

## Pressemitteilung

Nr. 35 vom 24. Mai 2022

### **Neue Gegenmaßnahme gegen unerwünschte drahtlose Überwachung**

**Drahtlos funktionierende Geräte, wie Router oder Sprachassistenten, sind in unseren Haushalten mittlerweile omnipräsent. Zugleich gefährdet die drahtlose Kommunikation unsere Privatsphäre: Passive Lauscher sind in der Lage, durch abgehörte Hochfrequenzsignale an sensible Daten zu gelangen. Intelligente reflektierende Oberflächen könnten eine wirksame Gegenmaßnahme sein.**

Smarte Geräte sollen unseren Alltag erleichtern. Zugleich sind sie jedoch ein Einfallstor für passive Lauschangriffe. Um eine mögliche Überwachung des Bewegungsprofils in den eigenen vier Wänden zu verhindern, haben Forscher\*innen vom Max-Planck-Institut für Sicherheit und Privatsphäre (MPI-SP), des Horst-Görtz-Instituts für IT-Sicherheit (HGI) und der Technischen Hochschule Köln (TH Köln) ein neuartiges System zum Schutz der Privatsphäre bei drahtloser Kommunikation entwickelt. Das Verfahren, basierend auf der Technologie intelligenter reflektierender Oberflächen, stellen die Forscher\*innen am 24. Mai 2022 auf dem IEEE Symposium on Security and Privacy vor.

#### **Überwachung von Räumlichkeiten aus der Ferne**

Fast alle Internet-of-Things-Geräte (IoT), wie beispielsweise Sprachassistenten, Schlösser und Kameras, sind auf drahtlose Verbindungen angewiesen, die auf hochfrequenten Funksignalen basieren. Obwohl bereits kryptographische Verfahren zum Einsatz kommen, um die Vertraulichkeit von Daten zu gewährleisten, können passive Lauscher noch immer sensible Informationen aus abgehörten Hochfrequenzsignalen nutzen. Dies ist möglich, da die Ausbreitung der Signale von der physikalischen Umgebung der Geräte beeinflusst wird → durch Reflexionen an Wänden, Gegenständen und anwesenden Personen. Angreifer können solche Effekte aus der Ferne wahrnehmen und durch die Anwendung einfacher statistischer Methoden zum Beispiel darauf schließen, dass sich gerade eine Person im überwachten Raum bewegt.

#### **Innovativer Ansatz gegen drahtlose Abhörangriffe**

Um dieser als „Adversarial Wireless Sensing“ bezeichneten Methode entgegenzuwirken, untersuchte das Team die Anwendung intelligenter reflektierender Oberflächen (Intelligent Reflecting Surfaces = IRS). Die IRS gelten als zukunftsweisende Technologie zur Einrichtung intelligenter Funkumgebungen: Viele reflektierende Elemente sind hierbei über eine Oberfläche verteilt und ihr Reflexionsverhalten ist individuell und elektronisch einstellbar. Dadurch können die Elemente die auftreffenden Funkwellen dynamisch manipulieren. So können IRS beispielsweise so konfiguriert werden, dass sie Signale in eine bestimmte Richtung reflektieren.

Mit ihrem Ansatz sind die Forscher\*innen weltweit die ersten, die IRS als praktische Gegenmaßnahme gegen passive drahtlose Abhörangriffe vorschlagen. Als neuartige Gegenmaßnahme haben sie ein System mit dem Titel „IRShield“ entwickelt: IRShield nutzt einen speziell entwickelten Algorithmus, der eine zufällige IRS-Konfiguration erzeugt, also die reflektierenden Elemente zufällig

Referat Kommunikation und Marketing  
Presse- und Öffentlichkeitsarbeit  
Christian Sander  
0221-8275-3582  
pressestelle@th-koeln.de

#### **Technische Hochschule Köln**

Postanschrift:  
Gustav-Heinemann-Ufer 54  
50968 Köln

Sitz des Präsidiums:  
Claudiusstraße 1  
50678 Köln

Pressemitteilung Nr. 35 vom 24. Mai 2022  
IRShield

ausrichtet. Das verschleiert die drahtlosen Kanäle so, dass Angreifer keine Informationen über Bewegungen im Raum mehr aus dem Signal auslesen können. IRShield ist dabei als eigenständige, datenschutzfreundliche Erweiterung für die Plug-and-Play-Integration in bestehende drahtlose Infrastrukturen konzipiert. Im Gegensatz zu bisherigen Forschungsarbeiten auf dem Gebiet konnten die Forscher\*innen mit IRShield drei wichtige Anforderungen mit ihrem Ansatz erfüllen: (1) Die Lösung funktioniert unabhängig von den eingesetzten Geräten, den verwendeten Funkwellenformen und Standards, (2) sie beeinträchtigt die Qualität der drahtlosen Verbindung nicht und (3) sie erreicht eine sehr hohe Kanalverschleierung.

### **Zukunftsweisende Forschungsergebnisse**

Das Team testete, wie erfolgreich IRShield hochmoderne Angriffe zur Erkennung menschlicher Bewegungen mit handelsüblichen Wi-Fi-Geräten verhindern kann: 95 Prozent der Angriffe waren dank IRShield erfolglos. In bestimmten Fällen machte es die Bewegungserkennung unabhängig von der Strategie des Angreifers sogar weitgehend unmöglich. Die Ergebnisse des Teams können als Ausgangspunkt für viele weitere Arbeiten dienen, die zum Beispiel IRS-Konfigurationen optimieren oder Methoden fortschrittlicherer Angreifer untersuchen.

### **Förderung**

Die Arbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projekts MetaSEC (Förderkennzeichen 16KIS1234K) und der Deutschen Forschungsgemeinschaft im Rahmen des Exzellenzclusters Cyber Security in the Age of Large-Scale Adversaries, CASA (EXC 2092 – 390781972) unterstützt.

### **Originalveröffentlichung**

Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, Christof Paar: IRShield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing, IEEE Symposium on Security and Privacy, 2022, DOI:  
<https://doi.ieeecomputersociety.org/10.1109/SP46214.2022.00097>

Die **TH Köln** zählt zu den innovativsten Hochschulen für Angewandte Wissenschaften. Sie bietet Studierenden sowie Wissenschaftlerinnen und Wissenschaftlern aus dem In- und Ausland ein inspirierendes Lern-, Arbeits- und Forschungsumfeld in den Sozial-, Kultur-, Gesellschafts-, Ingenieur- und Naturwissenschaften. Zurzeit sind rund 27.000 Studierende in etwa 100 Bachelor- und Masterstudiengängen eingeschrieben. Die TH Köln gestaltet Soziale Innovation – mit diesem Anspruch begegnen wir den Herausforderungen der Gesellschaft. Unser interdisziplinäres Denken und Handeln, unsere regionalen, nationalen und internationalen Aktivitäten machen uns in vielen Bereichen zur geschätzten Kooperationspartnerin und Wegbereiterin.