RUHR-UNIVERSITÄT BOCHUM

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

Nachgehackt - The Bochum Podcast on IT Security

The world is becoming increasingly digital and IT security is becoming more and more important in everyday life. In the podcast „Nachgehackt“, host Henrik Hanses talks to experts and other exciting guests about different aspects of IT security - in a way that is also understandable for laypeople.

The podcast is presented by Cube 5 - Creating Security, the Horst Görtz Institute for IT Security at Ruhr University Bochum, the Cluster of Excellence CASA, PHYSEC GmbH, Bochum Economic Development and eurobits e. V.

„Nachgehackt“ is available on Spotify, Apple Podcast and wherever podcasts are available. Nachgehackt“ can be also watched as a video podcast on YouTube.

EDITORIAL

photo: ms

IT security is now an integral part of our digital experience. But this was not always the case: exactly 20 years ago, many experts still considered the research field of our department to be a niche topic. In defiance of the prevailing predictions, the Horst Görtz Institute for IT Security was founded at Ruhr University Bochum back in 2003, and the first German degree programme in IT security was established.

A lot has changed over the years. Back then, attacks on private individuals used to be isolated incidents carried out by non-professional hackers. Today, we are every day confronted with new headlines about cyber attacks on public authorities, companies and even critical infrastructures. Edward Snowden has made us aware of the true extent to which we are exposed to surveillance. Protection against such attacks is therefore essential for our society and economy.

In Bochum, we are researching the basic principles of IT security. This Rubin edition reveals what our researchers come up with in order to stay one step ahead. After all, this is and always has been the cornerstone of IT security: not only to be faster, but also to be more creative than your opponent.

We are aided in our endeavours by intelligent monkeys (page 28), mathematical lattice fences (page 10) and holes in a computer housing (page 44), to name but a few. But what exactly is it all about? Find out more here.

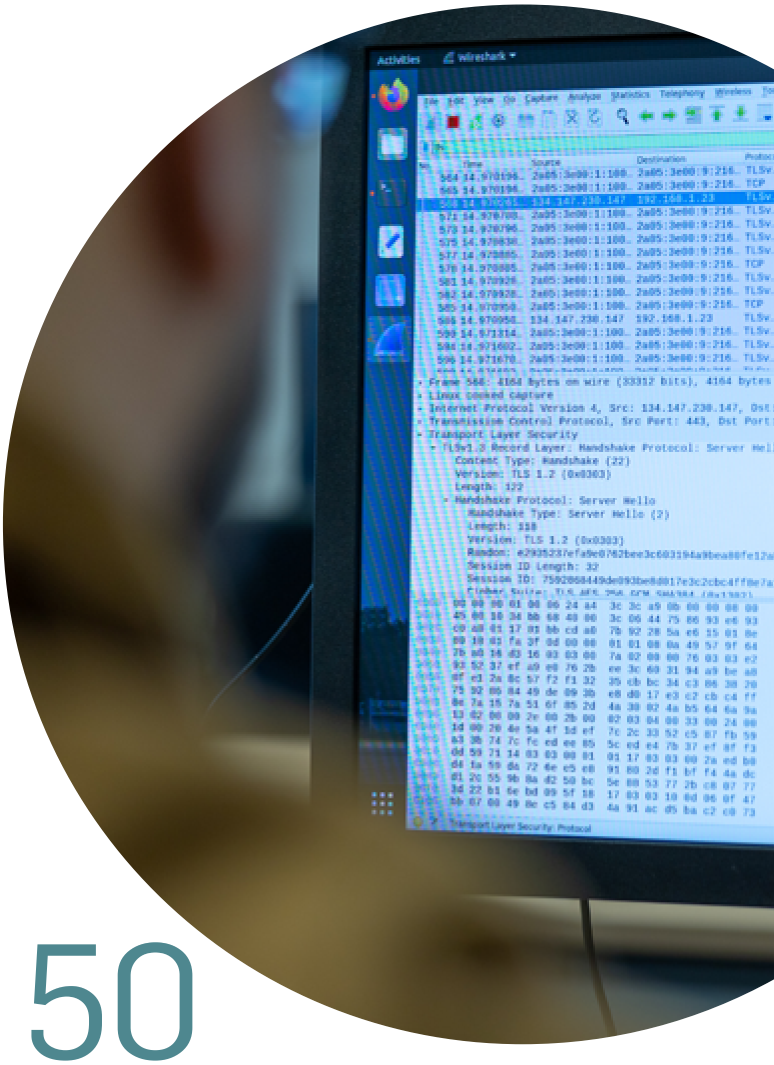
We hope you enjoy this edition.

Yours, Eike Kiltz,
Speaker of the Cluster of Excellence CASA
at the Horst Görtz Institute for IT Security

RUBIN ONLINE
All articles of this special issue:
➔ **news.rub.de/rubin-it-security-2023**

CONTENTS

14

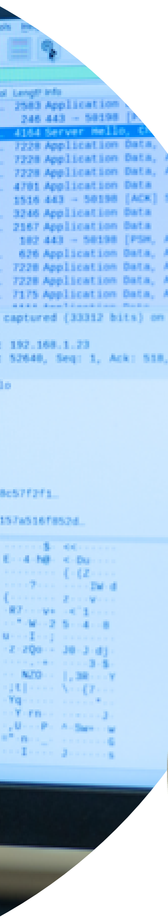


50

36

10

> ” FINALLY, I CAN EXPLAIN WHAT MY RESEARCH IS GOOD FOR. “
>
> Eike Kiltz



```
d Length Info
. 2583 Application
.  246 443 → 50198 [
. 4164 Server Hello, C
. 7228 Application Data,
. 7228 Application Data,
. 7228 Application Data, Ap
. 4701 Application Data
. 1516 443 → 50198 [ACK] Seq=
. 3246 Application Data
. 2167 Application Data
.  182 443 → 50198 [PSH, ACK] Seq
.  626 Application Data, Applicati
. 7228 Application Data, Applicatio
. 7228 Application Data, Application
. 7175 Application Data, Application
 captured (33312 bits) on interface a
: 192.168.1.23
: 52640, Seq: 1, Ack: 518, Len: 4096
lo
8c57f2f1…
157a516f852d…
```

40

rippple
TRON
WOW
wow much coin how money so crypto plz mine v rich very currency
ADA

49
CYB

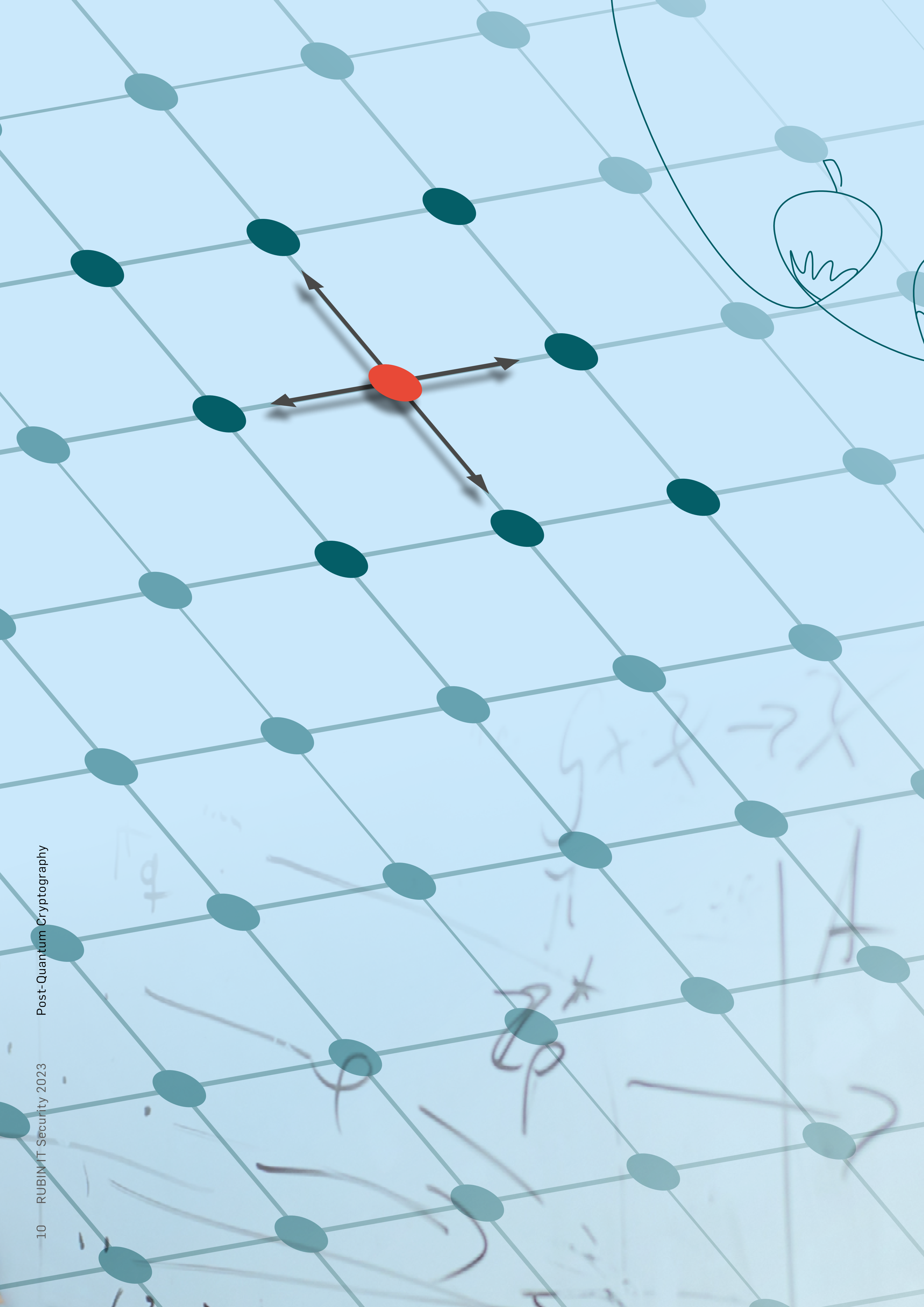
ARTWORK “APES”

On the face of it, art and IT security appear to be two diametrically opposed worlds. Members of the Cluster of Excellence CASA, the Horst Görtz Institute for IT Security and the Max Planck Institute for Security and Privacy have explored how the disciplines can mutually enrich each other in an artist residency. For two months, the researchers had an intensive exchange with the media artist Marco Barotti on research topics and visions for the future. Based on that, Barotti created the artwork “APES”, which can be seen here at an exhibition in Seoul. The kinetic sound sculptures present an unusual view of IT security, data protection, surveillance and sustainability. (photo: Marco Barotti)

one
you

DIS/PLAY

Bringing IT security to life – that's what the artwork "DIS/PLAY" is about. Artist Ralf Baecker created it for the Cluster of Excellence "CASA – Cyber Security in the Age of Large-Scale Adversaries". The installation is spread across the research and work areas in the MC building on the campus of Ruhr University Bochum. Displays distributed throughout the rest of the house respond to people passing by with messages that comment on the topics of surveillance and privacy in a humorous way. At the same time, the messages are sent throughout the building and eventually displayed in a large installation in the Open Space. The artwork thus transforms the building into a giant, distributed computer and screen: bits and bytes stream through the building, swarms of characters and numbers move through corridors and rooms. (photo: RUB, Kramer)



Post-Quantum Cryptography

THREE TOUGH NUTS FOR **QUANTUM COMPUTERS** TO CRACK

Algorithms made in Bochum are becoming the global standard for secure encryption in the age of quantum computing. They've arrived just in time.

It's still early in the morning and a bitterly cold day. You're about to leave for work. Fortunately, the car can be preheated remotely from your smartphone. Frozen door locks are also a thing of the past. The car can be opened effortlessly with the fingerprint scanner. Then, a brief voice command turns on the radio. The engine starts and the head-up display lights up. Off you go on a journey that feels safe even when you're a little tired, thanks to the lane keeping assist system.

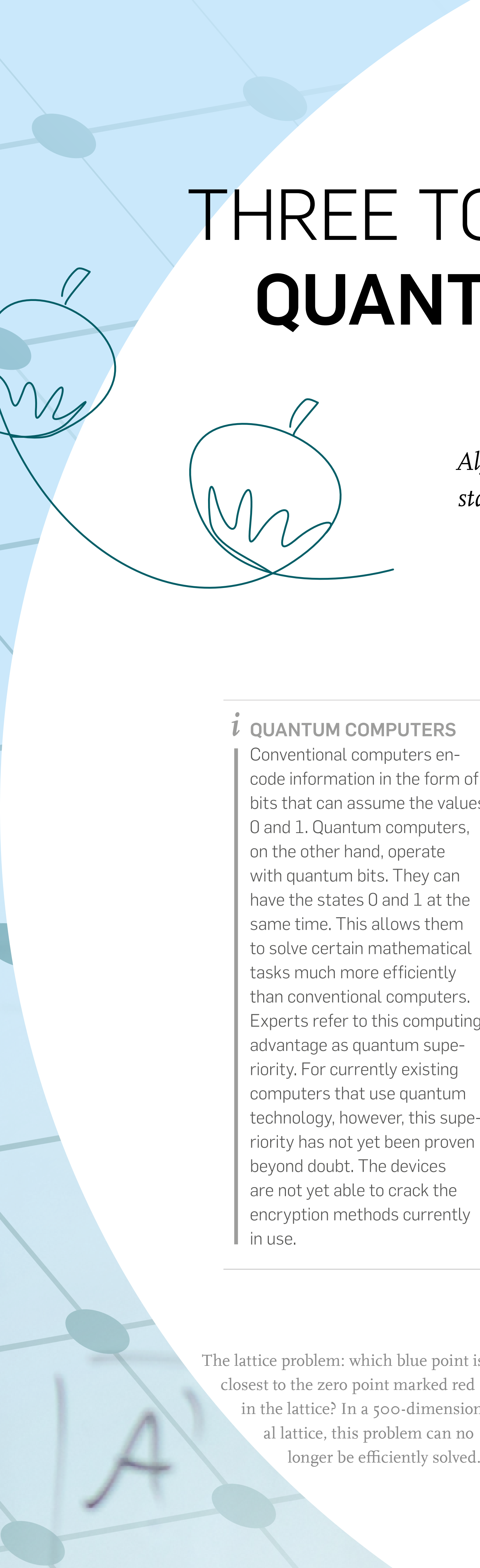
A modern car is more or less a computer. And like with all other computers, attackers can potentially gain control over the on-board systems. Therefore, the electronics in smart cars must be protected against cyberattacks. This includes not only the attacks that are possible today, but also those of tomorrow – because a car has a long lifespan. Vehicles that roll off the assembly line today may be around long enough to experience the age of quantum computers.

"Quantum computers will be able to crack some of the current encryption technologies without any problems," points out Professor Eike Kiltz. He heads the Chair for Cryptography and is one of the spokespersons for the Cluster of Excellence CASA – Cyber Security in the Age of Large-Scale Adversaries at the Horst Görtz Institute for IT Security. To ensure that today's technology will still be secure in the future, Eike Kiltz and his colleagues have developed new methods to protect data from attacks with quantum computers. CASA members Professor Tanja Lange, Professor Peter Schwabe and Professor Daniel Bernstein were instrumental in this work.

The team won a highly prestigious competition organised by the US National Institute of Standards and Technology (NIST) in 2016. NIST competitions have already taken place on a range of topics, with the aim of finding the best possible solutions to the most pressing problems in IT security. Research groups worldwide can submit their proposed solutions; the best approaches are then filtered out in a step-by-step process lasting several years. In the 2016 competition on secure ▸

i QUANTUM COMPUTERS

Conventional computers encode information in the form of bits that can assume the values 0 and 1. Quantum computers, on the other hand, operate with quantum bits. They can have the states 0 and 1 at the same time. This allows them to solve certain mathematical tasks much more efficiently than conventional computers. Experts refer to this computing advantage as quantum superiority. For currently existing computers that use quantum technology, however, this superiority has not yet been proven beyond doubt. The devices are not yet able to crack the encryption methods currently in use.



The lattice problem: which blue point is closest to the zero point marked red in the lattice? In a 500-dimensional lattice, this problem can no longer be efficiently solved.

algorithms against quantum computer attacks, 82 proposals were submitted. Four of them are now to be standardised, as NIST 2022 announced. Of these four winning methods, three come from the CASA Cluster of Excellence.

In the past, methods that have won the NIST competition have caught on at a worldwide scale. It can therefore be assumed that the quantum-safe CASA algorithms will be used for encryption and digital signatures all over the world in the future. The NSA, the largest foreign intelligence service in the United States, is already recommending that the US government use the Crystals-Kyber and Crystals-Dilithium methods, in the development of which Eike Kiltz and Peter Schwabe were involved.

Crystals-Kyber is used for encryption – for example, of data sent by e-mail or of credit card information submitted for online shopping. Crystals-Dilithium is designed to secure authentication processes, i.e. it's used when a person or an object has to prove their identity. For example, when an operating system is being updated, the software must prove that it is an official product of the manufacturer and doesn't come from a hacker.

With Crystals-Kyber and Crystals-Dilithium – fans of Star Wars and Star Trek will recognise that the names are an homage to the films – Eike Kiltz' research has been directly translated into application. For him, an unusual experience. This is because the computer scientist usually operates at the very edge of theory. Now, the CASA team's algorithms will be implemented all over the world. "We bear a great responsibility," says Kiltz, aware of this fact and at the same time pleased. "Finally, I can explain what my research is good for."

With their electronics, today's cars are effectively computers – and therefore vulnerable to cyberattacks. The quantum computers of tomorrow could be able to break today's encryption. Thus, it is important to protect technical devices with a long lifespan, such as cars, with future-proof algorithms.

At the core of his research are highly abstract questions, so-called hard mathematical problems. "These are problems that many brilliant minds have grappled with over the past decades without ever finding a solution," he explains. One of them is the lattice problem that constitutes the backbone of Crystals-Kyber and Crystals-Dilithium. To visualise the problem, imagine a two-dimensional lattice that has a zero point somewhere. Everywhere where lines cross, there are so-called intersection points. The question is: which intersection point is closest to the zero point? This is easy to answer for a two-dimensional lattice. The more dimensions you add, the more difficult it becomes. Above about 500 dimensions, there is no efficient solution to the problem.

The CASA algorithms are based on the lattice problem in a slightly simplified form: the search is not for the nearest intersection point, but for any intersection point that lies within a certain radius around the zero point. If, for example, a software update wants to prove to the operating system that it comes from an official software manufacturer, it must prove that it knows a secret – namely one of these intersection points near the zero point.

Since the lattice problem is mathematically different from the method on which standard encryption is based, quantum computers won't be able to solve it any more than conventional computers. "Quantum computers only have an advantage when it comes to highly specific tasks," says Eike Kiltz. This is always the case, for example, when you can express a task as a period-finding task. A period is the distance between the repetition of values in a function. If you imagine a sine curve, the period comprises a mountain and a valley of the curve. If a powerful quantum computer did exist, it could determine the period of any function very quickly.

This would be a problem for the commonly used encryption method RSA, which is based on the problem of prime factorisation. This mathematical exercise involves finding out, for a number with several hundred digits, which two prime numbers you'd have to multiply to get this number. This question can't be efficiently solved with conventional computers. Quantum computers, however, could do this easily, because prime factorisation can be described as a period-finding task. The same doesn't apply to the lattice problem. It is therefore safe from quantum computer attacks.

The Bochum-based researchers have now optimised their Crystals-Kyber and Crystals-Dilithium methods to such an extent that they can keep up with today's standard RSA method in terms of efficiency. The new methods are even two to three times faster than RSA, but they require ciphers that are 20

> ”FINALLY, I CAN EXPLAIN WHAT MY RESEARCH IS GOOD FOR.“
>
> Eike Kiltz

Together with colleagues, Eike Kiltz has developed new algorithms that are effective against quantum computer attacks. With these algorithms, the researchers won a multi-year competition.

to 30 times longer. “This means that you need a little more storage space, but you can use a smaller processor,” points out Eike Kiltz.

Still, it will take quite some time before the processes gain traction worldwide. Crystals-Kyber and Crystals-Dilithium are expected to be standardised in two years. According to Eike Kiltz’ estimates, implementation will then take another five to ten years. “The development process will be completed just in time,” says the Bochum-based researcher. He assumes that in 10 to 20 years quantum computers might exist that will be able to break conventional encryption methods. This still sounds a long way off. “But you have to consider that intelligence services, for example, store encrypted data that may still be relevant in the future – and in the future they may be able to decrypt it with the help of quantum computers,” illustrates Kiltz. Plus, there are the cars mentioned above, which will hit the roads in the coming years equipped with all kinds of electronics; they may still be driving around when quantum computers have long since become a reality.

text: jwe, photos: ms

i THIRD AWARD-WINNING METHOD

It wasn’t only Crystals-Kyber and Crystals-Dilithium that secured the CASA team its success in the NIST competition for quantum-safe methods, but also the Sphincs+ algorithm. Sphincs+ can be used to create secure digital signatures. It is based on hash functions. Hash functions create an output from any input, such as a file, that looks completely different from the input. If a minor change were made to the input file, the resulting output would look completely different. This is how the hash functions disguise the structure of the data. The method was for the most part developed by CASA member Peter Schwabe, a researcher working at the Max Planck Institute for Security and Privacy in Bochum.

Information Technology

APP-CEPTED?

Many countries have tried to reduce the infection rate with the help of Covid-19 apps. These only make a difference if people use them. Recent surveys show which factors play a role for the user acceptance of these apps.

Following the outbreak of the Sars-Cov-2 virus, many countries around the world introduced smartphone apps in an attempt to control the pandemic more effectively by enabling contact tracing and breaking infection chains as quickly as possible. The German government, too, urged citizens to install the so-called Corona-Warn-App, which would notify them if they recently had close contact with a person infected with the virus. How effective such apps are depends to a large extent on how widely they are accepted and, ultimately, how many people use them. What motivates people to use Covid-19 apps? And what puts them off? A research team at the Horst Görtz Institute for IT Security at Ruhr University Bochum led by Professor Markus Dürmuth and Dr. Christine Utz surveyed around 7,000 people on three continents to get to the bottom of these questions.

In order to figure out which factors influence people's decision to install an app or not, Utz and Dürmuth used a study design based on a technique extensively used in human-computer interaction and market research, the so-called vignette design. Market research in particular makes extensive use of this method. "Vignettes are short, fictitious scenarios that are presented to the survey participants who then have to answer questions about these scenarios. In our case, the questions are about fictitious Covid-19 apps with a range of different features that are based on real apps," explains Utz. "When it comes to Covid-19 apps, the context in which they are used is crucial," points out Dürmuth. "Which purpose does the app serve? What kind of data is collected and how long is it stored? Who can access the data? Our aim was to take all these dimensions and factors into account," says the IT expert.

In their studies, the researchers explored a total of eight app functionalities – such as the purpose of the app and the duration of data storage – with up to 16 different selection options. This combination resulted in around 50,600 different ▸

The Corona-Warn-App notified people if they recently had close contact with a person infected with the virus.

15:47

CORONA WARN-APP

Risiko-Ermittlung aktiv

Niedriges Risiko

Begegnungen mit niedrigem Risiko an 1 Tag

Am 14.03.2023

Aktualisiert: Heute, 13:45 Uhr

Tests erfassen und andere warnen

Selbsttest, PCR- und Schnelltest

Warnen Sie andere, wenn Sie positiv getestet sind, oder fordern Sie Ihr digitales COVID-Testzertifikat an. Finden Sie Teststellen in Ihrer Umgebung.

Weiter

Bestätigte Neuinfektionen

Bundesweit

Warn

über die C

Covid-19 warning apps are used to reduce the infection rate.

scenarios. One of them was, for example: "Imagine an app that is used for quarantine control and shares your location with the public health department and the local police once per hour." Every participant was presented with ten such scenarios and asked to rate how likely they would be to use each presented app. "The advantage of this design is that it ultimately enables us to calculate from the data how various factors influence overall acceptance and to precisely describe which factors influence user acceptance to a great extent and which do not," outlines Dürmuth.

For the initial surveys in summer 2020, the researchers addressed 1,000 participants from China, the USA and Germany each. "In China, where the pandemic first broke out, people are more accustomed to government-issued apps, which is why this country was of interest for us," explains Dürmuth. Germany was also an obvious choice as a destination for the study. "In terms of privacy expectations, Germany represents the European attitude during this period," Dürmuth continues. "The USA were massively hit by the virus at the time of our first study. We expected that people in the USA would view the use of the apps in a different light and consider, for example, the protection of their privacy less important," Utz explains the choice.

At the time the survey was launched, the pandemic had reached different stages in different countries – and so had the use and deployment of Covid-19 apps. "In China, the widely used WeChat and Alipay apps had already issued health plugins. About 60 per cent of Chinese respondents said they were using them," points out Utz. The situation was different in Germany and the USA at that point, with no apps or only a few apps available on the market. "In the summer of 2020, in the USA, about seven per cent of participants resorted to healthcare apps; in Germany, about four per cent used NINA, the warning app issued by the Federal Office of Civil Protection and Disaster Assistance," says Dürmuth.

This changed over the course of a year, as revealed by follow-up surveys in winter 2020 and spring 2021 conducted with participants from Germany and the USA. In early 2021, 43 per cent of all respondents in Germany were already using an app, most of them the Corona-Warn-App. The numbers also increased in the USA; however, the overall usage rate re-

> "THE POSITIVE ASPECTS AND THE OVERALL BENEFITS OUTWEIGH THE SCEPTICISM."
>
> Christine Utz

Christine Utz and her colleagues have analysed the user acceptance of Covid-19 warning apps.

mained comparatively low over the three survey rounds. “In spring 2021, only eleven per cent of Americans said they used an app. One possible explanation is that there was no unified app solution for all states,” hypothesises Utz.

The researchers attribute the notable increase in app use in Germany primarily to the nationwide availability of the new Covid-19 warning app and its widespread use. As Dürmuth puts it, “People who are familiar with the app are more willing to use it.” Moreover, the survey data shows that despite all initial scepticism, people generally seemed to be willing to use apps to help fight the pandemic. “The positive aspects and the overall benefits outweigh the scepticism,” says Utz. In fact, as evidenced by the survey results in Germany and the US, Covid-19 apps were perceived more and more favourably as time went on. In the third round of the survey in spring 2021, 294 out of 1,000 Germans and 302 out of 1,000 US Americans reported that they did not see any negative aspects about the apps. Utz and Dürmuth also attribute this result to the pandemic situation during the survey periods. “The second survey in particular coincided with a period of high infection rates and lockdowns,” Utz sums up the context.

And yet: regardless of the availability of apps and the pandemic situation, it became apparent over the entire survey period that, on all continents, people’s willingness to use Covid-19 apps depends heavily on how well their private data is protected. “The question of what happens to my private identity-related data affects my willingness to use the app to a large extent,” stresses Dürmuth.

Back in the summer of 2020, 292 out of 1,000 Germans cited concerns about data privacy as the main reason why they did not use Covid-19 apps. In the USA, this applied to 337 of the 1,000 respondents, and in China to 179. These reservations persisted throughout the three rounds of the survey: in the third round, 226 of 1,000 respondents from Germany and 257 of 1,000 respondents from the USA still regarded the apps as invading their privacy, which was one of the main reasons for not using them. Moreover, people feared surveillance by the state – this concern was expressed by 174 participants in Germany and 70 in the USA in the first round of the survey. In all countries, the question which institution receives the data plays a crucial role in people’s decision for or against an app. “Our survey showed that there is a high level of trust in public health institutions – in Germany, for example, this includes the Robert Koch Institute (RKI) and universities. People tend to make their data more readily available to these trusted institutions. But this is fundamentally different if the recipient is a private company, the general public or law enforcement, depending on the country,” says Utz.

In Germany, the prospect of private data being passed on to certain recipients such as the police or private companies reduces people’s willingness to use Covid-19 apps to a considerable degree. In China, people are more willing to share their movement data with the public. People are sceptical only with regard to private companies. “Here, sharing personal data with state institutions is an integral element of everyday life,” says Utz. Overall, the three countries have one thing in common: “People are more willing to use government-issued healthcare apps for less invasive purposes, such as tracking contacts or gathering information, than for invasive purposes, such as monitoring quarantines,” explains Dürmuth.

What does this imply for the development of apps in the future? Utz and Dürmuth appeal to the architects of future state-issued healthcare apps to take users’ privacy concerns seriously. “It’s necessary to explain in great detail how the apps work in practice, and what they can and cannot do. The apps must be transparent about the purposes for which data is collected and stored, who receives it and what societal and especially individual benefits result from continued app use,” the researchers conclude.

text: lb, photos: ms

Start-Up

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 ▸

i **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.

sysm
systems for
tailored GSM solutions
AN to Core Network
Visit us at http://sysmocom.de/
First-hand expertise in protocol R&D from A-bis to SS7/
Support, training and development for Open
Low-cost GSM plus-call platform sysmoBTS
Small, app-style autonomous GSM network
https://osmocom.org/

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.

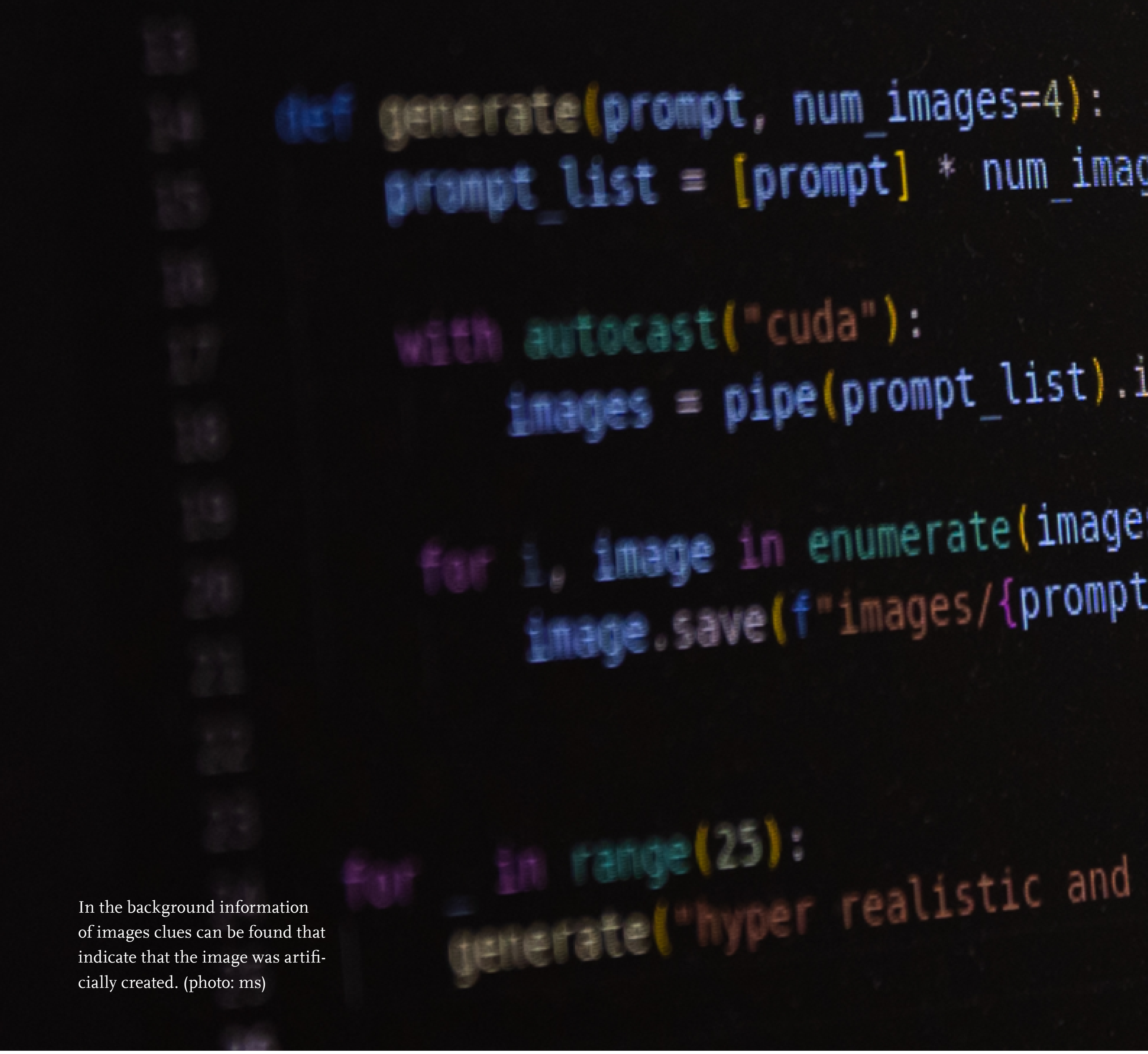
"We have been working on security issues in 4G and 5G networks for years and have a huge head start in terms of know-how," Rupprecht points out. Although the specifications are publicly available, the question remains: who can understand and implement thousands of pages of complex information? Radix 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



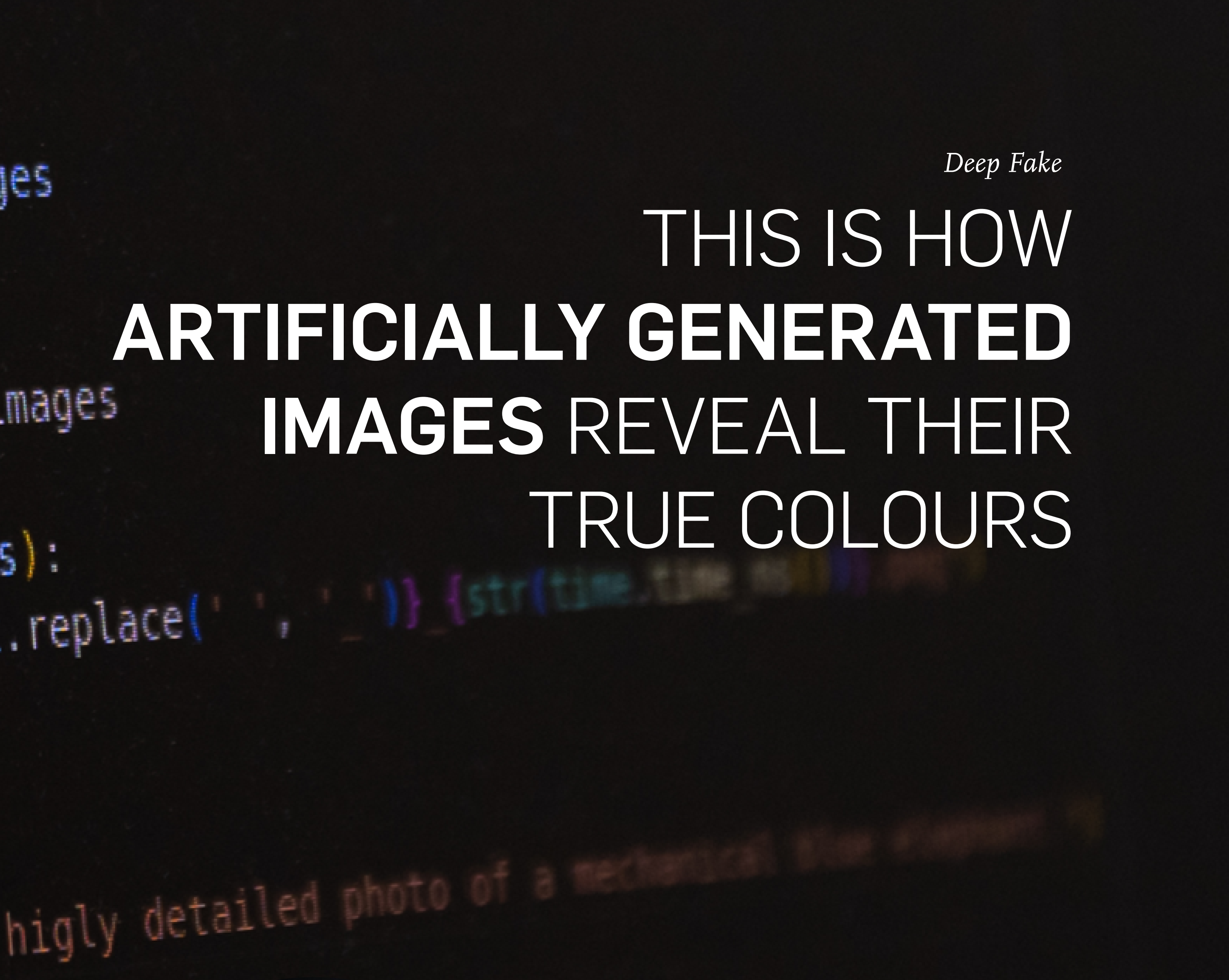
```
def generate(prompt, num_images=4):
    prompt_list = [prompt] * num_imag

    with autocast("cuda"):
        images = pipe(prompt_list).i

    for i, image in enumerate(image
        image.save(f"images/{prompt

for _ in range(25):
    generate("hyper realistic and
```

In the background information of images clues can be found that indicate that the image was artificially created. (photo: ms)

Humans often have no chance whatsoever of distinguishing artificially created images, audio or videos from the real deal. This is why researchers of the Horst Görtz Institute for IT Security are working on automated recognition

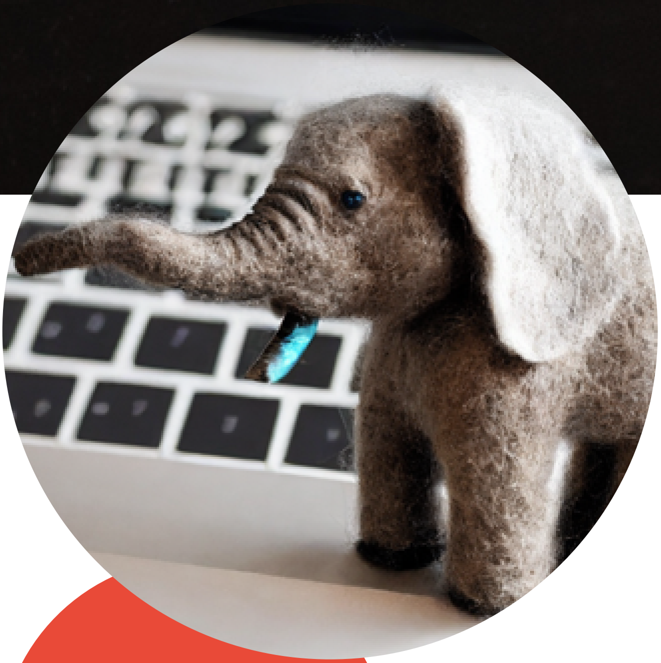
Vladimir Putin stands behind a lectern and addresses the USA: he has very much the means to undermine democracy in the USA – but he claims that he doesn't have to. The US would take care of that themselves. Society is divided already. The video looks real – but it is not. Youtube is flooded with such clips, some of which are quite well done, some of which are not. "It's still a lot of work, but if you want to, you can, for example, superimpose the face of a famous person on the body of another person so skilfully that viewers won't notice it at first glance," says Jonas Ricker.

For his doctoral thesis, which he is writing at the Faculty of Computer Science, he has specialised in fake images. The focus of his work, however, is not videos but photos. He can whip up several links at the drop of a hat that will show you pictures of people who don't exist or where you can try



Deep Fake

THIS IS HOW **ARTIFICIALLY GENERATED IMAGES** REVEAL THEIR TRUE COLOURS



Looks like the real thing: this wool elephant was created by text-to-image generation. (photo: Hugging Face)

to guess whether the picture of the depicted person is real or not. The fake images are generated using deep learning, a machine learning method – hence the name "deep fake". "When older methods are used, you can sometimes spot anomalies in the symmetry," he points out. "For example, different earrings will be a telltale sign, as will asymmetrical glasses. But the methods are getting better and better, and studies have proven that people tend to be rather bad at distinguishing real images from fake ones."

One process for generating such images is called GAN, short for generative adversarial networks. "Basically, such networks are always divided into two parts: one part generates the image, another, the so-called discriminator, decides whether the generated image looks real or not," Jonas Ricker illustrates. "Picture it like this: one part is a counterfeiter, the oth- ▸

er part is the police who have to tell fake banknotes from real ones." The artificial intelligence makes this decision on the basis of many real images that are fed in as a learning dataset. At first, the generator merely generates any random pixels. As it progresses, it learns more and more through feedback from the discriminator. The discriminator also gets better and better at distinguishing the generator's images from real ones. The generator and discriminator train each other, so to speak, which ultimately results in images that look deceptively real.

In an article published in 2020, Jonas Ricker's former colleague Joel Frank describes a way of detecting fake images. The key lies in the so-called frequencies. "It's difficult to explain what frequencies are in images," says the researcher. The best way is to think of frequencies as light-dark differences. Low frequencies are common in people's faces. High frequencies can be found in hair, for example, and they are perceived at a more subconscious level. Consequently, an image in which high frequencies have been altered will look almost exactly the same to us as the original image. However, technology is not so easily fooled: "When it comes to high frequencies, GAN-generated images show characteristic deviations from real photos," explains Jonas Ricker. In artificially generated images, high frequencies occur in excess. This is traceable, and it allows the images to be distinguished from real photos.

Jonas Ricker is currently working on another class of models for image generation, the so-called diffusion models. While GANs were already introduced in 2014, diffusion models have only been researched for roughly three years, with outstanding results. "The basic principle of diffusion models sounds surprising at first," says Ricker: "A real image is destroyed step by step by adding Gaussian noise. After a few hundred steps, no image information is left, the image is completely distorted. The goal of the model is now to reverse this process to reconstruct the original image – which is a difficult problem."

Artificial intelligences are able to create images that humans cannot distinguish from photographs. (photos: ms)

> ”ULTIMATELY, ANY IMAGE MAY BE TREATED WITH SUSPICION AND CAN BE POTENTIALLY DISPUTED, EVEN IMAGES THAT ARE USED AS EVIDENCE IN A COURT OF LAW.“
>
> Jonas Ricker

The key is not to predict the image directly, but to proceed step by step, as with noise. With a sufficiently large amount of training data, the model can learn to make a noisy image a little bit less noisy. By repeating the process again and again, completely new images can then be created from random noise. “One weakness of this method is the long processing time due to the several hundred steps involved,” admits Jonas Ricker. “Still, techniques for optimisation have already been introduced and research is constantly making progress.”

Recently, diffusion models have caused quite a stir with so-called text-to-image generation. This allows images to be generated on the basis of text input – with an astonishing level of detail. These models are trained with the aid of countless image-text pairs sourced from the internet. Both this data collection and the actual training require a lot of computing power and are therefore extremely expensive. Until recently, only large companies like Google (Imagen) and OpenAI (DALL-E 2) were able to train these models in high quality – ▸

and they keep the models largely under wraps. Today, there's also "stable diffusion", a freely accessible model that anyone can use, provided that their computer has enough power. The requirements are moderate, and websites do exist that allow you to create images for your own texts.

The diffusion model is powered by an organisation that has the necessary resources and computing power thanks to a donation. "The model is already very good at generating deceptively real images and will continue to improve in the future," believes Jonas Ricker. This makes it even more difficult to distinguish real images from those generated in this manner. Here, the frequency approach is already less accurate than it is for GAN images. "Another approach is to use the reflections of light in the eyes in order to tell the difference – this, at least, is possible with pictures of humans," says Jonas Ricker. He's currently testing various approaches that make it possible to distinguish images generated by the model from real photos. A universal detector that works for all types of GAN images doesn't actually work that well for this type of image – unless you fine-tune it to make it more accurate. This means that the detector, which is supplied with a lot of real and fake images as learning material along with the relevant information if they are indeed real or fake, is fed additional training data in order to optimise the detection for the new data. This is how it can learn to correctly tell which images have been generated by the diffusion model. How it does this, however, is unclear.

The ability to distinguish between real and fake images is crucial not only in order to expose fake news, including those in video format, but also to detect fake profiles on social media. Such profiles are used on a large scale, for example to influence public opinion in the political arena. "This is exactly what the CASA Cluster of Excellence aims to do: expose large-scale adversaries such as governments or intelligence agencies that have the resources to use deep fakes to spread propaganda," says Jonas Ricker.

The detection of fake photos is also relevant under criminal law, for example when it comes to unintentional pornography in which people's faces are pasted onto the bodies of others. "Generally speaking, the mass of artificially created images leads to a loss of trust, including the trust in reputable media, points out Jonas Ricker. "Ultimately, any image may thus be treated with suspicion and can be potentially disputed, even images that are used as evidence in a court of law."

Even though Ricker aims to ensure that fake pictures can be detected automatically, he reckons that it will ultimately come down to something else entirely: "I think in the end of the day genuine pictures will have to be certified," he speculates. "A feasible approach might be to use cryptographic methods, which would have to be integrated in the photographer's camera, making every genuine image verifiable beyond doubt."

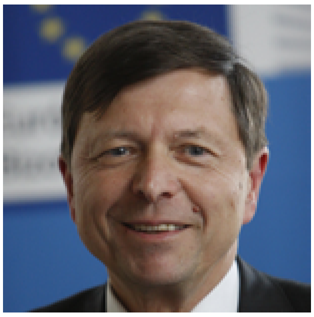
md

> „THE MASS OF ARTIFICIALLY CREATED IMAGES LEADS TO A LOSS OF TRUST, INCLUDING THE TRUST IN REPUTABLE MEDIA."
>
> Jonas Ricker

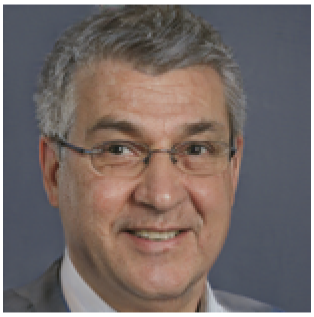
Quiz

WHICH **PERSON IS REAL?**

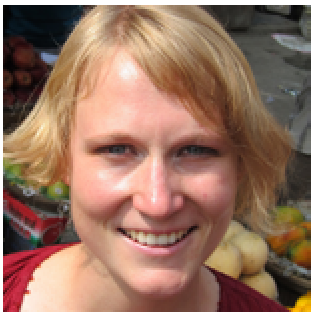
One of each pair of faces is real, the other one is artificially generated. Which faces are real?
The answers can be found on page 62.
All images are taken from the website whichfaceisreal.com.



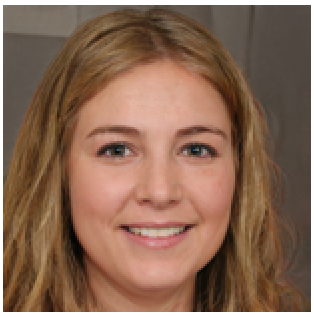
1 a ○



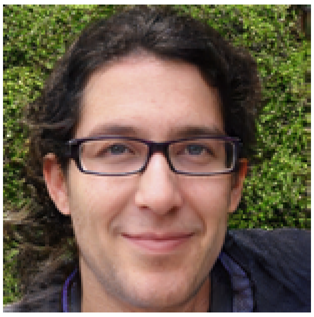
1 b ○



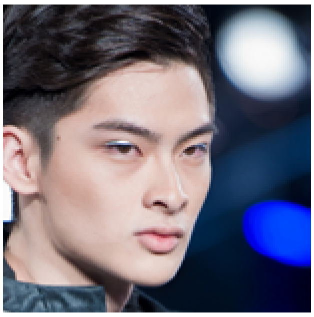
2 a ○



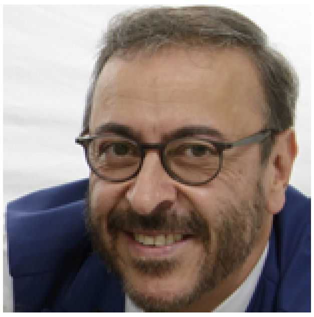
2 b ○



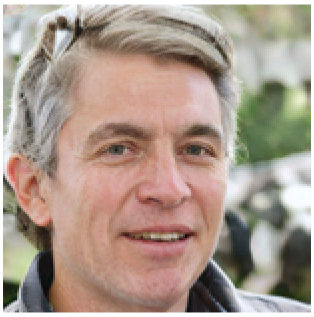
3 a ○



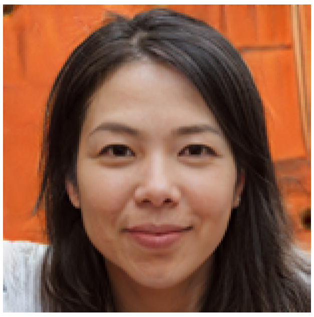
3 b ○



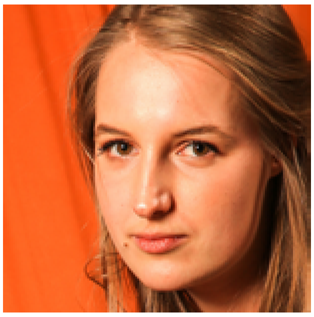
4 a ○



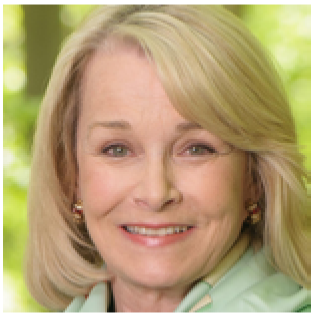
4 b ○



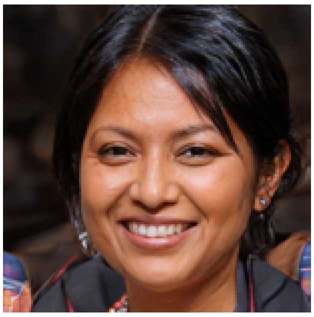
5 a ○



5 b ○



6 a ○



6 b ○

Fuzzing

INTELLIGENT MONKEYS

Researchers from Bochum are particularly quick at finding security vulnerabilities in IT systems. Their trick: they focus on the essentials – and explain it with the theorem of the infinitely typing monkeys.

A program code is a bit like a jungle: complex in structure, difficult to view from the outside, with countless paths that can be taken through it. Finding vulnerabilities in such code is like looking for animals among the trees in the jungle: you know they are there, but you can't see them directly. This is why PhD student Tobias Scharnowski is developing new methods to efficiently detect programming errors in the jungle of ones and zeros. He is conducting research at the Chair of System Security at the Horst Görtz Institute of Ruhr University Bochum, supervised by Professor Thorsten Holz.

The researchers are primarily interested in embedded systems: "We are trying to increase the security of computers that most people don't even know are computers at all," explains Scharnowski. Examples of such embedded systems include smart light bulbs, refrigerators connected to the internet and intelligent thermostats, to name but a few. All these objects contain electronic control technology with many lines of program code in which errors may have crept in. But household appliances are not the only things on the IT experts' agenda. Above all, they are interested in industrial control systems, for example in critical infrastructures such as energy supply. These are areas where security gaps could have dramatic consequences.

Scharnowski and Holz use what is known as fuzzing to detect errors in program code. Fuzzers are algorithms that feed the tested software with random inputs and check whether they can crash the application with them. Such crashes indicate programming errors. The fuzzer keeps varying the input in order to explore as many program components as possible step by step.

Fuzzing is already established for certain areas of application, for example to test operating systems such as Windows or Linux. It has not yet been widely used to test embedded systems, however, because they pose a number of challeng-

i

EMBEDDED SYSTEMS

An embedded system is a combination of hardware and software that serves a specific purpose within a larger system – in a car, for example, this includes electronic controls of the seats. An embedded system is essentially a computer that serves a narrowly defined purpose.

SOFTWARE, HARDWARE, FIRMWARE

Hardware is the term used to describe all devices in the computing sector; unlike software and firmware, it exists in the physical world. Software and firmware, on the other hand, are programs that only exist in the virtual world. Firmware is a specific type of software that is used to control hardware, i.e., it fulfils a precisely defined purpose for a given piece of hardware.

FUZZING

Fuzzing is a method used for identifying vulnerabilities in software. In the process, the software is fed many different inputs and run until an input causes it to crash. A program crash indicates a bug.

The IT specialists search for errors in the programming code of firmware, a specific type of software that is needed for the control of hardware.

es: the software – the so-called firmware – is embedded in a hardware with which it interacts. Researchers usually have little information about the hardware and how it works. "It's like a black box for us," describes Thorsten Holz. In addition, this black box is usually not particularly powerful – often the systems have relatively little memory and slow processors. This is a problem if the researchers want to carry out fuzzing directly on the system. It would take far too long to try out all possible inputs and wait for the system's response. This is why the team doesn't analyse the firmware directly in the industrial control unit or in the light bulb. Instead, they recreate the hardware virtually – this process is called emulation.

The emulator makes the firmware believe that it is inside the real device. For this, it has to interact with the program in exactly the same way as the real hardware would. "This means we have to imitate all the interfaces that exist between hardware and firmware," explains Thorsten Holz. Once this is accomplished, the researchers can test the firmware in a powerful system. Still, it would take a long time if they let their fuzzer try out all theoretically conceivable inputs. That's why the researchers add another step to the fuzzing process by narrowing down the possible inputs.

First, they model the framework in which the inputs must be located in order to be logical for the firmware. For example: let's assume that the hardware is a refrigerator with a temperature sensor. The refrigerator hardware can report the measured temperatures to the refrigerator's software, i.e., its firmware. Realistically, it's not possible for just any given temperature to occur, it has to fall within a certain range. Therefore, the firmware is only programmed for a certain temperature range. It could not process other values at all, so there is no need to fuzz them.

"We only use the inputs in the fuzzing process that the firmware expects and can handle," points out Thorsten Holz and compares the process to the Infinite Monkey Theorem: "This theorem states that, if you let monkeys type on a key- ►

> »IF A SYSTEM HAS NEVER BEEN TESTED WITH FUZZING, IT WILL HAVE UNDISCOVERED VULNERABILITIES.«
>
> Thorsten Holz

board for long enough, they would eventually come up with the works of Shakespeare." The same applies to the fuzzer: if you let it try again and again, it would, by chance, eventually use meaningful inputs. But it would take a long time. "We want to make our monkeys a bit more intelligent, though," says Tobias Scharnowski. "We take away all the keys they don't need and try to get them to press only useful keys. With the inputs that are left, we can still test the code all the way down." This makes fuzzing with the Bochum system – known as Fuzzware – particularly efficient.

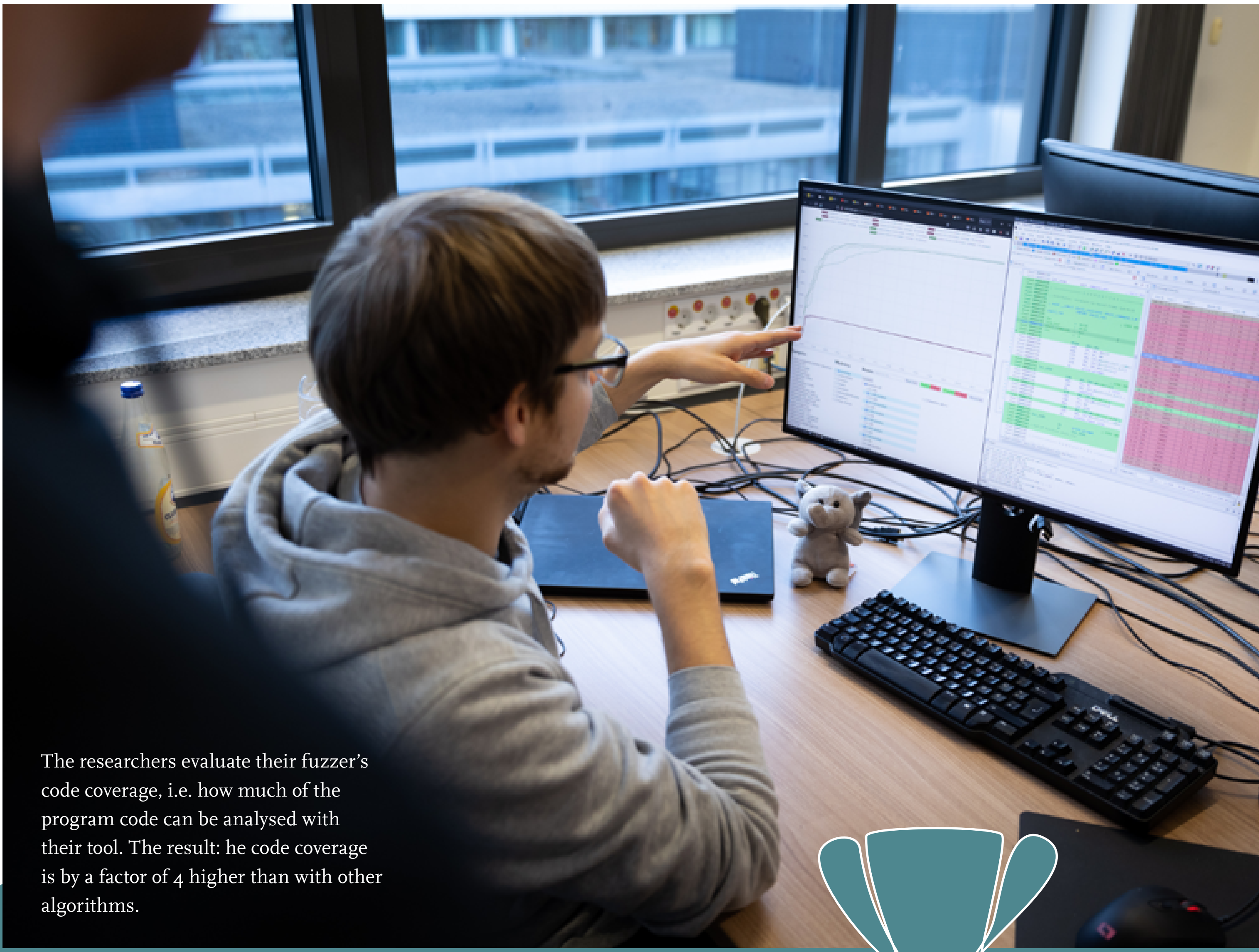
Together with colleagues from Santa Barbara and Amsterdam, the Bochum team tested 77 firmwares using Fuzzware. Compared to conventional fuzzing methods, they sorted out up to 95.5 per cent of all possible inputs. This enables Fuzzware to check up to three times more of the program code than conventional methods in the same amount of time. In the process, the group also identified additional vulnerabilities that had remained undetected with other fuzzing methods. "You can always find something," says Thorsten Holz. "If a system has never been tested with fuzzing, it will have undiscovered vulnerabilities."

In the case of embedded systems in particular, it is almost impossible for programmers to create the perfect code. "In order to talk to the hardware of embedded systems, you have to use a low-level programming language," explains Tobias Scharnowski. For many applications, programmers can't simply fall back on code snippets that have been developed for other applications. They have to build their code from scratch. Edge cases – namely states that the system rarely encounters – may then not be taken into account. "For our fuzzers, however, these states are easy to analyse," says Scharnowski. "They can therefore help make the systems more robust." By reporting any vulnerability they identify to the manufacturers, the researchers contribute to greater security in industry, light bulbs and refrigerators, to name but a few.

text: jwe, photos: ms

Tobias Scharnowski is PhD student at the Horst Görtz Institute for IT Security.

For many years, Thorsten Holz was one of the Principal Investigators of the Cluster of Excellence CASA.



The researchers evaluate their fuzzer's code coverage, i.e. how much of the program code can be analysed with their tool. The result: he code coverage is by a factor of 4 higher than with other algorithms.

Interview

"A RIPPLE WENT THROUGH THE CROWD"

Software companies are delighted when researchers find bugs in their code before attackers do. They even organise bug-finding competitions. The Bochum team has already won plenty of prizes.

Mr. Scharnowski, people in your field often talk of bug bounties. What do you mean by that?
It's a kind of bonus programme offered by software companies for detecting vulnerabilities. The more serious the vulnerability you discover, the higher the prize. Some manufacturers even run competitions.

Have you ever taken part in one?
In 2020, I entered the Pwn2Own competition in Miami together with some colleagues. It was organised by various manufacturers from the industrial security sector and was about devices that control industrial plants. One of the elements we attacked was the so-called DNP3 protocol, which is used for communication between control systems, for example in the critical energy sector. We were the only ones who managed to reach the highest category for this task and gained complete control over the program.

That sounds like a remarkable success.
Yes, that was quite an exceptional experience. The competition had different targets, and it started with an announcement of which team would tackle which target. When our idea was presented, a ripple went through the crowd.

And what did you win?
Between the three of us, we received 87,500 US dollars in prize money. It gives us the freedom to buy software and equipment for our next adventures of this kind.

jwe

Interview

SHIELDED DATA PROCESSING IN THE CLOUD

Using cloud services without running into trouble with the General Data Protection Regulation – the company Edgeless Systems makes it possible. Founder Dr. Felix Schuster reflects on the somewhat difficult entry into a new market.

It was just the two of them on a park bench – this is how Felix Schuster and Thomas Tendyck celebrated the launch of their company Edgeless Systems in the spring of 2020 during the coronavirus lockdown. A good two years later, they have a team of 15, high-profile customers and a prestigious company headquarters in Bochum. Still, the start was not always easy, as Felix Schuster recounts in an interview.

Mr. Schuster, you understand how to use cloud applications, for example in the USA, without coming into conflict with the General Data Protection Regulation (GDPR). What exactly do you offer your customers?

We programme software for secure cloud computing – the marketing term is confidential computing. The fundamental problem with cloud computing is that data is usually processed in plain text. This means that employees of cloud providers or authorities may be able to access it. As a result, companies from the EU can't use these cloud services, which are mostly based in the USA.

We make sure that you can use the cloud like your own computer. The reason why this is possible is that, for almost ten years now, processor manufacturers have been building functions into the hardware that allow data to be processed in encrypted form. Prior to that, data could be encrypted during transport and on the hard disk, but had to be decrypted

for processing. With our software, we ensure that the data remains encrypted at all times, and that this fact can be verified. The processor issues a certificate confirming what has been done with the data and that it hasn't been decrypted at any time.

For which type of applications is this significant?
A typical scenario is that a company has an application running locally, but wants to move it to the cloud in order to save resources. An example of this would be personnel management software. This involves personal data that requires high levels of protection. Or an example from our practice: our partner Bosch collects data from smart cars. Here, we are talking about intellectual property, and pictures of passers-by can also be involved. The cloud hardware facilitates the shielding and encrypted processing of this data, so to speak. But since that doesn't work on its own, it needs software like ours.

Can every customer then use these functions quite easily or do you need to bring in people with IT expertise?
Our programme is based on Kubernetes, a very common application in clouds, which is usually already in use at the customer's organisation. The basic features are therefore often known to the users. But there has to be someone on site who knows the ropes.

You started out by offering your software free of charge and as an open source. How can you finance yourself on that basis?
Currently, it's pretty much common practice to offer a kind of extended free trial version to begin with. Obviously, you run the risk that users will be satisfied with it and stick with it, or that the competition will copy the programme. But the advantage is that you have a very low-threshold offer for potential

▸

i EDGELESS SYSTEMS

The two founders of Edgeless Systems met while studying at Ruhr University Bochum. They laid the groundwork for their start-up with the support of the start-up incubator Cube 5. Cube 5 is based at the Horst Görtz Institute for IT Security and the Faculty of Computer Science at Ruhr University and is part of the Worldfactory Start-up Centre. The company currently has 15 employees, ten of them full-time. The founders are looking to recruit new staff, preferably from Ruhr University, where most of the current members of staff had studied.

The company programs software for secure cloud computing.

customers. The first step has already been taken, and maybe the customer will come back to us to purchase an enterprise version.

In a market as new as ours, this is a good way to see where customers stand. It also helps to identify and acquire new clients. A year after the first free offer, we received many attractive requests. Unlike in the US, however, this business model is rather uncommon here, and you're met with incomprehension. But we've been much better received by investors.

Seeing that the market is still so young, is there any competition to speak of?
Yes, there's a lot of competition actually, especially in the USA. But our product is the most mature. The market just has to figure that out. Currently, very few customers know what secure cloud computing is – they may be aware of their problem, but they don't know the solution. There's still a lot of explaining to do.

Doesn't the GDPR play into your hands?
It can definitely be a driving factor. With this in mind, we would also like to cooperate more with European cloud providers. We would then be able to develop a service on the provider's side, and the customers wouldn't have to do anything themselves, but could simply be sure that their data is protected.

> ”CURRENTLY, VERY FEW CUSTOMERS KNOW WHAT SECURE CLOUD COMPUTING IS.“
>
> Felix Schuster

The team currently consists of 15 employees and is supposed to grow in the future.

Let's go back to the beginnings of Edgeless Systems: was it always your wish to start your own business?
I already wanted to start a software company when I was still at school. During my studies, I worked in a small company, and that's when the wish solidified. One of my main reasons to pursue a PhD was to search for exciting technologies as a basis for starting up a company.

What does your typical workday look like today?
Well, I'm no longer involved in the technical side of things. They are the domain of my co-founder Thomas Tendyck. I still take care of the product vision and parts of the architecture. Other core tasks include public relations, customer acquisition, staff recruitment and the acquisition of investor funds. In addition, there are many other minor tasks relating to human resources, operations and finances.

Have you ever regretted the start-up?
I have at times – there are always ups and downs. But in general it was a good decision. It's a lot of fun, though very stressful. I have learned to handle it.

If you could look into the crystal ball and get a glimpse of the next five years, what would you like to see?
As an enterprise, we're still in the phase of optimising the product market fit – which is perfect if, for example, you can offer a vaccine during a pandemic, so you have exactly the product that the market is demanding at the moment. We're currently trying to achieve this fit. We're learning a lot. We want to become the platform for highly secure cloud computing.

In five years, we should have scaled our business model and have over 100 employees. Looking still further into the future, we should be ready for an IPO or a sale of the company. These are the two goals for venture-backed companies like us.

Which advice would you give yourself if you could go back two years?
We started out with a fairly engineering mindset and got bogged down in some areas in order to minimise the risk. Looking back, I'd say we should have taken more risks at an earlier stage and accepted the possibility of failure. And: this is an exciting but also a difficult market. Next time, I'd choose a market that is already somewhat more developed.

That sounds like you'd consider another start-up after a possible sale of your company?
Definitely. But maybe after taking some time off first.

text: md, photos: ms

Secret services want to know as much as possible. For example, they try to circumvent data encryption. This can cause collateral damage, warn Bochum researchers.

Intentional vulnerabilities in encryption algorithms seem tempting to secret services and law enforcement agencies alike – after all, they allow supposedly secure information to be read. Professor Gregor Leander and Dr. Christof Beierle from the Chair of Symmetric Cryptography and Dr. David Rupprecht from the Chair of System Security discuss the sense and nonsense of such backdoors and describe a very long-lasting example of such a gap. Together with international colleagues, they showed that current smartphones still have the insecure mobile phone encryption GEA-1 installed. It has been around since the 1990s, and according to mobile phone standards, it should have disappeared in 2013.

Professor Leander, Dr. Rupprecht, Dr. Beierle, you are looking for secret backdoors. What exactly is that?

David Rupprecht: A backdoor is a kind of in-built weak link in the encryption process. You can think of it like a master key that shouldn't exist in the first place. In the case we are investigating, it is physically located in a chipset installed in mobile phones, i.e. on the hardware.

Gregor Leander: In our case, it's symmetric cryptography. This means that all those legitimately involved in the communication – in this case mobile phones and cell towers – have the same key. The underlying algorithm is, so to speak, the recipe for producing these keys.

Rupprecht: In order to generate the key, which, by the way, is regenerated with every new contact between the mobile phone and the mast, an additional secret code stored on the SIM card of the mobile phone is needed. Based on this, the GEA key is calculated by an algorithm, both from the mobile phone and the mobile mast. The result means for both of them: we are friends, we can communicate.

Which data is affected by the security vulnerability in GEA-1?

Leander: Basically, all of them. But this is not relevant for all data. Because when I use online banking, for example, the data is additionally encrypted by the bank, end-to-end, so it is not decrypted at all in between.

Christof Beierle: In the 1990s, when GEA encryption was first introduced, this was not yet the case.

Leander: However, such backdoors are less about the actual contents of the information that is sent back and forth, but rather about metadata, which is often underestimated. It's about the information: who communicates with whom and when? This metadata is of tremendous value. This is evident from the fact that Meta Platforms introduced end-to-end encryption for WhatsApp without much pressure from users. This seems like a contradiction, because Facebook lives off data. The reason is simple: Facebook still sees the metadata. And this is enough.

Who instigates the installation of backdoors in the systems?

Leander: Such backdoors are of course in the interest of the secret services and law enforcement agencies. Invariably, backdoors for these purposes are always being discussed, even if they don't make much sense. In the case of GEA-1, you have to remember that it was developed in the 1990s. At that time, cryptography was considered a weapon. Powerful cryptography was not allowed to be exported abroad, there were strict export restrictions. But of course people wanted to sell mobile phones to other countries, too. So they had to get around these export restrictions.

Beierle: We have a document from 1998 on the requirements for the cipher. One of them was: the encryption had to be exportable according to certain restrictions. That means: it had to be just weak enough to get through, but not too weak either.

Who sets such standards as those governing encryption?

Rupprecht: In the case of GEA, it was the European Standard Organisation ETSI, a kind of DIN institute at European level. The organisation includes, for example, large manufacturers, companies such as Deutsche Telekom, as well as governmental organisations.

Leander: We can't rule out the possibility that members of the secret services were also employed there at the time. ▶

Interview

SECURITY WITH AN **IN-BUILT VULNERABILITY**

Gregor Leander, David Rupprecht and Christof Beierle (from left) deal with backdoors in computer systems.

The former weaknesses of cryptography are now known, and the procedures have become more public.

Has the backdoor in GEA-1 been exploited?

Leander: As far as GEA is concerned, we don't know whether it was used or not. But in other cases, it has been proven that backdoors were exploited.

Rupprecht: The revelations published by Edward Snowden, for example, brought to light that Angela Merkel's mobile phone was bugged. If you wonder how that could have been accomplished, you quickly come up with encryption methods that work not unlike GEA and are used for voice telephony. Here, too, a relatively weak algorithm was integrated.

Dr. Leander, you've just indicated that you don't consider deliberately built-in backdoors to be useful as far as the authorities are concerned.

Leander: There are 1,000 legitimate reasons for law enforcement and intelligence agencies to want such backdoors to exist. But they are the wrong way to go. A master key like that can also be found by someone who may have criminal intentions. And once the loophole is there, it is always there – after all, we can see that it hasn't been possible to eliminate GEA-1 to this day, even though it should have been done years ago.

Rupprecht: There is another aspect: if everyone knows that only weak algorithms are allowed, criminals will hide from the authorities by using secure encryption. Criminals don't care that cryptography is forbidden. They simply switch to their own system. In addition, of course, there are fundamental principles of democracy such as the protection of privacy. Mass surveillance is not compatible with democratic values.

How come GEA is still integrated in the latest devices, even though we know that the encryption has a backdoor?

Rupprecht: Well, the manufacturing industry is huge, so maybe it just slips under the radar because it's not a priority at the moment.

Should we assume that encryption algorithms with backdoors are active in all our devices?

Leander: No. We are now keeping a close eye on things.

Rupprecht: Not in end devices. This is currently an issue in the network products, for example routers, on which the internet is based. There are examples of more recent encryptions with backdoors. A recent case is the manipulation of random number generators by the US secret service NSA. Randomness is often necessary in encryption algorithms, and if you ensure that zeros instead of ones are generated super randomly, you can simplify the encryption keys. In the case of NSA, the manipulated algorithm was so slow that no one wanted it, so companies were paid to put it in.

Leander: On the other hand, cryptographic algorithms without a backdoor do exist.

Rupprecht: There's been a shift since the 1990s: the weaknesses of cryptography at that time are now known, and the algorithms have become more public.

Beierle: It's always suspicious when algorithms are not public. The GEA1 standard, for example, was secret.

Leander: Today, the selection of encryption methods is pub-

The problem of backdoors remains abstract for many. However, the industry community really wants to do something.

> „CRIMINALS DON'T CARE THAT CRYPTOGRAPHY IS FORBIDDEN."
>
> David Rupprecht

lic and transparent. Researchers submit proposals, which are evaluated in a multi-stage process. If there's even a hint of ambiguity, the proposal is immediately rejected. So there are no more deliberate weaknesses in public encryption protocols. This is also one of the reasons why we at the Cluster of Excellence CASA believe that protection against secret services like the NSA is possible: mathematical algorithms do exist that no-one in the world can break. Therefore, we can be hopeful.

What are your plans for your future activities?

Leander: We will continue to look for backdoors. There are indications that they exist, the only problem is finding them. We are looking for them in a structured way. We look at large programmes, sift out the cryptography and analyse them – especially the ones that are new to us. Some of them are secret. In the case of GEA-1, a whistleblower tipped us off, and the same applies to another case we are currently investigating.

How come there is no public outcry when such discoveries come to light?

Leander: There's no outcry from users, but there is a great echo in the press. The interest is there.

Beierle: Maybe there wasn't such a big outcry at GEA, because the method is so old and no longer poses a danger.

Rupprecht: We have to make end users understand what is at stake. But the problem remains very abstract for many. The situation is different in the industry. Manufacturers are really willing to do something about it.

Leander: You really have to distinguish between users and decision-makers. End users don't care about their data. Quite the contrary, considering how they use social media. The same applies to using amazing services on the internet for free – how does that work? Simply by having your data harvested. But people don't care about that. The decision-makers have to care. It's like driving a car: if seat belts weren't compulsory, no-one would wear them.

text: md, photos: ms

Cryptocurrencies

SHARED IRRESPONSIBILITY

Cryptocurrencies are not subject to centralised governance. The community holds the power – but fails to do all that needs to be done. As a result, the collateral of the currency might be at risk.

Bitcoin, Litecoin, Dogecoin, Digibyte – the list of all currently existing cryptocurrencies is very long. So long, in fact, that it would be hard to decipher their names if they were all squeezed onto one A4 page. Thousands of virtual currencies are out there, and they have long ceased to be a niche product. Millions of people use them. When using cryptocurrencies, IT security is of paramount importance. After all, money is nothing more than data, which, like all data, is potentially vulnerable to cyberattacks.

Professor Ghassan Karame addresses the question of how watertight various cryptocurrencies really are. He heads the Chair for Information Security at the Horst Görtz Institute for IT Security at Ruhr University Bochum and is an advocate for decentralised platforms, like the ones on which cryptocurrencies are based. The idea behind it is simple: power is not bundled in one central entity, for example in a bank. Rather, decisions are always made by some majority of users. “In such systems, it should be very hard for a central body

Bitcoin is one of the best-known cryptocurrencies. The source code is freely available on the internet – and has been extensively copied. This is how so many new virtual currencies have been created.

to impose censorship, and they are robust against faults and misbehaviour because a large community of developers monitors the technology," as Karame outlines two advantages of decentralised platforms. "The idea is brilliant, and more likely than not, it is the future," he adds. Just like any other IT technology, however, cryptocurrencies are also vulnerable to security breaches. As early as 2012, Karame and his collaborators detected a critical issue in the usage of the Bitcoin system that allowed people to spend the same Bitcoins multiple times to pay for different transactions. "It was as though you could buy a burger with a five-euro note and then use the same note again to pay for an ice cream," explains the researcher.

In 2015, Karame and his collaborators documented another critical vulnerability that emerged after Bitcoin adapted its system to a larger number of users. "We showed that if we had control over as few as tens of laptops in the system, we could stop information flow in the entire Bitcoin system," as Ghassan Karame describes the severity of the vulnerability. Bitcoin

▸

i CRYPTOCURRENCIES

When it comes to virtual currencies, the money is not issued resp. controlled by a central bank. Rather, it's the users who take care of all that. Sums of money are allocated to individuals who can store them in a digital wallet. Probably the best-known cryptocurrency is Bitcoin.

In Germany, people own cryptocurrency mainly for the sake of experimentation, speculation or as an asset in their financial investments. Whereas in countries under autocratic leadership, virtual money is often considered an attractive option, because crypto-financial transactions aren't regulated by the state. In countries with extreme inflation, they can also offer financial stability: if the currency of a country collapses, cryptocurrency won't be affected by the crash.

has long since addressed both security gaps. But Bitcoin is not the only currency out there, there are plenty of copies floating around. The source code for Bitcoin is freely available on the internet. Anyone can copy it and launch their own cryptocurrency. This is how Dogecoin was created, for example, which has become the No. 1 cryptocurrency in the gaming industry. "There are so many cryptocurrencies that we don't even know all of them, and we certainly don't know who is running them," points out Ghassan Karame; he is one of the Hub Leaders in the Cluster of Excellence CASA. That's the trouble with decentralised systems. Since decision-making power is shared, it is complicated for researchers to report security vulnerabilities.

IT security is governed by the ethical imperative of "responsible disclosure". If a security vulnerability is detected and confirmed, the researchers must always notify the operator of the compromised product first and allow them sufficient time to fix the bug before it is publicly disclosed. This is to ensure that the exposures are patched before attackers can exploit them. But to whom are you supposed to report errors in a decentralised system, when it sometimes isn't even clear who is running the system? Or if you don't even know how many and which systems are affected? Who decides in such a structure whether the software has to be updated to close security gaps? And how can you control whether a vulnerability has been patched? There are no answers to these questions yet.

Regarding the security vulnerabilities described above, Karame and his collaborators were in discussion with the various Bitcoin developers. "There, the staff responded diligently and swiftly," he recalls. But no advance warning ever came for the numerous copies of Bitcoin. Ghassan Karame intends to find out what the real-world impact of these unclear structures really is. He and his team examined various virtual currencies that are slightly modified copies of Bitcoin. They are widely known under the umbrella term "altcoins". The researchers checked how long it took until security vulnerabilities in various altcoin source codes were closed after they had transpired – including the serious security vulnerability detected by Karame's team and disclosed in 2015, for example.

"In a nutshell: the results were a shock," as Ghassan Karame puts it. While Bitcoin fixed the vulnerability in just seven days, it took, for example, Litecoin 114 days, Dogecoin 185 days and Digibyte almost three years. "Three years in which you could have crashed the entire cryptocurrency system with tens of laptops," Ghassan Karame points out and illustrates the scale of the problem: "Imagine if it took Visa three years to fix a security flaw in credit card payments."

The result of the analysis made in Bochum sounds simple, but the path to the numbers was lengthy. Bitcoin's full source code as well as each modification of the code are freely available on a platform called "GitHub". This offers multiple opportunities for cloning and importing patches from this public project. For example, anyone who wants to create a Bitcoin

Ghassan Karame heads the Chair for Information Security at Ruhr University Bochum.

The source code for many applications, also for the crypto currency Bitcoin, is freely available on the internet – you can easily copy it and launch your own cryptocurrency.

copy, i.e. an altcoin, can copy the source code in GitHub into their own project using a simple command.
If a security update for Bitcoin is available and an altcoin developer decides to install it, they typically use the "rebase" command. This means they don't have to laboriously rewrite their own code, but can transfer the necessary information directly from the Bitcoin code to the own. The researchers identified the problem as follows: while GitHub typically tracks the timestamp of each code modification, the use of the rebase command can result in the loss of this metadata. As a result, it's no longer straightforward to tell from the source code when a security update was implemented.

Therefore, the team had first of all to develop a tool with which they could approximate the time of a security update for forked source code. The tool is based on an existing archive service that keeps track of all events on public repositories of GitHub, such as modifying the code or perform a rebase operation. This allowed the researchers to match updates in the code with the respective events in the archive, in order to estimate the timestamp of the security patch.

This is how the researchers analysed 44 of the most serious security vulnerabilities documented for Bitcoin and altcoins. Invariably, the same pattern emerged over and over again: for many altcoins, the number of days it took to fix the flaws was in the three-digit or even four-digit range. "We believe that some cryptocurrencies haven't managed to patch some of the vulnerabilities to this day," says Karame. He's certain that the problem is actually much more serious than his initial analysis showed. "I'm almost afraid to dig down any deeper," he continues. "We've seen only the tip of the iceberg so far, I'm sure." Therefore, the researcher urges caution: "Users need to be more careful when picking a cryptocurrency. They shouldn't base their decision solely on the prospects of profit. It's no use at all to make a bunch of money if it can disappear in a puff of smoke the next day due to a security breach." In theory, people should only trade cryptocurrencies whose operators have a policy of security updates. Currently, however, users have little chance of finding out whether this is the case. It remains to be seen whether this gap will be closed when decentralised platforms become even more popular.

text: jwe, photos: ms

> "THE RESULTS WERE A SHOCK."
>
> Ghassan Karame

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.

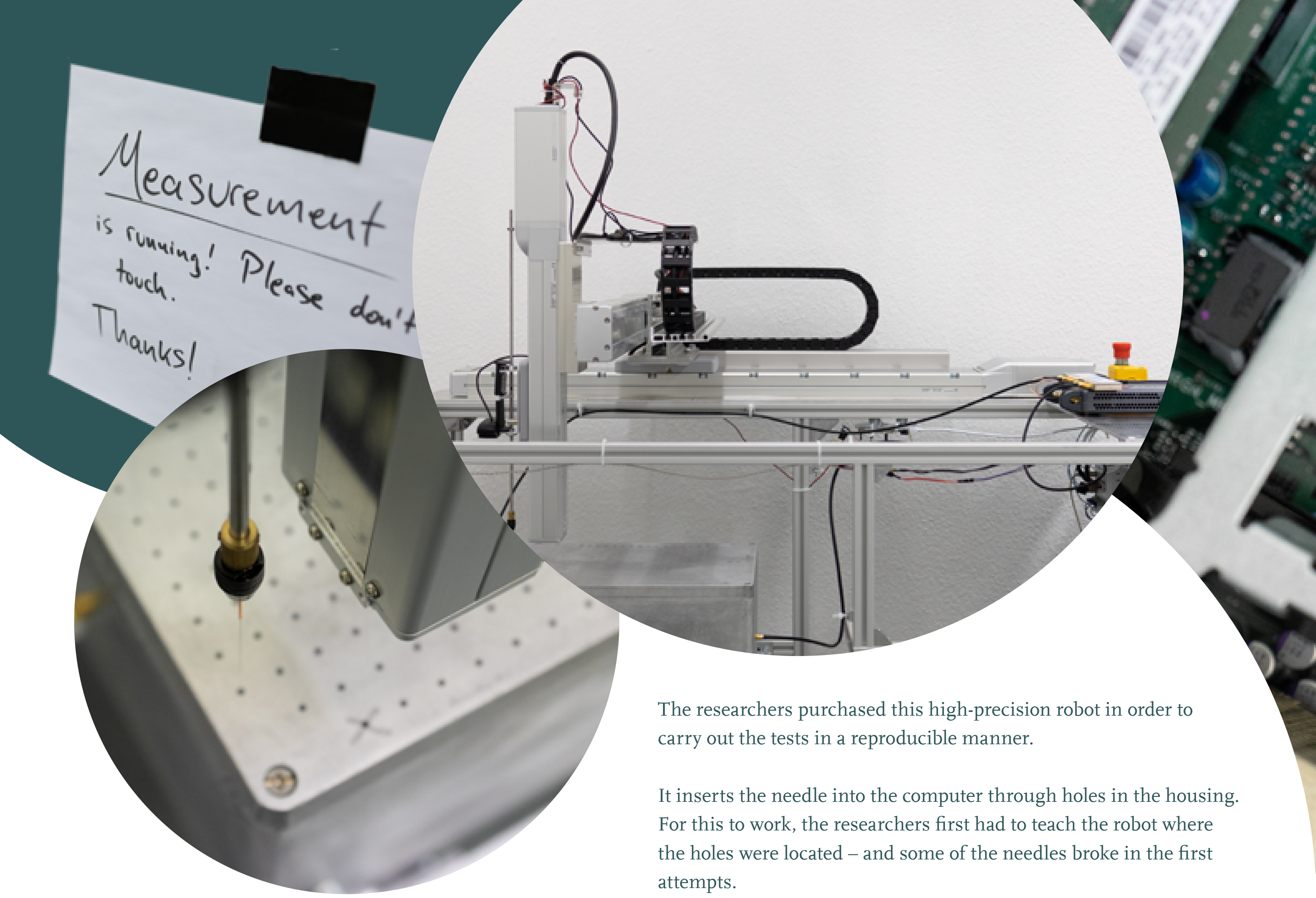
For this purpose, the researchers employ radio waves. They install two antennas in the system that they want to monitor: a transmitter and a receiver. The transmitter sends out a special radio signal that spreads everywhere in the system and is reflected by the walls and computer components. All these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



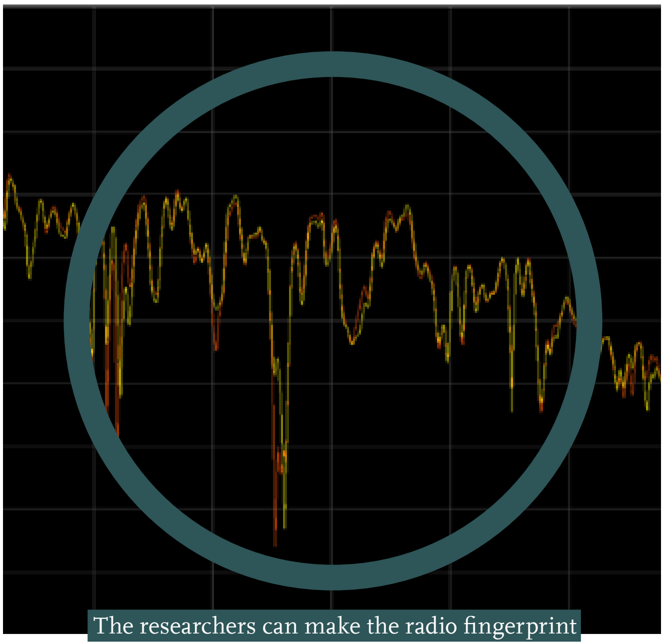
The researchers purchased this high-precision robot in order to carry out the tests in a reproducible manner.

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.

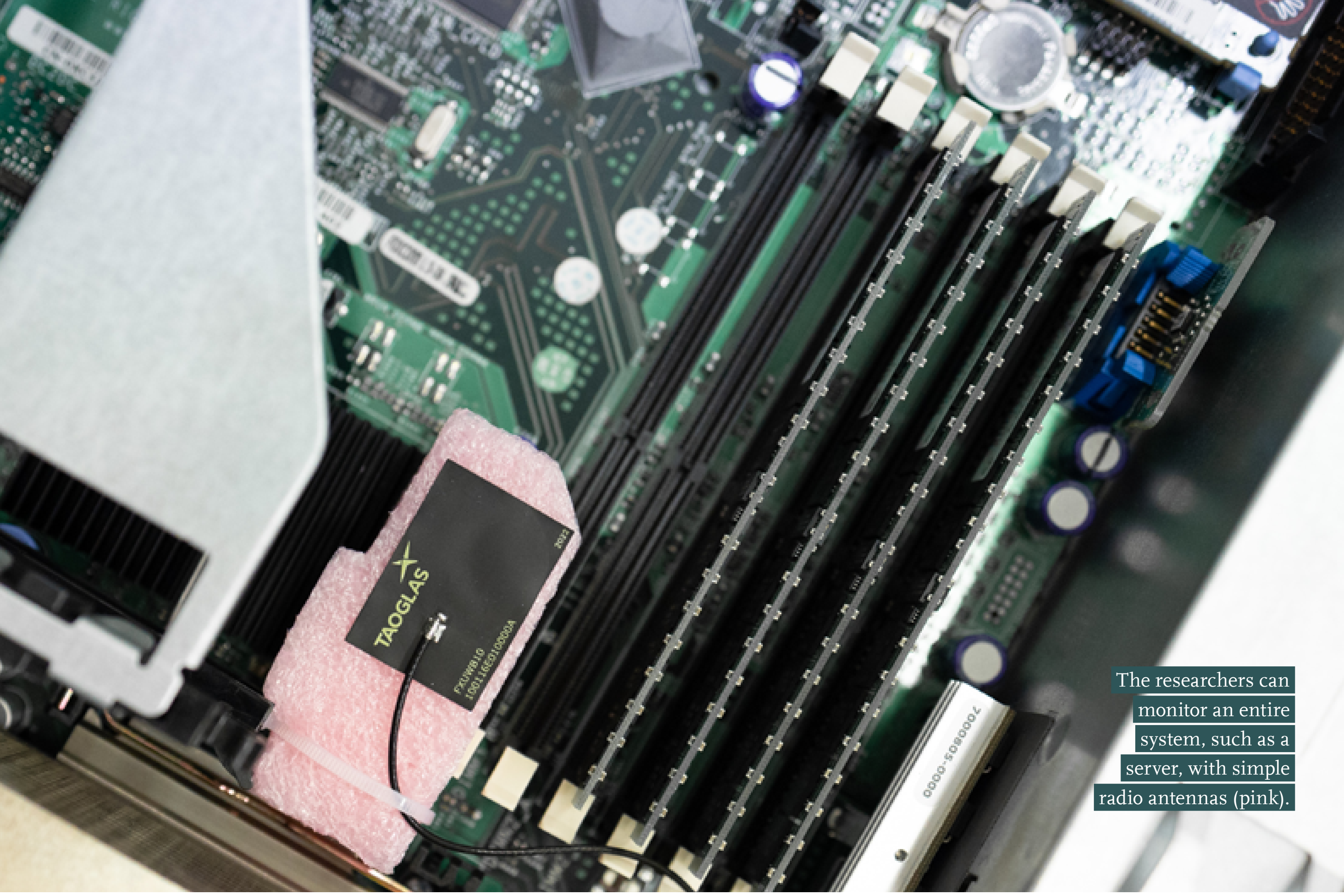
as characteristic of the system as a fingerprint. Tiny changes to the system are enough to have a noticeable effect on the fingerprint, as a demonstration by the two researchers shows: they have built their radio technology into an old computer housing. The measured radio signal is rendered visible on 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

The Human Factor

HOW SAFE DO **PEOPLE AROUND THE WORLD** FEEL ON THE INTERNET?

Who has ever been hit by cybercrime? How do people protect themselves from it? A survey reveals similarities and differences between different groups around the world.

When it comes to the internet, "evil is everywhere under the sun", as the popular quote goes. By adopting safe practices, however, we can make it more difficult for cybercriminals to steal our data or cause damage in other ways. But what constitutes safe practices? What do you have to do to protect yourself from data theft and similar crimes? "There's a lot of confusion about this, among people from all over the world," is what Franziska Herbert has learned. The psychology graduate is currently completing her dissertation in the CASA Cluster of Excellence at the Horst Görtz Institute for IT Security. In collaboration with Professor Markus Dürmuth, Professor Angela Sasse and other researchers, she has conducted a comprehensive survey that assesses the human factor in IT security.

More than 12,000 individuals in twelve countries took part in the online survey, which focused on what people understand safe behaviour in cyberspace to be, how they approach it and what misconceptions they may have. Participants came from China, Germany, the UK, India, Israel, Italy, Mexico, Poland, Saudi Arabia, Sweden, the USA and South Africa. They represent 42 per cent of the world's population. The questions revolved, for example, around end-to-end encryption, WiFi surfing, the https standard, virtual private networks (VPN), and passwords. "It emerged that some risks are equally well understood by all participants around the world," points out Franziska Herbert, who designed the survey together with the team. One of these is the phenomenon of shoulder surfing, where unauthorised persons obtain personal data simply by looking over a user's shoulder.

Certain misconceptions, however, are apparently also widespread around the world. "For example, in all the countries we covered in the survey, 80 per cent of the participants believe that it is necessary to change passwords periodically to keep them secure," says Franziska Herbert. IT security experts actually used to recommend this for a long time, until it turned out that this practice actually doesn't do any good at all. "All that happens is that passwords become more and more insecure as a result, because otherwise users won't be able to remember them. It's much better to choose really strong passwords that are not easy to crack – a password manager is very helpful for this purpose," explains Franziska Herbert. "Once you have a secure password, you can stick to it, as long as it doesn't fall into the wrong hands."

Participants in all countries also agreed with the statement that their computers could be infected by malware when they click on a link. "This only happens in a few exceptional cases," say the researchers. "Most of the time, further actions are needed, such as entering data on the website accessed via the link."

The researchers also found that uncertainty about IT security issues prevailed across the board among participants worldwide. "This is reflected in the fact that our survey participants chose exactly the middle on a scale ranging from 'completely agree' to 'completely disagree' on many questions," says the researcher.

In addition to all the similarities, the researchers also identified differences between participants from different countries, especially with regard to the scale of the assessments. "We found the biggest differences to exist between Western and non-Western countries," says Herbert. The researchers include China, India, Mexico, Saudi Arabia and South Africa among the latter. "Compared to participants from Germany, participants in all other countries were more likely to have misconceptions about malware, device security and passwords," outlines Franziska Herbert. German participants were the least likely to agree with misconceptions – even though they still fell in the middle of the scale between 'completely agree' and 'completely disagree'. The highest level of agreement with misleading statements came from participants from China and India.

In public, a glance over the shoulder is enough to spy out passwords, for example.

80 %

OF THE PARTICIPANTS BELIEVE THAT IT IS NECESSARY TO CHANGE PASSWORDS PERIODICALLY TO KEEP THEM SECURE.

Two examples from the survey:

“I am more likely to catch malware when I visit a porn site than when I visit a sports site.” Approximately 49 per cent of respondents in Germany agreed with this misconception, while 75 per cent from Saudi Arabia and 86 per cent from China agreed with it.

The correct statement “Links in emails can lead me to fake websites in order to intercept my login data” was agreed to by 87 per cent of German participants and 78 per cent of Chinese participants.

All groups participating in the survey had in common that they tended not to consider family and friends an IT security risk. “That’s not how we see it,” says Markus Dürmuth. There are risks, especially when people share a computer or passwords. When it comes to domestic violence or stalking, it’s often people in a user’s closest circle who pose a threat. “And there’s another thing: among friends, pranks may be played that are not at all funny for the victim,” concludes the researcher.

text: md, photos: ms

Franziska Herbert wants to know how safe people feel on the internet and what experiences they have had.

The calculations for the RACCOON attack were run on the Chair's own cloud.

Data Security

THE TELLTALE ZERO

Attacks on the TLS protocol are both rare and highly complex. And yet, the encryption experts at Ruhr University Bochum are constantly tracking down new ones.

The thick volume that contains all technical details on the TLS encryption protocol has roughly a thousand pages. This means that the TLS standard is as thick as three Harry Potter novels. “It takes a lot of time and crypto know-how to understand and keep track of all of its features,” says Dr. Robert Merget from the Chair for Network and Data Security at the Horst Görtz Institute for IT Security at Ruhr University Bochum, which has been specialising in Transport Layer Security (TLS) for years. This cryptographic encryption protocol ensures that, for example, connections between internet browsers and servers or between different email servers are secure. Merget and his colleagues know the standard pretty much by heart and have consequently mastered every trick and every TLS encryption spell.

They have been developing a TLS analysis tool since 2015. It enables companies to implement TLS with as few errors as possible to ensure that there are no security gaps left for attackers to exploit. Almost every day, the researchers come across vulnerabilities that occur during implementation, so-called bugs. “By contrast, systematic attacks on the TLS standard have become rather rare,” points out Merget. But they do still happen. In 2020, the encryption expert discovered a highly specialised attack on a specific TLS algorithm, and alerted the crypto community to the threat of a malicious RACCOON attack.

“We use easy-to-remember names for vulnerabilities that are otherwise quite technical. This makes it easier for us to talk about them in the community,” explains Merget. While research institutes are part of the community, it is primarily IT companies such as Google, Microsoft and Cloudflare who have a vested interest in ensuring that TLS is as secure as possible and who are constantly trying to improve it.

The TLS encryption protocol is public and can be viewed by all. “The algorithms are public, but the keys that are used are secret,” outlines Merget. “Think of it like a secret ▸

language.” When using a secret language in the past, it was often done by swapping letters. People who knew the exact code – that is, who knew which letter had to be substituted for another letter – were able to decode the message. However, keeping the method a secret turned out to be quite difficult and insecure. This is why today’s encryption experts choose a different approach. “Modern algorithms are public, but the keys for the algorithms are secret. It’s the same with TLS. The attacker has access to the encryption principle, but the keys are kept secret,” explains Merget. The main purpose of TLS cryptography is to prevent third parties from intercepting communications. Moreover, the protocol has two additional properties: firstly, TLS is used for authentication, and secondly for data integrity.

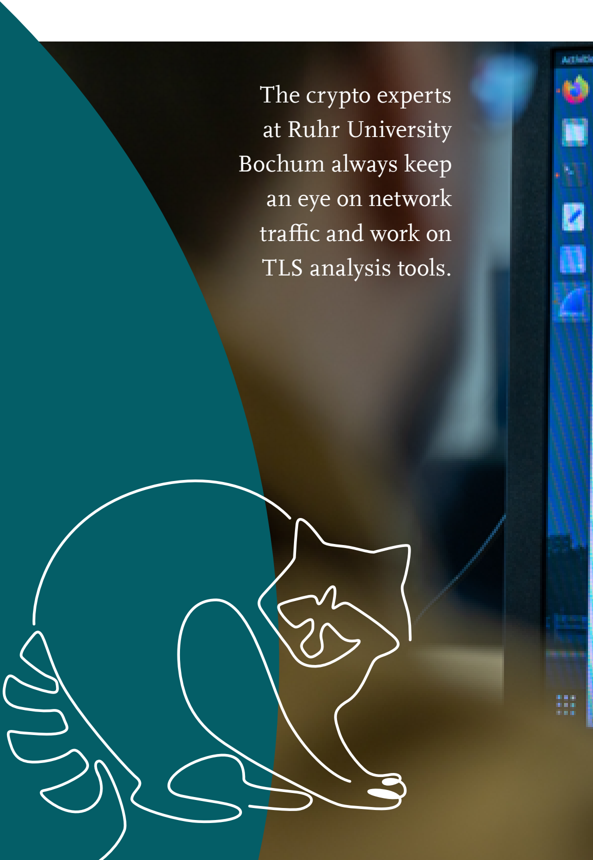
About four billion users worldwide use TLS today. And each of them has different preferences and requirements for the encryption protocol. This explains why so many developers have been refining and tweaking the TLS standard for years – and also why the protocol is today considered secure. This was, after all, not always the case. “Since 1994, since TLS has been created, the protocol has been the target of numerous attacks. Most notably, there were many attacks between 2011 and 2016,” says Merget. But as he points out: “As a rule, this is not an attack that can be carried out by your local neighbourhood hacker. These are difficult high-tech attacks, such as might be executed by secret services. Usually, ordinary users have nothing to fear from them.” Since 2018, since the introduction of the modernised TLS 1.3 standard, the number of attacks has decreased significantly. And yet: attacks on the TLS versions introduced between 1996 and 2018 do still take place. In 2020, Robert Merget discovered the vulnerability in question, which he dubbed RACCOON.

The RACCOON attack targets the so-called Diffie-Hellman key exchange protocol, i.e. a very specific algorithm that can be used in TLS to ensure that, for example, a bank and its client can exchange a shared secret, a shared key. In very concrete terms, the attacker exploits a timing vulnerability in the key derivation when the Diffie-Hellman algorithm is used:

THE INVENTION OF TLS

The encryption protocol TLS was developed in 1994 by the company Netscape (today: Firefox) and was initially called SSL (the acronym stands for: Secure Sockets Layer). In 1999, the Internet Engineering Task Force renamed SSL in TLS, because they believed that the protocol for data security on the internet shouldn’t be in the hands of one corporation.

The focus of Robert Merget’s research is on the TLS encryption protocol



The crypto experts at Ruhr University Bochum always keep an eye on network traffic and work on TLS analysis tools.

> ”SINCE 1994, SINCE TLS HAS BEEN CREATED, THE PROTOCOL HAS BEEN THE TARGET OF NUMEROUS ATTACKS.“
>
> Robert Merget

the duration of the key derivation and with it the cryptographic processing of the secret gives the attacker the information he needs to decrypt the data and, as a result, to break the confidentiality of the protocol.

“Timing is a so-called side channel, one of many, that allows us to infer the secret key of an algorithm and possibly even to crack it,” elaborates Merget. “Let’s say I encrypt the word dog or the word mouse. It takes longer for me to encrypt the word mouse because it has more letters. An attacker can measure the time it takes me to encrypt communication, and then use the measured time to deduce what was encrypted.” In addition to time, factors such as rising temperatures or the power consumption of devices likewise provide information about the computing operations of an algorithm – these, too, are side channels that may enable attackers to obtain keys.

The concept behind the RACCOON attack is easy to understand. “Broadly speaking, the Diffie-Hellman key is always based on calculations with a remainder,” says Merget. In the mathematical derivations of the Diffie-Hellman key exchange, calculations are continued with the remainder without the leading zeros.

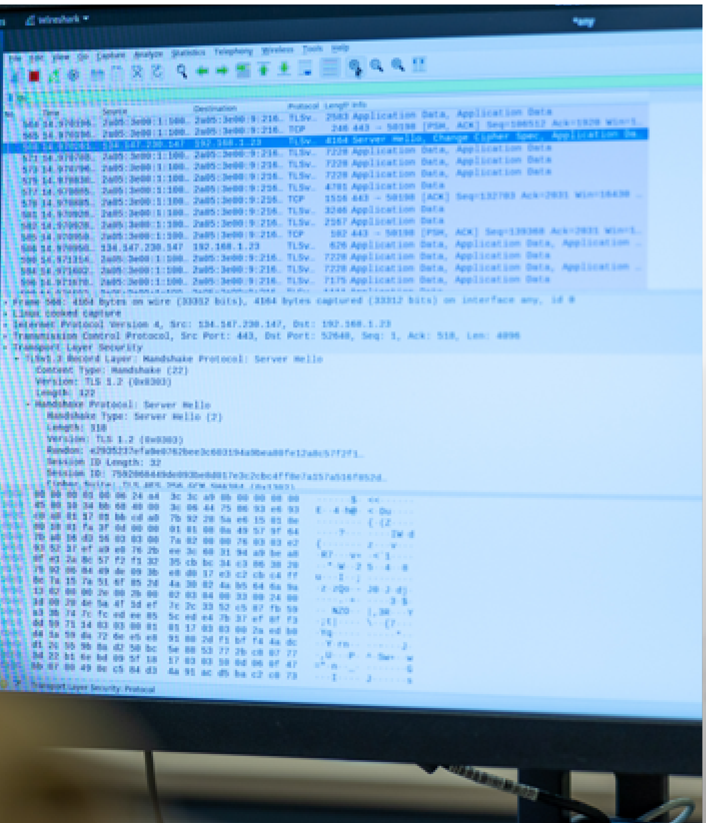
“Processing smaller numbers can be done more rapidly because of the smaller data volume. This gives the attacker an advantage: he observes how fast an operation was executed and then concludes whether or not there was a leading zero,” explains Merget. This is the vulnerability that the attacker exploits. He can then reconstruct the secret key from the information he has gathered. “However, to do this, he needs complicated mathematical procedures used in linear algebra,” adds Merget.

To find out just how widespread the vulnerability is, Merget sent data packets via a dedicated internet line to approximately 100,000 servers that use TLS. “Three per cent of the world’s internet responded and was affected by this vulnerable TLS configuration,” points out Merget.

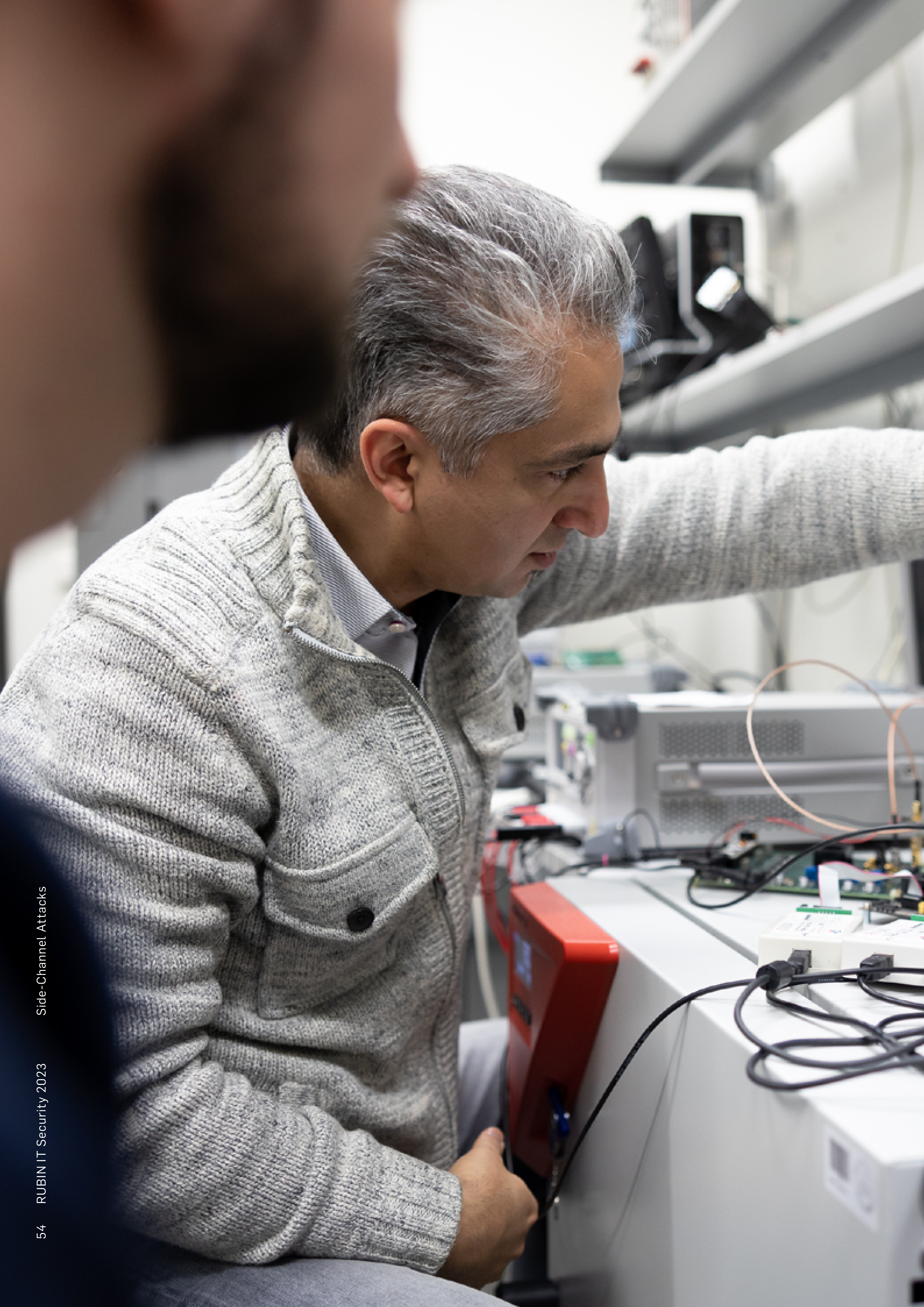
“In the first step, we contacted all developers of major TLS implementations and warned them. We then reported the case to the Federal Office for Information Security and asked them to support us in the so-called responsible disclosure process,” says Merget. The purpose of this process for the disclosure of security vulnerabilities, which is well-established in IT security, is to notify manufacturers promptly about vulnerabilities and to provide updates and patches before the public becomes aware of them.

But how can the vulnerability be fixed? “The best course of action is to use the latest and most secure version of TLS, TLS 1.3,” recommends Merget. Overall, however, the researcher is convinced that the TLS protocol is very secure: “It is extremely difficult to still detect vulnerabilities.”

text: lb, photos: ms



Tricky calculations: mathematical methods from linear algebra are used for decoding.

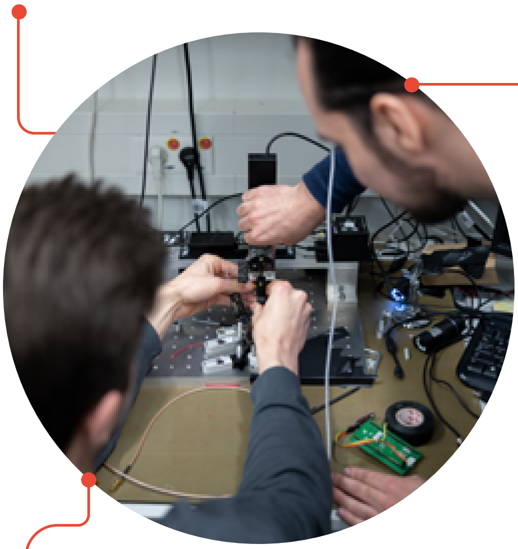


Side-Channel Attacks

WHEN THE **CHIP** NEEDS A COOLING BREAK

Many encryption algorithms are mathematically proven to be one hundred per cent secure. Nevertheless, they sometimes fail to protect confidential data. This is because encryption doesn't happen merely in theory.

An electronic chip is a bit like a person who has to solve a complicated problem under extreme time pressure. Many people know what it feels like when the brain is working at full throttle and the head starts to overheat. You may also get a craving for sweets, because you feel you need more energy. Deep in thought, you might even start muttering under your breath. An electronic chip that is tasked with encrypting data works in a similar way. While it's doing its job, it may get warm, its power consumption may increase, and it may emit acoustic signals. And all this can pose a security risk. Namely, if the changes to the physical parameters reveal something about the data that the chip is in the process of encrypting.



Nicolai Müller (on the left), David Knichel (on the right) and their colleagues develop tools that help manufacturers make electronic circuits more secure.

It has repeatedly been shown that this can happen. In such cases, researchers use the term side-channel attacks, because it is not the encryption algorithm itself that is cracked, but additional information is used to read out confidential data. ▸

The research team: Nicolai Müller, Pascal Sasdrich, David Knichel and Amir Moradi (from left)

The time alone that it takes to encrypt certain data can tell us something about the content of the data itself. "Such attacks don't require a lot of effort at all," says Dr. Pascal Sasdrich from the Horst Görtz Institute for IT Security at Ruhr University Bochum. "It's not something that can only be done by organisations like the NSA. Theoretically, anyone can carry out side-channel attacks from their garage. The necessary equipment only costs around 200 euros." Targets may include transponder keys, card readers and smart home technologies, to name but a few.

Pascal Sasdrich is conducting research at the Faculty of Computer Science in the Emmy Noether Junior Research Group "Computer-Aided Verification of Physical Security Properties" (CAVE). Together with colleagues from Professor Amir Moradi's Implementation Security group, he is focusing on how to find out whether an electronic component is protected against side-channel attacks – and how to build a secure electronic circuit. "When implementing cryptographic processes, manufacturers often want chips to be as small as possible, as efficient as possible or as fast as possible," lists Pascal Sasdrich. Security is usually not their top priority. In addition, a single careless mistake in the implementation of the encryption technology is enough to open a gateway to attackers. The Bochum-based team is therefore developing tools to help manufacturers implement encryption technology.

To this end, it must first be possible to determine whether an existing electronic circuit is secure or not. The group has developed the so-called SILVER method for this purpose. The acronym stands for Statistical Independence and Leakage Verification. This name already reveals what the key to success is: statistical independence. SILVER checks whether the observable physical parameters such as power consumption and temperature during encryption are statistically independent of the data that is being encrypted. In case of statistical independence, no inferences can be drawn from the physical parameters as to the content of the data.

"Traditionally, other criteria used to be applied for the verification of secure circuits, rather than statistical independence," says Pascal Sasdrich. "The methods were based on hypotheses or estimates and sometimes produced false negative results." In other words, methods were classified as insecure, even though they were in fact not insecure at all. Such errors don't occur with the SILVER method.

"SILVER is one hundred per cent secure, because it is based on a highly comprehensive analysis," stresses Amir Moradi, adding, however, that "it doesn't yet work for larger circuits, because the workload would skyrocket." For large circuits, the Bochum-based researchers are currently using simulation-based methods, which prove to be efficient even for complex systems. "However, they aren't one hundred per cent secure," admits Moradi. His team is now looking for feasible options to verify the security of larger circuits with a high degree of reliability.

Couldn't we simply break down these more complex systems into several components and check them one by one? "You can look at individual parts and prove that they are secure. But if you then put them together, that doesn't mean that the entire circuit is secure, too," explains Pascal Sasdrich. This is because the interfaces between the components can constitute a gateway for attackers.

David Knichel and Nicolai Müller, likewise members of the Implementation Security research group in Bochum, are working on solutions to this problem. The IT experts are developing modules for electronic circuits that can be securely combined with each other in such a way that the assembled circuit, too, is guaranteed to be resistant to side-channel attacks. These individual modules are referred to as gadgets. "You don't need many different gadgets to build a circuit," explains David Knichel.

The gadgets map, for example, certain logical operations, such as the multiplication of two bits – a frequently needed

i BITS

A bit is the smallest unit of information used by conventional computers. It has the values "0" and "1". Complex information is made up of a large number of bits, which are linked together by logical operations during computing processes.

The researchers develop tools that support manufacturers to improve the security of electronic cirtuits.

operation. However, if a separate gadget were used for every logical operation that has to run in the circuit, the whole structure would take up an extremely large amount of space. The reason is that many bits have to be multiplied together in the encryption process. David Knichel and his colleagues are therefore working on expanding the range of functions of individual gadgets, for example so that one gadget can multiply several bits simultaneously. This would make the circuit faster and smaller.

The gadgets developed by the Bochum-based team aren't components that physically exist, however, but are available as code instead. "We use a common hardware description language," says Knichel. This means that he and his colleagues provide a construction manual for manufacturers, so to speak.

Still, protecting electronic circuits from side-channel attacks manually is a tedious task. "We have therefore developed a tool called AGEMA, which can convert an unprotected circuit into a verifiably secure one at the push of a button," points out Nicolai Müller. AGEMA stands for Automated Generation of Masked Hardware. The tool checks which logical operations exist in a circuit and replaces insecure components with the secure gadgets. "We can also take specific preferences into account, i.e. optimise the circuit for speed and size, for example," adds Müller.

The tools developed so far represent the first steps in basic research, rather than solutions that can be used on an industrial scale. After all, a lot of research is still being invested in the automated protection of electronic circuits against side-channel attacks. The IT experts in Bochum will also dedicate much of their efforts to developing optimised solutions – only taking an occasional cooling break.

text: jwe, photos: ms

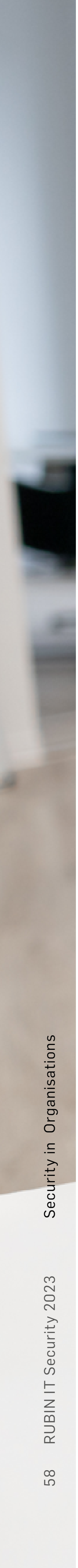
> ”
> THEORETICALLY, ANYONE CAN CARRY OUT SIDE-CHANNEL ATTACKS FROM THEIR GARAGE.
> “
>
> Pascal Sasdrich

The gadgets developed by the team from Bochum are based on a modular design and provide a basis for secure electronic circuits.

Organisations

HOW TO RECONCILE IT **SECURITY AND PRODUCTIVITY**

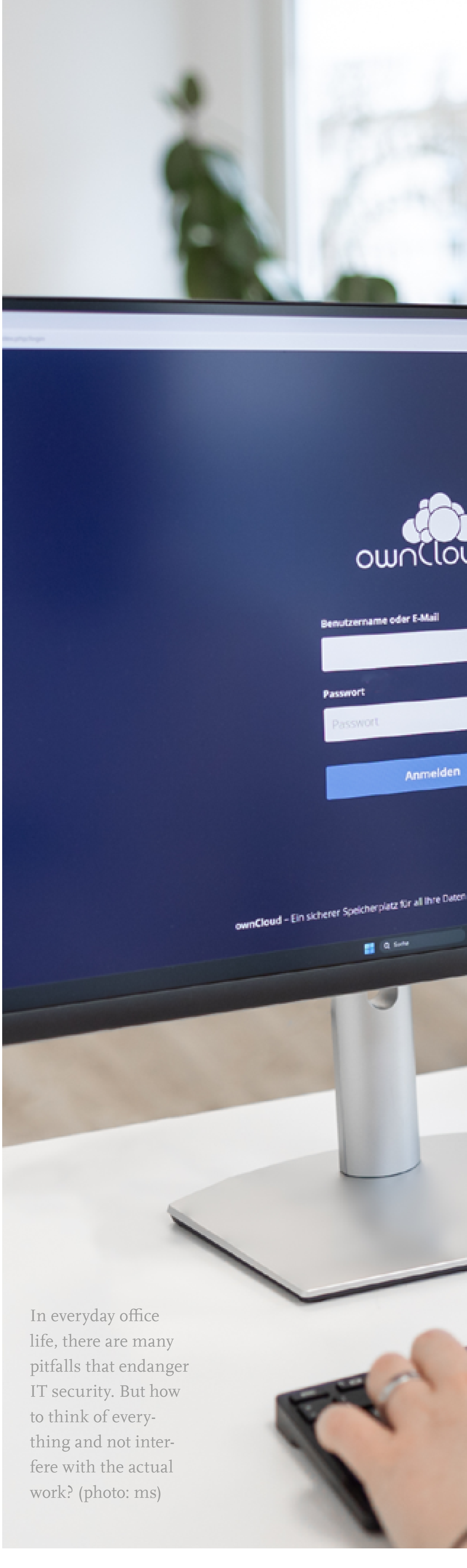
Uta Menges and Jonas Hielscher want to lift the label of being a nuisance from IT security measures and incorporate them more effectively into everyday life.



IT security – many people roll their eyes at the mere sound of the word. Everybody realises, of course, that it is a matter of great importance. The spectacular attacks on IT systems of organisations in recent years are frightening; entire universities and city administrations were sometimes offline for weeks. And the successful attacks are only the tip of the iceberg, because attempted attacks are a daily occurrence. But what are companies and organisations doing to ensure that their IT is secure? Ultimately, each and every individual has to contribute to this security. Why doesn't it actually work all that well and how could it be made to work?

This is the question explored by Uta Menges and Jonas Hielscher. The two form a tandem in the Graduate School SecHuman – Security for People in Cyberspace. Even though they're working together on their PhD thesis, their professional backgrounds couldn't be more different. While Jonas Hielscher studied computer science in Magdeburg, Uta Menges studied business psychology. She completed her Master's degree in the field of marriage, family and life coaching and has also worked in this area. How do they all go together?

"They go surprisingly well together," she says. "I can transfer what I've learned to the field of IT security." This is because the focus in both fields is on humans. "No matter how good the technological measures for the security of an IT system are, they won't work without the cooperation of the users," adds Jonas Hielscher. But research results have been ▸



In everyday office life, there are many pitfalls that endanger IT security. But how to think of everything and not interfere with the actual work? (photo: ms)

SECHUMAN GRADUATE SCHOOL

Since 2016, PhD students at Ruhr University Bochum have been researching security in cyberspace at the “SecHuman” Graduate School, which is funded by the NRW Ministry of Culture and Science. At the school, PhD students work not only with researchers from other disciplines, but also with actors from the industry. The SecHuman Graduate School, short for “Brave New World: Security for People in Cyberspace”, is located at the Horst Görtz Institute for IT Security in Bochum and is also integrated into the Cluster of Excellence CASA – Cybersecurity in the Age of Large-Scale Adversaries.

Jonas Hielscher (left) and Uta Menges want to know how IT security can be integrated into everyday working life so that it is not a hindrance. (photo: CASA, Caroline Schreer)

> „NO ONE CAN DO THAT ON A NORMAL WORKING DAY"
>
> Uta Menges

scarce on how to get organisations to support their employees in the transition to secure behaviour and not simply dump the burden on the end users. And Menges and Hielscher are not very happy with the way it's handled in practice either.

"Many companies commission providers, for example, to send fake phishing emails to their employees in order to sensitise the team to potential attacks," elaborates Jonas Hielscher. "But such one-off and one-dimensional measures don't effect much." In case of doubt, someone who has fallen for it has the feeling of being in the hot seat. That doesn't help anyone.

The two researchers ask completely different questions: How feasible is IT security for employees? Do employees know exactly what they have to do? Can measures really be implemented or is there no time for it in the daily work routine? Do the IT security measures compete with other tasks that need to be done? "For example: read every email very carefully and check it for indications of a phishing attack," illustrates Uta Menges. "No one can do that in a normal working day."

In addition to such questions, which are grouped under the umbrella term "productive security", the two PhD researchers also focus on communication about IT security. How do people talk about it? The implementers are often engineers. They talk about technology without taking their colleagues who are not technologically savvy on board. This communicative hurdle leads to misunderstandings and doesn't do anything to foster a cooperation based on mutual trust. But this is precisely what the researchers consider indispensable. "If someone has opened a phishing email and fallen into the trap, they mustn't be afraid to report the incident," says Uta Menges. "And it must be clear to whom." She calls for a healthy error culture: no one should be pilloried because they've made a mistake. Clear instructions are essential. All too often, however, employees are left alone with vague rules. Communication also includes the response of the help desk. If it's impersonal, IT security remains abstract.

Both researchers have also identified communication barriers between IT security professionals and the managers of institutions. "Professionals want to talk about products. Management is much more interested in the risk that needs to be contained. But there's no measure of how secure or insecure the behaviour of employees is," Jonas Hielscher explains. He and Uta Menges are venturing into largely unexplored territory. "You'd have to interview people, observe their behaviour, get their feedback, evaluate incidents. But none of that has been done yet, partly because it's so complicated," he says.

Based on her expertise as a psychologist, Uta Menges points out: if IT security is to succeed in organisations, self-efficacy is the most important aspect. In other words: IT security must be manageable. And it must be effective. "This may sound self-evident, but the decades-old narrative that everything's getting worse and nothing can be done anyway is stuck in many people's heads," says Uta Menges. "Those who have internalised it have a hard time taking action because they don't believe in it."

Uta Menges and Jonas Hielscher are tackling the issue with a number of partners from the industry. Together with a large enterprise in North Rhine-Westphalia, they are coaching more than a dozen trainees to become ambassadors for IT security. They've met the Chief Information Security Officer and got his mobile phone number. The goal is to create a network across the company's many subsidiaries with over 20,000 employees. This is how IT security is to be given a face. Since November 2021, the two researchers have been communicating with a group of 28 Swiss Chief Information Officers from various companies. Among other things, they help design workshops and stay up to date on everyday problems in the companies.

"This PhD thesis is only just evolving as we work on it," says Jonas Hielscher. Still, both are fascinated by their field of research. "It's pioneering work and can't be planned – after all, it's humans who are the focus," says Uta Menges. Plenty of research questions are still open. The research field of human-centred security is still young, the concept only emerged around 2000. "But there's an ever increasing number of professorships, it's a growing field," as Jonas Hielscher is pleased to say. "And our results will certainly not fall on deaf ears."

md

i DAMAGE CAUSED BY IT ATTACKS

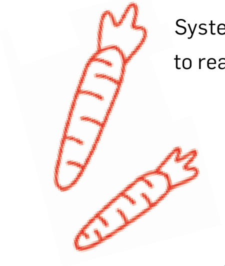
No one can put an exact figure on how much economic damage is caused by IT attacks, as there is no obligation to report such incidents in Germany. The figure published by the industry association Bitcom, which amounts to around six per cent of the gross domestic product, is therefore only an estimate, and Jonas Hielscher believes it is too high.

Ransomware attacks, in which IT systems are encrypted by external parties in order to extort a ransom, frequently hit medium-sized companies, whose protection is often inadequate.

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*



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

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

CASA IN THE PODCAST „EXZELLENT ERKLÄRT“

„Our data is encrypted when we surf the web or send a message on Messenger. Until now, many of these methods have been quite secure – but when the quantum computer is released, this security will be over.

That is why the Cluster of Excellence CASA has developed encryption methods that can even withstand quantum computers. We are also investigating how to make IT security more user-friendly. Prof. Eike Kiltz and Prof. M. Angela Sasse chat with podcaster Larissa Vassilian about their research.

The Podcast

57 clusters of excellence, 1 podcast. „Exzellent Erklärt“ regularly features one of the Clusters of Excellence funded within the Excellence Strategy of the Federal and State Government.

It takes us right across Germany, and the topics are as varied as the locations: From African studies to the future of medicine. Join us for the next episode and immerse yourself in the exciting world of cutting-edge research!

Listen here:

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Gefördert durch
DFG Deutsche
Forschungsgemeinschaft

RUHR
UNIVERSITÄT
BOCHUM
RUB

Do you know our HGI newsletter?

Do you know our HGI Newsletter? Keep up to date with the latest IT security research, events and projects.

Click here to subscribe:

RUHR
UNIVERSITÄT
BOCHUM
RUB

HORST
GÖRTZ
INSTITUTE