

Reverse engineering and hacking Ecovacs robots:
the bad and the really bad
HITCON CMT 2024 – Dennis Giese, braelynn

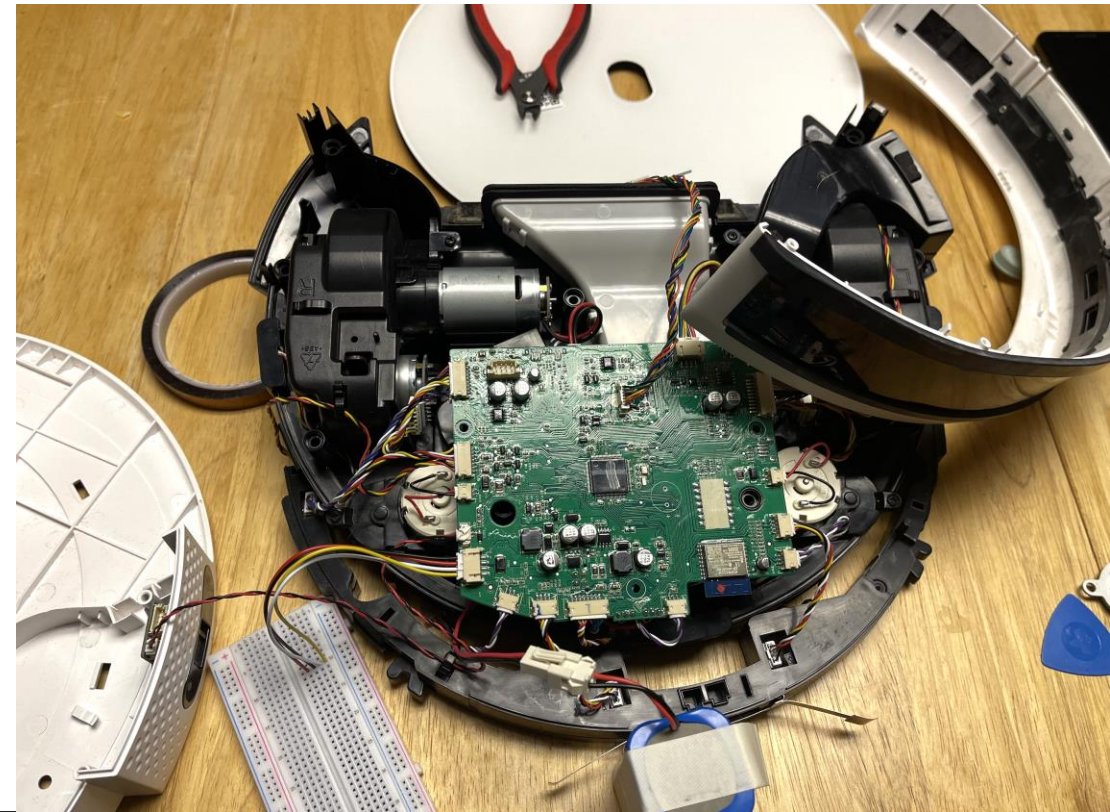
About Dennis

- “Security Researcher” aka Hardware Hacker
 - Research field: Wireless and embedded Security&Privacy
- Interests: Reverse engineering of interesting devices
- Vacuum Robot (and IoT) collector
 - Rooting of vacuum robots
 - <https://robotinfo.dev>



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, Smart locks



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

Past research on robots

- CCC Congress 34C3 (2017)
- HITCON CMT (2018)
- DEFCON 26 (2018)
- DEFCON 29 (2021)
- DEFCON 31 (2023) + CCC Camp 2023
- CCC Congress 37C3 (2023)
- DEFCON 32 (2024)



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 have problems
 - Independent of origin, size, market share
 - This talk: Ecovacs
- Research part of private projects
 - No sponsorship by companies or organizations
 - Any statements are our own opinion 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 DEEBOT T30 *
- 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/only ones researching Ecovacs robots
- The vendor knows about most of our findings
 - ... they tried to fix some and failed
 - ... seem to ignore the worst vulnerabilities until recently*

Shoutout to Chris Anderson
(@0xHexHijinx)

Collaborative effort



@tihmstar and Dennis hacking Robot cameras at NULLCON Goa 2023

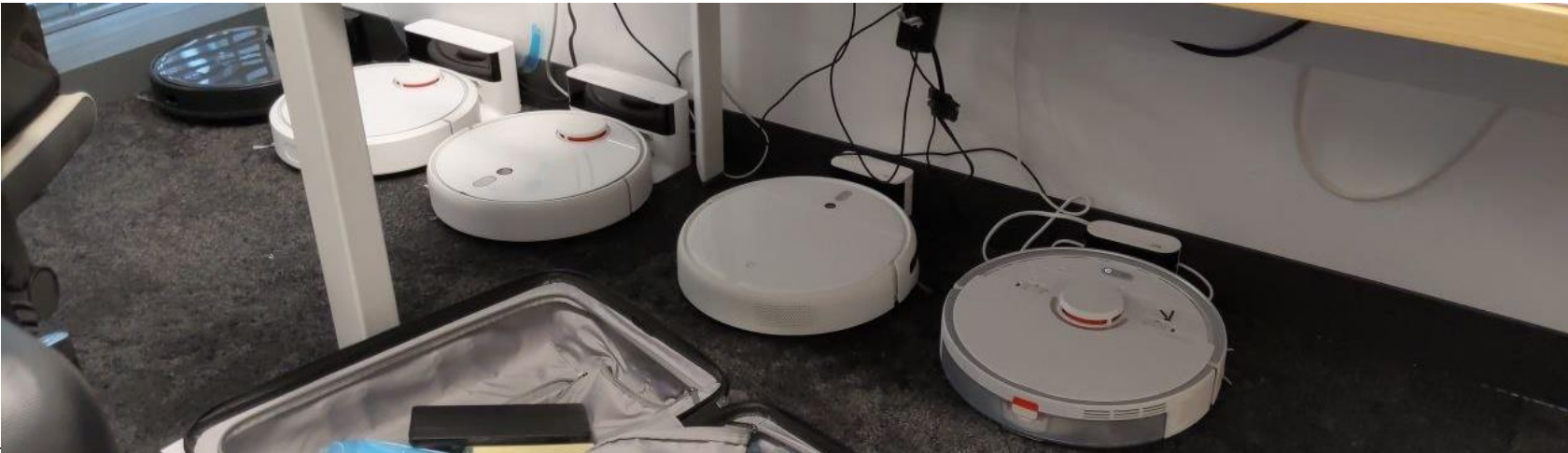


Lawnmower hacking at CCC Camp 2023 in the ZTL/N.O.R.T.x village with Dennis, Maurice, Axel L., Micha B., Mona, Antre (no picture, because forgot to make one :/)

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

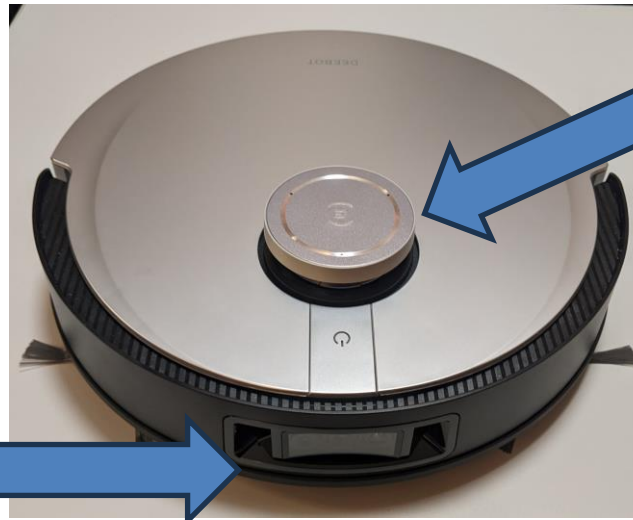


Why do we not trust IoT?

- 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



Cameras



Microphones??



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
- Root access is the only way to verify that a device is „clean“

ARTIFICIAL INTELLIGENCE

A Roomba recorded a woman on the toilet. How did it end up on Facebook

Robot vacuum companies say your images supply chain for data from our d

by **Eileen Guo**
December 19, 2022

In the fall of 2020, gig workers in Venezuela posted photos on social media forums where they gathered to talk shop. The photos captured sometimes intimate, household scenes captured

Bloomberg

• Live Now Markets Economics Industries Tech AI Politics Wealth Pursuits Opinion Business

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/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/>


<https://www.bloomberg.com/news/articles/2022-08-05/amazon-s-irobot-deal-is-about-roomba-s-data-collection#xj4y7vzkg>

Can you rely on Certifications?

S8 Pro Ultra


Reactive 3D-Hindernisumgehung

Clever genug, um nicht in Schwierigkeiten zu geraten



ETSI EN 303 645

www.tuv.com ID 111126374



Protected Privacy IoT Service

www.tuv.com ID 1111252031

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



Independently Tested. Consumer Trusted.

AIR CLEANER SUGGESTED CLOSED ROOM SIZE

545 SQUARE FEET

CLEAN AIR DELIVERY RATE TESTED
The higher the CADR numbers, the faster the units clean the air

TOBACCO SMOKE >352 DUST >384 POLLEN >390

E ECOVACS ROBOTICS - KJ600G-BX11

Ecovacs Robotics Co., Ltd.
No.518 Songwei Road, Wusongjiang Industry Park,
Guoxiang Street, Wuzhong District, Suzhou, Jiangsu, China.

Portable air cleaners are most effective in rooms where all doors and windows are closed. Suggested room size is based on 4.8 Air Changes per Hour.

www.ahamverifide.org

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



Allergy Care

www.tuv.com ID 1111254005



ETSI EN 303 645

www.tuv.com ID 1111249326



2PFG CH0003

www.tuv.com ID 000000600

AIVI 3.0 Obstacle Avoidance

Identify and recognize common household obstacles and furniture.




2PFG CH0003

www.tuv.com ID 000000600



ETSI EN 303 645

www.tuv.com ID 000000600

*DEEBOT T10 PLUS has obtained the German TÜV Rheinland privacy and security certification

Xiaomi Robot Vacuum X10+



ETSI EN 303 645

www.tuv.com ID 1111254930

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

Passed ISO/IEC 27001:2013 Information Security Certification

Protected privacy Certified by TÜV Rheinland

Source: Ecovacs iOS application loading screen

*L10s Ultra is certified-safe by TÜV SÜD and meets ETSI EN 303 645 cyber security standards for IoT products

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

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.




2PFG CH0003

www.tuv.com ID 000000600



ETSI EN 303 645

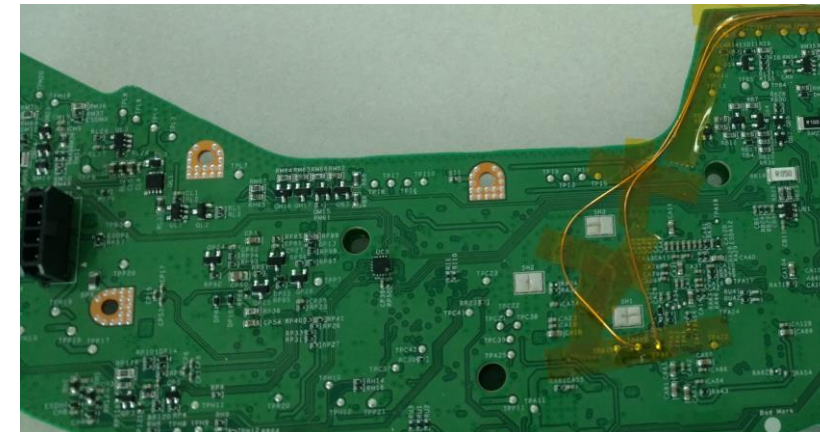
www.tuv.com ID 000000600

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

ROBOT HACKING JOURNEY

First work in 2017

- 34C3 (2017) and DEF CON 26 (2018)
 - Work together with Daniel Wegemer
 - Targets: Xiaomi Vacuum Robot / Roborock S5
 - OTA broken, local updates possible
- Released in 2019
 - Targets: Roborock S6, S5 Max, S7 and others
 - Custom bootloader tool, requiring teardown



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



New rooting methods

- DEFCON29 (2021)
 - Targets: Roborock S6 MaxV, Dreame L10
 - Bypass Secure boot and security features
- DEFCON31 and CCC Camp 2023
 - Targets: Dreame, Roborock, Narwal, Shark
 - Secure Boot bypass thru bootloader magic
- Issue: finding new rooting methods becomes annoying
 - Solution: let's attack a new vendor



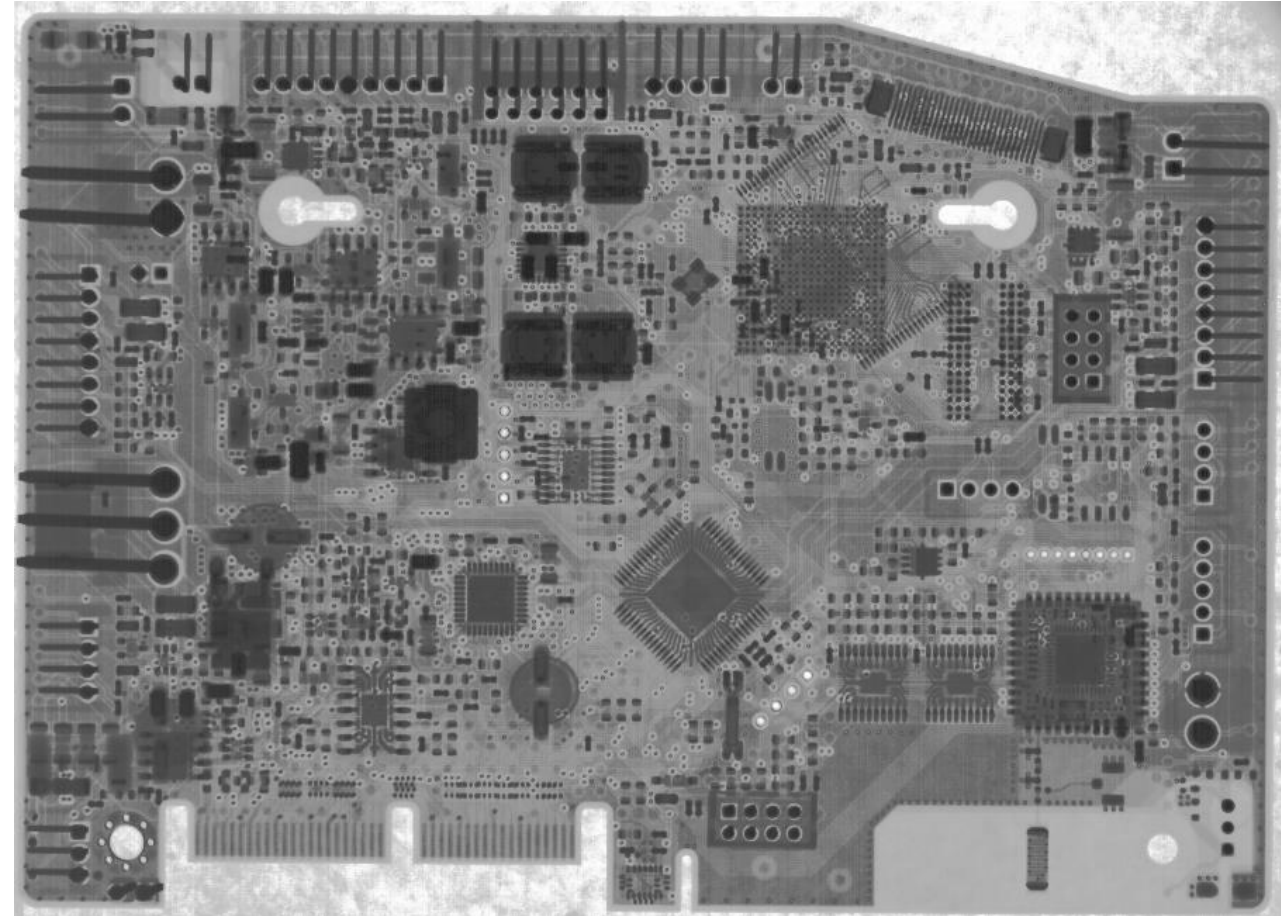
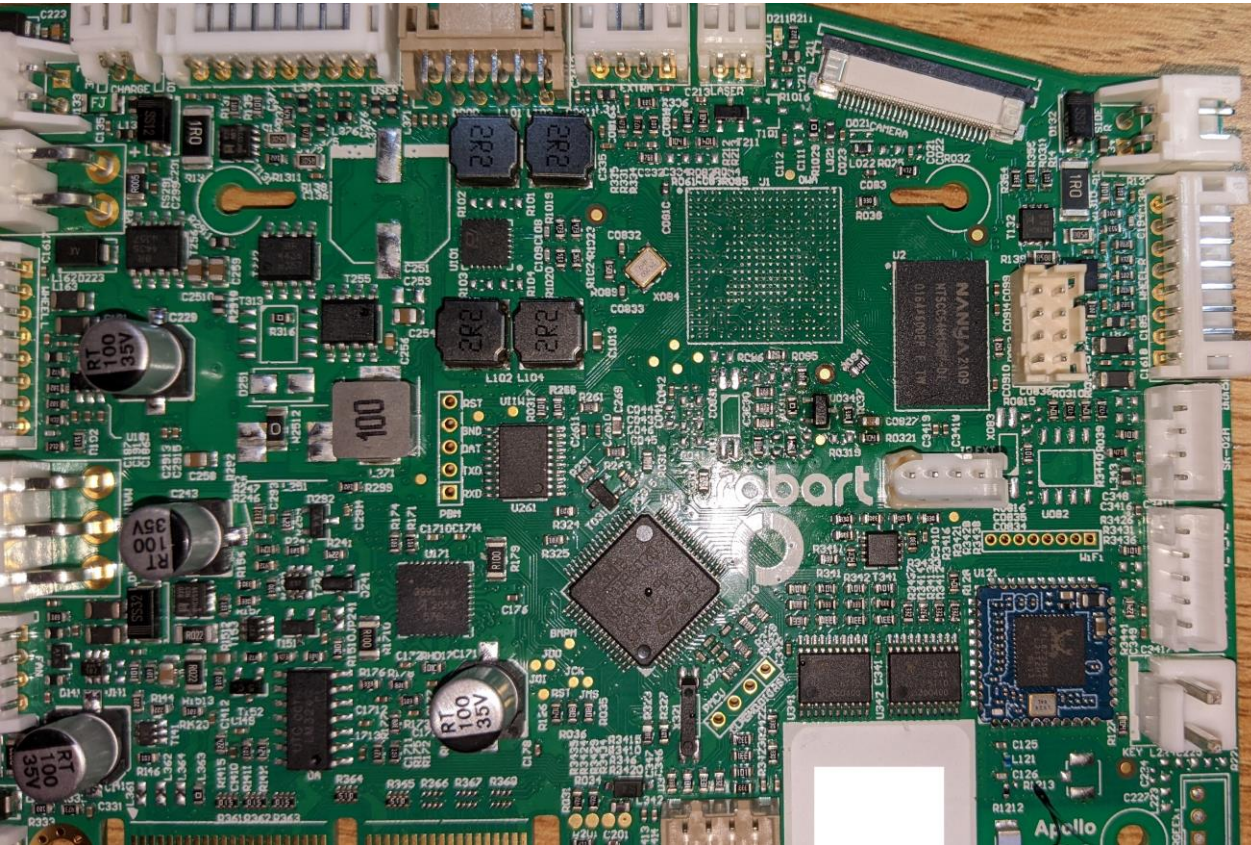
https://dontvacuum.me/talks/DEFCON29/DEFCON29-Robots_with_lasers_and_cameras.html

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
 - Archivement: modified filesystem
- Potential target for more rooting efforts in the future
- Independently: braelynn hacked Ecovacs and Yeedi robots

De-obfuscation of obfuscation With X-Rays

- Example: Shark Robot



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

Products

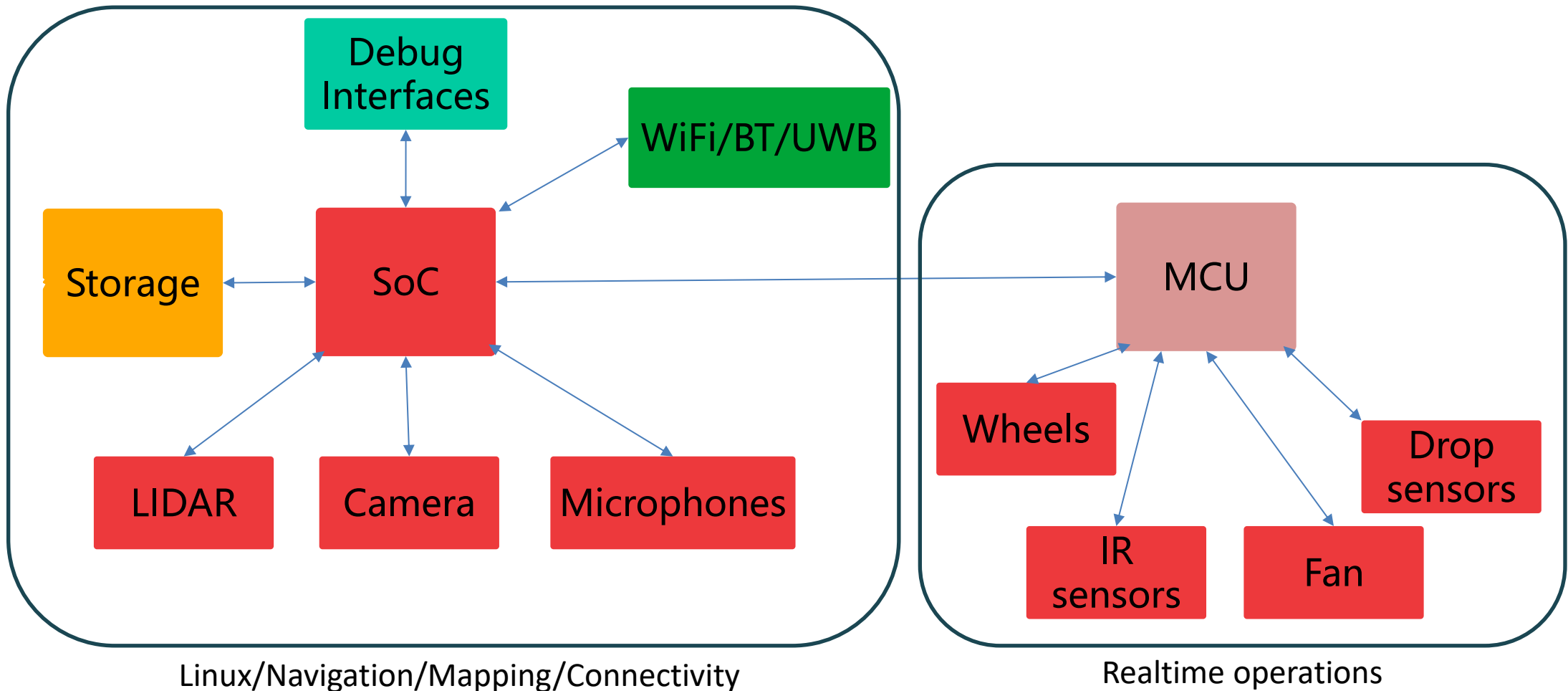


More than 170 SKUs!



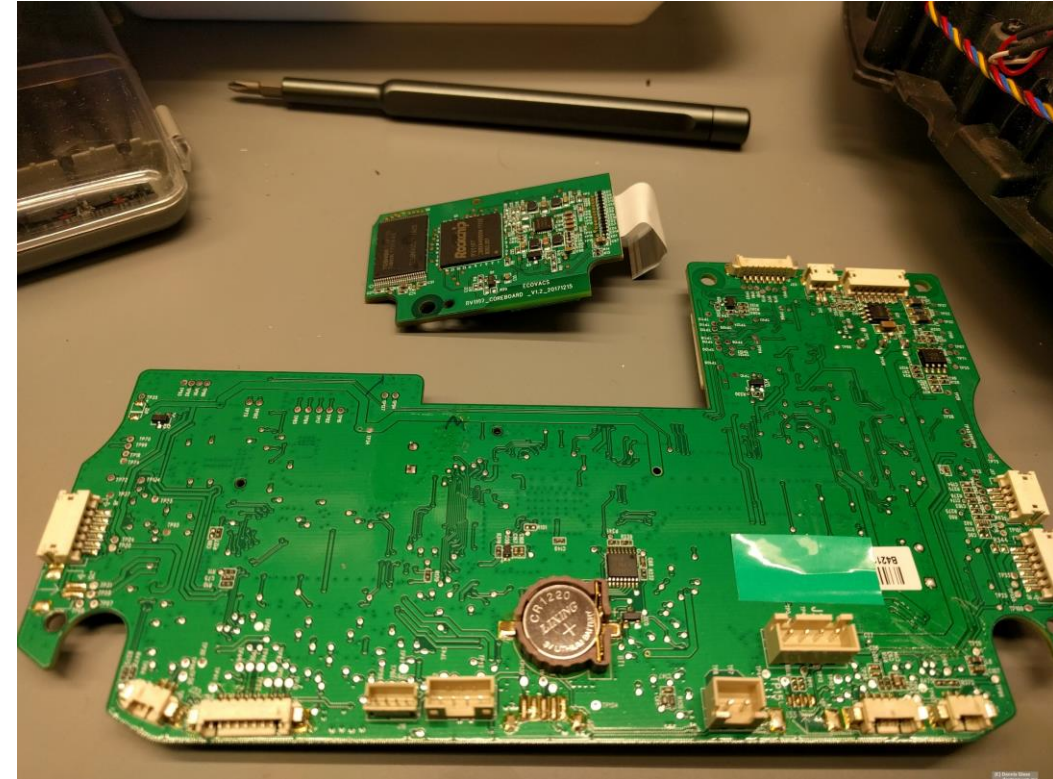
HARDWARE

Hardware



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 hardware: Not interesting for hacking

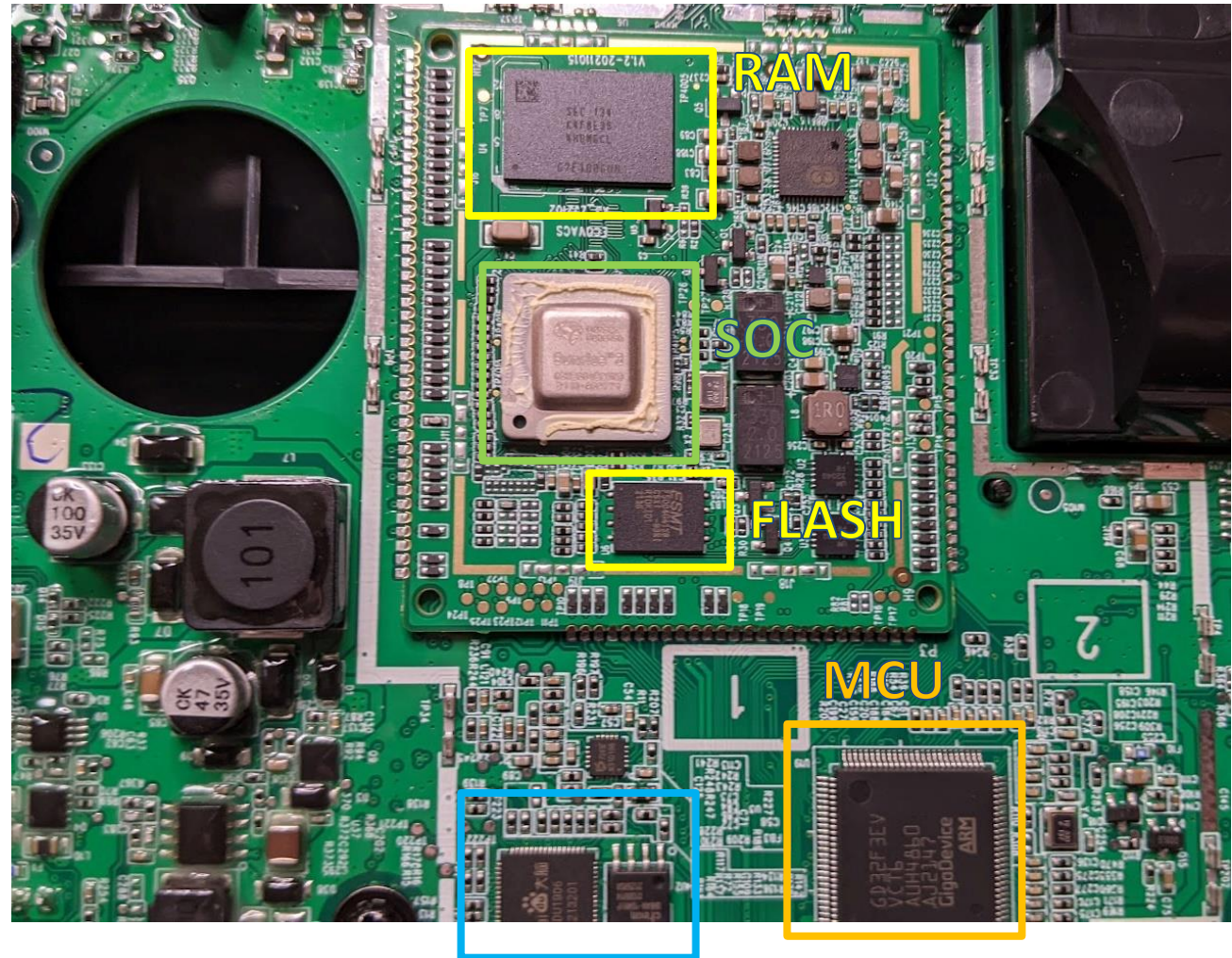
Deebot Vacuum robots

- Interesting and cheap hardware
- Similar hardware for multiple generations
- Example X1
 - Features:
 - Station control
 - Voice assistant
 - Remote view



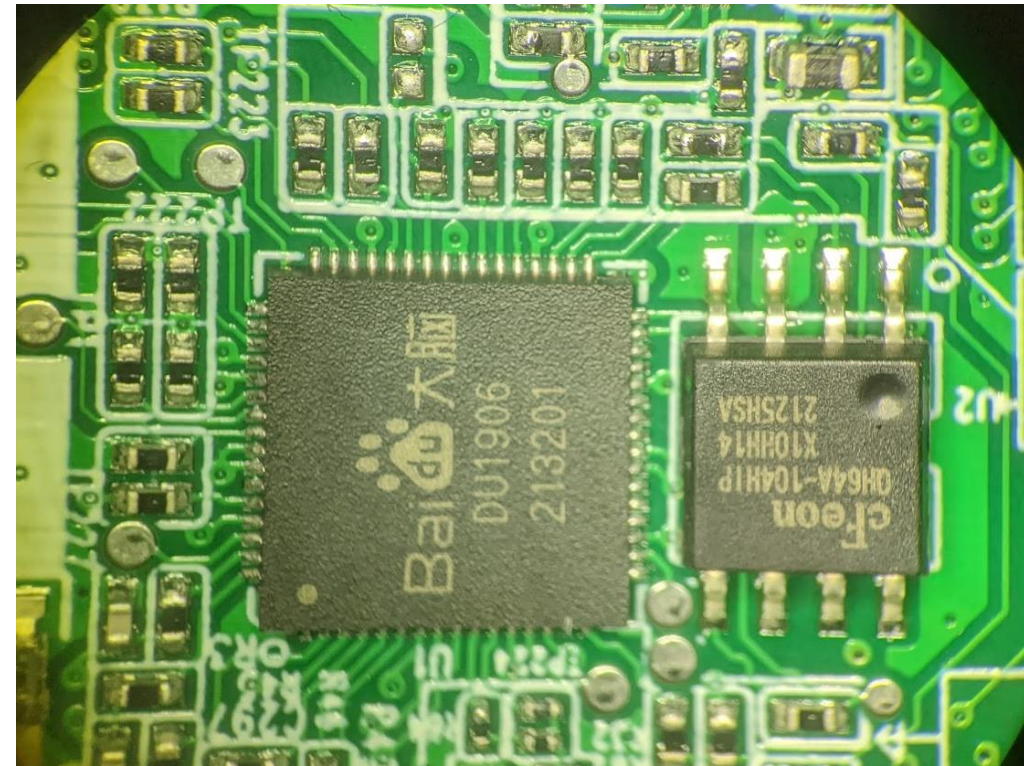
Hardware: Deebot X1

- Same hardware as in X2*
- 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



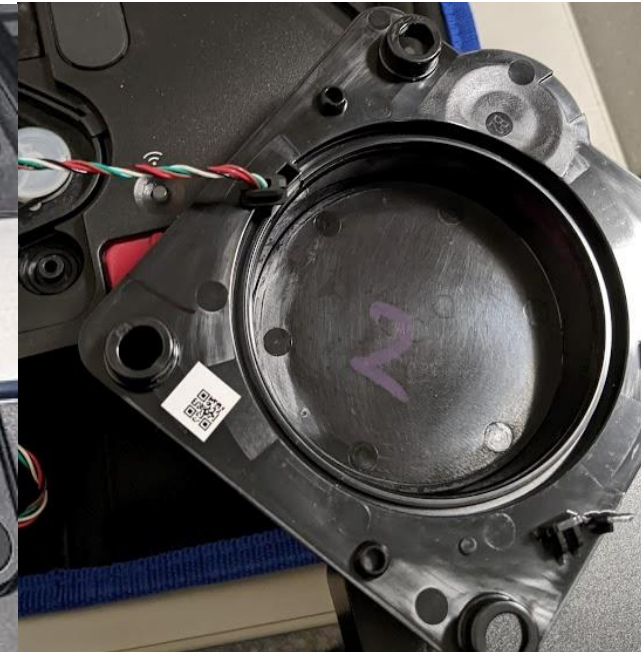
Hardware: Deebot X1

- 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

Fun fact: 2-in-1 robot
Deebot X1 + Deebot 900 serie
Connected via Ethernet



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

Goat G1 Lawnmowing Robot

- Released
 - 2023 in EU, AU
 - 2024 in US (G1-GX)
- Navigation
 - GPS
 - Visual, ToF
 - UWB Beacons
- Features:
 - Optional LTE
 - Remote view/Patrol

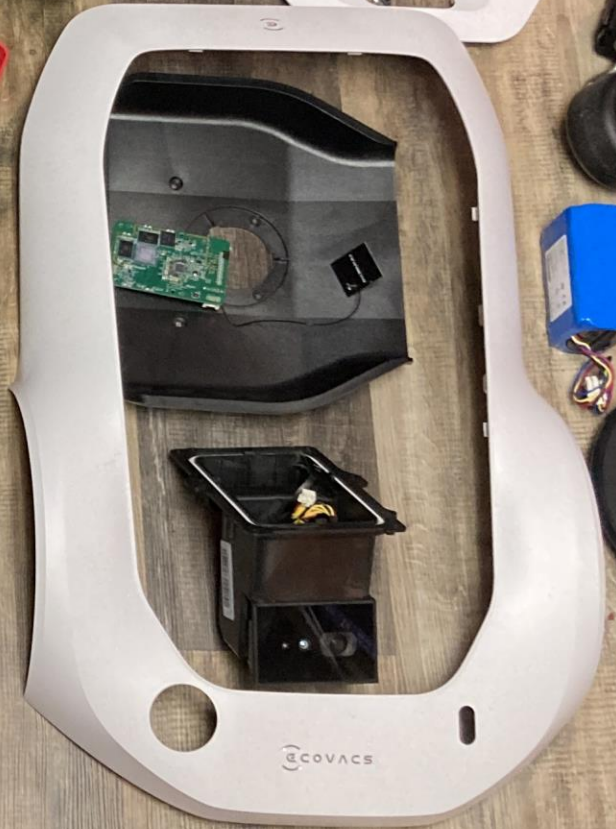
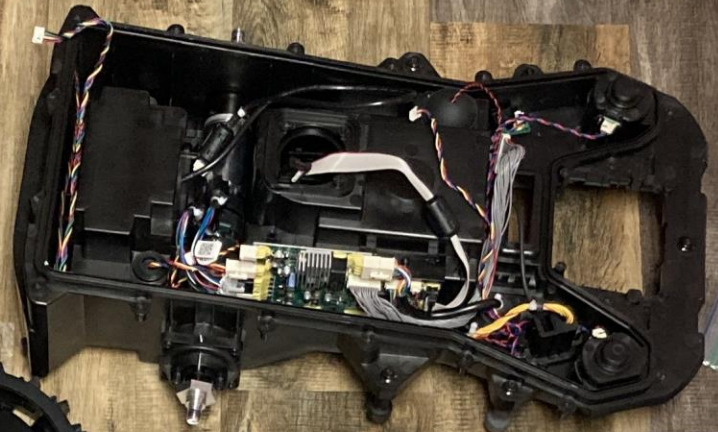


Secure with TÜV Rheinland-certified
data protection.



Reliable Gardening Security

Binocular cameras capture real-time courtyard images to provide all-around protection. Your data stays safe and secure with TÜV Rheinland-certified data protection.



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

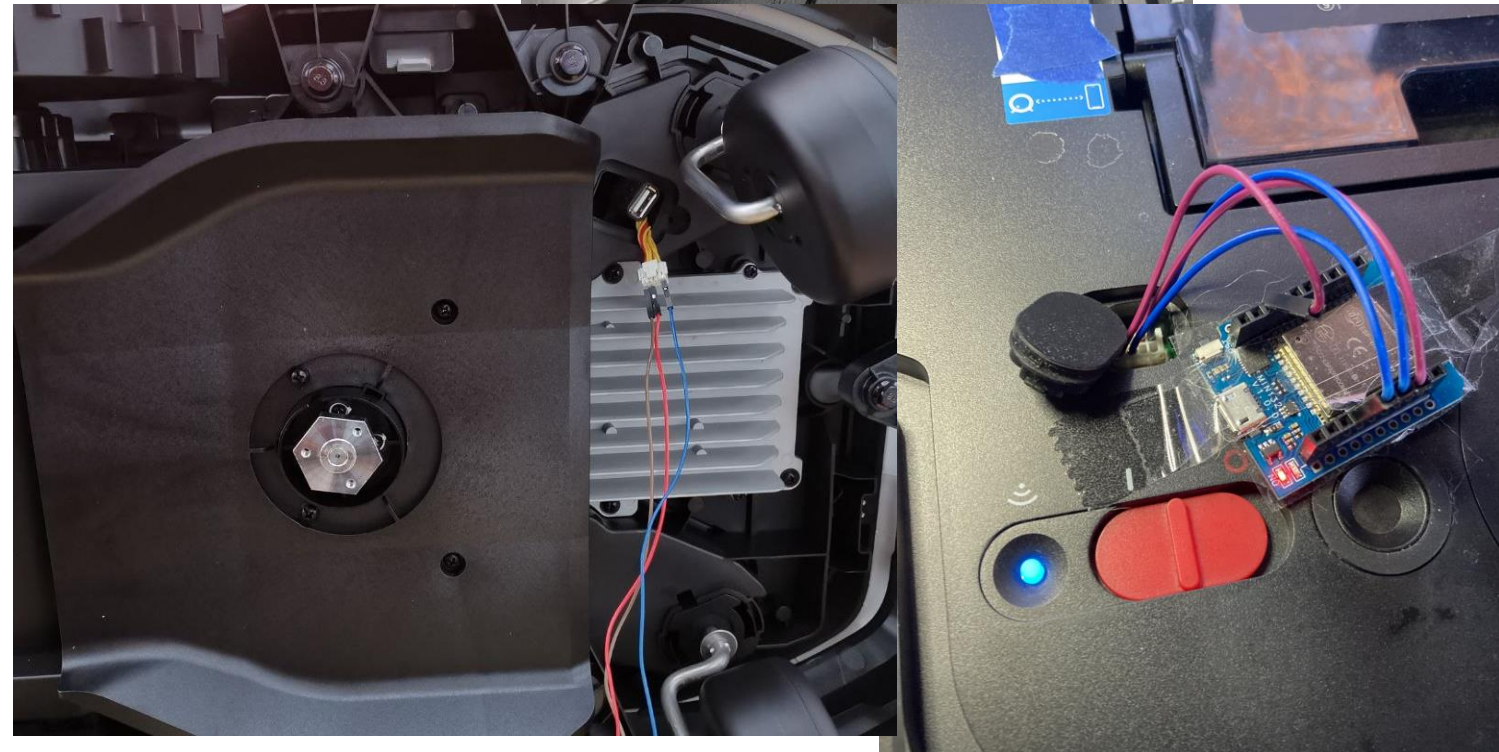
- Sensors
 - 360° Camera (3MP)
 - Front Camera (2MP)
 - ToF Camera
 - Rain detector
 - Bump switches



Debug Ports

- Similar for all models since 2019
- Provides:
 - UART
 - 3.3V
 - SWD
 - USB

Easy to debug and root without breaking warranty seals!



SOFTWARE

Ecovacs Software

- Linux OS
- ROS Melodic Morenia
- Custom Ecovacs software: „Medusa“
- Software packages:
 - Full Python 2.7 environment
 - AWS Kinesis SDK (remote camera access outside of PRC)
 - Alibaba Aliyun SDK (remote camera access inside of PRC)
- Good: little or no protections against rooting



AI models

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

```
"_name": "obj_ErTongFang",  
"_name": "obj_JianShenFang",  
"_name": "obj_YiMaoJian",  
"_name": "obj-TaTaMi",  
"_name": "obj_sandbasin",  
"_name": "obj_bei_bowl",  
"_name": "obj_wan_bowl",  
"_name": "obj_big_shack",  
"name": "obj_sml_shack",  
"_name": "obj_shit",
```

Firmware updates

Ecovacs Deebot X2 Omni (US)

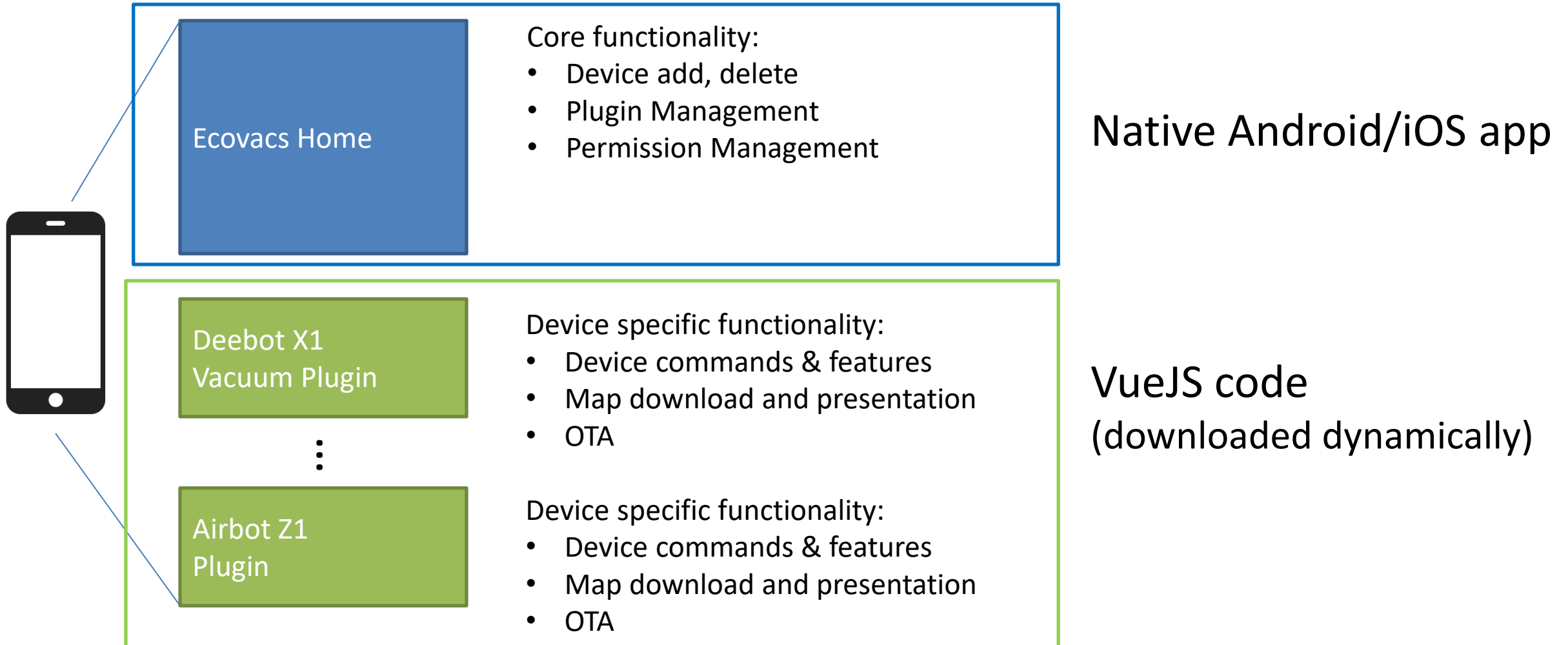
| MD5 | Filename | Version | Datetime | Size |
|----------------------------------|----------------------------------|---------|------------------|------------|
| 0036e1d9f9ebb2851849f648429180e7 | zj2228_fw-1.39.2.bin | 1.39.2 | 21/08/2023 01:42 | 236,02 MB |
| a460c4a940ef5ecd164dc6db75705a60 | 304c1c01012a33751edd4c4b2bcb987c | 1.62.0 | 20/11/2023 02:34 | 217,986 MB |
| aeb41d49fb9d2296a17af64c579e2e61 | 1e39fa53974426404f6bea2fc343f4a8 | 1.70.0 | 29/12/2023 01:20 | 218,327 MB |
| bad05c5a5ca96881cbccf4654cf2e0bb | fdeda7cf4bd1ff216677d37dd4b45f02 | 1.75.0 | 30/01/2024 02:00 | 225,764 MB |
| 326dbf455c7442a1c2e3802485e252a8 | 87014780532514635a5b4aa63710ed95 | 1.76.0 | 22/03/2024 02:26 | 225,764 MB |

← Oct 2023 Release

← Mar 2024 EOL?

| Version | Changelog |
|---------|---|
| 1.39.2 | Fixed known issues and optimized user experience. |
| 1.62.0 | Fixed known issues and optimized user experience. |
| 1.70.0 | Fixed known issues and optimized user experience. |
| 1.75.0 | Fixed known issues and optimized user experience. |
| 1.76.0 | Fixed known issues and optimized user experience. |

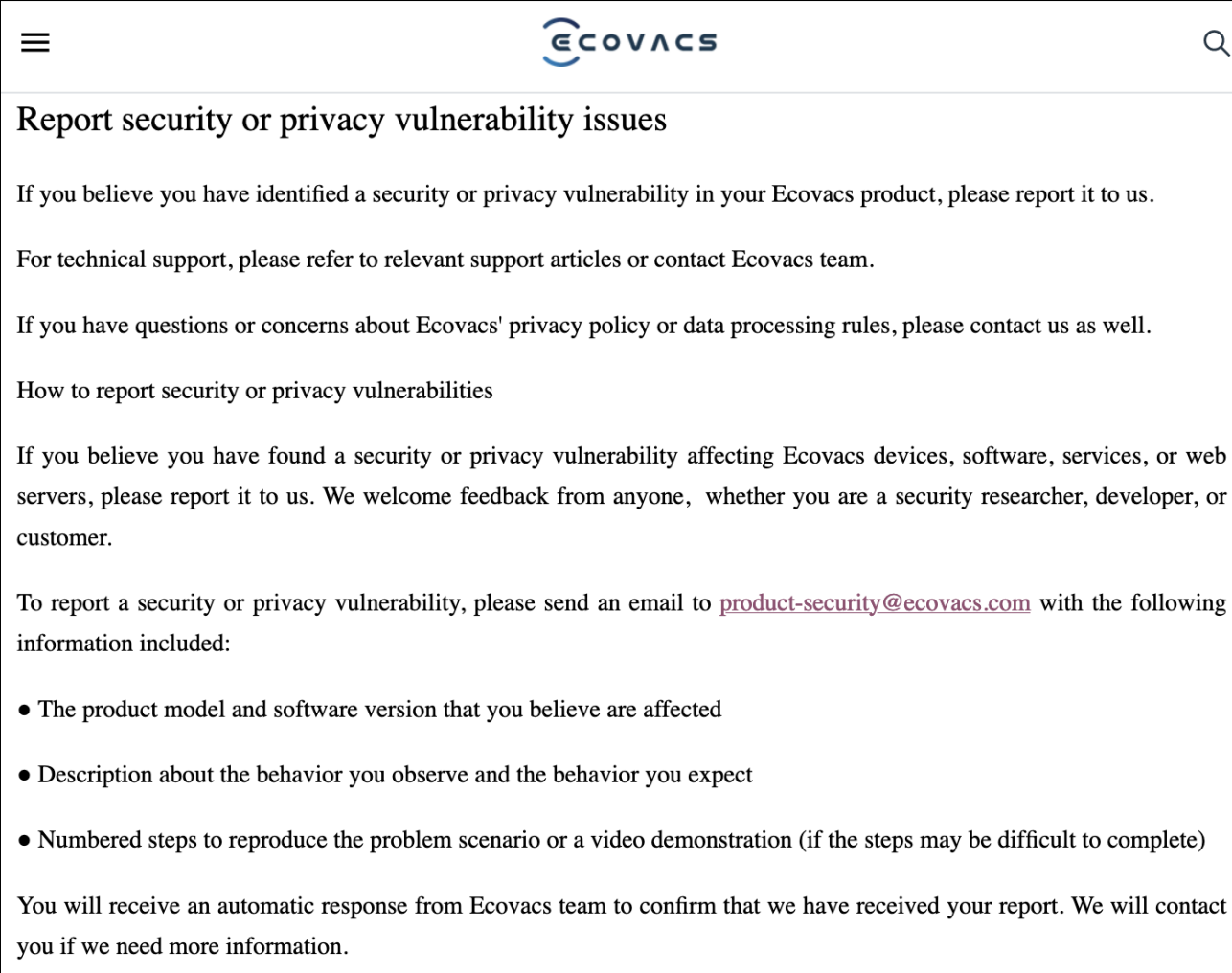
App Structure



SECURITY & PRIVACY

Ecovacs security

- No real, collaborative bug bounty program
 - promises acknowledgement on public bulletin board
 - ...bulletin board doesn't exist?
- Never replied to our reports*
 - Same experience for other researchers
- Some bugs are silently patched



The screenshot shows the top of a web browser displaying the Ecovacs website. The page title is "Report security or privacy vulnerability issues". The content includes instructions on how to report a security or privacy vulnerability, such as sending an email to product-security@ecovacs.com. The page also lists the information required for a report, including the product model and software version, a description of the behavior, and numbered steps to reproduce the problem. The Ecovacs logo is visible in the top right corner of the page.

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.

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?



Ecovacs certifications

- Ecovacs boasts multiple security certifications from TÜV Rheinland
 - Claims to meet ETSI 303 645
 - Hardware and software certifications
- Mobile application loading screens advertise ISO/IEC 27001:2013

Passed ISO/IEC 27001:2013 Information Security Certification
Protected privacy Certified by TÜV Rheinland

Source: Ecovacs iOS application loading screen

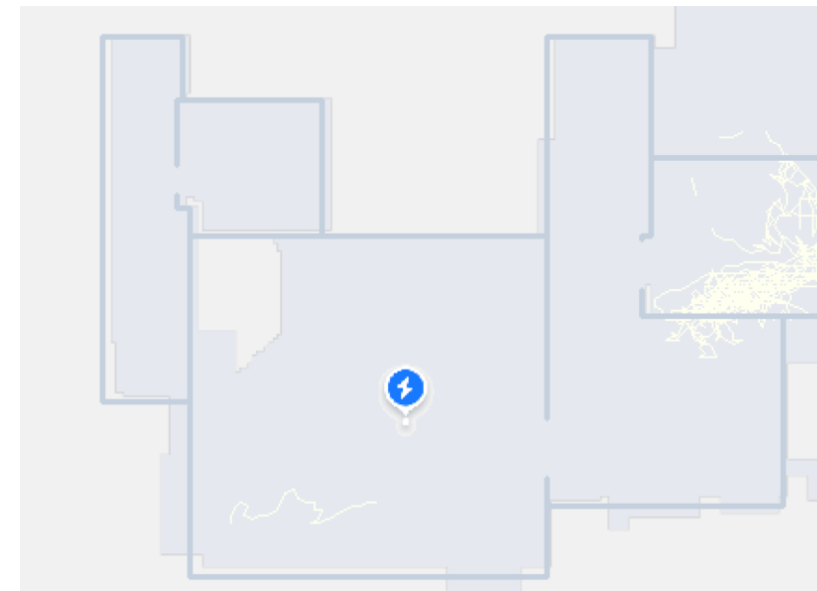
FINDINGS

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



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, Neighbor Wi-Fi access points
 - “Hello Yiko” traffic logs
- Factory reset: does not fully erase all information
 - Sensitive log files remain
 - Additional problem: flash wear leveling

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

TLS sadness in the App

- Ecovacs Home app correctly checks certificates
 - However, the robot-specific plugins don't always do
- Plugins accept self-signed certificates
 - Risk in insecure Wi-Fi networks, e.g. Airport, Hotels
 - 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 Robot

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

```
CRITICAL - [redacted]: 13.56.199.251:443:api-ngiot-[redacted].area.robotwv.ecouser.net for test real_cert_dustca intercepted data = 'b'POST /api/idi/data_collect/upload/generalData?auth.with=device&auth.name=[redacted]&auth.mid=[redacted]&auth.res=9UEt&auth.ts=[redacted]&auth.sign=[redacted]&rn=aiCalibrationFile&meta=%7B%22device_info%22:%20%7B%22product%22:%22zj2228%22,%22fw%22ts%22:%22[redacted]2%22%7D,%20%22data_info%22:%20%7B%22files%22:%5B%22AI_para.txt%22,%22distance_table%22,%22inner.json%22%5D%7D%7D&fmt=b&dType=bin HTTP/1.1\r\nHost: api-ngiot-[redacted].area\r\nUser-Agent: curl/7.64.0\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Length: 25200\r\nExpect: 100-continue\r\n\r\n
```

```
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
```

```
...
```

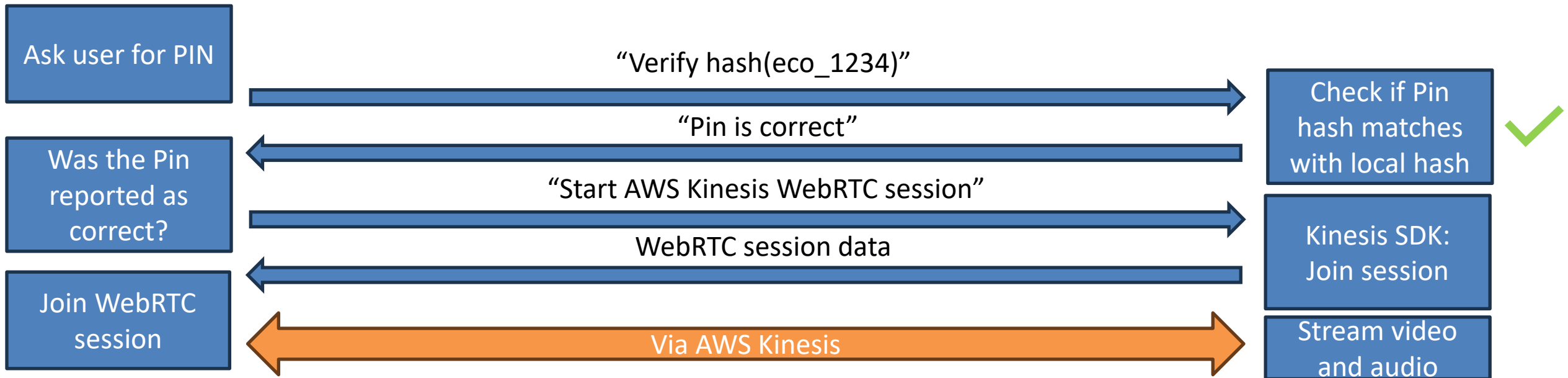
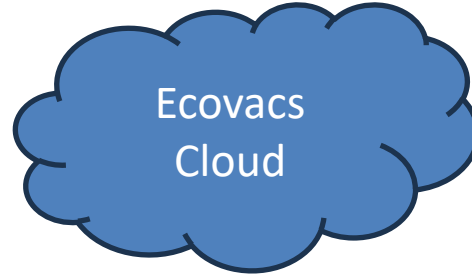
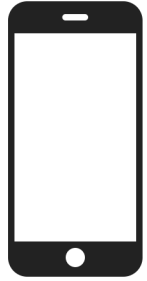
Sneaky live video

- 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

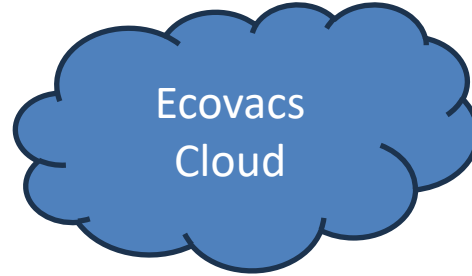
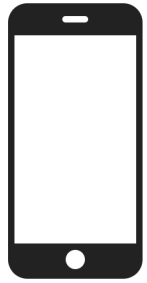
Live video ap(p)ocalypse

- App allows live audio+video access on robot
 - Functionality provided by AWS Kinesis
- Owner and shared users can access feature
- 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



Live video ap(p)ocalypse



PIN
1234

Ask user for PIN

“Verify hash(eco_1235)”

Check if Pin hash matches with local hash

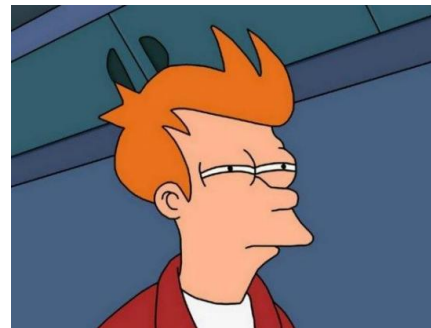


“Pin is incorrect”

Was the Pin reported as correct?

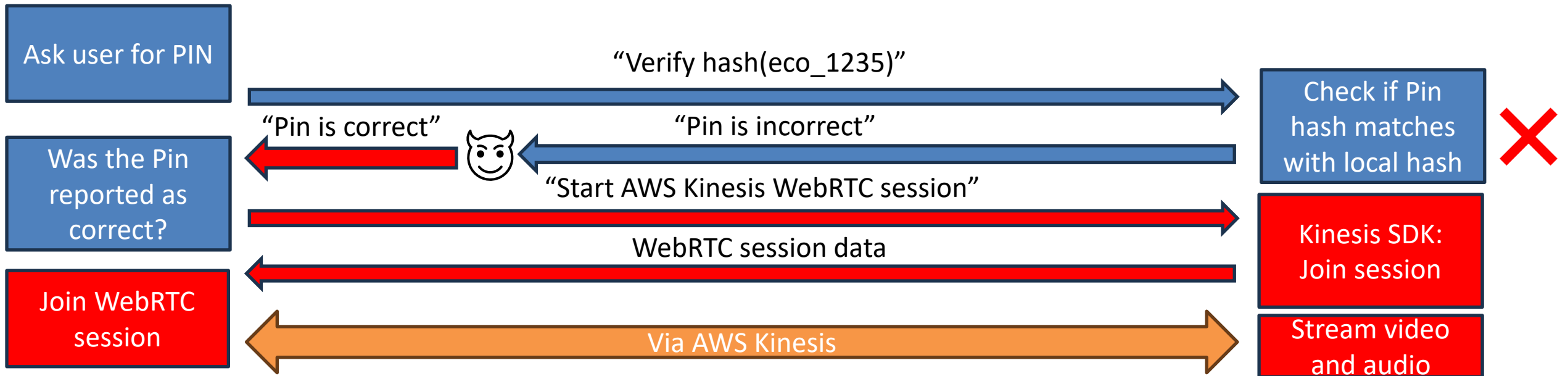
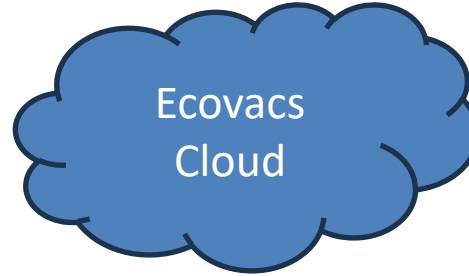
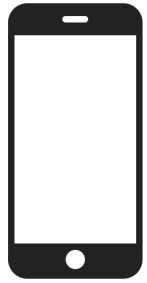


Show error „Wrong pin!”

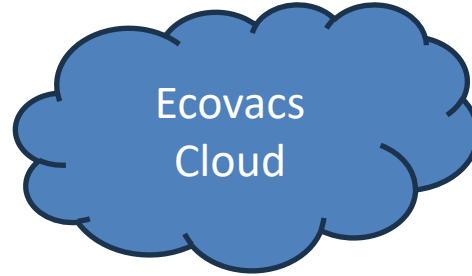
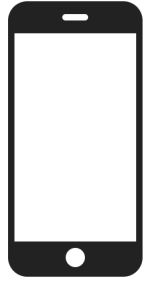


Are PIN verification and WebRTC tied together?

Live video ap(p)ocalypse



Live video ap(p)ocalypse



Not caring about any PIN

“Start AWS Kinesis WebRTC session”

WebRTC session data

Kinesis SDK:
Join session

Join WebRTC session

Via AWS Kinesis

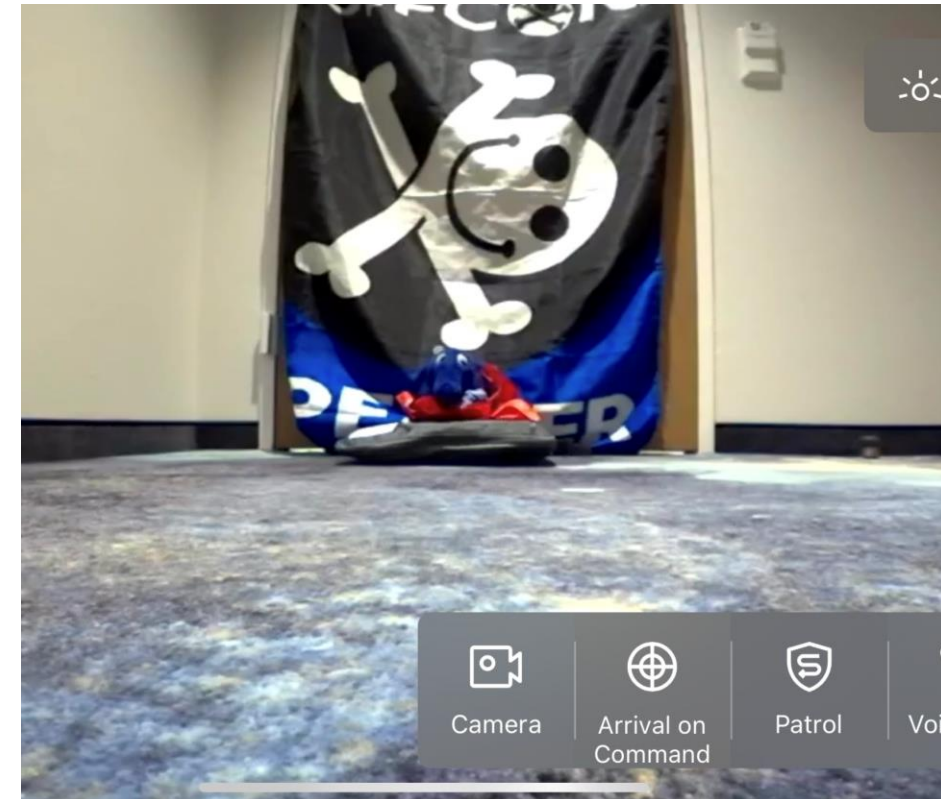
Stream video and audio

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

Live video ap(p)ocalypse

- PIN protection implemented in app
 - 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

- Reported in 2023
- Unsuccessful fix pushed
 - some plugins updated
 - no firmware fixes
- Downgraded app still works

The image shows two side-by-side screenshots. The left screenshot is from Burp Suite Community Edition v2023.10.3.5, displaying the HTTP history and proxy settings. The right screenshot is from a mobile app interface for a DEEBOT X1 TURBO robot, showing a status bar and buttons for 'Enter Smart Cleaning' and 'Enter Video Manager'.

Burp Suite HTTP History Table:

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type |
|-----|-------------------------------------|--------|---------------------------------------|--------|--------|-------------|--------|-----------|
| 993 | https://api-app.dc-eu.w... | POST | /api/appsvr/app.do | ✓ | | 200 | 322 | JSON |
| 992 | https://sa-eu-datasink.ecovacs.c... | POST | /sa?project=production | ✓ | | 200 | 145 | text |
| 991 | https://api-app.dc-eu.w... | POST | /api/appsvr/app.do | ✓ | | 200 | 319 | JSON |
| 990 | https://sa-eu-datasink.ecovacs.c... | POST | /sa?project=production | ✓ | | 200 | 145 | text |
| 989 | https://api-app.dc-eu.w... | POST | /api/iot/devmanager.do?mid=2o4lnm&... | ✓ | | 200 | 259 | JSON |

Match and replace rules table:

| Item | Match | Replace |
|----------------|------------------------------|---|
| Response body | "code":10001,"msg":"pwd i... | "code":0,"msg":"ok" |
| Request header | ^User-Agent.*\$ | User-Agent: Mozilla/4.0 (compatibl... |
| Request header | ^User-Agent.*\$ | User-Agent: Mozilla/5.0 (iPhone; CP... |
| Request header | ^User-Agent.*\$ | User-Agent: Mozilla/5.0 (Linux; U; A... |
| Request header | ^If-Modified-Since.*\$ | |
| Request header | ^If-None-Match.*\$ | |
| Request header | ^Referer.*\$ | |

Bluetooth remote code execution

- Newer vacuum robots and all lawn mowing robots use BLE for provisioning
 - Lawnmowers: BT is always active
 - Vacuums: BT is active for 20 minute after booting / daily reboot
- Communication between app and robots via GATT protocol
 - Payload encrypted with static AES key such as “12345678ecovacs”
 - Input validation is... insufficient

These devices have
cameras and
microphones

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.



BLE RCE payload creation

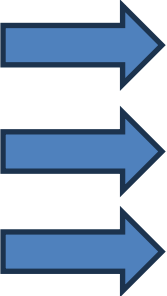
- Command for execution: `“/etc/rc.d/play_boot_music.sh start”`
- Embedding in JSON payload
- Generation of encrypted payload
- **6046507365744E657450696E003100303030300030303031004361320071004
B6944006ABD4D5CBF917DA0EDEF04AD99A5462325DF036E9E934D524E43F9
B0D43E5CF6CC1F06DF5AAB803F1BFBD4C5E338DCE48C9B6EBA5C507602051
8A4A9367F5F8244D7DF78B91EB6C6BCEBC940F2AEDFBC97CF0A**

Link to the payload and more info:
<https://dontvacuum.me/talks/HITCON2024>

BLE RCE payload execution

- Robot software receives payload and decrypts it
- Parsing of payload and extraction of “foo”
- Generation of command line, transmit “foo” via environment variable
- **‘foo=’; /etc/rc.d/play_boot_music.sh start; ’ /usr/bin/somestuff’**
- Execution of command line

We tested this with 50 meters distance (165ft).



```
bar = JsonObjectGetString(v1, "foo");  
snprintf(&command, 256LL, " foo =\"%s\" %s", bar , " /usr/bin/somestuff ");  
(unsigned int)popen((__int64)&command, (__int64)&v16, 1024LL)
```

BLE RCE video demo (Target: Goat G1)



BLE RCE live demo (Target: X2)

Robot worm scenario



ROOTING

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 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 and well hidden
- 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
- Forgotten Autostart feature
 - Check if „/data/autostart“ exists
 - Run any .sh scripts in that folder
- Surviving factory resets
 - Factory resets delete* all files from /data
 - Idea: make file immutable with “chattr”


TAKE-AWAY LESSONS

Can you rely on Certifications?

S8 Pro Ultra


Reactive 3D-Hindernisumgehung

Clever genug, um nicht in Schwierigkeiten zu geraten



ETSI EN 303 645

www.tuv.com ID 1111263374




Protected Privacy IoT Service

www.tuv.com ID 1111252031

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

Xiaomi Robot Vacuum



ETSI EN 303 645

www.tuv.com ID 1111254930

2013 Information Security Certification

Protected privacy Certified by TÜV Rheinland

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

*L10s Ultra is certified-safe by TÜV SÜD and meets ETSI EN 303 645 cyber security standards for IoT products

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

CE

AI-HAM VERIFIDE Independently Tested. Consumer Trusted.

AIR CLEANER SUGGESTED CLOSED ROOM SIZE **545 SQUARE FEET**

CLEAN AIR DELIVERY RATE TESTED
The higher the CADR numbers, the faster the units clean the air

TOBACCO SMOKE DUST POLLEN

352 384



Allergy Care

www.tuv.com ID 1111254005



ETSI EN 303 645

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>


AIVI 3.0 Obstacle Avoidance

Identify and recognize common household obstacles and furniture.

2PIG CH0003

www.tuv.com ID 2000003950



ETSI EN 303 645

www.tuv.com ID 3000003950

*DEEBOT T10 PLUS has obtained the German TÜV Rheinland privacy and security certification




2PIG CH0003

www.tuv.com ID 2000003950

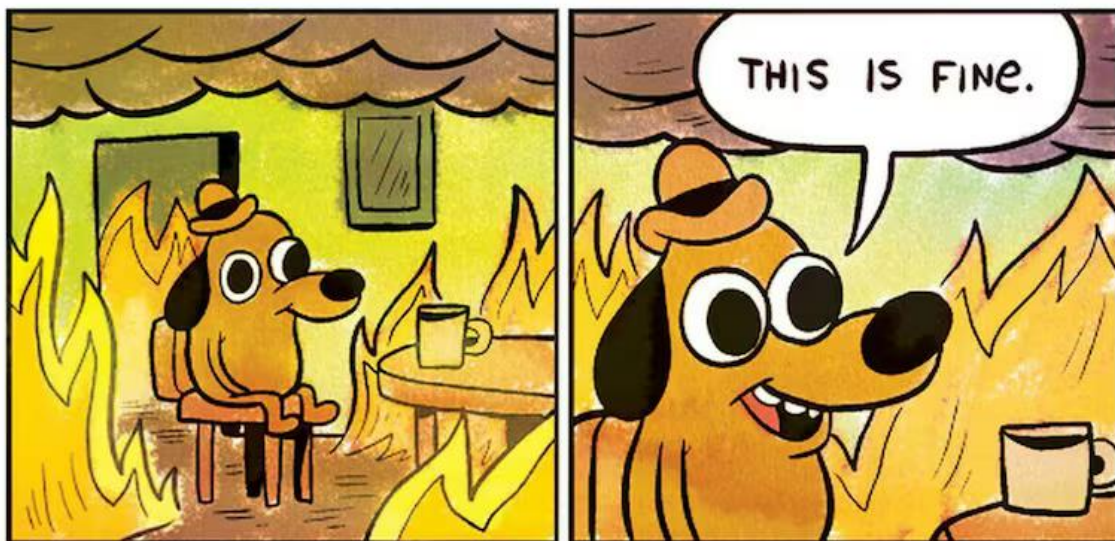


ETSI EN 303 645

www.tuv.com ID 3000003950

Ecovacs response

- Attacks are very hard
- Don't worry, everything is fine



KC Green



Lorenzo Franceschi-Bicchierai

@lorenzofb

Finally, Ecovacs responds to the researchers' findings, saying it won't fix the bugs.

"Users can rest assured that they do not need to worry excessively about this," Ecovacs said in a statement. (Including the whole statement here.)

techcrunch.com/2024/08/09/eco...

ECOVACS places the highest priority on data security and customer privacy. To address the issues raised by Dennis Giese and Braelynn, the ECOVACS Security Committee has initiated an internal review process of network connections and data storage. Following this comprehensive internal review, it has been concluded that security issues pointed out by Giese and Braelynn are extremely rare in typical user environments and require specialized hacking tools and physical access to the device. Therefore, users can rest assured that they do not need to worry excessively about this. Nevertheless, we remain committed to proactively improve our products based on our review findings, as we have always done.

ECOVACS respects the practice of security experts who identify potential vulnerabilities through research and proactively share their findings with companies. We believe that the interaction between security experts and companies, through offensive and defensive testing and the publication of results, contributes to the improvement of product security.

ECOVACS has always prioritized product and data security, as well as the protection of consumer privacy. We assure customers that our existing products offer a high level of security in daily life, and that consumers can confidently use ECOVACS products.

Regards,
ECOVACS Security Committee

11:33 AM · Aug 14, 2024 · 7,589 Views

<https://twitter.com/lorenzofb/status/1822002515279270079>

Ecovacs damage control

- Direct email to us (16.08.2024)
 - Acknowledged that email to product security team from December 2023 was overlooked
 - “conducted an in-depth verification and self-examination”

Ecovacs damage control

- BLE RCE for Ecovacs Goat G1
 - Implementation of "securer authentication mechanism", proper encoding and command validation. OTA by next week
- Video PIN Bypass:
 - "Client-based authentication is not so secure", "Server or Robot-based authentication will be implemented" (next week)
- broken TLS certificate verification, token leak:
 - "plan to strengthen ECOVACS HOME app security in several upcoming product updates"

<https://techcrunch.com/2024/08/22/ecovacs-says-it-will-fix-bugs-that-can-be-abused-to-spy-on-robot-owners/>

Vulnerable devices and apps

- Devices with vulnerable BLE devices
 - Impacts Goat lawnmower, X2 derived devices
 - Turn off devices when not in use
 - Wait for firmware update and fix
- Devices that do not use BLE
 - Do not update firmware if you want to keep root access
- Vulnerable apps
 - Do not connect to insecure/untrusted WiFi APs

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
 - Warning: even a factory-reset leaves 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*

Summary

- We have root for most released Ecovacs robots
 - Usage of their UART interface and authentication
 - BLE RCE to get initial access
 - 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

Acknowledgements:

Daniel Wegemer

Chris Anderson (<https://twitter.com/0xHexHijinx>)

Sören Beye (<https://twitter.com/hypfer>)

Tihmstar (<https://twitter.com/tihmstar>)

Aapo Oksman (<https://twitter.com/aapooksman>)

Contact:

See: <http://dontvacuum.me>

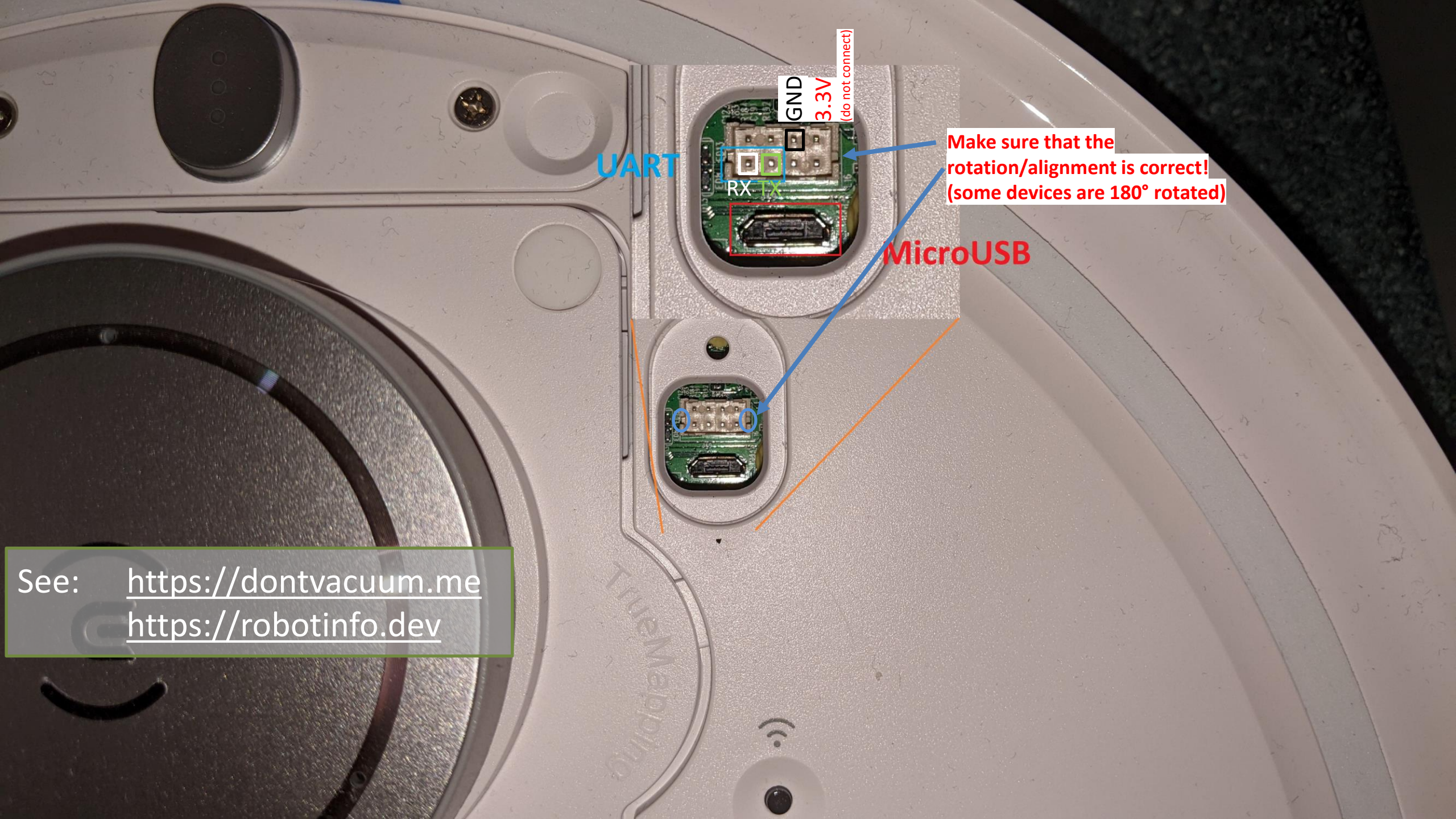
Telegram: <https://t.me/dgiese>

Twitter: dgi_DE

Emails: dennis@dontvacuum.me

hi@braelynn.io





UART

GND
3.3V
(do not connect)

RX TX

Make sure that the rotation/alignment is correct!
(some devices are 180° rotated)

MicroUSB

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

True Mapping