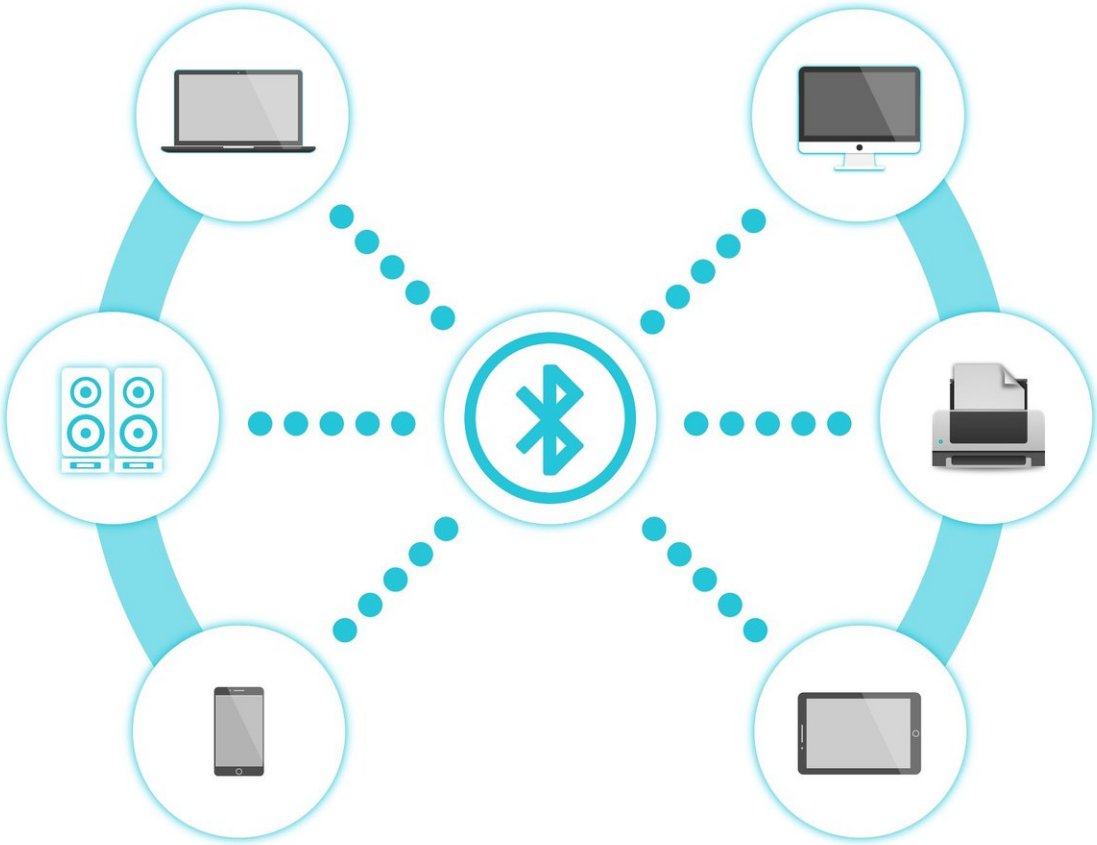
Study uncovers new threat to security and privacy of Bluetooth devices

November 17 2022, by Tatyana Woodall



Credit: CC0 Public Domain

Mobile devices that use Bluetooth are vulnerable to a glitch that could

allow attackers to track a user's location, a new study has found.

The research revolves around Bluetooth Low Energy (BLE), a type of Bluetooth that uses less energy when compared to Bluetooth Classic (an earlier generation of Bluetooth). On smartwatches and smartphones, billions of people rely on this type of wireless communication for all types of activities, ranging from entertainment and sports to retail and health care.

Yet due to a design flaw in Bluetooth's protocol, users' privacy could be at risk, said Yue Zhang, lead author of the study and a postdoctoral researcher in computer science and engineering at The Ohio State University. Zhang recently presented the findings at the ACM Conference on Computer and Communications Security (ACM CCS 2022). The study also received a "best paper" honorable mention at the conference.

Zhang and his adviser, Zhiqiang Lin, professor of computer science and engineering at Ohio State, proved the threat by testing over 50 market-available Bluetooth devices as well as four BLE development boards. They reported the flaw to major stakeholders in the Bluetooth industry, including Bluetooth Special Interest Group (SIG) (the organization that oversees the development of Bluetooth standards), hardware vendors such as Texas Instruments and Nordic, and operating systems providers such as Google, Apple and Microsoft.

Google rated their findings as a high-severity design flaw and gave the researchers a bug bounty award.

But the good news is that Zhang and Lin also developed a potential solution to the problem that they successfully tested.

Bluetooth devices have what are called MAC addresses—a string of

random numbers that uniquely identify them on a network. About once every 20 milliseconds an idle BLE device sends out a signal advertising its MAC address to other nearby devices that it could connect with.

The study identifies a flaw that could allow attackers to observe how these devices interact with the network, and then either passively or actively collect and analyze the data to break a user's privacy.

"This is a new finding that nobody has ever noticed before," said Zhang. "We show that by broadcasting a MAC address to the device's location, an attacker may not physically be able to see you, but they would know that you're in the area."

One of the reasons researchers are concerned about such a scenario is because a captured MAC address could be deployed in what is called a replay attack, which may allow the attacker to monitor the user's behaviors, track where the user has been in the past or even figure out the real-time location of the user.

"Bluetooth SIG was certainly made aware of the MAC address tracking threat, and to protect devices from being tracked by bad actors, a solution called MAC address randomization has been used since 2010," said Lin.

Later in 2014, Bluetooth introduced a new feature called the "allowlist" which only allows approved devices to be connected, and prevents private devices from accessing unknown ones. But according to the study, this allowlist feature actually introduces a side channel for device tracking.

Zhang and Lin proved the new tracking threat is real by creating a novel attack strategy they called Bluetooth Address Tracking (BAT). The researchers used a customized smartphone to hack into more than 50

Bluetooth gadgets—most of them their own devices—and showed that by using BAT attacks, an attacker could still link and replay a victim's data, even with frequent MAC randomization.

As of yet, BAT attacks are undefeated, but the team did create a prototype of a defensive countermeasure. Called Securing Address for BLE (SABLE), their solution involves adding an unpredictable sequence number, essentially a timestamp, to the randomized address to ensure that each MAC address can only be used once to prevent the replay attack. The study noted it was successfully able to stop attackers from linking up to the victim's devices.

The results of their experiment showed that SABLE only slightly affects battery consumption and overall device performance, but Lin hopes to use the new attack and its countermeasure to raise awareness in the community. "The lesson learned from this study is that when you add new features to existing designs, you should revisit previous assumptions to check whether they still hold."

The research is published in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*.

More information: Yue Zhang et al, When Good Becomes Evil, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (2022). DOI: 10.1145/3548606.3559372

Provided by The Ohio State University

Citation: Study uncovers new threat to security and privacy of Bluetooth devices (2022, November 17) retrieved 20 March 2024 from https://techxplore.com/news/2022-11-uncovers-threat-privacy-bluetooth-devices.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.