# New research reveals alarming privacy and security threats in smart homes

October 26 2023


Credit: CC0 Public Domain

An international team of researchers, led by IMDEA Networks and Northeastern University in collaboration with NYU Tandon School of Engineering, Universidad Carlos III de Madrid, IMDEA Software, University of Calgary, and the International Computer Science Institute, has unveiled findings on the security and privacy challenges posed by the ever-growing prevalence of opaque and technically complex Internet of Things (IoT) devices in smart homes.

Smart homes are becoming increasingly interconnected, comprising an array of consumer-oriented IoT devices ranging from smartphones and smart TVs to virtual assistants and CCTV cameras. These devices have cameras, microphones, and other ways of sensing what is happening in our most private spaces—our homes. An important question is, can we trust that these devices in our homes are safely handling and protecting the sensitive data they have access to?

"When we think of what happens between the walls of our homes, we think of it as a trusted, private place. In reality, we find that smart devices in our homes are piercing that veil of trust and privacy—in ways that allow nearly any company to learn what devices are in your home, to know when you are home, and learn where your home is," said David Choffnes, Associate Professor of Computer Science and Executive Director of the Cybersecurity and Privacy Institute at Northeastern University.

"These behaviors are generally not disclosed to consumers, and there is a need for better protections in the home."

The research team's extensive study, titled "In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes," was presented at the ACM Internet Measurement Conference (ACM IMC'23) in Montreal (Canada). The paper delves for the first time into the intricacies of local network interactions between 93 IoT devices and mobile apps, revealing a plethora of previously undisclosed security and privacy concerns with actual real-world implications.

While most users typically view local networks as a trusted and safe environment, the study's findings illuminate new threats associated with the inadvertent exposure of sensitive data by IoT devices within local networks using standard protocols such as UPnP or mDNS. These threats include the exposure of unique device names, UUIDs, and even

household geolocation data, all of which can be harvested by companies involved in surveillance capitalism without user awareness.

According to Vijay Prakash, Ph.D. student from NYU Tandon who co-authored the paper, "analyzing the data collected by IoT Inspector, we found evidence of IoT devices inadvertently exposing at least one PII (Personally Identifiable Information), like unique hardware address (MAC), UUID, or unique device names, in thousands of real world smart homes.

"Any single PII is useful for identifying a household, but combining all three of them together makes a house very unique and easily identifiable. For comparison, if a person is fingerprinted using the simplest browser fingerprinting technique, they are as unique as one in 1,500 people. If a smart home with all three types of identifiers is fingerprinted, it is as unique as one in 1.12 million smart homes."

These local network protocols can be employed as side-channels to access data that is supposedly protected by several mobile app permissions such as household locations.

"A side channel is a sneaky way of indirectly accessing sensitive data. For example, Android app developers are supposed to request and obtain users' consent to access data like geolocation. However, we have shown that certain spyware apps and advertising companies do abuse local network protocols to silently access such sensitive information without any user awareness," said Narseo Vallina-Rodriguez, Associate Research Professor of IMDEA Networks and co-founder of AppCensus.

"All they have to do is kindly asking for it to other IoT devices deployed in the local network using standard protocols like UPnP."

"Our study shows that the local network protocols used by IoT devices

are not sufficiently protected and expose sensitive information about the home and the use we make of the devices. This information is being collected in an opaque way and makes it easier to create profiles of our habits or socioeconomic level," adds Juan Tapiador, professor at UC3M.

The impact of this research extends far beyond academia. The findings underscore the imperative for manufacturers, software developers, IoT and mobile platform operators, and policymakers to take action to enhance the privacy and security guarantees of smart home devices and households.

The research team responsibly disclosed these issues to vulnerable IoT device vendors and to Google's Android Security Team, already triggering security improvements in some of these products.

**More information:** Aniketh Girish et al, In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes, *Proceedings of the 2023 ACM on Internet Measurement Conference* (2023). DOI: 10.1145/3618257.3624830

Provided by IMDEA Networks Institute