE devices can (and often do) send advertisements.
- This means we can scan for them and don't need to know their address to connect.
- Most BLE devices primarily use the **GATT** protocol.
- Modern headphones use it for discovery and status info (e.g., Battery Level).

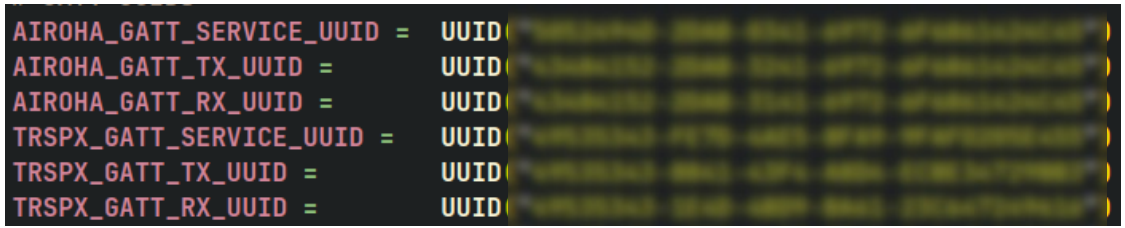


So, can we dump flash via BLE, too?

OMG yes, we can!
😱

Bluetooth Low Energy as Transport

- **Our Protocol** is built on GATT.
- **GATT** has services.
- **Services** have characteristics.
- **Characteristics** can be read from, written and subscribed to
- **Services & Characteristics** can be discovered and have UUIDs.
- **UUIDs** for our protocol are sometimes vendor specific.



ERNW
providing security.

Wait a minute, ...

- We didn't have to pair here either!
- We can discover headphones via BLE advertisements.
- We just read and write to GATT characteristics to use our protocol.

Recap

- We know the protocol is available sans-auth via ***BLE*** and ***Bluetooth Classic***.
- We can scan for vulnerable devices.
- We can use it to dump flash.

What else can it do?

ERNW
providing security.

Things we know the protocol can do:

- Read RAM (Command to read bytewise from any virtual address).
- Read/Write flash
- FOTA (Firmware Over the Air?) operations
- Get Bluetooth Link Keys
- Get Bluetooth Address
- Read out build version
- … a ton of other stuff, some of which we didn‘t try yet

ERNW
providing security.

This bad. But how bad exactly?

ERNW
providing security.

Bluetooth live demos? 😱

Live Demos!

ERNW
providing security.

Run code

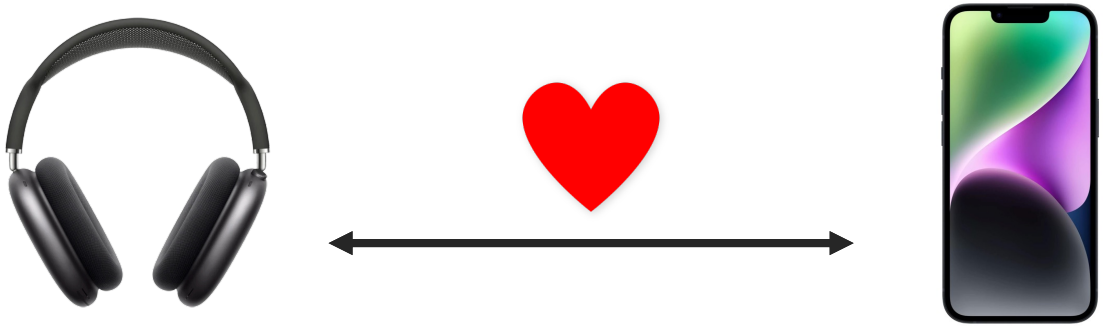
Eavesdrop

Extract data

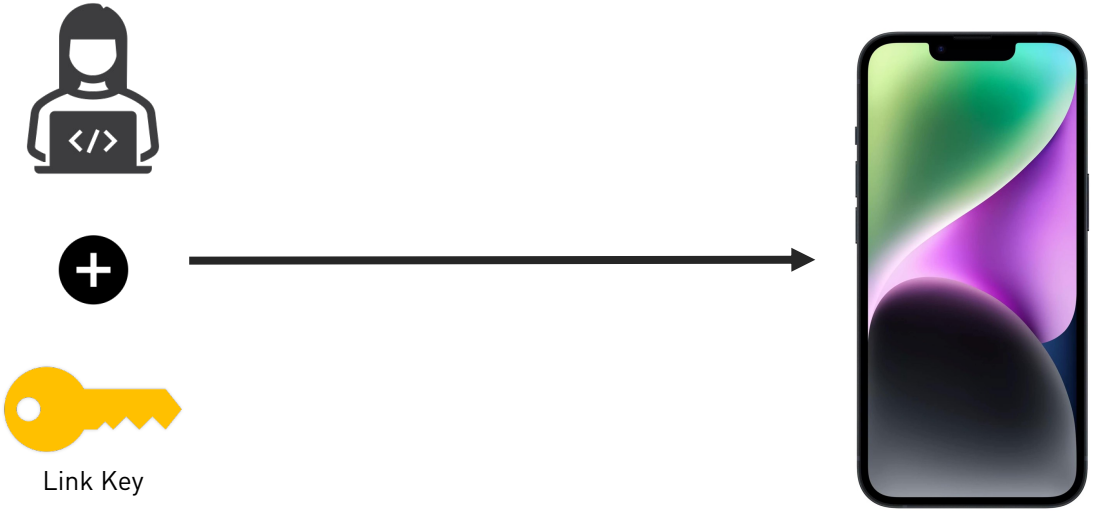
Get Link Key

ERNW
providing security.

Remember that?



Becoming the Headphones



Hands Free Profile (HFP)

- **Call Control**
  - Answer, reject, end calls
  - Dial a number (including redialing the last number)
- **Audio Routing**
  - Transfer audio between phone and hands-free device
- **Caller Information Access**
  - Read caller ID
  - Access signal strength, battery level
- **Network Information**
  - Query carrier/operator name
  - Subscriber Number (local phone number)
- **Voice Assistant**
  - Trigger Voice Assistant (Gemini/Google Assistant/Siri)
- **Phone Book Access**
  - Non-standard AT commands for phonebook access

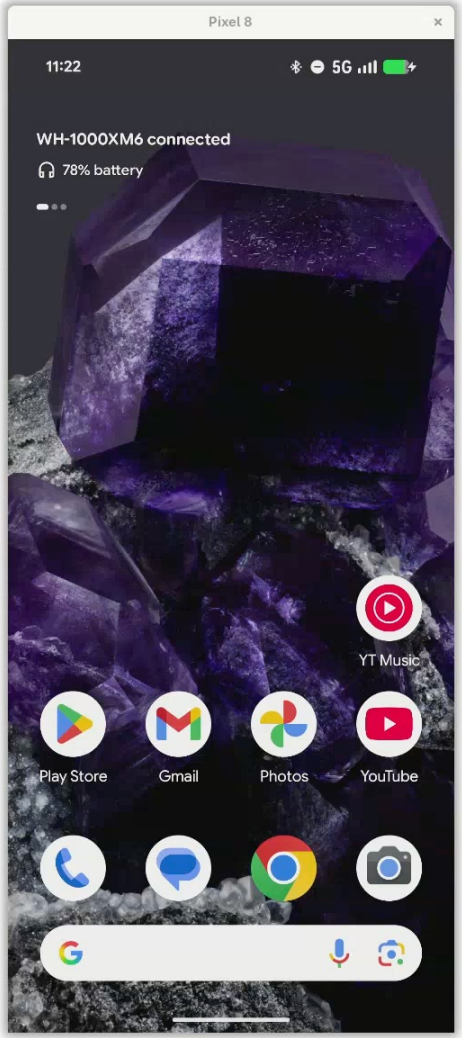
This depends on a per Headphone Setting in Android.

Also, there is a whole Bluetooth profile for phone book access (**PBAP**). That's better suited to the task.

ERNW
providing security.

Demo Video

```
✘ frieder@fswork-ng  RACE/airoha-race
```



CVEs

CVE-2025-20700:
Missing authentication for GATT service.

CVE-2025-20701:
Missing authentication (pairing) for Bluetooth Classic.

CVE-2025-20702:
Critical capabilities of custom protocol.

Airoha has registered these CVEs but has not published them yet.

No

No

No

These devices do not have an Airoha Bluetooth chip!

No

No

No

No

Airoha & Affected Devices

→ We can search for other devices with Airoha Bluetooth chips.

Search the internet

ERNW
providing security.

52audio.com

For extremely detailed teardowns and awesome pictures!

拆解报告：beyerdynamic拜雅AMIRON 300真无线降噪耳机

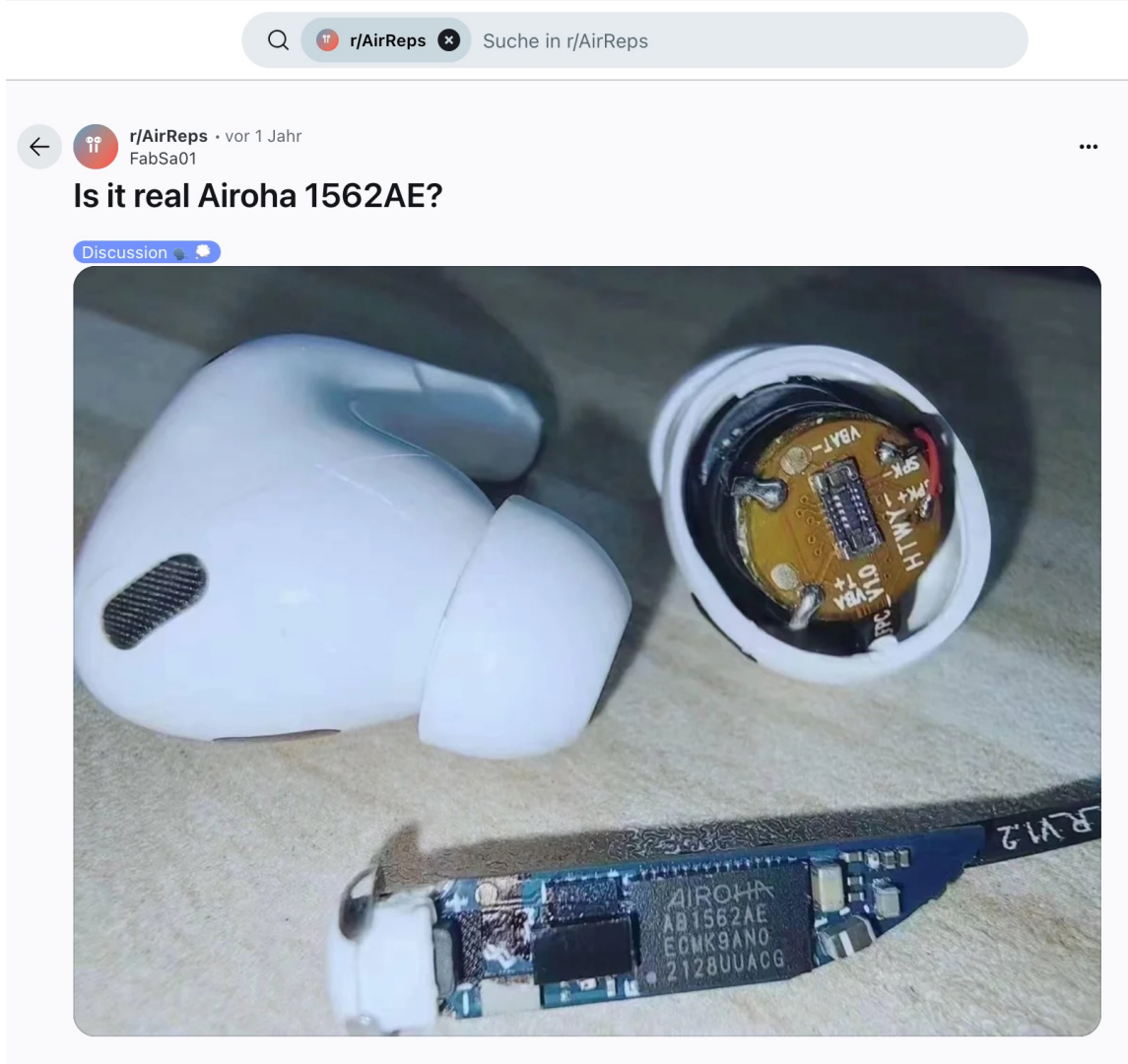
Wen5
11 2 月, 2025 • TWS蓝牙耳机

beyerdynamic拜雅是一个诞生于1924年的国际知名音频品牌，在2024年的一百周年之际，拜雅举办了「未来之声 · FUTURE PRISTINE SOUND」新品发布会，推出了AMIRON 100（阿米罗100）、AMIRON 300（阿米罗300）和AVENTHO 300 （阿凡途 300）三款新品，均继承了标志性的拜亚音质，同时采用不同的设计理念，以适应不同场景使用需求。

ERNW
providing security.

AirPods replicas

There is an active community around Airoha-based AirPods replicas.



ERNW
providing security.

There are a ton of potentially vulnerable devices.

ERNW
providing security.

There are a ton* of potentially vulnerable devices.

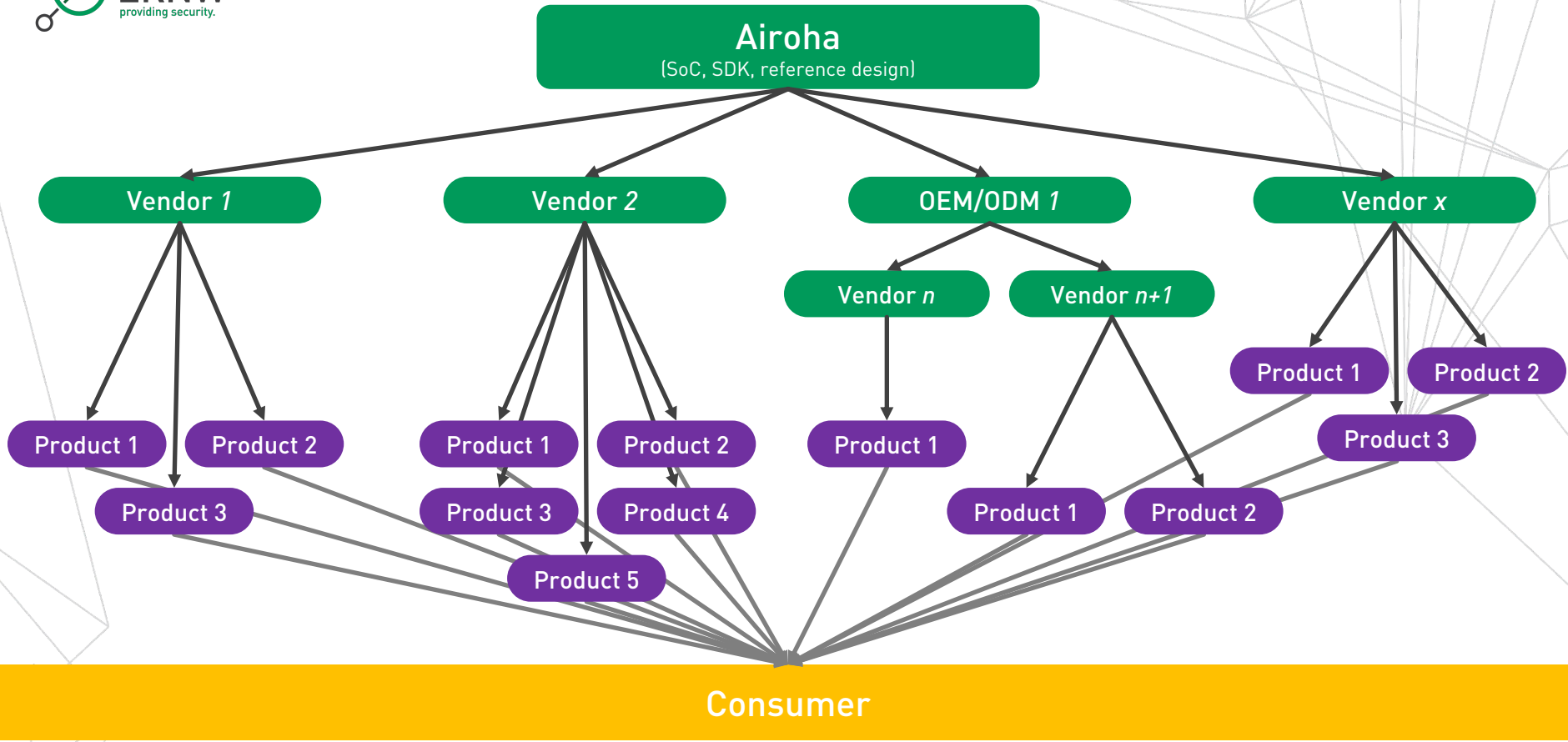
* We estimate the number to be > 100 different device models

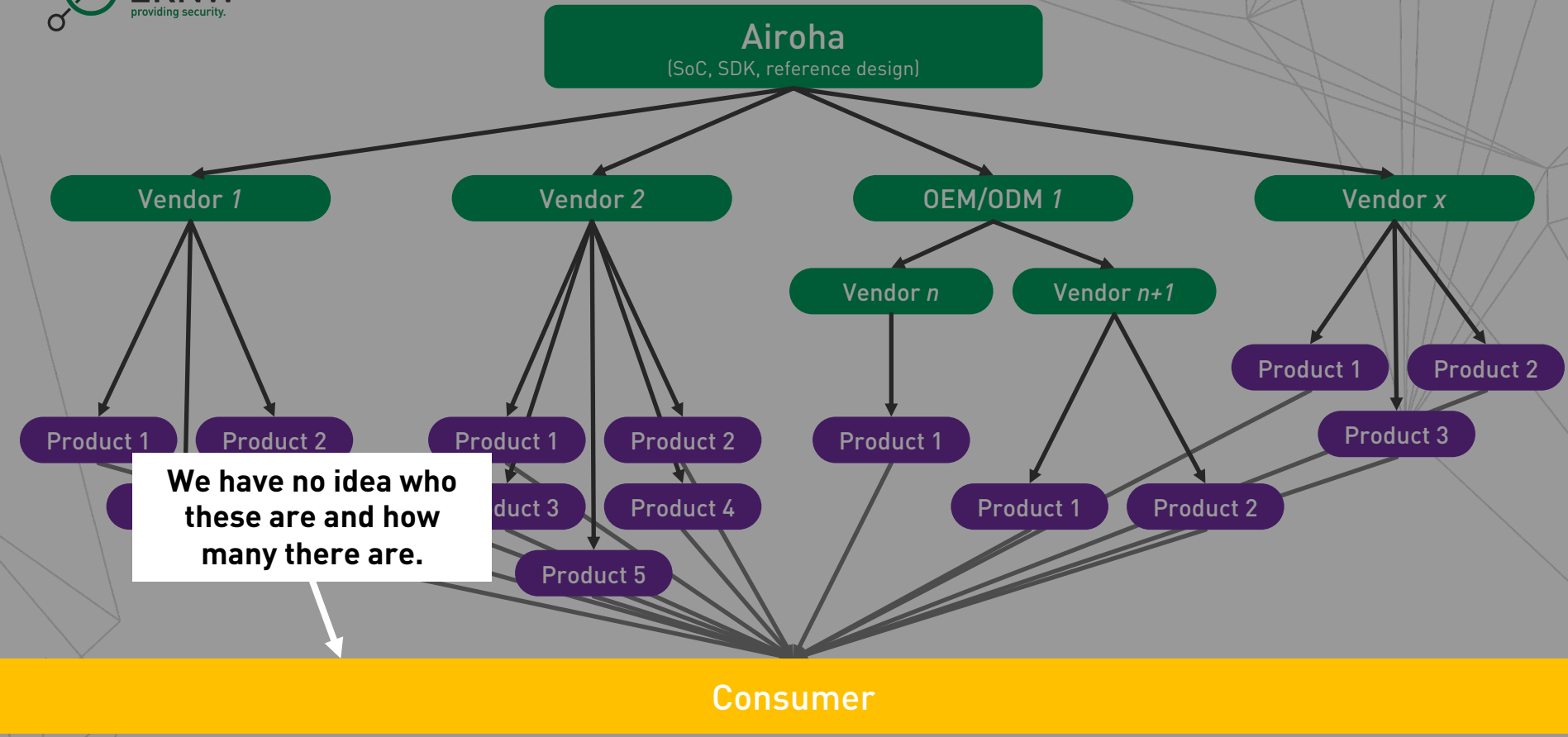
ERNW
providing security.

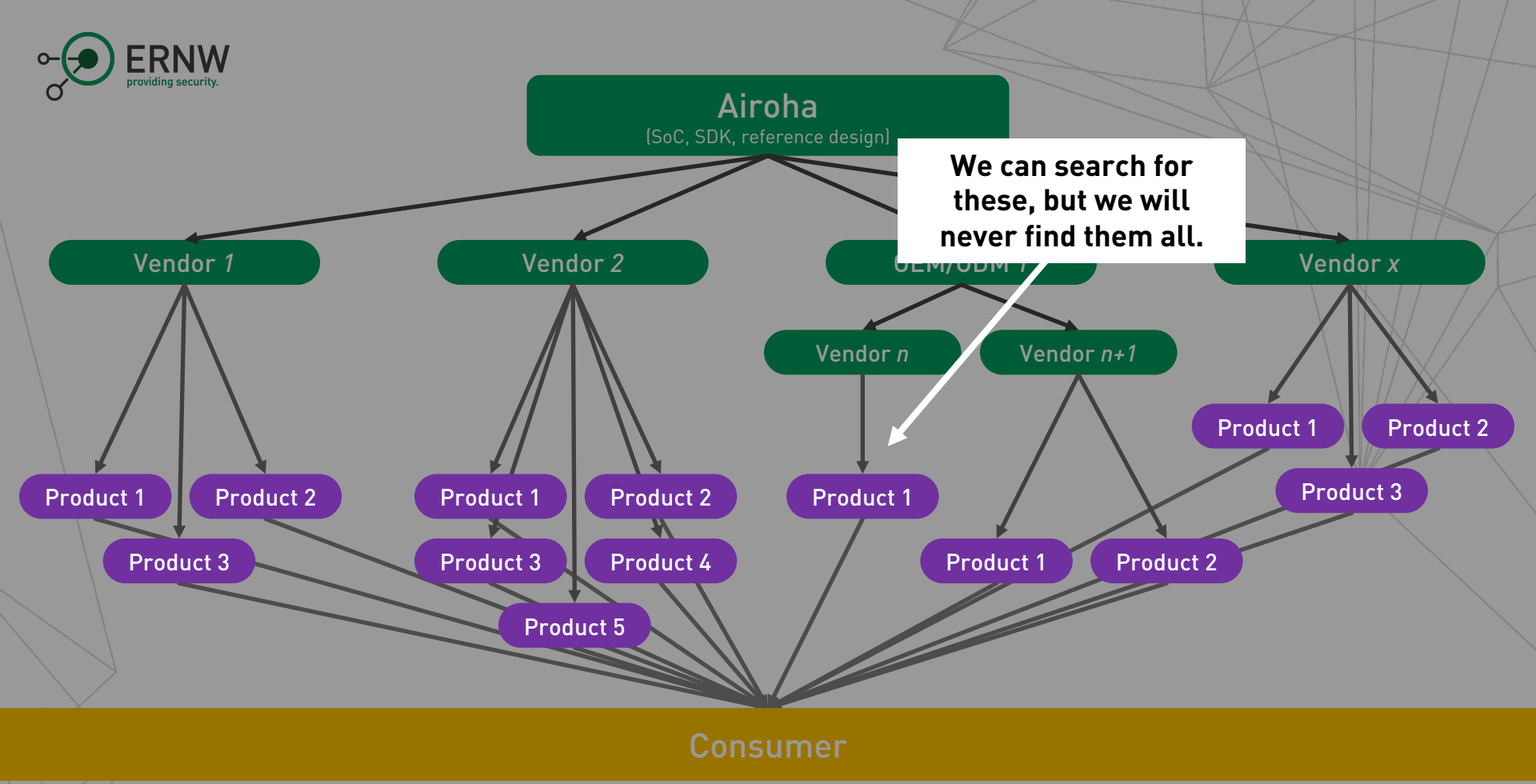
But we could only verify a subset of these.

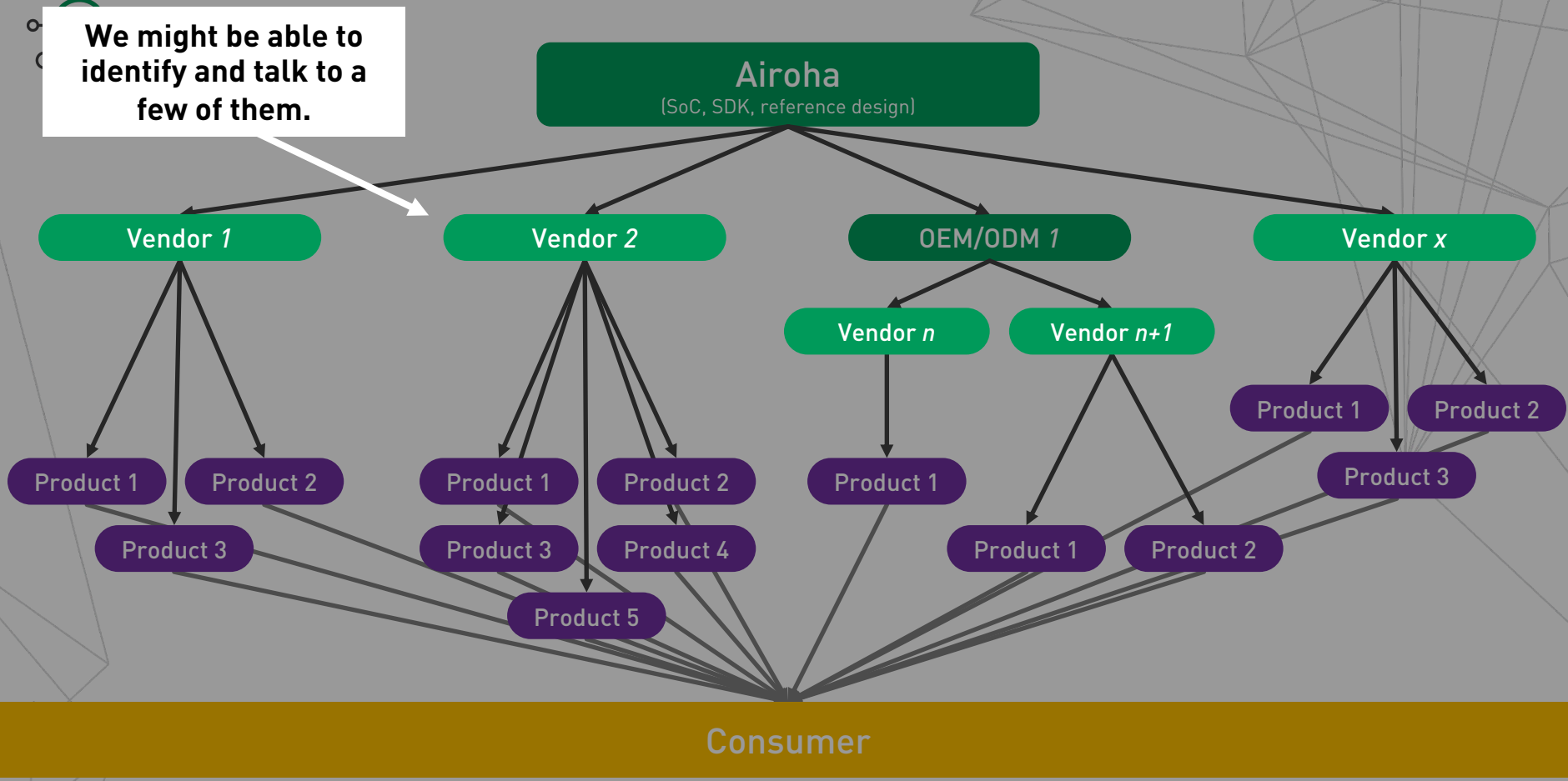
ERNW
providing security.

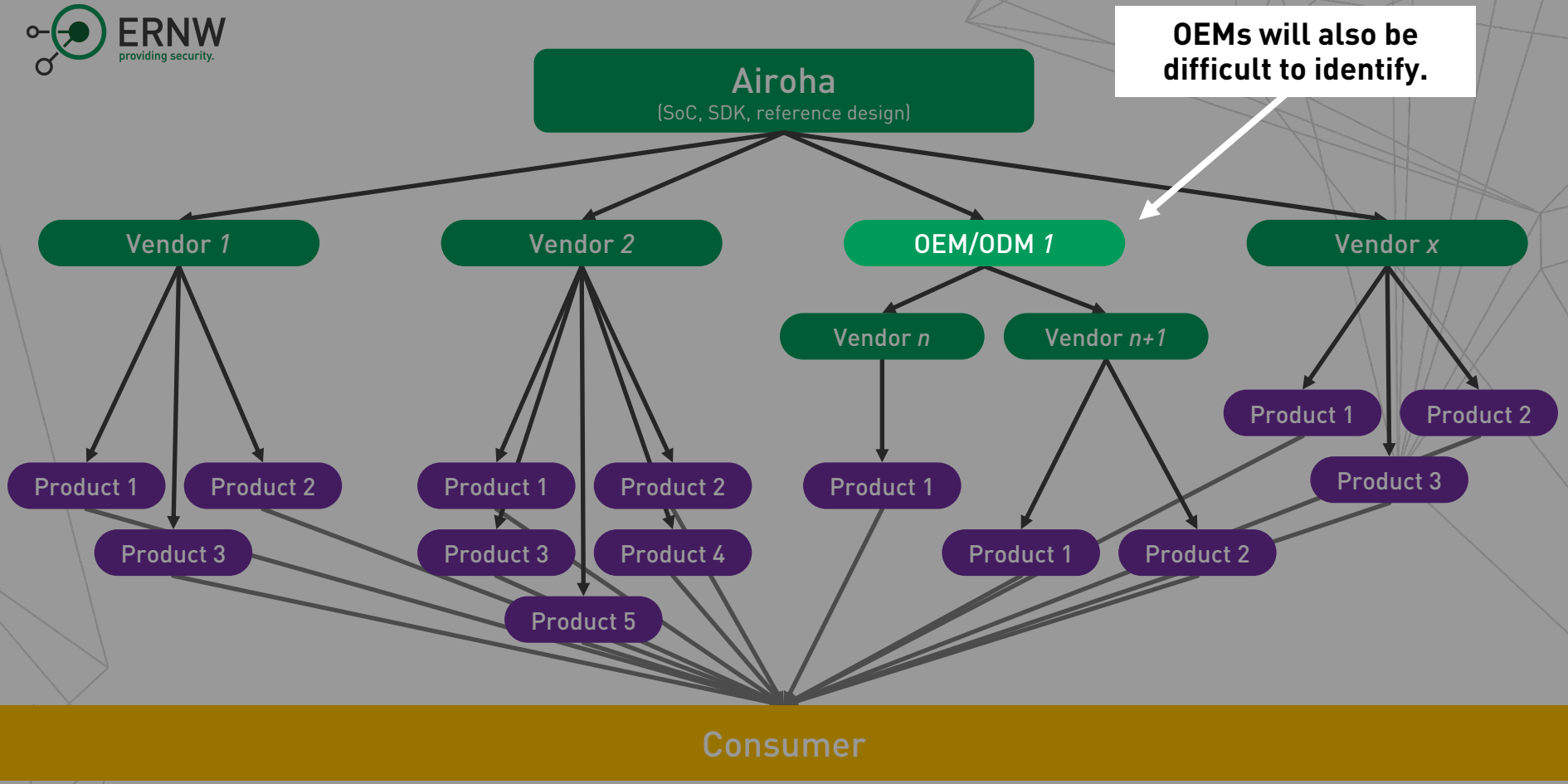
Disclosure


Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 1
Product 2
Product 3
Product 4
Product 5
Product 1
Product 1
Product 2
Product 1
Product 2
Product 3
Consumer


Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 4
Product 5
We have no idea who these are and how many there are.
Consumer

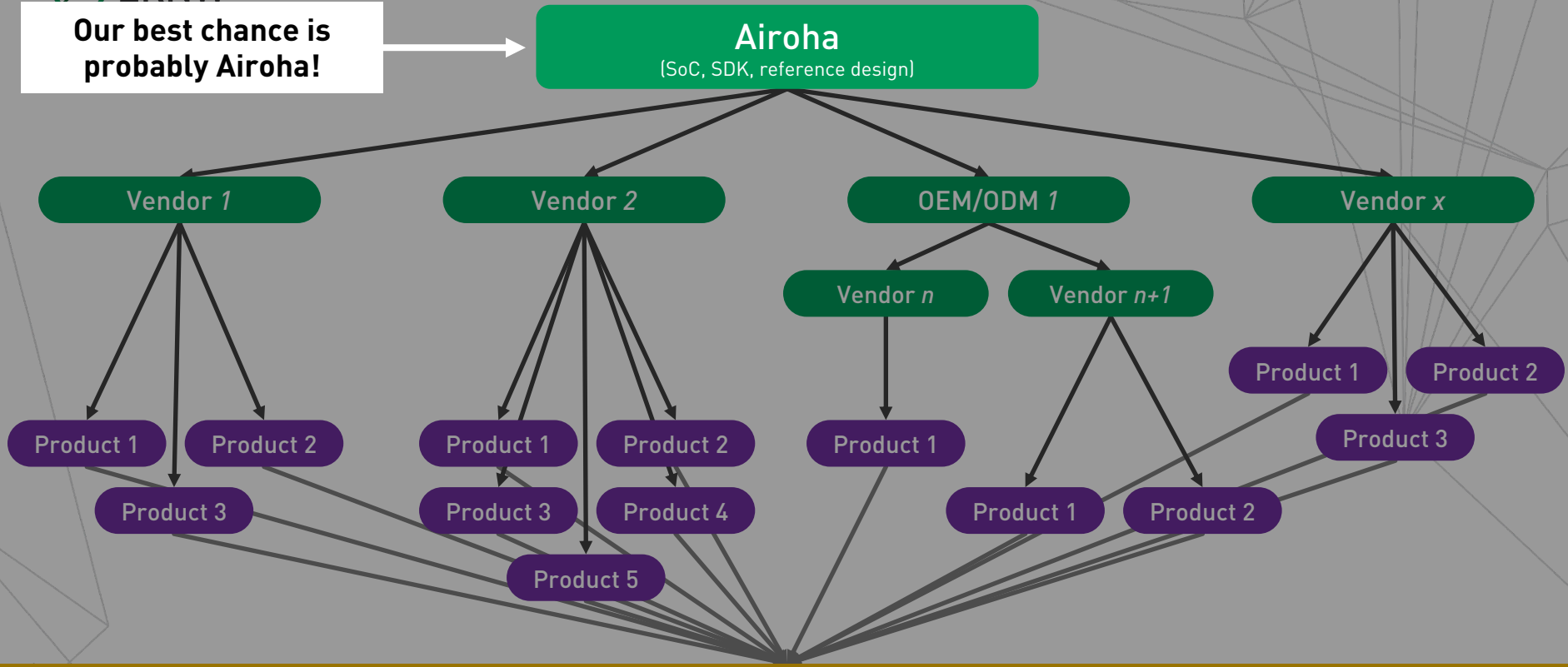

ERNW
providing security.
Airoha
(SoC, SDK, reference design)
We can search for these, but we will never find them all.
Vendor 1
Vendor 2
Vendor n
Vendor n+1
Vendor x
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer

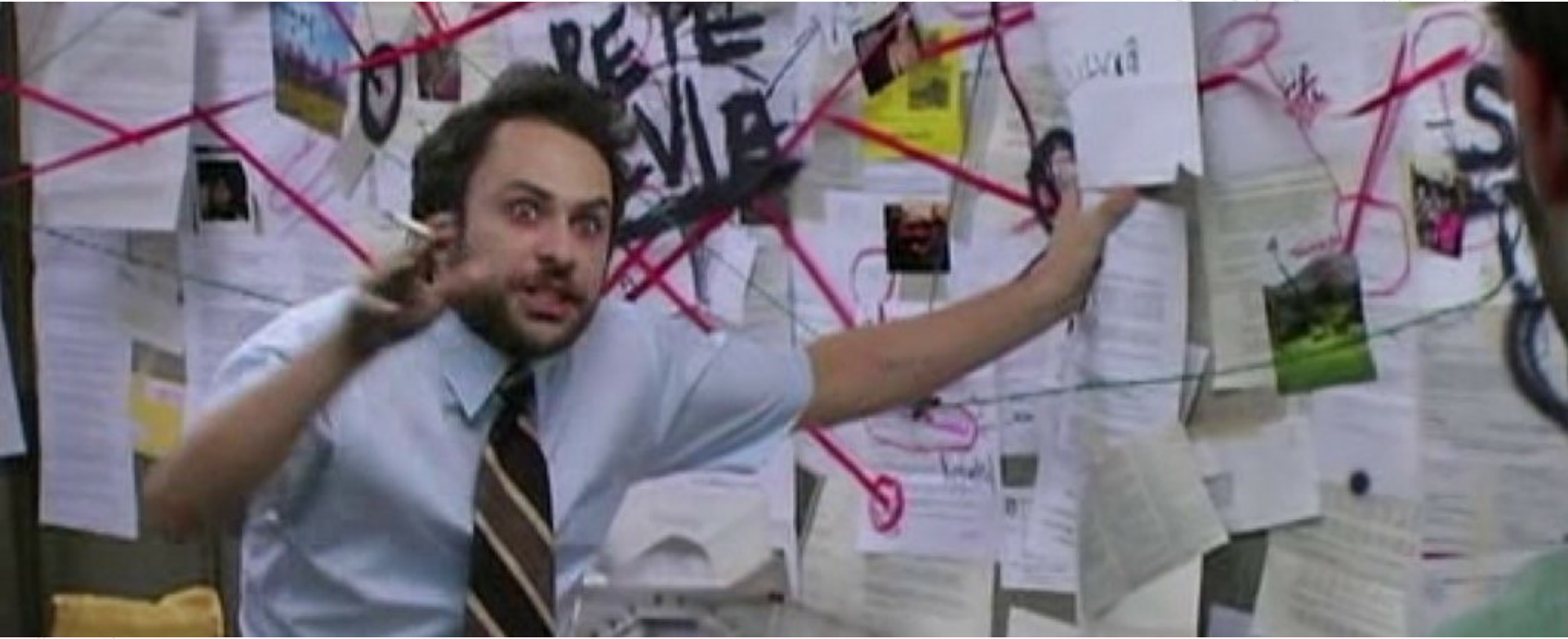

We might be able to identify and talk to a few of them.
Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer


ERNW
providing security.
OEMs will also be difficult to identify.
Airoha
(SoC, SDK, reference design)
Vendor 1
Vendor 2
OEM/ODM 1
Vendor x
Vendor n
Vendor n+1
Product 1
Product 2
Product 3
Product 4
Product 5
Consumer

ERNW

Our best chance is probably Airoha!





ERNW
providing security.

Airoha's security disclosure page looks really good!

AIROHA

What You Can Expect From Us

- We aim to respond within a maximum of 3 to 5 business days upon receiving the initial report. If you do not hear back from us after a week you submitted the initial report, please send it to us again.
- We will make best effort to address the security vulnerabilities by including but not limited to releasing patches to our OEM partners within 90 days and communicate with the stakeholders as needed.

- **Can I use the encrypted channel to submit a security report?**

Yes, please use our PGP Public Key to send the encrypted security report to security@airoha.com.

Disclosure Timeline: Short Version

March 25th

ERNW contacts Airoha with technical writeup of vulnerabilities and list of currently known vulnerable devices.

April 24th

After several different communication attempts ERNW tells Airoha it will contact some of the vendors about the issue.

ERNW contacts three vendors of whom only one responds.

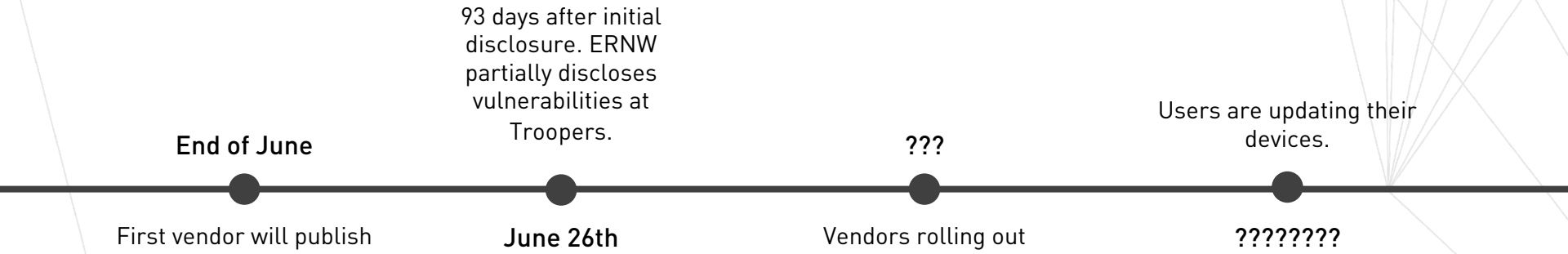
May 27th

Airoha's first response to ERNW. Communication and exchange between ERNW starts. Airoha is committed to fix issues with priority.

June 4th

Airoha supplies device manufacturers with an SDK update with mitigations. Manufacturers start developing and shipping patches for their products.

Disclosure Timeline: Short Version



ERNW
providing security.

Okay, come on, finally tell us the vulnerable devices!

ERNW
providing security.

These are the devices we saw and were able to confirm

Bose

- Quiet Comfort Earbuds[1]

MoerLabs

- EchoBeatz

Jabra

- Elite 8 Active[1,3]

Jlab

- Epic Air Sport ANC

JBL

- Live Buds 3
- Endurance Race 2

Beyerdynamic

- Amiron 300

Teufel

- Airy TWS 2

Sony

- WH-1000XM6[2]
- WF-1000XM3
- WF-1000XM5
- CH-720N
- WH-1000XM5[2,3]
- WF-1000XM4
- WH-1000XM4[2,3]
- WH-XB910N
- WI-C100
- WH-CH520
- ULT Wear
- WF-C510-GFP
- WF-C500
- Link Buds S

Marshall

- WOBURN III
- STANMORE III
- ACTON III
- MAJOR V
- MINOR IV
- MOTIF II

Things we noticed (not exhaustive):

1: No BLE (GATT)
2: Some protocol messages are filtered
3: No Classic pairing vuln

ERNW
providing security.

What now?

ERNW
providing security.

Patching & Disclosure

- Further technical details in a few weeks.
- Firmware updates?

Vendors & Security

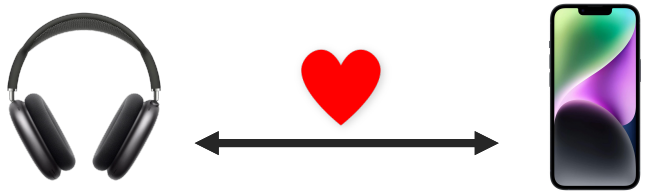
- Pentest your devices before you sell them for $500.
- Make sure you receive disclosure mails.
- Offer security contacts in addition to bug bounty platforms.

Users

- Update your headphones!
- Maybe use cable headphones if you feel like you might be a target.
- Remove old Bluetooth pairings.

Closing Thoughts

- As smart phones are getting more secure, peripherals become more interesting.
- HID devices got some scrutiny already.
- Smart Watches? See Nils' talk from yesterday.
- Even physical compromise may be worth the effort (remember USB HID?)



Security Advisory Blog Post

- More details will follow in a blog post and white paper in a few weeks.
- There will be a more technical version of this talk in the future.
- We will release information on how to check whether your own devices are affected.
- If you're developing headphones and are unsure whether you are affected talk to us.

fsteinmetz@ernw.de
dheinze@ernw.de

twillnix@infosec.exchange
ttdennis@chaos.social

www.insinuator.net