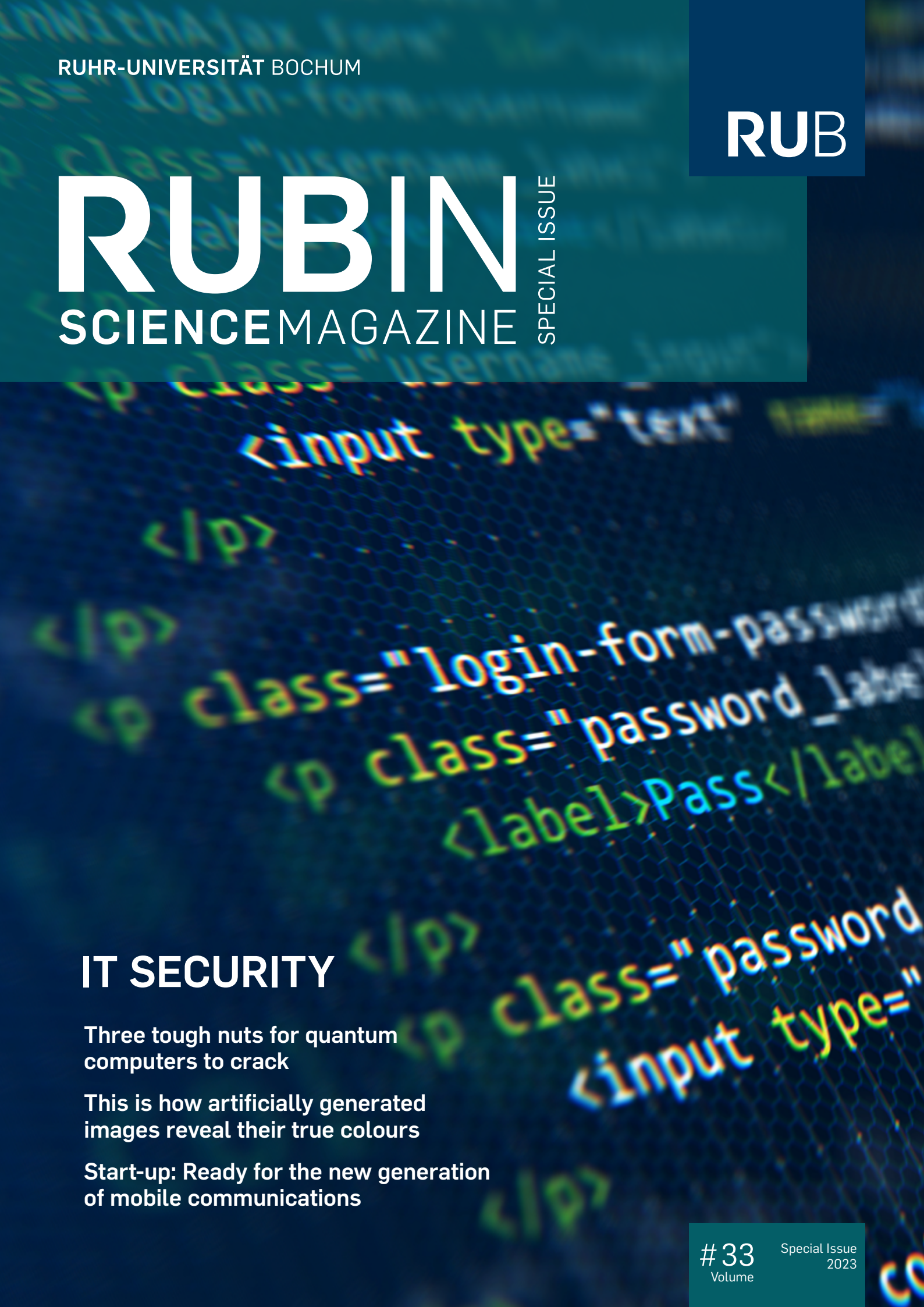
RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCEMAGAZINE

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

READY FOR THE NEW GENERATION OF MOBILE COMMUNICATIONS

5G has plenty more to offer than 4G. Radix Security makes sure that it doesn't leave any security gaps open.

When you pull out your smartphone to get directions or find out when the next bus is leaving, you usually get an answer right away. The processes in the background run so fast that you hardly notice they exist. But the data being transmitted has to cross a lot of interfaces. The smartphone has to connect to the nearest cell tower. That cell tower, in turn, is part of a nationwide network built and operated by the big telecom companies. Thus, the end user (almost) always has reception and can use his cell phone as a mobile device in the truest sense of the word.

To enable such connections anytime, anywhere, regardless of whether the device being used is the latest iPhone or a Nokia LTE banana phone, all parties involved must agree on the same communication standards. This applies not only to German networks, but also to networks around the world. The 3rd Generation Partnership Project (3GPP) is the organization responsible for negotiating and publishing these standards.

The so-called specifications comprise thousands of pages, and Dr. David Rupprecht is far more familiar with them than he would like to be. He and his colleagues at the Department of System Security at the Horst Görtz Institute for IT Security focused on the small and large errors in the standard. This is because such specification errors have a direct impact on the security of a connection and thus directly affect every single user of a network.

But that's just the beginning: even if the specification were 100 percent waterproof, the implementation step would still be missing. This is where pages and pages of instructions are used as a basis for implementing components. "In other words, anyone building components for a mobile network has to read thousands of pages of text, interpret them correctly, and finally convert them into bug-free code. And as if that were not enough of a challenge, they also have to deal with the enormous complexity of networks and components," says Rupprecht. And even assuming we have a 100 percent secure implementation, does it necessarily follow that we will have completely secure networks? "Unfortunately, even that's not enough," explains Rupprecht. "The different components ▸

FUNDING

The foundation of Radix Security is supported by the start-up incubators Cube 5 at Ruhr University Bochum and Mercator Launch at Radboud Universiteit.

Those who use their smartphones in everyday life do not question the processes that run in the background.

have to work together in a complex setup. Hardware from different manufacturers comes together, which means that the interaction has to be configured with great precision. This is the third and final source of error in the process.

In 2021, for example, David Rupprecht and researchers from the Chair of Symmetric Cryptography proved that the 2G cellular standard is very insecure. "We showed that it even had deliberately built in vulnerabilities that made it possible to intercept data," he explains (see page 36). The encryption algorithms were so weak that it couldn't have been an accident; it was a backdoor that had been deliberately adopted and implemented in the 1990s. Although this algorithm is still built into modern smartphones, the researchers believe that these vulnerabilities no longer pose a threat. After all, 2G is long outdated and hardly used anymore.

"Every ten years there's a new generation of mobile networks," says Rupprecht. With 2G, the focus was primarily on mobile telephony, 3G introduced mobile Internet. Since 4G, the focus has clearly been on using the Internet through applications. "The iPhone hit the market, and mobile Internet became a mass phenomenon," as David Rupprecht describes the period around 2010, when the standard was first introduced. To this day, most mobile connections use 4G. In his dissertation at the CASA Cluster of Excellence, Rupprecht examined the vulnerabilities of this generation.

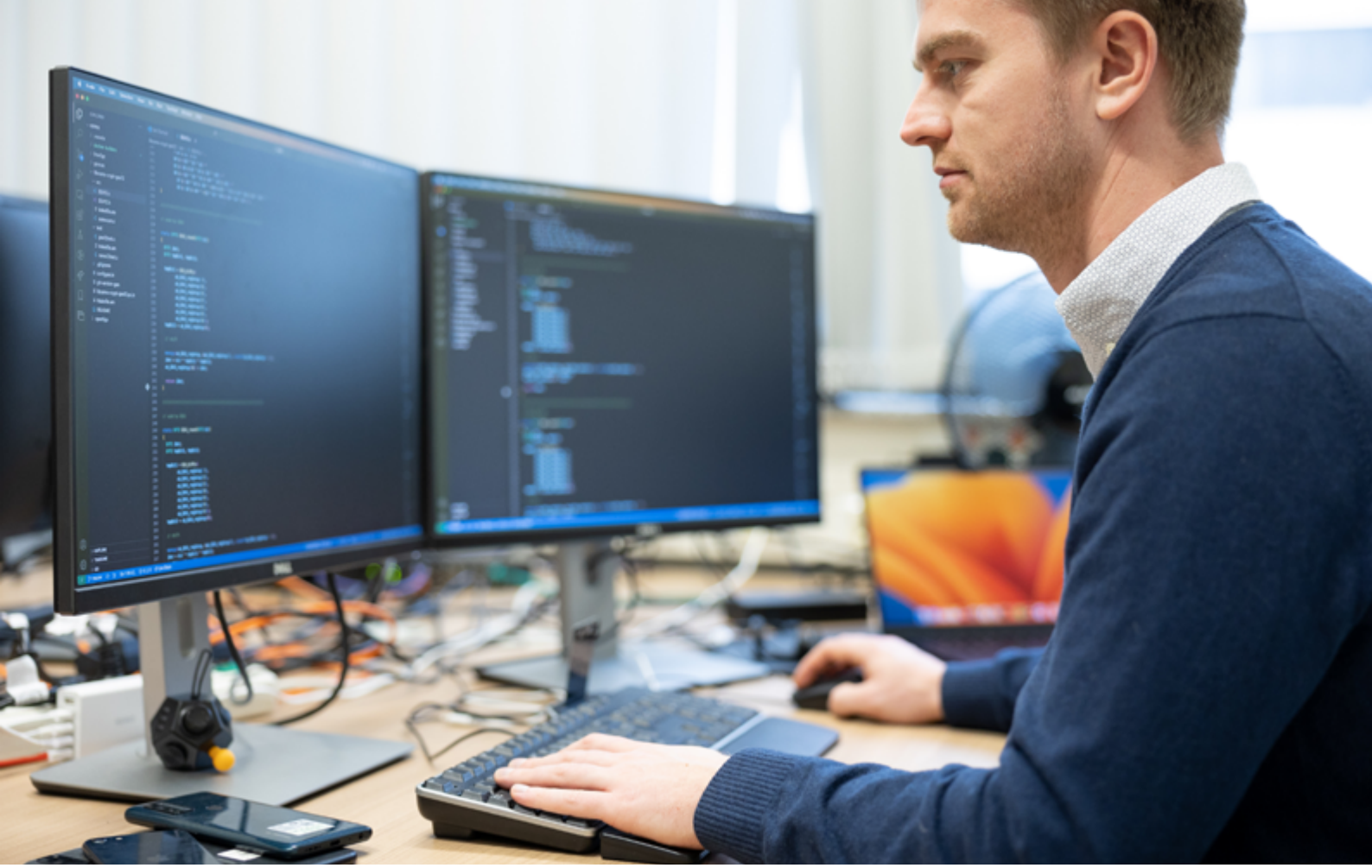
"In the process, we identified a number of vulnerabilities in CASA that affect just about every smartphone user. One of them made it possible to eavesdrop on phone calls. Wherever possible, the vulnerabilities have been closed by the manufacturers or operators," emphasizes David Rupprecht. Still, there is no such thing as ultimate security, because any gain in security always comes at the expense of performance. "The 3GPP committee has to weigh the pros and cons and take into account other important factors such as speed and battery life," he explains. In addition, security-related settings included in the specifications can sometimes be turned on and off by a network operator.

That much said, any analysis of security gaps in the current generation of mobile phones will always benefit the next generation as well. "The appropriate control measures can thus be planned right from the start and integrated into the next generation," explains David Rupprecht.

As far as he's concerned, the fifth generation (5G) is already in the spotlight. "5G is particularly interesting because it opens up many new application possibilities, such as internet of things (IoT). Cars will be able to communicate with traffic lights, factories will improve their internal networks, and critical infrastructure will gain new networking capabilities." In the case of factory networks, it's robots and industrial equipment that will be connected via a local 5G campus network – and for the first time by private operators. "This means that everyone can suddenly become a network operator," stresses David Rupprecht. The responsibility for the secure implementation and configuration of 5G networks now

> "5G IS PARTICULARLY INTERESTING BECAUSE IT OPENS UP MANY NEW APPLICATION POSSIBILITIES, SUCH AS INTERNET OF THINGS."
>
> David Rupprecht

David Rupprecht founds the company Radix Security together with Katharina Kohls.



David Rupprecht knows thousands of pages of specifications that ensure that everything works safely and smoothly in mobile networks.

lies with the private operators. This is where Radix Security comes in, a company that Rupprecht is currently building together with Professor Katharina Kohls.

"We have been working on security issues in 4G and 5G networks for years and have a huge head start in terms of know-how," Rupprecht points out. Although the specifications are publicly available, the question remains: who can understand and implement thousands of pages of complex information? Radix Security is committed to making 5G security accessible and helping campus network operators build and operate their networks securely. There are currently around 300 campus networks in Germany, including the Ruhr University Bochum, which operates one for research purposes.

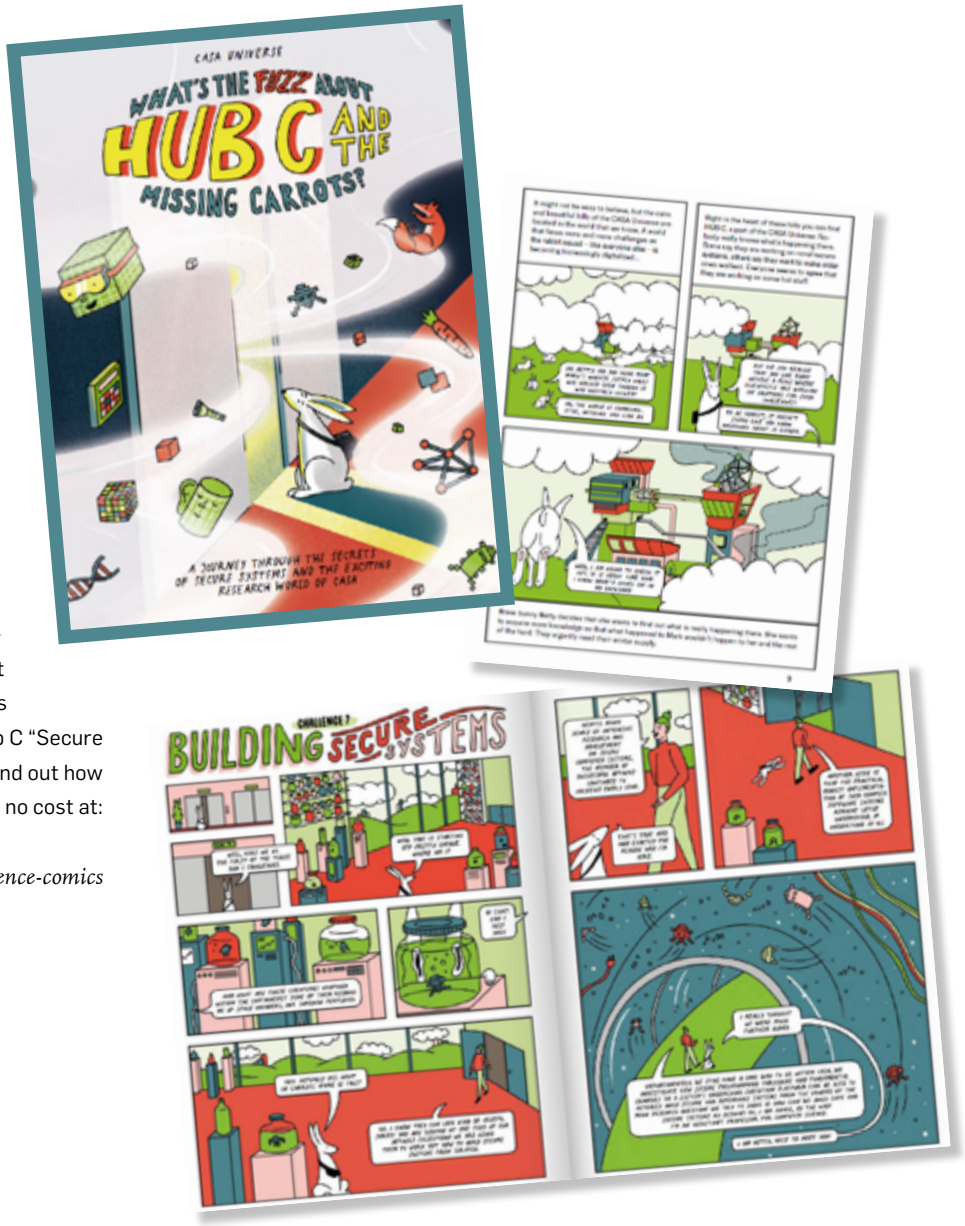
"At this stage, when campus networking technology is still in its relative infancy, we find that security plays little or no role," says Rupprecht. This is problematic because it takes far more resources to secure a network after the fact than it does to build security into the design from the beginning. "After the first exchanges, we realized that campus network operators have very different ideas about security requirements. This is where Radix Security will be doing a lot of outreach and training to educate about the security risks and opportunities of campus networks."

When it comes to securing a campus network, the right tool is essential. On the one hand, the goal is to prevent attacks by detecting weaknesses in the implementation and configuration of network components. The Radix Security test tool allows the user to test components for their security properties in a way that goes beyond the standard. For example, it checks whether a component issues important key material. If this is the case, the entire security of the network is compromised.

"In addition to testing, we need to enable a campus network to detect and defend itself against attacks," concludes David Rupprecht. To this end, Radix Security is developing an attack detection system tailored to campus network operators. The fundamental problem lies in the complexity of the networks and the open air interface. Unlike a wired network, an attacker only needs to be in the physical vicinity of the network to attack it. "In terms of all our developments and ideas, we benefit from being close to the university," Rupprecht adds. "The university gives us an advantage over our competitors; our research infrastructure, such as the CASA Cluster of Excellence, means that our customers benefit from cutting-edge research to protect themselves against the latest attacks."

text: md, photos: ms

EDITOR'S DEADLINE



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