

Design flaws create security vulnerabilities for 'smart home' internet-of-things devices

2 May 2019



Credit: CC0 Public Domain

Researchers at North Carolina State University have identified design flaws in "smart home" Internet-of-Things (IoT) devices that allow third parties to prevent devices from sharing information. The flaws can be used to prevent security systems from signaling that there has been a break-in or uploading video of intruders.

"IoT devices are becoming increasingly common, and there's an expectation that they can contribute to our safety and security," says William Enck, co-author of a paper on the discovery and an associate professor of computer science at NC State. "But we've found that there are widespread flaws in the design of these devices that can prevent them from notifying homeowners about problems or performing other security functions."

"Essentially, the devices are designed with the assumption that wireless connectivity is secure and won't be disrupted—which isn't always the case," says Bradley Reaves, co-author of the paper and an assistant professor of computer science at NC

State. "However, we have identified potential solutions that can address these vulnerabilities."

Specifically, the researchers have found that if third parties can hack a home's router—or already know the password—they can upload network layer suppression malware to the router. The malware allows devices to upload their "heartbeat" signals, signifying that they are online and functional—but it blocks signals related to security, such as when a motion sensor is activated. These suppression attacks can be done on-site or remotely.

"One reason these attacks are so problematic is that the system is telling homeowners that everything is OK, regardless of what's actually happening in the home," Enck says.

These network layer suppression attacks are possible because, for many IoT devices, it's easy to distinguish heartbeat signals from other signals. And addressing that design feature may point the way toward a solution.

"One potential fix would be to make heartbeat signals indistinguishable from other signals, so malware couldn't selectively allow heartbeat signals to pass through," says TJ O'Connor, first author of the paper and a Ph.D. student at NC State.

"Another approach would be to include more information in the heartbeat signal," O'Connor says. "For example, if a device sends three motion-sensor alerts, the subsequent heartbeat signal would include data noting that three sensor alerts had been sent. Even if the network layer suppression malware blocked the sensor alert signals, the system would see the [heartbeat](#) signal and know that three sensor alerts were sent but not received. This could then trigger a system warning for homeowners."

"No system is going to be perfect, but given the widespread adoption of IoT devices, we think it's

important to raise awareness of countermeasures that [device](#) designers can use to reduce their exposure to attacks," Enck says.

More information: "Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things," enck.org/pubs/oconnor-wisec19b.pdf

Provided by North Carolina State University

APA citation: Design flaws create security vulnerabilities for 'smart home' internet-of-things devices (2019, May 2) retrieved 18 June 2021 from <https://techxplore.com/news/2019-05-flaws-vulnerabilities-smart-home-internet-of-things.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.