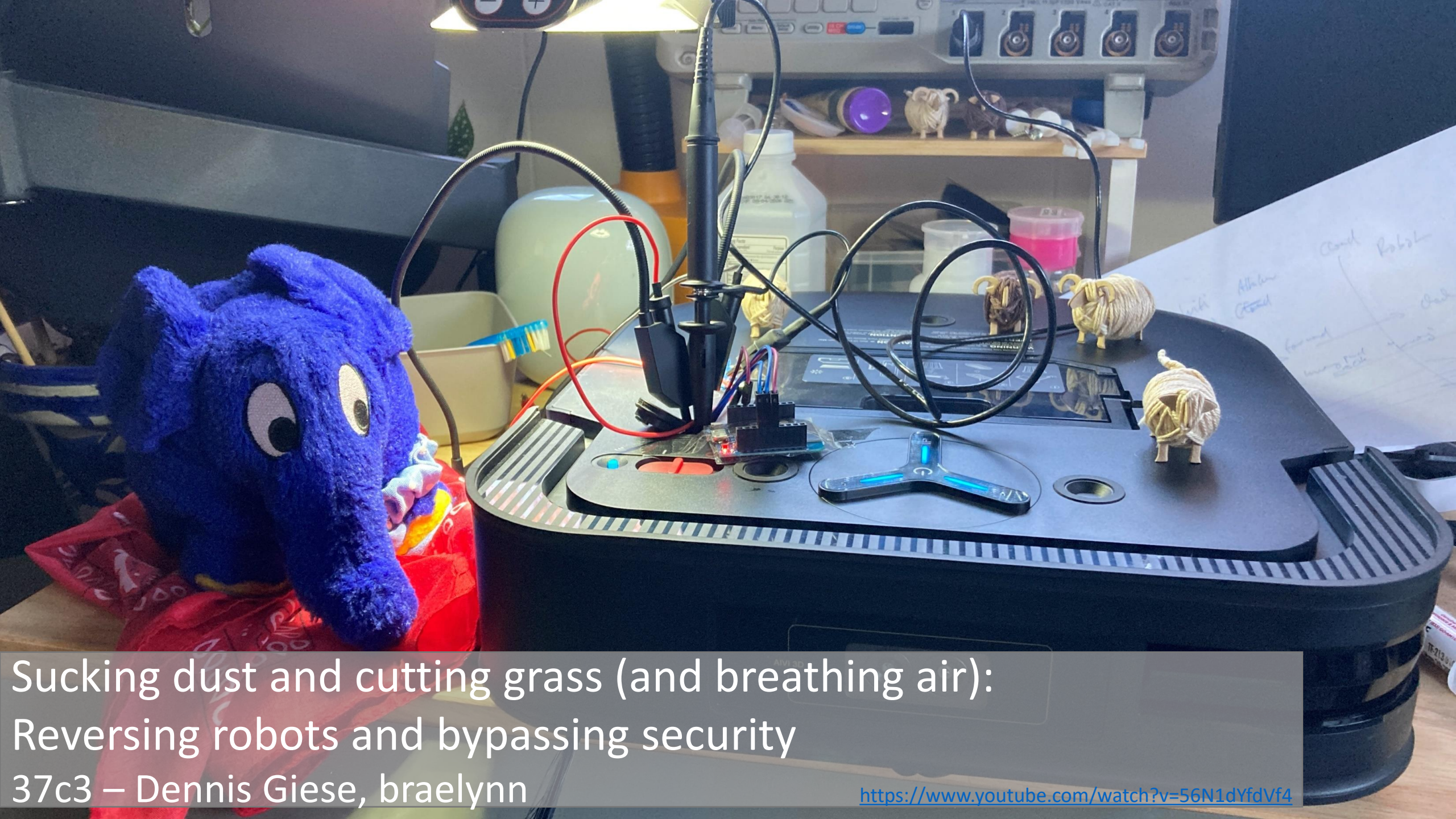


Sucking dust and cutting grass (and breathing air): Reversing robots and bypassing security

37c3 – Dennis Giese, braelynn

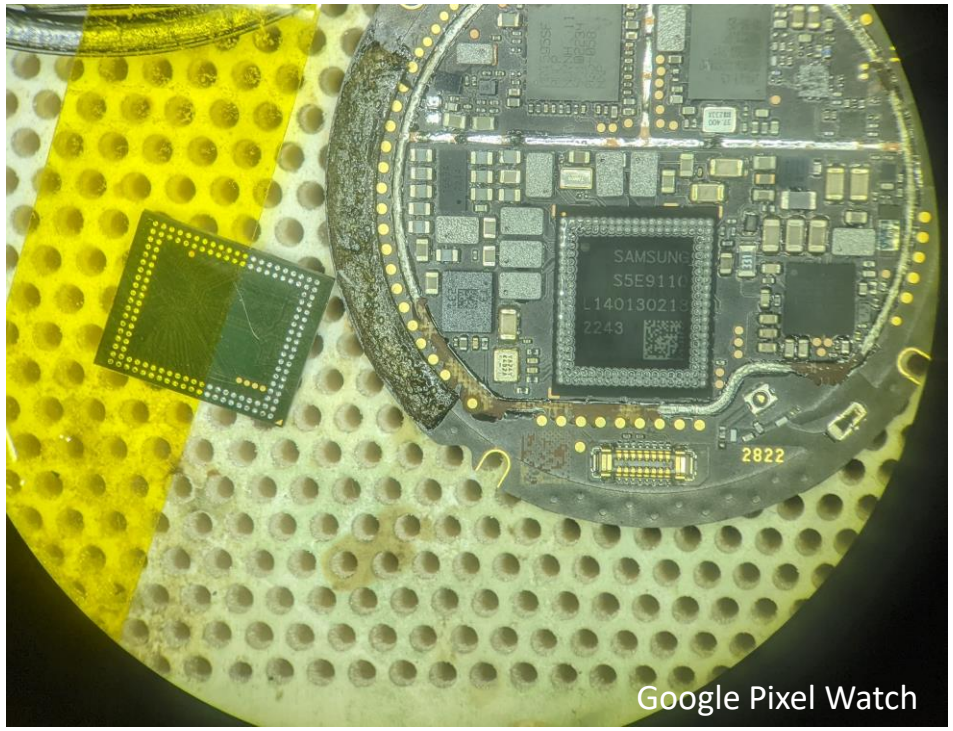
https://www.youtube.com/watch?v=56N1dYfdVf4

About Dennis

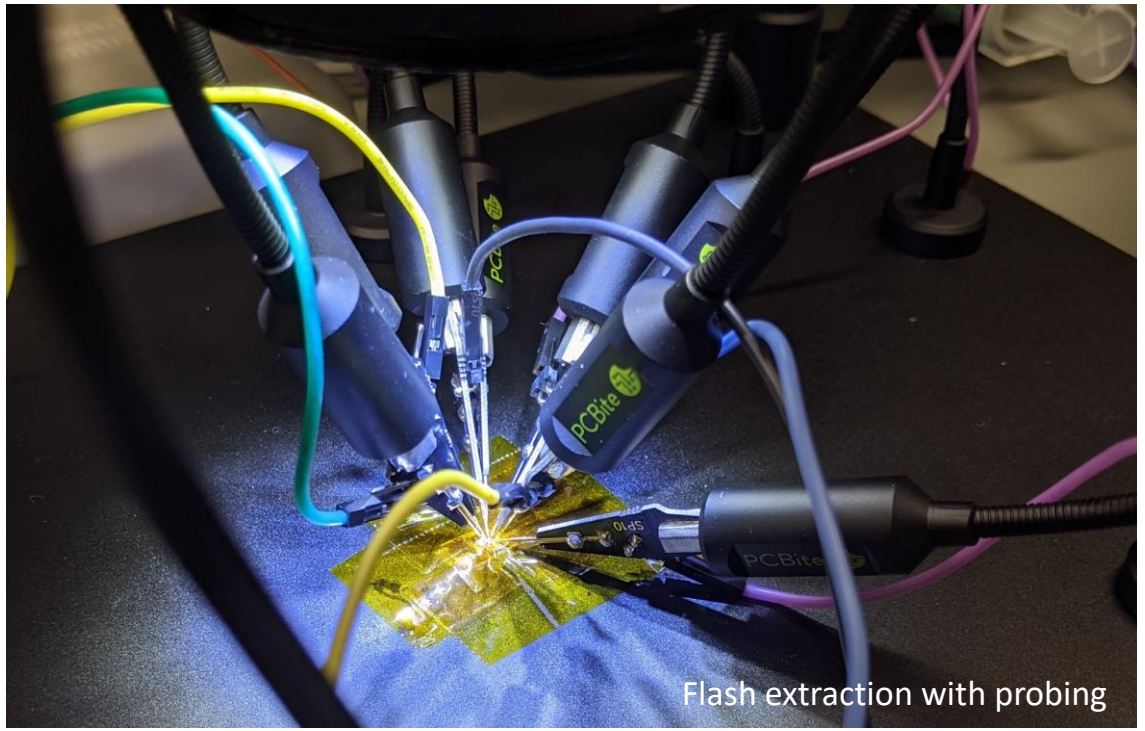
- “Security Researcher” aka Hardware Hacker
  - Research field: Wireless and embedded Security&Privacy
- Vacuum Robot (and IoT) collector
  - All brands: iRobot, Roborock, Dreame, Xiaomi, Shark, Narwal, Ecovacs, …
- Interests: Reverse engineering of interesting devices
  - Current research: Robots, Smart Speakers, Flash memory

Dennis's Projects

- Flash reverse-engineering and forensics
  - Analysis of embedded devices and flash memory itself
  - Example: Amazon Echo Dot (2021)



Google Pixel Watch



Flash extraction with probing

https://dl.acm.org/doi/10.1145/3448300.3467820

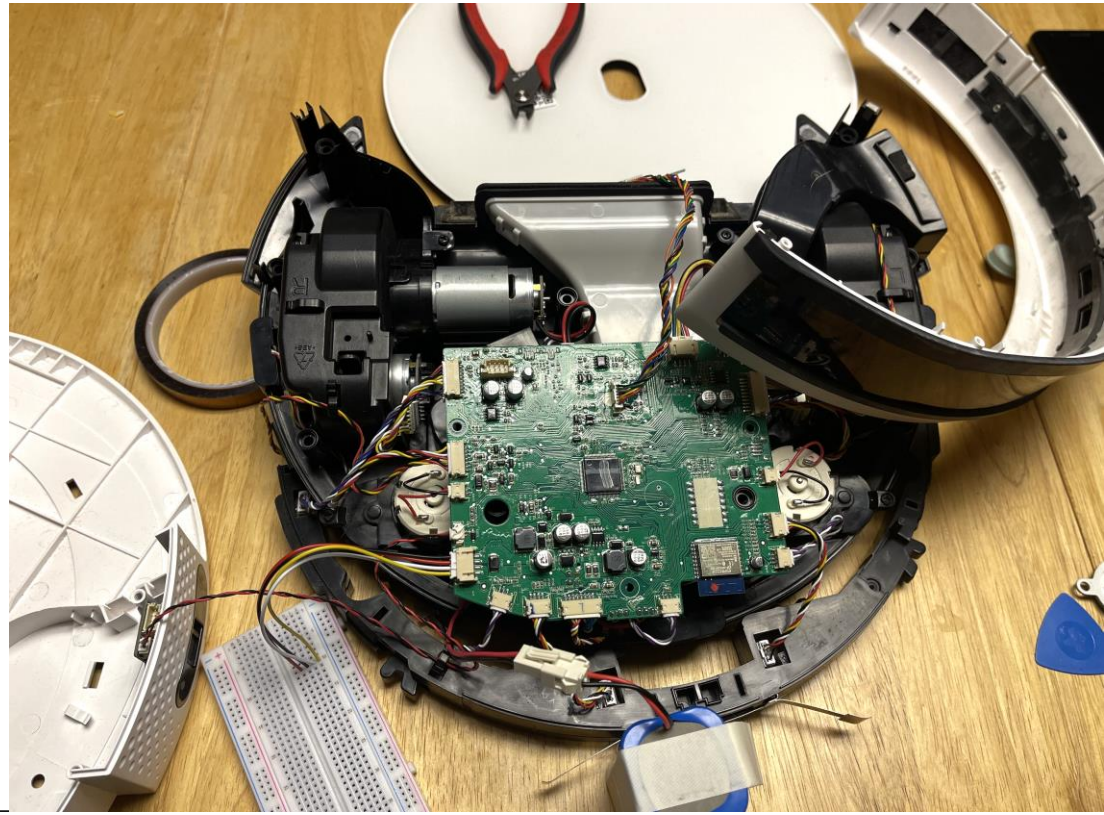
Dennis's Projects

Robotinfo.dev

- Systematic analysis of robots
  - Hardware, Software
  - Sensors
- Focus: security and privacy
- Tracking of firmware changes
- Source: emulated devices, app
- Base for further research

About braelynn

- Hacks things for Leviathan Security Group
  - (this talk is entirely personal research and does not reflect their views ;))
- Focus: Application Security and APIs
- Started robot hacking during COVID
- Now: Hardware hacking for fun
  - Robots, Cameras



Goals of this talk

- Understand Security & Privacy risks of IoT devices
- Get an overview of vacuum robot hacking
- Learn about vulnerabilities and how to find them
- Ultimate goal: get root access without disassembly

- Xiaomi (2017,2018)
- Roborock (2018, 2021, 2023)
- Dreame (2021, 2023)
- Narwal and others (2023)
- ?

- Xiaomi (2017,2018)
- Roborock (2018, 2021, 2023)
- Dreame (2021, 2023)
- Narwal and others (2023)
- Ecovacs

Disclaimers

- We do not claim that any vendors use sensors to spy on you!
  - (but they can in theory)
- We cover primarily physical attacks (or proximity attacks) on devices
- Many vendors are affected
  - Independent of origin, size, market share
  - Previous talks: Xiaomi, Roborock, Dreame
  - This talk: Ecovacs
- Research part of private projects
  - No sponsorship by companies or organizations
  - Any statements are private and not representing any organization

Devices covered in this Talk

- Ecovacs DEEBOT 900 Series
- Ecovacs DEEBOT N8/T8 *
- Ecovacs DEEBOT N9/T9 *
- Ecovacs DEEBOT N10/T10
- *Ecovacs DEEBOT X1 **
- Ecovacs DEEBOT T20 *
- *Ecovacs DEEBOT X2 **
- Ecovacs Goat G1
- *Ecovacs ~~Spybot~~ Airbot Z1*
- Ecovacs Airbot AVA
- Ecovacs Airbot ANDY
- Yeedi *

We will only focus on devices that run Linux.

Device with Cameras
Device with Microphone / "Hi YIKO"
* = wildcard

About this talk

- Result of 5 years of research and experiments
- Not the first ones researching Ecovacs robots
  - Prior work of others has different focus
- Work is not finished (yet)
- The vendor has been unaware of our findings until today

  … but they may have noticed some of our activities

  … expect updates coming soon

Collaborative effort

@tihmstar and Dennis hacking Robot cameras at NULLCON Goa 2023

Lawnmower hacking at CCC Camp 2023 in the ZTL/N.O.R.T.x village with Dennis, Maurice, Axel L., Micha B., Mona, Antre (no picture, because forgot to make one :/)

https://nullcon.net/
https://events.ccc.de/camp/2023/hub/camp23/en/assembly/nort/

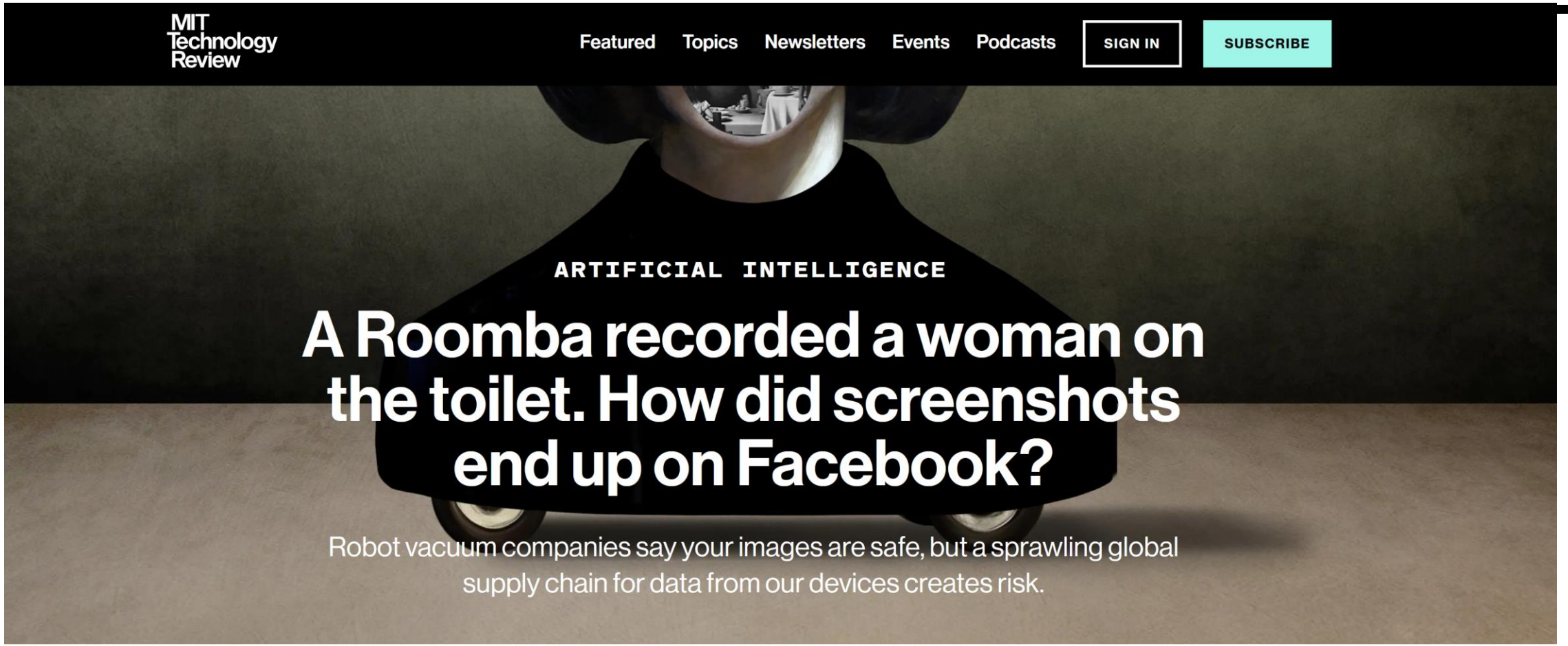
MOTIVATION

Why do we want to root devices?

- Play with cool hardware
- Stop devices from constantly phoning home
- Use custom Smart Home Software
- Diagnosis of broken devices
- Verification of privacy claims

Why do we not trust IoT?

- Devices are connected to the home network
- Communication to the cloud is encrypted, content unclear
- Developing secure hardware and software is hard
- Vendors get caught with shady behavior
- (We’ve done IoT research for a long time…)



MATTHIEU BOU

by **Eileen Guo**
December 19, 2022

In the fall of 2020, gig workers in Venezuela posted a series of images to online forums where they gathered to talk shop. The photos were mundane, if sometimes intimate, household scenes captured from low angles—including

MIT Technology Review

10 of 13

Image captured by iRobot development devices, being annotated by data labelers.

Image captured by iRobot development devices, being annotated by data labelers. The woman's face was originally visible, but was obscured by MIT Technology Review. The Roomba J7's front light is reflected on the oven.

Fun fact:
Vendors panicked and started to change firmwares, apps and privacy policies

MIT Technology Review

Your Roomba Is Also Gathering Data about the Layout of Your Home

The CEO of iRobot is pushing the company toward a broader vision of the smart home. It could soon sell maps of the interiors of people's houses.

By Michael Reilly

July 25, 2017

Bloomberg

Live Now | Markets | Economics | Industries | Tech | AI | Politics | Wealth | Pursuits | Opinion | Busi

BusinessweekTechnology

Amazon's Roomba Deal Is Really About Mapping Your Home

In buying iRobot, the e-commerce titan gets a data collection machine that comes with a vacuum.

By Alex Webb

August 6, 2022 at 12:40 AM GMT+10

Updated on August 7, 2022 at 2:22 AM GMT+10

https://www.technologyreview.com/2017/07/25/150346/your-roomba-is-also-gathering-data-about-the-layout-of-your-home/
https://www.bloomberg.com/news/articles/2022-08-05/amazon-s-irobot-deal-is-about-roomba-s-data-collection#xj4y7vzkg

More sensors?

Cameras

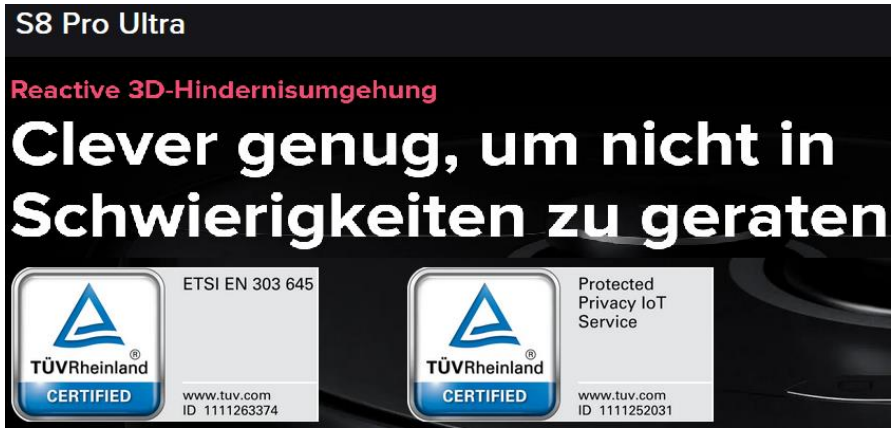
Microphones??

https://www.ecovacs.com/us/deebot-robotic-vacuum-cleaner/DEEBOT-X1-OMNI-BLACK

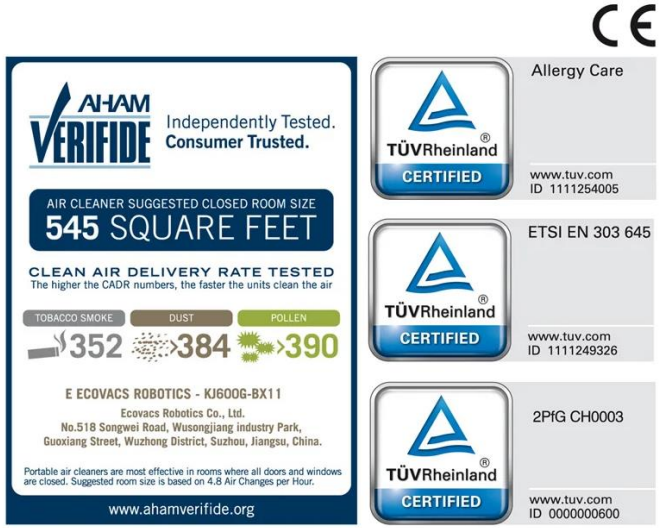
Risks of devices with cameras

- Devices might store pictures indefinitely … and some do. both cloud and local
- Used devices might be problematic
  - Previous owner installed rootkit
  - New owner cannot verify software
  - Result: Device might behave maliciously on your network
- Rooting is the only way to verify that a device is „clean“

Can you rely on Certifications?



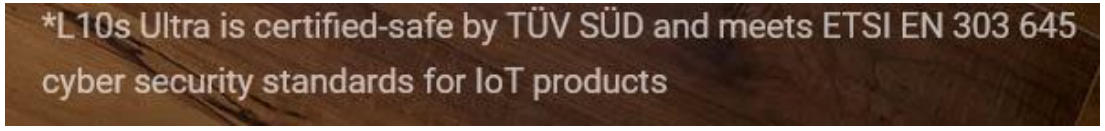
Source: https://de.roborock.com/pages/roborock-s8-pro-ultra



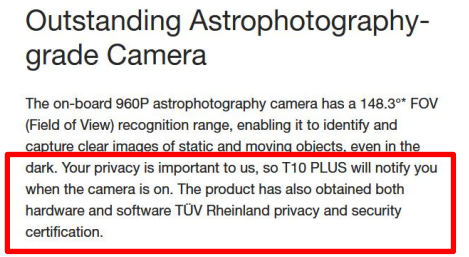
Source: https://www.ecovacs.com/global/airbot-air-purifier-robot/airbot-z1

Source: https://www.mi.com/global/product/xiaomi-robot-vacuum-x10-plus/

Source: Ecovacs iOS application loading screen



Source: https://www.dreametech.com/products/dreamebot-l10s-ultra



Source: https://www.ecovacs.com/global/deebot-robotic-vacuum-cleaner/deebot-t10-plus

ROBOT HACKING FROM 2017 TILL TODAY

First work in 2017

- Work together with Daniel Wegemer
- Xiaomi Vacuum Robot / Roborock S5
- Findings:
  - Firmware images: unsigned and encrypted with weak key
  - Custom firmware could be pushed from local network
- Result:
  - Rooting without disassembly
  - Beginning of custom Software and Voice packages
- Publication: 34C3 (2017) and DEF CON 26 (2018)

Quickly fixed by manufacturer after publication. Introduction of signatures and other countermeasures.

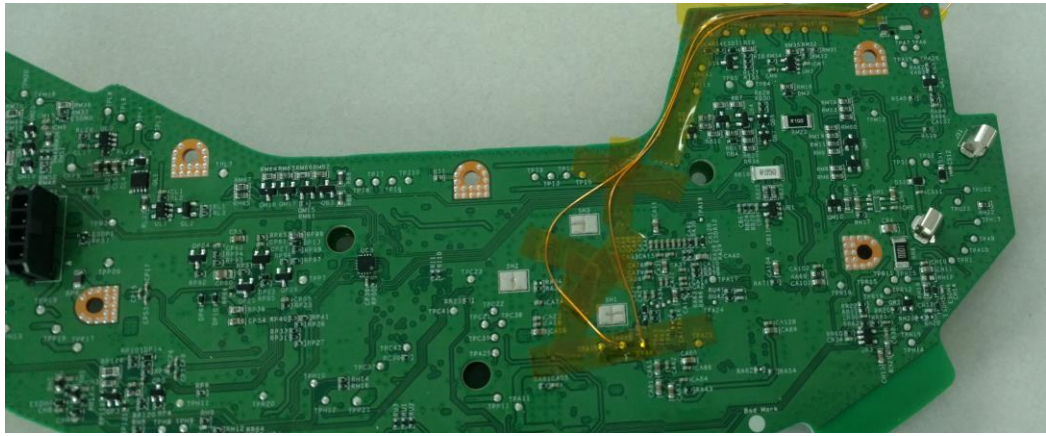
First look at Ecovacs (2018)

- After CCC talk in 2017:
  - Ecovacs Deebot 900 from an influencer
  - early firmware with debug symbols
- Findings:
  - Firmware unprotected, TLS broken, no integrity protection
  - Device can be rooted by MITM by using malicious OTA
  - Problem: hardware extremely weak
- Results were never published as project was abandoned

Really bad youtube video of teardown:
https://www.youtube.com/watch?v=BrM9JJoX72g

Rooting methods for new models (2019)

- Developed for Roborock S6, S5 Max, S7 and others
- New approach:
  - push device into bootrom mode
  - Load custom tool into memory
  - patch filesystem
  - Disadvantage: requires teardown of device
- Reaction of the vendor:
  - Lockdown of bootloaders
  - Enforcing SecureBoot and binary signatures
  - Key storage in OPTEE/Trustzone



Cameras became more common in vacuum robots

Hackers fight back (2021)

- Presented at DEFCON29
- Method to bypass Roborock security features
- New Vendor: Dreame Technologies
  - Powerful devices with cameras
  - Easy rooting method without disassembly via USB
  - Not targeted before, so vendor has no countermeasures

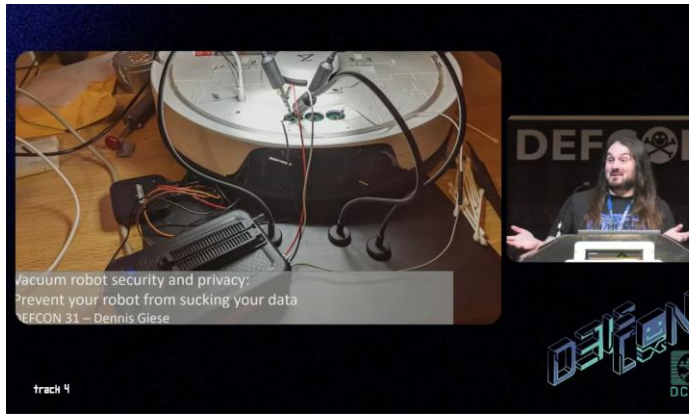
Roborock: Introduced more encryption and more sneaky countermeasures
Dreame: enforcing SecureBoot, integrity checks and a malicious tamper detection

https://dontvacuum.me/talks/DEFCON29/DEFCON29-Robots_with_lasers_and_cameras.html

Taking a look again on Ecovacs (2021)

- Ecovacs releases more powerful models
- Features very similar to competition, but with lower price
- Analyzed device: Deebot X1
  - Time to root: 30 minutes
  - Results: modified filesystem, emulation of devices
- Potential target for more rooting efforts in the future
- Independently: braelynn hacked Ecovacs and Yeedi robots

Hackers fight back again (2023)

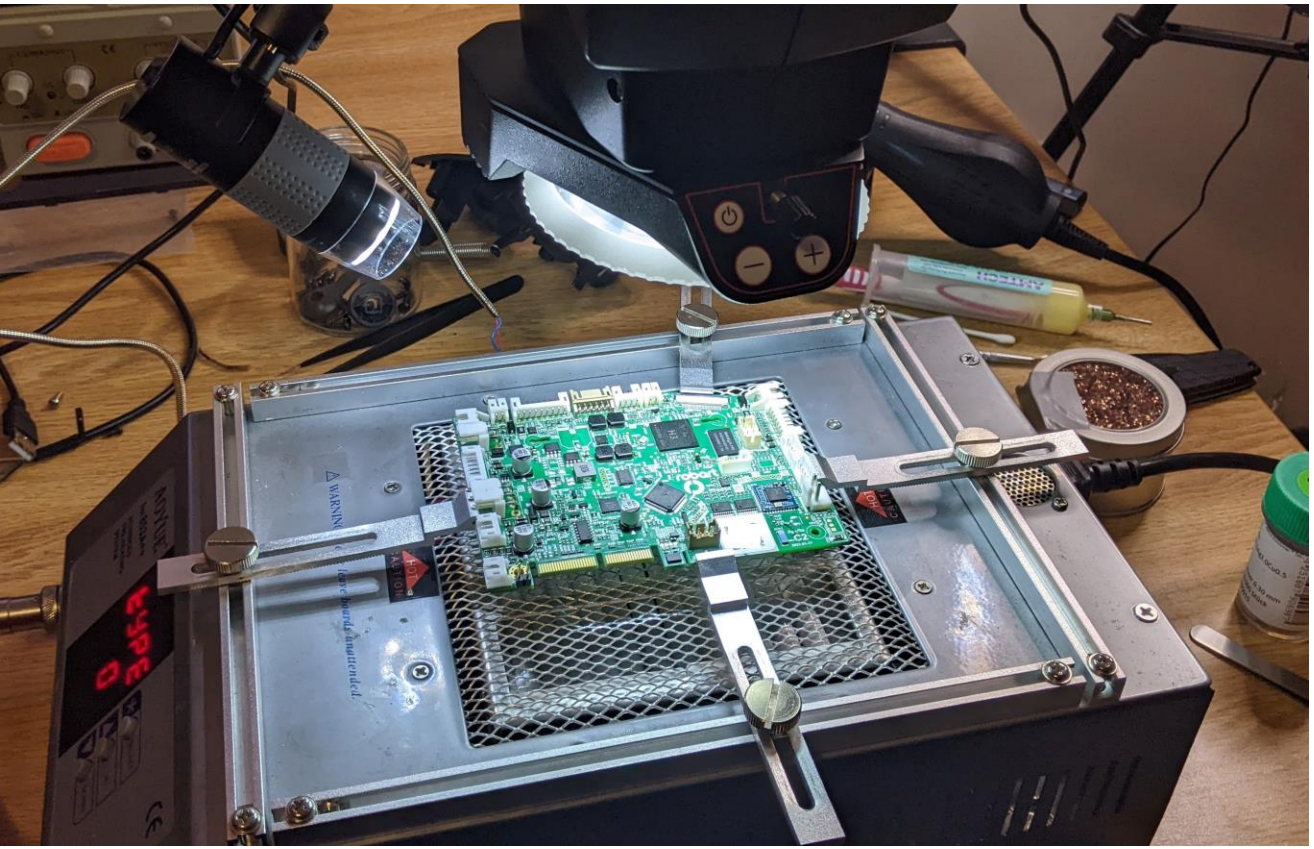


- Presented at DEFCON31 and CCC Camp 2023
- New method: disabling SecureBoot verifications by tampering with bootloader config
  - Idea: trick the U-Boot bootloader to patch itself
  - Result: All existing security mechanisms defeated
  - Applied to multiple vendors: Xiaomi, Dreame, Roborock, Narwal, Shark Robot, etc.
- Issue: finding new rooting methods becomes annoying
  - Solution: let's attack a new vendor

https://dontvacuum.me/talks/DEFCON29/DEFCON29-Robots_with_lasers_and_cameras.html

De-obfuscation of obfuscation

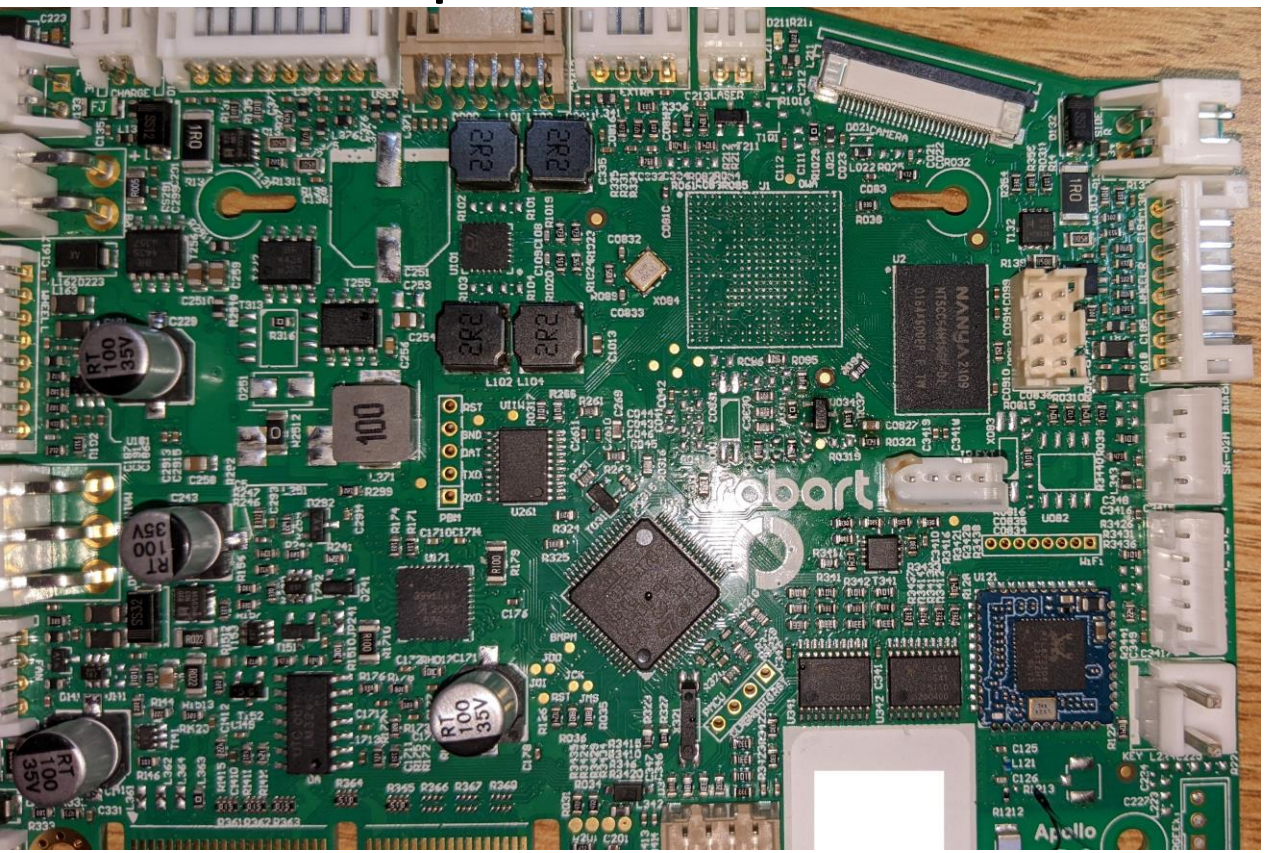
- Example: Shark Robot

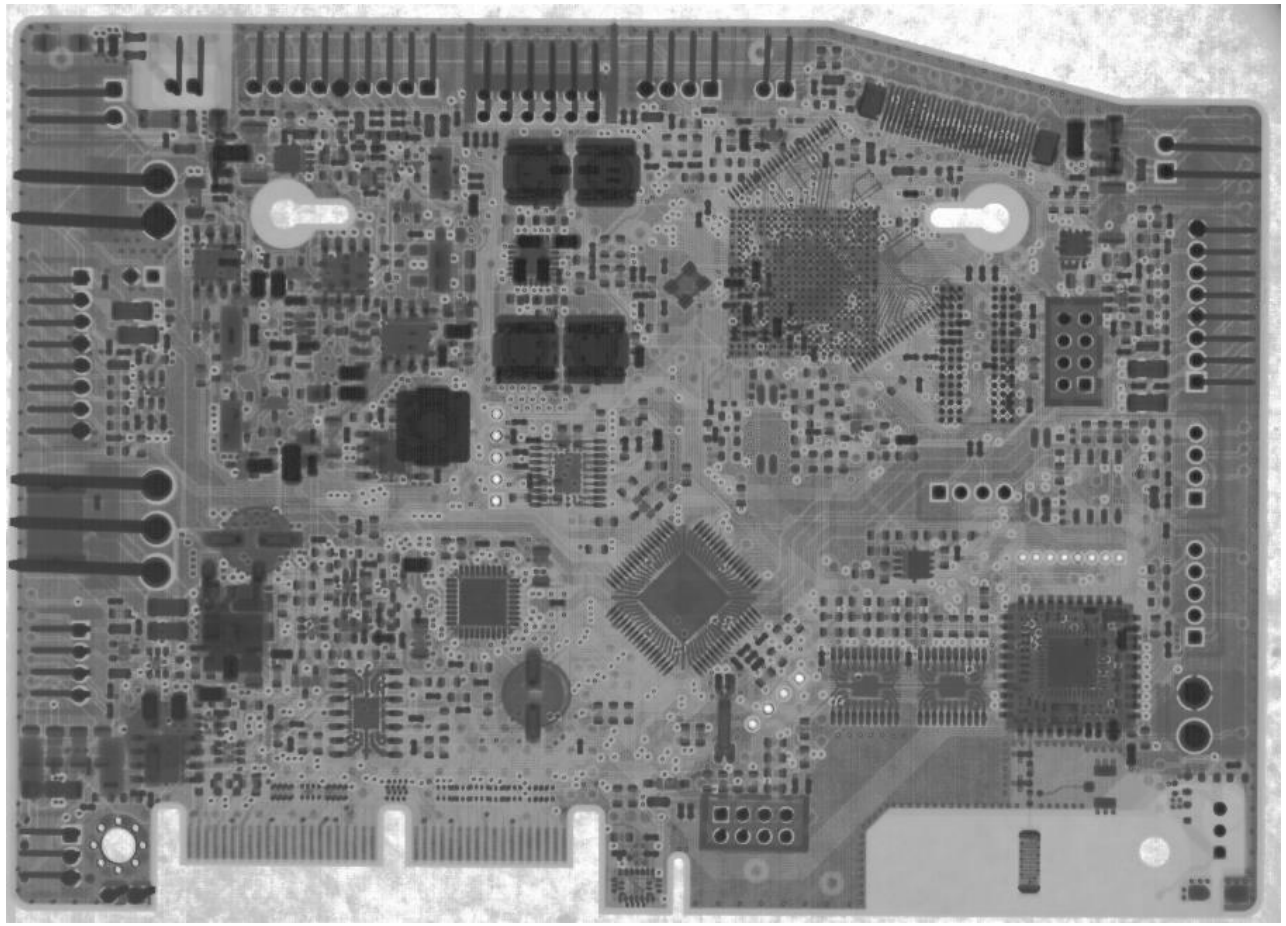


Device designed in 2020 with our research in mind!

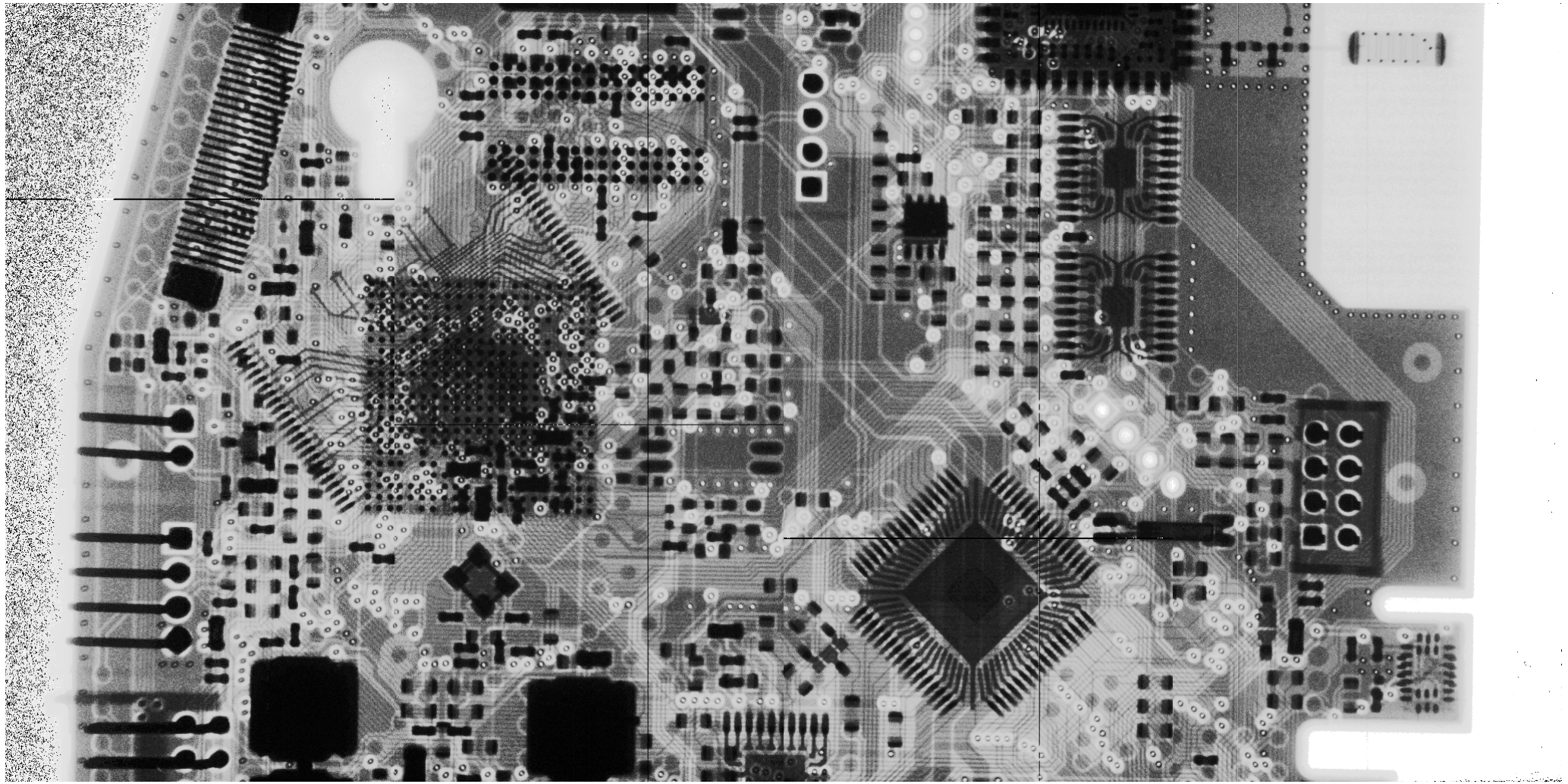
De-obfuscation of obfuscation With X-Rays

- Example: Shark Robot





De-obfuscation of obfuscation



ECOVACS ECOSYSTEM

Why Ecovacs?

- Founded in 1998 in Suzhou, China
  - Original intent: production of OEM vacuum cleaners
- Introduction of their flagship model “Deebot” vacuum in 2007
- 17% market share in 2020, second to iRobot
  - Global market share is likely higher now
  - Currently, Ecovacs market cap is 5x higher than iRobot’s

Early rendition of Deebot

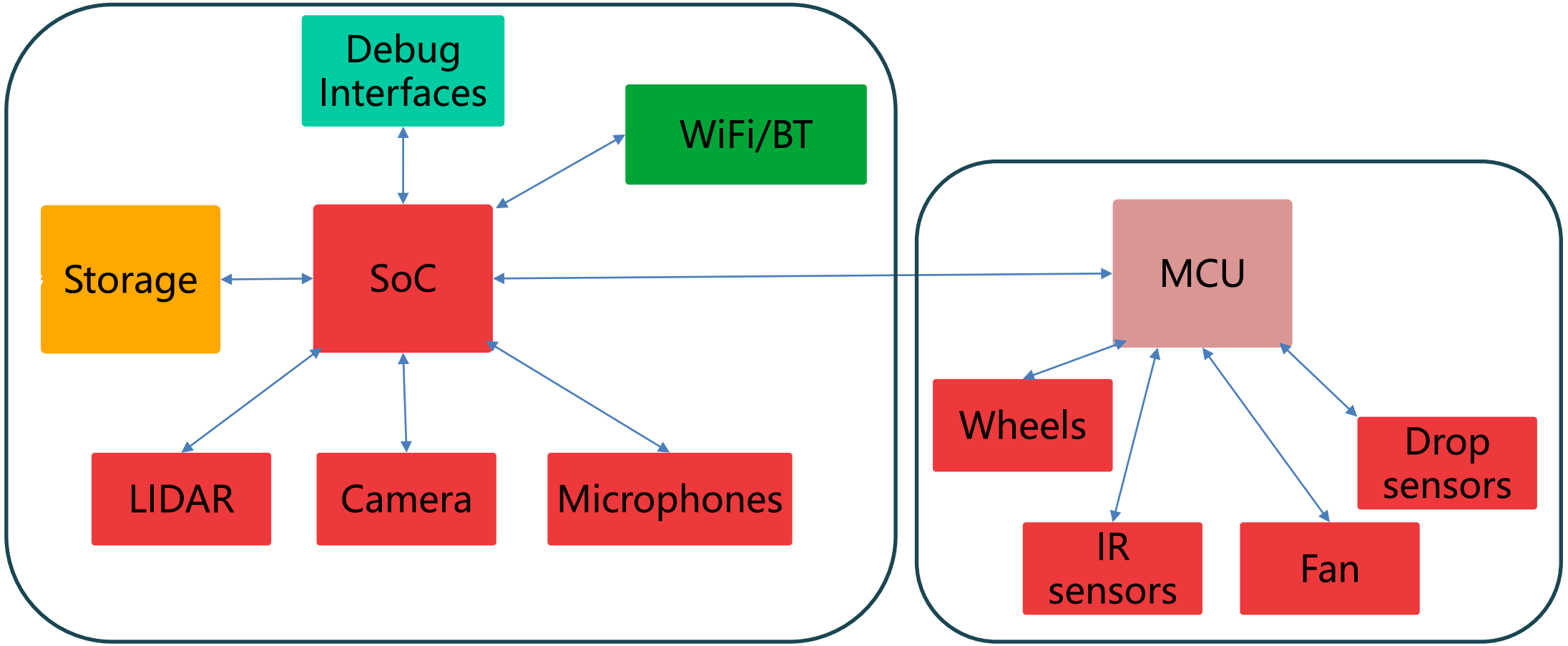
Image source: https://www.ecovacs.com/us/newsroom/official-news/ecovacs-25th-anniversary
Data source: Statista

Products

More than 130 SKUs!

Source: Ecovacs.com and Ecovacs Home App

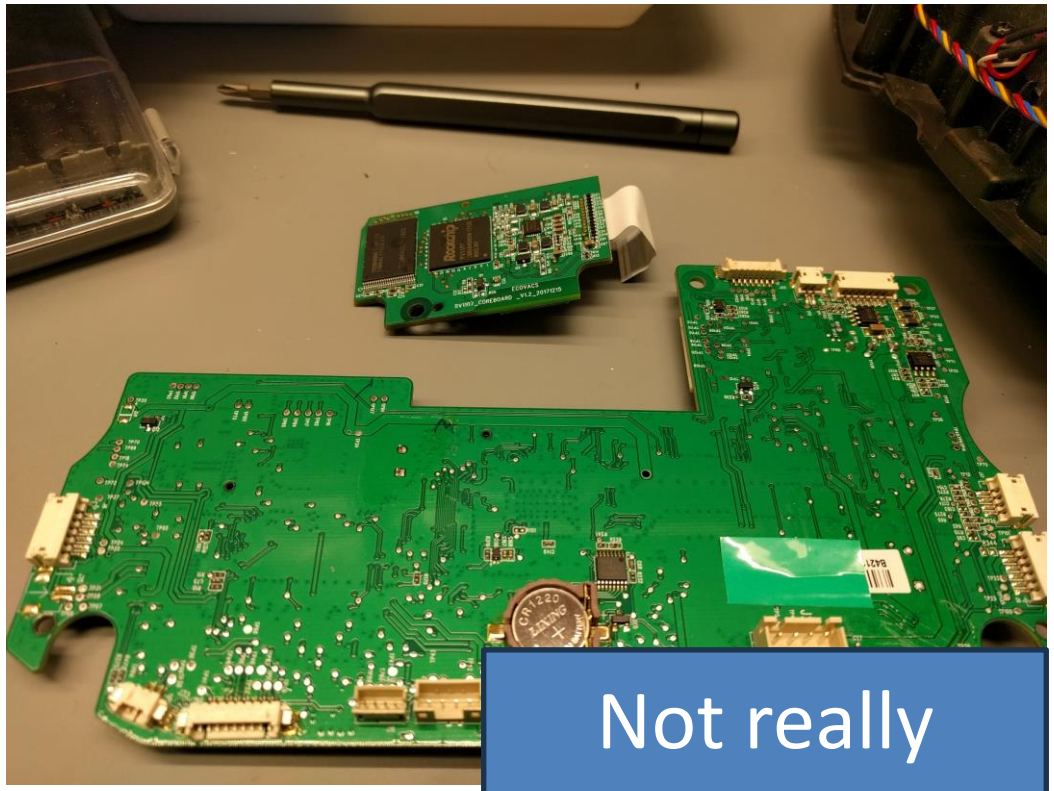
Hardware



*Not all device models have Cameras/Lidars/Microphones

Hardware: Deebot 900 series

- Released 2018
- Based on Rockchip RV1107
  - 1 ARM cores, 128 Mbyte RAM
- 256 MByte NAND Flash
- Sensors:
  - LIDAR
  - IR sensors
- Weak in comparison to Xiaomi Robots

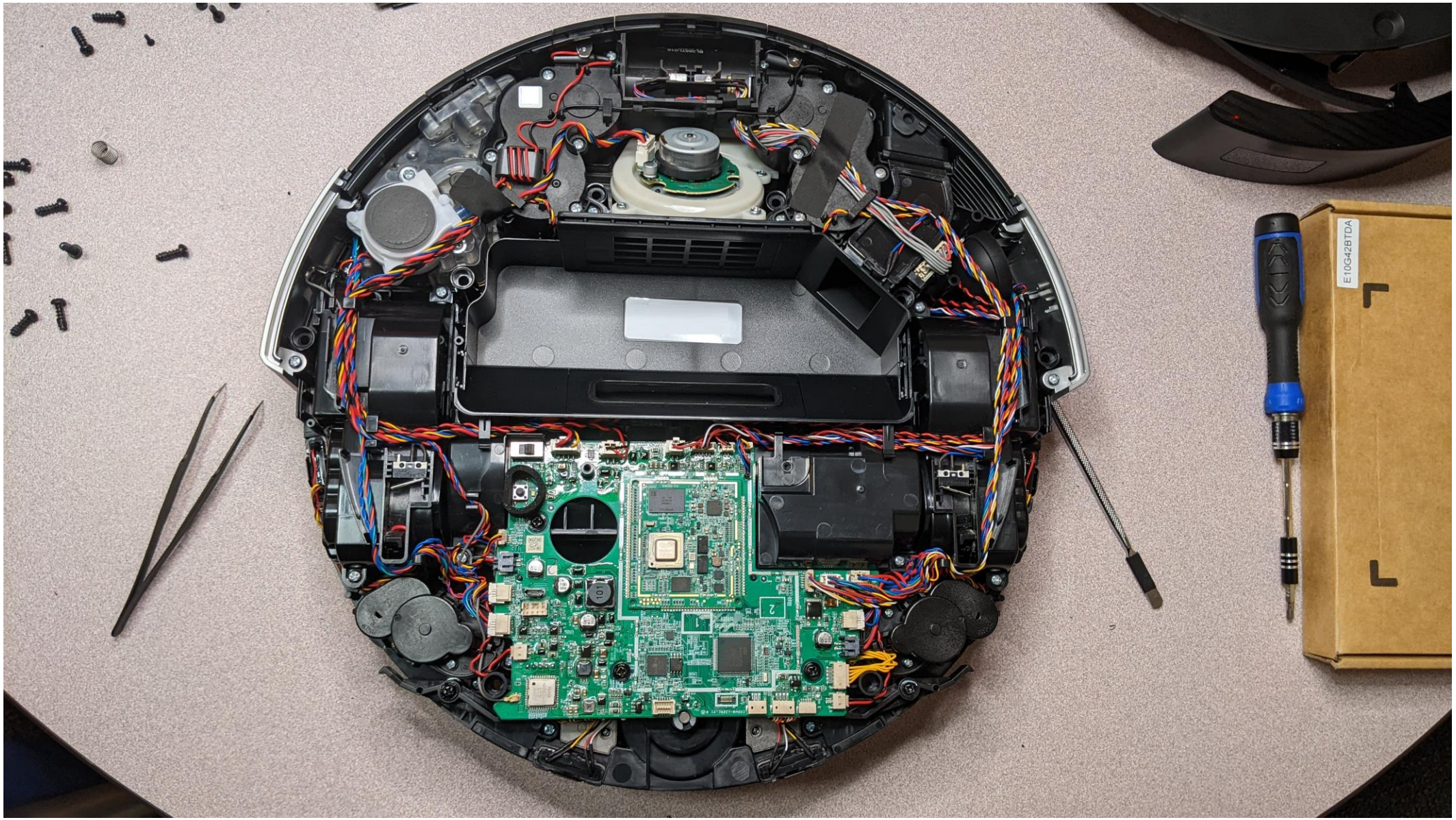


Not really interesting for hacking

https://dontvacuum.me/teardowns/ecovacs-deebot-900
https://rockchip.fr/RV1107%20datasheet%20V1.1.pdf

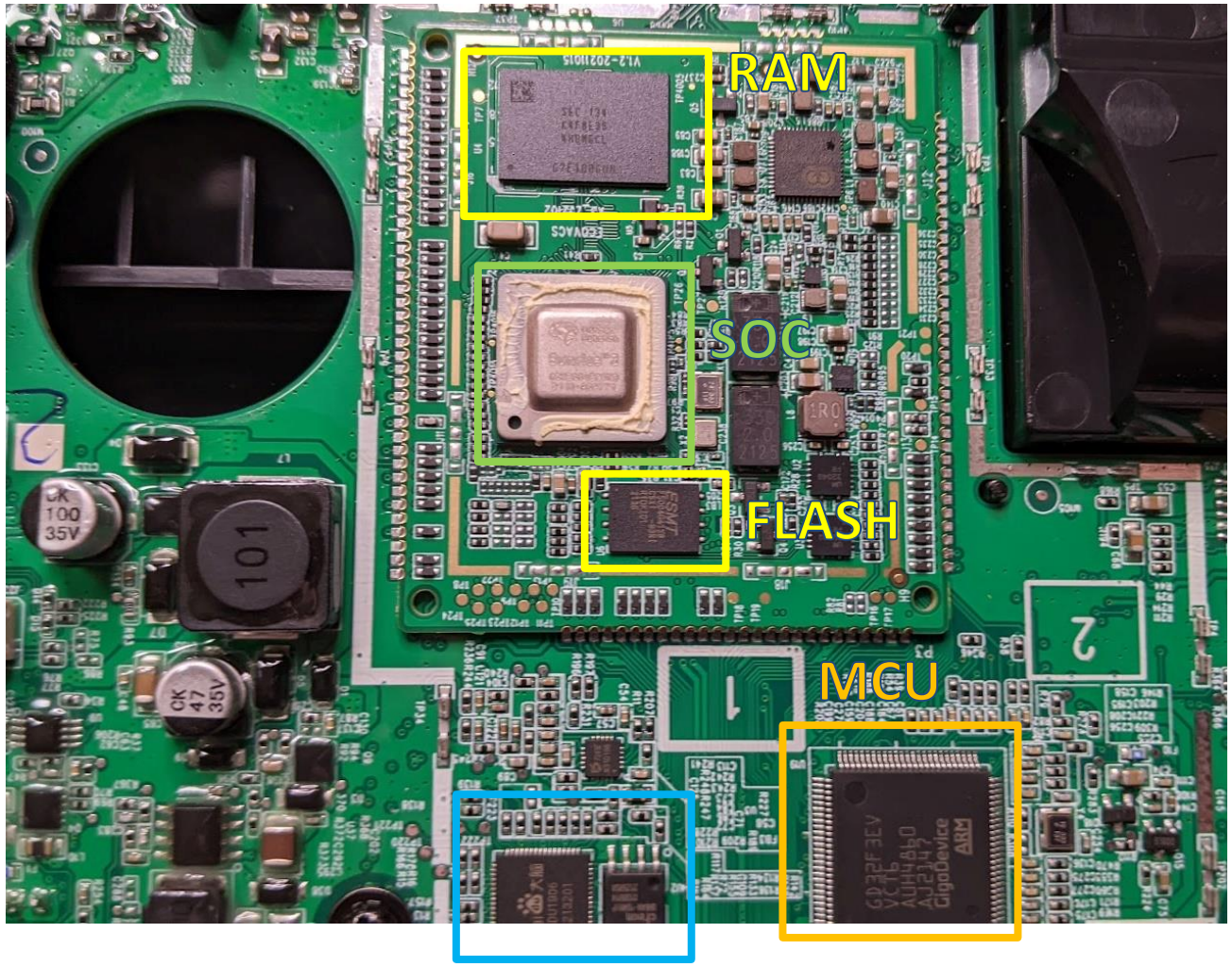
Deebot X1 Vacuum Robot

- Released 2022
- Variants of base station:
  - Omni: Dust-Auto-empty + Mop
  - Turbo: Mop-Only
- Features:
  - Station control
  - Remote view


E10G42BTDA

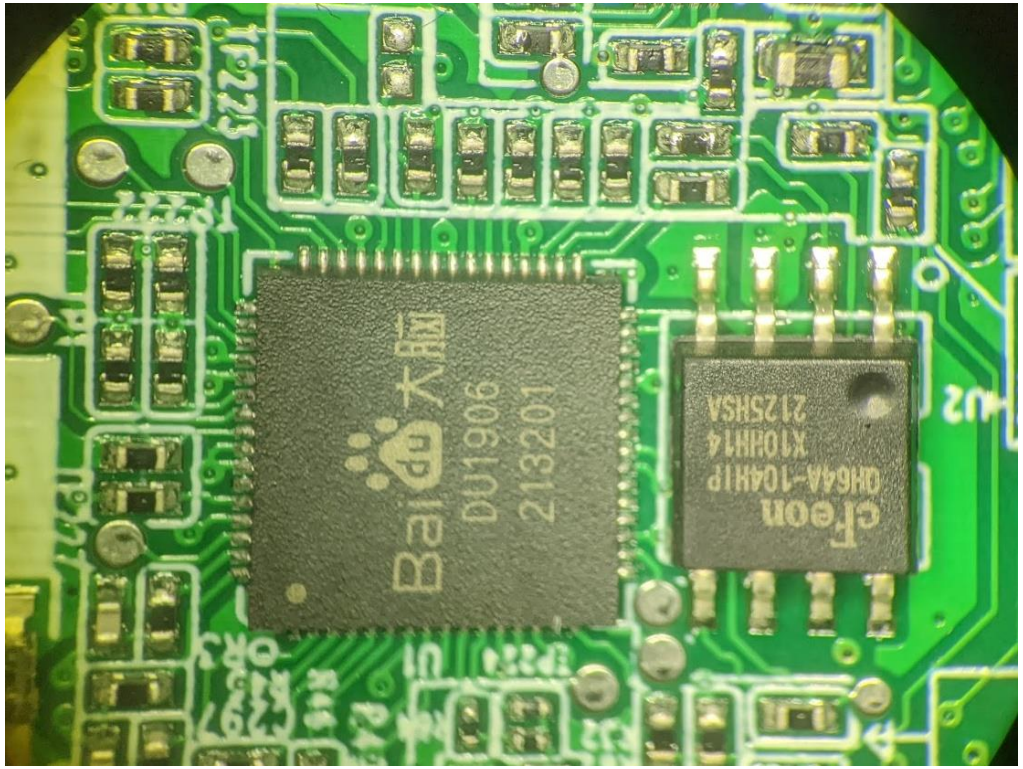
Hardware: Deebot X1

- Based on: Horizon X3 SoC
  - 4x Cortex-A53 processor
  - 1x Cortex-R5 core
  - AI accelerator
- 2 GByte DDR4 RAM
- 512 Mbyte SPI NAND flash
- GD32 MCU



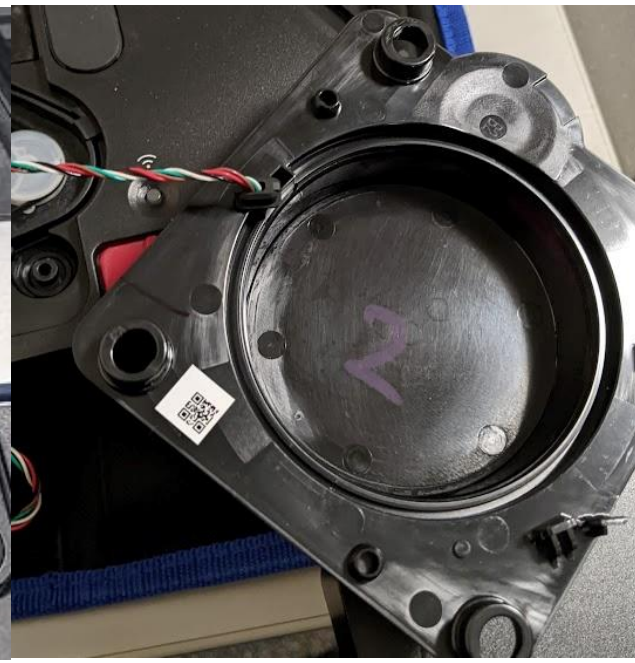
Hardware: Deebot X1

- Special chip: Baidu AI/DSP IC
  - DU1906 voice processing chip
  - Own firmware on SPI flash
  - Wake-up word detection



Hardware: Deebot X1

- Sensors
  - Lidar
  - Microphone array
  - Camera+Line Lasers
  - Lots of IR distance sensors



Airbot Z1

- Released 2023
- Based on hardware platform of X1
  - Difference: additional camera
  - 6 Microphones
- Features:
  - Bluetooth speaker
  - Air filter and Humidifier
  - Home Patrol

Source: https://www.ecovacs.com/de/airbot-air-purifier-robot/airbot-z1

KI-Starlight-Kamera

Die 960P-RGB-Starlight-Kamera des AIRBOT Z1 nimmt Tag und Nacht gestochen scharfe Bilder auf und überwacht zuverlässig die Wohnung während deiner Abwesenheit. Diese Sicherheitsfunktion wurde vom TÜV Rheinland zertifiziert und gibt dir die Gewissheit, dass deine Privatsphäre sicher geschützt ist.

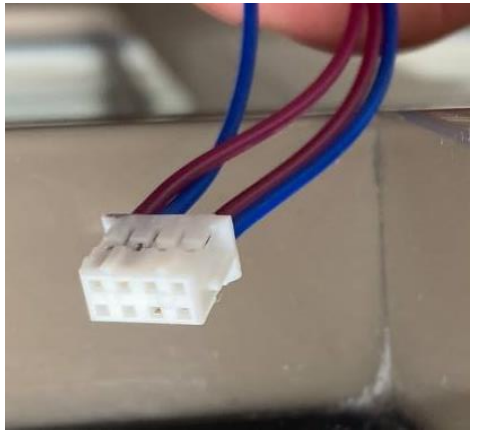
Unterbrechungsfreie interaktive Sprachkommunikation

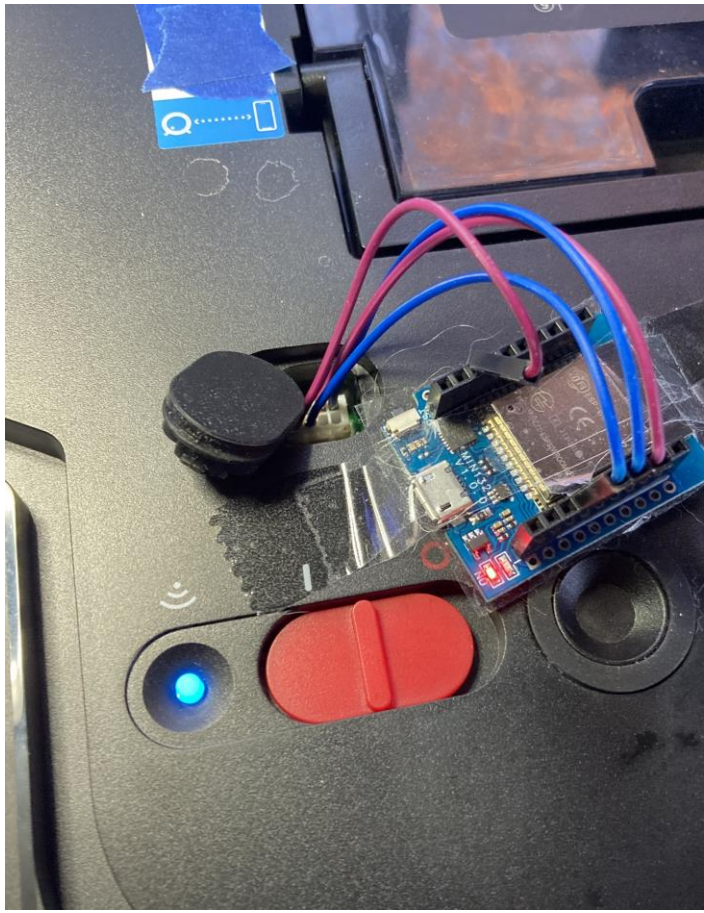
Ausgestattet mit sechs Mikrofonen und einem Zweikanal-Lautsprecher ermöglicht der AIRBOT Z1 unterbrechungsfreie Videoanrufe, um mit deinen Freunden und deiner Familie in Verbindung zu bleiben.

Source: https://www.ecovacs.com/de/airbot-air-purifier-robot/airbot-z1

Debug Ports

- Same for all models since 2019
- Part#: PHDR-08VS
- Provides:
  - UART
  - 3.3V
  - SWD
- Micro-USB





https://www.digikey.com/en/products/detail/jst-sales-america-inc/PHDR-08VS/1166102

Goat G1 Lawnmowing Robot

- Released 2023 in EU
- Navigation
  - GPS
  - Visual, ToF
  - UWB Beacons
- Features:
  - Remote view
  - Patrol feature

GOAT G1

Mehr erfahren

Sorgfältig. Perzeptiv. Intelligent.
G1 ist nicht nur ein Rasenmäher. Er ist auch
ein Gartenwächter

Rund-um-die-Uhr-Gartenüberwachung

Binokulare Kameras erfassen Echtzeitbilder im Innenhof, um Rundumschutz zu bieten. Das TÜV Rheinland-Zertifikat garantiert den Schutz deiner Daten.

Hardware: Goat G1

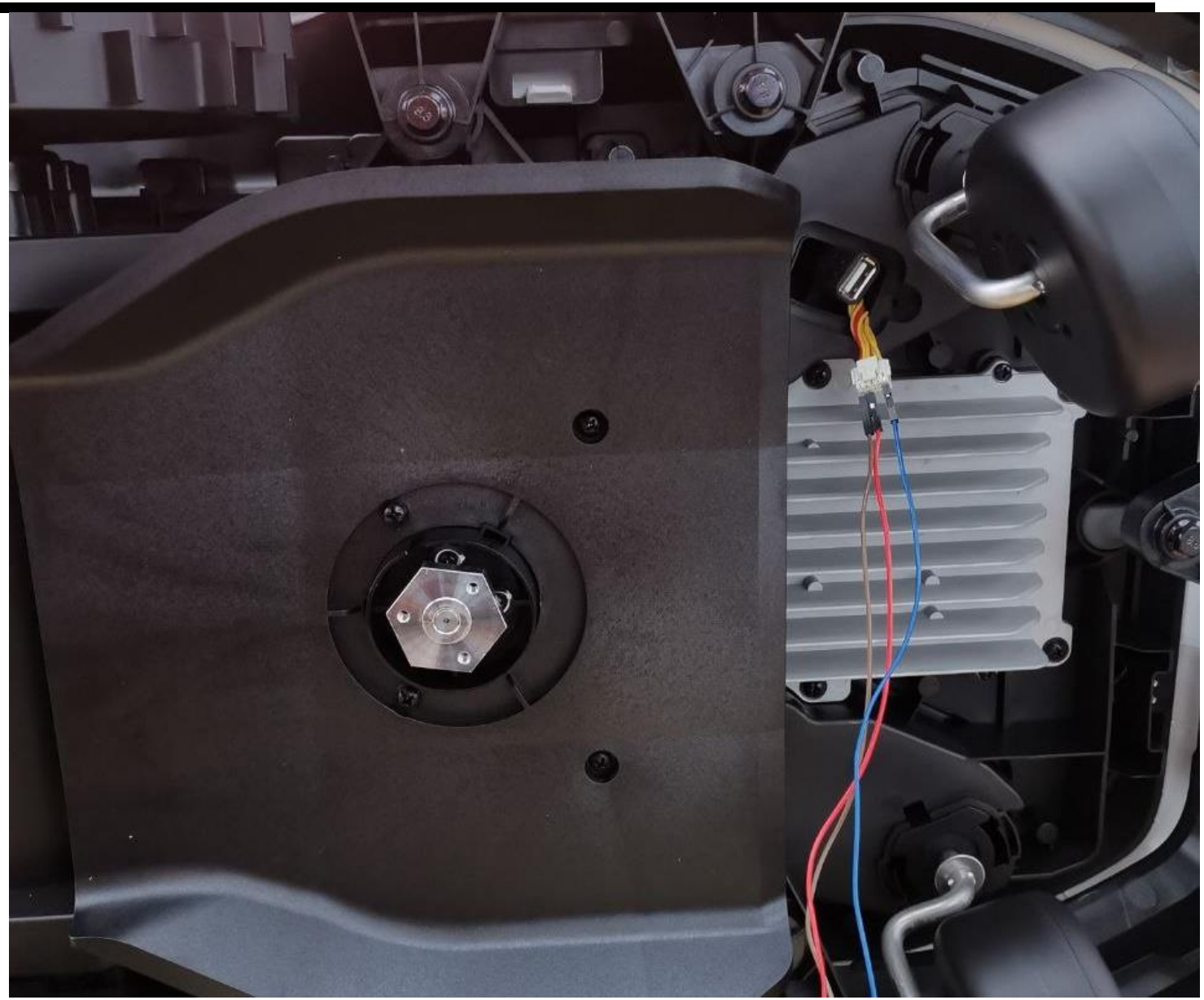
- Based on: Rockchip RK3588
  - 4x Cortex-A76
  - 4x Cortex-A55
  - AI accelerator
- 4 GByte DDR4 RAM
- 16 Gbyte eMMC flash
- Multiple GD32 MCUs
  - Display, Knife assembly

Hardware: Goat G1

- Sensors
  - 360° Camera (3MP)
  - Front Camera (2MP)
  - ToF Camera
  - Rain detector
  - GPS
  - Bump switches
  - LTE (optional)

Debug Ports

- Easy to access ports
  - USB
  - UART
  - JTAG
  - SWD



Software

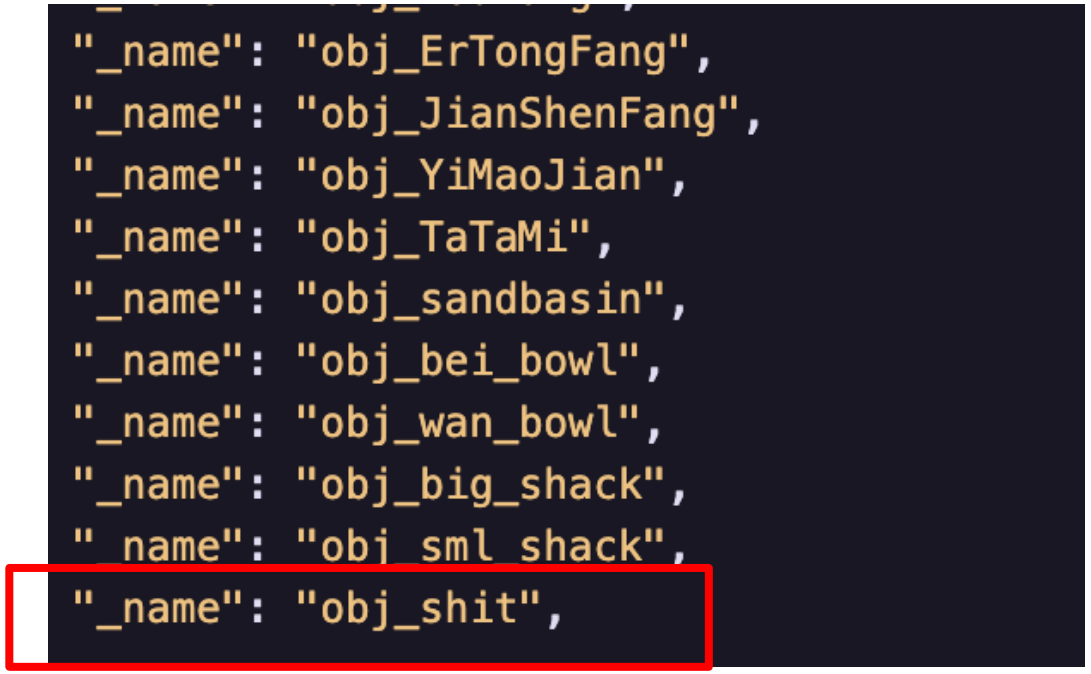
- Linux OS
- ROS Melodic Morenia
  - Open-source robotics software
  - Used for navigation
- „Medusa“
  - Custom Ecovacs software
  - Tasks: Cloud communication, logging, OTA updates, Robot control, remote camera access, etc.

Software

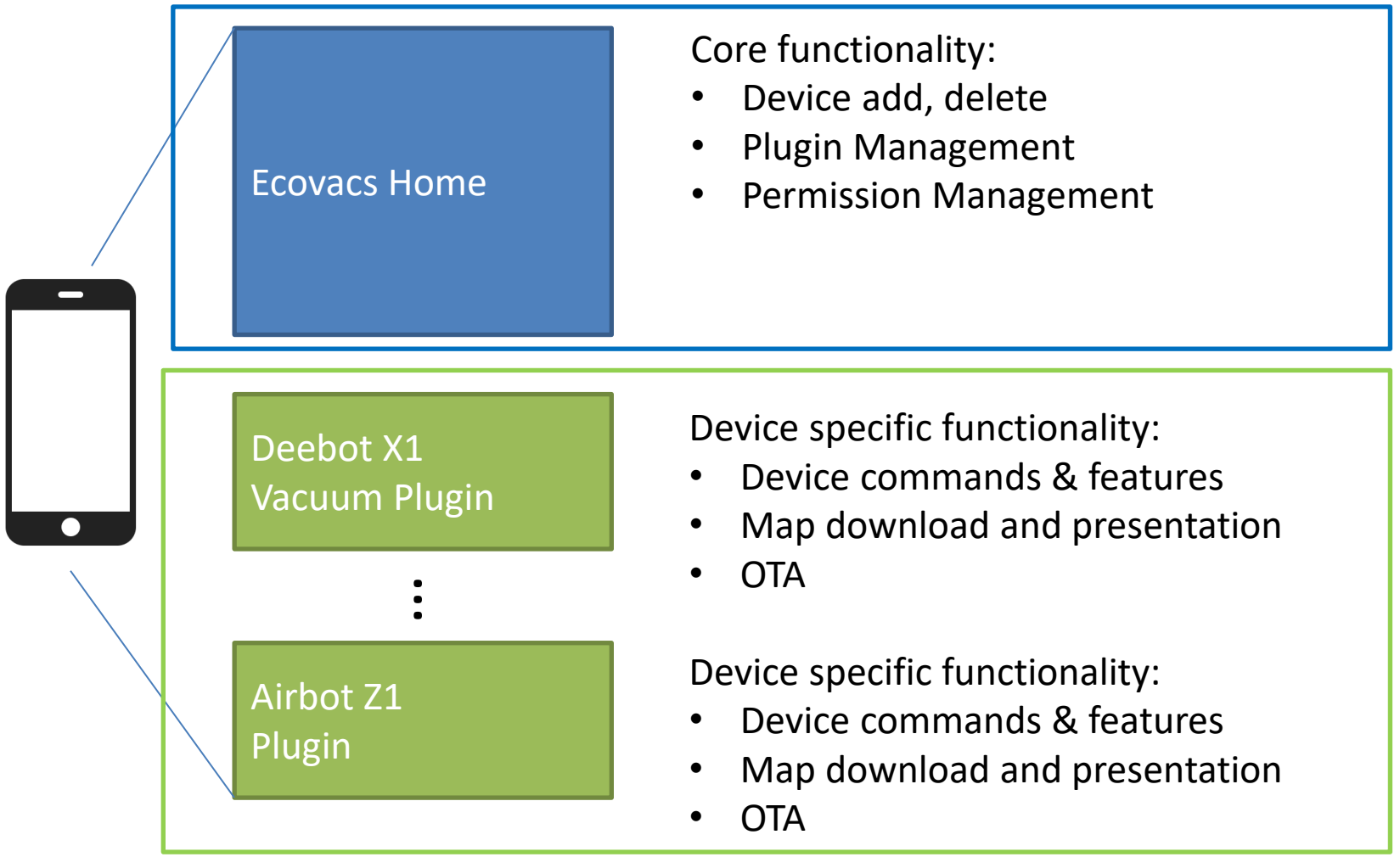
- Software packages:
  - Full Python 2.7 environment
  - AWS Kinesis SDK (remote camera access outside of China)
  - Alibaba Aliyun SDK (remote camera access inside of China)
  - Lots of „messy“ bash scripts
    - Example: „audio_record.sh“

AI models

- Tensorflow and OpenCV is used for detection
- Typical objects:
  - Furniture
  - Cable
  - Pets and Pet „remains“
- Lawn Mower:
  - Small animals
  - Face Recon



App Structure

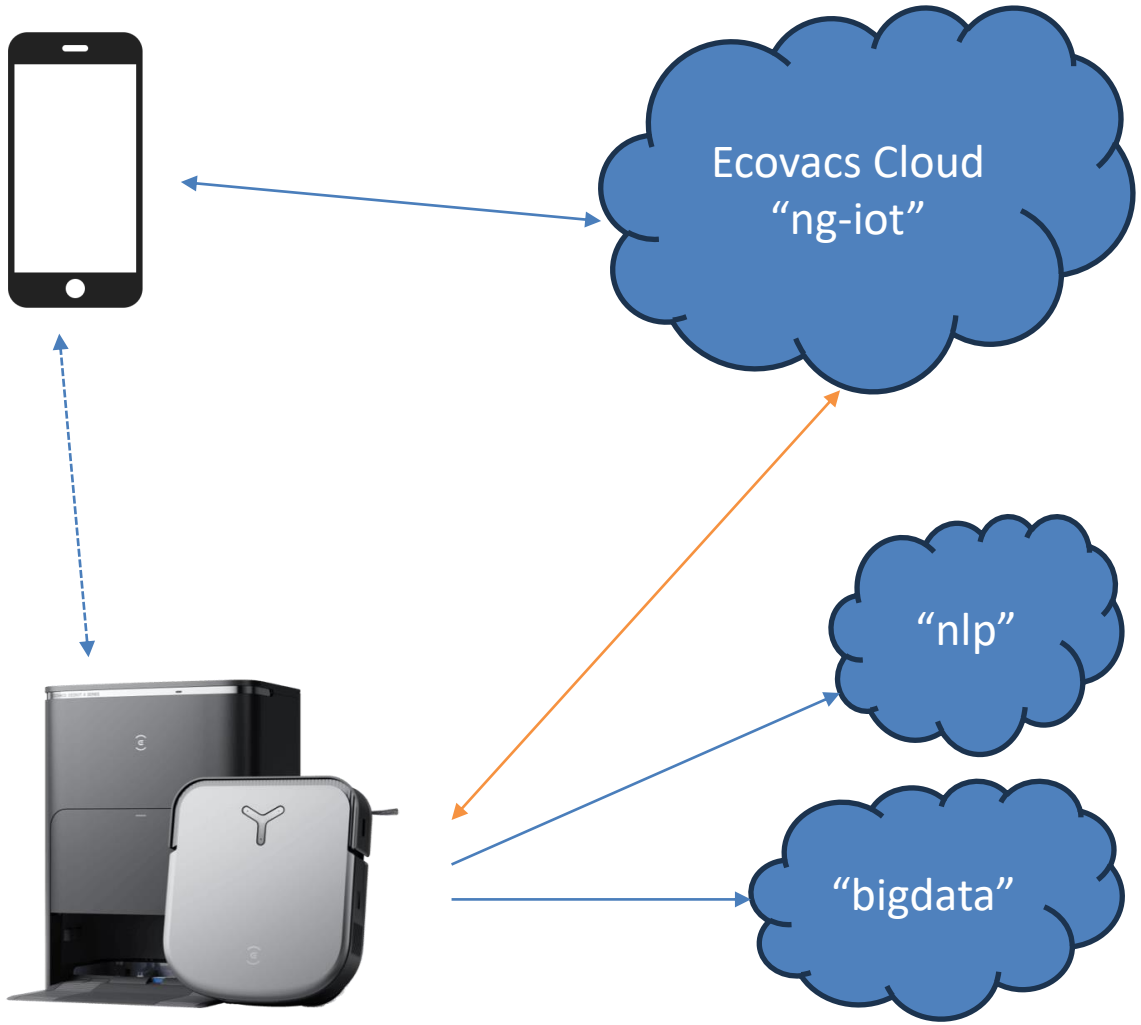


Native Android/iOS app

VueJS code
(downloaded dynamically)

Communication Relations

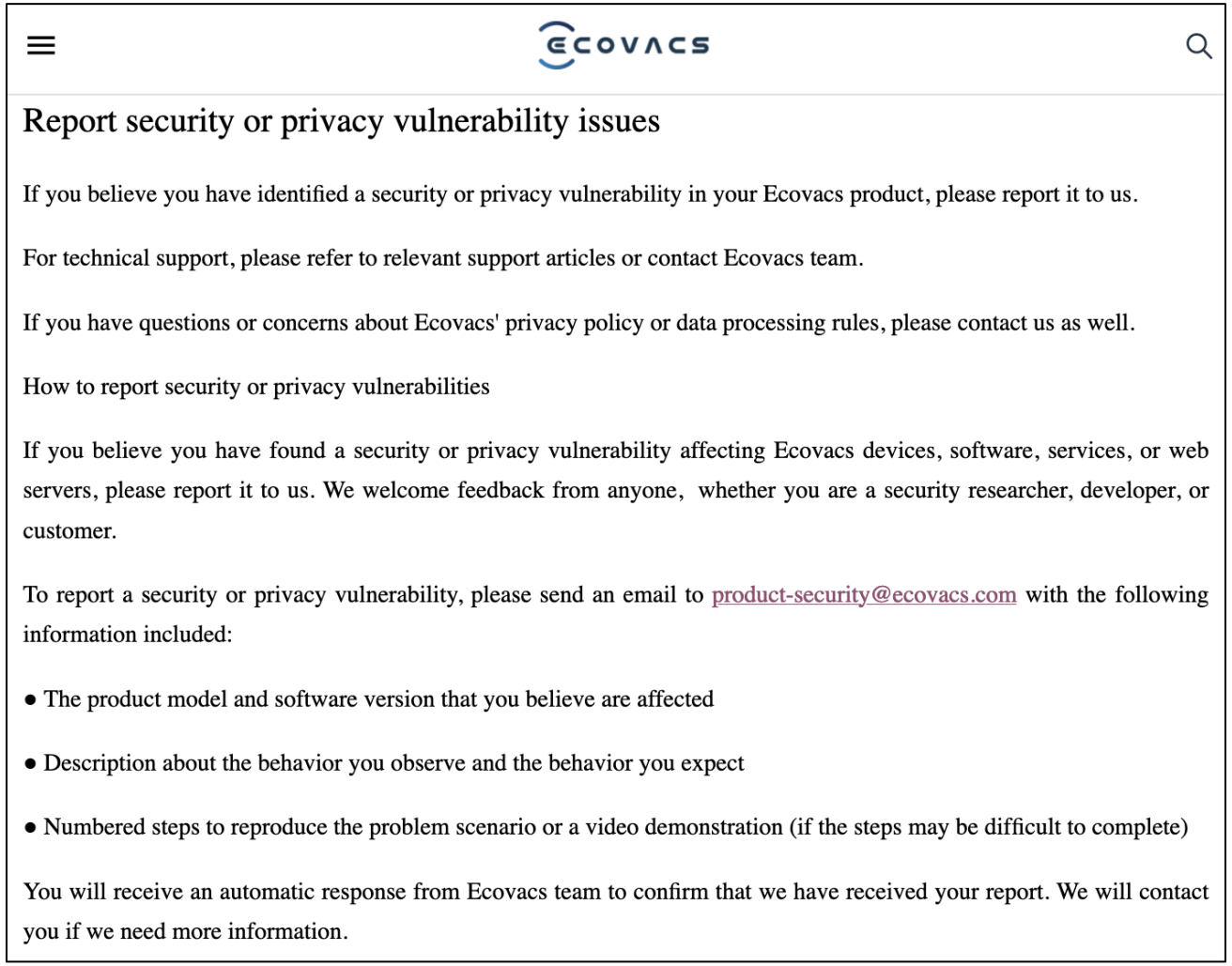
- Direct communication
  - Only while provisioning via Bluetooth
  - Fallback for mowers
- NG-IoT
  - MQTT endpoint
  - Acts as proxy between device and App



nlp is used by the „Hello Yiko“ voice assistant

Ecovacs security

- No real, collaborative bug bounty program
  - promise acknowledgement on public bulletin board
  - …bulletin board doesn't exist?



ECOVACS

Report security or privacy vulnerability issues

If you believe you have identified a security or privacy vulnerability in your Ecovacs product, please report it to us.

For technical support, please refer to relevant support articles or contact Ecovacs team.

If you have questions or concerns about Ecovacs' privacy policy or data processing rules, please contact us as well.

How to report security or privacy vulnerabilities

If you believe you have found a security or privacy vulnerability affecting Ecovacs devices, software, services, or web servers, please report it to us. We welcome feedback from anyone, whether you are a security researcher, developer, or customer.

To report a security or privacy vulnerability, please send an email to product-security@ecovacs.com with the following information included:

- The product model and software version that you believe are affected
- Description about the behavior you observe and the behavior you expect
- Numbered steps to reproduce the problem scenario or a video demonstration (if the steps may be difficult to complete)

You will receive an automatic response from Ecovacs team to confirm that we have received your report. We will contact you if we need more information.

Source: https://www.ecovacs.com/global/report-issues

Privacy policy

- No guarantees that data stays in user locale
- Generally, regional AWS services used
- Photos and videos sent to Ali Cloud Video for AI analysis in certain models
- Lots of telemetry data collected

Privacy concerns

- Vacuums equipped with microphones and cameras
  - Can they be enabled remotely without user notice?
  - Where is the data sent?
- AI
  - Why do robots need face recon AI models?
  - Is telemetry data being used to train AI?

Privacy concerns

Unauthorized Access to Video Feeds

The first common fear about robot vacuum camera privacy is outsiders gaining unauthorized access to the device's video feed or recordings. In a story that went viral in 2022, pictures of a female sitting on a toilet, captured by a robotic vacuum cleaner, circulated around the Internet. The manufacturer responded by saying that the image had been taken as part of the device's training, but the fact that the image had been captured and made public left a bad taste in people's mouths.

DEEBOT robot vacuums counter hackers accessing cameras by **encrypting all data gathered by the device** (including videos) with the AES-128 (128-bit Advanced Encryption Standard.

Can Robot Vacuum Cameras Be Hacked?

2023-08-14

CONTENTS

1.Why Do Smart Vacuums Have Cameras?
2.What Kind of Data Do Robot Vacuums Gather?

Source: https://www.ecovacs.com/us/blog/robot-vacuum-privacy-concerns

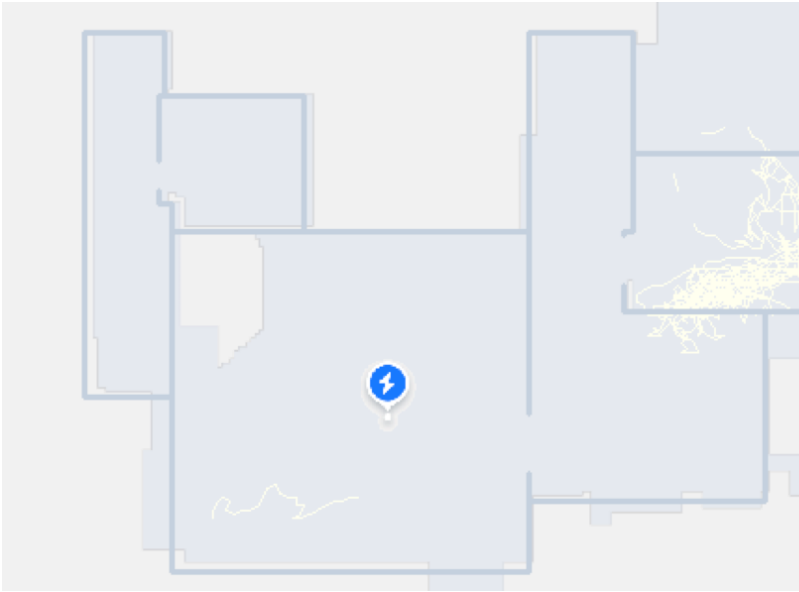
FINDINGS

Data harvesting

- Mobile apps and robots are chatty, a lot of communication with Ecovacs servers
- Key data collection API endpoints: “bigdata”, “data_upload”
- Telemetry data collected
  - Live coordinates of robot location in home
  - Wi-Fi access points, network data
  - Additional information if robot gets stuck
  - AI pictures? (even if not opted in)

Data retention in the Cloud

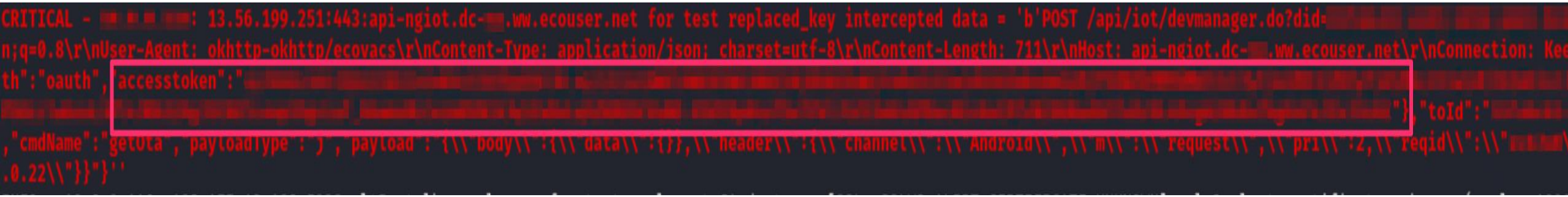
- Maps and pictures are stored in a NoSQL database
  - Anyone who knows the ObjectID can access the data
- Maps associated with robots seem to remain on servers
  - Survive factory reset
  - Re-pairing to different account
  - Deletion of account has no effect
- Tokens remain valid after account deletion
  - Access to robot still possible



TLS sadness in the App

- Ecovacs Home app correctly checks certificates
  - However, the robot-specific plugins don't always do
- Plugin accepts self-signed certificates
  - Risk in insecure Wi-Fi networks, e.g. Airport, Hotels, 37C3
  - No warning or error shown in App
- Leaks user account auth tokens
  - Allows the attacker full access to account and devices
  - Tokens expire after 7 days

TLS sadness in the App



Encoded PASTE A TOKEN HERE

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.ey

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "c": "
  "u": "
  "r": "
  "t": "a",
  "iat": 170339
  "exp": 170399
}
```

TLS sadness in the Robot

- MQTT & TLS connections accept self-signed certs
  - Perfect tool: certmitm by Aapo Oksman
  - Allows MITM
  - OTA updates can be injected

down_audio_hook.sh

```
#!/bin/sh
…
wget --no-check-certificate -T 60 -O /tmp/${LANGUAGE_ID}.tar.gz_ ${LANGUAGE_URL} && mv /tmp/${LANGUAGE_ID}.tar.gz_ /tmp/${LANGUAGE_ID}.tar.gz
…
```


https://github.com/aapooksman/certmitm

User Data storage on device

- User data partition not encrypted
- Lots of log, configs, maps and pictures stored on partition
  - Live Video pin (MD5 hash), mower pin (plaintext)
  - Wi-Fi credentials, BT addresses
  - Neighbor Wi-Fi access points
  - “Hello Yiko” traffic logs
- Factory reset: does not fully erase all information
  - Additional problem: flash wear leveling

Selling a used device, even if it is factory reset: Risk to your privacy!

Learn about IoT and wear leveling here: https://dontvacuum.me/papers/ACMWisec-2021/

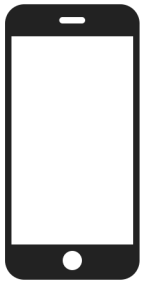
Sneaky live video

- Audio warning when camera is accessed
  - At start of access and every 5 minutes
  - Implementation: sound file is played
- Problem:
  - Localized sound files stored on /data
  - sound files can be deleted or replaced
- Attack: replace warning with empty file

Live video ap(p)ocalypse

- App allows live audio+video access on robot
  - Functionality provided by AWS Kinesis
- Owner and shared users can access feature
- Can be protected by PIN
  - Asks for PIN before connecting
  - Can only be changed and reset by owner
  - Reset requires account credentials

Live video ap(p)ocalypse



Ecovacs Cloud

PIN 1234

"Is Pin set and enabled?"

Check if Pin enabled in JSON file

"Pin is set"

Ask user for PIN

"Verify hash(eco_1234)"

Check if Pin hash matches with local hash

"Pin is correct"

Was the Pin reported as correct?

"Start AWS Kinesis WebRTC session"

Kinesis SDK: Join session

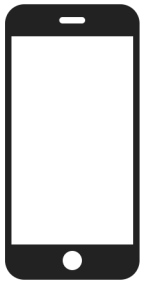
WebRTC session data

Join WebRTC session

Via AWS Kinesis

Stream video and audio

Live video ap(p)ocalypse



Ecovacs Cloud

PIN 1234

"Is Pin set and enabled?"

Check if Pin enabled in JSON file

"Pin is set"

Ask user for PIN

"Verify hash(eco_1235)"

Check if Pin hash matches with local hash

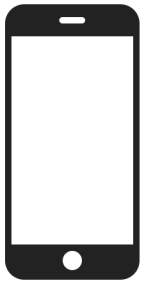
"Pin is incorrect"

Was the Pin reported as correct?

Show error „Wrong pin!"

Are PIN verification and WebRTC tied together?

Live video ap(p)ocalypse



Ecovacs Cloud

PIN 1234

"Is Pin set and enabled?"

Check if Pin enabled in JSON file

"Pin is set"

Ask user for PIN

"Verify hash(eco_1235)"

Check if Pin hash matches with local hash

"Pin is correct"

"Pin is incorrect"

Was the Pin reported as correct?

"Start AWS Kinesis WebRTC session"

Kinesis SDK: Join session

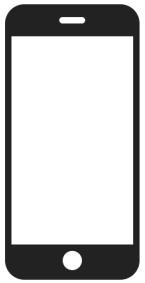
WebRTC session data

Join WebRTC session

Via AWS Kinesis

Stream video and audio

Live video ap(p)ocalypse



Ecovacs Cloud

PIN 1234

Not caring about any PIN

"Start AWS Kinesis WebRTC session"

WebRTC session data

Kinesis SDK: Join session

Join WebRTC session

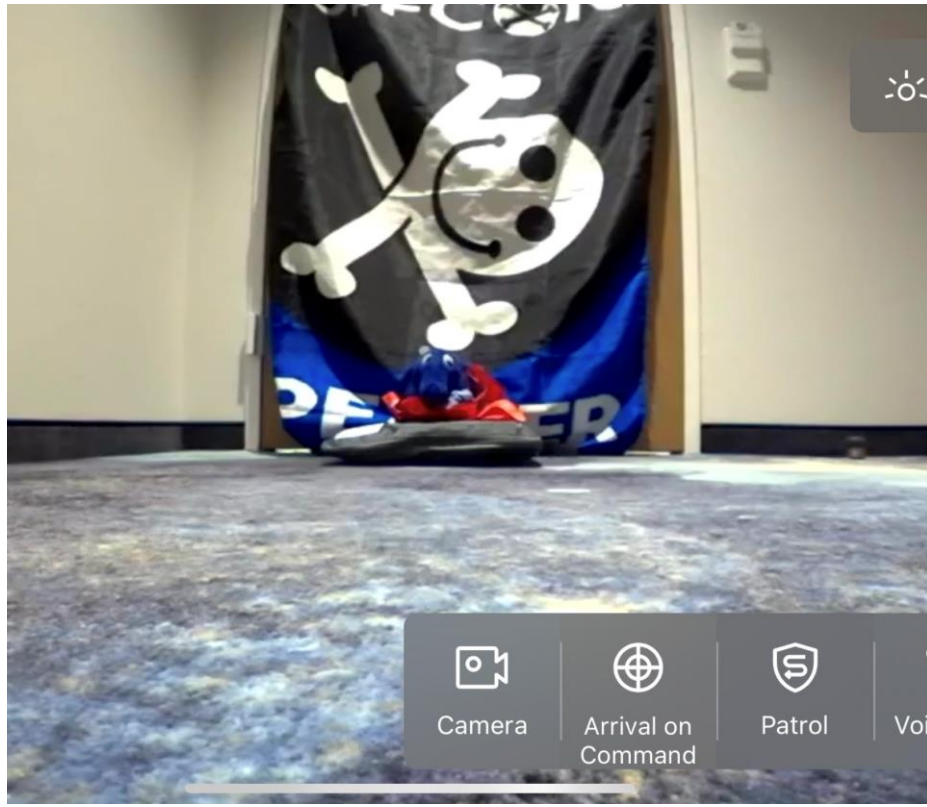
Via AWS Kinesis

Stream video and audio

Note: This is NOT a vulnerability in AWS Kinesis. The issue is in Ecovacs implementation!

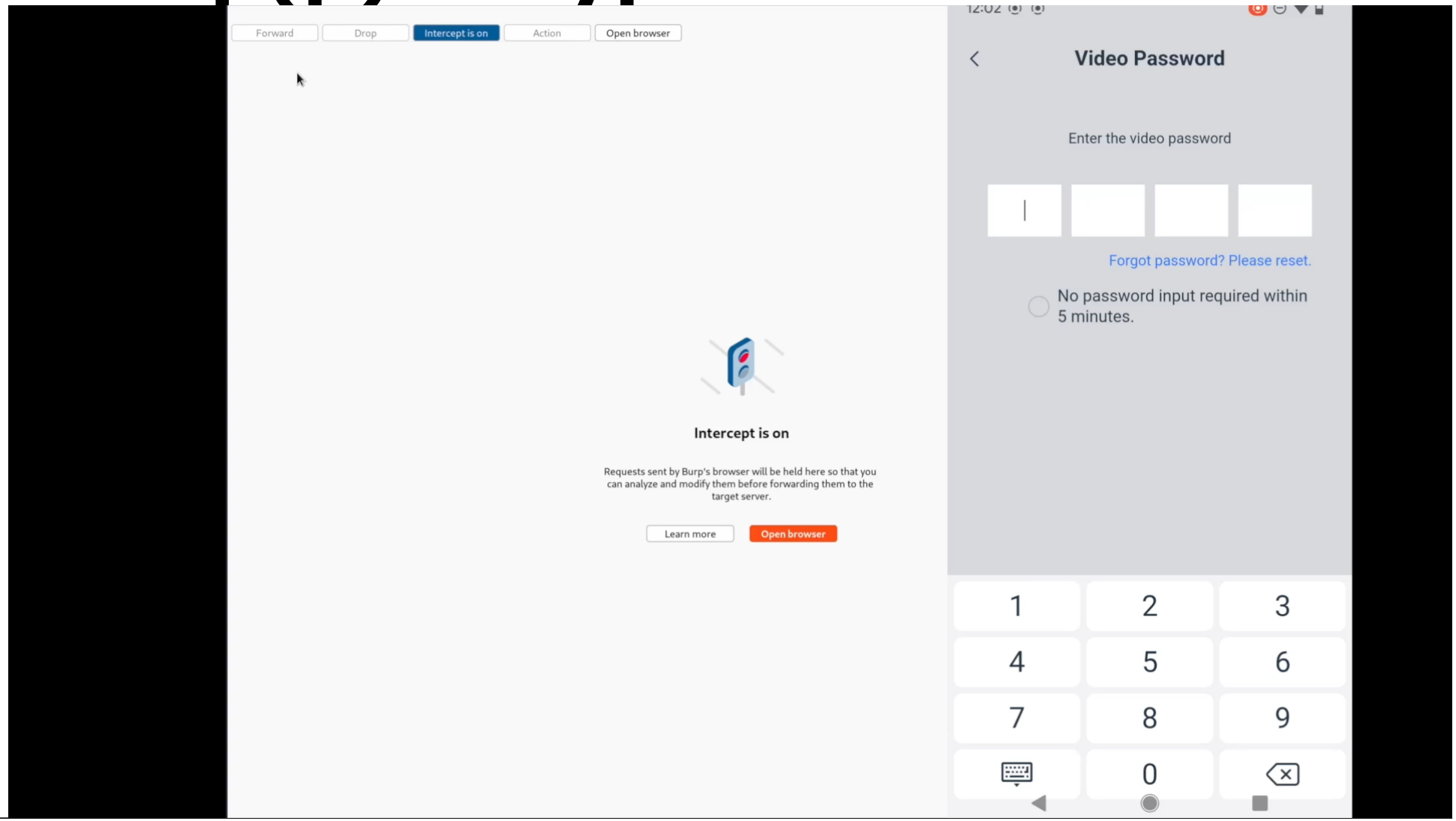
Live video ap(p)ocalypse

- PIN protection based on the “Honor system”
  - Client-based authentication and ACL enforcement
  - Robot does not keep track of successful authentications
- Log of video stream access relies on honesty of app
- Really bad in combination with TLS issue or shared accounts
- Even worse: If sound files have been tampered



„Honor“ system also applies to other aspects in the App

Live video ap(p)ocalypse DEMO



Recording here: https://youtu.be/zGHnLVdKMXA

*Free lawn mowers

- Ecovacs Goat G1 has anti-theft mechanism integrated
  - If robot gets picked up, PIN is required to unlock
  - Alarm can get triggered
- Problem:
  - Protection is implemented in SoC (and not in MCU)
  - Pin is stored in plaintext on robot
  - Attacker can dump the pin after stealing the device
- Other mowers have the same issue

Do not keep your mower outside unprotected!

Solution: improvement of locking mechanism

*lawn mower not actually free. Do not steal robots!!!
We give this talk in the winter on purpose, so that people can protect their devices

ROOTING AND DISCONNECTING ECOVACS FROM THE CLOUD

Related work

- Sucks https://github.com/wpietri/sucks
  - Python client interface that allows control of robots
  - Talks to the cloud
  - Abandoned in 2021
- Bumper https://github.com/bmartin5692/bumper
  - Standalone implementation of Ecovacs servers
  - Robots and official App (or Sucks) connects to Bumper
  - Allows control of the robots
  - Requires DNS redirection and SSL CA import on phone
  - Confirmed to work for older models (pre-2020)

Related work

- Home Assistant plugin
  - Integrated in HA since version 0.77
  - Based on py-sucks
  - Connects to Ecovacs cloud and allows robot control

Countermeasures

- Many interesting binaries are obfuscated
  - Lots of XOR and byte shifting to hide strings
- Anti-debugging features
  - Detection of LD_PRELOAD
  - Detection of ptraces and debuggers
- SecureBoot / Android Verified Boot (AVB)
  - Enabled on some devices
  - Usage of dm-verity to protect rootfs

Root shell

- Login shell is accessible via UART
- Problem: every device has a different root password
  - Not hard-coded, set at boot time
- Function well hidden and obfuscated
- Responsible program: “eco_passwd”
- Computation:

  base64(sha256({model}d4:3d:7e:fa:12:5d:C8:02:8F:0A:E2:F5{sn}\n))
- Tool: https://builder.dontvacuum.me/ecopassword.php

Firmware updates

- Firmware is encrypted but not signed
- Encryption key dynamically computed
  - Differs by firmware version, metadata, device model
  - Algorithm well hidden and protected against debugging
- Reverse engineering supported by „tihmstar“
- AES 128 CBC IV and Key derived from:

Format string: "vX2Z3X3RhcmdldCA%s1jdSAt%sbyBtYW4%dy5iaW4%s%x825xx%s„

% ("ECO-PT", model, section_type, "", section_len, "jeff-hk@126.com")

Persistence: RootFS modification

- Only a few models check for integrity of RootFS
- Example: Deebot X1
  - Partitions are SquashFS packed in JFSS2
  - No signatures or verifications
  - Can be unpacked and repacked
- Verification depends on SDK version and SoC used

Persistence: Autostart

- Forgotten debugging feature
- At bootup:
  - Check if „/data/autostart“ exists
  - Run any .sh scripts in that folder
- Reminder: „/data“ not encrypted or protected in any way
- Limitation: disabled on some devices

Persistence: Factory resets

- Factory resets delete* all files from /data
- Filesystem is not recreated
- Idea: make file immutable
  - Use “chattr” to add immutable attribute
  - Immutable files will survive factory resets and updates

Future Work

Valetudo

How about Lawn Art using the robot as a printer? ☺

- Use ROS directly to build a “open-source” Robot
- Revive existing projects “Bumper”, “Sucks”
- Port “Valetudo” to Ecovacs
  - MQTT is not MIIO => New transport needs to be implemented
  - WIP (don’t ask when it will be done)
- Lawn mowers: find effective ways to prevent theft
- Persistence for all existing models
- Looking for more shady stuff in the firmware

We need your help with this!

THE TALE OF CERTIFICATIONS

Types of cybersecurity certifications

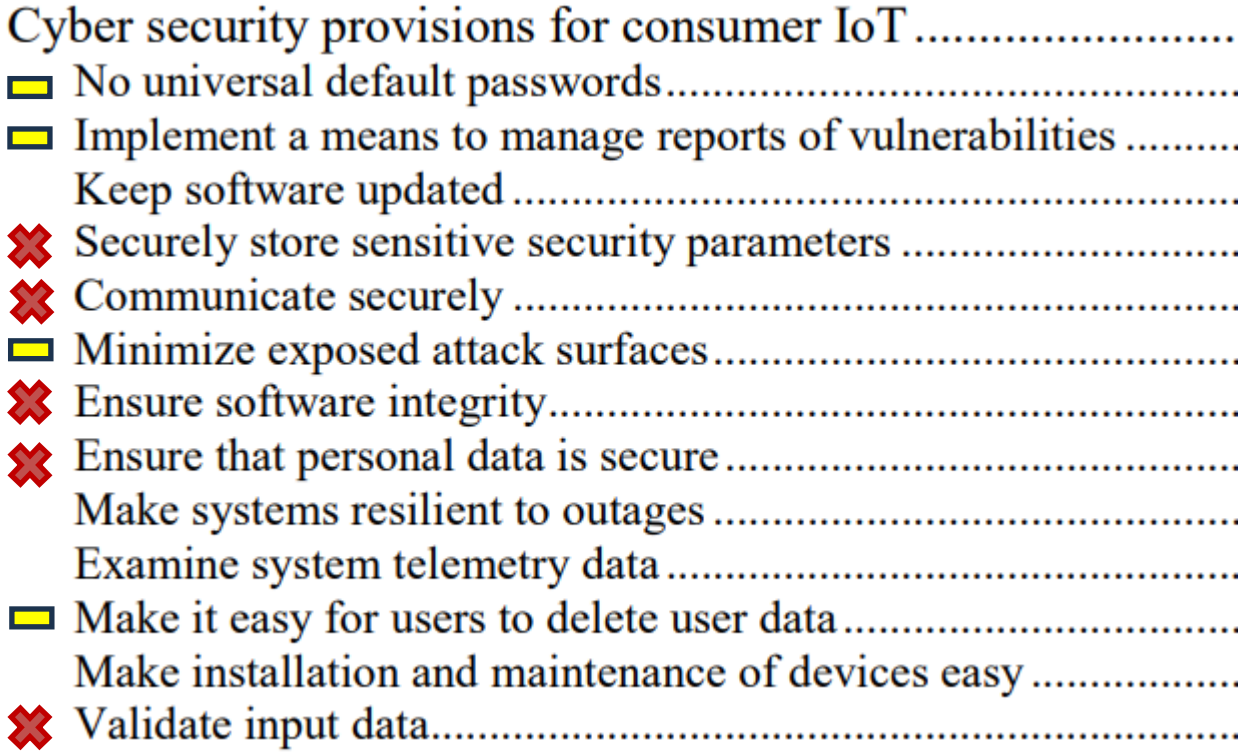
- International standards: ISO/IEC 27001, ETSI EN 303 645
- US standards: NIST Cybersecurity for IoT Program, NISTIR
  - Regional standards: California Consumer Privacy Act, Colorado Privacy Act, etc.

Ecovacs certifications

- Ecovacs boasts multiple security certifications from TÜV Rheinland
  - Standards set by ETSI 303 645 must be met
  - Hardware and software certifications
- Mobile application loading screens advertise ISO/IEC 27001:2013
  - Will be deprecated April 2024

Are standards being met?

- From our research: no, not completely



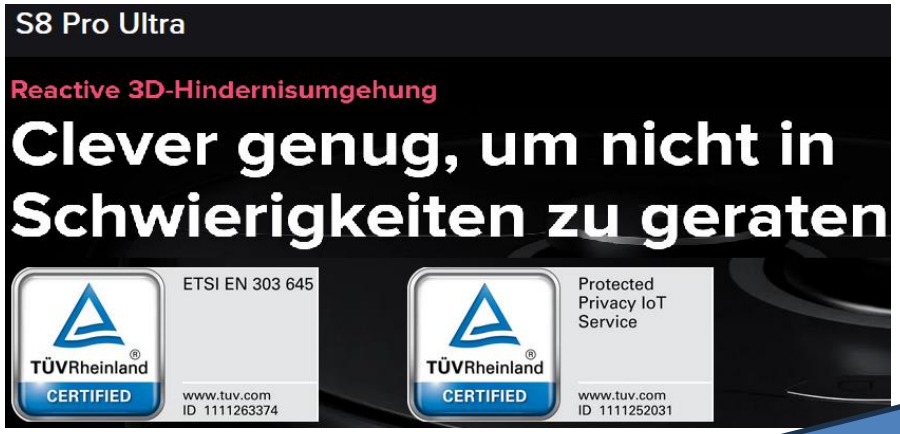
Summary of ETSI 303 645 requirements

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Validity of certifications

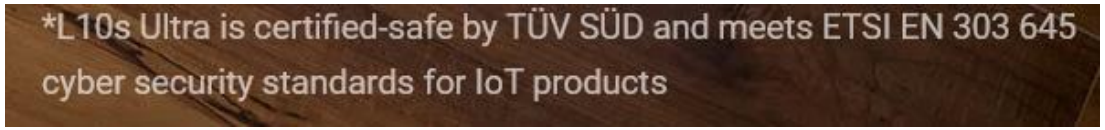
- Should authoritative security certifications exist?
  - ¯_(ツ)_/¯
  - False sense of security for both consumers and vendors
- Pentesters will always miss vulns
  - …but how many would overlook this amount of low hanging fruit?

Can you rely on Certifications?

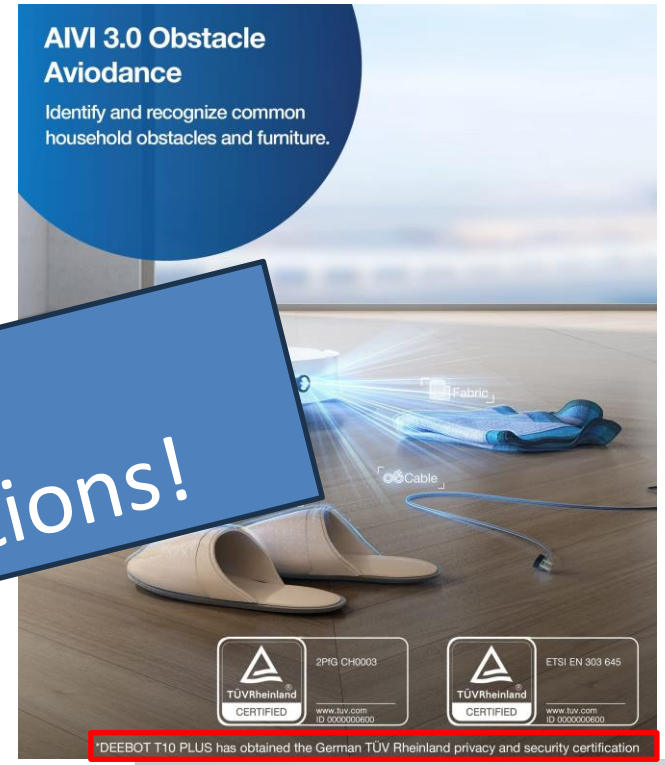


Source: https://de.roborock.com/pages/roborock-s8-pro-ultra

Source: https://www.mi.com/global/product/xiaomi-robot-vacuum-x10-plus/



Source: https://www.dreametech.com/products/dreamebot-l10s-ultra



All Devices and Apps have been compromised regardless of certifications!

Source: Ecovacs iOS application loading screen

Outstanding Astrophotography-grade Camera

The on-board 960P astrophotography camera has a 148.3°* FOV (Field of View) recognition range, enabling it to identify and capture clear images of static and moving objects, even in the dark. Your privacy is important to us, so T10 PLUS will notify you when the camera is on. The product has also obtained both hardware and software TÜV Rheinland privacy and security certification.

Source: https://www.ecovacs.com/global/deebot-robotic-vacuum-cleaner/deebot-t10-plus

TAKE-AWAY LESSONS

Used devices

- Be careful with used devices
  - May come with compromised firmware
  - Difficult to verify
- Do a factory reset before selling/disposing
  - Devices contain a lot of sensitive data
  - Check the manual for a factory-reset
  - Hint: a Wi-Fi reset does not delete any data
  - Warning: even a factory-reset might leave data behind

Choose your partners/roommate wisely

- Devices can be weaponized for stalking
- Remove shared access to accounts
- Change passwords
- When in doubt: do a factory reset and reprovision devices*

Unprovisioned devices

- Do not keep your devices in unprovisioned mode
  - Alternatively: make sure that it disables itself

unprovisioned

„Hey, here are the credentials to MY WiFi“

„Thanks! I am now connected to YOUR account“

„Please give me the Livestream of the camera “

Summary

- We have rooting methods for most released Ecovacs robots
  - Usage of their UART interface and authentication
  - Persistence and operation of custom firmware for some
- We can validate and verify vendors claims
- There are a lot of security and privacy issues
  - Applies to App, Robots and Cloud
  - Certifications did not help to prevent them
- Work allows further research into IoT and AI

Final notes

- Do not use the knowledge for bad things!
- Help others if they need help with rooting.
- If unsure, ask first, before bricking your device.

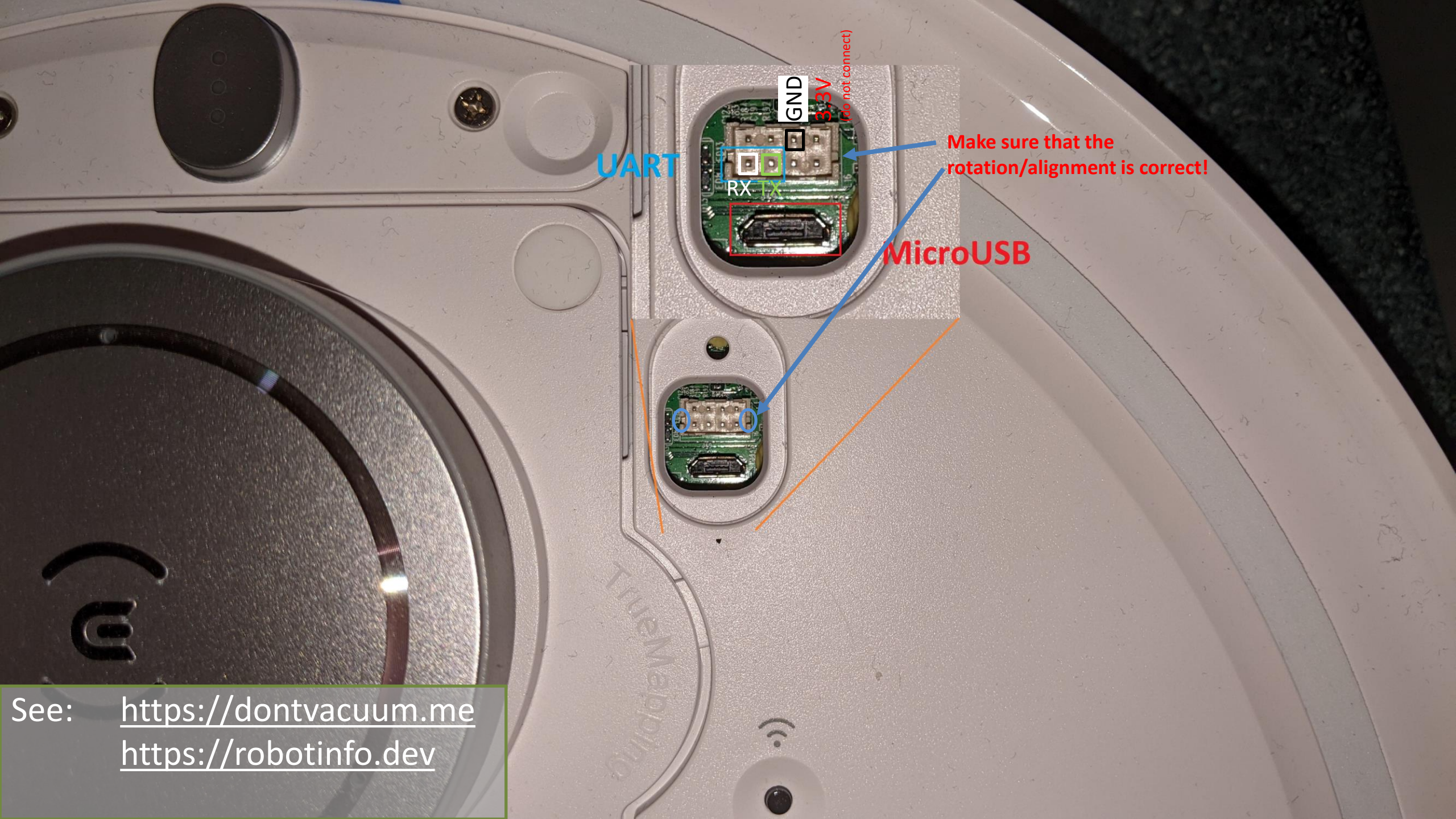
Acknowledgements

- Daniel Wegemer
- Sören Beye (https://twitter.com/hypfer)
- Tihmstar (https://twitter.com/tihmstar)
- Aapo Oksman (https://twitter.com/aapooksman)

- And all the testers in the community!

Contact:

See: http://dontvacuum.me
Telegram: https://t.me/dgiese
Twitter: dgi_DE
Emails: dennis@dontvacuum.me
hi@braelynn.io



See: https://dontvacuum.me
https://robotinfo.dev