Peekaboo! Here's a system to guarantee smart home privacy

May 31 2022, by Daniel Tkacik

Credit: Pixabay/CC0 Public Domain

Many internet-connected devices—let's use smart speakers as an example—share data to the cloud when you interact with them. How do you know your speaker isn't always listening? How do you know it's not

sharing more information than is necessary to fulfill your request?

There's currently no way to check, but CyLab researchers are close to a solution.

"People are concerned that their devices are capturing and sharing too much data," says CyLab's Haojian Jin, a Ph.D. student in the Human-Computer Interaction Institute. "Companies want to tell users that they only collect certain pieces of information, but they currently have no way to actually prove it."

Introducing Peekaboo

Jin and a team of researchers have developed a new privacy-sensitive architecture for developers to build smart home apps, which the team refers to as "Peekaboo." The system takes requests from developers to share certain pieces of data and ensures only the essential pieces of data to fulfill their request are shared with them.

The system, described in a paper titled "Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes," was presented at the IEEE Symposium on Security and Privacy last week.

"In the privacy world, we have a principle called 'data minimization,'" says Jin. "The companies that collect the data should only be collecting the minimum amount of data to fulfill their objectives."

This concept is even written into the EU's General Data Protection Regulation (GDPR), Jin points out. Article 5 (1) (c) of the GDPR reads, "Personal data shall be limited to what is necessary in relation to the purposes for which they are processed."

Under the Peekaboo architecture, developers first declare all the data they intend to collect and under what conditions, where that data is being sent, and the granularity of the data itself—for example, whether they'd like to collect the number of hours watched on a smart TV per week, per month, per quarter, etc. Then, an in-home hub mediates between all devices in the home and the outside Internet.

"The hub enforces the sharing of only data declared by the developer," says Jin. "And users and third-party auditors can inspect the incoming data requests as well as the outgoing data flows."

Giving users more control of their privacy in smart homes

The essence of the Peekaboo architecture, Jin says, is that users can have more control over their data. If a developer sends in a request to collect a piece of information—let's pretend they want to know the number of hours of spent watching a smart TV in a single day—the user can modify the request on the hub to only share the number of hours spent watching their smart TV over a whole month, if they're more comfortable with that.

In addition, Peekaboo in the future could help make privacy nutrition labels—which are now being deployed by both Apple and Google—more accurate. Right now, there is no way to enforce and verify that apps are behaving consistently with their privacy nutrition labels, which are produced manually by developers and have been found to be inaccurate at times. But since Peekaboo both enforces and verifies data sharing in accordance with developers' requests, privacy nutrition labels could be automatically generated and updated to accurately portray data collection and use.

Lastly, as the Internet of Things continues to grow and people accumulate hundreds of IoT devices in their homes, Peekaboo can help manage the smart home holistically.

"The Peekaboo protocol will allow users to manage privacy preferences for all of their devices in a centralized manner through the hub," Jin says. "Imagine not just a privacy nutrition label for an individual device, but a privacy nutrition label for an entire home."

More information: Haojian Jin et al, Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes, *Conference Proccedings of 2022 IEEE Symposium on Security and Privacy* (2022). DOI: 10.1109/SP46214.2022.00142. www.computer.org/csdl/proceedi … 1600b571/1CIO8pmx6jm

Provided by Carnegie Mellon University