Your 'Smart Home' Technology Spies On You Day And Night

POSTED BY: VIA STUDYFINDS

OCTOBER 31, 2023

https://www.technocracy.news/your-smart-home-technology-spies-on-you-day-and-night/

Every electronic device in your home – from appliances and smart meters to doorbells – forms a personal "Internet of Things." The primary vendors hoover up data, exchange or sell it to others; that is the expected outcome. But a mishmash of security hubris leftover lets black hat hackers assemble an IoT profile on you to see when you are home, what valuables you might have, etc. Figuratively speaking, it leaves you naked as a jaybird for all to peer into your home.

Every major appliance in your house is equipped with a Wi-Fi circuit board (refrigerators, air conditioners, TVs, washers, dryers, and smart meter). Ring and Nest devices communicate with Wi-Fi. Smart "assistants" like your smartphone, Alexa, and Siri all use Wi-Fi. Since most of these devices are never upgraded with software or firmware, they are vulnerable to hackers.

Not surprisingly, AI is seen as the solution. Get ready to fork over more money in addition to identity theft, title lock, virus protection, malware software, etc. Technocracy.News Editor

International researchers are issuing a dire warning of security and privacy concerns lurking within smart homes. Led by IMDEA Networks and Northeastern University, scientists were able to demonstrate a variety of security and privacy threats due to the local network interactions of Internet of Things (IoT) devices and mobile apps.

As **smart homes** continue to evolve, they encompass a wide array of consumer-focused IoT devices, including **smartphones**, smart TVs, virtual assistants, and CCTV cameras. These devices come equipped with cameras, microphones, and various sensors that can perceive activities within our most intimate spaces – our homes. However, can we truly trust these devices to handle and safeguard the sensitive data they collect?

Ubicomp 2020 Presentation: IoT Inspector: Crowdsourcing IoT Network Traffic at Scale -- https://youtu.be/-uzG3B1Z7J8?si=MrzUy4Jy5Kw9VSTx *(5 min)*

"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," says David Choffnes, associate professor of computer science and executive director of the Cybersecurity and Privacy Institute at Northeastern University, in a **media release**. "These behaviors are generally not disclosed to consumers, and there is a need for better protections in the home."

Alarming Findings On 'Smart Home' Tech

For the study, researchers delved into the intricacies of local network interactions among 93 IoT devices and **mobile apps** and were able to unveil numerous previously undisclosed security and privacy concerns with real-world implications.

Contrary to the common perception that local networks are secure environments, the study highlights new threats linked to the inadvertent exposure of sensitive data by IoT devices within local networks using standard protocols like UPnP or mDNS. These threats include the revelation of unique device names, UUIDs (Universally Unique Identifiers), and even the geographic location of households. These can be exploited by companies involved in surveillance capitalism without the users' knowledge.

"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," explains study co-author Vijay Prakash, PhD student from the New York University Tandon School of Engineering. "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."

The Potent Weapon of Local Network Protocols

The study underscores how local network protocols can serve as side channels to access data that is theoretically protected by **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**," explains Narseo Vallina-Rodriguez, associate research professor of IMDEA Networks and co-founder of AppCensus. "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. 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," adds Juan Tapiador, professor at the Universidad Carlos III de Madrid. "This information is being collected in an opaque way and makes it easier to create profiles of our habits or socioeconomic level."

Wider Implications and Calls for Action

The implications of this research go beyond academia, emphasizing the need for manufacturers, software developers, IoT and mobile platform operators, and policymakers to take decisive action to enhance the privacy and security of smart home devices and households. Researchers have already responsibly disclosed these issues to vulnerable IoT device vendors and Google's Android Security Team, prompting security improvements in some of these products.

Read full story here… https://studyfinds.org/smart-homes-security-threats/