RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCE MAGAZINE

SPECIAL ISSUE

IT SECURITY

Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications

#33
Volume

Special Issue
2023

Hardware Protection

WHEN THE **HARDWARE** TRAPS **CRIMINALS**

Up to now, protecting hardware against manipulation has been a laborious business: expensive, and only possible on a small scale. And yet, two simple antennas might do the trick.

Payment transactions, business secrets, documents that are important for national security: today, the world's most valuable secrets are often no longer stored on paper, but rather as ones and zeros in virtual space. When we suspect that these secrets are in danger, we usually imagine a threat from afar – attackers trying to capture confidential data through cyberattacks. But there is another threat, a much more direct way to get into other people's systems, namely by tampering with the hardware. The valuable information is ultimately nothing more than electrical currents that travel between different computer components via conductive paths. A tiny metallic object, positioned in the right place on the hardware, can be enough to tap into these data streams.

"Fraudsters have used this simple method, for example, to tap credit card data from card readers," say Paul Staat and Johannes Tobisch. Both are doing their PhDs at the Horst Görtz Institute for IT Security at Ruhr University Bochum and research at the Max Planck Institute for Security and Privacy in Bochum. As members of Professor Christof Paar's team, they are developing methods to protect against hardware manipulation. They are cooperating with Professor Christian Zenger from the Ruhr University spin-off company PHYSEC, who laid the foundations for this technology when he was a researcher at Ruhr University and who has recently been appointed as Junior Professor at the Faculty of Electrical Engineering and Information Technology.

Mechanisms designed to protect hardware from tampering do exist, of course. "Typically, it's a type of foil with thin wires in which the hardware component is wrapped," explains Staat. "If the foil is damaged, an alarm is triggered." However, this method can only be used to protect small components, not the whole system: it's impossible to wrap an entire computer case in the foil, but only an individual key component like a memory element or a processor, for example. But Tobisch and Staat are working on a technology that would monitor entire systems for manipulation – and wouldn't be so expensive.

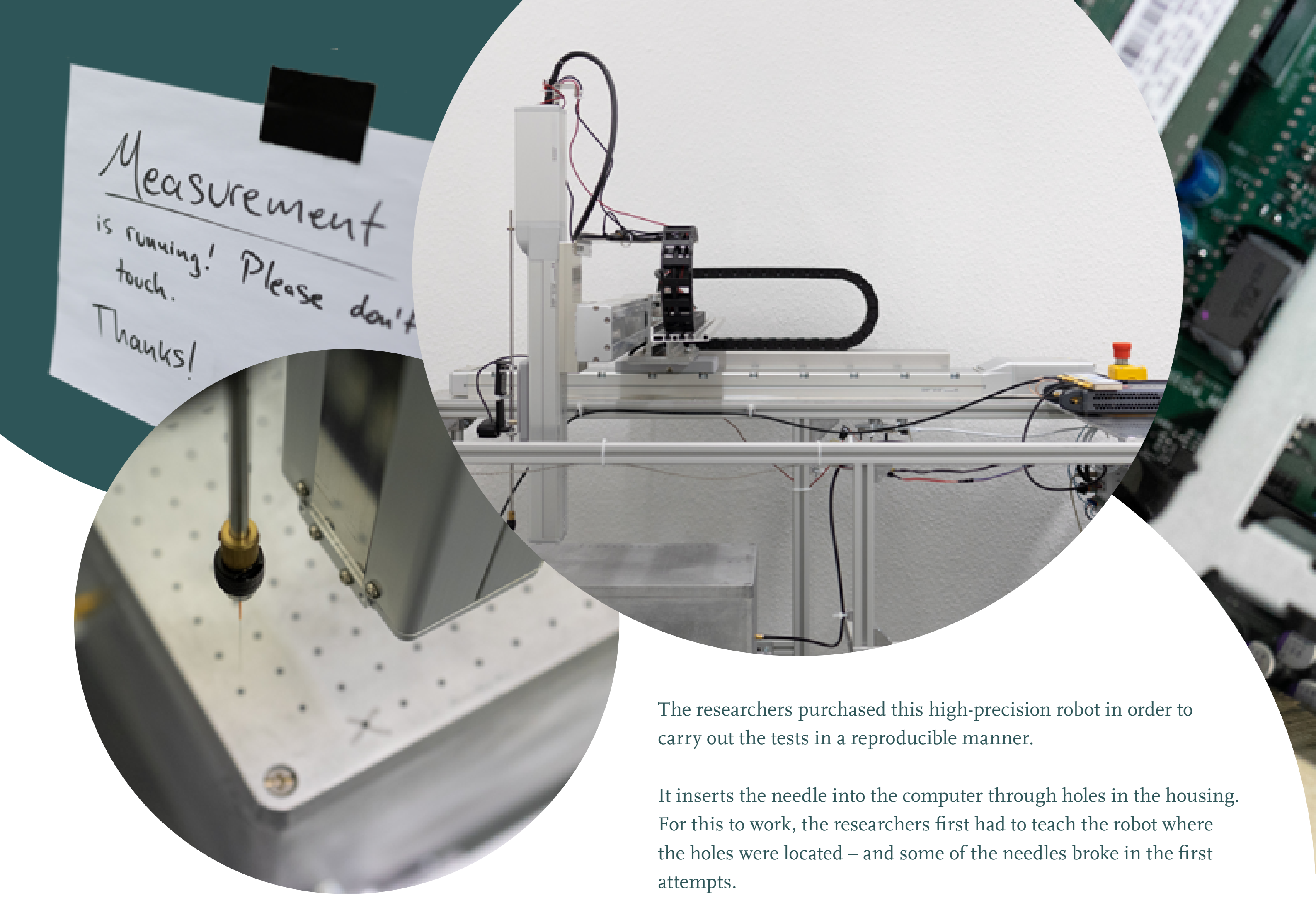
For this purpose, the researchers employ radio waves. They install two antennas in the system that they want to monitor: a transmitter and a receiver. The transmitter sends out a special radio signal that spreads everywhere in the system and is reflected by the walls and computer components. All these reflections cause a signal to reach the receiver that is ▸

Paul Staat (left) and Johannes Tobisch are doing their PhDs at Ruhr University and conducting research at the Max Planck Institute for Security and Privacy in Bochum.

i MANIPULATED CARD READERS

Researchers from Cambridge showed as early as 2008 how easily various card readers can be manipulated – even though the manufacturers had built in protection against manipulation. This protection, however, only secures individual components of the devices, such as the processor. But the data can still be tapped on the circuit board tracks: the researchers succeeded in reading out both the data of the cards and the PINs that were entered. Criminals adopt a similar approach and even modify card readers in such a way that data can be read out and transmitted via Bluetooth. "There's a regular market for such manipulations," says Paul Staat.

With the aid of a high precision robot, the researchers investigate, whether their new method can detect hardware manipulations.



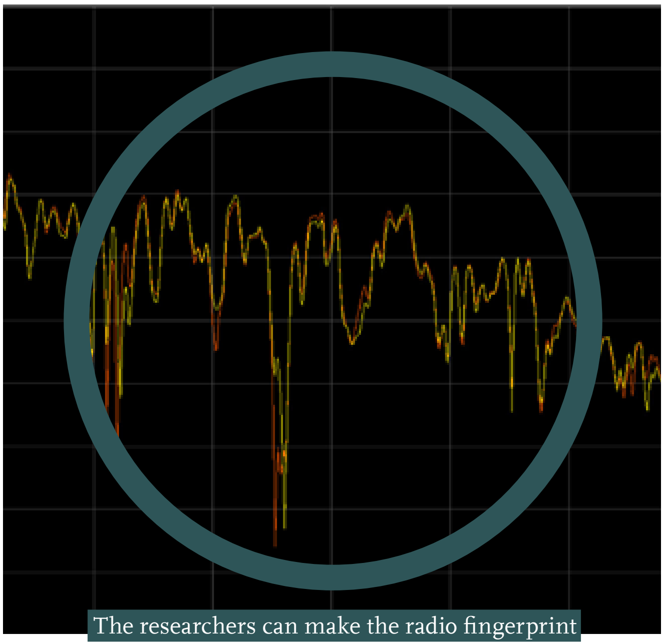
The researchers purchased this high-precision robot in order to carry out the tests in a reproducible manner.

It inserts the needle into the computer through holes in the housing. For this to work, the researchers first had to teach the robot where the holes were located – and some of the needles broke in the first attempts.

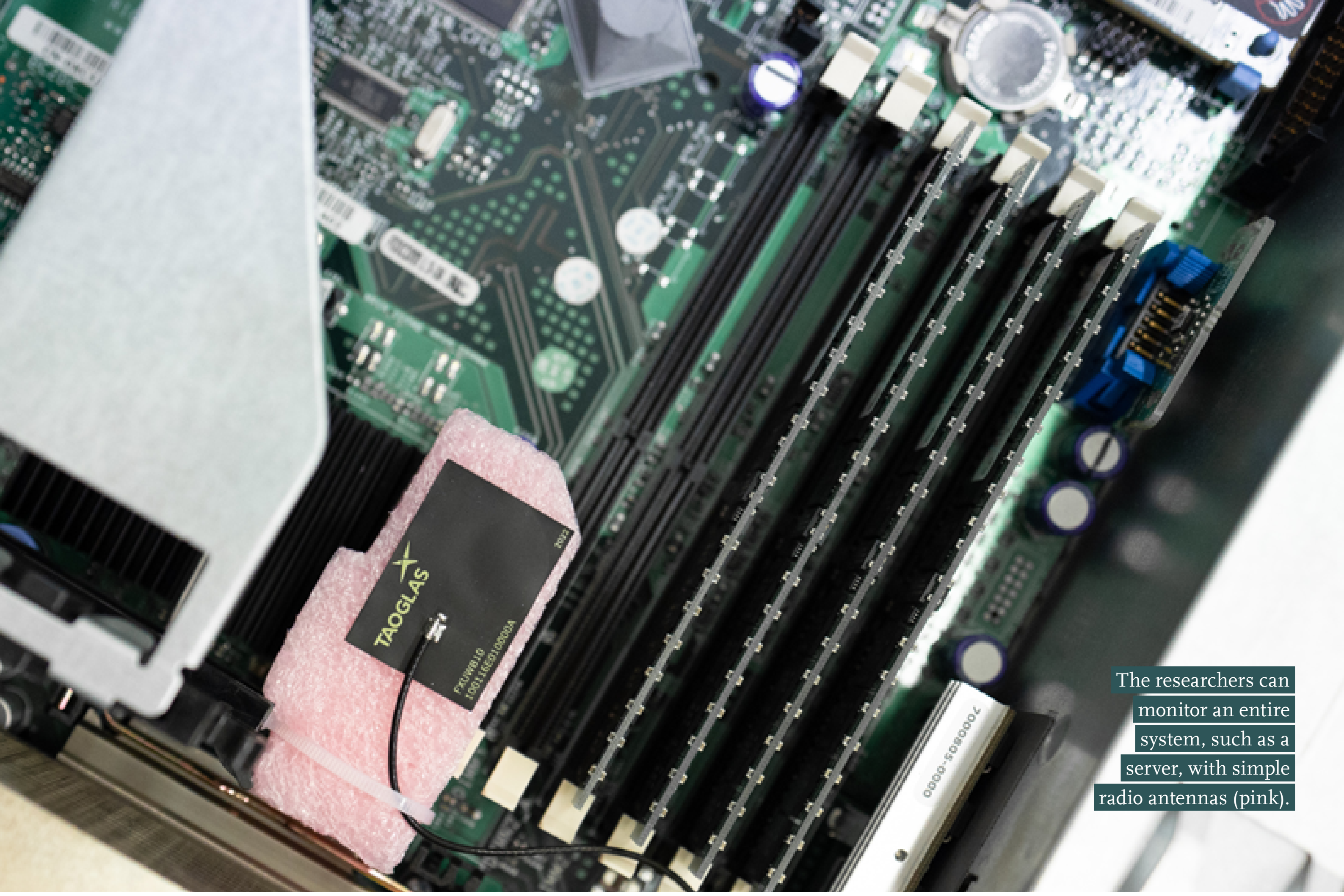
as characteristic of the system as a fingerprint. Tiny changes to the system are enough to have a noticeable effect on the fingerprint, as a demonstration by the two researchers shows: they have built their radio technology into an old computer housing. The measured radio signal is rendered visible on a laptop as a curve that shows the strength of the signal at different frequencies in real time. Then, Staat and Tobisch unscrew one of the screws on the outside of the housing a little. The frequency curve reacts with a noticeable deflection that wasn't there before.

For their research, Johannes Tobisch and Paul Staat take a more systematic approach. Their test object is a conventional computer with holes drilled in its casing at regular intervals. Through these holes, the researchers can let a fine metal needle penetrate the inside of the system and check whether they notice the change in the radio signal. In the process, they vary the thickness of the needle, the position and the depth of penetration. To ensure that the experiment takes place under controlled and reproducible conditions, the researchers have specifically purchased a high-precision robot that inserts the needle into the housing with micrometre precision.

"A unique aspect of our approach is that we are carrying out the experiment while the computer is running," points out Tobisch. This causes all kinds of interference. "The fans are like little hoovers and the processor is like a heater," il-



The researchers can make the radio fingerprint visible as a curve (red). It shows the strength of the signal at different frequencies. If the needle penetrates the system, the curve will show significant deflections (yellow). (Image: Paul Staat)



The researchers can monitor an entire system, such as a server, with simple radio antennas (pink).

lustrates Staat. These fluctuations in the ambient conditions affect the radio signal. The researchers have to measure such disturbances and factor them out in order to determine whether fluctuations in the signal are legitimate or the result of manipulation.

The IT experts from Bochum can reliably detect the penetration of a needle 0.3 millimetres thick with their system from a penetration depth of one centimetre. The system still detects a needle that is only 0.1 millimetres thick – about as thick as a hair – but not in all positions. “The closer the needle is to the receiving antenna, the easier it is to detect,” explains Staat. The thinner and further away the needle, the more likely it is to go undetected. The same applies to the penetration depth: the deeper the needle is in the system, the easier it is to detect. “Therefore, in practical applications, it makes sense to think carefully about where you place the antennas,” as Tobisch sums up the findings. “They should be as close as possible to the components that require special protection.”

Johannes Tobisch and Paul Staat let their experiment run for ten days, thus showing that the measuring system remains stable over a prolonged period. Later, they even extended the measurement period to a whole month. In addition to expensive high-precision measuring technology for recording the fingerprint, they also compared the radio signal with simple technology that sells for a handful of euros. They found that this technology did the job, too, albeit with a slightly lower hit rate. “It’s always a compromise between cost and accuracy,” says Paul Staat.

Depending on the intended use, the impact of ambient conditions would also have to be taken into account. After all, if the temperature or humidity in the room changes, these changes can also affect the radio fingerprint. “We hope to tackle such problems in the future with the help of machine learning,” anticipates Johannes Tobisch. The idea is that artificial intelligence could autonomously learn which changes in the radio signal are due to non-critical changes in the surroundings and which are due to manipulation.

“Fundamentally, there’s nothing standing in the way of a broad application of this technology. It is suitable for both high-security applications and everyday problems,” stresses Christian Zenger, founder and CEO of PHYSEC. The IT company already uses the technology to prevent unauthorised manipulation of critical infrastructure components. “There are plenty of other technical systems that need to be protected not only from remote cyberattacks but also from hardware manipulation,” he adds. “Examples include control units in cars, electricity meters, medical devices, satellites and service robots.”

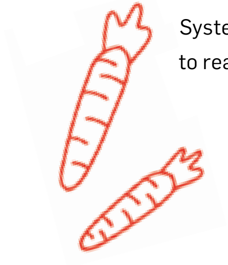
text: jwe, photos: ms

EDITOR'S DEADLINE

CASA UNIVERSE
WHAT'S THE FUZZ ABOUT HUB C AND THE MISSING CARROTS?
A JOURNEY THROUGH THE SECRETS OF SECURE SYSTEMS AND THE EXCITING RESEARCH WORLD OF CASA
CHALLENGE 1
BUILDING SECURE SYSTEMS

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

↗ *casa.rub.de/en/outreach/science-comics*



Answers
DEEP FAKE-QUIZ
The following faces are real:
1a, 2a, 3b, 4a, 5b, 6a

??

LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

GRAPHIC DESIGN, ILLUSTRATION, LAYOUT:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639

Reprinting with reference to source and submission of proof copies