TechXplore

Smart speakers, wearables, sensors: How up-to-date are such permanently connected IoT devices?

December 20 2023, by Anne-Catherine Jung

Cybersecurity risks trough IoT devices?
News study analyses 52 billion smart devices and how up-to-date they are

Credit: Fraunhofer ISI

By 2023, billions of Internet of Things (IoT) devices found their way into almost every area of life, industry and critical infrastructures. As these permanently connected smart devices process very sensitive data, their up-to-dateness is essential—especially in times of hacker attacks, data misuse or industrial espionage.

In this context, a new Fraunhofer ISI study analyzed data of 52 billion devices, their geographical location—and whether their installed firmware is up-to-date and which impact the European General Data Protection Regulation has on this. The findings show that it is only a matter of time before very serious cyberattacks could easily happen.

Users track their health and fitness with wearables, place smart speakers with powerful microphones in their living rooms, and install cheap sensors from no-name manufacturers to automate tasks in their smart homes. The same applies for industry, where Industrial IoT devices connect and monitor machines for example. Most of these devices are quickly forgotten, once they are installed and run.

Possible vulnerabilities in outdated firmware and updates or patches are often ignored, even if some manufacturers of IoT devices provide them—which is not always the case since many of them prioritize fast time-to-market and provide only infrequently software or firmware updates and patches. This can create serious privacy and security threats for users.

Policymakers around the world have become aware of these threats that users are faced with and pursue strong regulations such as the European GDPR. Further, the "right for updates" stipulated in an EU directive and in force since 2022, is another important step towards more secure devices. Very recently, the EU commission signed the Cyber Resilience Act which introduces a legal obligation for manufacturers to provide consumers with timely security updates during several years after the purchase.

Which impact does this have on the manufacturers of smart devices?

A new study tried to provide answers to this and other questions and analyzed 400 terabytes of real-world data from the IoT search engine Censys.io from October 2015 until the end of November 2021. The analysis consists of data from 52 billion devices. Out of them, 175 million devices revealed analyzable information, leading to a data set containing 7,116 distinct models from 384 manufacturers categorized into 17 different device types.

The data allows comparisons between a wide variety of countries, namely all EU member states, G7 states, and Switzerland but also Russia and the Ukraine, as well as Asian countries, such as Malaysia, Indonesia, Singapore, Japan and the U.K. The findings show that the majority of the devices are deployed in the U.S. (52%), followed by Germany (7%), Russia (4%), the U.K. (4%), Japan (4%), France (4%), Canada (3%), Poland (3%), Singapore (1%), Indonesia (1%) and other countries (16%).

Major cybersecurity risks due to old firmware and device age

Examining the status quo of end 2021, the age of the firmware running on the devices in Germany is 689 days, respectively 1.9 years (y). Further, the devices have not received any other update (software update , patch etc.) for almost one year (351 days).

On an EU level, the situation is even worse with a firmware update delay of 930 days (2.5 y) and other updates being ignored for 411 days (1.1 y). This means that the use of many of these devices is associated with major cybersecurity risks and that data protection is no longer possible here—the devices are vulnerable and easy prey for hacker attacks, for example.

Looking at the device age and the geographical differences, the results find that devices in Ireland are most up-to-date (239 days), whereas Portugal brings up the rear with 786 days. If we look to Southeast Asia, it becomes clear that Singapore performs best (299 d) and Malaysia worst (477 d, 1.3 y). The oldest devices can be found in Japan (716 days, almost 2 years).

Has the GDPR improved the up-to-dateness of the installed firmware?

Regarding the question of whether the situation has changed for the better since the European General Data Protection Regulation (GDPR) went into effect—it contains explicit regulations on this issue—the study shows interesting findings: While on the global level, the devices' age has decreased, the situation is quite different for Europe: In fact, for 28 out of 35 EU member states, the devices' age increased on average 99 days.

Dr. Frank Ebbers, author of two research papers on this topic (one published in the *2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS)* and one in *IEEE Transactions on Software Engineering*), interprets the results. "The low up-to-dateness-rate should alarm both manufacturers and users but also policymakers and sharpen the focus on this issue. It is also surprising that the GDPR [did not have] the expected impact on software updates within the EU.

"This might be explained by the fact that users believe now that GDPR is in force that only companies are responsible for updates and that these organizations care more about the privacy of customers."

Ebbers believes that the manufacturers, the regulatory authorities and the users themselves have a responsibility here. "Only through the joint efforts of these three partners is it possible to create a more secure IT infrastructure. "

It is often said that the situation can be improved with automatic updates, so-called "over-the-air" updates. He takes a critical view of this. "The first question that arises here is who is liable for damage caused by errors in automatic updates. Just think of the medical sector, where a faulty update of portable ECG devices can cost lives."

Regulatory authorities should therefore issue recommendations to manufacturers that force (or nudge) them to incorporate good update mechanisms into the devices, which can then be easily understood by end users. In addition, updates should become a prerequisite for commissioning in Europe as part of CE labeling.

More information: Frank Ebbers, Effects of the GDPR in Southeast Asia vs. Europe—A Large-Scale Analysis of IoT Devices, *2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS)* (2023). DOI: 10.1109/ICSECS58457.2023.10256372

Frank Ebbers, A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild, *IEEE Transactions on Software Engineering*

(2022). DOI: 10.1109/TSE.2022.3163969

Provided by Fraunhofer-Gesellschaft

Citation: Smart speakers, wearables, sensors: How up-to-date are such permanently connected IoT devices? (2023, December 20) retrieved 28 April 2024 from https://techxplore.com/news/2023-12-smart-speakers-wearables-sensors-up-to-date.html