Study Determines Smart Home Devices Leave Homeowners Vulnerable to Privacy Breaches

October 30, 2023 - A new study titled In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes has shown that smart home systems arenâ€™t actually as private as we might think they are. These popular systems which are pushed heavily by the likes of Amazon, Google and Apple offer their users a number of conveniences, including upgraded home security. But as it turns out, they also leave homeowners vulnerable to privacy violations and network security issues.

Researchers determined that IoT (Internet of Things) devices and mobile apps often collect and transmit sensitive information without adequate disclosure to consumers. This lack of transparency can lead to the exposure of personally identifiable information (PII) and other sensitive data.

IoT devices donâ€™t work without internet access, and that access is normally provided via a local network in the home. Contrary to the perception that local networks are secure environments, the research uncovers vulnerabilities in the way IoT devices communicate over standard protocols. These vulnerabilities can result in the inadvertent exposure of unique device names, their IDs, and even the geographic locations where they are located.

Companies involved in surveillance and data collection, sometimes referred to as "surveillance capitalism," can exploit these vulnerabilities to gain insights into users' homes, their presence or absence, and the devices they own. This information can be used for various purposes, including targeted advertising and profiling. It is also worth pointing out that this information isnâ€™t just valuable to companies that want to exploit the data. Itâ€™s also quite valuable to hackers and cybercriminals. And there is no reason in the world to believe that they wonâ€™t try to gain access to it.

Combining different identifiers (e.g., device IDs, device names, etc...) makes a household highly unique and easily identifiable. This level of specificity can raise serious privacy concerns, as it allows for pinpointing and tracking individual homes with a high degree of accuracy.

One very disturbing determination from the study was that when users of these devices download mobile applications that arenâ€™t secure, or which come from unknown sources, those applications may be able to bypass network protocols

and share information even if they have been specifically denied permission to do so.

None of this should really be a surprise. Weâ€™ve warned readers about smart devices now for years. The study provides confirmation of some of our initial fears and raises new concerns about the security and privacy of smart homes, highlighting the need for better protection, transparency, and responsible data handling in the growing IoT ecosystem. It underscores the importance of addressing these issues to maintain user trust and safeguard personal data in the smart home environment.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS