Ecovacs robot vacuums get hacked

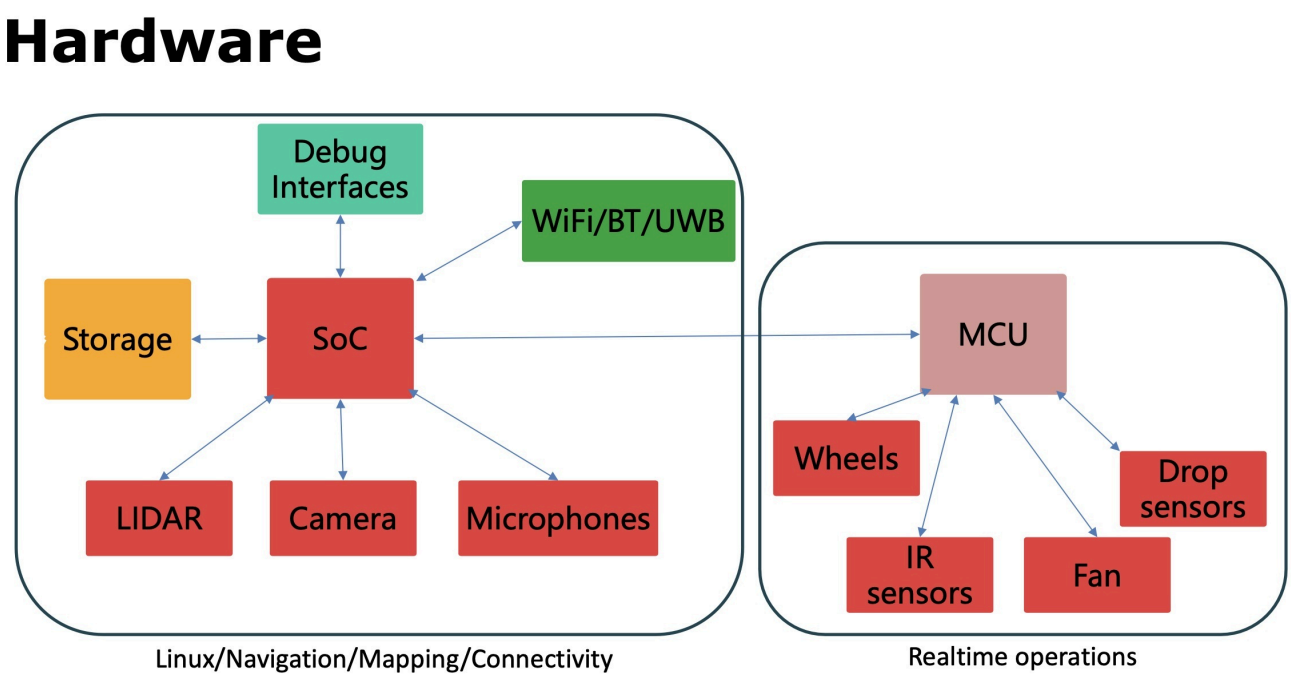
Kaspersky Team

Imagine: you get up in the night for a glass of water, walk across the unlit landing, when out of the darkness a voice starts yelling at you. Not nice, you'd surely agree. But that's the new reality for owners of vulnerable robot vacuums, which can be commanded by hackers to turn from domestic servants into foul-mouthed louts. And that's not all: hackers can also control the robot remotely and access its live camera feed.

The danger is clear and present: recently, cases of cyberhooligans hijacking vulnerable robot vacuums to prank people (and worse) have been seen in the wild. Read on for the details…

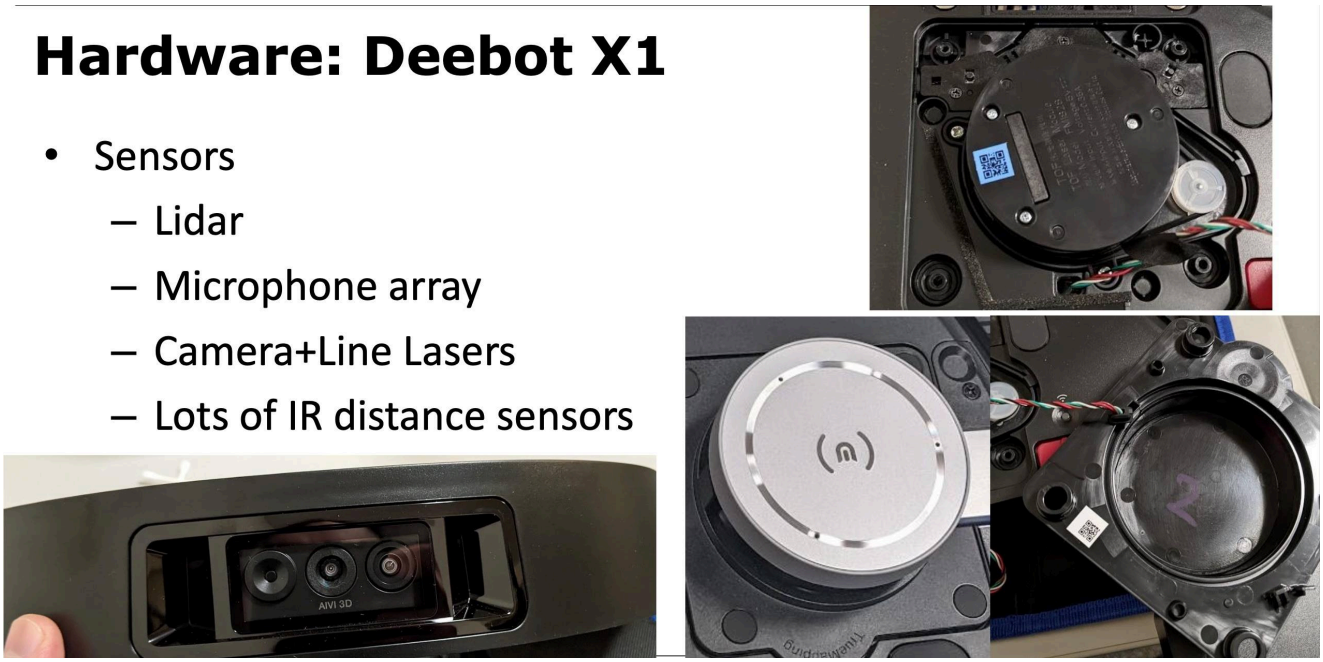
How a robot vacuum works

Let's start with the fact that a modern robot vacuum is a full-fledged computer on wheels, usually running on Linux. It comes with a powerful multi-core ARM processor, a solid chunk of RAM, a capacious flash drive, Wi-Fi, and Bluetooth.



Today’s robot vacuum is a full-fledged computer on wheels Source

And of course, the modern robot vacuum has sensors everywhere: infrared, lidar, motion, camera (often several of each), and some models also have microphones for voice control.



The Ecovacs DEEBOT X1 has not only a camera, but an array of microphones Source

And naturally, all modern robot vacuums are permanently online and hooked up to the vendor’s cloud infrastructure. In most cases, they communicate aplenty with this cloud — uploading piles upon piles of data collected during operation.

Vulnerabilities in Ecovacs robot vacuums and lawn mowers

The first report of vulnerabilities in Ecovacs robot vacuums and lawnmowers surfaced in August 2024, when security researchers Dennis Giese (known for hacking a Xiaomi robot vacuum) and Braelynn Luedtke gave a talk at DEF CON 32 on reverse engineering and hacking Ecovacs robots.

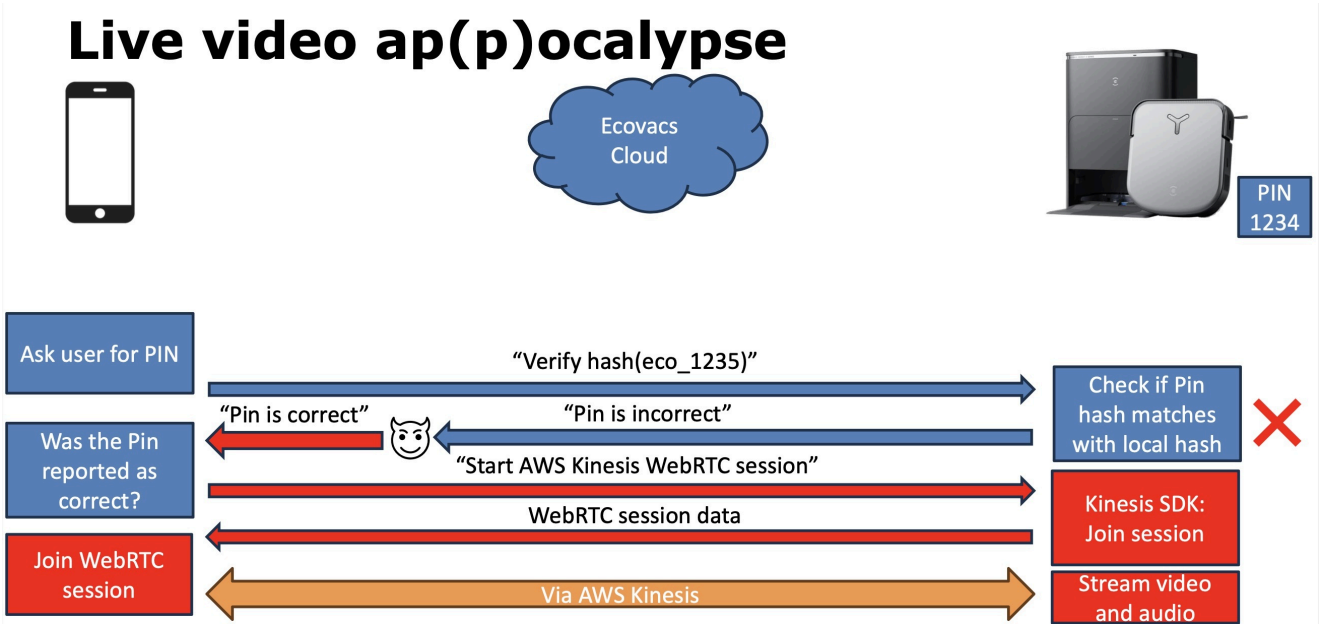
Goat G1 Lawnmowing Robot

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

The Ecovacs GOAT G1 can also be equipped with GPS, LTE and a long-range Bluetooth module Source

In their talk, Giese and Luedtke described several methods for hacking Ecovacs robot vacuums and the mobile app that owners use to control them. In particular, they found that a potential hacker could access the feed from the robot's built-in camera and microphone.

This is possible for two reasons. First, if the app is used on an insecure network, attackers can intercept the authentication token and communicate with the robot. Second, although in theory the PIN code set by the device owner secures the video feed, in practice it gets verified on the app side — so it can be bypassed.

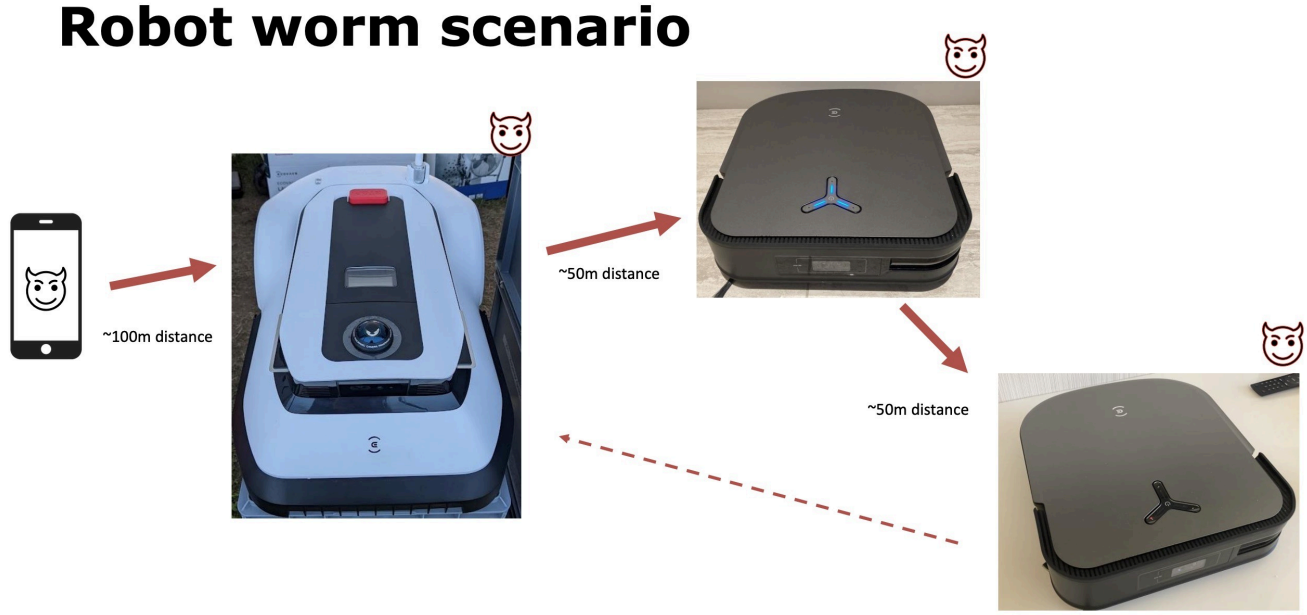


The PIN code for securing the video feed from an Ecovacs robot vacuum is verified on the app side, which makes the mechanism extremely vulnerable Source

The researchers also managed to gain root access to the robot's operating system. They found it was possible to send a malicious payload to the robot via Bluetooth, which in some Ecovacs models gets turned on after a scheduled reboot, while in others it's on all the time. In theory, encryption should protect against this, but Ecovacs uses a static key that's the same for all devices.

Armed with this knowledge, an intruder can get root privileges in the operating system of any vulnerable Ecovacs robot and hack it at a distance of up to 50 meters (~165 feet) — which is precisely what the researchers did. As for robot lawnmowers, these models are hackable at more than 100 meters (~330 feet) away, since they've got more powerful Bluetooth capabilities.

Add to that that, as mentioned already, today's robot vacuums are full-fledged Linux-based computers, and you can see how attackers can use one infected robot as a means to hack others nearby. In theory, hackers can even create a network-worm to automatically infect robots anywhere in the world.



Bluetooth vulnerability in Ecovacs robots could lead to a chain of infection
Source

Giese and Luedtke informed Ecovacs about the vulnerabilities they found, but received no response. The company did try to close some of the holes, say the researchers, but with little success and ignoring the most serious vulnerabilities.

How the Ecovacs robot vacuums were hacked for real

It appears that the DEF CON talk generated great interest in the hacker community — so much so that someone seems to have taken the attack a step further and deployed it on Ecovacs robot vacuums out in the real world. According to recent reports, owners in several U.S. cities had been hit by hackers and made to suffer abuse from their robot servants.

In one incident in Minnesota, an Ecovacs DEEBOT X2 started moving by itself and making strange noises. Alarmed, its owner went into the Ecovacs app and saw that someone was accessing the video feed and remote-control feature. Writing it off as a software glitch, he changed the password, rebooted the robot and sat down on the couch to watch TV with his wife and son.

But the robot kicked back into life almost straight away — this time emitting a continuous stream of racial slurs from its speakers. Not

knowing what to do, the owner turned off the robot, took it into the garage and left it there. Despite this ordeal, he is grateful that the hackers made their presence so obvious. Far worse, he says, would have been if they'd simply secretly monitored his family through the robot without revealing themselves.

Hijacking a live video feed of an Ecovacs robot vacuum Source

In a similar case, this time in California, another Ecovacs DEEBOT X2 chased a dog around the house, again shouting obscenities. And a third case was reported from Texas, where, you guessed it, an Ecovacs robot vacuum went walkabout and hurled abuse at its owners.

The exact number of hacks of Ecovacs robot vacuums is unknown. One reason for this, alluded to above, is that the owners may not be aware of it: the hackers may be quietly observing their daily lives through the built-in camera.

How to guard against robot vacuum hacking?

The short answer is: you can't. Unfortunately, there's no universal method of protecting against robot vacuum hacking that covers all bases. For some models, in theory, there's the option of hacking it yourself, getting

root access, and unlinking the machine from the vendor's cloud. But this is a complex and time-consuming procedure that the average owner won't consider attempting.

A serious problem with IoT devices is that many vendors, sadly, still pay insufficient attention to security. And they often prefer to bury their heads in the sand — even declining to respond to researchers who helpfully report such issues.

To reduce the risks, try do your own research on the security practices of the vendor in question before purchasing. Some actually do a pretty good job of keeping their products safe. And, of course, always install firmware updates: new versions usually remove at least some of the vulnerabilities that hackers can exploit to gain control over your robot.

And remember that a robot connected to home Wi-Fi, if hacked, can become a launchpad for an attack on other devices connected to the same network — smartphones, computers, smart TVs, and so on. So it's always a good idea to move IoT devices (in particular, robot vacuums) to a guest network, and install reliable protection on all devices where possible.