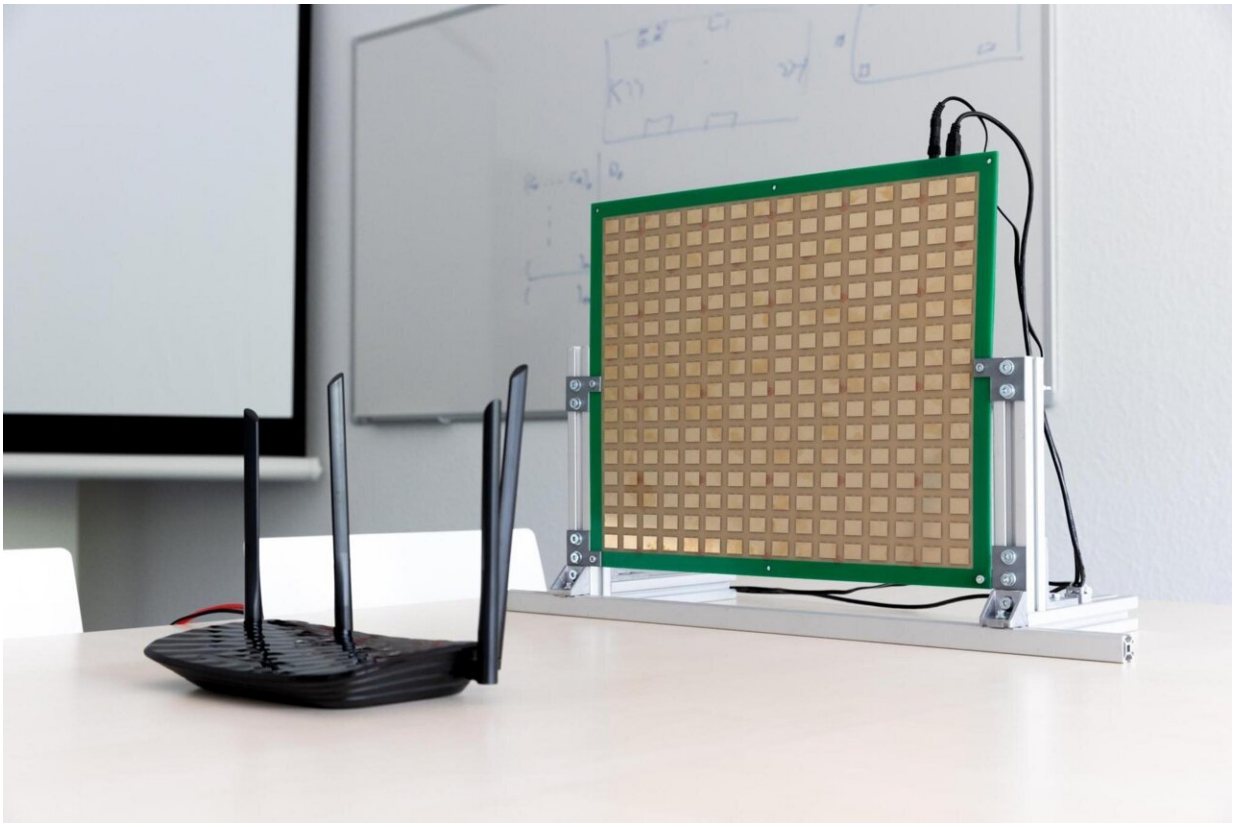
New countermeasure against unwanted wireless surveillance

May 24 2022



The intelligent reflecting surface IRShield is positioned next to a Wi-Fi router for obfuscation of the environment-dependent wireless channel. Credit: CASA, Michael Schwettmann

Smart devices are supposed to make our everyday lives easier. At the

same time, however, they are a gateway for passive eavesdropping. To prevent possible surveillance of the movement profile within one's home, researchers from the Max Planck Institute for Security and Privacy, the Horst Görtz Institute for IT Security at Ruhr-Universität Bochum and the Cologne University of Applied Sciences have developed a novel system for protecting privacy in wireless communication. The method, based on the technology of intelligent reflective surfaces, will be presented by the researchers on 24 May 2022 at the IEEE Symposium on Security and Privacy.

Surveillance of premises from a distance

Almost all Internet-of-Things devices, such as voice assistants, locks and cameras, rely on wireless connections based on high-frequency radio signals. Although cryptographic techniques are already in use to ensure data confidentiality, passive eavesdroppers can still exploit sensitive information from intercepted radio frequency signals. This is possible because the propagation of the signals is affected by the physical environment of the devices—by reflections from walls, objects and people present. Attackers can perceive such effects from a distance and, by applying simple statistical methods, conclude, for example, that a person is currently moving in the monitored room.

Innovative approach against wireless eavesdropping attacks

To counter this method known as "adversarial wireless sensing," the team investigated the use of Intelligent Reflecting Surfaces (IRS). IRS are considered a forward-looking technology for establishing intelligent wireless environments: here, many reflective elements are distributed over a surface and their reflective behavior can be individually and electronically adjusted. This allows the elements to dynamically

manipulate the incident radio waves. For example, IRS can be configured to reflect signals in a specific direction.

With their approach, the researchers are the first in the world to propose IRS as a practical countermeasure against passive wireless eavesdropping attacks. As a novel countermeasure, they have developed a system called "IRShield." IRShield uses a specially designed algorithm that creates a random IRS configuration, i.e., randomly aligns the reflective elements. This disguises the wireless channels in such a way that attackers can no longer read information about movements in the room from the signal.

In this context, IRShield is designed as a standalone, privacy-friendly extension for plug-and-play integration into existing wireless infrastructures. In contrast to previous research in the field, the IRShield researchers were able to meet three important requirements with their approach: the solution works independently of the devices, radio waveforms, and standards used; it does not compromise the quality of the wireless link; and it achieves very high channel obfuscation.

Pioneering research results

The team tested how successfully IRShield can prevent state-of-the-art human motion detection attacks using off-the-shelf Wi-Fi devices: 95 percent of the attacks were unsuccessful thanks to IRShield. In certain cases, it even made motion detection largely impossible, regardless of the attacker's strategy. The team's findings can serve as a starting point for much further work, such as optimizing IRS configurations or investigating methods used by more advanced attackers.

More information: IRShield: A countermeasure against adversarial physical-layer wireless sensing, IEEE Symposium on Security and Privacy, USA, 2022, DOI: 10.1109/SP46214.2022.00097. doi.ieeecomputersociety.org/10 … 9/SP46214.2022.00097

Provided by Ruhr-Universitaet-Bochum