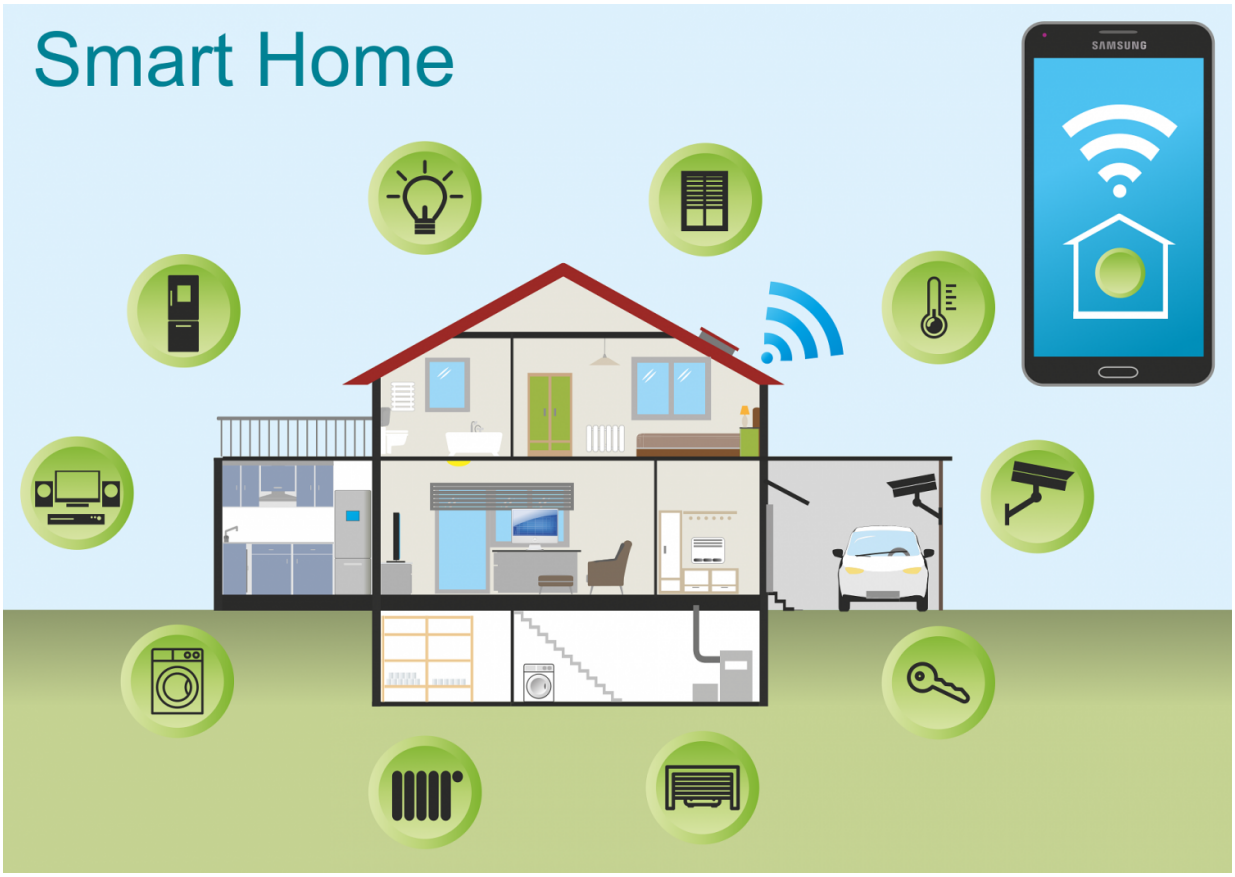
Researchers examine eavesdropping on smart-home traffic metadata

August 31 2017, by Nancy Owano



Credit: CC0 Public Domain

(Tech Xplore)—Uh-oh. Those smart-home devices can reveal personal information about your home activities and encryption does not resolve

the risk either. A study indicates that ISPs can infer activities by analyzing Internet traffic from homes with these IoT devices.

"The majority of connected devices require Internet access to function, and when this avenue is carved into your home, there is also the risk of compromise, spying, and data theft," said Charlie Osborne in *ZDNet*.

The study is titled "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic" by Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster from Princeton University.

Devin Coldewey in *TechCrunch* had a clear rundown of how this kind of attack would work:

"It's a pretty straightforward attack: the IoT devices often identify themselves voluntarily, usually by connecting to specific domains or URLs. Even if they didn't, there are simple ways of profiling them based on observation and some known data. The researchers demonstrated this by showing that various devices show distinct patterns of data transmission."

The study team tested a number of smart home devices. They found all "revealed potentially private user behaviors through network traffic metadata," said *ZDNet*. The researchers found "it takes only a small amount of smart home traffic metadata to detect and track home activities," *ZDNet* added.

This was seen across a sampling of smart device types from various manufacturers. The researchers said, "Given the effectiveness of traffic rate privacy attacks on all tested devices, we believe that smart home owners should be concerned about traffic rate metadata across all types of smart home devices."

No, it does not matter if there is encryption. *ZDNet* said, "ISPs or other passive network adversaries would be able to tap in and use this data against you."

But what if you have a VPN? Charlie Osborne in *ZDNet* said that it is an option "but this does not completely mask IoT traffic patterns. Tracking IoT device data becomes more difficult, but not impossible."

The authors wrote that "We find that certain common device combinations and user activity patterns minimize the ability of a VPN to obfuscate smart home traffic metadata."

At this point, it may be worthwhile to just consider how privacy can be compromised in this manner. The authors wrote that "Many smart home devices have always-on sensors that capture users' offline activities in their living spaces and transmit information about these activities outside of the home, typically to cloud services run by device manufacturers."

What kinds of activities? Smart home devices may involve your sleeping patterns, exercise routines, child behaviors, or medical information, for example.

Kieren McCarthy, *The Register*, wrote "Given the fact that the same patterns are repeated, it would be very easy for an ISP to build a model that instantly analyzed and stored such patterns. And if an ISP can do it, anyone who can grab your internet traffic would be able to do the same."

But the study, which is on arXiv, also provides a way for a person to blind any ISP who attempts spying in this manner. The two key words for this solution turn out to be "traffic shaping." Michael Mimoso in *Threatpost* said the authors suggested that "a relatively straightforward technique known as traffic rate shaping is a solid strategy for mitigating

privacy risks posed by these devices."

In exploring different strategies for mitigating the privacy risks, they discussed the merits of traffic shaping.

"Our experiments show that traffic shaping can effectively and practically mitigate many privacy risks associated with smart home IoT devices. We find that 40KB/s extra bandwidth usage is enough to protect user activities from a passive network adversary. This bandwidth cost is well within the Internet speed limits and data caps for many smart homes."

According to their paper, "Our results indicate that independent link padding is reasonable given smart home Internet speeds and data caps."

Mimoso explained: "The researchers propose traffic shaping through independent link padding which shapes traffic rates to a constant size, eliminating the ability to snoops to infer activity from spikes and certain traffic patterns."

The Register explained this, too: "What did work, however, was adding noise to the system through independent link padding (ILP). The team wrote some code (under 100 lines, they say) that ran on the router and padded or fragmented all data packets to a constant size, and then buffered traffic or sent cover traffic to hide actual device data."

Nonetheless, the authors stated that, while their proposed traffic shaping was practical, "improved regulation of ISPs and other passive network observers may also be necessary to offset the unique privacy challenges posed by IoT devices."

For their lab setup, they said, they turned to several commercially available IoT devices as a testbed for their traffic metadata attack and

for developing the protection strategy. They configured a Raspberry Pi 3 Model B as an 802.11n wireless access point for the gateway router. The Raspberry Pi 3 has a built-in WiFi antenna. The Raspberry Pi ran Raspbian Jessie OS, a version of Debian Linux optimized for the Raspberry Pi platform.

More information: Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic, arXiv:1708.05044 [cs.CR] arxiv.org/abs/1708.05044

Abstract

The growing market for smart home IoT devices promises new conveniences for consumers while presenting new challenges for preserving privacy within the home. Many smart home devices have always-on sensors that capture users' offline activities in their living spaces and transmit information about these activities on the Internet. In this paper, we demonstrate that an ISP or other network observer can infer privacy sensitive in-home activities by analyzing Internet traffic from smart homes containing commercially-available IoT devices even when the devices use encryption. We evaluate several strategies for mitigating the privacy risks associated with smart home device traffic, including blocking, tunneling, and rate-shaping. Our experiments show that traffic shaping can effectively and practically mitigate many privacy risks associated with smart home IoT devices. We find that 40KB/s extra bandwidth usage is enough to protect user activities from a passive network adversary. This bandwidth cost is well within the Internet speed limits and data caps for many smart homes.

https://techxplore.com/news/2017-08-eavesdropping-smart-home-traffic-metadata.html