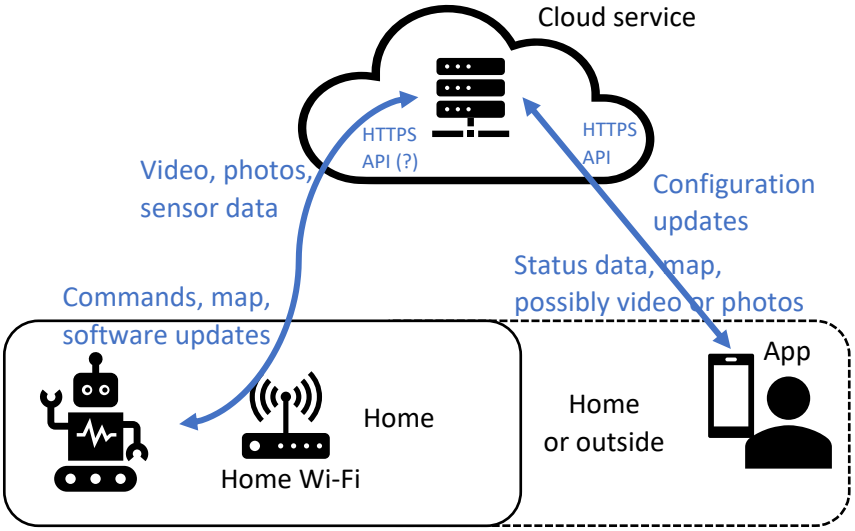
Threat analysis of a robotic vacuum cleaner - summary

Tuomas Aura, 2022-11-23

Since the example vacuum robot is a consumer device, let's assume is used in a home. With minor changes, the same analysis applies also if the vacuum robot is used in an office or other business premises.



Assets

- Privacy of the user and their home
  - Photos or video from robot camera
  - Floorplan (processed in cloud)
- User's personal information, such as name, email, and address
- User's belongings at home
  - Anything that could be stolen
  - Anything that could be damaged by the robot
- The vacuum robot
  - The device itself
  - Robot firmware
  - Machine-learning models used by the robot
- Home wireless network and other devices there

Participants / potential attackers

- Robot owner and family members
- Manufacturer

    - App producer
    - Cloud service provider
    - Insiders: their employees
- Hackers on the internet
- Neighbors or anyone within the range of the wireless network

Threats / potential attacks

Spying and violation of user privacy

The biggest security concern is that the robot has a **camera and sensors that could be used for spying** on people at home. Some cleaning robot apps give users remote access to the camera feed and audio and ability to **drive the robot around** the home, which could be misused to enable more effective spying.

- **Family members or employees** who have authorized access to the robot could use it to spy on each other or on their guests.
- **Employees of the robot manufacturer** (insiders) and **hackers** who compromise the cloud service could misuse the video and other data that is uploaded to the cloud.
- Other people who may want to get access to the camera include **neighbors, stalkers, political opponents** etc.
- Someone with access to the camera could **publish embarrassing photos or videos online**.
- Users **worry about being spied on** – even when it is not true –, which might reduce sales. The product should be designed to minimize such concerns, e.g., by not having a camera.
- Criminals may record video or photos of large numbers of victims and then **blackmail** them, threatening to publish their photos or video.
- Phishing emails sometimes claim to have video or photos recorded at the victim's home and try to blackmail them – even when they do not have any. A user with a camera-enabled product might believe them.

To get the video or photos, the adversary needs to gain access to the robot and its camera. There are some simple ways this can happen:

- They could be a family member.
- They could have been added as a legitimate user, and the robot owner **forgot to remove** access afterwards.
- If they have **physical access** to the robot, they may be able to add themselves as another user (depends on the system design). They could also modify the robot's software configuration by hacking the hardware, although that seem less likely.
- They could **compromise the honest user's credentials** to the cloud service and access the robot though the cloud.
- Spies could compromise the robot configuration in the **supply chain**.

Any published leaks of private information will be a PR disaster for the manufacturer (or cloud service provider, if separate) and lead to **loss of reputation**. The manufacturer could also be **blackmailed**.

Compromised cloud service and mass surveillance

The manufacturer's legitimate access to many robot cameras and other sensors could be misused for **mass surveillance** or **targeted surveillance**.

- The manufacturer could **analyze the collected data for unauthorized purposes** that are unnecessary for the operation of the vacuum robot. They may innovate new ideas and push the limits of what kind of use of the data is allowed. They could also **sell the data**, or the company may get acquired with the user data.
- The **government could use the robots for mass or targeted surveillance** of homes and offices. The manufacturer and cloud service provider may have to comply with the government requirements. The proliferation of remotely controllable cameras in homes and offices **contributes to surveillance society**.
- **Spies** could compromise the cloud service, become insiders to control it, or compromise the robot configuration and software in the supply chain. The manufacturer may be required to help the spies of their own country.
- **Burglars** and other criminals may use the camera and other sensor data to select victims, to find valuable property, learn about pets and alarms, and to time their visits so that the owners are not at home. They would probably get access to the camera through corrupt insiders or by paying hackers.

In addition to the video or camera images, an adversary with access to the cloud can also get some other data:

- The cloud builds a **floor map** of the home, and the user may add annotations to the map. The cloud also stores the robot **cleaning schedule**, which may leak some information about the owner's personal schedule.
- The cloud stores some personal information on the users, such as their name and email – possibly even the street address. Having **identifying and address information** makes the video and other sensor data much more valuable.

Harmful control of the robot

In addition to collecting data, the adversary may gain control of the robot and misuse it.

- They can cause **nuisance** by controlling the robot remotely and driving around with it.
- The robot could be used to **harass pets** or to **damage furniture.** In addition to controlling the robot remotely, the cloud service can modify the robot behavior by updating the software or ML models.
- They could **break the robot**, e.g., by driving it down the stairs.
- The robot battery could be caused to overcharge or overheat and **start a fire**. The threat is quite serious, but the attacker needs to override safety controls, which may require firmware changes.

Mobile app security

The mobile app security is a complex area of its own, ranging from connection security (TLS) and user authentication to software updates and app permissions. All threats that apply to mobile apps in general also apply to the vacuum robot app.

- One specific threat is that a **lost or stolen phone** might have access to the cloud service and, thus, to the robot. The typical countermeasures are locking the phone screen and an online user interface for revoking access. High-security apps may add additional layers of protection such as reauthentication the user when opened, but that would make the app less usable.

The app is unlikely to compromise the user's phone and other data on it. Or if this is possible, then any app can do the same.

Connection security for the robot

In addition to accessing the robot API in the cloud service, the robot will upload video or photos, which are needed for learning. The connection between the robot and the cloud service is likely to use a standard security protocol. Any weaknesses are usually in the choice or authentication credentials.

- Should find out how the client authentication is implemented for the robot-to-cloud API. Use of **default client credentials** is a common mistake.
- Should find out which **security protocol** (TLS, DTLS, SRTP) is used for sending video to the cloud and how the client and server are authenticated for that connection. Most likely it all goes over TLS with password or certificate authentication for the client. If any non-standard security protocol is used, it could be completely insecure.

Note that the Wi-Fi network is just a part of the Internet. The robot-to-cloud connection goes over the public internet, and it needs to have end-to-end security. Thus, the security of the Wi-Fi network (e.g., sniffing, spoofing, and man-in-the-middle attacks on the wireless access link) is of no special interest.

Misuse of access to home Wi-Fi

Notwithstanding the above, there are other interesting threats related to the Wi-Fi network.

- The robot has **access to home Wi-Fi network**. An adversary that can control the robot remotely can also access the home Wi-Fi network via the robot and mount attacks against other computers and devices there – unless the robot is isolated to a separate VLAN or guest network.
- The robot contains the Wi-Fi credentials and could leak them to the cloud service. The impact of this is mitigated by that fact that, to use the credentials, the adversary needs to be in the range of the wireless network.

Registration and ownership of the robot

The device must be linked to at least one user account in the cloud service before it can be used. Typically, the cloud service registers the device to one owner, but there could also be multiple equal users.

- The process of registering a new device needs closer investigation. Could the registration process be misused to captures control of the device?
- When the device is transferred to a new owner, could the previous owner retain control of the robot, or could the new owner see the previous owner's data?
- To discourage theft, the cloud service could trace stolen devices and prevent their use – unless the ownership is released by the previous owner. If such theft-prevention features have been implemented, they lead to new threats. First, the old owner could misuse the tracing feature to trace the new owner. Second, it might be possible to bypass the theft prevention. Third, some second-hand devices could be bricked so that no known person has access to them.

Threats that start from hacking the robot

Compromised IoT devices are a common concern. In the case of vacuum robots, attacks that start by compromising the robot are not high on the priority list, but let's list some of them anyway:

- IoT devices are not always secure code, or they may be used long after they **stop receiving security updates**. Compromised IoT devices may become bots in a **botnet**. However, this mostly applies to devices that are directly accessible from the internet. Since the vacuum robot is in the home network behind a router and its firewall, it is not exposed to direct attacks from the internet.
- Adversaries that have access to the local network may be able to scan the robot for open network ports that do not require authentication, e.g., ones used for its initial configuration. This is a minor threat because an adversary who has access to the local network probably finds more interesting targets than the robot.
- The robot **firmware could be modified in the supply chain**, or the cloud could send a **malicious software update** to the robot.
- A competitor could buy a robot, reverse engineer it, and **steal the firmware** for use in its own products.
- The robot APIs (or app API) in the cloud service could have vulnerabilities that can be exploited to gain control of the cloud service or to access the data on it. The adversary can buy one robot, reverse engineer its credentials and the cloud API, and then target the cloud service. The robot API in the cloud is more likely to have vulnerabilities than the app API because it may use custom software solutions or less tested technologies.

Machine-learning related threats

Recently, threats against machine learning have received a lot of attention. They are probably not serious threats in this case but let us consider them briefly.

- In evasion attacks, the adversary would modify the look of objects in the home so that the robot misclassifies them and, for example, does not recognize the stairs and falls. Since the

adversary needs to be physically at the location, this attack does not make much sense; it is far easier to throw the robot down the stairs.

- In data poisoning, the homeowners would feed the could system intentionally misleading video and sensor data or misleading feedback, so that the model learns the wrong things. The cloud service will use the data and feedback from all users to train a common model, and that model might learn the wrong things. This attack seems rather far-fetched, though.
- In **model stealing**, a competitor could reverse engineers the robot and steal the machine-learning model that it uses for identifying objects. This is a somewhat realistic threat because developing the model requires lots of labelled training data and computational resources, which the competitor might not have. (On the other hand, stealing the backbox model by learning to imitate it would not be easy because the results of the image classification are not directly visible on the external interfaces of the system.)

Other notes

- If one robot is compromised by exploiting a vulnerability, the **attack may be repeatable** for large numbers of robots.
- The **cloud service is a single point of failure**. If the manufacturer goes out of business or is hit by a cyberattack, all their robots around the world may stop working.
- Similarly, the country or area where the robot is used could become under cyberattack or sanctions, in which case they can no longer access the cloud service. The failure of a vacuum robot in a single household is not much of a threat, but if all home automation devices in the whole country stop working, that can be seen as a **societal vulnerability**.