The smart home tech inside your home is less secure than you think, research finds

October 26 2023, by Cesareo Contreras

David Choffnes is among a group of researchers that recently uncovered security and privacy vulnerabilities in smart home devices. Credit: Matthew Modoono/Northeastern University

Our homes are getting smarter every day. The next time you buy a toaster, fridge or dishwasher, setup might involve connecting to your

home WiFi network and downloading an app on your phone.

But such interconnectivity comes with risk, says David Choffnes, associate professor of computer sciences at Northeastern University.

"We are moving from this idea where the walls of our home are our private space to now the spaces within the walls have all these devices that communicate over the internet," Choffnes says.

Ideally, smart home gadgets, otherwise known as Internet of Things (IoT) devices, make people's lives easier. Tasks like setting the thermostat, making your morning coffee or ordering new ink for your printer could be easily automated or completed via your smartphone with some of these products.

"(But) when these things communicate, either with each other or over the internet, they do so in a way that we can't see," Choffnes says.

Some of these devices are sharing out their location, which in turn allows other devices within their local network to locate them, Choffnes says. A local network in this context means a group of connected devices within a specific location like a house.

"They're also sending out other pieces of information that are unique to the home, meaning that even if you try your best to preserve your privacy, turn off tracking on your phone, whether its iOS and Android, all of these mechanisms that you put in place to your protect yourself can fall apart," Choffnes says.

"Trackers online can tell who you are by the collection of devices in your home because that's going to be unique to you," he adds.

New research by Choffnes and a team of others sheds light on the

privacy and security flaws of this emerging technology category. The team will present its research this week at the ACM Internet Measurement Conference in Montreal.

For the study, the team tested 93 IoT devices to see how they interact within a local network.

The results of the research have been illuminating, Choffnes explains.

"One of the things that we observed is that devices will scan their local network to figure out what is every other device in your home," Choffnes adds. "For example, your Amazon smart speaker could learn if you have a smart fridge. It could learn about your printer. It might learn your name because if you have, for instance, an Apple HomePod, usually the default name of that thing is your name, like "Dave's HomePod.'"

The team also found security issues with how the mobile apps connected with these devices work.

"On Android, mobile apps can get around permission restrictions that Android imposes, like access to geolocation or access to unique identifiers, by simply querying devices or sending messages to other devices on the home network and getting them to tell the app the same information that OS was keeping away from them," he says.

Choffnes notes that Google has acknowledged the team's findings and is working with them to develop mitigation efforts that "could be implemented via the Android OS, app review processes, and general IoT standardization efforts."

Choffnes stresses that these systems do not have to operate in this manner. It's possible for devices to work interoperably without such big

privacy and security risks.

"There's a way that they can discover each other without exposing information that could be used to track us," Choffnes says.

In the research, the team points to a number of potential solutions, including calling for more standardization among these devices. They point to the Matter smart home protocol as one example, though they note that the system doesn't yet address the specific vulnerabilities the team discovered.

Tinanru Hu, a doctoral student at Northeastern, and Daniel J. Dubois, an associate research scientist at Northeastern, were among the authors of the research.

Hu says companies haven't been greatly incentivized to standardize. One of the goals of the research is to help the public know about these issues.

"Through our research, we want to make the user aware of this problem," he says. "When more users know about the problem, they can motivate the companies toward the best privacy and security standardization efforts."

Regulations and more government involvement could also help curtail some of these issues, the team notes, pointing to the EU Cyber Resilience Act and the U.S. National Cybersecurity Strategy.

This story is republished courtesy of Northeastern Global News https://news.northeastern.edu/.

Provided by Northeastern University

Citation: The smart home tech inside your home is less secure than you think, research finds

(2023, October 26) retrieved 27 April 2024 from https://techxplore.com/news/2023-10-smart-home-tech.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.