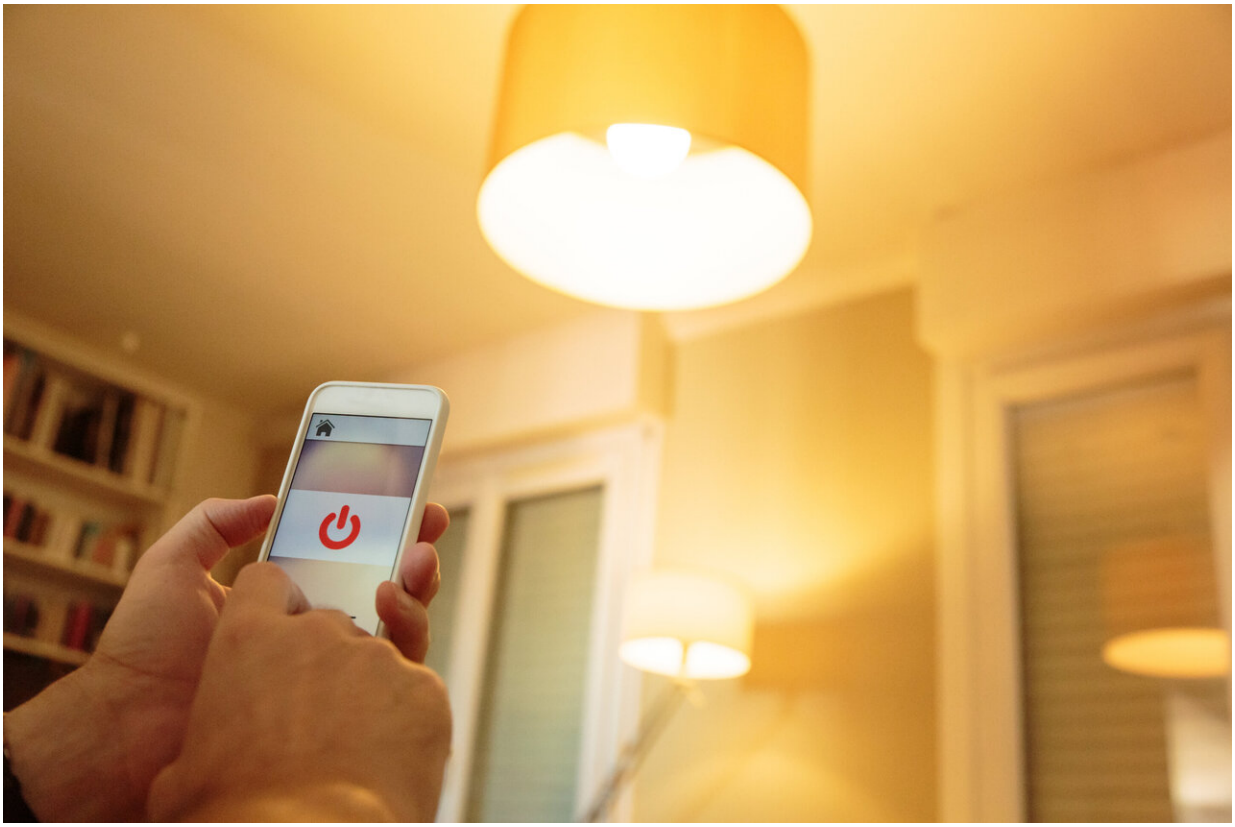
Study warns of security gaps in smart light bulbs

October 23 2019, by Milady Nazir



UTSA researchers review the security gaps on smart bulbs exposing consumers to hacks. Credit: UTSA

Smart bulbs are expected to be a popular purchase this holiday season. But could lighting your home open up your personal information to

hackers?

Earlier this year Amazon's Echo made global headlines when it was reported that consumers' conversations were recorded and heard by thousands of employees.

Now researchers at UTSA have conducted a review of the security holes that exist in popular smart-light brands. According to the analysis, the next prime target could be that smart bulb that shoppers buy this coming holiday season.

"Your smart bulb could come equipped with infrared capabilities, and most users don't know that the invisible wave spectrum can be controlled. You can misuse those lights," said Murtuza Jadliwala, professor and director of the Security, Privacy, Trust and Ethics in Computing Research Lab in UTSA's Department of Computer Science. "Any data can be stolen: texts or images. Anything that is stored in a computer."

Some smart bulbs connect to a home network without needing a smart home hub, a centralized hardware or software device where other internet of things products communicate with each other. Smart home hubs, which connect either locally or to the cloud, are useful for IoT devices that use the Zigbee or Z-Wave protocols or Bluetooth, rather than Wi-Fi.

If these same bulbs are also infrared-enabled, hackers can send commands via the infrared invisible light emanated from the bulbs to either steal data or spoof other connected IoT devices on the home network. The owner might not know about the hack because the hacking commands are communicated within the owner's home Wi-Fi network, without using the internet.

This study, titled "Light Ears: Information Leakage via Smart Lights," was coauthored by Anindya Maiti and published in the September 2019 issue of the journal Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.

Smart bulbs have moved beyond novelty to a lucrative mature market. Last year consumers spent close to $8 billion, and that amount is expected to more than triple to $28 billion in less than a decade.

"Think of the bulb as another computer," adds Jadliwala. "These bulbs are now poised to become a much more attractive target for exploitation even though they have very simple chips."

Jadliwala recommends that consumers opt for bulbs that come with a smart home hub rather than those that connect directly to other devices. He also recommends that manufacturers do a better job in developing security measures to limit the level of access that these bulbs have to other smart home appliances or electronics within a home.

More information: Anindya Maiti et al, Light Ears, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (2019). DOI: 10.1145/3351256

Provided by University of Texas at San Antonio