TechXplore

How hackers could use Wi-Fi to track you inside your home

November 15 2019, by Rob Mitchum

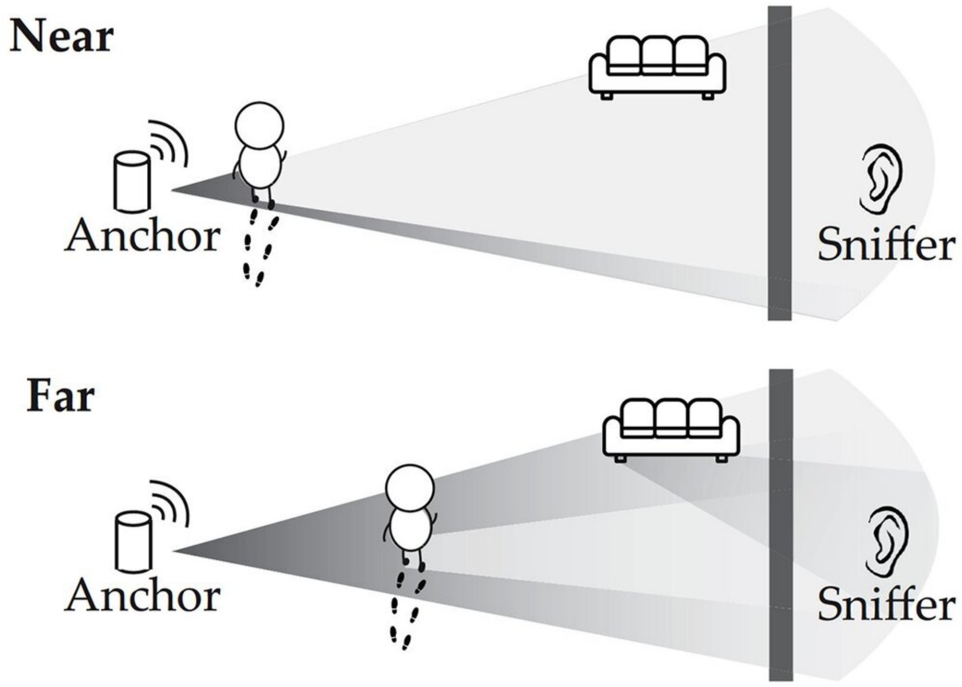

Illustration shows how inexpensive devices can turn Wi-Fi signals into motion detectors. Credit: University of Chicago

As connected devices such as voice assistants, security cameras, and smart appliances grow in popularity, the homes and offices where they are installed become increasingly filled with a dense web of Wi-Fi signals.

A new study from University of Chicago and University of California, Santa Barbara researchers finds that external attackers can use inexpensive technology to turn these ambient signals into motion detectors, monitoring activity inside a building without being detected themselves.

With only a small, commercially available Wi-Fi receiver, an attacker from outside the target site can measure the strength of signals emitted from connected devices and monitor a site remotely for motion, sensing whether a room is occupied. The research, led by leading UChicago computer scientists Heather Zheng and Ben Zhao, reveals the technique of these attacks as well as potential defenses.

"It's what we call a silent surveillance attack," said Zheng, a Neubauer Professor of Computer Science at the University of Chicago and expert on networking, security and wireless technologies. "It's not just about privacy, it's more about physical security protection. By just listening to existing Wi-Fi signals, someone will be able to see through the wall and detect whether there's activity or where there's a human, even without knowing the location of the devices. They can essentially do a monitoring surveillance of many locations. That's very dangerous."

The research builds upon earlier findings that exposed the ability to "see through walls" using Wi-Fi signals. However, previous methods detected indoor activity by sending signals into the building and measuring how they are reflected back to a receiver, a method that would be easy to detect and defend against. The new approach requires only "passive listening" to a building's existing Wi-Fi signals, does not need to transmit any signals or break encryption, and grows more accurate when more connected devices are present, raising significant security concerns.

"The worrisome thing here is that the attacker has minimal cost, can stay silent without emitting any signal, and still be able to get information about you," Zheng said.

Connected devices typically do not communicate with the internet directly, but do so by regularly transmitting signals to an access point, a hardware device such as a router. When a person walks nearby either device in this conversation, it changes the signal subtly, such that the perturbation can be detected by a nearby receiver "sniffing" the signal. That's enough information for an observer to know if a person (or large animal, the researchers add) is in the room, with very high accuracy.

Because most building materials do not block the propagation of Wi-Fi signals, the receiver does not even need to be in the same room or building as the access point or connected devices to pick up these changes. These Wi-Fi sniffers are available off the shelf and inexpensive, typically less than $20. They're also small and unobtrusive, easy to hide near target locations, and passive—sending no signal that could be detected by the target.

The researchers also suggested different methods to block this surveillance technique. One protection would be to insulate buildings against Wi-Fi leakage; however, this would also prevent desirable signals, such as from cellular towers, from entering. Instead, they propose a simple technical method where access points emit a "cover signal" that mixes with signals from connected devices, producing false data that would confuse anyone sniffing for Wi-Fi signatures of motion.

"What the hacker will see is that there's always people around, so essentially you are creating noise, and they can't tell whether there is an actual person there or not," Zheng said. "You can think about it as a privacy button on your access point; you click it on and sacrifice a little bit of the bandwidth, but it protects your privacy."

Zheng hopes that router manufacturers will consider introducing this privacy feature in future models; some of those firms have announced new features that use a similar method for motion detection, marketed as a home security benefit. The UChicago research has already received attention from Technology Review, Business Insider and other tech publications, raising awareness of this new vulnerability.

The study also reflects a growing research area in the Department of Computer Science, examining issues around increasingly prevalent connected "Internet of Things" devices. The IoT Security and Privacy Group, which includes Zhao and Zheng and additional faculty members including Nick Feamster, Blase Ur, and Marshini Chetty, will investigate both the benefits and potential vulnerabilities of these technologies, and a new IoT Lab in the Center for Data and Computing provides devices for researchers and students to hack and study for research.

More information: "Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors," Zhu et al., accepted for the Network and Distributed Systems Security (NDSS) symposium in February 2020. arxiv.org/abs/1810.10109

Provided by University of Chicago

Citation: How hackers could use Wi-Fi to track you inside your home (2019, November 15) retrieved 20 April 2024 from https://techxplore.com/news/2019-11-hackers-wi-fi-track-home.html