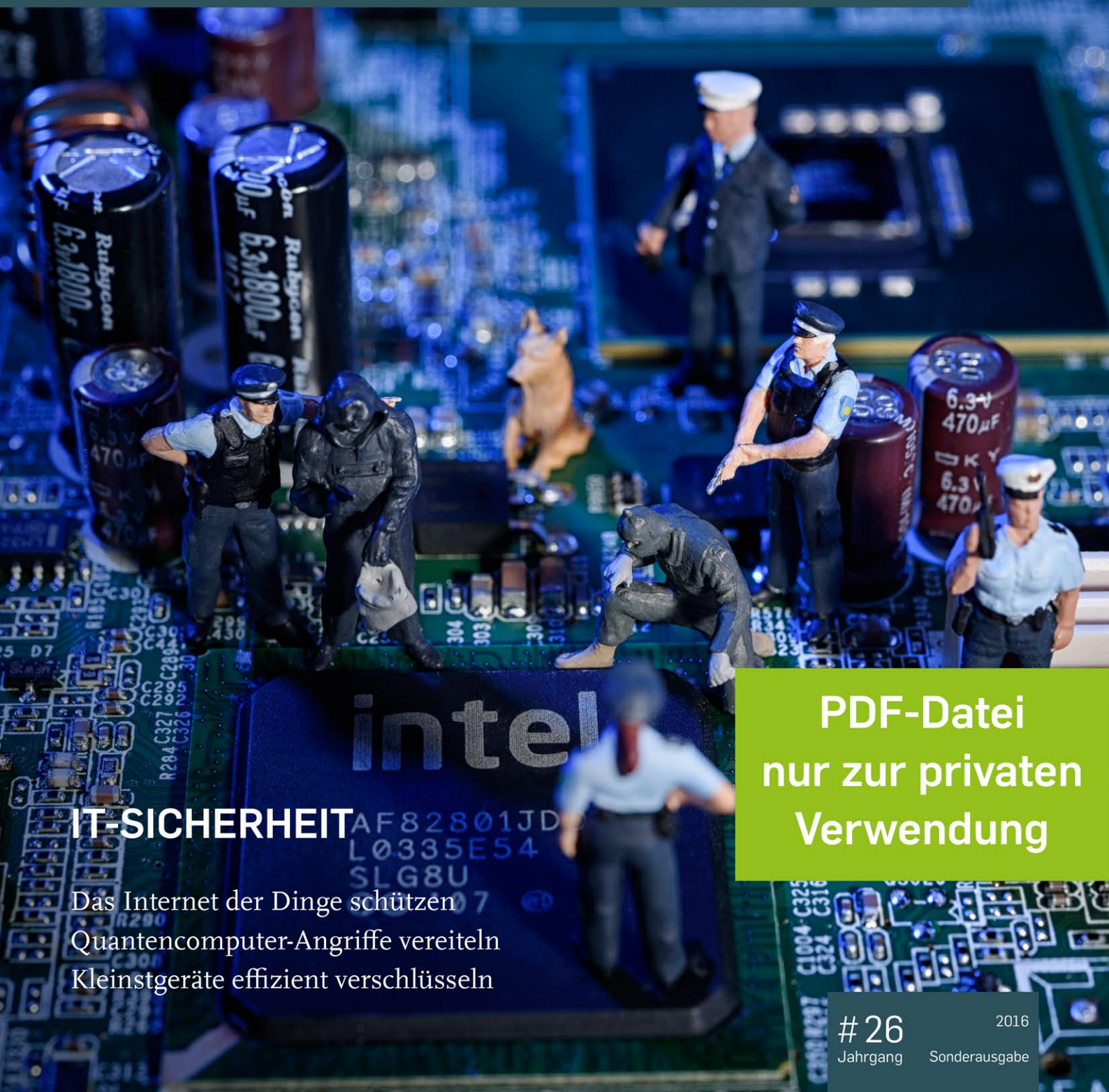
RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE



IT-SICHERHEIT

Das Internet der Dinge schützen
Quantencomputer-Angriffe vereiteln
Kleinstgeräte effizient verschlüsseln

#26 Jahrgang 2016 Sonderausgabe

IMS Messsysteme GmbH
World Market Leader in Measuring Systems

Interesse an modernster Messtechnik?

Sie sind der Meinung, **junge Ingenieurinnen und Ingenieure** sollten in jeder Hinsicht gefördert und anspruchsvolle Zukunftsperspektiven geboten werden? Dann teilen Sie unsere Überzeugung.

Finden Sie spannende und herausfordernde Möglichkeiten und steigen Sie bei uns ein!

Zur Verstärkung unserer Ingenieur-Teams suchen wir dauerhaft

HOCHSCHULABSOLVENTEN (W/M)

in den Bereichen Elektrotechnik und Informatik (TH/FH)

Zudem bieten wir Ihnen Möglichkeiten Abschlussarbeiten bei uns zu schreiben.

Wer wir sind?

Die IMS Messsysteme GmbH ist der Weltmarktführer für Messsysteme in der Walzindustrie mit Hauptsitz in Heiligenhaus, NRW und Niederlassungen weltweit. Wir sind der Innovationsführer hochpräziser radiometrischer und optischer Messsysteme in der Stahl-, Aluminium- und Kupferindustrie.

Was Sie mitbringen?

- Erfolgreich abgeschlossenes Hochschulstudium (TH/FH)
- Gute Englischkentnisse in Schrift und Wort
- Selbstständiges und eigenverantwortliches Arbeiten im Team
- Idealerweise erste Erfahrung in Mess- und Regeltechnik

Weitere Informationen zu unseren Stellenangeboten finden Sie im Internet unter

www.ims-gmbh.de/karriere
bewerbung@ims-gmbh.de

IMS Messsysteme GmbH
Dieselstraße 55 • 42579 Heiligenhaus

Foto: rs

SICHERHEIT IM DIGITALEN ZEITALTER

Der digitale Wandel ist in allen Bereichen unseres Lebens angelangt; unaufhaltsam durchdringt er alle Schichten und Aspekte der Gesellschaft. Die zunehmende Digitalisierung der Arbeits- und Lebenswelt bietet viele Chancen. Gleichzeitig wachsen auch die Herausforderungen für Datenschutz und -sicherheit: Der Austausch von persönlichen sowie wirtschaftlich relevanten Daten ermöglicht es, viele Aktivitäten in die virtuelle Welt zu verlagern; das schafft Raum für Begehrlichkeiten und Manipulationen. Nicht erst durch die Enthüllungen von Edward Snowden ist bekannt, wie wichtig es für einen modernen Staat ist, Informations- und Kommunikationssysteme abzusichern.

Neben den etablierten Diensten wie E-Mail und World Wide Web rücken das Internet der Dinge und Konzepte wie Industrie 4.0 in den Fokus. Zunehmend werden Geräte in die Lage versetzt, untereinander und mit dem Internet zu kommunizieren – von industriellen Produktionsmaschinen über Küchengeräte und Fernseher bis zum Automobil und Flugzeug. Sogar Einmalartikel und Gebrauchsgegenstände können an das Internet angebunden sein; es existieren zum Beispiel intelligente Leuchtmittel, die Nutzer per Smartphone-App fernsteuern können.

Dadurch entstehen ebenso viele verschiedene neue Einsatzszenarien wie Gefahren. Auf einer Sicherheitskonferenz in Las Vegas wurde im Sommer 2015 zum Beispiel demonstriert, wie einfach es ist, ein vernetztes Auto zu manipulieren und von Ferne die Bremsen zu betätigen – ein eindringliches und besorgniserregendes Beispiel für Gefahren in diesem Bereich. Bei der Digitalisierung spielt die IT-Sicherheit daher eine zentrale Rolle: Nur sichere und vertrauenswürdige IT-Prozesse werden es ermöglichen, die Informationstechnik nachhaltig positiv einzusetzen.

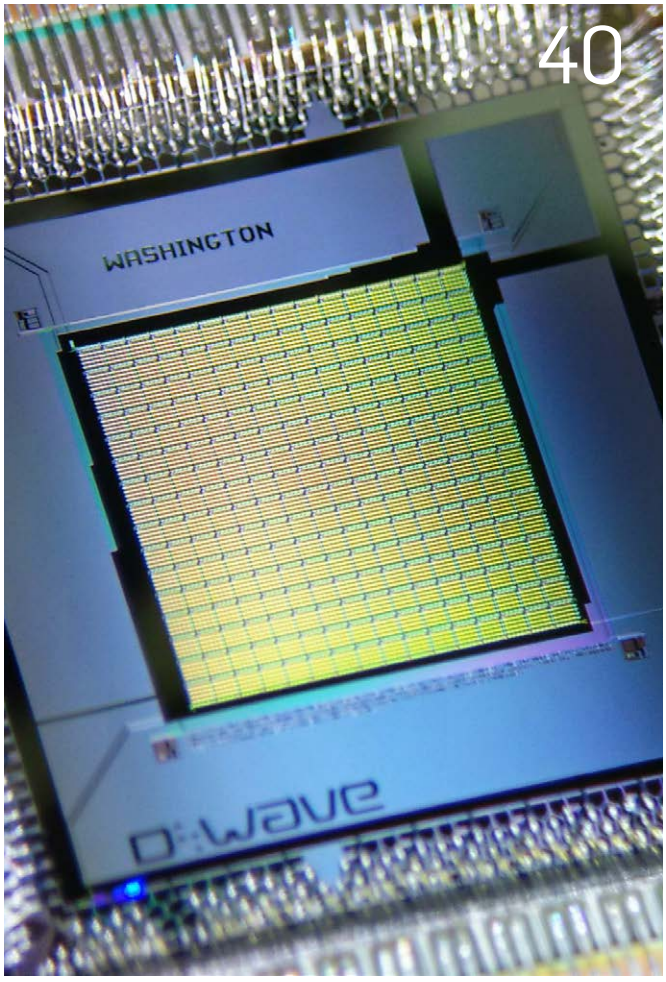
Dazu wollen wir am Horst-Görtz-Institut für IT-Sicherheit (HGI), dem national führenden Institut in diesem Bereich, beitragen. Wir decken viele Aspekte der modernen IT-Sicherheit und Kryptografie ab: Unsere Arbeit reicht von theoretischen Überlegungen zu Sicherheitsprotokollen und Kryptografie über Forschung zu Authentifizierungsverfahren bis hin zu praktischen Aspekten wie der Sicherheit von Softwaresystemen oder Hardwarebausteinen. Auf den folgenden Seiten geben wir einen Einblick in die unterschiedlichen Facetten von IT-Sicherheit und beleuchten einige Themen, mit denen wir uns in den vergangenen Monaten und Jahren beschäftigt haben. Entdecken Sie die spannende Forschung an unserem Institut und lernen Sie mehr über IT-Sicherheit, die in Zukunft noch wichtiger werden wird, als sie es heute bereits ist.

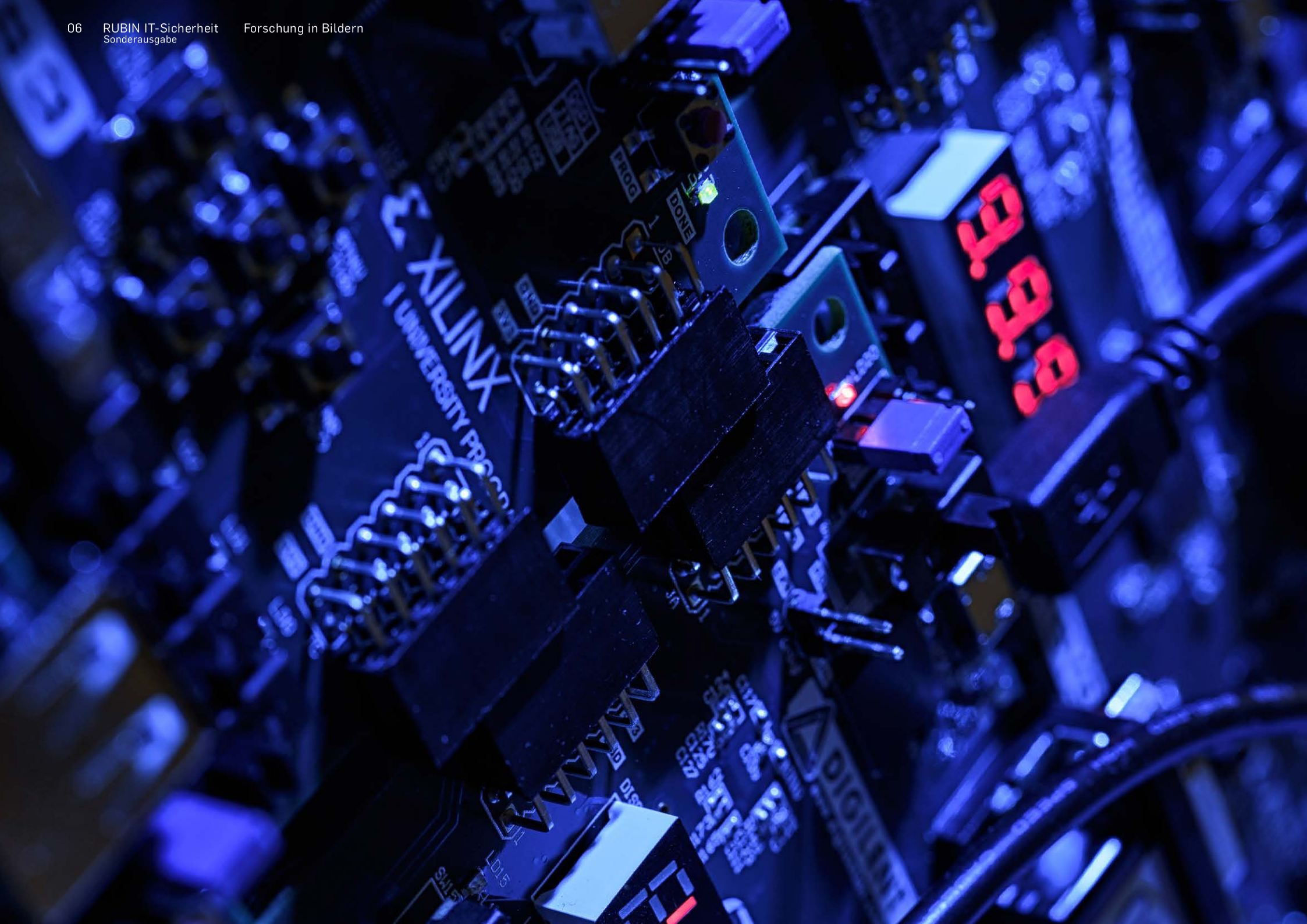
Es grüßt Sie herzlich

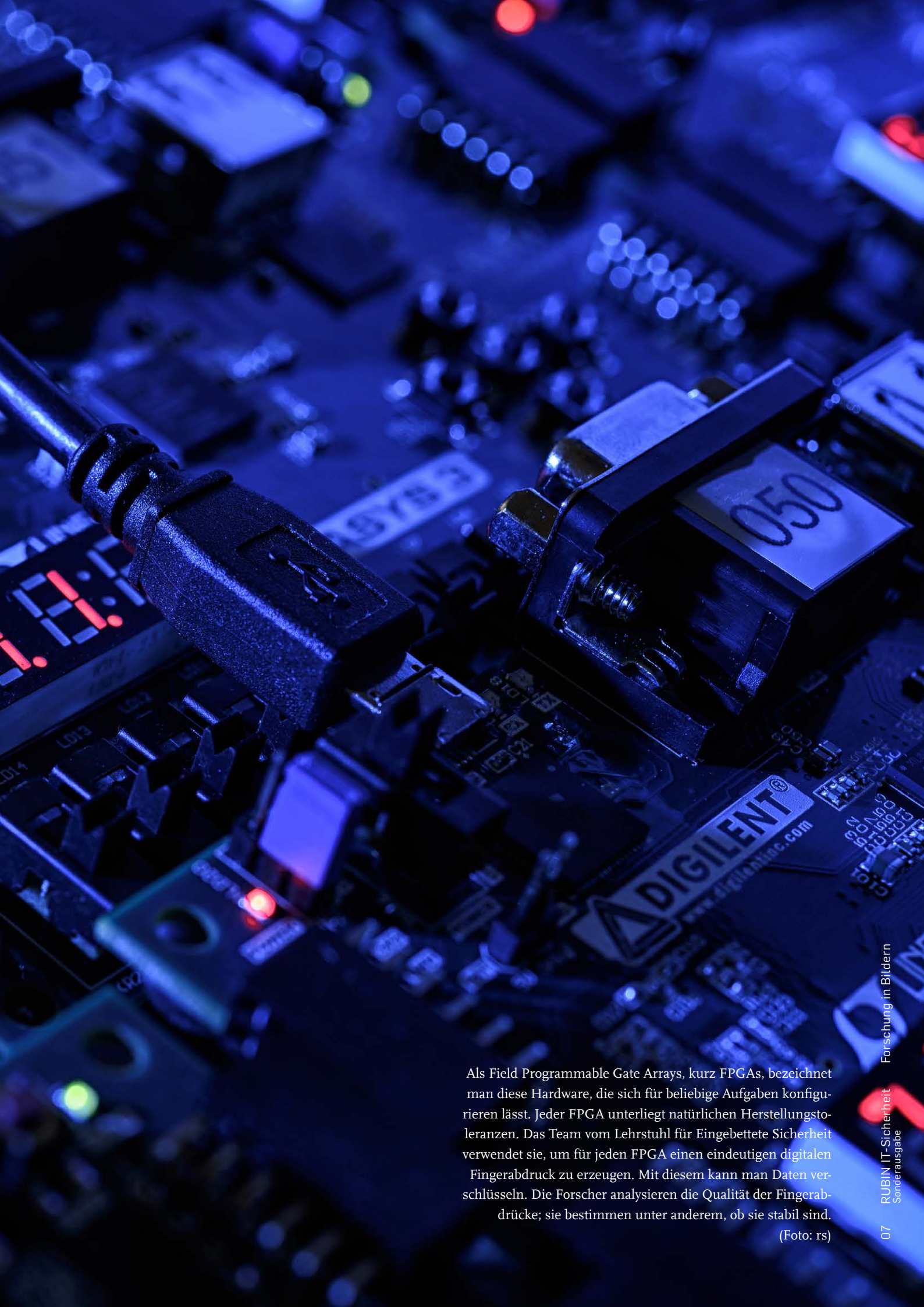
Prof. Dr. Thorsten Holz
Vorstand des Horst-Görtz-Instituts für IT-Sicherheit (HGI)

Aktuelle Infos finden Sie auch auf http://hgi.rub.de

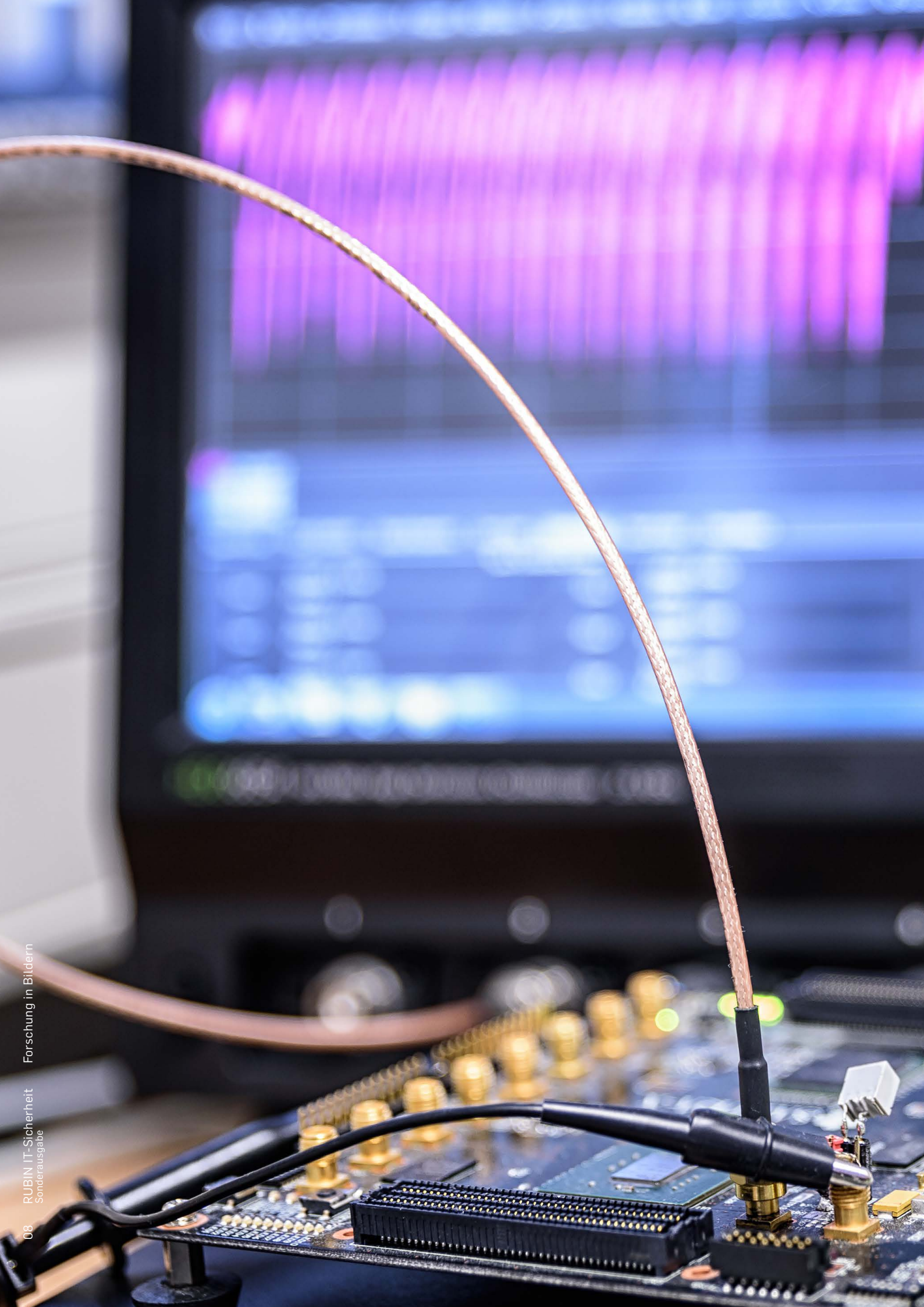
INHALT



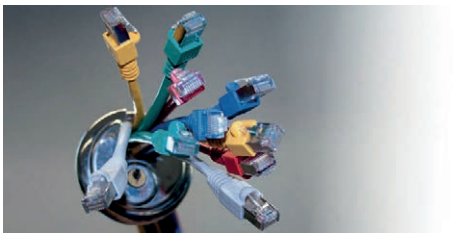

XILINX
PROG
DONE



Als Field Programmable Gate Arrays, kurz FPGAs, bezeichnet man diese Hardware, die sich für beliebige Aufgaben konfigurieren lässt. Jeder FPGA unterliegt natürlichen Herstellungstoleranzen. Das Team vom Lehrstuhl für Eingebettete Sicherheit verwendet sie, um für jeden FPGA einen eindeutigen digitalen Fingerabdruck zu erzeugen. Mit diesem kann man Daten verschlüsseln. Die Forscher analysieren die Qualität der Fingerabdrücke; sie bestimmen unter anderem, ob sie stabil sind. (Foto: rs)



Um Kryptoverfahren für Kleinstgeräte zu testen, entwickeln Forscher die zentralen Komponenten der Geräte und bauen sie auf Evaluierungsplattformen ein. Mit diesen können sie zeigen, dass Angreifer selbst unter optimalen Laborbedingungen nicht erfolgreich sein können. (Foto: rs)



ifAsec
Institut für Applikations-Sicherheit

SCUDOS-Security Protection: IT-Netze umfassend schützen und smart managen

SCUDOS-Security Protection: Secure IT-networks with Smart Management

Der Bedrohung der IT-Infrastruktur durch Cyber-Attacken aus dem Internet wird mittlerweile mit großem Aufwand entgegengewirkt. In Zeiten von BYOD und IoT verursachen Angriffe innerhalb eines zunehmend undurchsichtigen LAN-Netzwerkes mindestens ebenso große Schäden. Stichwort: Advanced Persistent Threats.

Besonders im Mittelstand besteht großer Handlungsbedarf, denn häufig sind dort Netzwerke unzureichend abgesichert. Ohne die Kenntnisse, welche Geräte sich in einem Netzwerk befinden und welche Dienste sie zur Verfügung stellen, kann kein effektiver Schutz bestehen. Nur wer sein Netzwerk kennt, kann sich effektiv schützen.

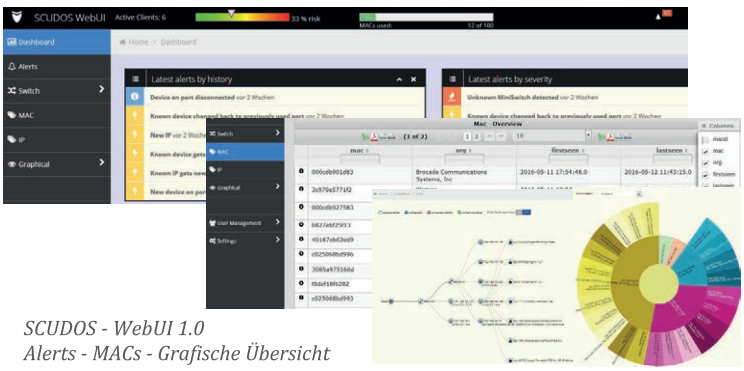
Wirksam begegnen Sie internen Angriffen mit Hilfe der innovativen Sicherheitslösung *SCUDOS-Security Protection*, durch Abkehr vom traditionellen perimeterbasierten Sicherheitskonzept hin zu einem *Zero-Trust-Modell*. Mit diesem Sicherheitsprodukt *Made In Germany* schützen und managen Sie Ihre IT-Netze effizent und intelligent.

Unser innovativer Ansatz zielt besonders auf:

- Erkennung sämtlicher Geräte und Dienste im Netzwerk
- Darstellung der Netzwerk-Topologie
- Verbindungshistorie aller Geräte und Real-Time-Inventarisierung
- Eliminierung unberechtigter Verbindungen fremder Geräte
- Erkennung von MITM-Szenarien
- Policy Enforcement

Weitere Merkmale, die SCUDOS auszeichnen:

- Dynamisches VLAN-Management
- Automatische Port-Abschaltung
- Unterstützung namhafter Application-Firewalls
- Simultane Verwaltung physikalisch getrennter Netzwerke
- Mandantenfähige Datenbasis zur Implementierung eines Security-as-a-Service Konzeptes



SCUDOS - WebUI 1.0
Alerts - MACs - Grafische Übersicht

CISOs are throwing in enormous resources at mitigating external attacks against IT-infrastructures, but what about threats from within the perimeter? Traditional approaches often fall short when facing challenges such as dynamic perimeters, BYOD strategies or APTs. It is only when you know exactly which devices are connected to the network and what services they are providing that you can achieve an effective protection.

As a tool following the *zero trust* approach, *SCUDOS-Security Protection* provides

- discovery of every single device and service in the network
- visualization of network topology
- connection history of every device and real-time inventory
- elimination of unauthorized connections to unknown devices
- detection of MITM setups
- policy enforcement

Additional unique features include

- dynamic VLAN management
- automatic port shutdown
- top application firewall support
- concurrent management of physically separate networks
- multitenancy to build up a Security-as-a-Service offering

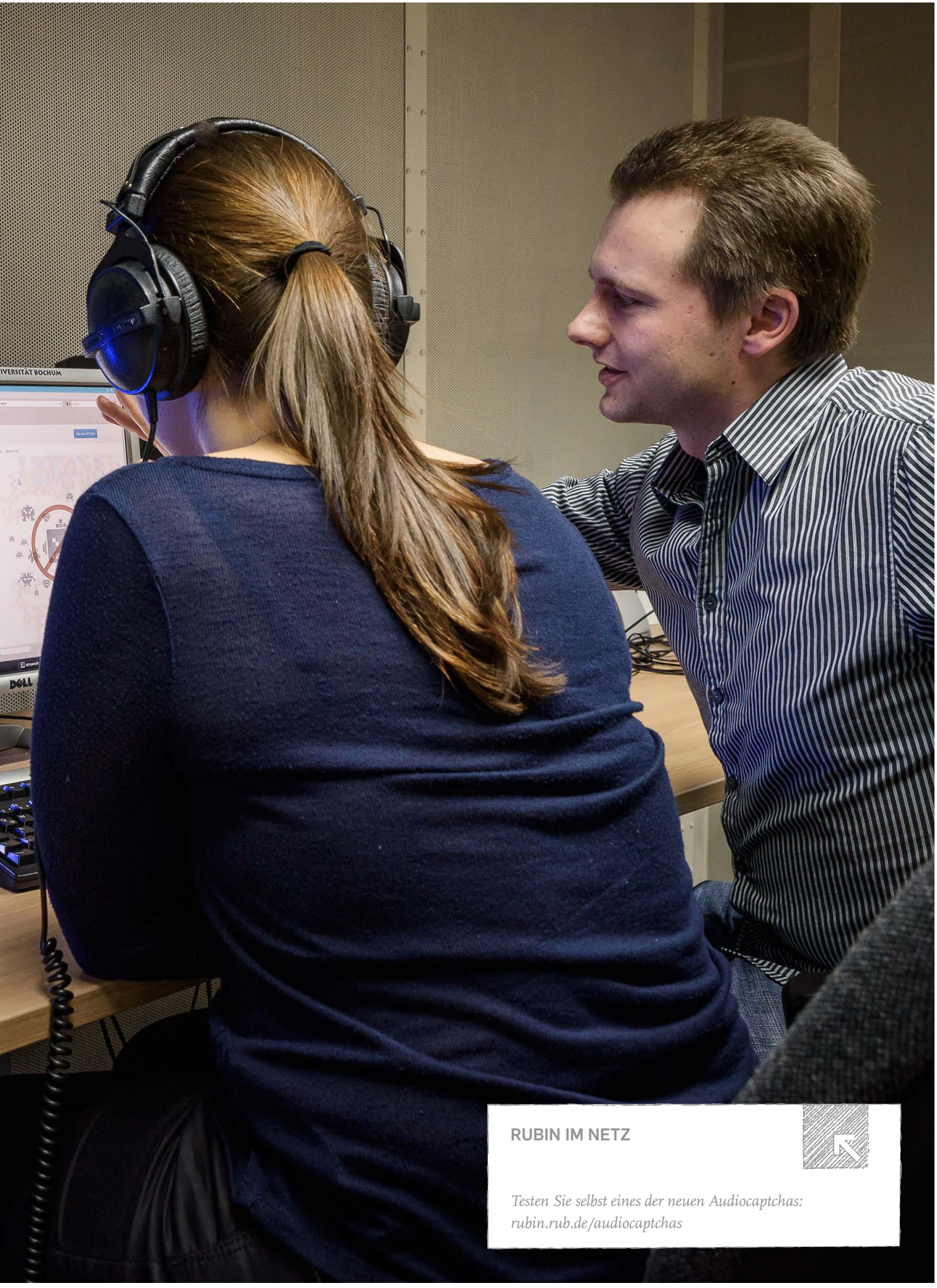
Profitieren auch Sie von *SCUDOS-Security Protection*, unserer zukunftsweisenden Lösung zum Schutz und smarten Management Ihrer Netzwerke.

Fordern Sie das *SCUDOS-Security Protection* Whitepaper an:

ifAsec GmbH
Institut für Applikations-Sicherheit
Emil-Figge-Straße 80
44227 Dortmund
Tel +49 231 976146-26 info@ifasec.de
Fax +49 231 976146-28 https://ifasec.de

MENSCH UND MASCHINE IM INTERNET UNTERSCHEIDEN

Um Spam zu vermeiden, muss man sich auf zahlreichen Webseiten als Mensch ausweisen, indem man eine schwer erkennbare Zeichenfolge eingibt. Für Sehbehinderte gibt es Audiocaptchas, deren Qualität aber ausbaufähig ist.



RUBIN IM NETZ

Testen Sie selbst eines der neuen Audiocaptchas:
rubin.rub.de/audiocaptchas

Abb. 1: Dorothea Kolossa leitet die Arbeitsgruppe Kognitive Signalverarbeitung des Instituts für Kommunikationsakustik.

Wer im Internet unterwegs ist, kommt an Captchas nicht vorbei. Die kleinen Felder mit den schwer leserlichen Buchstaben- oder Zahlenfolgen sollen dazu dienen, menschliche Internetnutzer von maschinellen zu unterscheiden, wobei Letztere unsere E-Mail-Postfächer mit Spam verstopfen. Für sehende Menschen ist die Eingabeprozedur einfach nervig. Die Zeichen sind oft so schlecht zu lesen, dass wiederholte und zeitraubende Versuche notwendig sind. Für Sehbehinderte stellt sie jedoch ein echtes Problem dar. Die Lösung sind Audiocaptchas. Dabei hört der Nutzer ein synthetisch erzeugtes und mehr oder weniger verzerrtes Wort oder eine Folge von Ziffern oder Buchstaben, die er anschließend per Tastatur eingeben muss. Als sehendem User fallen einem die Audiocaptchas im Internet bisweilen gar nicht auf. Nicht jede Webseite hat eins, und da, wo sie angeboten werden, verstecken sie sich meist hinter einem kleinen Button, der nicht direkt ins Auge fällt. Doch Audiocaptchas funktionieren häufig schlecht, die verzerrte Sprache ist für Computer ähnlich gut zu verstehen wie für Menschen, wenn nicht sogar besser.

Prof. Dr. Dorothea Kolossa und ihr Doktorand Hendrik Meutzner beschäftigen sich mit der Entwicklung sicherer Audiocaptchas. Dringen aus Meutzners Büro bisweilen gruselig verzerrte Laute mit viel Nachhall, so darf man sich daher nicht wundern. Immer wieder hört sich der 32-Jährige Audiocaptchas an. Für Ungeübte sind diese oft nur schwer zu verstehen. „Die Herausforderung ist, die Signale so schwierig zu machen, dass die Maschine Probleme damit hat, und gleichzeitig so einfach, dass Menschen die Aufgabe gut lösen können“, sagt Dorothea Kolossa, die die Arbeitsgruppe Kognitive Signalverarbeitung des Instituts für Kommunikationsakustik leitet.

Bei den Maschinen handelt es sich um automatische Spracherkenner. Solche Systeme kennt man zum Beispiel von Navigationsgeräten oder Handys, die sich per Sprachbefehl steuern lassen. „Bei den gängigen Audiocaptchas werden alle Ziffern und Buchstaben auf eine sehr ähnliche Art und Weise ausgesprochen. Das macht es Angreifern einfach, Modelle daraus abzuleiten und Spracherkenner darauf zu trainieren“, erklärt Meutzner.

Um sicherere Captchas zu entwickeln, analysieren er und Dorothea Kolossa, wo die Unterschiede zwischen menschlicher und maschineller Sprachverarbeitung liegen. Dazu gehört auch, dass die beiden sich mit den neurophysiologischen Grundlagen beschäftigen. Sie wollen nachvollziehen, wie das menschliche Gehirn mit eingehenden Sprachsignalen umgeht und wo es der Technik voraus ist. „Es ist zum Beispiel sehr aufschlussreich für uns zu verstehen, wie der Mensch zwei oder mehr gleichzeitig eingehende akustische Signale voneinander trennt“, sagt Dorothea Kolossa (Abb. 1). Wenn er sie über beide Ohren präsentiert bekommt, kann der Mensch sogar bis zu fünf gleichzeitig eintreffende Signale auseinanderhalten. Fachleute nennen diesen Effekt auditorisches Streaming. Möglich wird das unter anderem durch die Zeitverzögerung, mit der die Töne an beiden Ohren eintreffen. Außerdem wirkt der zwischen den Ohren liegende Schädel dämpfend, sodass die Lautstärke der Signale an beiden Ohren meist unterschiedlich ist. Um mehr darüber zu erfahren, wie auditorisches Streaming genau realisiert wird, ist Dorothea Kolossa eine Kooperation mit der University of California, Berkeley eingegangen. Die Wissenschaftler betrachten dabei die neuronalen Signale vom Innenohr bis zum auditorischen Kortex.

Bei der Entwicklung neuer Audiocaptchas nutzt Hendrik Meutzner diese menschliche Überlegenheit aus. Eines seiner Captchas präsentiert den Hörerinnen und Hörern eine Folge von Zahlen, wobei sich immer zwei von ihnen teilweise überlagern. Zusätzlich erschwert Nachhall, das Gesprochene zu verstehen. Ein anderes seiner Captchas nutzt das menschliche Sprachverständnis. Es präsentiert dem Hörer eine Folge von Wörtern, von denen manche einen Sinn ergeben und der Rest

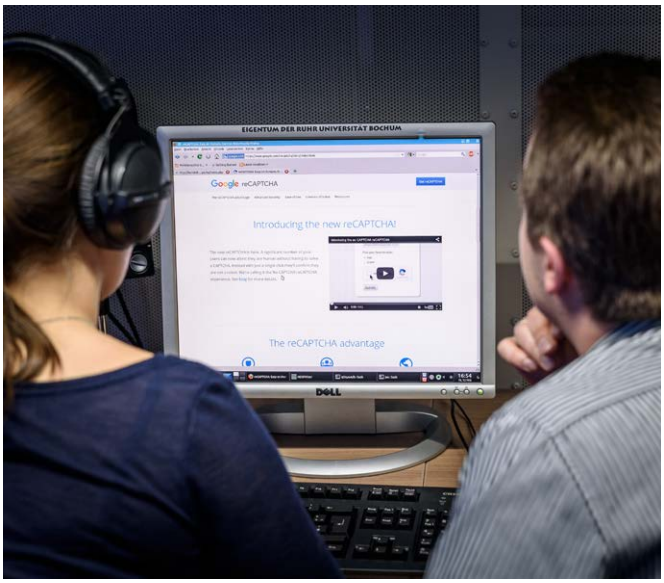


Abb. 2: In einem speziellen Labor lässt Hendrik Meutzner die verschiedenen Audiocaptchas von Probandinnen und Probanden testen. Zusätzliche Testpersonen findet er im Internet auf einer Crowdsourcing-Plattform.

Kauderwelsch ist. Der Mensch ist in der Lage, die sinnvollen Wörter zu erkennen. Der Maschine fällt das schwer, da sich die Wörter im Spektralbereich stark ähneln. Bei diesem Captcha lag die menschliche Erfolgsrate bei 60 Prozent im Vergleich zu 14 Prozent bei der Maschine. Bei dem Audiocaptcha, das von einer großen Web-Suchmaschine momentan eingesetzt wird, liegt die Erfolgsrate für den Menschen hingegen bei 24 Prozent. Die Maschine ist ihm mit 63 Prozent Trefferrate haushoch überlegen; das hat Meutzner ebenfalls in eigenen Tests herausgefunden.

Um zu prüfen, wie gut seine Captchas für Menschen zu lösen sind, nutzt Hendrik Meutzner zwei Methoden: Zum einen lädt er Probandinnen und Probanden in das institutseigene Audiometrielabor ein und lässt sie die Captchas lösen (Abb. 2). Da er für seine Tests aber sehr viele Versuchspersonen braucht, lässt er die Captchas parallel im Internet auf einer speziellen Crowdsourcing-Plattform testen. „Dieses Vorgehen wird immer attraktiver in der Wissenschaft, denn es ist sehr mühsam und zeitaufwendig, Versuchspersonen vor Ort zu finden und die Tests mit ihnen durchzuführen. Auf der Crowdsourcing-Plattform haben wir die Möglichkeit, eine große Zahl von Versuchspersonen vergleichsweise einfach zu rekrutieren“, erzählt Meutzner. Abstriche muss man allerdings in der Qualität der Antworten machen. „Im Labor sind die Probanden einfach konzentrierter und die Rahmenbedingungen wie Ruhe und technisches Equipment sind optimal. Aber die Kombination von beiden Methoden ist für uns ideal.“

Text: rr, Fotos: rs

Abb. 1: Erkennen Sie, was dargestellt ist? Wenn nicht, hilft Ihnen ein Blick auf die nächste Doppelseite. Mooney-Bilder wie dieses hier könnten in Zukunft eingesetzt werden, wenn Internetuser ihr Passwort für einen Account vergessen haben. (Bild: rs)

PASSWÖRTER SICHERER MACHEN

Passwörter sind ein notwendiges Übel, wenn es darum geht, seine Daten geheim zu halten. Leider sind die sichersten auch die, die am schwersten zu merken sind.

Prof. Dr. Markus Dürmuth von der Arbeitsgruppe Mobile Sicherheit kennt das Problem: „Keiner mag Passwörter. Um sich das Leben leichter zu machen, nehmen viele von uns das immer gleiche Kennwort für unterschiedliche Konten oder wählen Passwörter, die so leicht zu erraten sind, dass sie keinen ausreichenden Schutz darstellen." Dürmuth (Abb. 2) erforscht verschiedene Verfahren. Besonderes Augenmerk hat er in einer Studie auf Passwörter für mobile Geräte gelegt. Bei ihnen ist die Eingabe besonders umständlich. Schnell ist versehentlich die falsche Ziffer auf dem kleinen Display eingetippt. Zudem sind Sonderzeichen und Zahlen auf der zweiten und dritten Tastaturebene versteckt.

Auf Androidhandys ist seit einiger Zeit eine grafische Passwortalternative verfügbar. Sie erleichtert zumindest das Entsperren des Gerätes. Dabei ziehen die Handynutzer auf dem Display eine Linie mit dem Finger, um einige der angezeigten Punkte miteinander zu verbinden (Abb. 3). Wie sicher das Verfahren ist, war lange Zeit nicht besonders gut untersucht. Viele Studien nahmen die Anzahl der möglichen Passwörter als Maßstab. Bei einem Drei-mal-drei-Feld gibt es immerhin 389.112 Möglichkeiten, wenn man davon ausgeht, dass man jede Stelle nur einmal verwenden darf und das Passwort aus vier bis neun Punkten besteht. Bei der klassischen PIN, die der Anwender eintippt, ist die Zahl der theoretisch möglichen Kombinationen deutlich geringer; bei einer dreistelligen PIN liegt sie bei gerade einmal 1.000, bei einer vierstelligen bei 10.000.

In der Realität nutzen Besitzerinnen und Besitzer von Mobilgeräten ihre Möglichkeiten, ein sicheres Passwort zu erstellen, jedoch längst nicht aus. Um es sich leichter merken zu können, verwenden sie immer wiederkehrende Muster, wie Markus Dürmuth und Kollegen bei einem Experiment herausfanden. Dafür baten sie in der Mensa der Ruhr-Universität 400 Studierende, sich ein grafisches Passwort zum Entsperren eines Handys auszudenken. Um möglichst realistische Ergebnisse zu bekommen, trafen die Forscher einige Vorkehrungen: Die Testpersonen mussten sich das Passwort merken, während sie essen waren. In dieser Zeitspanne konnten andere Personen versuchen, den Code zu knacken. Das Muster musste also leicht genug sein, um es sich merken zu können, und schwer genug, damit kein anderer es erraten konnte.

Bei dem Experiment boten die Wissenschaftler den Testper-

Abb. 2: Markus Dürmuth leitet die Arbeitsgruppe Mobile Sicherheit an der Ruhr-Universität Bochum.

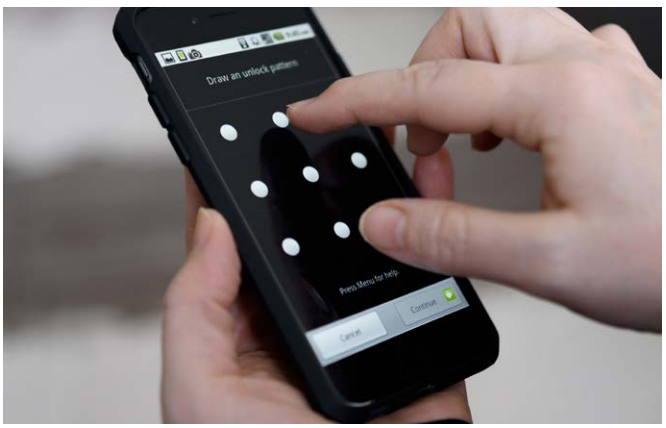


Abb. 3: Auf Androidgeräten ist dieses grafische Passwortverfahren weit verbreitet: Der Nutzer verbindet Punkte, statt ein Wort oder eine Zahlenkombination einzutippen.

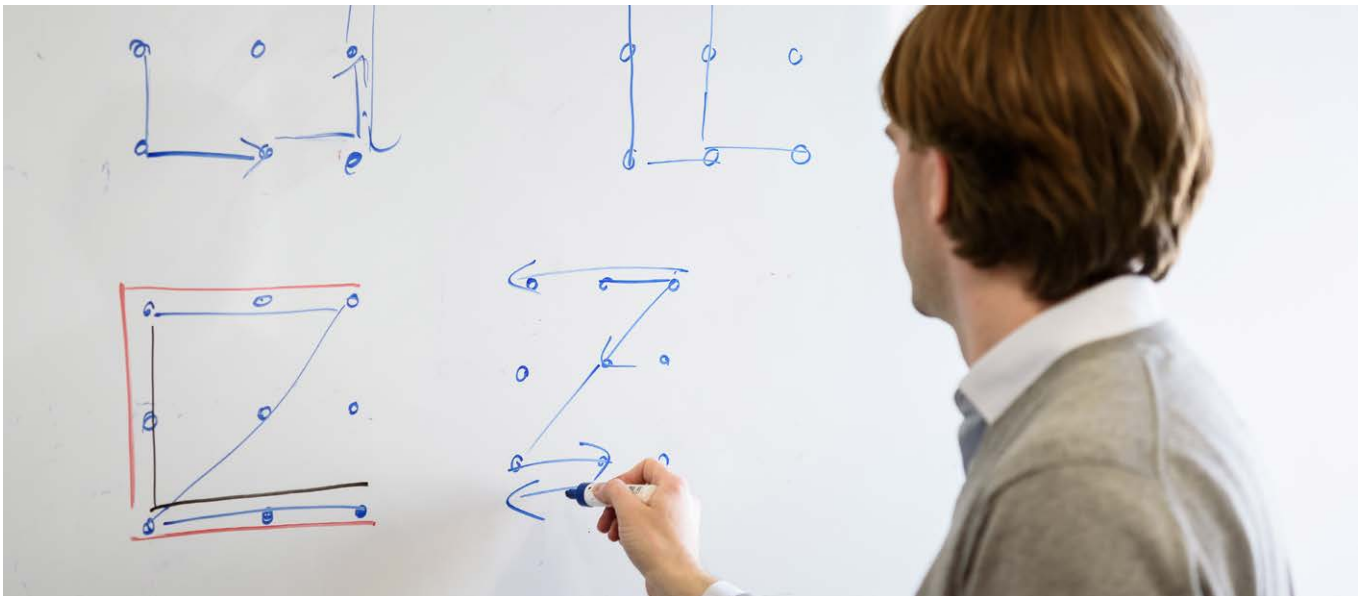


Abb. 4: Zum Entsperren ihres Handys müssen Androidnutzer einige Punkte auf einem Drei-mal-drei-Feld miteinander verbinden. Viele wählen ein „L“ oder „Z“ als Muster, wie Markus Dürmuth zeigt.

sonen neben dem klassischen Drei-mal-drei-Feld auch Felder mit alternativen Punktanordnungen an. Es kam heraus, dass die Testpersonen bei der herkömmlichen Anordnung häufig beispielsweise ein „L“ oder ein „Z“ in verschiedenen Variationen wählten (Abb. 4). „Von zufällig gewählten Mustern kann in den meisten Fällen also nicht die Rede sein“, so Dürmuth. Dieben mache man es so viel zu leicht, das Passwort zu erraten. Die sichersten Passwörter brachte die kreisförmige Anordnung der Ziffern auf dem Handydisplay hervor (Abb. 5). Sie verführte am wenigsten dazu, gängige Muster zu wählen.

Ebenfalls mit Passwörtern beschäftigt sich Markus Dürmuth in einem zweiten Projekt. Hier geht es darum, die Sicherheit bei der sogenannten Fallback Authentification zu verbessern. Dies ist das Verfahren, mit dem wir ein Passwort zurücksetzen können, wenn wir es vergessen haben. Es gibt zwei verbreitete Methoden, wie das geschieht: Beim „Reset by Email“ bekommt der User ein neues Passwort per E-Mail zugeschickt. Diese Vorgehensweise birgt jedoch Risiken, da die Mail mit dem neuen Passwort im Klartext übertragen wird. Zudem kommt sie unter Umständen in einem Konto an, das zwar zum Zeitpunkt der ursprünglichen Anmeldung aktuell war, inzwischen aber vielleicht gar nicht mehr genutzt wird und an das man sich nicht mehr erinnert. Die zweite Methode ist die der Sicherheitsfragen. Dabei stellt der Rechner dem User eine Frage wie beispielsweise „Wie lautet der Mädchenname der Mutter?“. Die korrekte Antwort hat man festgelegt, als man den Account eingerichtet hat. Schwachstelle hierbei: „Mit ein bisschen Glück und Recherche kann der Angreifer einige der Sicherheitsfragen richtig beantworten“, meint Markus Dürmuth.

Abb. 5: Bei einem Experiment testeten die Wissenschaftler, ob Nutzer sicherere Passwörter generieren, wenn die Punkte auf dem Androidhandy nicht als klassisches Drei-mal-drei-Feld angeordnet sind. (Grafik: Agentur der RUB, Zalewski)

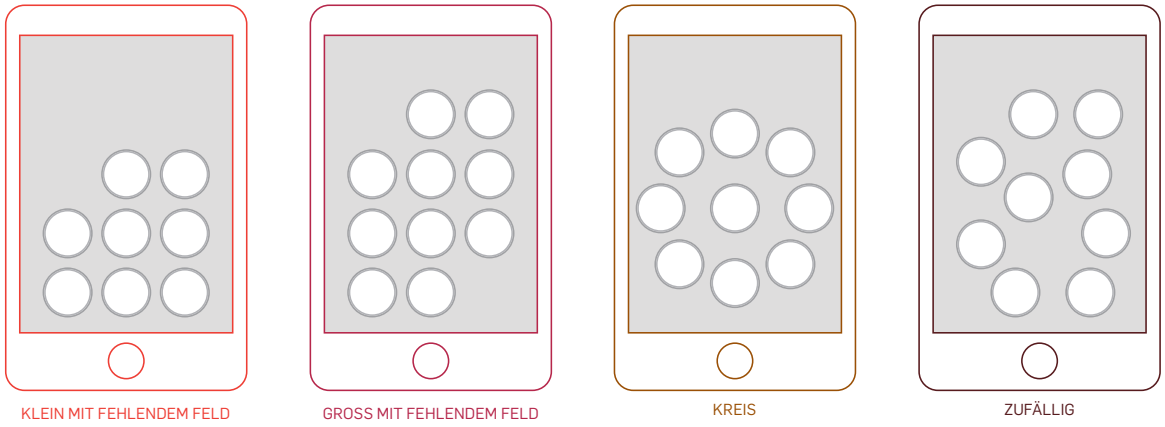


Abb. 6: Das Originalbild zum gezeigten Mooney-Bild auf Seite 16.
Wer es einmal gesehen hat, wird das Mooney immer wieder sofort erkennen.

„KEINER MAG PASSWÖRTER.“

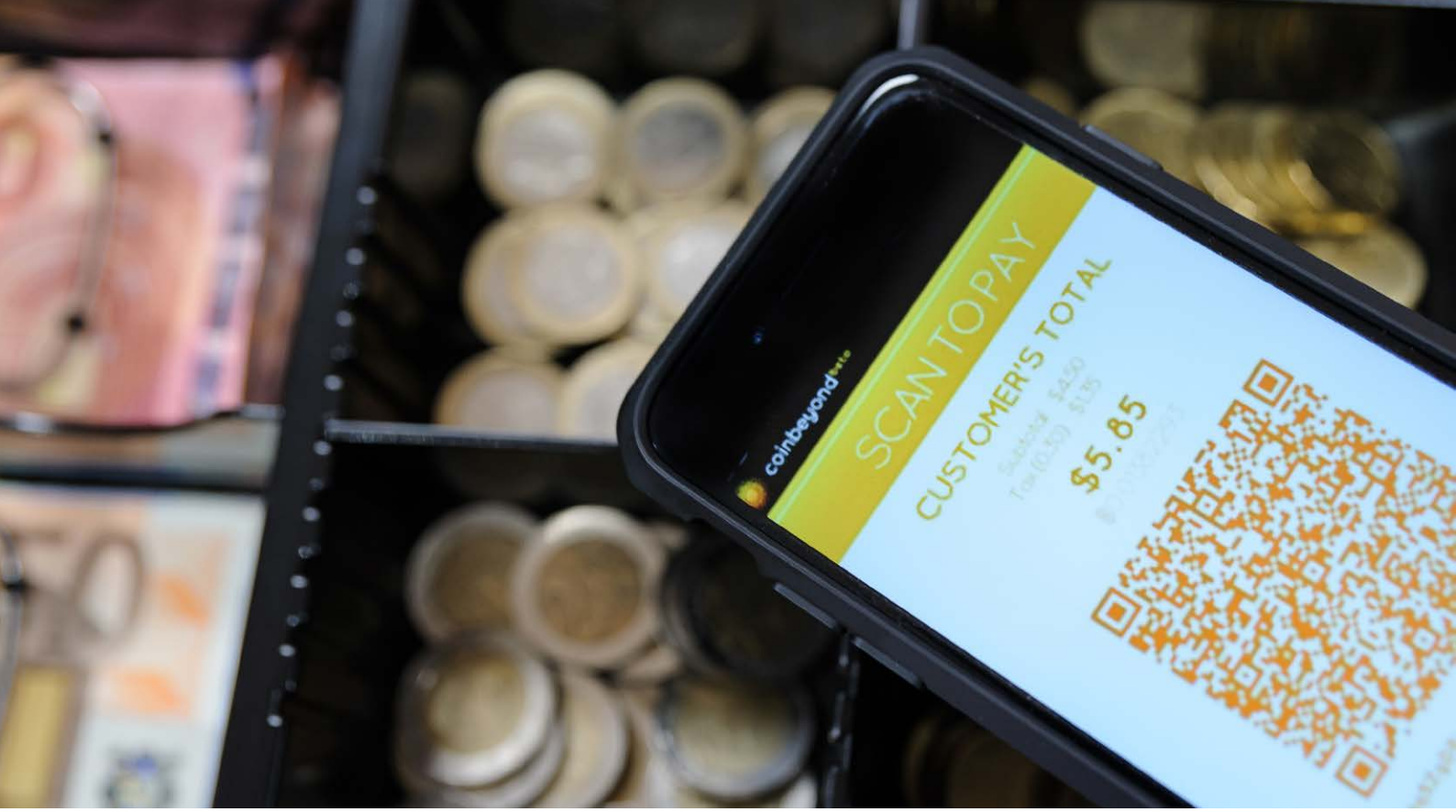
Ein Fall, bei dem Hacker genau diese Schwachstellen genutzt haben und der 2012 durch die Medien ging, ist der des US-Journalisten Matt Honan. Angreifer hackten zunächst seinen E-Mail-Account und nutzten dann die Fallback Authentification, um sich neue Passwörter für weitere Accounts erstellen zu lassen. Damit übernahmen sie Schritt für Schritt alle seine anderen Konten und stahlen so Honans gesamte digitale Identität.

Markus Dürmuth hat gemeinsam mit einer Kollegin der University of California, Berkeley, und einem Kollegen des „Institut National de Recherche en Informatique et en Automatique“ (INRIA), Grenoble, eine Alternative zu dem beschriebenen Verfahren entwickelt. Sie nutzen dabei sogenannte Mooney-Bilder (Abb. 1). Das sind Schwarz-Weiß-Bilder, die mit einem speziellen Filter bearbeitet wurden. Sieht man ein Mooney-Bild, erkennt man darauf erst einmal nichts. Erst wenn man das Originalbild zu sehen bekommt, erkennt man auch auf dem Mooney das Motiv (Abb. 6) – ein Effekt, der für lange Zeit anhält. Man spricht von Priming oder Prägung auf das Bild. Ihren Ursprung haben die Bilder in der Hirnforschung. Hier setzte der Psychologe Craig Mooney sie in den 1950er-Jahren ein, um diesen sogenannten Aha-Effekt mittels Magnetresonanztomografie näher zu untersuchen.

Bei der Fallback Authentification nutzt Dürmuth den Mechanismus so: Statt sich für den Fall der Fälle eine Sicherheitsfrage und die entsprechende Antwort zu überlegen, bekommt der Anwender in der Primingphase zehn Mooneys und die dazugehörigen Originalbilder gezeigt. Vergisst er dann irgendwann sein Passwort, bekommt er 20 Mooneys gezeigt und soll angeben, was er erkannt hat. „Der echte Kontoinhaber wird die zehn Mooneys wiedererkennen, auf die er geprägt wurde“, so Dürmuth. „Die anderen zehn kann er jedoch nicht identifizieren. Er bekommt dann direkt ein neues Kennwort zugewiesen.“ Ein Hacker würde sich dadurch verraten, dass er entweder gar keine Mooneys erkennt, oder aber auch solche, die dem eigentlichen Nutzer unbekannt sind.

Einen Haken hat das Verfahren allerdings noch: Wenden es verschiedene Webseiten an, kann es im ungünstigsten Fall sein, dass der Nutzer bei einer Seite auf ein Mooney geprägt wird, das auf einer anderen als nicht geprägt gilt – mit der Folge, dass er es dort erkennt, obwohl ihn das als Hacker kennzeichnet. „Wir verfolgen das Projekt daher noch weiter. Allerdings denke ich schon, dass es eine echte und gute Alternative zum bisherigen Verfahren ist“, sagt Dürmuth.

Text: rr, Fotos: rs



ENERGIEEFFIZIENTE SICHERHEITSMECHANISMEN FÜR DIGITALE WÄHRUNGEN

Um Betrügereien mit digitalen Währungen wie Bitcoin zu verhindern, sind ausgeklügelte Sicherheitsmechanismen am Werk. Noch fressen sie allerdings immense Mengen Strom.

Mittlerweile gibt es Hunderte von digitalen Währungen, mit denen Nutzer rein virtuell existierendes Geld bewegen können. Verbreitet hat sich bislang allerdings vor allem eine Währung, nämlich Bitcoin (Info). Anders als beim Euro oder Dollar gibt es dafür keine Zentralbank, die das Geld verwaltet. Die Aufgabe wird stattdessen dezentral von den Bitcoin-Nutzerinnen und -Nutzern übernommen. Für diese digitalen Währungen interessiert sich Prof. Dr. Sebastian Faust von der Arbeitsgruppe Angewandte Kryptographie (Abb. 1). Um zu verstehen, welche Fragen er erforscht, muss man sich zunächst detaillierter ansehen, wie das System funktioniert.

Im Bitcoin-Netzwerk sind einzelnen Nutzern virtuelle Beträge zugeordnet, die sich mithilfe von Transaktionen übertragen lassen. Eine besondere Herausforderung bei digitalen Währungen ist es zu unterbinden, dass Leute ihr virtuelles Geld doppelt ausgeben. Um diese und andere Betrügereien zu verhindern, besitzt das System einen ausgeklügelten Sicherheitsmechanismus (siehe Infografik, Seite 22).

Ein Teil der Nutzer, sogenannte Miner, sammeln und überprüfen alle Transaktionen. Neue Transaktionen fassen sie in einem Block zusammen und versuchen, diesen in einer frei zugänglichen Datenbank zu veröffentlichen, der Blockchain. Dabei will jeder Miner der schnellste sein, denn: Für jeden neuen Block erhält er derzeit eine finanzielle Belohnung von 25 Bitcoins, was nach dem Umrechnungskurs im Mai 2016 rund 10.000 Euro entspricht. Damit ein Miner einen Block veröffentlichen und somit letztendlich für gültig erklären kann, muss er zuvor ein kryptografisches Rätsel lösen, das Proof-of-Work-Rätsel. Das ist schwierig und erfordert jede Menge Rechenpower. So konkurrieren alle Miner um die Veröffentlichung des jeweils nächsten Blocks. Im Durchschnitt passiert das alle zehn Minuten.

Beim Proof-of-Work-Rätsel bekommen die Miner, vereinfacht gesagt, eine mathematische Funktion vorgegeben, deren Ausgabe sich wie eine Zufallszahl verhält. Ihre Aufgabe ist es, zu dieser Funktion einen bestimmten Input zu finden, sodass der Output der Funktion mit sehr vielen Nullen beginnt.

An die Lösung des Rätsels können sich die Miner nicht schrittweise herantasten, sondern müssen viele verschiedene Inputs ausprobieren, bis sie einen passenden finden. Dafür müssen sie permanent rechnen. Aber warum der Aufwand?

Da sich prinzipiell alle Bitcoin-Nutzer als Miner betätigen können, ist nicht auszuschließen, dass sie sich zig Identitäten zulegen. Könnten diese zusätzlichen Identitäten helfen, Proof-of-Work-Rätsel zu lösen, somit häufiger Blöcke zu veröffentlichen und mehr Gewinn zu machen? Nein, denn dafür ist nur die Rechenleistung ausschlaggebend. Mit einem handelsüblichen Rechner bräuchte man inzwischen Jahre, um eine Lösung für ein Proof-of-Work-Rätsel zu finden. Aus diesem Grund betätigen sich hauptsächlich Firmen als Miner oder sogenannte Mining-Pools, also Zusammenschlüsse von Einzelpersonen, die die Gewinne teilen. „Die Sicherheit des Systems ist mittelfristig gewährleistet, solange mindestens 50 Prozent der gesamten Rechenleistung von ehrlichen Minern kontrolliert werden“, sagt Sebastian Faust.

Experten schätzen, dass das Bitcoin-Netzwerk wegen der Proof-of-Work-Methode eine höhere Rechenleistung hat als Google – und damit ist es nicht gerade umweltschonend. Mit seinen Kolleginnen und Kollegen hat Faust eine energieeffizientere Alternative vorgeschlagen. Das Bochumer Rätsel basiert auf Speicherplatz anstatt auf Rechenleistung; es nennt sich Proof-of-Space-Rätsel. Der Nutzer muss es zu Beginn einmal rechenintensiv initialisieren; dabei wird eine große Menge an Festplattenspeicher belegt. Dann kann er das Rätsel ohne großen weiteren Rechenaufwand lösen. Das ist jedoch nur möglich, solange er tatsächlich den Speicher für die Lösung des Rätsels zur Verfügung hat.

Vereinfacht dargestellt funktioniert das System wie folgt: Der Rätsellöser muss eine Reihe von Zahlen nach aufsteigendem Wert sortieren und die sortierte Liste speichern. Wenn er das Rätsel veröffentlichen will, wird er nach der Zahl an einer bestimmten Position in der Liste gefragt. Hat er die sortierte Liste wie erfordert gespeichert, kann er die Antwort schnell auslesen. „Das ist die Grundidee, aber in Wahrheit ist das Rätsel natürlich komplizierter“, erklärt Sebastian Faust. Eine Gruppe am Massachusetts Institute of Technology in Boston und am Institute of Science and Technology Austria in Wien hat das Proof-of-Space-Konzept bereits erweitert und darauf basierend eine neue digitale Währung erfunden.

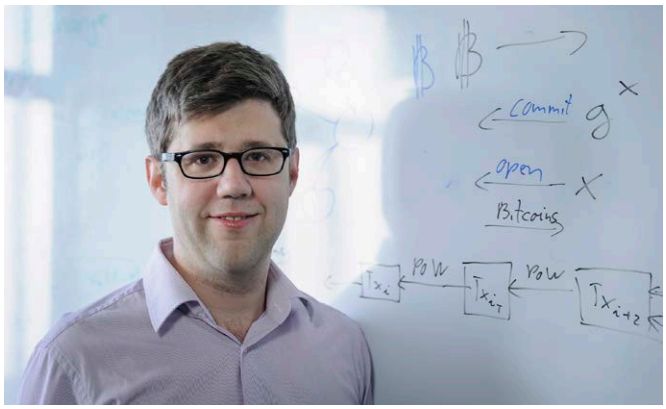


Abb. 1: Sebastian Faust erforscht digitale Währungen.

DIGITAL ZAHLEN MIT BITCOINS

INFO

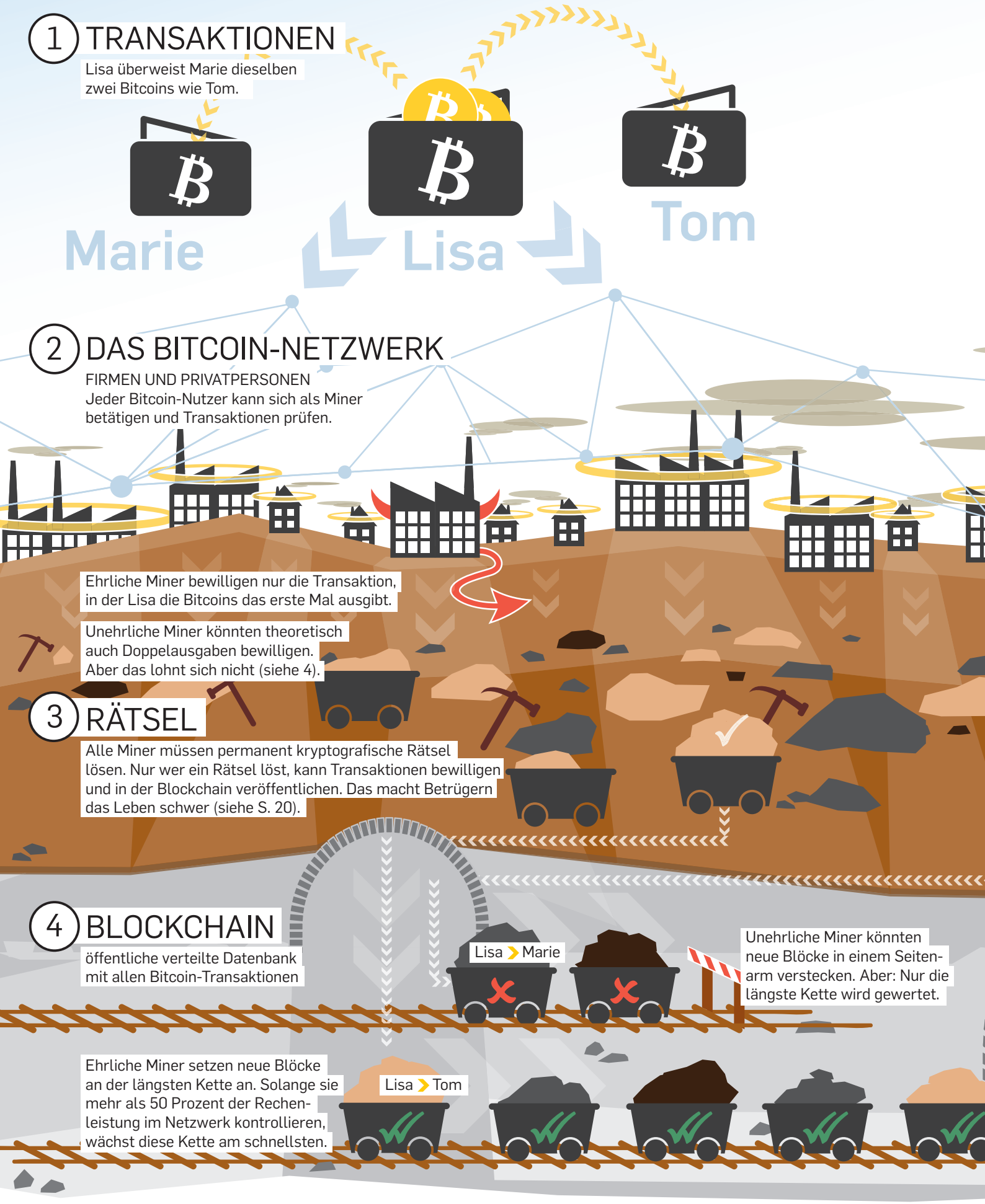
Bitcoins können Interessierte im Internet bei sogenannten Exchanges erwerben. Entsprechend dem aktuellen Wechselkurs werden Euro, Dollar oder andere Währungen in das digitale Geld umgetauscht. Ein Bitcoin war im Mai 2016 rund 390 Euro wert. Jeder Bitcoin-User besitzt einen geheimen Schlüssel, der ihm oder ihr die Coins zuordnet. Einige große Firmen, zum Beispiel der Computeranbieter Dell oder das Online-Reisebüro Expedia, akzeptieren inzwischen Bitcoins. Da die Währung eine gewisse Anonymität gewährleistet, ist sie aber auch bei vielen illegalen Transaktionen im Einsatz.

Die Bochumer Gruppe beschäftigt sich aber auch mit weiteren Aspekten des Bitcoin-Netzwerks, zum Beispiel mit der Sicherheit von Smart Contracts. Das sind Verträge, die Zahlungen nur unter bestimmten automatisch prüfbaren Bedingungen ausführen. Angenommen Person A möchte Person B ein Geheimnis verkaufen, aber dieses erst herausgeben, wenn sie das Geld erhalten hat. Person B wiederum möchte nur zahlen, wenn sie das Geheimnis bekommen hat. Ein Smart Contract würde die Garantie liefern, dass beide Seiten bekommen, was die Abmachung verspricht. Die Technik erlaubt einen fairen und einfacheren Zahlungsverkehr und könnte zum Beispiel Notare ersetzen. Gleichzeitig erschließen sich damit neue Anwendungsfälle wie Smart Property: die automatisierte Verwaltung von Besitz über die Blockchain, was etwa für Mietwagen oder -wohnungen denkbar wäre. Grundsätzlich könnten Smart Contracts Betrug verhindern und den internationalen Handel vereinfachen.

Für die Zukunft hat Sebastian Faust noch einen weiteren Plan: „Wir möchten das Bitcoin-System gern formal analysieren und beweisen, dass es sicher ist.“ Eine formale Analyse gibt es bislang nur von Erfinder Satoshi Nakamoto. Aus ihr stammt die Angabe, dass das Netzwerk sicher ist, solange ehrliche Nutzer mehr als 50 Prozent der Rechenleistung kontrollieren. Amerikanische Forscher haben allerdings bemängelt, die Auswertung basiere auf sehr vielen, teils vereinfachten Annahmen.

„Es reicht nicht aus, zwischen ehrlichen und unehrlichen Nutzern im Bitcoin-Netzwerk zu unterscheiden“, weiß Sebastian Faust. Denn es kann unter Umständen gewinnbringender sein, Transaktionslisten nicht direkt zu veröffentlichen, wenn man ein Rätsel gelöst hat, sondern zunächst abzuwarten, was im Netzwerk passiert. Faust: „Eigentlich muss man Bitcoin mit Konzepten aus der Spieltheorie analysieren, um die Praxis möglichst realitätsgetreu abzubilden.“ Das eines Tages hinzubekommen, ist ein Ziel seiner Gruppe.

Text: jwe, Fotos: rs


1 TRANSAKTIONEN
Lisa überweist Marie dieselben zwei Bitcoins wie Tom.
Marie
Lisa
Tom
2 DAS BITCOIN-NETZWERK
FIRMEN UND PRIVATPERSONEN
Jeder Bitcoin-Nutzer kann sich als Miner betätigen und Transaktionen prüfen.
Ehrliche Miner bewilligen nur die Transaktion, in der Lisa die Bitcoins das erste Mal ausgibt.
Unehrliche Miner könnten theoretisch auch Doppelausgaben bewilligen. Aber das lohnt sich nicht (siehe 4).
3 RÄTSEL
Alle Miner müssen permanent kryptografische Rätsel lösen. Nur wer ein Rätsel löst, kann Transaktionen bewilligen und in der Blockchain veröffentlichen. Das macht Betrügern das Leben schwer (siehe S. 20).
4 BLOCKCHAIN
öffentliche verteilte Datenbank mit allen Bitcoin-Transaktionen
Lisa › Marie
Unehrliche Miner könnten neue Blöcke in einem Seitenarm verstecken. Aber: Nur die längste Kette wird gewertet.
Ehrliche Miner setzen neue Blöcke an der längsten Kette an. Solange sie mehr als 50 Prozent der Rechenleistung im Netzwerk kontrollieren, wächst diese Kette am schnellsten.
Lisa › Tom
LEGENDE
BITCOIN
KRYPTOGRAFISCHE RÄTSEL
RÄTSEL GELÖST
TRANSAKTION GÜLTIG

BITCOIN: ZAHLEN MIT DIGITALER WÄHRUNG

Da virtuelles Geld nicht physisch existiert, lässt es sich theoretisch leicht doppelt ausgeben. Aber schummeln lohnt sich nicht im Bitcoin-Netzwerk.

Grafik: Agentur der RUB, Zalewski

WIE MATHEMATIK PATIENTEN SCHÜTZT

Patientenakten könnten Hinweise enthalten, wie man Krankheiten frühzeitig erkennen kann. Doch wie kann man die gesammelten Daten auswerten, ohne die Privatsphäre zu verletzen? Hier hilft Mathematik.

Patientenakten könnten wichtige Hinweise enthalten, wie man Krankheiten früher erkennen kann.

Selbstständig lernende Computerprogramme können große Datenmengen durchforsten und Regelmäßigkeiten aufspüren. Solche Programme kommen zum Beispiel in modernen Spam-Filtern zum Einsatz: Sie beobachten, welche E-Mails die Benutzer als Spam markieren, und lernen daraus, was Spam-E-Mails ausmacht, ohne dass man ihnen explizit vorgibt, woran sie das erkennen können. Dieses maschinelle Lernen hilft nicht nur, Spam-Filter zu verbessern, sondern generell dort, wo große Datenbestände auf Muster untersucht werden sollen, etwa bei Suchmaschinen, bei automatischer Spracherkennung oder auch bei der Analyse medizinischer Daten. Hier könnten Algorithmen in einem Stapel von Patientenakten Zusammenhänge erkennen und beispielsweise Kriterien finden, Krankheiten frühzeitig zu diagnostizieren.

„Dabei muss jedoch sichergestellt werden, dass die Privatsphäre einzelner Patienten geschützt ist“, warnt Prof. Dr. Hans Simon vom Lehrstuhl Mathematik und Informatik (Abb. 1). Er beschäftigt sich zusammen mit den Doktoranden Francesco Alda und Filipp Valovich mit der Frage, wie empfindliche Daten statistisch ausgewertet werden können, ohne die Anonymität der beteiligten Personen preiszugeben.

Speziell untersuchen die Mathematiker eine Form des maschinellen Lernens, die auf sogenannte Zählanfragen eingeschränkt ist. Das funktioniert wie folgt: Wenn ein Algorithmus zum Beispiel eine Patientendatenbank auswerten soll, ist es ihm nur gestattet, Ja/Nein-Fragen zu stellen und zu zählen, bei wie vielen Patienten die Antwort „Ja“ lautet (Abb. 2). Erlaubte Fragen sind zum Beispiel: Ist die Person Raucher? Ist die Person männlich? Wiegt die Person mehr als 80 Kilogramm? ▸

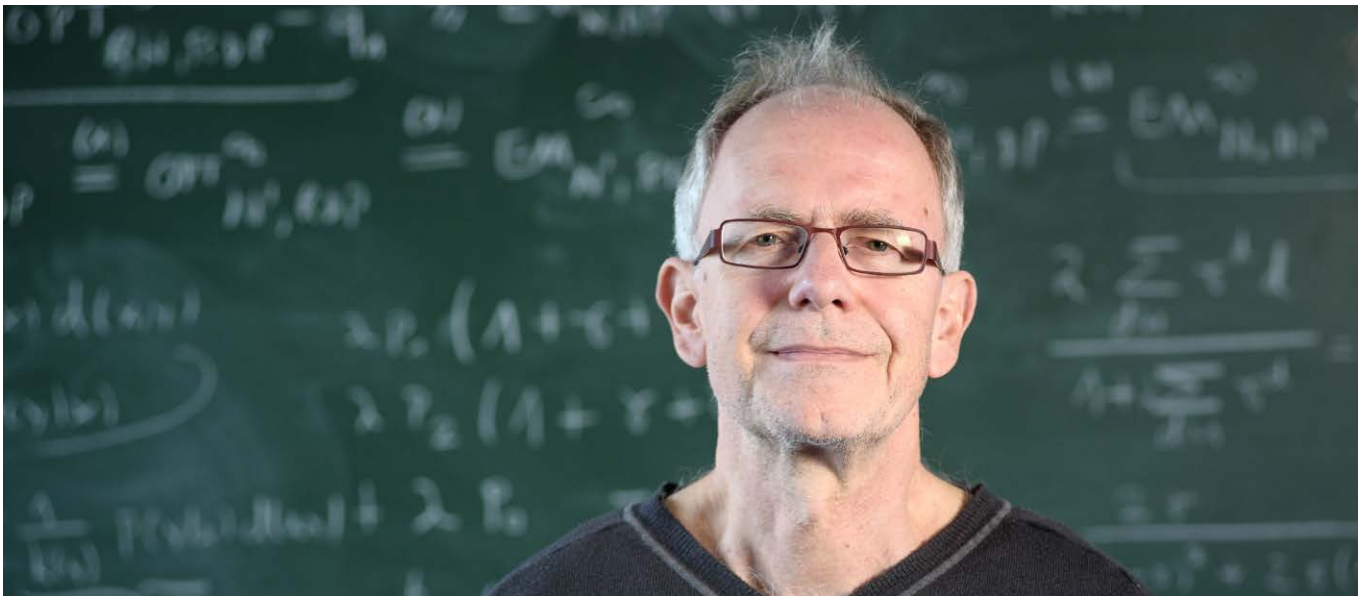


Abb. 1: Hans Simon leitet an der RUB den Lehrstuhl für Mathematik und Informatik.

Schickt ein Lern-Algorithmus diese Fragen an eine Patientendatenbank, erhält er als Antwort drei Zahlen: die Anzahl der Raucher, die Anzahl der Männer und die Anzahl der Patienten, die schwerer als 80 Kilogramm sind. Das Prinzip der Zählanfragen klingt anonym – schließlich ist das Resultat bloß eine statistische Zusammenfassung. Trotzdem ist es möglich, Informationen über einzelne Patienten zu gewinnen. Hans Simon und seine Mitarbeiter untersuchen deshalb Mechanismen wie „Randomized Response Schemes“, die die Privatsphäre der Patienten schützen sollen.

Dabei werden die Patientendaten verrauscht, das heißt, sie werden zufällig verändert. Vereinfacht gesprochen ist es so, als würde bei jedem Patienten gewürfelt und die Augenzahl auf die Werte in der Akte aufaddiert. Das Verfahren verändert die einzelnen Patientendaten heftig und unvorhersehbar, macht sich im Idealfall bei statistischen Zusammenfassungen jedoch nicht stärker bemerkbar als eine ohnehin in den Daten vorhandene statistische Zufallsschwankung. Um dem Idealfall nahe zu kommen, muss das Verrauschen bestimmte Rahmenbedingungen erfüllen. „Unsere Herausforderung ist es, solche Rahmenbedingungen zu finden und klar zu formulieren“, erklärt Hans Simon. „Wir suchen also Bedingungen für das zufällige Verrauschen, die einerseits dafür sorgen, dass die einzelnen Daten so stark verändert werden, dass die Patienten nicht mehr identifiziert werden können, andererseits aber garantieren, dass der veränderte Datenbestand trotzdem ähnliche Antworten an den Lern-Algorithmus zurückliefert wie der ursprüngliche Datenbestand.“

Das ist in einem Satz schnell beschrieben, bedeutet in der Praxis für Mathematiker aber eine kleinteilige, komplexe Gedankenarbeit. Zuerst müssen sie genau definieren, was die Begriffe bedeuten, um die es geht: Was soll es exakt heißen, dass Patienten „anonym“ bleiben? Was soll es exakt heißen, dass die Antworten an den Lern-Algorithmus „ähnlich“ sind? Anschließend suchen sie nach Bedingungen, aus denen sich herleiten lässt, dass das Verrauschen die Patientendaten anonymisiert, aber statistische Zusammenfassungen nicht substanziell verfälscht.

Die Mathematiker um Hans Simon beschäftigen sich bei ihrer Suche mit „Differential Privacy“. Das Konzept geht auf die US-amerikanische Informatikerin Cynthia Dwork zurück und gibt Antwort auf die Frage, was Anonymität streng mathematisch bedeuten kann: Differential Privacy ist ein Maß dafür, wie gut ein einzelner Patient in einer Datenbank identifiziert werden kann. Dazu nimmt man an, man hat eine konkrete Zählanfrage und zwei Datenbanken A und B, die sich nur in einem einzigen Patienten unterscheiden. Das zufällige Verrauschen erfüllt Differential Privacy, wenn es so gut wie egal ist, ob die Datenbank A oder die Datenbank B gefragt wurde; das heißt, wenn die Wahrscheinlichkeit für eine bestimmte Sammelantwort auf die Zählfrage in beiden Fällen ähnlich ist. „Das Gesamtergebnis der Anfrage hängt also nicht so stark von einem einzelnen Patienten ab“, erläutert Hans Simon. Ebenso nutzen er und seine Kollegen exakte Definitionen, um mathematisch genau festzulegen, was es heißt, dass aus den verrauschten Daten ähnliche statistische Schlüsse gezogen werden können wie aus den Originaldaten; man spricht hier von Accuracy.

Hans Simons Team möchte beim Verrauschen der Daten beide Anforderungen erfüllen, das heißt sowohl Differential Privacy als auch Accuracy gewährleisten. Dafür haben die Forscher einen Trick angewandt: Sie haben einen Zusammenhang zu einem anderen Thema in der Mathematik erkannt, zu sogenannten linearen Arrangements. Dorthin haben sie das Problem übersetzt. Die Wissenschaftler stellen sowohl jede einzelne Patientenakte als auch jede erlaubte Zählanfrage als einen Vektor dar, das heißt als einen Pfeil in einem geometrischen Raum. Eine Ja-Antwort liegt vor, wenn die Pfeile von

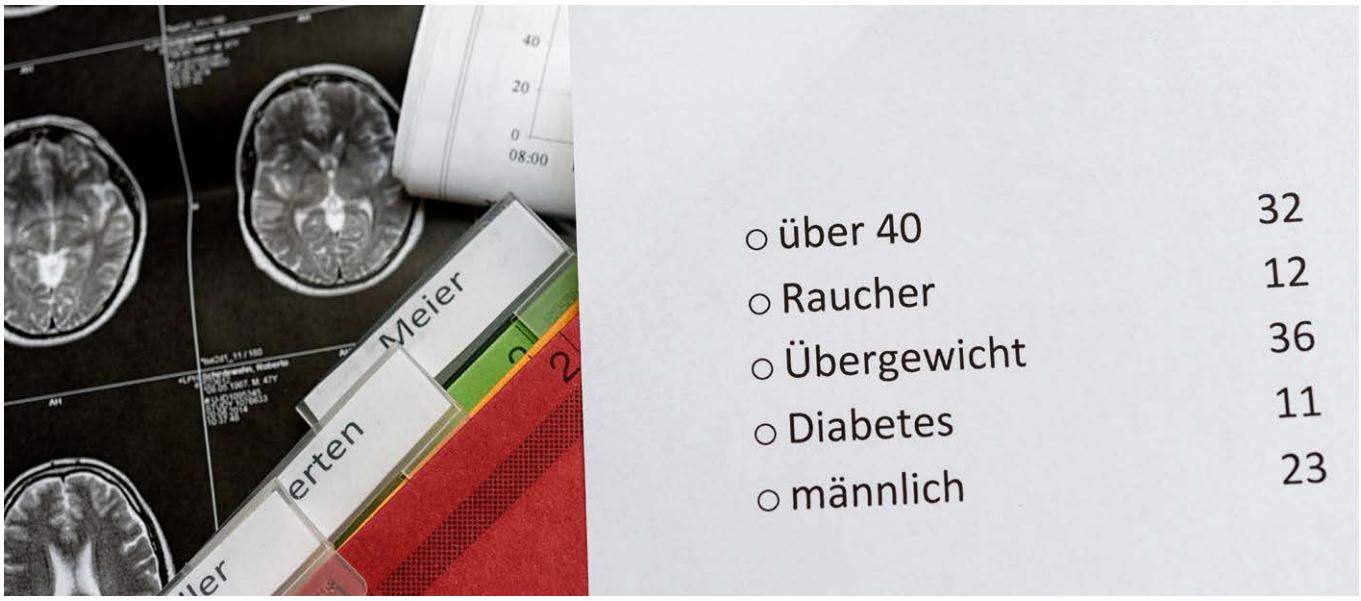


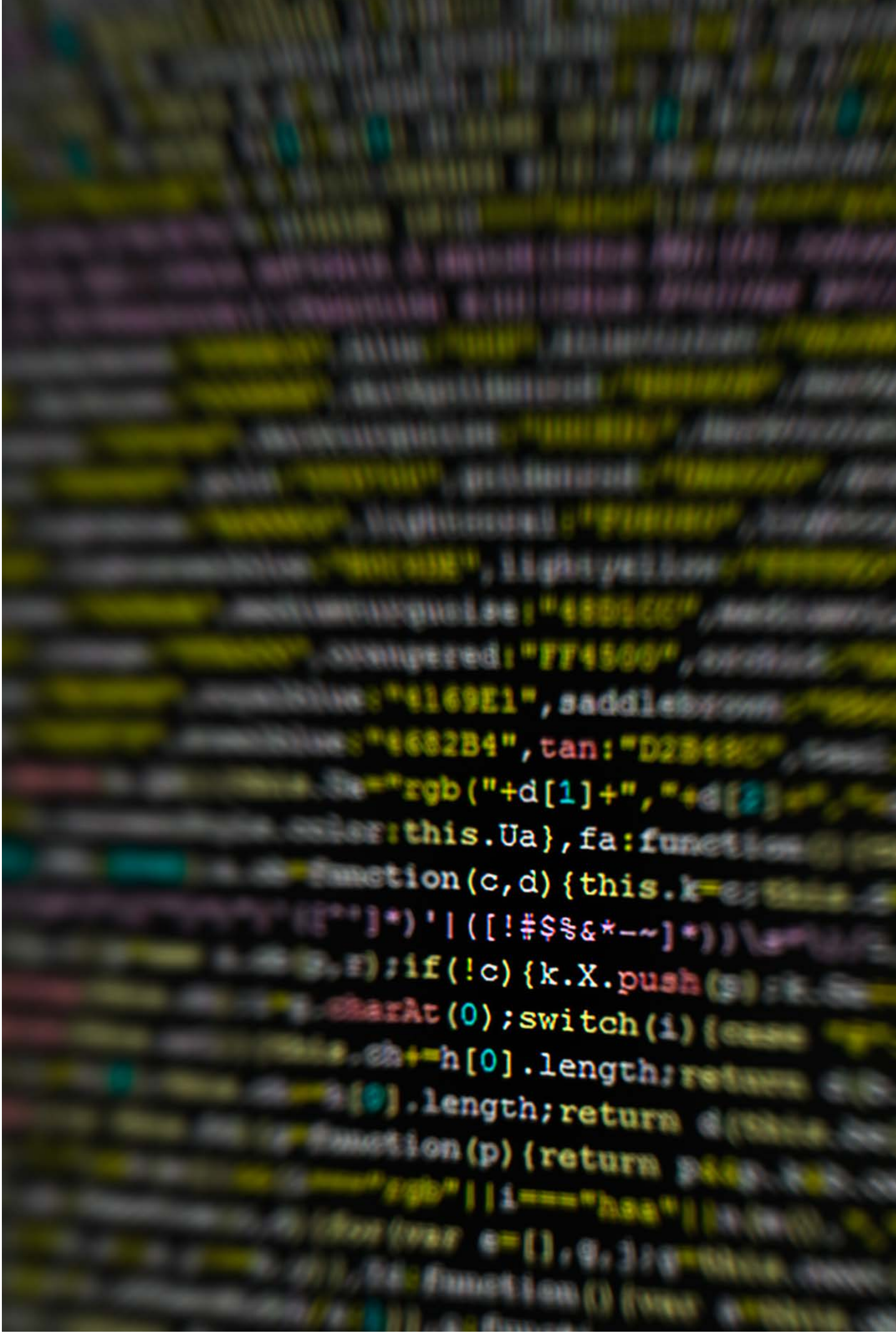
Abb. 2: Patientinnen und Patienten bleiben bei Analysen ihrer Gesundheitsdaten selbst dann nicht vollständig anonym, wenn die Auswertalgorithmen nur Ja/Nein-Fragen stellen, zum Beispiel: Ist die Person Raucher?

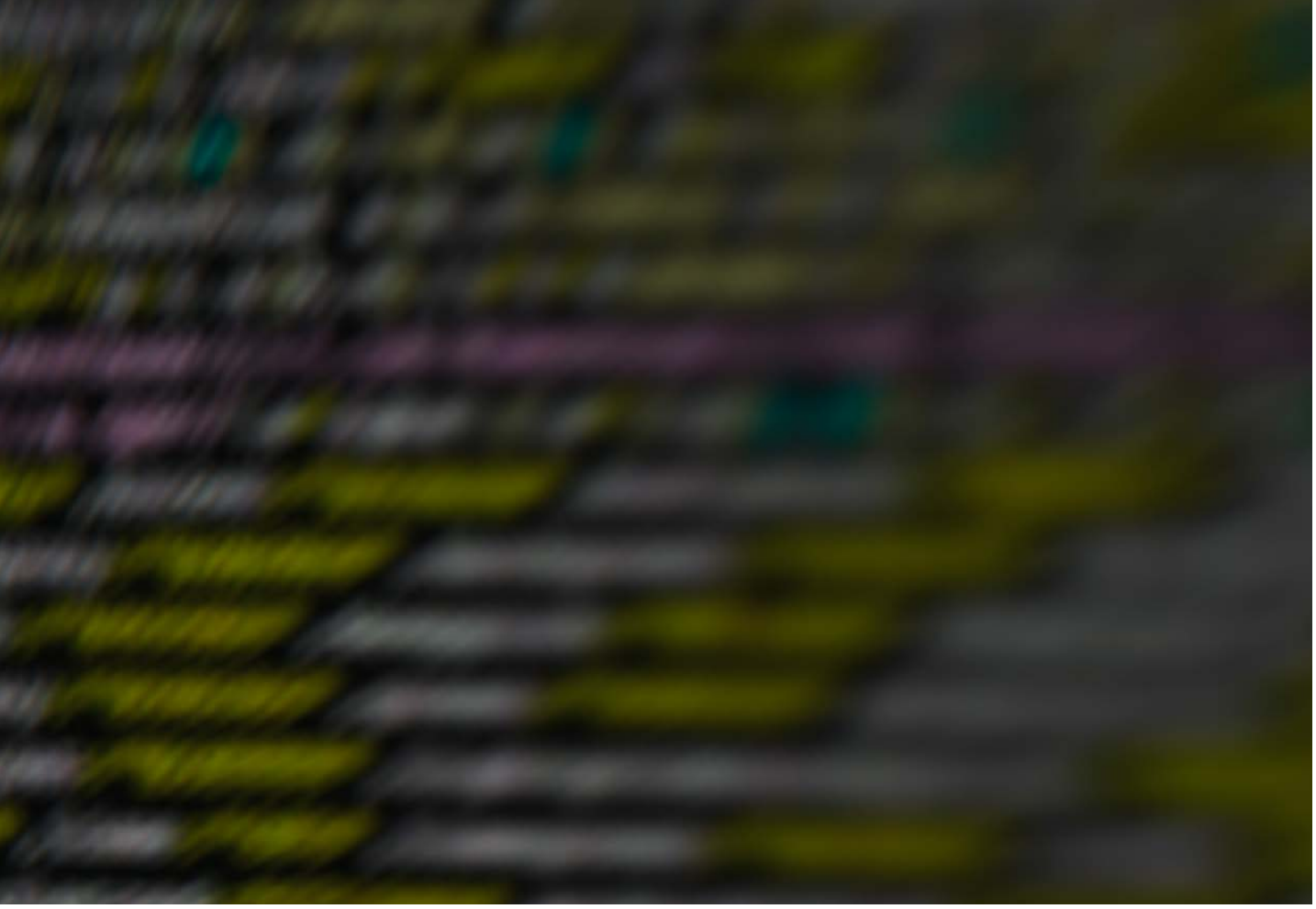
Patientenakte und Zählanfrage einen spitzen Winkel bilden. Eine Nein-Antwort liegt vor, wenn die Pfeile einen stumpfen Winkel bilden. Nun wird das Verrauschen nicht mehr auf den ursprünglichen Patientendaten ausgeführt, sondern auf den ihnen zugeordneten Pfeilen. Hans Simon und sein Team haben bewiesen, dass das Verrauschen mit diesem Verfahren gut funktioniert, das heißt sowohl Differential Privacy als auch Accuracy erfüllt. Die Voraussetzung ist, dass die spitzen Winkel wirklich spitz sind, das heißt deutlich kleiner als 90 Grad, und die stumpfen Winkel wirklich stumpf, also deutlich größer als 90 Grad.

Die Bochumer Mathematiker haben ein erstes Zwischenziel erreicht, wollen ihre Forschungsergebnisse aber noch erweitern. „Das Übersetzen der Patientendaten und Algorithmus-Anfragen in den geometrischen Raum ist eine große Hürde“, bedauert Hans Simon. „Es gibt kein allgemeines Rezept, wie man das anstellen kann. Zudem gibt es Typen von Datenbankanfragen, von denen man weiß, dass sie nicht geeignet geometrisch dargestellt werden können.“

Hans Simon hat eine Vision, die auf eine Idee des US-amerikanischen Forschers Avrim Blum zurückgeht: „Es wäre großartig, wenn sich reale Daten durch synthetische Daten ersetzen ließen, aus denen man keine Informationen mehr über die Patienten gewinnen, aber die gleichen statistischen Schlüsse ziehen kann.“ Man könnte solche synthetischen Daten dann unbeschränkt für die Allgemeinheit zugänglich machen. „Aus vorliegenden Ergebnissen der Forschergemeinde weiß man, dass sich dieses Idealziel nicht erreichen lassen wird“, sagt Hans Simon. Es könnte aber eine Triebfeder sein, die weitere wichtige Ergebnisse im Spannungsfeld zwischen statistischer Datenanalyse und Privatheit hervorbringt.

Text: Aeneas Rooch, Fotos: rs


"rgb("+d[1]+",
this.Ua},fa:
function(c,d){this.
]*)'|([!#$%&*-~]*)
if(!c){k.X.push
At(0);switch(i)
h[0].length;
.length;return
function(p){return
"rgb"||i==="hsa"



SICHERHEITSLÜCKEN IM VERNETZTEN HAUSHALT SCHLIESSEN

Auto, Kühlschrank, Haustechnik – viele Alltagsgegenstände werden in Zukunft online sein. Das eröffnet zahlreiche neue Angriffsziele. Von Bochumer Forschern entwickelte Methoden sollen Schwachstellen in unterschiedlicher Software automatisch erkennen und schließen.

Mit manipulierten Abgaswerten von Dieselfahrzeugen hat Volkswagen monatelang Schlagzeilen gemacht. Emissionstests in den Vereinigten Staaten deckten den Skandal auf. Allerdings muss man keine Schadstoffe messen, um festzustellen, dass es bei dem Autohersteller nicht mit rechten Dingen zugeht. Ein IT-Spezialist aus Hamburg und IT-Sicherheitsexperten aus Bochum analysierten die Software für die Motorsteuerung und konnten so genau nachvollziehen, wie der Konzern bei seinem Betrug vorgegangen ist (Info). Dafür hatten sie noch nicht einmal den Original-Quellcode zur Verfügung, da dieser ein Betriebsgeheimnis des Herstellers ist. Stattdessen lag die Software als Binärcode aus Nullen und Einsen vor – ein Format, das ein Prozessor direkt verwerten kann, aber für Menschen nicht lesbar ist.

Wie man in solch einem Binärcode Auffälligkeiten findet, weiß Prof. Dr. Thorsten Holz vom RUB-Lehrstuhl für Systemsicherheit (Abb. 1). Mit seinem Team entwickelt er Methoden für die automatische Analyse von Software. Das Primärziel der Forscher ist dabei nicht, die Betrügereien von Volkswagen oder anderer Konzerne zu enttarnen. Die IT-Experten spüren Schwachstellen in unterschiedlichen Programmen auf, um das Internet der Dinge sicherer zu machen. ▸

Immer mehr Gegenstände sind mit dem Internet verbunden (Abb. 2); schon bald wird es normal sein, dass nicht nur Drucker, Computer und Telefone online sind, sondern auch Autos, Kühlschränke und vieles mehr. Auf allen vernetzten Geräten läuft Software, die in der Regel Sicherheitslücken aufweist. „Durchschnittlich finden sich in einer gut gepflegten Software ein bis zwei sicherheitskritische Schwachstellen pro 20.000 Zeilen Code“, sagt Thorsten Holz. Das Betriebssystem Windows besteht beispielsweise aus 40 bis 50 Millionen Zeilen, die demnach Tausende von Sicherheitslücken enthalten müssten. Ein Drucker hat immerhin noch mehrere Hunderttausend Zeilen Code.

Mit dem Internet der Dinge dringt die vernetzte Welt in alle Bereiche des Alltags vor – umso wichtiger wird der Schutz vor Angriffen. Aber woher sollen die Sicherheitslösungen für so viele verschiedene Geräte kommen? Eine Herausforderung für IT-Experten ist es, dass die Geräte im Internet der Dinge verschiedene Prozessoren beinhalten. Bisherige Sicherheitslösungen funktionieren meist nur für einen bestimmten Typ. Ideal wäre aber ein einziges Tool, das Schwachstellen in vielen verschiedenen Gegenständen aufdeckt, egal welcher Prozessor eingebaut ist. Das Tool sollte dabei nicht auf den Quellcode der Originalsoftware angewiesen sein. Denn die ist häufig Betriebsgeheimnis des Herstellers.

Für genau solch ein Werkzeug wollen die RUB-Forscher die Basis schaffen. Der Europäische Forschungsrat unterstützt sie dabei im Projekt „Leveraging Binary Analysis to Secure the Internet of Things“, kurz Bastion. Der Clou der Bastion-Methode: Sie braucht keinen Quellcode, sondern nur den Binärcode, der aus jedem Gerät ausgelesen werden kann. Darin soll das Tool automatisch Schwachstellen erkennen, unabhängig davon für welchen Prozessor die Software geschrieben ist.

Geräte benötigen für ihre Aufgaben unterschiedlich komplexe Prozessoren. Elektronische Türschlüssel besitzen zum Beispiel Mikrocontroller, die klein und billig sind und nicht viel Strom verbrauchen. Sie können gerade einmal rund 20 Befehle ausführen, darunter arithmetische Operationen wie Addition und Subtraktion oder Befehle wie „Springe an eine bestimmte Stelle des Codes“. Intel-Prozessoren in Computern hingegen müssen vor allem schnell sein. Sie sind wesentlich komplexer und verstehen rund 500 Befehle, auch arithmetische Operationen und Sprungbefehle. Sie können aber noch viel mehr. Etwa mit einem einzigen Befehl eine Verschlüsselung ausführen, die eigentlich aus hunderten Einzelschritten besteht.

Ein einfacher Mikrocontroller könnte also ein Programm, das auf einem Intel-Prozessor läuft, niemals verstehen. Hinzu kommt, dass die Prozessoren unterschiedliche Sprachen nutzen. Sie arbeiten zwar alle mit dem Binärcode, verarbeiten also Befehle in Form von Nullen und Einsen. Aber ein identischer Befehl – etwa „Addiere zwei Zahlen“ – kann auf einem Mikrocontroller durch eine andere Folge von Nullen und Einsen dargestellt sein als auf einem Intel-Prozessor, obwohl beide das Gleiche meinen. Damit ihre Sicherheitsanalysen unabhängig vom Prozessor sind, übersetzen die Bochumer Forscher die Binärcodes zunächst in eine Zwischensprache.

Abb. 1: Thorsten Holz möchte das Internet der Dinge sicherer machen.

Ein Additionsbefehl eines Mikrocontrollers sieht in der Zwischensprache dann genauso aus wie ein Additionsbefehl eines Intel-Prozessors.

„Das ist Fleißarbeit“, erzählt Holz, denn es gilt, viele verschiedene Instruktionen zu übersetzen. „Unsere Zwischensprache enthält weniger als zwei Dutzend Befehle. Was komplexe Prozessoren in einem einzigen Schritt tun, müssen wir in vielen kleinen Einzelschritten machen.“ Den Verschlüsselungsbefehl eines Intel-Prozessors würden die Wissenschaftler zum Beispiel in eine lange Folge von arithmetischen und logischen Operationen sowie Sprungbefehlen zerlegen.

Ist ein Programm in die Zwischensprache übersetzt, kann Thorsten Holz' Team es automatisch analysieren, um Schwachstellen aufzudecken. Die Forscher suchen nach Programmierfehlern, über die Angreifer die Software unter ihre Kontrolle bringen können (Info 2). Kritisch sind etwa Stellen im Code, an denen eine Variable eigentlich nur eine bestimmte Länge haben darf, aber Angreifer über diese Grenze hinausschreiben können. Oder logische Fehler: Sie können auftreten, wenn das Programm prüft, ob eine Variable einer bestimmten Bedingung entspricht, etwa kleiner, größer oder gleich null ist. Vergisst der Programmierer, eine dieser Bedingungen abzufragen, können Angreifer sich unter Umständen über die Lücke Zugang verschaffen. Haben die Forscher Programmierfehler aufgespürt, untersuchen sie im nächsten Schritt, ob diese sicherheitskritisch sind. Denn nicht jede Lücke hat Folgen in der Praxis. „Manchmal gibt es zwar Programmierfehler in der Software“, erklärt Thorsten Holz, „aber nicht alle Fehler können von einem Angreifer ausgenutzt werden.“

In ihrer Analyse ermitteln die Forscher, unter welchen Bedingungen eine bestimmte Stelle des Codes aufgerufen wird. Dazu verwenden sie Standardverfahren wie die symbolische Ausführung. Sie füttern das zu untersuchende Programm, etwa eine Taschenrechner-App, mit Variablen statt konkreten Zahlen. Ein Beispiel: Statt fünf und acht bekommt die App als Input die Platzhalter Alpha und Beta. Ein Algorithmus berechnet dann, welche Werte die Variablen annehmen müssen, um einen gewissen Punkt im Programmcode zu erreichen. „Das

Abb. 2: Immer mehr Geräte, auch im Haushalt, sind mit dem Internet verbunden. Sie bieten viele neue Angriffsziele.

Ergebnis könnte etwa lauten, dass Alpha zwischen 100 und 500 liegen muss, um an die sicherheitskritische Schwachstelle im Code zu gelangen“, veranschaulicht Holz. Die Softwareanalyse besteht also aus drei Schritten: übersetzen in die Zwischensprache, aufspüren von Programmierfehlern und testen, unter welchen Bedingungen die Schwachstellen relevant werden.

Thorsten Holz möchte aber nicht nur Sicherheitslücken automatisch finden, sondern Nutzerinnen und Nutzer auch vor diesen schützen. Mit seinem Team entwickelt er daher auch Methoden, die sicherheitsrelevante Schwachstellen automatisch schließen. Dazu muss der Code der Originalsoftware verändert werden. Da die Analysen auf Ebene der Zwischensprache erfolgen, fügen die Forscher die neuen Sicherheitslösungen ebenfalls in der Zwischensprache hinzu. Damit der Prozessor diese Instruktionen ausführen kann, muss der Befehl allerdings in seine Binärsprache zurückübersetzt werden. „Es ist, als würde man einen deutschen Text ins Englische übersetzen, eine Passage hinzufügen, und dann zurück ins Deutsche übersetzen“, verdeutlicht Holz. „Beim letzten Übersetzungsschritt hakt es derzeit noch. Aber ich bin optimistisch, dass wir das hinbekommen.“

Dass die Methode im Prinzip funktioniert, haben er und seine Kollegen am Beispiel des Internet Explorers bereits gezeigt. 2015 spürten die IT-Experten eine Sicherheitslücke in dem Programm auf, die sie automatisch schließen konnten. „Natürlich haben wir auch den Hersteller kontaktiert und über die Schwachstellen informiert“, erklärt Holz das übliche Vorgehen. „Microsoft hat die Lücken inzwischen mit einem Update beseitigt.“ Manchmal dauert es allerdings eine Weile, bis Sicherheitslücken auffliegen und Hersteller sie beheben. Genau hier sollen die Methoden helfen, die Thorsten Holz mit seinem Team entwickelt. Sie schützen Anwenderinnen und Anwender auch dann vor Angriffen, wenn Sicherheitslücken noch nicht offiziell geschlossen sind – und zwar egal, ob es sich um einen Internetbrowser, ein Telefon oder einen Kühlschrank handelt.

Derzeit ist das Bochumer Verfahren noch nicht komplett prozessorunabhängig. Aber bis zum Projektende 2020 ist noch jede Menge Zeit, um dieses Ziel zu realisieren. In einer Machbarkeitsstudie haben die Forscher schon gezeigt, wie man prinzipiell Schwachstellen unabhängig von der Prozessor-Architektur in Binärcode finden kann. Außerdem haben sie den Binärcode für drei Prozessortypen namens Intel, ARM und MIPS schon erfolgreich in die Zwischensprache übersetzt. Weitere Typen sollen folgen.

Text: jwe, Fotos: rs

SO MANIPULIERTE VOLKSWAGEN DIE MOTORSTEUERUNG

INFO

Bei einer Abgasuntersuchung durchläuft ein Auto einen bestimmten Prüfzyklus. In diesem ist genau definiert, wie lange der Wagen Gas geben muss und wann wieder abgebremst wird. Die Volkswagen-Software für die Motorsteuerung von Dieselfahrzeugen checkt mehrmals pro Sekunde, ob sich das Auto in einem solchen Prüfzyklus befindet. Falls ja, bleibt das Fahrzeug in einem schadstoffarmen Modus, ansonsten schaltet die Motorsteuerung verbotenerweise in einen Modus mit höheren Emissionen. Dieses Vorgehen konnte das Team um Thorsten Holz mit ihren Analysemethoden im Programmcode genau nachvollziehen. Sie unterstützten den Hamburger IT-Spezialisten Felix Domke, der die Software zuvor auf andere Weise untersucht hatte – und zu dem gleichen Ergebnis gekommen war.

SCHWACHSTELLEN IM DSCHUNGEL DES PROGRAMMCODES AUFSPÜREN

INFO

Für die Schwachstellensuche übersetzen die RUB-Forscher eine Software zunächst in die Zwischensprache und stellen sie anschließend in Form eines Graphen dar: Jedes Programm hat einen Startpunkt. Von dort aus verzweigt sich der Graph wie die Äste eines Baumes. Jeder Ast repräsentiert einen möglichen Weg, den das Programm einschlagen kann. Angenommen, die Forscher stellen eine Taschenrechner-App in Form eines Graphen dar. Würden sie zwei plus vier in die App eingeben, würden sie entlang eines bestimmten Astes durch den Graphen laufen und die Addition durchführen; ein anderer Ast repräsentiert den Fall, dass zwei Zahlen voneinander subtrahiert werden; wieder ein anderer eine Multiplikation. Ein Graph, der die gesamte App abbildet, hat sehr viele Äste und Verzweigungen. Die Graphen-Analyse ermöglicht Holz' Team, das komplexe Geflecht kompakt darzustellen und zu untersuchen.

Im Gespräch

KRYPTOGRAFIE IM ZEITALTER DER QUANTENCOMPUTER

Weltweit arbeiten Forscherinnen und Forscher an der Entwicklung des Quantencomputers. Er würde heutige Computer bei manchen Aufgaben um ein Vielfaches in ihrer Rechenleistung übertreffen und könnte einige aktuelle Verschlüsselungen mühelos knacken. Die Arbeitsgruppe Sichere Hardware von Prof. Dr. Tim Güneysu entwickelt bereits jetzt kryptografische Methoden, die Quantencomputerangriffen standhalten würden.

Herr Güneysu, mit Ihrer Arbeitsgruppe Sichere Hardware entwickeln Sie Verschlüsselungstechniken, die selbst von Quantencomputern nicht gebrochen werden können. Noch gibt es aber keine Quantencomputer.
Das stimmt. Allerdings muss Sicherheit immer an die Zukunft denken. Wir nutzen derzeit zwei Arten von kryptografischen Systemen, die symmetrischen und die asymmetrischen (Abb. 1). Gerade Letztere braucht man, um aufwendige Sicherheitsdienste zu realisieren, die in unglaublich vielen Systemen zum Einsatz kommen. Zum Beispiel wenn man sich bei Amazon einloggt und seine Kreditkarteninformationen übertragen möchte. Dann muss erst einmal ein geheimer Schlüssel zwischen dem Nutzer und Amazon ausgehandelt werden, bevor die verschlüsselte Datenübertragung beginnen kann. So etwas findet millionenfach pro Tag statt.
Aktuell sind hierfür zwei Klassen asymmetrischer Verfahren im Einsatz, bei denen man jetzt bereits weiß, dass sie im Zeitalter des Quantencomputers gebrochen sein würden. Wann es ausreichend leistungsfähige Quantencomputer geben wird, ist eine andere Frage. Aber wir müssen gewappnet sein. Zum

Personenbezogene Daten, die auf der Gesundheitskarte gespeichert sind, wollen wir auch in vielen Jahren noch sicher wissen.

einen müssen alternative Systeme bis zu diesem Zeitpunkt im Markt etabliert werden; zum anderen möchte man auch nicht, dass die verschlüsselten Daten von heute in einigen Jahren mit Quantencomputern nachträglich geknackt werden können.

Wie unterscheiden sich die kryptografischen Verfahren, die vor Quantencomputerangriffen schützen, von den herkömmlichen Verfahren?

Quantencomputer ermöglichen ein völlig neuartiges Rechenmodell (Info). Je nach Einsatzgebiet werden sie eine deutlich höhere Rechenleistung erzielen als die heutigen Computer. Die Verfahren der Post-Quanten-Kryptografie, also jene asymmetrischen kryptografischen Verfahren, die gegen Quantencomputerangriffe sicher sind, setzen auf besonders schwere Probleme der Mathematik, die sich auch mit dem Berechnungsmodell eines Quantencomputers voraussichtlich nicht effizienter lösen lassen (siehe „Schwere mathematische Probleme als Basis für neue Verschlüsselungstechniken“, Seite 36). Leider sind die Instanzen dieser Probleme oft aber nur dann wirklich schwer lösbar, wenn sie mit großen Parametern arbeiten, also mit sehr langen Schlüsseln. In unserem EU-Projekt „Post-Quantum Cryptography“ haben wir in diesem Zusammenhang vier existierende Klassen von kryptografischen Verfahren identifiziert, die sich prinzipiell als Ersatz für heutige Verfahren eignen würden.

Wie groß ist denn der Unterschied in der Länge?

Üblich ist heutzutage eine Länge zwischen 128 Bit und 4.096 Bit für die Schlüsselparameter gängiger Verfahren. Anders ausgedrückt entsprechen 128 Bit dabei 16 Zeichen; das könnte man sich fast sogar noch im Kopf merken. Entsprechend gut lassen sich diese Schlüssellängen auch auf kleinsten Geräten integrieren. Bei den hochsicheren Verfahren der Post-Quanten-Kryptografie liegen die Schlüsselgrößen im Bereich einiger hundert Kilobyte bis Megabyte, also bei einer Million Zeichen und mehr. Hier ist es wiederum nicht trivial, mit solch langen Schlüsseln zu arbeiten, geschweige denn, sie sich zu merken. ▸

Die Quantencomputer würden sicher kein Problem damit haben, lange Schlüssel zu verarbeiten oder zu speichern.

Ja, aber die Quantencomputer von morgen sind gar nicht das Problem, sondern die Kleinstgeräte von heute. Überall steckt bereits Kryptografie drin, in Bankkarten, Gesundheitskarten, in elektronischen Türschlössern. In Zukunft werden solche Geräte wahrscheinlich so leistungsfähig sein wie unsere Smartphones heute. Aber derzeit sind sie das nicht, und dennoch müssen wir uns und unsere Daten vor den Angriffen von morgen schützen. Dabei sind Gesundheitsdaten üblicherweise durchaus langzeitkritisch. Wenn jemand heute in der Lage ist, solche Daten abzufangen und zwischenzuspeichern, soll er sie auch in 15 Jahren mit dem Quantencomputer nicht erfolgreich entschlüsseln können. Von genau diesem Problem betroffen sind alle technischen Geräte mit hoher Lebensdauer. Satelliten zum Beispiel, die man einmal in die Umlaufbahn schießt und die dann Jahrzehnte sicher kommunizieren müssen.

Sie arbeiten an einer Lösung für genau dieses Problem: Kleinstgeräte vor Quantencomputerangriffen schützen.

Wir untersuchen alternative asymmetrische Verschlüsselungsverfahren, die auch im Zeitalter des Quantencomputers noch Sicherheit gewährleisten. Dabei ist es ein primäres Ziel, alternative Techniken zu entwickeln, um die großen Schlüsselparameter in den Griff zu bekommen, sodass wir sie selbst in Kleinstgeräte implementieren können.

Wann sind die Verfahren einsatzbereit?

Aus dem Bauch heraus würde ich schätzen in etwa fünf bis zehn Jahren. Es muss eine genügend große Akzeptanz und ein Vertrauen in die jeweiligen Verfahren gegeben sein, bis diese Einzug in offizielle oder industrielle Standards halten können. Erfahrungsgemäß vergehen für diesen Prozess einige Jahre. Das ist in der Regel die Voraussetzung, bevor die neuen Verfahren in den ersten Produkten tatsächlich auch zum Einsatz kommen.

Das Interview führte Julia Weiler. Foto: rs

QUANTENCOMPUTER

INFO

Quantencomputer erzielen eine deutlich höhere Rechenleistung als herkömmliche Computer, da sie nicht auf den Regeln der klassischen Digitaltechnik basieren, sondern auf denen der Quantenmechanik. Die kleinste Informationseinheit, mit der ein klassischer PC arbeitet, ist das Bit, das die beiden Zustände 0 und 1 annehmen kann. Zu einem bestimmten Zeitpunkt kann es sich entweder in dem Zustand 0 oder dem Zustand 1 befinden. Quantenbits, kurz Qubits genannt, können hingegen beide Zustände gleichzeitig annehmen; dem liegt der physikalische Effekt der Superposition zugrunde.

Ein herkömmlicher Computer, der mit zwei Bits arbeitet, kann vier Bit-Konfigurationen speichern: 00, 01, 10 und 11, wobei jeweils die erste Ziffer in den vier Ziffernpaaren den Zustand des ersten Bits wiedergibt und die zweite Ziffer den Zustand des zweiten Bits. Zu jedem Zeitpunkt kann sich der klassische Zwei-Bit-Computer nur in einem dieser vier Zustände befinden. Ein Quantencomputer mit zwei Bits könnte die gleichen Bit-Konfigurationen speichern – allerdings alle vier Konfigurationen gleichzeitig. Fügt man einem solchen System weitere Bits hinzu, steigt die Rechenleistung exponentiell an. Quantencomputer wären allerdings nicht in jeder Hinsicht ein Ersatz für herkömmliche Rechner. Stattdessen wären sie nur für spezielle Aufgaben geeignet. Eine davon wäre das Brechen der heutzutage verwendeten asymmetrischen Kryptografie.

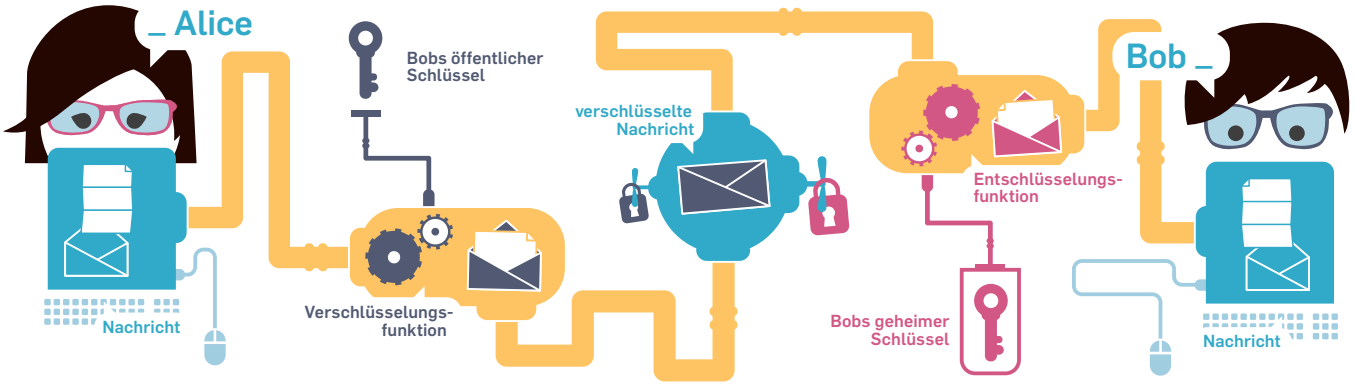


Abb. 1: Die asymmetrische Kryptografie verwendet Schlüsselpaare aus zwei Bestandteilen. Der eine Teil des Schlüssels ist öffentlich, der andere geheim. Beide Schlüssel stehen in enger mathematischer Beziehung; es ist jedoch aufgrund eines schweren mathematischen Problems unmöglich, aus dem öffentlichen Teil den privaten Schlüssel zu rekonstruieren. Eine Nachricht, die Alice an Bob sendet, kann mit Bobs öffentlichem Schlüssel verschlüsselt werden. Um sie zu entschlüsseln, bedarf es jedoch zwingend Bobs privatem Schlüssel, den aber nur er kennt. (Grafik: Agentur der RUB, Zalewski)

VERSCHLÜSSELUNGSVERFAHREN FÜR KLEINSTGERÄTE

Es ist eine Herausforderung, sichere Verschlüsselungsverfahren, die vor Quantencomputerangriffen schützen würden, in Kleinstgeräte zu implementieren. Aufgrund des Platzangebots und des hohen Kostendrucks sind nur leistungsschwache Prozessoren und kleine Speicher verfügbar. RUB-Ingenieure entwickeln Lösungen für dieses Problem.

Kryptografische Verfahren lassen sich in zwei Arten unterteilen, die symmetrischen und asymmetrischen Verfahren, wobei Letztere aufgrund der zugrunde liegenden Strukturen deutlich komplexer sind. Bei symmetrischen Verfahren nutzen Sender und Empfänger den gleichen Schlüssel, um eine Nachricht zu verschlüsseln und anschließend wieder zu entschlüsseln. Bei asymmetrischen Verfahren verwenden Sender und Empfänger hingegen unterschiedliche Schlüssel (siehe Grafik Seite 34), die über einen mathematischen Algorithmus miteinander zusammenhängen. Asymmetrische Verschlüsselungsverfahren werden für viele Anwendungen mit erweiterten Sicherheitsanforderungen benötigt, zum Beispiel zum Erstellen digitaler Signaturen.

Die asymmetrischen Verfahren, die heute im Einsatz sind, wären nicht mehr sicher, wenn es Quantencomputer gäbe (siehe „Kryptografie im Zeitalter der Quantencomputer“, Seite 32). Im EU-Projekt „Post-Quantum Cryptography“ suchen Forscherinnen und Forscher daher nach neuen kryptografischen Lösungen. Vier Klassen von mathematischen Verfahren kommen in Frage: die codierungsbasierte Kryptografie, die gitterbasierte Kryptografie sowie die Kryptografie auf Basis multivariater quadratischer Gleichungssysteme oder Hashfunktionen.

Das Team um Prof. Dr. Tim Güneysu (Abb. 1) hat dafür in enger Kooperation mit dem Lehrstuhl für Eingebettete Sicherheit zunächst vielversprechende Verfahren identifiziert und untersucht, wie sich diese in Kleinstgeräte, beispielsweise Smartcards, implementieren lassen. „Die hashbasierte Kryptografie haben wir bei unserer Betrachtung bislang etwas ausgeklammert, da sie bereits sehr gut untersucht ist“, sagt Güneysu. Auch die Kryptografie über multivariate quadratische Gleichungssysteme steht nicht im Fokus. Denn: „Bei einigen dieser Systeme ist die Sicherheitslage nicht klar. Daher müssen wir ihre Akzeptanz für die Praxis als eher schwierig bewerten“, erzählt Güneysu. Viele der multivariaten quadratischen Verfahren wurden ebenso schnell vorgestellt, wie sie wieder gebrochen wurden. Es lohne sich also nur bedingt, viel Arbeit zu investieren, um Vertreter dieser Klasse für Kleinstgeräte zu optimieren.

Als vielversprechend bezeichnet der IT-Sicherheitsexperte die gitter- und codierungsbasierte Kryptografie. Diese Verfahren haben nicht nur das Potenzial, vor Quantencomputerangriffen zu schützen, sondern das Team konnte auch zeigen, dass sie sich in Kleinstgeräte implementieren lassen. Die Herausforderung: Für die neuen Verfahren sind zum Teil komplizierte Algorithmen und große Schlüssel erforderlich, die die Systemkosten deutlich erhöhen – ein großes Problem, wenn die Technik in kleinen, günstigen Rechensystemen zum Einsatz kommen soll.

Abb. 1: Tim Güneysu entwickelt effiziente Verschlüsselungsalgorithmen für kleine Geräte.

Um das Problem in den Griff zu bekommen, nutzten die Forscher insbesondere alternative Repräsentationen der kryptografischen Verfahren, die zum Beispiel Strukturen in den Codes einführen, um damit die Schlüsselgröße reduzieren zu können. Sie optimierten auch die Algorithmen, indem sie sie an die Zielplattform anpassten. Je nach Verfahren konnten die Ingenieure dabei komplexe Schritte mit anderen Berechnungen zusammenfassen oder sogar gänzlich vermeiden, ohne die Sicherheit des Verfahrens zu mindern. Auf diesem Weg zeigte das Bochumer Team, dass Kleinstgeräte mit den heute verfügbaren oft leistungsschwachen Prozessoren selbst im Zeitalter des Quantencomputers Sicherheit bieten können.

Text: jwe, Foto: rs

SCHWERE MATHEMATISCHE PROBLEME ALS BASIS FÜR NEUE VERSCHLÜSSELUNGS-TECHNIKEN

IT-Sicherheitsexperten träumen von unangreifbaren Verschlüsselungsverfahren. Vision oder Fantasterei?

Der Start in den Urlaub beginnt für viele Menschen mit einer Herausforderung: Wie sollen all die Sachen in den Koffer, die Tasche oder den Rucksack passen? Mathematisch gesehen ist es tatsächlich nicht trivial, einen Algorithmus zu finden, der einen Rucksack so vollpackt, dass die Gegenstände darin zusammengenommen einen möglichst hohen Nutzen erfüllen.

„Die Entscheidung, eine Zahnbürste mitzunehmen, fällt sicher leicht“, sagt Prof. Dr. Eike Kiltz vom Lehrstuhl für Kryptographie. „Sie ist klein und hat einen hohen Nutzen. Aber was ist mit dem Föhn? Nehme ich den auch mit?“ Hinter dem Rucksackbeispiel steckt ein schweres mathematisches Problem, für das Wissenschaftler seit über hundert Jahren keine effiziente Lösung gefunden haben. Allerdings wäre der Rucksack in ihrer Variante des Problems bedeutend größer als im wahren Leben.

Eike Kiltz beschäftigt sich mit genau solchen schweren Problemen der Mathematik. Basierend auf ihnen entwickelt er neue Verschlüsselungs- und Authentifizierungsverfahren, die quasi nicht zu knacken sind. „Wenn jemand es schaffen würde, die Verfahren zu brechen, könnte er auch ein mathematisches Problem lösen, an dem die schlausten Köpfe der Welt seit 100 oder 200 Jahren arbeiten“, vergleicht Kiltz. Mit diesem Ansatz wählt der Wissenschaftler eine ganz andere Herangehensweise als üblich. Normalerweise werden neue kryptografische Verfahren nach dem Ad-hoc-Prinzip konzipiert. Kiltz erklärt: „Jemand denkt sich ein Verfahren aus, dann versuchen andere, es zu brechen. Schaffen sie es nicht, heißt es, dass es sicher ist.“ Die Bochumer Mathematiker basieren ihre Sicherheitsalgorithmen stattdessen auf Probleme, die schon seit ein paar hundert Jahren ungelöst sind. Die Algorithmen gestalten sie dabei so effizient, dass sie sich in Kleinstgeräte implementieren lassen, zum Beispiel in einen elektronischen Garagentoröffner. „Man hat lange gedacht, dass das nicht geht, weil die Chips in diesen Geräten nicht leistungsstark genug sind“, so Kiltz. 2011 veröffentlichte seine Gruppe jedoch ein Prototypverfahren, das genau das konnte.

Nun arbeiten die Forscher daran, die Verfahren noch effizienter und für neue kryptografische Fragestellungen nutzbar zu machen. Großes Potenzial räumen sie dabei der sogenannten gitterbasierten Kryptografie ein. Sie fußt auf folgendem schweren mathematischen Problem: Stellen wir uns ein Gitter vor (Abb. 1), das an einer Stelle einen Nullpunkt besitzt. Überall dort, wo sich zwei Linien kreuzen, liegen weitere Punkte, die wir Kreuzungspunkte nennen. Frage: Welcher Kreuzungspunkt liegt am nächsten beim Nullpunkt? Für ein zweidimensionales Gitter ist dieses Problem leicht zu lösen; auch in einem dreidimensionalen Gitter könnten wir die Antwort relativ schnell finden. Aber je mehr Dimensionen hinzukommen, desto schwieriger wird die Aufgabe. Mit rund 500 Dimensionen lässt sich das Problem nicht mehr effizient lösen.

Je nachdem wie man die Parameter wählt, fällt das Gitterproblem in die Klasse der sogenannten NP-vollständigen Probleme. Diese umfasst die schwersten Probleme der Mathematik, zu denen auch das oben beschriebene Rucksackproblem gehört sowie eine Vielzahl weiterer Vertreter. Sie wären eine ideale Grundlage für möglichst sichere neue Verschlüsselungstechniken.

Für ihre Arbeit wählen die Mathematiker jedoch eine leicht vereinfachte Version des Gitterproblems. Die Aufgabe lautet dann nicht: Finde denjenigen Kreuzungspunkt im Gitter, der am nächsten zum Nullpunkt liegt. Sondern: Finde einen beliebigen Kreuzungspunkt, der in einem engen Radius um den Nullpunkt liegt. Die Wissenschaftler testen dabei verschiedene Parameter, die das Gitterproblem ein wenig leichter oder schwerer machen, und versuchen, darauf basierend einen kryptografischen Algorithmus zu erarbeiten, der sich auch auf kleinen Geräten implementieren lassen würde.

Gitterbasierte Verfahren zur Authentifizierung haben die RUB-Forscher schon relativ weit entwickelt. „Wir sind fast im Endstadium“, fasst Eike Kiltz zusammen. Authentifizierungsprotokolle werden immer dann gebraucht, wenn ein Objekt seine Identität beweisen muss, zum Beispiel der elektronische Garagenöffner. Schließlich muss sichergestellt sein, dass ein bestimmter Öffner nur das zugehörige Tor entriegelt. Im Protokoll könnte das so funktionieren: Der Öffner authentifiziert sich beim Garagentor, indem er beweist, dass er ein internes Geheimnis kennt, zum Beispiel einen Kreuzungspunkt nahe dem Nullpunkt im Gitter. ▸

Einen Rucksack so zu packen, dass der Inhalt einen möglichst hohen Nutzen erfüllt, ist mathematisch gesehen nicht trivial – zumindest bei einem sehr großen Rucksack. Solche Probleme können die Basis für Verschlüsselungstechniken sein.

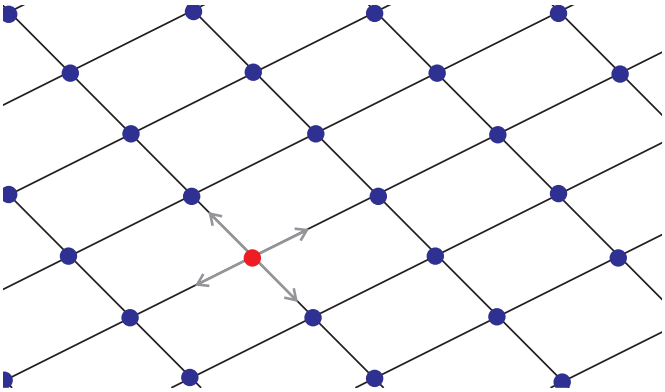
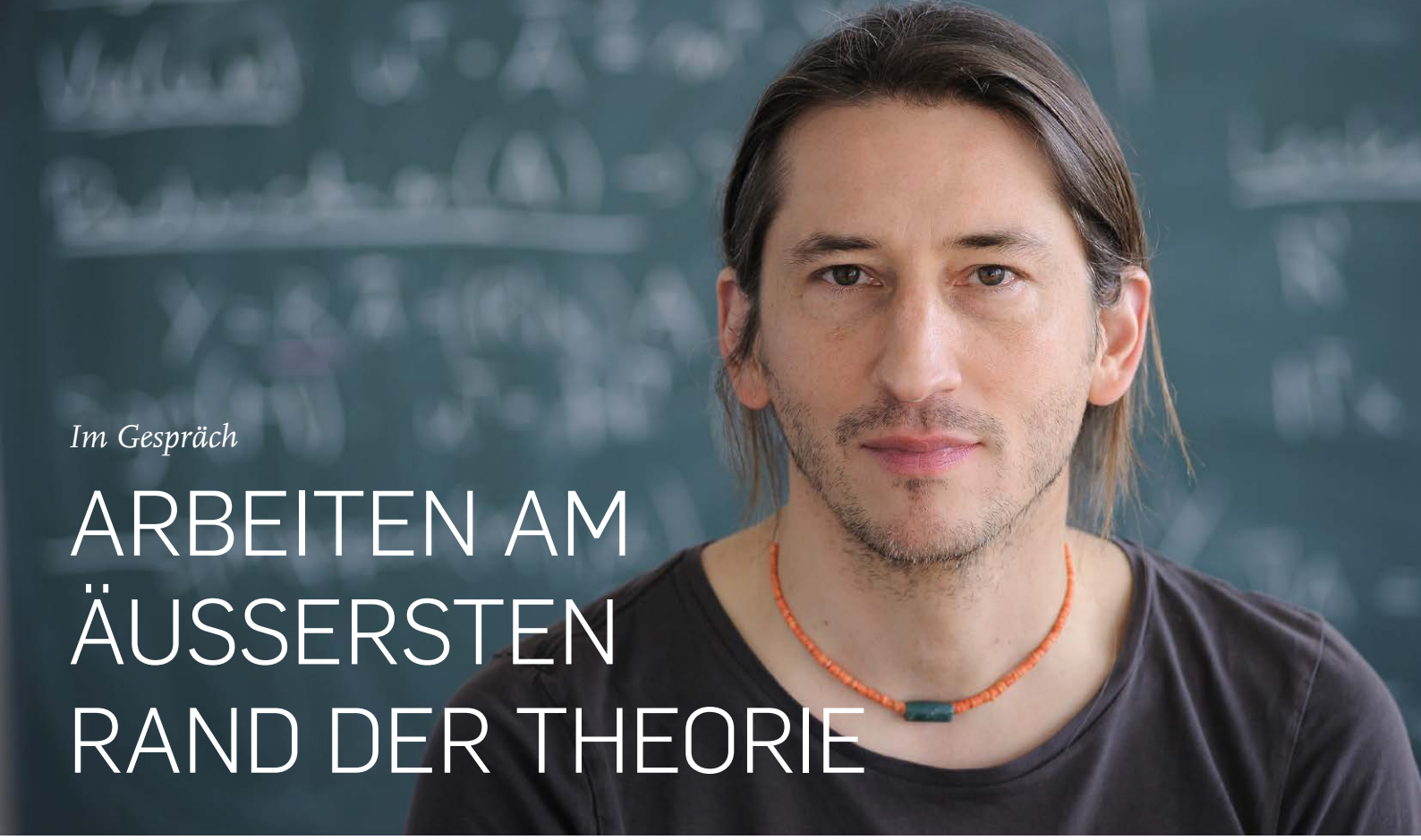


Abb. 1: Das Gitterproblem: Welcher der blauen Punkte liegt am nächsten an dem rot markierten Nullpunkt des Gitters? Bei einem 500-dimensionalen Gitter ist dieses Problem nicht mehr effizient zu lösen.

Kryptografische Protokolle sind aber nicht nur für die Authentifizierung nötig; auch Verschlüsselungen sind im Alltag ständig im Einsatz. Wenn zum Beispiel zwei Personen eine geheime Botschaft über das Internet austauschen wollen oder eine Smartcard mit dem Kartenlesegerät kommunizieren möchte, muss die Nachricht verschlüsselt sein, damit Dritte sie nicht mitlesen können. Für diesen Zweck könnten gitterbasierte Verfahren ebenfalls nützlich sein. Allerdings sind die darauf basierenden Verschlüsselungsprotokolle derzeit noch nicht effizient genug, um sie auf kleinen Geräten zu implementieren. Ein paar Jahre Arbeit müssten sie noch investieren, schätzt Eike Kiltz.

Mit einer eierlegenden Wollmilchsau vergleicht der Mathematiker die gitterbasierten Verfahren, weil sie so vielfältig einsetzbar sind. Sie taugen sowohl zur Verschlüsselung als auch zur Authentifizierung, funktionieren auf kleinen Geräten und würden sogar vor Angriffen durch Quantencomputer schützen (siehe „Kryptografie im Zeitalter der Quantencomputer“, Seite 32), falls es diese eines Tages gäbe. Neben ihrer anwendungsorientierten Arbeit betreiben die RUB-Mathematiker auch Grundlagenforschung. Sie versuchen, die Gitter mathematisch zu verstehen. Was macht das Gitterproblem so einzigartig schwer, dass alle bisherigen Techniken bei der Lösung versagen? Das ist eine der Fragen, die die Forscher umtreibt. Die Erkenntnisse könnten eines Tages in die anwendungsorientierte Arbeit einfließen.

Text: jwe, Foto: rs



Im Gespräch

ARBEITEN AM ÄUSSERSTEN RAND DER THEORIE

Eike Kiltz beschäftigt sich mit besonders schweren Problemen der Mathematik – theoretischer und abstrakter kann Forschung kaum sein. Ein Einblick in seinen Arbeitsalltag.

Prof. Kiltz, Sie entwickeln neue kryptografische Verfahren basierend auf besonders schweren Problemen der Mathematik. Braucht man dazu nur Papier und Bleistift oder simulieren Sie auch am Computer?
Wir simulieren nichts. Es kommt zwar vor, dass mathematisch arbeitende Gruppen auch Computersimulationen nutzen oder Dinge in der Praxis umsetzen. Aber meine Gruppe arbeitet am äußersten theoretischen Rand; theoretischer kann es nicht mehr werden. Wir sitzen hier mit Papier und Bleistift und denken nach.

Der Computer kommt bei Ihnen also gar nicht zum Einsatz.
Nur wenn ich eine E-Mail schreiben will oder ein Textbearbeitungsprogramm brauche. Oder wenn ich ein Algebra-Programm anschmeiße, um fünf mal sieben auszurechnen oder ein Polynom zu faktorisieren; also etwas Triviales, wofür ich zu faul bin, das im Kopf zu machen.

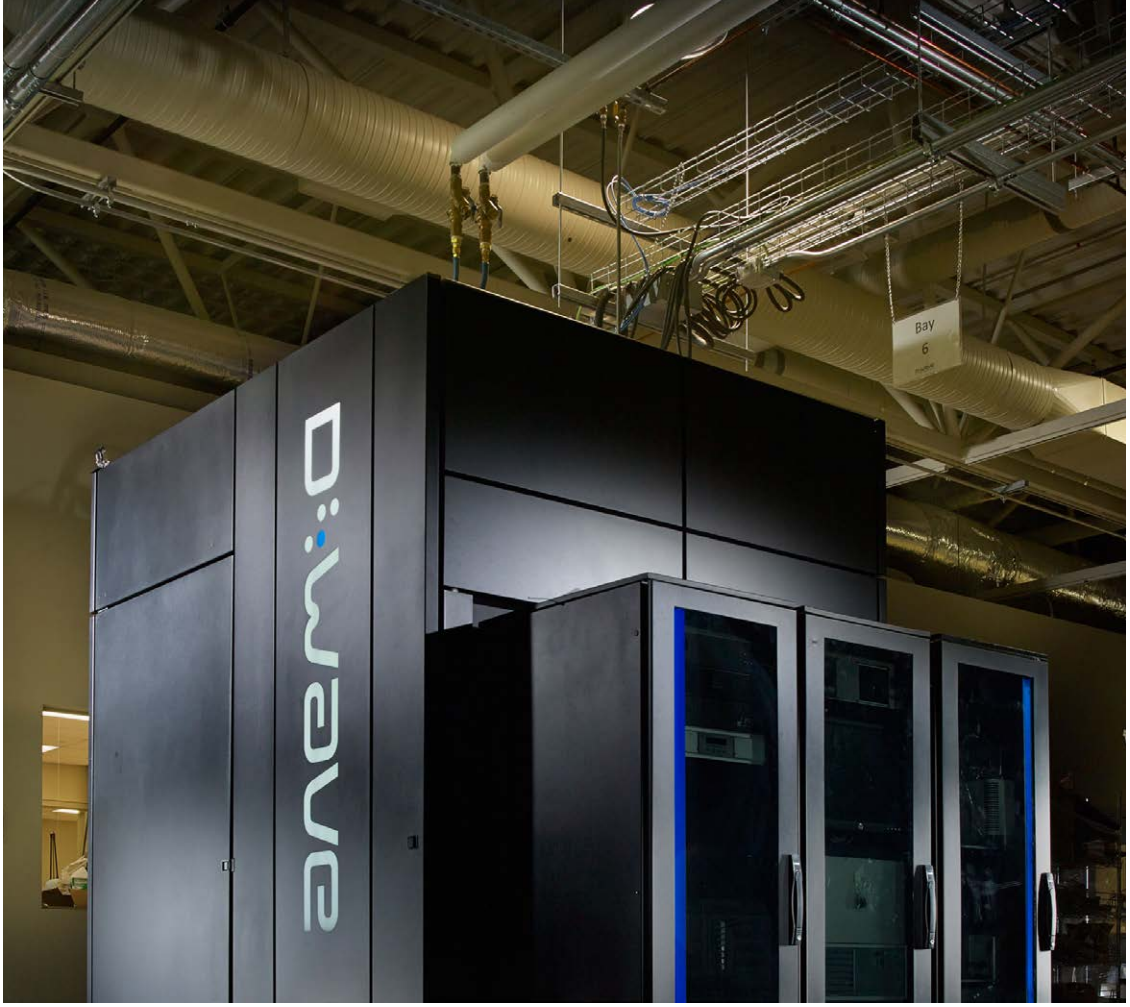
Das klingt, als würden Sie viel alleine arbeiten – oder denkt man auch gemeinsam nach?
Das hängt von der einzelnen Person ab. Ich persönlich finde es besser, wenn ich auch mal die Zeit habe, alleine nachdenken zu können. Andere Leute suchen den Dialog. Teilweise ist unser Fach also schon kommunikativ. Aber manchmal muss man sich einfach für ein paar Stunden oder sogar Tage einschließen und ein Problem lösen.

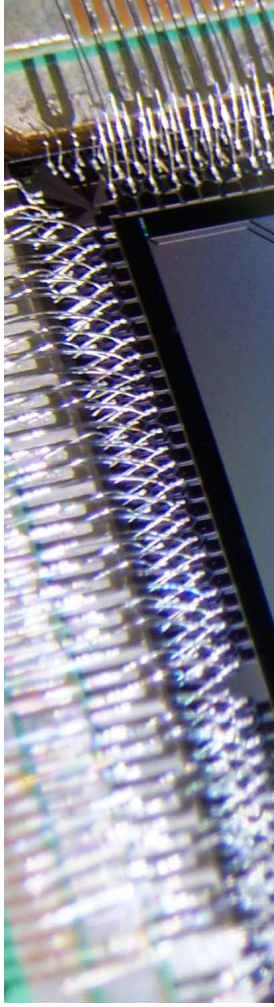
In vielen Disziplinen müssen die Ergebnisse interpretiert werden. Wie sieht es bei dem aus, was Sie letztendlich auf den Zettel schreiben?
Am Ende schreiben wir ein Theorem auf, das sagt, aus A folgt B. Wenn der Beweis korrekt geführt ist, gibt es daran nichts mehr zu rütteln. Dann stimmt das. Das ist das Schöne an der Mathematik – das, was ich daran so sehr liebe.

Heißt das, dass alle Algorithmen, die Sie entwickeln, in der Praxis unangreifbar sind? Weil Sie eindeutig bewiesen haben, dass sie sicher sind?
Es ist mir schon passiert, dass ich ein neues kryptografisches Schema erfunden habe, das jemand gebrochen hat. Obwohl ich bewiesen hatte, dass es sicher ist. Was ist da passiert? In dem Beweis war ich von bestimmten Voraussetzungen ausgegangen, an die sich der Angreifer nicht gehalten hat. Beim nächsten Mal müsste man das Modell also erweitern und diese Bedingungen mit in den Beweis einbeziehen.

Eine so abstrakte, theoretische Arbeit ist sicher nicht jedermanns Sache. Wie kam es, dass Sie sich dafür entschieden haben?
In Mathe war ich schon in der Schule ganz gut. In anderen Sachen eben nicht. Ich wäre gern Fußballprofi geworden, aber dafür hat es leider nicht gereicht. Ganz pragmatisch habe ich also das gemacht, was ich gut konnte. Und jetzt bin ich hier. Bereut habe ich es bislang noch nicht.

Das Interview führte Julia Weiler. Foto: rs





HARTE NUSS FÜR DEN QUANTENCOMPUTER

Ein Quantencomputer ist bislang nur Theorie. Trotzdem können IT-Experten jetzt schon bestimmen, wie leicht er gängige Verschlüsselungen knacken könnte. Mit einem Trick aus der Logik.

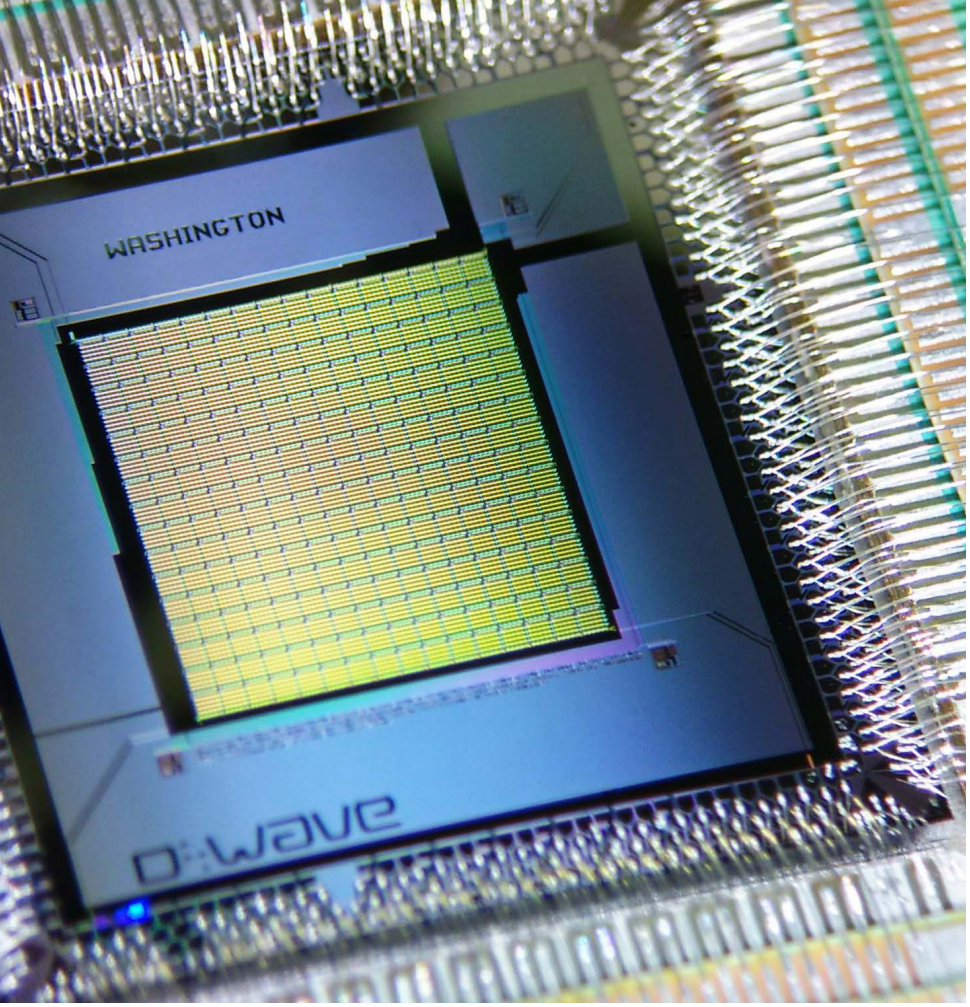
Auf der Suche nach Verschlüsselungsverfahren, die selbst von einem leistungsstarken Quantencomputer nicht schnell geknackt werden können, befasst sich Prof. Dr. Alexander May (Abb. 1) mit sogenannten schweren mathematischen Problemen. Es handelt sich um Berechnungen, für die es noch keinen effizienten Algorithmus gibt, das heißt, für die ein Computer bei umfangreichen Daten sehr lange braucht. Eine große Zahl in ihre Primfaktoren zu zerlegen, ist beispielsweise ein solches Problem.

Auf den ersten Blick haben die schweren Probleme nicht unbedingt etwas mit Verschlüsselungsverfahren zu tun. Aber IT-Wissenschaftler nutzen sie als Hilfsmittel: Sie stellen zwischen einer bestimmten Verschlüsselungsmethode und einem Problem einen Zusammenhang her. So können sie herausfinden, wie schwer das Verfahren zu brechen ist.

In der theoretischen Informatik interessieren sich Wissenschaftler dafür, wie viele Schritte ein Algorithmus für eine Berechnung benötigt. Die exakte Zahl können sie in der Regel nicht ermitteln, aber sie können abschätzen, wie viele Schritte von der Größenordnung her höchstens gebraucht werden – gewissermaßen ob es eher 10, 100 oder 1.000 sind.

„Wir verknüpfen nun die Anzahl der Rechenschritte, die ein Algorithmus zum Lösen eines schweren Problems braucht, mit der Anzahl der Rechenschritte, die zum Knacken eines Codes nötig wären“, erklärt Alexander May, Professor für Kryptologie und IT-Sicherheit an der Ruhr-Universität Bochum. „So können wir etwas darüber herausfinden, wie schwer der Code zu brechen ist.“

Seine Kollegen und er nehmen dazu an, es gäbe einen Algorithmus, der eine Verschlüsselung in einer bestimmten



Die Firma D-Wave brachte 2010 nach eigenen Angaben den ersten Quantencomputer auf den Markt. Kritiker bezweifeln allerdings, dass der Rechner wirklich mit Quanteneffekten arbeitet und die enorme Rechenpower erzielt, die mit einem richtigen Quantencomputer möglich wäre. (Fotos: Courtesy of D-Wave Systems Inc.)

Zeit T knackt, zum Beispiel in 2^{80} Schritten – etwas mehr als eine Quadrillion, eine Zahl mit 25 Stellen. Wie genau dieser Algorithmus funktionieren könnte, ist für die Wissenschaftler nicht von Belang; sie nehmen lediglich an, dass er existiert. „Der Algorithmus ist eine Blackbox", erläutert May. „Wir arbeiten nur mit der Annahme, dass es ihn gibt und dass er die Verschlüsselung in der angenommenen Zeit bricht." Mithilfe logischer Argumente leiten er und seine Mitarbeiter dann daraus ab, wie lange das Lösen eines schweren Problems dauert. „Üblicherweise ist das ein Vielfaches der Zeit T, die zum Brechen der Verschlüsselung benötigt wird, also $c \cdot T$", so May. „Wir versuchen bei unserer Arbeit, in der Argumentation einen möglichst kleinen Faktor c zu erreichen, damit die Aussagen über das schwere Problem und über das Brechen der Verschlüsselung nicht allzu weit auseinanderliegen."

Ist dies geschafft, haben die Wissenschaftler beispielsweise einen Zusammenhang wie diesen hergestellt: Wenn die Verschlüsselung in $T = 2^{80}$ Schritten gebrochen werden kann, kann das schwere Problem in $c \cdot T$ Schritten gelöst werden. Ist $c = 2^{10}$, also in 2^{90} Schritten. Wohlgemerkt ist die Aussage rein hypothetisch, aber die Wissenschaftler nutzen nun einen üblichen Trick aus der Logik: Sie drehen die Folgerung um. Dabei müssen sie beide Aussagen verneinen.

Zum Beispiel kann die gültige Folgerung „Wenn der Hund gesund ist, hat er vier Beine" umgedreht werden; damit sie gültig bleibt, müssen die Aussagen aber negiert werden: „Wenn der Hund nicht vier Beine hat, ist er nicht gesund." Ebenso dreht Alexander May den gefundenen Zusammenhang zwischen dem Brechen eines Codes und einem schweren Problem um: Wenn das schwere Problem nicht in 2^{90} Schritten gelöst werden kann, kann die Verschlüsselung nicht in 2^{80} Schritten gebrochen werden.

Da May für seine Argumentation keine einzige Eigenschaft des hypothetischen Code-Brech-Algorithmus genutzt hat – außer der bloßen Existenz –, ist er sich sicher: „Die umgedrehte Aussage gilt für alle denkbaren Algorithmen, auch für die, die erst noch erfunden werden." Diese Art, eine Frage auf eine andere zu verlagern, nennt man Reduktion. Alexander May und seine Mitarbeiter haben die Frage, ob ein Code schnell zu brechen ist, nun also auf eine andere Frage zurückgeführt, nämlich wie schnell ein schweres Problem zu lösen ist (siehe "Schwere Probleme", Seite 43).

Als schwer bezeichnen IT-Wissenschaftler zum Beispiel das Teilsummenproblem: Angenommen, es liegt eine Liste mit Zahlen vor, ist es dann möglich, eine Menge von Zahlen in dieser Liste zu finden, die sich just zu null aufsummiert? Ist die Liste zum Beispiel –9, –3, 1, 4, 5, so lautet die Antwort ja, weil sich –9, 4 und 5 gerade zu null addieren. Dieses Beispiel mag einfach sein. Doch die benötigte Zeit hängt exponentiell von der Länge der Liste ab (siehe „Schwere Probleme"). Zu überprüfen, ob es in einer Liste eine Menge von Zahlen gibt, die sich zu null aufsummiert, ist somit ein schweres Problem.

Alexander May und seine Kollegen interessieren sich für solche Probleme, weil sie sie als Hilfsmittel nutzen, um etwas über die Sicherheit kryptografischer Verfahren auszusagen. Aus der Zeit, die es braucht, ein schweres Problem zu lösen, schließen sie nur durch logische Argumentation auf die Zeit, die das Knacken eines kryptografischen Verfahrens benötigt. ▸

Abb. 1: Alexander May arbeitet an Verschlüsselungsalgorithmen, die selbst ein leistungsstarker Quantencompute nicht knacken könnte. (Foto: rs)

Dabei ist es selten möglich, die Zeit exakt anzugeben. Allerdings können sie Schranken finden. „Wir wissen dann, wie viel Zeit ein Verfahren maximal braucht“, erläutert Alexander May. „Allerdings wissen wir nichts darüber, ob es nicht auch schneller gehen kann.“

Die Herausforderung für die Wissenschaftler besteht darin, möglichst enge Grenzen zu finden, in denen sich die tatsächliche Laufzeit befindet. Für das Teilsummenproblem braucht ein übliches Programm $n \cdot 2^n$ Rechenschritte. May hat festgestellt, dass es jedoch deutlich schneller erledigt werden kann, nämlich mit etwa $2^{0{,}3 \cdot n}$ Rechenschritten, eine enorme Verringerung.

Das Teilsummenproblem ist für ihn deshalb so interessant, weil es vermutlich auch für einen Quantencomputer eine harte Nuss ist. „Das Zerlegen in Primfaktoren, auf dem fast die gesamte gängige Verschlüsselung basiert, kann von einem Quantencomputer schnell erledigt werden. Das wissen wir heute bereits, auch wenn es ihn noch nicht gibt“, sagt May.

Doch das Teilsummenproblem bedeutet auch für einen Quantencomputer langwierige Berechnungen (Abb. 2). Deshalb konstruiert Alexander May Verschlüsselungsverfahren, die er mithilfe logischer Argumentation mit dem Teilsummenproblem verbindet. „Diese neuartigen Verschlüsselungen werden dann auch sicher sein, wenn der Quantencomputer kommt“, sagt er.

Aeneas Rooch

Abb. 2: Langzeitkritische Daten, etwa Bank- oder Gesundheitsdaten, sollten auch in vielen Jahren noch geschützt sein – selbst wenn es Quantencomputer gäbe, die heute gängige Verschlüsselungen mühelos brechen könnten. (Foto: rs)

SCHWERE PROBLEME

Schwere Probleme nennt man in der theoretischen Informatik Berechnungen, für die ein Computer besonders lange braucht. Allerdings ist nicht der konkrete Zeitbedarf auf einem bestimmten Computer gemeint, sondern die Anzahl der benötigen Rechenschritte, abhängig davon, wie viele Eingaben gemacht wurden. Diese sogenannte Laufzeit ist unabhängig davon, welcher Computer genutzt wird; sie gibt Informatikern Aufschluss darüber, wie kompliziert eine Berechnung ist.
Beispielsweise gilt das Sortieren einer Liste von Zahlen nicht als schwer. Denn sollen n Zahlen sortiert werden, benötigen gängige Sortieralgorithmen dazu nicht mehr als etwa $n \cdot n$ Rechenschritte. Zum Sortieren von zehn Zahlen sind also nicht mehr als 100 Schritte erforderlich, zum Sortieren von 20 Zahlen nicht mehr als 400. Denn die Algorithmen haben eine quadratische Laufzeit oder sind sogar schneller: Verdoppelt sich die Größe der zu sortierenden Liste, dauert die Sortierung im schlimmsten Fall etwa viermal so lang. Anders ist es beim sogenannten Teilsummenproblem, das folgende Frage stellt: Angenommen, es liegt eine Liste mit Zahlen vor, ist es dann möglich, eine Menge von Zahlen in dieser Liste zu finden, die sich zu null aufsummiert? Enthält die Liste n Zahlen, so benötigt ein übliches Programm maximal etwa $n \cdot 2^n$ Rechenschritte. Was für Nichtmathematiker nicht wüster als das $n \cdot n$ vom Sortieren aussieht, ist für Experten ein gewaltiger Unterschied: Verdoppelt sich die Listenlänge, wird die Laufzeit mehr als quadriert. Enthält die Liste beispielsweise fünf Elemente, so weiß man, dass der Algorithmus im Großen und Ganzen nicht mehr als $5 \cdot 2^5$, also 160 Schritte braucht; bei einer Listengröße von zehn Zahlen sind es jedoch bereits $10 \cdot 2^{10}$, also 10.240 Schritte. Dabei handelt es sich also um ein schweres Problem.

Aeneas Rooch

HARDWARE-TROJANER:

EINFALLSTÜREN FÜR GEHEIMDIENSTE

Trojaner auf Computerchips einzubauen ist eine aufwendige aber auch sehr raffinierte Angriffsart. Dort sind sie so gut wie nicht zu finden. Ein Vorteil, den vor allem Geheimdienste gerne für sich nutzen würden.

Prof. Dr. Christof Paar hat es geschafft: Der Leiter des Lehrstuhls für Eingebettete Sicherheit an der Ruhr-Universität Bochum hat 2016 einen der hart umkämpften Advanced Grants des Europäischen Forschungsrats (ERC) erhalten. Das schafft nicht jeder, denn gefördert wird nur, wer bahnbrechende Pionierforschung auf höchstem internationalen Niveau betreibt. Dass er die Förderung bekommen hat, zeigt die Bedeutung des damit verbundenen Forschungsvorhabens: Paar will Mechanismen entwickeln, die vor allem das Internet der Dinge sicherer machen. Sein Augenmerk richtet er dabei auf eine spezielle Sicherheitslücke: auf die Manipulation von Computerchips, also von Hardware-Bausteinen. Diese findet man heute nicht nur in PCs und Laptops, sondern in allen mit Elektronik ausgestatteten Geräten; sei es in der Kreditkarte, im Auto oder im Smartphone, aber auch in großen industriellen Anlagen oder medizinischen Geräten.

Angreifer können diese Chips potenziell derart manipulieren, dass die darauf laufenden Verschlüsselungsverfahren ausgehebelt oder persönliche Daten unproblematisch ausgelesen werden können. Genauso gut können sie über manipulierte Hardware auch Funktionen umprogrammieren oder die Kontrolle über Geräte und Systeme übernehmen. Das kann im Fall von Autos genauso bedrohlich sein wie bei Drohnen.

Im Gegensatz zu herkömmlichen Software-Trojanern, die man sich beispielsweise über bösartige E-Mail-Anhänge einfangen kann, handelt es sich bei Hardware-Trojanern um Sicherheitsschwachstellen, die Hersteller von Anfang an in ihre Geräte einbauen oder die bei der Chipfertigung eingefügt wer-

Foto: rs

den könnten. Hierbei ist besonders bedenklich, dass über 90 Prozent aller heimischen Hardware-Chips zwar in Deutschland entworfen, jedoch in Asien gefertigt werden.

Warum sollten Hersteller oder Chipfabrikanten dies tun? Christof Paar glaubt, die Antwort zu kennen: „Regierungen in aller Welt könnten an Hardware-Trojanern ein großes Interesse haben. Seit Edward Snowden seinen Enthüllungsbericht geschrieben hat, wissen wir, dass Geheimdienste einen großen Aufwand betreiben, um Sicherheitssysteme auf verschiedenste Weise auszuhebeln." Verweigern können sich die Firmen oft nur sehr schwer. Auch wenn sie ein hohes Risiko eingehen: Kommt heraus, dass sie ihre Kunden auf diese Art hintergehen, ist es mit deren Vertrauen vorbei. So geschehen in den 1980er-Jahren bei der „Crypto AG". Die Schweizer Firma stellte im Kalten Krieg Verschlüsselungsgeräte für Regierungen her. Später kam heraus, dass die National Security Agency, kurz NSA, dafür gesorgt hatte, dass die Geräte so manipuliert waren, dass die NSA die Verschlüsselung mit diesen Geräten brechen konnte. ▸

Abb. 1: Christof Paar leitet den Lehrstuhl für Eingebettete Sicherheit an der RUB. (Foto: rs)

Hintertüren oder Backdoors nennt man die eingebauten Sicherheitslücken in Fachkreisen. „Dass Manipulationen von Sicherheitslösungen theoretisch möglich sind, wussten Wissenschaftler schon lange“, so Christof Paar (Abb. 1). Überrascht habe ihn und seine Kolleginnen und Kollegen aber das Ausmaß, in dem die NSA Angriffe gegen Kryptolösungen umgesetzt hatte. Grund genug für den Forscher, sich intensiv mit dem Thema auseinanderzusetzen. Mit den Fördermitteln, die er durch den ERC-Grant bekommen hat, ist ihm das möglich. Das Forschungsprojekt, das Christof Paar zusammen mit mehreren Doktoranden in Angriff genommen hat, besteht aus zwei Teilen: Zunächst nehmen die Wissenschaftler die Perspektive der Angreifer ein und überlegen sich, welche Hardware-Trojaner überhaupt effektiv sind. Nur wenn die Wissenschaftlerinnen und Wissenschaftler das wissen, können sie auch wirksame Gegenmaßnahmen entwickeln. Eine besondere Schwierigkeit hierbei ist, dass moderne Chips oft aus mehreren zehn Millionen elementaren Bausteinen, sogenannten Logikgattern, bestehen. Ein Angreifer muss jedoch oft nur minimale Änderungen an einigen wenigen dieser Bausteine vornehmen, um einen Trojaner zu realisieren. Im zweiten Teil wollen die Forscher dann Lösungen entwickeln, mit denen sich diese Manipulationen verhindern lassen.

An Ideen, wie man Hardware-Trojaner einsetzen könnte, mangelt es Christof Paar nicht. Der manipulierte Chip könnte den Rechenfehler zum Beispiel nur ausführen, wenn ein bestimmter Auslöser vorhanden ist. „Das könnten bei einer Drohne oder bei einem Auto bestimmte GPS-Koordinaten sein“, so Paar. „Nur wenn man sich in der entsprechenden Region befindet, würde der Trojaner aktiv.“

Besonders raffiniert wäre es von den Angreifern, erklärt Paar, wenn sie nicht die Logikgatter austauschen würden, also die Schaltkreise verändern würden. Das könnten besonders gewiefte Anwender unter Umständen noch detektieren, wenn die Chips zum Beispiel mit speziellen Mikroskopen inspiziert würden. Praktisch unsichtbar seien hingegen Manipulationen am Herzstück jedes Computers, an den sogenannten Transistoren. Von den winzig kleinen Rechenmaschinen gibt es inzwischen bis zu einer Milliarde auf einem Chip (Abb. 2 und 3). „Es ist sehr einfach, einen Transistor beispielsweise etwas langsamer zu machen“, sagt Paar. Dafür müsse man nur wenige Atome in dem Halbleiter verändern, aus dem der Transistor besteht. Oder winzige Verbindungslinien zwischen den Transistoren wenige Nanometer dünner machen.

Befürchtungen, dass seine Forschung durch die Geheimdienste gefährdet werden könnte, hat der 52-Jährige nicht. „Gerade in Europa wird meine Forschung sehr positiv gesehen. Mein Ziel ist es ja zu verstehen, was sehr entschlossene und finanzstarke Angreifer anrichten können. Inzwischen gibt es zumindest in Europa einen breiten Konsens, dass Hardware-Manipulationen eine ernsthafte Bedrohung für Bürger, Wirtschaft und den Staat sind.“ *rr*

> „REGIERUNGEN IN ALLER WELT KÖNNTEN AN HARDWARE-TROJANERN EIN GROSSES INTERESSE HABEN.“

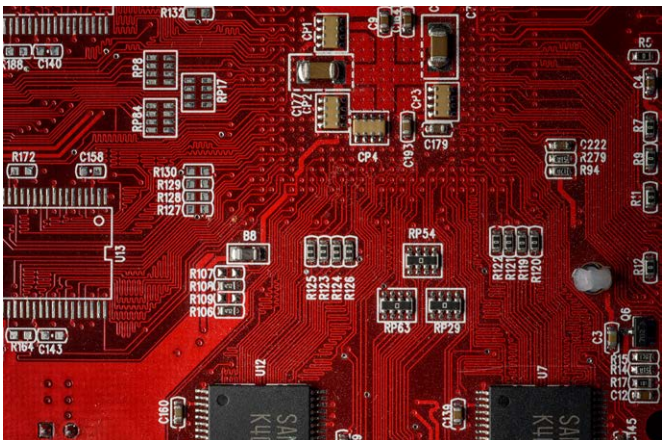


Abb. 2: Dünne Linien verbinden die einzelnen Elemente auf der Leiterplatte. Unten im Bild sind zwei Chips zu sehen. In ihrem Inneren sieht es ähnlich aus, nur dass alles noch viel kleiner ist. (Foto: rs)

Abb. 3: Das Innere eines Chips: immer dichter, immer komplexer. Bis zu einer Milliarde Transistoren sorgen für rechnerische Höchstleistungen. (Bild: iStock, amadeusamse)

escrypt
Embedded Security by ETAS

Security Consultant (m/w)
Projektleiter Embedded Security (m/w)
Software Engineer (m/w)

Als international agierendes und stark wachstumsorientiertes Unternehmen im Bereich der Embedded Security unterstützen wir alle Branchen, die einen Bedarf an Sicherheitslösungen in eingebetteten Systemen haben. ESCRYPT GmbH ist ein 100 %iges Tochterunternehmen der ETAS GmbH, einem Mitglied der Bosch-Gruppe, und ein führendes Systemhaus in diesem Bereich.

Zur Verstärkung unseres Teams in unserer Niederlassung in **Stuttgart** bzw. **Bochum** suchen wir zum nächstmöglichen Zeitpunkt:

Security Consultant (m/w) SCAS-1506-STR

Ihre Aufgaben: Konzeption und Durchführung von Sicherheitsanalysen (Automotive Systems), Analyse und Konzeption von Sicherheitslösungen vernetzter Automotive-Dienste, hardwarenahe Entwicklung von Secure Automotive Systems, Auswertung und Präsentation der Ergebnisse mit Verbesserungsvorschlägen, Beratung der Kunden bei Umsetzung, Erstellung von Entscheidungsvorlagen zu neuen Sicherheitslösungen und Konzepten

Projektleiter Embedded Security (m/w) PL-1511-STR

Ihre Aufgaben: Koordination und Herleitung des Erfolgs des Projekts, fachliche Leitung eines Teams, interne und externe Berichterstattung, Auswertung und Präsentation der Ergebnisse, Beratung der Kunden bei Umsetzung, Analyse und Konzeption von Sicherheitslösungen vernetzter Automotive-Dienste

Software Engineer (m/w) SI-1511-BO

Ihre Aufgaben: Design, Implementierung und Test von (AUTOSAR) Basis-Software-Komponenten nach Norm-/Prozessanforderungen (aSPICE/ISO26262), Anforderungsmanagement, statische Code-Analyse, Mitarbeit am Produktentwicklungsprozess

Unsere fachlichen Anforderungen

- Fachhochschul-, Universitätsabschluss im Bereich der Elektrotechnik, Informatik, IT-Sicherheit oder vergleichbar
- mehrjährige Berufserfahrung
- Spezialkenntnisse in den beschriebenen Aufgaben
- sehr gute Deutsch- und Englischkenntnisse

Unser Angebot

Wir geben Ihnen die Möglichkeit langfristig in einem dynamischen, hoch qualifizierten, international erfahrenen Team eigenverantwortlich tätig zu sein. Ihr Umfeld wird abgerundet durch ein sympathisches und offenes Arbeitsklima, spannende Herausforderungen, abwechslungsreiche Tätigkeiten, flache Hierarchien und gute Bezahlung.

Interessiert Sie diese Herausforderung?

Dann senden Sie uns Ihre aussagefähigen Bewerbungsunterlagen inkl. Zeugnissen unter der jeweiligen Kennziffer ausschließlich per E-Mail an jobs@escrypt.com

Noch Fragen?

Ich helfe Ihnen gerne weiter.

Helene Mensler

Telefon:
+49 234 43870-247

LEICHTE BEUTE FÜR HACKER: NAVIGATIONSSYSTEME

Autofahrer vertrauen dem GPS bei der Routenplanung fast blindlings, und auch in der Industrie und anderen Bereichen spielt es bei der Orts- und Zeitbestimmung eine wichtige Rolle. Greifen Hacker das System an, können sie großen Schaden anrichten. In der Arbeitsgruppe Informationssicherheit forscht man an Abwehrmaßnahmen.

Schwer beeindruckt zeigte sich NRWs Ministerpräsidentin Hannelore Kraft im Sommer 2015, als Juniorprofessorin Christina Pöpper ihr demonstrierte, wie leicht das Global Positioning System (Info) und damit auch jedes andere Navigationssatellitensystem von Hackern manipuliert werden kann. Anlass des Besuchs war die jährliche Sommerreise der Politikerin, die sie nutzte, um sich am Horst-Görtz-Institut einen Einblick in den aktuellen Stand der IT-Sicherheitsforschung geben zu lassen.

Christina Pöpper und ihre Mitarbeiter simulierten in ihrer Präsentation für die Ministerin eine Autofahrt zu deren Dienstsitz nach Düsseldorf. Wie im wahren Leben auch gaben sie dafür die Zieladresse in ein Navigationsgerät ein und starteten die Anwendung. Dann die Überraschung: Obwohl das Gerät den Raum nicht verließ, bewegte sich der Positionspfeil in Richtung Landeshauptstadt. Ursache war nicht etwa ein Fehler in der Software, sondern ein Angriff auf das GPS, durchgeführt von den IT-Experten. Sie gaukelten dem Gerät eine Fahrt vor, die in der Tat gar nicht stattfand. Ein reelles Szenario, das ein Angreifer auch während echter Fahrten durchführen könne, so Christina Pöpper: „GPS wird seit etwa 1992 verwendet. Dass es angreifbar ist, weiß man bereits seit 2002. In der Zwischenzeit wurden schon viele Vorschläge für Gegenmaßnahmen entwickelt, doch bisher gibt es keine Abwehr, die gegen alle Angriffe schützt. Die Frage ist immer, wie stark der Angreifer ist."

Wie ernst das Problem ist, sieht man daran, dass selbst die US Navy dem GPS nicht mehr ihr volles Vertrauen entgegenbringt. 2006 war die astronomische Navigation zugunsten der Orientierung mittels GPS aus den Lehrplänen verschwunden – bis vor Kurzem. Die Navy stuft das Sicherheits- und Ausfallrisiko bei GPS so hoch ein, dass die Ausbildung der Offiziere inzwischen auch wieder am Sextanten stattfindet. „Als ich davon gehört habe, war ich durchaus überrascht. Schließlich geht man häufig davon aus, dass die Entwicklung im militärischen Bereich weiter fortgeschritten ist als im zivilen", so Pöpper.

Gemeinsam mit ihrem Doktoranden Kai Jansen tüftelt die Informatikerin an einer Lösung des Problems. Denn auf GPS gänzlich zu verzichten, ist keine Alternative. Ein Vorteil des Systems ist, dass es so vielseitig einsetzbar ist. Ob im Navigationsgerät im Auto, in der elektronischen Fußfessel, der Luftfahrt oder im Handy – sie alle greifen auf GPS zurück. Da es sich außerdem nicht nur zur Positionsbestimmung, sondern zudem zur Zeitsynchronisierung eignet, setzt man das System auch in der Industrie ein, um Maschinen und Messungen zeitlich aufeinander abzustimmen.

Die Zeitberechnung bei GPS beruht auf seiner Funktionsweise: Um die eigene Position zu bestimmen, misst der Empfänger die exakte Signallaufzeit zwischen mehreren Satelliten und sich. Insgesamt umkreisen mehr als 24 Satelliten auf hohen Bahnen die Erde. An jedem Punkt der Erde hat man

zu mindestens vier von ihnen Kontakt (Abb. 1). Ihre genauen Bahnparameter senden sie ständig in ihrem Signal mit. Der Empfänger weiß also genau, woher das Signal kommt. Außerdem hat jeder Satellit eine Atomuhr an Bord und kann sehr genau den Sendezeitpunkt seines Signals angeben. Je weiter der Satellit vom Empfangsgerät entfernt ist, desto mehr Zeit vergeht, bis das Signal ankommt. Anhand der bekannten Parameter Sendezeitpunkt und Sendeort der vier empfangenen Signale wird der Empfängerort bestimmt; das funktioniert unter gleichzeitiger Berechnung der eigenen lokalen Zeit beim Empfangsgerät.

Will ein Angreifer das System manipulieren, kann er dafür einen Satellitensimulator nutzen. Der handliche Kasten, den auch die Bochumer IT-Experten für ihre Forschungszwecke einsetzen und der üblicherweise dem Testen von GPS-Empfängern dient, generiert Satellitensignale und verschickt sie über eine Antenne. Die Signale erscheinen so täuschend echt, dass die meisten Empfangsgeräte den Unterschied nicht bemerken. Ein Umstand, den Angreifer nutzen können, um dem Empfangsgerät zu suggerieren, es wäre an einem anderen Ort, als es tatsächlich ist. Diese Vorstellung dürfte bei vielen Menschen sogleich Horrorszenarien wie entführte Flugzeuge, fehlgeleitete Geldtransporter oder im Untergrund abgetauchte Fußfesselträger hervorrufen.

Der Lösungsansatz von Christina Pöpper und Kai Jansen beruht auf der Überlegung, was passiert, wenn ein Fahrzeug

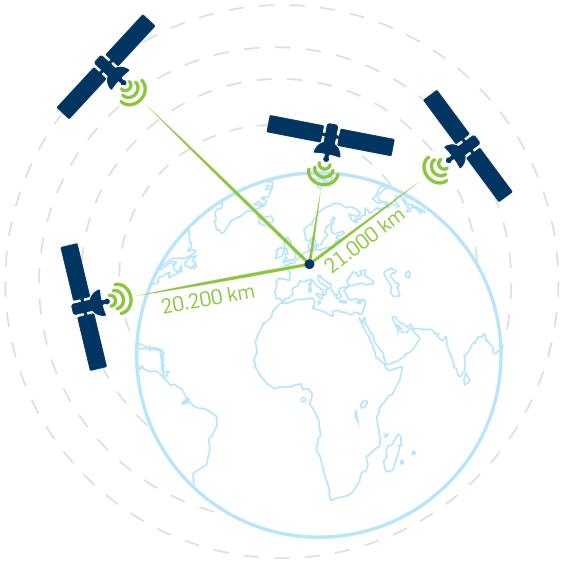


Abb. 1: Um seine Position mittels GPS bestimmen zu können, muss das eigene Empfangsgerät zu vier Satelliten Kontakt haben. Je weiter ein Satellit vom Empfangsgerät entfernt ist, desto mehr Zeit vergeht, bis das Signal bei diesem ankommt. Sind Sendezeitpunkt und Sendeort der vier empfangenen Signale bekannt, kann das Gerät seinen Aufenthaltsort berechnen.
(Grafik: Agentur der RUB, Zalewski)

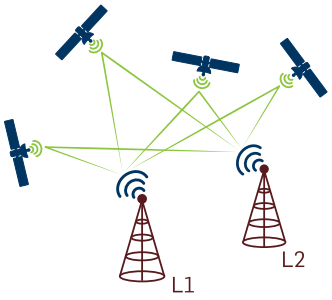
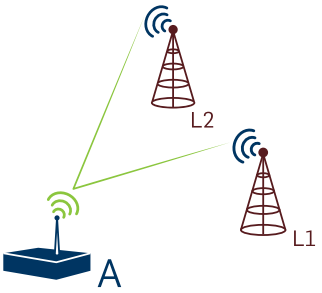
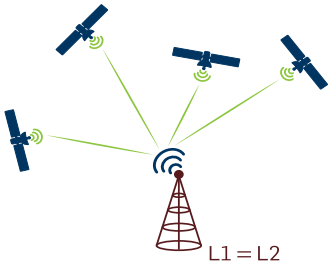


Abb. 2: Normale Situation: Zwei Empfangsgeräte an den Positionen L1 und L2 möchten ihre Position bestimmen. Dafür müssen sie von mindestens vier Satelliten Signale empfangen. Ihre berechneten Positionen unterscheiden sich voneinander.



Reale Angriffssituation: Der Angreifer sendet vier Satellitensignale, kombiniert in einem Signal, an die zwei Empfangsgeräte.



Angriffssituation aus Sicht der GPS-Empfänger: Die zwei Empfangsgeräte bestimmen jeweils ihre Positionen L1 und L2, die zur gleichen falschen Position zusammenfallen. Dies kann detektiert werden.

Grafiken: Agentur der RUB, Zalewski

oder eine Maschine nicht nur ein Empfangsgerät nutzt, sondern gleichzeitig mehrere, die einen gewissen Abstand voneinander haben. In dem Fall, dass sie echte Satellitensignale empfangen, unterscheiden sich die berechneten Positionsdaten der Empfangsgeräte leicht voneinander, nämlich in dem Maß, wie sich ihre tatsächlichen Positionen voneinander unterscheiden. Sendet jedoch ein Angreifer die Signale mittels Simulator, so sehen diese für jedes einzelne Empfangsgerät täuschend echt sowie identisch aus. Nur durch den Abgleich der verschiedenen Empfänger miteinander lässt sich der Angriff detektieren, denn alle Empfangsgeräte glauben nun, an der gleichen (falschen) Position zu sein, was ja nicht der Fall ist (Abb. 2). Grund dafür ist, dass die relativen Empfangszeiten mehrerer Signale, die über den Satellitensimulator versendet werden, für mehrere Empfangsgeräte identisch sind. Dies ist nicht der Fall beim Empfang legitimer Satellitensignale, da sie von verteilten Positionen in der Erdumlaufbahn versendet werden.

„Dass wir auf diese Weise Angriffe detektieren können, haben wir bereits gezeigt. Momentan arbeiten wir noch an Detailfragen. Zum Beispiel, wie groß der Abstand zwischen den Empfangsgeräten sein muss, damit sie auch beim Empfang echter Signale aufgrund nicht zu vermeidender Ungenauigkeiten nicht dieselbe Position für sich ermitteln würden“, sagt Christina Pöpper (Abb. 3). Um das herauszufinden, stieg Kai Jansen samt Equipment sogar auf das Dach des IC-Gebäudes, da der Signalempfang hier besonders gut ist. Nach heutigem Erkenntnisstand beträgt der minimale Abstand der Geräte zwei bis drei Meter. Liegen die Empfänger näher beieinander, steigt die Fehlerrate. Pöpper: „Das lässt sich an großen Fahrzeugen oder Maschinen wie LKW oder Schiffen gut realisieren, da man hier die Empfangsgeräte weit genug entfernt voneinander positionieren kann. Für Handys, Fußfesseln oder andere Bereiche ist diese Lösung jedoch nicht einsetzbar.“ Grund genug für Christina Pöpper und ihr Team, weiter in dem Bereich zu forschen.

Text: rr, Fotos: rs

Abb. 3: Christina Pöpper leitet die Arbeitsgruppe Informationssicherheit am Horst-Görtz-Institut.

GPS

Das Global Positioning System, kurz GPS, wurde in den 1970er-Jahren für das US-Militär entwickelt, welches vorher andere Navigationssysteme genutzt hatte. GPS bringt den Vorteil mit sich, dass die Empfangsgeräte nur Signale empfangen und nicht selber senden. So kann navigiert werden, ohne dass der Feind Informationen über den eigenen Standort erhält. Seit 1992 nutzt auch die Zivilbevölkerung GPS.

RUBIN IM NETZ

Mehr zur Forschung von Christina Pöpper
Sicherheit im Uni-WLAN: Die richtige Konfiguration entscheidet. rubin.rub.de/eduroam

Werden Sie eine von uns.

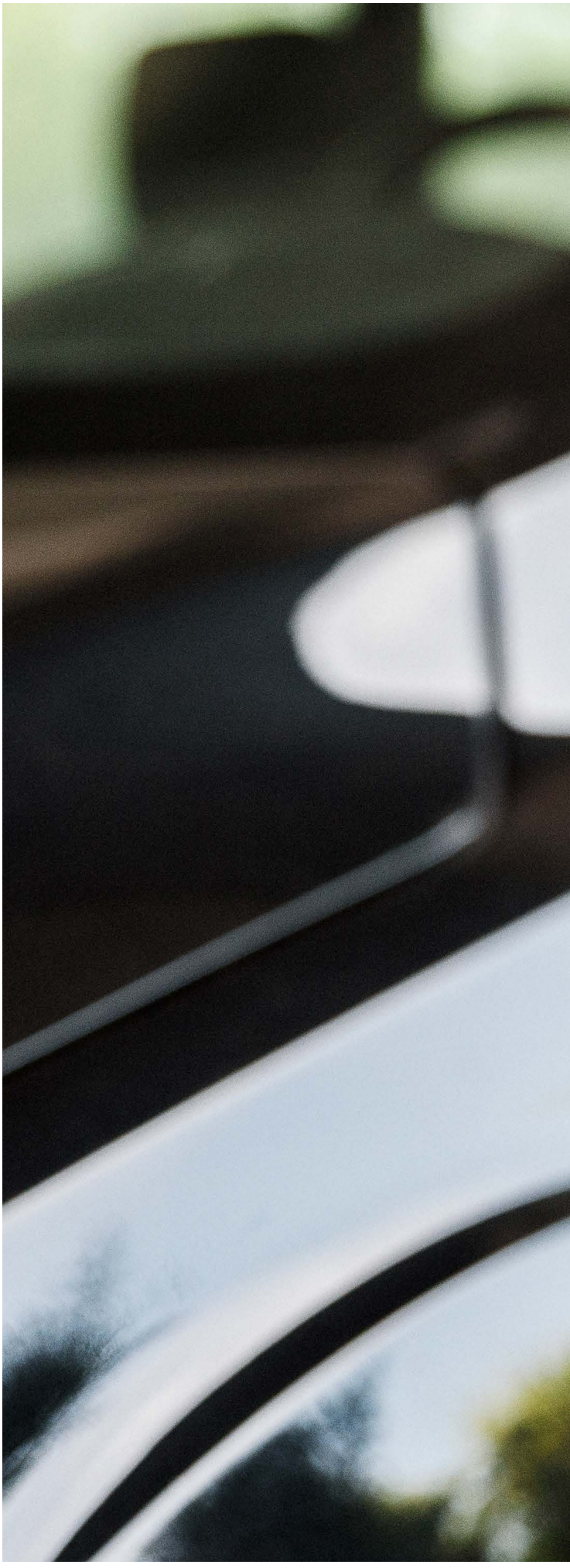
Genau wie Maria del Pozo Gomez, Ingenieurin der Verfahrenstechnik bei der thyssenkrupp Industrial Solutions – unserem Experten für Chemieanlagen und Raffinerien. Als eine von uns ist sie für die Planung und Inbetriebnahme von Werken zur Chlorgewinnung verantwortlich und findet ihr Einsatzgebiet überall auf der Welt. Wenn auch Sie in Zukunft Verantwortung bei internationalen Projekten übernehmen wollen, werden Sie eine von uns.
www.thyssenkrupp.com/karriere

engineering.tomorrow.together.

thyssenkrupp

KLEINER CODE FÜR GROSSE SICHERHEIT

Von unterwegs die Heizung steuern oder per Funk die Tür verschließen – vernetzte Geräte bieten faszinierende Möglichkeiten, müssen aber gegen Hackerangriffe geschützt sein.



Ein Autoschlüssel ist ein unscheinbarer Gegenstand, enthält aber komplizierte Mathematik: Wer seinen Wagen aus ein paar Schritten Entfernung per Funk öffnet, will schließlich sicher sein, dass es Verbrechern nicht möglich ist, das Funksignal abzufangen und dem Auto den Befehl zum Öffnen auch ohne Schlüssel vorzuspielen; die Kommunikation zwischen Auto und Autoschlüssel wird deshalb mit mathematischen Verfahren verschlüsselt. Ein Autoschlüssel ist allerdings kein Hochleistungscomputer: Mit seinem billigen Chip und seiner kleinen Batterie schafft er keine komplizierten Berechnungen. Er ist damit ein Härtefall für IT-Experten wie Prof. Dr. Gregor Leander (Abb. 1). Der Professor für IT-Sicherheit ist auf sogenannte Lightweight-Kryptografie spezialisiert und entwickelt an der RUB sparsame Verschlüsselungsverfahren. Sie können in kleinen, billigen Sensoren und Chips eingesetzt werden, wo nur wenig Rechenleistung und Strom zur Verfügung stehen – etwa im Fensterrahmen, im Thermostatknopf oder im Autoschlüssel. Trotzdem sind sie sicher. „Es ist kein Problem, ein sicheres oder ein einfaches Verschlüsselungsverfahren zu finden“, sagt der Wissenschaftler. „Aber die sicheren Verfahren sind meistens kompliziert, und die einfachen Verfahren sind meistens unsicher. Die Herausforderung besteht also darin, beides gleichzeitig zu schaffen: Sicherheit und Einfachheit.“ Das klingt selbstverständlich, aber das ist es nicht: „In der Industrie werden häufig superschlechte Algorithmen eingesetzt“, beklagt Gregor Leander. Er und seine Kollegen wollen Abhilfe schaffen. ▸

Ein Autoschlüssel sollte nur das eine Auto öffnen, zu dem er gehört. Um das sicherzustellen, laufen auf dem Mikroprozessor im Inneren des Schlüssels kryptografische Protokolle.

Abb. 1: Gregor Leander entwickelt sparsame Verschlüsselungsverfahren.

Abb. 2: Verschlüsselung steckt heutzutage in vielen Kleinstgeräten, zum Beispiel in diesem implantierbaren Defibrillator. Bei solchen Alltagsgegenständen ist besonders wichtig, dass sie sicher sind.

In der Kryptografie geht es darum, eine Nachricht so zu verändern, dass das Ergebnis für Außenstehende zwar nicht mehr verständlich ist, Eingeweihte es aber zurückübersetzen können. Jede Nachricht wird im Computer durch eine Abfolge der Ziffern Null und Eins, sogenannte Bits, dargestellt. Ziel in der Kryptografie ist es, eine gegebene Abfolge von Nullen und Einsen nach einem bestimmten Verfahren umzubauen. Das Verfahren umfasst zum einen eine Verschlüsselungsvorschrift, eine generelle Anleitung, die allgemein bekannt ist; zum anderen einen Schlüssel, eine spezielle Ergänzung zu der Vorschrift, die in jedem Einzelfall anders aussieht und möglichst geheim bleiben sollte. Die geschickte Kombination aus Vorschrift und Schlüssel macht ein Verschlüsselungsverfahren erst gut und sicher.

Gregor Leander beschäftigt sich konkret mit sogenannten symmetrischen Verschlüsselungsverfahren, bei denen sowohl der Absender einer Nachricht als auch der Empfänger den Schlüssel besitzt, der zum Chiffrieren und Dechiffrieren der Nachricht nötig ist. „In der Praxis werden so gut wie alle Daten mit symmetrischen Verfahren verschlüsselt“, sagt der IT-Wissenschaftler, „weil sie sehr schnell sind. Lediglich zum Austauschen des Schlüssels zwischen Sender und Empfänger benutzt man andere Verfahren.“ Unter den symmetrischen Verschlüsselungsverfahren konzentriert sich Gregor Leander auf sogenannte Blockchiffren, bei denen die zu verschlüsselnde Nachricht in Blöcke zerteilt wird und die Verschlüsselung blockweise stattfindet. Die Blöcke haben jeweils eine feste Länge. Oft besteht die Verschlüsselung auf einem solchen Block aus mehreren Runden: Ein Block aus den Ziffern Null und Eins wird also mehrfach hintereinander nach einer bestimmten Vorschrift mithilfe des Schlüssels verändert. „Das ist zum einen einfach zu programmieren“, erklärt Gregor Leander. „Außerdem erkennen wir bei einem Verfahren nach diesem Muster besser, warum es funktioniert, das heißt, warum es sicher ist.“

Da die Verschlüsselungsvorschrift allgemein bekannt ist, besteht das Ziel für Angreifer darin, den Schlüssel herauszufinden. Theoretisch ist das durch stumpfes Ausprobieren möglich. Denn auch der Schlüssel besitzt eine feste Länge und ist aus Computersicht ebenfalls nur eine Abfolge der Ziffern Null und Eins. Kennt man einen Klartext und das, was das Verschlüsselungsverfahren daraus gemacht hat, muss man der Verschlüsselungsvorschrift also bloß jeden möglichen Schlüssel vorsetzen, das heißt, jede mögliche Abfolge von Nullen und Einsen von der Länge des Schlüssels – bis man denjenigen Schlüssel gefunden hat, der den bekannten Klartext in den bekannten Geheimtext verwandelt.

Um zu verhindern, dass Angreifer genau das tun, wählt man in der Praxis Schlüssel aus, die so lang sind, dass das Durchprobieren aller möglichen Abfolgen von Bits unvorstellbar lange dauern würde. Doch ein Code kann nicht nur durch Ausprobieren geknackt werden, sondern auch durch geschicktes Analysieren. Hier suchen die Angreifer sozusagen Abkürzungen, das heißt mathematische Vereinfachungen, die es erlauben, den geheimen Schlüssel zu finden, ohne alle Möglichkeiten durchzuprobieren.

Ein Beispiel für eine solche mathematische Abkürzung ist die sogenannte lineare Kryptoanalyse. Hierbei versucht der Angreifer, das Verschlüsselungsverfahren durch eine lineare, also eine sehr einfache, Funktion anzunähern. Neben der Entwicklung neuer Verschlüsselungsverfahren geht es deshalb bei der Arbeit von Gregor Leander auch darum, im Allgemeinen besser zu verstehen, was symmetrische Verschlüsselungsverfahren sicher macht: „Die Herausforderung für uns ist, Verfahren zu erfinden, die nicht einfach durchschaut werden können“, so der Forscher. Zum Beispiel haben Gregor Leander und seine Kollegen das Verschlüsselungsverfahren „Present“ erfunden. Die International Organization for Standardization, kurz ISO, hat es inzwischen als Standard anerkannt. Dabei wird die zu verschlüsselnde Nachricht in Blöcke

Abb. 3: Funketiketten, in der Fachsprache RFID genannt, sind weit verbreitet. Nicht nur in Chipkarten kommen sie zum Einsatz, sondern mit ihnen werden auch Tiere markiert. Weil sie so klein sind, sind dafür besonders effiziente Verschlüsselungsalgorithmen gefragt.

> „DIE SICHEREN VERFAHREN SIND MEISTENS KOMPLIZIERT, UND DIE EINFACHEN VERFAHREN SIND MEISTENS UNSICHER.“

der Länge 64 Bit zerteilt, das heißt in eine Abfolge von 64 Einsen und Nullen. Diese 64 Bits werden wiederum in Abschnitten à 4 Bit betrachtet.

Zuerst werden die vier Nullen und Einsen in jedem Abschnitt nach einem bestimmten Rezept verändert. Danach werden alle 64 Bits gemischt. Anschließend beginnt die nächste Runde, in der die Bits wieder erst in Viererblöcken verändert und danach im ganzen 64er-Block gemischt werden, und so weiter. Sowohl die Veränderung der Viererblöcke als auch das Vertauschen der 64 Stellen müssen dabei bestimmte Voraussetzungen erfüllen, damit das Verfahren, obwohl es so einfach klingt, sicher ist. Zum einen sollen die Veränderungen möglichst wenig linear sein, das heißt gewissermaßen, sie dürfen nicht zu simpel sein. Zum anderen muss das Vertauschen möglichst wild ablaufen, damit Zeichen aus dem Anfang auch mit Zeichen vom Ende vertauscht werden und nicht nur Zeichen aus der nächsten Nachbarschaft die Plätze wechseln. Ziel ist es, dass die Nachricht nach mehreren Runden dieser einfachen Operationen möglichst stark und undurchschaubar verfremdet ist.

Gregor Leander arbeitet eng mit Forschern und Experten aus den Ingenieurwissenschaften zusammen. Die fachübergreifende Zusammenarbeit hält er für extrem wichtig. Denn um die passende Mathematik für kostengünstige und energiebeschränkte Anwendungen zu liefern, muss er verstehen, was kostengünstig und energiebeschränkt in Sachen Hardware überhaupt bedeutet. Schließlich können seine Algorithmen in vielfältigen praktischen Anwendungen zum Einsatz kommen. So nutzt nicht nur ein Autoschlüssel sparsame Kryptografie, sondern auch ein Herzschrittmacher: Ihn kann man per Funk einstellen, und selbstverständlich muss die Kommunikation hier ebenfalls abgesichert sein. Wie der Autoschlüssel besitzt auch der Herzschrittmacher keinen leistungsstarken Computer für die Verschlüsselung, und es gibt bloß eine kleine Batterie. „Dick Cheney, der ehemalige Vizepräsident der USA, hat aus Angst vor einem Anschlag per Funk angeblich die Fernsteuerungsfunktion seines Herzschrittmachers deaktivieren lassen“, berichtet Gregor Leander (Abb. 2). Der IT-Wissenschaftler selbst ist da gelassener, obwohl er einen großen Nachholbedarf sieht: „In der Praxis werden häufig unsichere Algorithmen verwendet.“

Dabei ist Lightweight-Kryptografie eine zentrale Herausforderung in der Industrie 4.0, die für die Produktion und Logistik intelligente, vernetzte Systeme benötigt. So dienen zum Beispiel Funketiketten, in der Fachsprache RFID für radio-frequency identification, nicht nur als Diebstahlsicherung, sondern werden auch genutzt, um Pakete nachzuverfolgen und Tiere zu kennzeichnen (Abb. 3). Sie sind in Reisepässen und Personalausweisen eingesetzt und finden sich in Form kontaktloser Chipkarten für Bus und Bahn. Die Verschlüsselungsverfahren, die Gregor Leander entwickelt, können all diesen Zwecken dienen.

Text: Aeneas Rooch, Fotos: rs

SCHWACHSTELLEN IM INTERNET-VERSCHLÜSSELUNGS-PROTOKOLL TLS

Beim E-mailen oder Onlineshoppen senden wir sensible Daten wie Passwörter und Kontoinformationen durch das Internet. Absolut sicher sind sie derzeit nicht.

Wer E-Mails abruft, sich in das universitäre WLAN Eduroam einwählt oder einen Onlineshop nutzt, ist auf eine verschlüsselte Datenübertragung angewiesen. Schließlich sollen Fremde keine Passwörter und Kontodaten mitlesen können. In all diesen Anwendungen ist das gleiche Verschlüsselungsprotokoll im Einsatz: TLS, kurz für Transport Layer Security. Bis vor ein paar Jahren galt es als absolut sicher. „Dann gingen verschiedene Angriffe auf das Protokoll um die Welt, und man hat gemerkt, dass es noch viel Verbesserungspotenzial gibt“, erzählt Prof. Dr. Jörg Schwenk vom Lehrstuhl für Netz- und Datensicherheit (Abb. 1). Gemeinsam mit seinem Team war er an einigen solcher Angriffe beteiligt. Die daraus resultierenden Erkenntnisse werden in eine neue Version von TLS einfließen, die die Internet Engineering Task Force derzeit standardisiert.

Die Transport Layer Security geht auf die Firma Netscape zurück, welche den ersten Internetbrowser auf den Markt brachte. „Die Entwickler haben sich relativ früh Gedanken darüber gemacht, dass man im Internet einen gewissen Schutz braucht, zum Beispiel für Onlineshops“, weiß Schwenk. Dafür brachten sie 1994 das Verschlüsselungsprotokoll Secure Socket Layer (SSL) heraus, dessen spätere Versionen in TLS umbenannt wurden. Die aktuelle Version trägt die Bezeichnung 1.2. Voraussichtlich 2016 oder 2017 wird dann der Nachfolger TLS 1.3 verfügbar sein. Darin ist quasi alles neu. Und zwar in zweierlei Hinsicht: zum einen auf Ebene der eigentlichen Verschlüsselung, zum anderen auf Ebene der Schlüsselaushandlung.

Um eine Nachricht zu verschlüsseln, sind zwei Dinge erforderlich: eine Verschlüsselungsvorschrift, die vorgibt, nach welchem Schema die Nachricht zu verändern ist. Und ein Schlüssel, den beide Parteien kennen müssen, um die Nachricht chiffrieren und dechiffrieren zu können. Die Verschlüsselungsvorschrift darf öffentlich bekannt sein, der Schlüssel jedoch nicht. Denn nur mit ihm kann man die Nachricht dechiffrieren. Solange der Schlüssel also geheim ist, ist der Inhalt der Nachricht geschützt. Damit zwei Parteien sicher miteinander kommunizieren können – etwa wenn ein Kunde oder eine Kundin Kreditkartendaten an einen Webshop übermitteln möchte –, müssen sich die beiden zunächst auf einen Schlüssel einigen, also ein gemeinsames Geheimnis aushandeln. In diesem Prozess können Sicherheitslücken auftreten, genauso wie bei der eigentlichen Verschlüsselung.

Jörg Schwenks Team gelang es zum Beispiel, den Schlüssel zu stehlen, den zwei Parteien mit TLS 1.2 aushandeln. Prinzipiell kann die Schlüsselaushandlung auf drei Wegen erfolgen; die meisten Probleme verursacht das sogenannte RSA-Handshake-Verfahren, benannt nach den Erfindern Rivest, Shamir und Adleman. Bildlich erklärt funktioniert es so: Der Server des Webshops schickt dem Kunden einen Briefkasten zu. Der Kunde steckt eine geheime Nachricht in den Briefkasten und schickt ihn zurück an den Server. Der öffnet den Briefkasten und kommt so an die geheime Nachricht heran. Diese Nachricht fungiert dann als Schlüssel, mit dem der Kunde seine Kreditkartendaten chiffriert.

Über einen sogenannten Bleichenbacher-Angriff verschaffte sich Schwenks Team Zugang zu dem Schlüssel: Dazu versahen die IT-Sicherheitsexperten die geheime Nachricht mit Fehlern, bevor sie sie in den Briefkasten steckten und an den Server schickten. Das machten sie nicht nur einmal, sondern immer wieder, wobei sie die geheime Nachricht jedes Mal leicht variierten. Der Server erwartet, dass die Nachricht in einer bestimmten Form bei ihm ankommt; sie muss mit den Ziffern Null und Zwei beginnen. Ist das nicht der Fall, startet der Server eine Fehlerbehandlung. Die Nachrichten der RUB-Forscher enthielten bewusst Fehler, fingen also nicht immer mit Null und Zwei an. Für die Fehlerbehandlung braucht der Server länger, als wenn er normal mit dem Schlüsselaustausch fortfahren kann. Dieser Zeitunterschied erlaubte Rückschlüsse auf den Inhalt der Nachricht, also auf den Schlüssel, der eigentlich geheim bleiben sollte.

Ein solcher Angriff auf die Transport Layer Security wird in Version 1.3 nicht mehr möglich sein. Das RSA-Handshake-Verfahren wird durch den Diffie-Hellman-Schlüsselaustausch ersetzt. „Mein Doktorvater Albrecht Beutelsbacher hat das Verfahren einmal wie folgt erklärt“, erinnert sich Schwenk. „Man steckt zwei geheime Zutaten in ein Rezept. Wenn man umgerührt hat, kann man nicht mehr herausfinden, was die

Beim Onlineshopping geben Kunden persönliche Daten in ihren Browser ein; das Verschlüsselungsprotokoll TLS soll dafür sorgen, dass sie sicher übertragen werden. Auch wer E-Mails sendet, verwendet häufig TLS.

Abb. 1: Jörg Schwenk deckte mit seinen Kollegen einige Schwachstellen im Internet-Verschlüsselungsprotokoll auf.

zwei Zutaten waren." Somit könnte auch niemand das Rezept nachmachen. Um den Schlüssel zu generieren, denken sich die zwei miteinander kommunizierenden Parteien jeweils ein Teilgeheimnis aus und mischen diese. Daraus entsteht der Schlüssel. Anschließend löschen beide Parteien die geheimen Zutaten, aus denen sie die Teilgeheimnisse erzeugt haben. Ohne diese Zutaten lässt sich der Schlüssel nicht erneut berechnen.

Das ist auch für die Praktiken von Geheimdiensten relevant. Schwenk erklärt: „Geheimgerichte in den Vereinigten Staaten können Firmen zwingen, Schlüssel herauszugeben, mit denen die Daten ihrer Kunden chiffriert sind." Die Geheimdienste können so tonnenweise verschlüsselte Informationen aufzeichnen und auf Halde legen; wenn sie Einblick benötigen, besorgen sie sich von den Firmen den Schlüssel und dechiffrieren die gespeicherten Daten. „Große Firmen wie Google oder Amazon wollen das aber nicht", so Schwenk. Mit dem Diffie-Hellmann-Verfahren wird es nicht mehr möglich sein, Daten aus der Vergangenheit zu entschlüsseln. Denn die geheimen Zutaten, aus denen der Schlüssel erzeugt wird, werden gelöscht, sobald sie nicht mehr gebraucht werden. „So können Geheimdienste nur noch von jetzt bis in die Zukunft abhören", sagt der Bochumer Wissenschaftler, „aber nicht mehr in die Vergangenheit."

Der oben beschriebene Angriff ist nur ein Beispiel dafür, wie das RUB-Team sich mit der Sicherheit von TLS beschäftigt hat. Dr. Juraj Somorovsky, Mitarbeiter am Lehrstuhl für Netz- und Datensicherheit, war zum Beispiel an dem Drown-Angriff beteiligt, der im März 2016 Aufsehen erregte. Er und seine Kollegen umgingen die Sicherheitsmechanismen der aktuellen TLS-Version 1.2, indem sie sich über eine Vorgängerversion Zugang verschafften. Häufig sind auf Servern alte Versionen von SSL und TLS installiert, um möglichst viele verschiedene Browser unterstützen zu können; denn ältere Browser kommen oft nicht mit den neuen Sicherheitsprotokollen zurecht.

> „MAN HAT FESTGESTELLT, DASS DAS GESAMTE DESIGN SCHLECHT IST."

Über Schwachstellen in den veralteten Protokollen konnten die Forscher beim Drown-Angriff die aktuellen TLS-Sicherheitsmechanismen aushebeln. Auf ähnlichem Wege gelang es einem anderen Team vom Lehrstuhl für Netz- und Datensicherheit, digitale Signaturen in der aktuellen TLS-Version 1.2 zu fälschen.

So trugen die RUB-Forscher dazu bei, dass die Transport Layer Security nun überarbeitet wird. „Der Anstoß dazu waren allerdings die vielen Angriffe auf die Verschlüsselung, nicht auf die Schlüsselaushandlung", berichtet Jörg Schwenk. Jedes halbe Jahr habe es jemand geschafft, die TLS-Verschlüsselung auf anderem Wege zu brechen. Schwenk: „Da hat man festgestellt, dass das gesamte Design schlecht ist."

Sicherheitsbedenken sind aber nicht der einzige Grund für den neuen TLS-Standard. Der Konzern Google setzte sich zum Beispiel für ein neues Verfahren für die Schlüsselaushandlung ein, weil ihm der aktuelle Handshake schlicht zu langsam ist. Jörg Schwenks Motivation, sich in den Prozess einzubringen, ist eine ganz andere. Um Geld geht es jedenfalls nicht. „Ich möchte relevante Forschung machen, die Impact hat", sagt er. So wie seine Arbeiten zur Transport Layer Security, die nun direkt in die praktische Anwendung münden.

Text: jwe, Fotos: rs

Am Puls der Zeit arbeiten – mit IT-Sicherheitslösungen von Rohde & Schwarz

Wo immer auf der Welt kommuniziert wird – Geräte und Systeme von Rohde & Schwarz machen dies oft erst möglich. Wussten Sie beispielsweise, dass der Mobilfunk, wie man ihn heute kennt, erst ab 1992 mit dem GSM-Systemsimulator von Rohde & Schwarz möglich wurde und weltweit Smartphones mit Hilfe von Rohde & Schwarz Messtechnik entwickelt, typgeprüft und produziert werden? Der Elektronikkonzern ist führender Lösungsanbieter in den Arbeitsgebieten Messtechnik, Rundfunk- und Medientechnik, Sichere Kommunikation sowie Funküberwachungs- und Funkortungstechnik.

Seit Februar 2016 ergänzt die Rohde & Schwarz Cybersecurity GmbH das Produktportfolio des Konzerns um das Arbeitsgebiet der Cyber-Sicherheit mit technisch führenden Lösungen für die Informations- und Netzwerksicherheit. Das Portfolio umfasst hochsichere Verschlüsselungslösungen, Next-Generation-Firewalls sowie Software für Netzwerkanalyse und Endpoint-Security. Ein spannendes Aufgabenumfeld – das findet auch Clemens Schulz, Systementwickler bei der Rohde & Schwarz Cybersecurity GmbH am Standort Bochum: „Hier arbeite ich an topaktuellen Themen in einem sehr praktischen Umfeld. Die Produkte, die wir gemeinsam entwickeln, treffen den Nerv der Zeit und helfen unseren Kunden in der IT-Sicherheit einen Schritt voraus zu sein."

Das Unternehmen bietet eine familiäre Umgebung und ist nicht den Einflüssen der Börse ausgesetzt. Das alles schafft viel Stabilität und vor allem: viel Freiraum für alle Mitarbeiterinnen und Mitarbeiter. Dies ist auch fest in der Unternehmenskultur verankert. Darüber hinaus bietet Rohde & Schwarz ein großes Spektrum an attraktiven Sozial- und Gesundheitsleistungen und ein umfangreiches Weiterbildungsangebot. Flexible Arbeitszeiten sorgen für eine optimale Work-Life-Balance. „Aus meiner Sicht finden die Mitarbeiter hier eine gute Verbindung zwischen Privat- und Berufsleben. Wir können uns unsere Zeit außerhalb der Kernarbeitszeit selbst einteilen," so Alexandra Weiß, Projektleiterin in Leipzig. Gute Bedingungen für einen Berufsstart, oder?

Weitere Informationen finden Sie auch auf der Rohde & Schwarz Karrierewebsite:
www.careers.rohde-schwarz.com

WIR FORSCHEN

Im Horst-Görtz-Institut für IT-Sicherheit laufen zahlreiche drittmittelfinanzierte Projekte. Die folgende Liste gibt einen Einblick in die Vielfalt der Forschungsthemen und Fördermittel, die die IT-Experten der RUB erfolgreich eingeworben haben.

FÖRDERUNG DURCH DEN EUROPÄISCHEN FORSCHUNGSRAT (ERC)

ERC Starting Grant: BASTION. Leveraging Binary Analysis to Secure the Internet of Things
03/2015 – 02/2020
Thorsten Holz

ERC Consolidator Grant: Efficient Resource Constrained Cryptography
11/2014 – 10/2019
Eike Kiltz

ERC Starting Grant: FSC. Fast and Sound Cryptography
2012 – 2017
Alexander May

FÖRDERUNG DURCH DIE DEUTSCHE FORSCHUNGSGEMEINSCHAFT (DFG)

DFG-Graduiertenkolleg: UbiCrypt
10/2012 – 03/2017
Markus Dürmuth, Sebastian Faust, Tim Güneysu, Thorsten Holz, Eike Kiltz, Dorothea Kolossa, Kerstin Lemke-Rust, Gregor Leander, Alexander May, Christof Paar, Christina Pöpper, Jörg Schwenk, Hans Ulrich Simon

DFG SPP 1736: Big Data
11/2015 – 10/2018
Eike Kiltz

Anwendungsspezifische Block Chiffren mit einem Fokus auf die Lineare Abbildung
03/2016 – 02/2019
Gregor Leander

Heisenbergprofessur: Symmetrische Kryptographie
05/2015 – 04/2018
Gregor Leander

Emmy-Noether-Projekt: LTS. Long Term Security
2010 – 2015
Christopher Wolf

Emmy-Noether-Projekt: Beyond Black-box Cryptography
04/2016 – 03/2021
Sebastian Faust

Tight Reductions in Cryptography
10/2015 – 09/2017
Tibor Jager

Implementierungsaspekte alternativer asymmetrischer Kryptoverfahren
10/2015 – 09/2017
Tim Güneysu

Strukturierte probabilistische Modelle für die audiovisuelle Spracherkennung
05/2015 – 03/2017
Dorothea Kolossa

FÖRDERUNG DURCH BUND UND LAND NRW

Secure-IP. Kryptographisch und physikalisch sichere IP-Technologie für FPGA-basierte Systeme
09/2011 – 08/2014
Tim Güneysu

iAID. innovative Anomaly- and Intrusion-Detection
03/2012 – 08/2014
Thorsten Holz

JSAgents. Schutz gegen Internet-Angriffe durch mobile JavaScript-Agenten
04/2012 – 03/2014
Thorsten Holz, Jörg Schwenk

iTES. Innovative Trustworthy Endpoint Security
03/2012 – 08/2014
Thorsten Holz

SASER. Safe and Secure European Routing
08/2012 – 07/2015
Thorsten Holz

PROPHYLAXE. Security for the Internet of Things
03/2013 – 08/2015
Christof Paar

UNIKOPS. Universell konfigurierbare Sicherheitslösung für Cyber-Physikalische Systeme
02/2013 – 02/2016
Christof Paar

nrw.uniTS-Wiss
07/2015 – 06/2018
Thorsten Holz

BERCOM. Ausfallsicherheit von kritischen Infrastrukturen unter Nutzung von gesicherter LTE-Kommunikation
09/2015 – 08/2018
Christina Pöpper, Thorsten Holz

BDSec. Big Data Security
04/2015 – 03/2018
Thorsten Holz

VERTRAG. Vertrauenswürdiger Austausch geistigen Eigentums in der Industrie
03/2015 – 02/2018
Jörg Schwenk

Cyber-Safe. Schutz von Verkehrs-, Tunnel- und ÖPNV-Leitzentralen vor Cyberangriffen
02/2015 – 01/2018
Thorsten Holz

OpenC3S. Open Competence Center for Cyber Security
10/2011 – 09/2017
Jörg Schwenk, Christof Paar

INSPECT. Organisierte Finanzdelikte – methodische Analysen von Geld-, Daten- und Know-How-Flüssen
11/2014 – 10/2016
Christof Paar

Photon FX². Photonische Fehler- und Angriffsanalyse von Sicherheitsstrukturen und Sicherheitsfunktionen
07/2013 – 06/2016
Christof Paar

FÖRDERUNG DURCH DAS BUNDESMINISTERIUM FÜR WIRTSCHAFT UND TECHNOLOGIE (BMWI)

SecMobil. Secure E-Mobility
2012 – 2014
Georg Borges, Tim Güneysu, Thorsten Holz, Christof Paar, Jörg Schwenk

SkIDentity
2012 – 2015
Jörg Schwenk

FÖRDERUNG DURCH DIE EUROPÄISCHE UNION

ECRYPT-CSA
03/2015 – 02/2018
Eike Kiltz

EDIVIDE. European Digital Virtual Design Lab
10/2011 – 09/2014
Kerstin Lemke-Rust

ECRYPT-NET. European Integrated Research Training Network on Advanced Cryptographic Technologies for the Internet of Things and the Cloud (EU ITN)
03/2015 – 02/2019
Tim Güneysu, Eike Kiltz, Alexander May, Christof Paar

SAFECrypto. Secure Architectures of Future Emerging Cryptography (EU RIA)
01/2015 – 12/2018
Tim Güneysu

PQCRYPTO. Post-Quantum Cryptography for Long-Term Security (EU RIA)
03/2015 – 02/2018
Tim Güneysu, Christof Paar

ICanHear. Improved Communication through Applied Hearing Research
01/2013 – 01/2017
Dorothea Kolossa

TWO!EARS
12/2013 – 11/2016
Dorothea Kolossa

FÖRDERUNG DURCH DIE ALEXANDER-VON-HUMBOLDT-STIFTUNG

Sofja Kovalevskaja Award: Cryptosystems Beyond the Next Generation
09/2010 – 10/2015
Eike Kiltz

FÖRDERUNG DURCH DIE GERMAN ISRAELI FOUNDATION

Secure Encryption in the Presence of Strong Adversaries
2013 – 2015
Eike Kiltz

FÖRDERUNG DURCH DIE HORST-GÖRTZ-STIFTUNG

Identitätsmanagement im Cloud Computing
12/2012 – 11/2015
Georg Borges, Jörg Schwenk, Brigitte Werners

WEITERE PROJEKTE

Secunet AG: Quantencomputer-resistente Kryptographie
02/2013 – 08/2014
Alexander May

REDAKTIONSSCHLUSS

(Bildquelle: Archivo del Nacionalismo (Artea), AN GE 65-20)

Dieses verschlüsselte Telegramm wurde im Spanischen Bürgerkrieg am 7. Juli 1936 vom Bilbao nach Madrid geschickt. Den Code knackte Luis Alberto Benthin Sanguino während seiner Masterarbeit 2013 an der RUB. Als Bolivianer, der sich mit klassischer Kryptanalyse beschäftigte, war er prädestiniert dafür, weil er auch der spanischen Sprache mächtig ist.

Auf das Telegramm stieß Historiker Dr. Ingo Niebel während seiner Forschungen über das Baskenland und den Spanischen Bürgerkrieg. Er ließ es befreundeten Wissenschaftlern am Bochumer Horst-Görtz-Institut für IT-Sicherheit zukommen, die es zum Gegenstand einer Masterarbeit machten. Die Ergebnisse veröffentlichte der Absolvent in „Cryptologia“, einer führenden Fachzeitschrift für historische Chiffren.

IMPRESSUM

HERAUSGEBER: Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Abteilung Wissenschaftskommunikation, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, Fax: 0234/32-14136, rubin@rub.de, http://rubin.rub.de

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Raffaela Römer (rr)

FOTOGRAFIE: Roberto Schirdewahn (rs), Offerkämpe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de

COVERFOTO: Roberto Schirdewahn

WEBAUFTRITT: Andreas Rohden, Abteilung Markenbildung, Dezernat Hochschulkommunikation der RUB

GRAFIK, LAYOUT UND SATZ: VISUELL MARKETING GMBH, Springorumallee 2, 44795 Bochum, Tel.: 0234/459803, www.visuell-marketing.com

DRUCK: VMK Druckerei GmbH, Faberstraße 17, 67590 Monsheim, Tel:. 06243/909-110, www.vmk-druckerei.de

AUFLAGE: 2.700

ANZEIGENVERWALTUNG UND -HERSTELLUNG: VMK GmbH & Co. KG, Faberstraße 17, 67590 Monsheim, Tel.: 06243/909-0, www.vmk-verlag.de

BEZUG: Die Sonderausgabe 2016 des Wissenschaftsmagazins RUBIN ist erhältlich im Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum, Gebäude ID. Das Wissenschaftsmagazin RUBIN erscheint zweimal im Jahr.

ISSN: 0942-6639

ZEITGEMÄSSER SCHUTZ GEGEN CYBERCRIME.
WILLKOMMEN IN SICHERHEIT.

Beratung durch einen starken Partner
Seit einigen Jahren sind Unternehmen existenziellen Bedrohungen ihrer IT-Infrastruktur ausgesetzt. Gefahren, die nicht nur eine technische Lösung erfordern, sondern auch Folgen für Organisation und Strukturen von Unternehmen haben. Als Experten mit mehr als zwei Jahrzehnten Erfahrung helfen wir Ihnen, praktische, realitätsnahe und umsetzbare Lösungen zu finden. So halten Sie Bedrohungen dauerhaft in Schach.

Wer einfach abwartet, verliert
Ob mit Penetrationstests von außen oder mit Analysen von innen: Wir ermitteln den Stand der Bedrohungen Ihrer IT-Netzwerke gründlich und schonungslos. Dank unserer IT Security Analysen erfahren Sie, wo Sie sich besser schützen müssen. Wir erklären Ihnen, wie sich Sicherheitslücken beheben lassen und helfen Ihnen bei der Umsetzung notwendiger Maßnahmen. Denn Angriff ist die beste Verteidigung.

Karriere @ r-tec
Wir wachsen schnell und arbeiten in einer hoch dynamischen Branche. Die besten Voraussetzungen für einen spannenden Job mit vielen Entwicklungsmöglichkeiten.

kununu TOP COMPANY www.kununu.com VON MITARBEITERN EMPFOHLEN!

WWW.R-TEC.NET

r-tec IT SECURITY

exceet
SECURE SOLUTIONS

HOUSTON WE SOLVED A PROBLEM

Seit über 10 Jahren unterstützen wir Unternehmen bei der Konzeption und Umsetzung ihrer Anforderungen in der IT-Sicherheit.

Mehr erfahren: www.exceet-secure-solutions.de/it-security

- Public Key Infrastructures
- Hardware Security Modules
- Trusted Services
- Embedded Security

Auf in neue Sphären

Sie wollen in die unendlichen Weiten der IT Security vordringen?
Wir suchen stets motivierte Teamplayer für Expeditionen in Sachen IT-Sicherheit, Embedded Security, PKI, Datenschutz und mehr.

www.exceet-secure-solutions.de/unternehmen/karriere