RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE

IT-SICHERHEIT

Wie sich künstlich erzeugte Bilder verraten

Drei harte Nüsse für Quantencomputer

Start-up: Fit für die neue Mobilfunkgeneration

#33 Jahrgang

Sonderausgabe 2023

Nachgehackt – Der Bochumer Podcast zu IT Security

Die Welt wird immer digitaler und IT-Sicherheit auch im Alltag immer wichtiger. Im Podcast „Nachgehackt“ spricht Moderator Henrik Hanses mit Expertinnen, Experten und anderen spannenden Gästen über unterschiedliche Aspekte der IT Security – und zwar so, dass es auch für Laien verständlich ist.

Der Podcast wird präsentiert von Cube 5 – Creating Security, dem Horst-Görtz-Institut für IT-Sicherheit an der Ruhr-Universität-Bochum, dem Exzellenzcluster CASA, der PHYSEC GmbH, der Bochum Wirtschaftsentwicklung sowie eurobits e. V.

„Nachgehackt“ gibt es bei Spotify, Apple Podcast und überall dort, wo es Podcasts gibt. Als Video-Podcast ist „Nachgehackt“ bei Youtube zu sehen.

EDITORIAL

Foto: ms

IT-Sicherheit ist als fester Bestandteil unseres digitalen Alltags nicht mehr wegzudenken. Doch das war nicht immer so: Vor genau 20 Jahren hielten viele Expert*innen die Inhalte unseres Fachbereichs noch für Nischen-Themen. Damals, 2003, wurde solchen Voraussagen zum Trotz das Horst-Görtz-Institut für IT-Sicherheit an der Ruhr-Universität Bochum gegründet und der erste deutsche Studiengang der IT-Sicherheit etabliert.

Seitdem hat sich vieles verändert. Früher hörten wir nur von vereinzelten Angriffen unprofessioneller Hacker*innen auf Privatpersonen. Heute lesen wir jeden Tag neue Schlagzeilen über Cyberangriffe auf Ämter, Unternehmen oder gar kritische Infrastrukturen. Seit Edward Snowden wissen wir, wie real wir alle der Gefahr von Überwachung ausgesetzt sind. Der Schutz vor diesen Angriffen ist damit essenziell für unsere Gesellschaft und Wirtschaft.

Wir in Bochum forschen an den Grundlagen dieser Sicherheit. In diesem Heft erfahren Sie, was unsere Wissenschaftler*innen sich einfallen lassen, um dafür immer einen Schritt voraus zu sein. Denn das ist und war in der IT-Sicherheit immer schon das A und O: nicht nur schneller zu sein, sondern auch kreativer als der Konterpart.

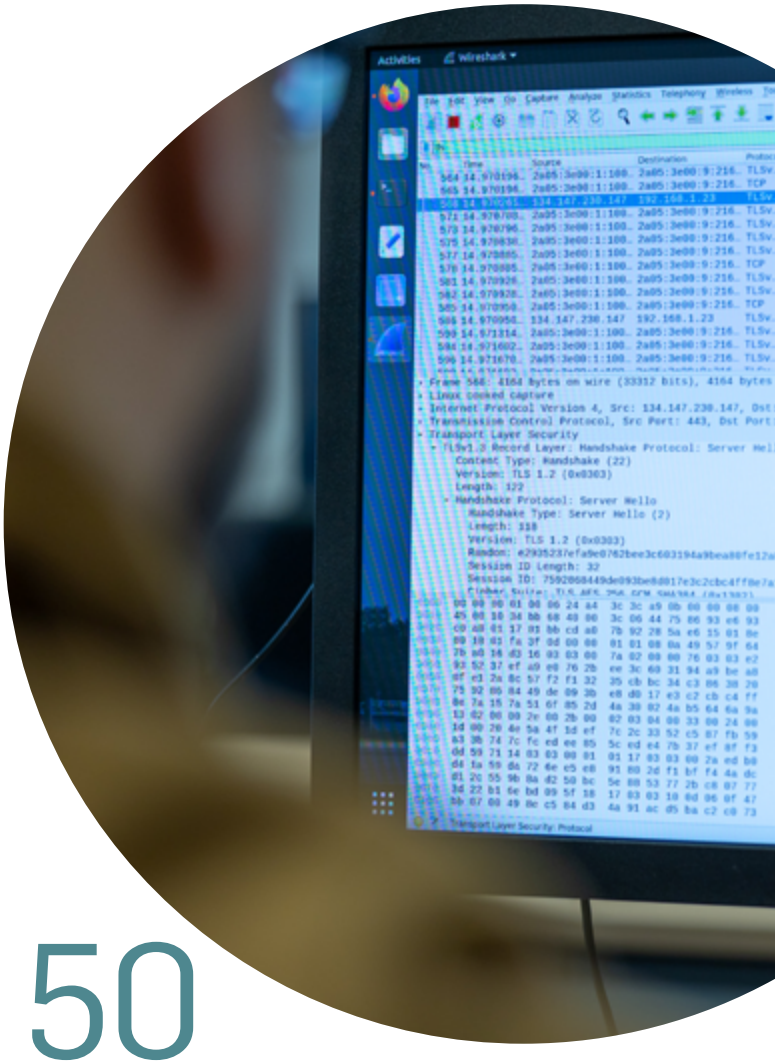
Dazu helfen uns beispielsweise intelligente Affen (Seite 28), mathematische Jägerzäune (Seite 10) oder Löcher in einem Computergehäuse (Seite 44) – was es damit alles genau auf sich hat: Lesen Sie selbst. Viel Vergnügen!

Ihr Eike Kiltz,
Sprecher des Exzellenzclusters CASA
am Horst-Görtz-Institut für IT-Sicherheit

RUBIN IM NETZ
Alle Artikel dieser Sonderausgabe:
→ **news.rub.de/rubin-it-sicherheit-2023**

INHALT

14



50

„ENDLICH KANN ICH MAL ERKLÄREN, WOFÜR MEINE FORSCHUNG GUT IST.“

Eike Kiltz


CYB

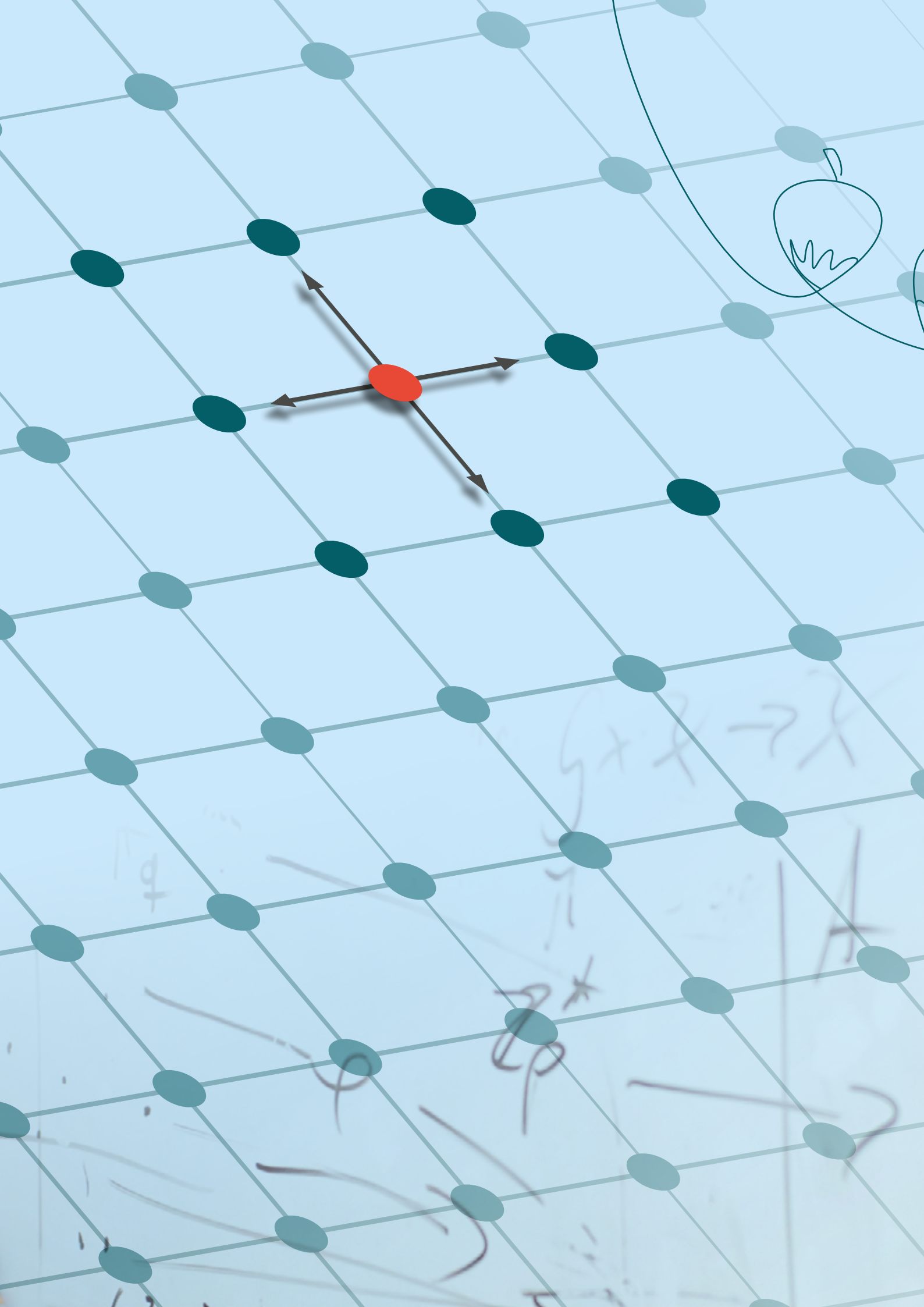
KUNSTWERK „APES“

Auf den ersten Blick wirken Kunst und IT-Sicherheit wie zwei vollkommen gegensätzliche Welten. Mitglieder des Exzellenzclusters CASA, des Horst-Görtz-Instituts für IT-Sicherheit und des Max-Planck-Instituts für Sicherheit und Privatsphäre haben im Rahmen einer Künstlerresidenz erkundet, wie sich die Disziplinen gegenseitig bereichern können. Zwei Monate lang tauschten sich die Wissenschaftlerinnen und Wissenschaftler intensiv mit dem Medienkünstler Marco Barotti zu Forschungsthemen und Zukunftsvisionen aus. Davon ausgehend schuf Barotti das Kunstwerk „APES“, das hier bei einer Ausstellung in Seoul zu sehen ist. Die kinetischen Klangskulpturen bieten einen außergewöhnlichen Blick auf IT-Sicherheit, Datenschutz, Überwachung und Nachhaltigkeit. (Foto: Marco Barotti)

SUPPLIES

DIS/PLAY

IT-Sicherheit erlebbar machen – das ist das Ziel des Kunstwerks „DIS/PLAY“. Der Künstler Ralf Baecker hat es für das Exzellenzcluster „CASA – Cyber Security in the Age of Large-Scale Adversaries“ geschaffen. Die Installation erstreckt sich über die Forschungs- und Arbeitsbereiche der Wissenschaftlerinnen und Wissenschaftler im Gebäude MC auf dem Campus der Ruhr-Universität Bochum. Im gesamten Gebäude verteilte Displays reagieren auf vorbeigehende Besucher mit Nachrichten, die das Thema Überwachung und Privacy auf humorvolle Weise kommentieren. Gleichzeitig werden die Nachrichten durch das ganze Haus geschickt und schließlich auf einer großen Installation im Open Space angezeigt. So verwandelt das Kunstwerk das Gebäude in einen riesigen verteilten Computer und Bildschirm: Bits und Bytes fließen durch das Gebäude, Schwärme von Zeichen und Zahlen bewegen sich durch Gänge und Räume. (Foto: RUB, Kramer)



DREI HARTE NÜSSE FÜR **QUANTENCOMPUTER**

Bochumer Algorithmen werden zum weltweiten Standard für die sichere Verschlüsselung im Zeitalter des Quantencomputings. Sie kommen gerade noch rechtzeitig.

i QUANTENCOMPUTER

Herkömmliche Computer codieren Informationen in Form von Bits, die die Werte 0 und 1 annehmen können. Quantencomputer hingegen arbeiten mit Quantenbits. Sie können gleichzeitig die Zustände 0 und 1 besitzen. Das erlaubt es ihnen, gewisse mathematische Aufgaben wesentlich effizienter zu lösen als herkömmliche Rechner. Fachleute sprechen bei diesem Rechenvorteil von der Quantenüberlegenheit. Für derzeit existierende Computer, die Quantentechnik einsetzen, ist diese Überlegenheit jedoch noch nicht zweifelsfrei bewiesen worden. Die Geräte können die derzeit gängigen Verschlüsselungsverfahren noch nicht knacken.

Das Gitterproblem als Basis neuer Algorithmen: 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.

Es ist noch früh am Morgen und bitterkalt. Gleich geht es los zur Arbeit. Zum Glück lässt sich das Auto über die Handysteuerung vorheizen. Auch vereiste Türschlösser gehören der Vergangenheit an. Öffnen kann man den Wagen mühelos über den Fingerabdruckscanner. Dann genügt ein kurzer Sprachbefehl, schon geht das Radio an. Der Motor startet, das Head-up-Display leuchtet auf. Los geht die Fahrt, die sich auch im etwas müden Zustand dank Spurhaltesystem sicher anfühlt.

Ein modernes Auto ist eigentlich eine Art Computer. Und wie bei allen anderen Computern können Angreifer sich potenziell Kontrolle über die Bordsysteme verschaffen. Daher sollte die Elektronik in smarten Autos vor Cyberattacken geschützt sein. Und zwar nicht nur vor den Angriffen, die jetzt schon möglich sind, sondern auch vor denen von morgen. Denn ein Auto hat eine lange Lebensdauer. Fahrzeuge, die heute vom Band rollen, werden eventuell lange genug halten, um das Zeitalter der Quantencomputer mitzuerleben.

„Quantencomputer werden einige der gängigen Verschlüsselungstechniken problemlos brechen können“, weiß Prof. Dr. Eike Kiltz. Er leitet den Lehrstuhl für Kryptografie und ist einer der Sprecher des Exzellenzclusters CASA (Cyber Security in the Age of Large-Scale Adversaries) am Horst-Görtz-Insitut für IT-Sicherheit. Damit die Technik von heute auch in Zukunft sicher ist, hat Kiltz zusammen mit Kolleginnen und Kollegen neue Verfahren entwickelt, die Daten vor Angriffen mit Quantencomputern schützen. Maßgeblich beteiligt waren die CASA-Mitglieder Prof. Dr. Tanja Lange, Prof. Dr. Peter Schwabe und Prof. Dr. Daniel Bernstein.

Das Team setzte sich in einem hochkompetitiven Wettbewerb durch, den das US-amerikanische National Institute of Standards and Technology, kurz NIST, 2016 ausgerufen hatte. NIST-Wettbewerbe gab es bereits zu verschiedenen Themen, mit dem Ziel, bestmögliche Lösungen für drängende Probleme der IT-Sicherheit zu finden. Forschungsgruppen weltweit können ihre Lösungsvorschläge einreichen; in einem mehrere Jahre dauernden, schrittweisen Verfahren werden dann die besten Ansätze herausgefiltert. Im Rahmen des 2016er Wettbewerbs zu sicheren Algorithmen gegen Quantencom- ▸

puter-Angriffe wurden 82 Vorschläge eingereicht. Vier davon sollen nun standardisiert werden, wie das NIST 2022 verkündete. Von diesen vier Gewinnerverfahren stammen drei aus dem Exzellenzcluster CASA.

Verfahren, die beim NIST-Wettbewerb gewonnen haben, haben sich in der Vergangenheit stets weltweit durchgesetzt. Es ist also davon auszugehen, dass die quantencomputersicheren CASA-Algorithmen künftig auf dem ganzen Globus zum Verschlüsseln und digitalen Signieren genutzt werden. Die NSA, der größte Auslandsgeheimdienst der Vereinigten Staaten, empfiehlt der US-Regierung bereits jetzt die Verfahren Crystals-Kyber und Crystals-Dilithium zu verwenden, an denen Eike Kiltz und Peter Schwabe beteiligt waren.

Crystals-Kyber dient der Verschlüsselung – etwa von Daten, die per E-Mail verschickt werden oder von Kreditkarteninformationen, die fürs Onlineshopping hinterlegt werden. Crystals-Dilithium ist zur Absicherung von Authentifizierungsprozessen gedacht, kommt also dann zum Einsatz, wenn ein Mensch oder ein Objekt seine Identität beweisen muss. So muss beispielsweise bei einem Update des Betriebssystems die Software beweisen, dass sie ein offizielles Produkt des Herstellers ist und nicht von einem Hacker stammt.

Mit Crystals-Kyber und Crystals-Dilithium – Fans von Star Wars und Star Trek werden erkennen, dass die Namen eine Hommage an die Filme sind – ist Eike Kiltz' Forschung direkt in die Anwendung gemündet. Eine ungewöhnliche Erfahrung für ihn. Denn üblicherweise spielt sich die Arbeit des Informatikers am äußersten Rand der Theorie ab. Nun werden die Algorithmen des CASA-Teams in der ganzen Welt zum Einsatz kommen. „Wir tragen eine große Verantwortung", ist Kiltz sich bewusst und freut sich zugleich: „Endlich kann ich mal erklären, wofür meine Forschung gut ist."

Dabei geht es im Kern seiner Arbeit um sehr abstrakte Fragen, sogenannte schwere mathematische Probleme. „Das sind Probleme, mit denen sich viele schlaue Köpfe in den vergangenen Jahrzehnten beschäftigt haben, ohne eine Lösung zu finden", erklärt er. Eines davon ist das Gitterproblem, das Crystals-Kyber und Crystals-Dilithium zugrunde liegt.

Um sich das Problem zu verdeutlichen, stellt man sich zunächst ein zweidimensionales Gitter vor, das an einer Stelle einen Nullpunkt besitzt. Überall dort, wo sich Linien kreuzen, befinden sich sogenannte Kreuzungspunkte. Die Frage lautet: Welcher Kreuzungspunkt liegt am nächsten beim Nullpunkt? Sie ist für ein zweidimensionales Gitter einfach zu beantworten. Je mehr Dimensionen man hinzunimmt, desto schwieriger wird es. Ab etwa 500 Dimensionen gibt es keine effiziente Lösung mehr für das Problem.

Die CASA-Algorithmen beruhen auf dem Gitterproblem in einer leicht vereinfachten Form: Gesucht wird nicht der nächstgelegene Kreuzungspunkt, sondern ein beliebiger Kreuzungspunkt, der sich in einem bestimmten Radius um den Nullpunkt befindet. Wenn ein Softwareupdate dem Betriebssystem beispielsweise beweisen möchte, dass es von einem offiziellen Softwarehersteller stammt, muss es nachweisen, dass es ein Geheimnis kennt – nämlich einen dieser Kreuzungspunkte in der Nähe des Nullpunkts.

Moderne Autos mit ihrer ganzen Elektronik sind Computer – und somit anfällig für Cyberattacken. Die Quantencomputer von morgen könnten in der Lage sein, heute gängige Verschlüsselungstechniken auszuhebeln. Daher ist es entscheidend, langlebige Technik wie Autos durch Algorithmen zu sichern, die den Attacken von morgen gewachsen sind.

Weil das Gitterproblem mathematisch andersartig ist als die Technik, auf der gängige Verschlüsselungen beruhen, werden Quantencomputer es genauso wenig lösen können wie herkömmliche Rechner. „Quantencomputer haben nur bei sehr bestimmten Aufgaben einen Vorteil", erklärt Eike Kiltz. Das ist zum Beispiel immer dann der Fall, wenn man eine Aufgabe als Periodenfinde-Aufgabe ausdrücken kann. Als Periode bezeichnet man den Abstand zwischen dem Auftreten gleicher Werte in einer Funktion. Stellt man sich eine Sinuskurve vor, so umfasst die Periode einen Berg und ein Tal der Kurve. Gäbe es einen leistungsfähigen Quantencomputer, dann könnte er die Periode einer beliebigen Funktion sehr schnell ermitteln.

Das wäre ein Problem für das gängige Verschlüsselungsverfahren namens RSA, das auf dem Problem der Primfaktorzerlegung basiert. Aufgabe bei dieser mathematischen Übung ist es, für eine Zahl mit mehreren hundert Stellen herauszufinden, welche zwei Primzahlen man miteinander multiplizieren müsste, um die Zahl zu erhalten. Mit herkömmlichen Rechnern ist diese Frage nicht effizient lösbar. Quantencomputer könnten das aber mühelos, weil man die Primfaktorzerlegung als Periodenfinde-Aufgabe beschreiben kann. Mit dem Gitterproblem geht das nicht. Daher ist es vor Quantencomputerangriffen sicher.

Ihre Verfahren Crystals-Kyber und Crystals-Dilithium haben die Bochumer Forschenden mittlerweile so weit opti-

„DIE ENTWICKLUNG KOMMT GERADE NOCH RECHTZEITIG.“

Eike Kiltz

Gemeinsam mit Kolleginnen und Kollegen hat Eike Kiltz neue quantencomputersichere Algorithmen entwickelt und damit einen mehrjährigen Wettbewerb gewonnen.

miert, dass sie in punkto Effizienz mit dem heute üblichen RSA-Verfahren mithalten können. Die neuen Verfahren sind sogar zwei- bis dreimal schneller als RSA, dafür brauchen sie 20- bis 30-mal so lange Chiffren. „Man braucht also etwas mehr Speicherplatz, dafür kann man einen kleineren Prozessor verwenden“, verdeutlicht Eike Kiltz.

Bis die Verfahren sich weltweit durchgesetzt haben, wird es aber noch ein wenig dauern. Zwei Jahre wird es brauchen, bis Crystals-Kyber und Crystals-Dilithium standardisiert sind. Die Implementierung, so schätzt Eike Kiltz, wird dann noch einmal fünf bis zehn Jahre erfordern. „Die Entwicklung kommt also gerade noch rechtzeitig“, sagt der Bochumer Forscher. Er geht davon aus, dass es in 10 bis 20 Jahren Quantencomputer geben könnte, die gängige Verschlüsselungsverfahren brechen können. Das klingt noch lange hin. „Aber man muss bedenken, dass zum Beispiel Geheimdienste verschlüsselte Daten speichern, die auch in Zukunft noch interessant sein können – und in Zukunft können sie sie vielleicht mithilfe von Quantencomputern entschlüsseln“, gibt Kiltz ein Beispiel. Und auch die eingangs erwähnten Autos, die mit allerhand Elektronik bestückt in den kommenden Jahren auf die Straßen entlassen werden, werden vielleicht immer noch herumfahren, wenn Quantencomputer längst Wirklichkeit geworden sind.

Text: jwe, Fotos: ms

i DRITTES GEWINNERVERFAHREN

Nicht nur mit Crystals-Kyber und Crystals-Dilithium, sondern auch mit dem Algorithmus Sphincs+ hat sich das CASA-Team im NIST-Wettbwerb um quantensichere Verfahren durchgesetzt. Sphincs+ kann zum sicheren Erstellen von digitalen Signaturen genutzt werden. Es basiert auf Hash-Funktionen. Hash-Funktionen erzeugen aus einem beliebigen Input, etwa einer Datei, einen völlig anders aussehenden Output. Würde man eine Kleinigkeit an der Eingangsdatei verändern, würde die resultierende Ausgabe trotzdem ganz anders aussehen. So verschleiern die Hash-Funktionen die Struktur der Daten. Das Verfahren wurde maßgeblich von CASA-Mitglied Peter Schwabe entwickelt, der am Bochumer Max-Planck-Institut für Sicherheit und Privatsphäre forscht.

Informationstechnik

APP-ZEPTIERT?

Viele Länder haben mithilfe von Corona-Apps versucht, das Infektionsgeschehen einzudämmen. Sie bringen aber nur etwas, wenn die Menschen sie auch nutzen. Neue Umfragen zeigen, welche Faktoren die Akzeptanz beeinflussen.

Der Ausbruch des Sars-Cov-2-Virus führte in vielen Ländern der Welt dazu, dass Smartphone-Apps eingeführt wurden, um Kontaktverfolgungen möglich zu machen, Infektionsketten schneller zu unterbrechen und so das Pandemiegeschehen besser kontrollieren zu können. Auch die Bundesregierung appellierte an die Bürgerinnen und Bürger, die sogenannte Corona-Warn-App zu installieren, um sich und andere über Kontakte mit Infizierten zu informieren. Die Effizienz solcher Apps beruht dabei wesentlich auf der Akzeptanz und damit der Verbreitung der App. Was motiviert Menschen dazu, Corona-Apps zu nutzen? Und was hält sie davon ab? Ein Forschungsteam am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität um Prof. Dr. Markus Dürmuth und Dr. Christine Utz hat ebendiese Fragen rund 7.000 Menschen auf drei Kontinenten gestellt.

Um herauszufinden, welche Faktoren die Entscheidung für oder gegen eine App maßgeblich bestimmen, griffen Utz und Dürmuth in ihren Umfragen auf eine besondere Forschungsmethode zurück, das sogenannte Vignetten-Design. Es findet vor allem in der Marktforschung häufig Anwendung. „Vignetten sind kurze, fiktive Szenarien, die den Befragten vorgelegt werden und zu denen sie dann Fragen beantworten müssen. In unserem Fall geht es um fiktive Corona-Apps mit unterschiedlichen Eigenschaften, die auf realen Apps beruhen“, erklärt Utz. „Bei Corona-Apps ist der Kontext, in dem sie genutzt werden, entscheidend“, hebt Dürmuth hervor. „Welchem Zweck dient die App? Welche Arten von Daten werden erhoben und wie lange werden sie gespeichert? Wer hat Zugriff auf die Daten? Wir wollten all diese Dimensionen und Faktoren berücksichtigen“, so der Informatiker.

Insgesamt acht App-Funktionalitäten – etwa Zweck der App oder Dauer der Datenspeicherung – mit bis zu 16 unterschiedlichen Auswahloptionen ließen die Forschenden in ihre Studien einfließen. Aus der Kombination ergaben sich ▸

Die Corona-Warn-App hat über Kontakte mit Infizierten informiert.


CORONA
Risiko-Ermittlung aktiv
Niedriges Risiko
Begegnungen mit niedrigem Risiko an 1 Tag
Am 14.03.2023
Aktualisiert: Heute, 13:45 Uhr
Tests erfassen und andere warnen
Selbsttest, PCR- und Schnelltest
Warnen Sie andere, wenn Sie positiv getestet sind, oder fordern Sie Ihr digitales COVID-Testzertifikat an. Finden Sie Teststellen in Ihrer Umgebung.
Weiter
Bestätigte Neuinfektionen
Bundesweit
Zertifikate
Scannen
Check-in
Tagebuch

Corona-Apps sollen dazu beitragen, das Infektionsgeschehen einzudämmen.

rund 50.600 Szenarien. Eines lautete beispielsweise: „Stellen Sie sich eine App vor, die der Quarantänekontrolle dient und dafür Ihren Aufenthaltsort stündlich an das Gesundheitsamt und die örtliche Polizei schickt." Den teilnehmenden Personen wurden jeweils zehn solcher Szenarien vorgelegt. Dann mussten sie angeben, mit welcher Wahrscheinlichkeit sie die beschriebenen Apps nutzen würden. „Der Vorteil dieses Designs ist, dass man aus den Daten am Ende den Einfluss verschiedener Faktoren auf die Gesamtakzeptanz herausrechnen kann und präzise beschreiben kann, welche Faktoren die Akzeptanz stark beeinflussen und welche nicht", fasst Dürmuth zusammen.

Für die ersten Befragungen im Sommer 2020 adressierten die Forschenden jeweils 1.000 Teilnehmende aus China, den USA und Deutschland. „Da man in China, also im Ursprungsland der Pandemie, insgesamt routinierter mit staatlichen Apps umgeht, fanden wir dieses Zielland spannend", erklärt Dürmuth. Auch Deutschland war als Untersuchungsland eine naheliegende Wahl. „Im Hinblick auf zum Beispiel Privacy-Erwartungen stand Deutschland stellvertretend für das damalige europäische Vorgehen", so Dürmuth weiter. „Die USA waren zum Zeitpunkt unserer ersten Studie massiv betroffen. Wir haben erwartet, dass die Menschen in den USA die Nutzung der Apps anders einschätzen, zum Beispiel, dass ihnen der Schutz ihrer Privatsphäre weniger wichtig wäre", begründet Utz die Wahl.

Zum Zeitpunkt der ersten Umfrage war die Pandemie in den Ländern unterschiedlich weit fortgeschritten – und ebenso die Nutzung und Verbreitung von Corona-Apps. „In China waren Apps von WeChat und Alipay mit zusätzlichen Gesundheits-Plugins bereits im Umlauf. Etwa 60 Prozent gaben an, diese auch zu nutzen", erklärt Utz. Anders sah es zu dem Zeitpunkt in Deutschland und in den USA aus, wo noch keine oder wenige Apps auf dem Markt waren. „In den USA griffen rund sieben Prozent auf Gesundheits-Applikationen zurück; in Deutschland nutzten im Sommer 2020 etwa vier Prozent die Warn-App des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, NINA", so Dürmuth. Das änderte sich im Laufe eines Jahres, wie Nachfolgebefragungen im Winter 2020 und Frühjahr 2021 unter Teilnehmenden aus Deutschland und den USA ergaben. So nutzten Anfang 2021 bereits 43 Prozent aller Befragten in Deutschland eine App, mehrheitlich die Corona-Warn-App. Auch in den USA stiegen

> „DIE POSITIVEN ASPEKTE UND DER GESAMTNUTZEN ÜBERWIEGEN DIE SKEPSIS."
>
> Christine Utz

Christine Utz hat gemeinsam mit Kolleginnen und Kollegen analysiert, welche Faktoren die Akzeptanz von Corona-Apps beeinflussen.

die Zahlen, allerdings blieb die Nutzungsrate insgesamt über die drei Umfragerunden vergleichsweise niedrig. „Im Frühjahr 2021 gaben nur elf Prozent der Amerikanerinnen und Amerikaner an, eine App zu nutzen. Das erklären wir uns unter anderem damit, dass es keine einheitliche App-Lösung für alle Bundesstaaten gab“, so Utz.

Den starken Anstieg der Nutzung in Deutschland führen die Forschenden vor allem auf die bundesweite Verfügbarkeit der neuen Corona-Warn-App und ihre Verbreitung zurück. „Wer die App kennt, ist auch mehr bereit, sie zu nutzen“, resümiert Dürmuth. Außerdem, so hebt er hervor, habe es von vornherein, trotz aller Skepsis, eine grundsätzliche Bereitschaft zur Nutzung einer App gegeben. „Die positiven Aspekte und der Gesamtnutzen überwiegen die Skepsis“, so Utz. Tatsächlich, so belegen die Umfrageergebnisse in Deutschland und den USA, nahm die positive Wahrnehmung von Covid-19-Apps zu. In der dritten Befragungsrunde im Frühjahr 2021 waren bereits 294 von 1.000 Deutschen und 302 von 1.000 US-Amerikanerinnen und -Amerikanern davon überzeugt, dass es keine negativen Aspekte der Apps gebe. Dieses Ergebnis führen Utz und Dürmuth auch auf das Pandemiegeschehen während der Umfragezeiträume zurück. „Insbesondere die zweite Befragung fiel in eine Phase mit hohen Infektionszahlen und Lockdowns“, erklärt Utz.

Und dennoch: Unabhängig von der Verfügbarkeit der Apps und vom Pandemiegeschehen zeigte sich über den gesamten Befragungszeitraum, dass die Nutzungsbereitschaft auf allen Kontinenten maßgeblich vom Schutz der privaten Daten abhängt. „Die Frage, was mit meinen privaten identitätsbezogenen Daten passiert, hat einen großen Einfluss auf meine Bereitschaft, die App zu nutzen“, so Dürmuth. Bereits im Sommer 2020 gaben 292 von 1.000 Deutschen die Sorge um die Privatheit der Daten als Hauptgrund an, warum sie Corona-Apps nicht nutzen. In den USA traf das auf 337 der 1.000 Befragten zu, in China auf 179. Die Befürchtungen hatten über die drei Umfragerunden Bestand: Auch in der dritten Runde nahmen noch 226 von 1.000 Deutschen und 257 von 1.000 Befragten aus den USA die Apps als Eingriff in die Privatsphäre wahr und als einen wichtigen Grund, sie nicht zu nutzen. Außerdem fürchtete man die Überwachung durch den Staat: Diese Sorge äußerten in der ersten Befragungsrunde 174 Teilnehmende in Deutschland und 70 aus den USA.

Insbesondere die Empfängerinstitution spielt bei der Entscheidung für oder gegen eine App in allen Ländern eine zentrale Rolle. „Unsere Umfrage hat ergeben, dass das Vertrauen in Gesundheitsinstitutionen – in Deutschland etwa das RKI oder Universitäten – hoch ist. Hier stellt man die Daten eher zur Verfügung. Wenn der Empfänger aber ein privates Unternehmen, die breite Öffentlichkeit oder die Strafverfolgung ist, sieht das, je nach Land, unterschiedlich aus“, weiß Utz. In Deutschland reduziere die Aussicht, dass diese privaten Daten an Dritte, etwa die Polizei oder private Unternehmen geraten, deutlich die Bereitschaft, solche Apps zu nutzen. In China teile man seine Bewegungsdaten bereitwilliger mit der Öffentlichkeit, nur privaten Unternehmen stünde man skeptisch gegenüber. „Hier gehört es zum Alltag, personenbezogene Daten mit staatlichen Institutionen zu teilen“, so Utz. Insgesamt gilt für alle drei Länder: „Man ist eher gewillt, staatliche Gesundheitsapps für weniger invasive Zwecke zu nutzen, etwa zur Kontaktverfolgung oder zur Gewinnung von Informationen, als für invasive Zwecke, wie etwa die Quarantäneüberwachung“, so Dürmuth.

Was folgt daraus für die Weiterentwicklung von Apps? Utz und Dürmuth appellieren an die Architektinnen und Architekten künftiger, staatlicher Gesundheitsapps, die Sorge der Nutzerinnen und Nutzer um die Privatsphäre ernst zu nehmen. „Es muss ganz genau erklärt werden, wie die Apps konkret funktionieren, was sie leisten können und was nicht. Die Apps müssen transparent beschreiben, für welche Zwecke Daten gesammelt und gespeichert werden, wer diese erhält und welcher persönliche und gesellschaftliche Nutzen daraus resultiert“, resümieren die Forschenden.

Text: lb, Fotos: ms

Start-up

FIT FÜR DIE NEUE **MOBILFUNK-GENERATION**

5G kann jede Menge mehr als 4G. Die Firma Radix Security sorgt dafür, dass es keine Sicherheitslücken öffnet.

Wenn man sein Smartphone zückt, um schnell nach dem richtigen Weg zu suchen oder zu schauen, wann der nächste Bus fährt, ist meist sofort die Antwort da. Die Prozesse im Hintergrund laufen so schnell, dass man kaum auf den Gedanken kommt, dass es sie gibt. Aber es sind jede Menge Schnittstellen, die gesendete Daten überwinden müssen. Das Smartphone muss sich mit dem nächsten Mobilfunkmast verbinden. So ein Mobilfunkmast ist wiederum Teil eines deutschlandweiten Netzwerks, das von den großen Telekommunikationsunternehmen eingerichtet und betrieben wird. Auf diese Weise hat man als Endnutzer (fast) immer Empfang und kann sein Telefon ganz mobil nutzen.

Um solche Verbindungen immer und überall zu ermöglichen, egal ob mit dem aktuellen iPhone oder einem LTE Banana Phone von Nokia, müssen sich alle Beteiligten auf die gleichen Standards für die Kommunikation einigen. Das gilt nicht nur für deutsche Netze, sondern auch weltweit. Das sogenannte 3rd Generation Partnership Project, kurz 3GPP, ist die Organisation, die für die Aushandlung und Veröffentlichung der entsprechenden Standards zuständig ist.

Die Spezifikationen umfassen Tausende Seiten, die Dr. David Rupprecht besser kennt, als ihm manchmal lieb wäre. Ihm und seinen Kolleginnen und Kollegen am Lehrstuhl Systemsicherheit am Horst-Görtz-Institut für IT-Sicherheit kam es dabei besonders auf die kleinen und großen Fehler im Standard an. Denn solche Spezifikationsfehler wirken sich direkt auf die Sicherheit einer Verbindung aus und betreffen damit direkt jeden einzelnen Nutzer eines Netzes.

Und das ist erst der Anfang: Selbst, wenn die Spezifikation zu 100 Prozent wasserdicht wäre, fehlt immer noch der Schritt hin zur Implementierung. Dabei werden seitenweise Anweisungen als Grundlage verwendet, um Komponenten zu implementieren. „Anders gesagt: Wer Komponenten eines Mobilfunknetzes baut, der muss Tausende Seiten Text lesen, korrekt interpretieren, und dann auch noch in fehlerfreien Code umsetzen. Und als wäre das nicht schon Herausforderung genug, kommt auch noch die enorme Komplexität von Netzen und Komponenten hinzu", so Rupprecht. Und nimmt ▸

i FÖRDERUNG

Die Gründung von Radix Security wird gefördert von den Gründungsinkubatoren Cube 5 der Ruhr-Universität und Mercator Launch der Radboud Universiteit.

Wer sein Smartphone im Alltag nutzt, hinterfragt die Prozesse nicht, die im Hintergrund laufen.

man eine 100-prozentig sichere Implementierung an – haben wir dann vollständig abgesicherte Netze? „Leider reicht auch das noch nicht aus“, erklärt David Rupprecht. „Die verschiedenen Komponenten müssen in einem komplexen Setup miteinander interagieren. Hardware von verschiedenen Herstellern trifft aufeinander, das Zusammenspiel muss also genauestens konfiguriert werden. Hier haben wir nun unsere dritte und letzte Fehlerquelle im Prozess.”

David Rupprecht und Forschende des Lehrstuhls für Symmetrische Kryptographie haben so zum Beispiel 2021 nachweisen können, dass der Mobilfunkstandard 2G sehr unsicher ist. „Wir konnten zeigen, dass es da sogar absichtlich eingebaute Schwachstellen gibt, die ein Ausspähen von Daten ermöglicht haben“, berichtet er (siehe Seite 36). Die entsprechenden Verschlüsselungsalgorithmen waren so schwach, dass das unmöglich ein Zufall sein konnte – vielmehr handelte es sich um eine Hintertür, die in den 1990er-Jahren mit Absicht beschlossen und eingebaut worden war. Obwohl der Algorithmus auch auf modernen Smartphones immer noch eingebaut ist, geht von diesen Schwachstellen wohl keine Gefahr mehr aus, schätzen die Forschenden. Denn 2G ist lange überholt und kaum mehr im Einsatz.

„Alle zehn Jahre gibt es eine neue Mobilfunkgeneration“, so Rupprecht. Während es bei 2G vor allem um mobile Telefonie ging, startet mit dem 3G-Standard das mobile Internet. Seit 4G steht die Nutzung des Internets in Form von Apps klar im Fokus. „Das iPhone kam auf den Markt, mobiles Internet wurde ein Massenphänomen“, so David Rupprecht über die Zeit um 2010 herum, als der Standard eingeführt wurde. Bis heute laufen die meisten Mobilverbindungen über 4G. In seiner Doktorarbeit am Exzellenzcluster CASA hat sich David Rupprecht mit Schwachstellen dieser Generation befasst.

„Währenddessen haben wir mit CASA verschiedene Schwachstellen gefunden, die eigentlich jeden Smartphone-Nutzer betreffen. Eine davon ermöglichte das Abhören von Telefongesprächen. Wenn möglich, wurden die Schwachstellen entsprechend von den Herstellern oder Betreibern geschlossen“, erklärt David Rupprecht. Letzte Sicherheit gibt es dadurch dennoch nicht, denn so ein Zugewinn an Sicherheit geht immer auf Kosten der Leistungsfähigkeit. „Das Gremium der 3GPP muss dann abwägen und andere wichtige Faktoren wie zum Beispiel Geschwindigkeit und Akkulaufzeit mit einbeziehen“, erläutert er. Zudem können sicherheitsrelevante Einstellungen, die in die Spezifikationen aufgenommen werden, mitunter noch vom Netzbetreiber an- und ausgeschaltet werden.

Dennoch hilft die Analyse von Sicherheitsmängeln der aktuellen Mobilfunkgeneration immer auch der folgenden. „Die entsprechenden Gegenmaßnahmen können gleich von vornherein mitgedacht und in die nächste Generation aufgenommen werden“, erklärt David Rupprecht. Für ihn steht mittlerweile schon die fünfte Generation (5G) im Vordergrund. „5G ist besonders interessant, weil es viele neue Anwendungsmöglichkeiten einführt, wie beispielsweise die Vernetzung von Dingen. Autos können mit Ampeln kommunizieren, Fabriken verbessern ihre internen Netze, kritische Infrastrukturen erhalten neue Vernetzungsmöglichkeiten.“ Im Fall der Fabrik-Vernetzung sind es Roboter und Industrieanlagen, die in lokalen 5G-Campusnetzen verbunden werden, und zwar erstmals in privater Regie. „Dadurch kann plötz-

> „5G IST BESONDERS INTERESSANT, WEIL ES VIELE NEUE ANWENDUNGSMÖGLICHKEITEN EINFÜHRT, WIE BEISPIELSWEISE DIE VERNETZUNG VON DINGEN.“
>
> David Rupprecht

David Rupprecht gründet die Firma Radix Security gemeinsam mit Katharina Kohls.

David Rupprecht kennt Tausende Seiten von Spezifikationen, die dafür sorgen, dass in Mobilfunknetzen alles sicher und reibungslos funktioniert.

lich jeder zum Netzbetreiber werden“, spitzt David Rupprecht zu. Die Verantwortung für die sichere Implementierung und Konfiguration der 5G-Netze liegt nun bei den privaten Betreibern. Hier setzt das Unternehmen Radix Security an, das Rupprecht gerade mit Prof. Dr. Katharina Kohls gründet.

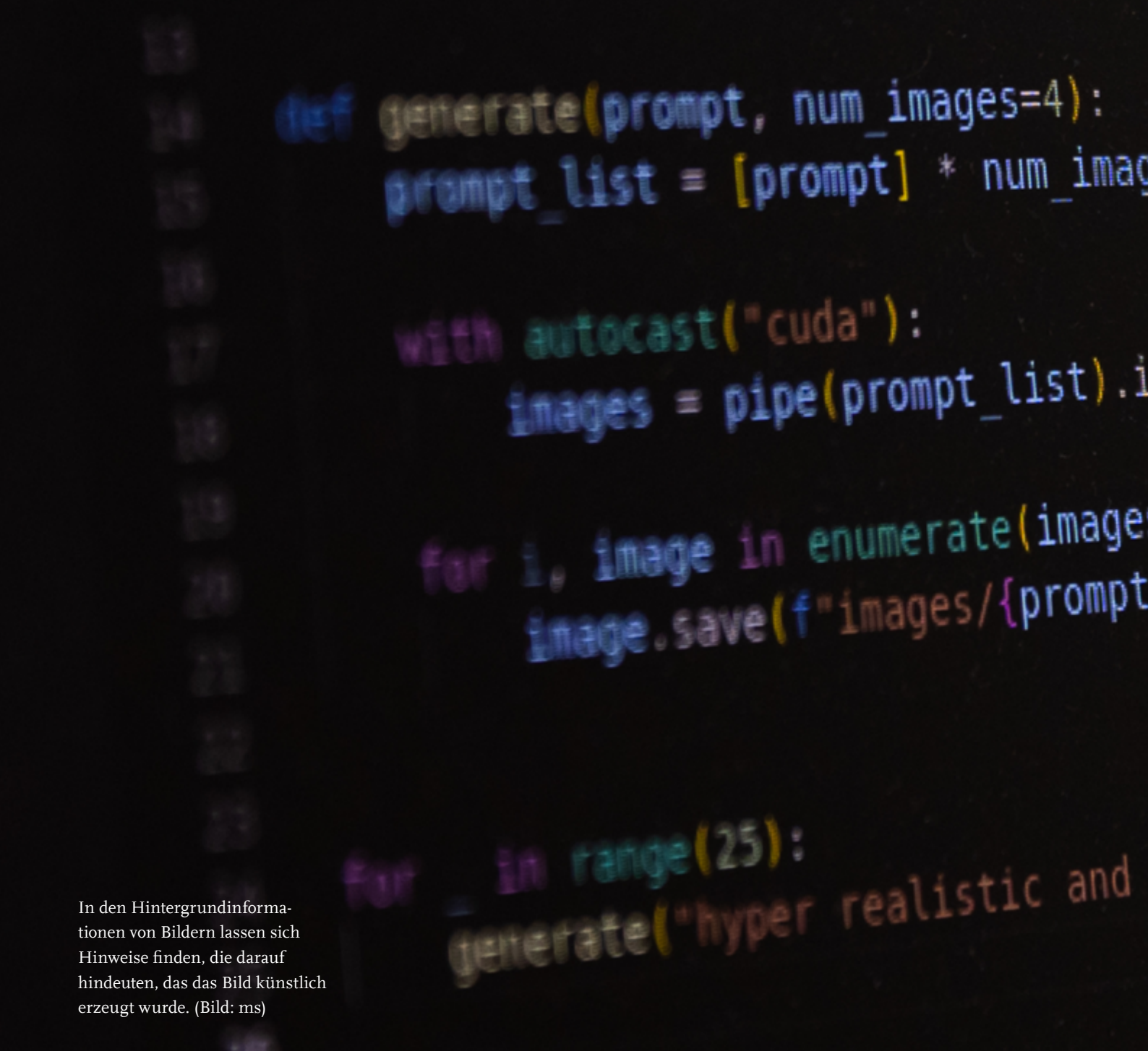
„Wir beschäftigen uns seit Jahren mit Sicherheitsfragen in 4G- und 5G-Netzen und haben einen enormen Wissensvorsprung“, sagt Rupprecht. Die Spezifikationen sind zwar öffentlich zugänglich – aber wer kann Tausende Seiten komplexer Informationen verstehen und umsetzen? Radix Security hat es sich zur Aufgabe gemacht, 5G-Sicherheit zugänglich zu machen und Campusnetzbetreiber dabei zu unterstützen, ihre Netze sicher aufzubauen und zu betreiben. Derzeit gibt es in Deutschland rund 300 Campusnetze, auch die Ruhr-Universität hat eines für Forschungszwecke.

„In der jetzigen Phase, in der die Technologie der Campusnetze noch recht jung ist, stellen wir fest, dass die Sicherheit keine oder nur eine geringe Rolle spielt“, so Rupprecht. Das ist problematisch, weil es viel ressourcenintensiver ist, ein Netz im Nachhinein abzusichern, als Sicherheit von Anfang an mitzuplanen. „Nach den ersten Gesprächen merken wir, dass die Betreiber ganz unterschiedliche Vorstellungen von Sicherheit haben. Hier wird Radix Security noch viel Aufklärung und Schulungsarbeit leisten, um über die Sicherheitsrisiken und Möglichkeiten der Campusnetze aufzuklären.“

Für die Absicherung eines Campusnetzes ist das richtige Werkzeug von großer Bedeutung. Zum einen geht es darum, Angriffe zu verhindern und damit Schwachstellen in der Implementierung und Konfiguration von Netzwerkkomponenten aufzudecken. Das Radix-Security-Testwerkzeug ermöglicht es, Komponenten über den Standard hinaus auf ihre Sicherheitseigenschaften zu überprüfen. Beispielsweise wird geprüft, ob eine Komponente wichtiges Schlüsselmaterial ausgibt. Wenn dies der Fall ist, wird die gesamte Sicherheit des Netzwerks kompromittiert.

„Zusätzlich zu den Tests müssen wir ein Campusnetz in die Lage versetzen, Angriffe zu erkennen und abzuwehren“, erklärt David Rupprecht. Radix Security entwickelt zu diesem Zweck ein Angriffserkennungssystem, das auf Campusnetzbetreiber zugeschnitten ist. Die grundsätzliche Problematik liegt in der Komplexität der Netzwerke und der offenen Luftschnittstelle. Im Gegensatz zu einem verkabelten Netzwerk muss sich ein Angreifer nur in der physischen Nähe des Netzwerks befinden, um es anzugreifen. „Bei all unseren Entwicklungen und Ideen hilft die Nähe zur Universität“, so Rupprecht. „Die Universität gibt uns einen Vorteil gegenüber unseren Mitbewerbern. Durch die Forschungsinfrastruktur, wie durch das Exzellenzcluster CASA, können unsere Kunden von Cutting-Edge-Forschung profitieren und sich so gegen die neuesten Angriffe schützen.“

Text: md, Fotos: ms



In den Hintergrundinformationen von Bildern lassen sich Hinweise finden, die darauf hindeuten, das das Bild künstlich erzeugt wurde. (Bild: ms)

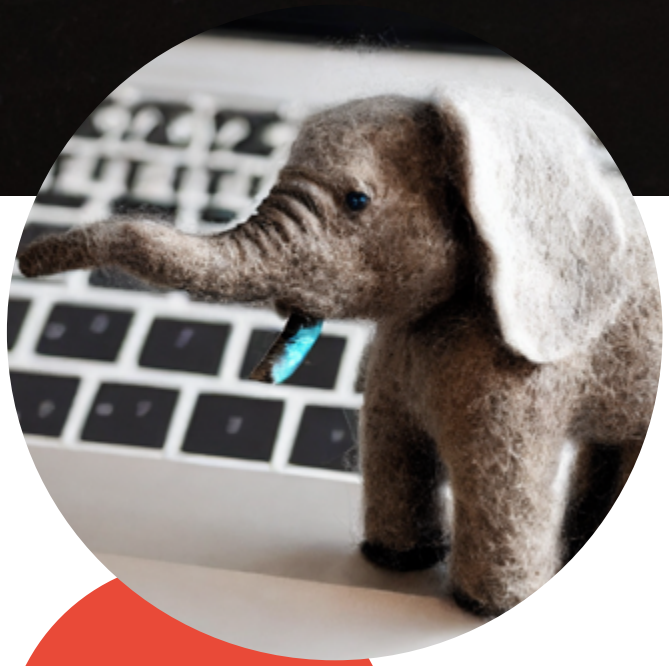
Menschen haben oft keine Chance, künstlich erzeugte Bilder, Audios oder Videos von echten zu unterscheiden. Deswegen arbeiten Forschende am Horst-Görtz-Institut für IT-Sicherheit an einer automatisierten Erkennung.

Wladimir Putin steht hinter einem Rednerpult und wendet sich an die USA: Man habe durchaus die Möglichkeit, die Demokratie Amerikas zu schädigen – doch habe man das gar nicht nötig. Die USA würden das schon selbst erledigen. Die Gesellschaft sei bereits gespalten. Das Video sieht aus wie echt – ist es aber nicht. Youtube ist voll von solchen Videos, die mal besser, mal schlechter gemacht sind. „Es ist schon noch viel Arbeit, aber wer will, der schafft es, zum Beispiel das Gesicht einer berühmten Persönlichkeit so gekonnt auf einen anderen Körper zu montieren, dass man es auf den ersten Blick nicht bemerkt“, sagt Jonas Ricker.

Er hat sich für seine Doktorarbeit, die er an der Fakultät für Informatik schreibt, auf gefakte Bilder spezialisiert. Im Mittelpunkt seiner Arbeit stehen allerdings nicht Videos,

Deepfake

WIE SICH **KÜNSTLICH ERZEUGTE BILDER** VERRATEN



Sieht aus wie echt: Dieser Wollelefant ist durch Text-zu-Bild-Generierung entstanden. (Bild: Hugging Face)

sondern Fotos. Er kann auf Anhieb mehrere Links aus dem Ärmel schütteln, unter denen man zum Beispiel Bilder von Personen anschauen kann, die nicht existieren, oder raten kann, ob das Bild einer gezeigten Person echt ist oder nicht. Die gefakten Bilder werden mithilfe von Deep Learning, einer Methode des maschinellen Lernens erzeugt – daher die Bezeichnung „Deepfake“. „Bei älteren Verfahren kann man manchmal sehen, dass es Auffälligkeiten bei der Symmetrie gibt“, zeigt er. „Zum Beispiel sind verschieden aussehende Ohrringe verräterisch oder asymmetrische Brillengläser. Aber die Methoden werden immer besser, und Studien haben belegt, dass Menschen bei der Unterscheidung echter und gefälschter Bilder eher schlecht sind.“

Ein Verfahren hinter der Erzeugung solcher Bilder nennt sich GAN für Generative Adversarial Networks. „Im Grunde ▸

sind solche Netzwerke immer zweigeteilt: Ein Teil generiert das Bild, ein anderer, der sogenannte Diskriminator, entscheidet, ob das generierte Bild echt aussieht oder nicht“, erklärt Jonas Ricker. „Man kann sich das so vorstellen, als wäre der eine Teil ein Geldfälscher, der andere Teil die Polizei, die gefälschte von echten Banknoten unterscheiden muss.“ Diese Entscheidung trifft die Künstliche Intelligenz auf der Basis vieler echter Bilder, die als Lerndatensatz einfließen. Am Anfang erzeugt der Generator einfach zufällig irgendwelche Pixel. Im Verlauf lernt er durch die Rückmeldung des Diskriminators immer mehr, worauf es ankommt. Auch der Diskriminator wird immer besser darin, die Bilder des Generators von echten zu unterscheiden. Generator und Diskriminator trainieren sich quasi gegenseitig, was schlussendlich zu täuschend echten Bildern führt.

In einem 2020 veröffentlichten Artikel beschreibt sein ehemaliger Kollege Joel Frank eine Möglichkeit, wie man gefälschten Bildern auf die Spur kommen kann. Der Schlüssel liegt in den sogenannten Frequenzen. „Es ist schwierig zu erklären, was Frequenzen bei Bildern sind“, so der Forscher. Am besten kann man sich Frequenzen als Hell-Dunkel-Unterschiede vorstellen. In Gesichtern von Menschen sind niedrige Frequenzen häufig. Hohe Frequenzen können zum Beispiel bei Haaren vorkommen. Die hohen Frequenzen werden unbewusster wahrgenommen. Ein Bild, bei dem hohe Frequenzen verändert wurden, sieht für uns daher fast genauso aus wie das originale Bild. Die Technik lässt sich aber nicht so leicht blenden: „Bei hohen Frequenzen gibt es bei GAN-erzeugten Bildern charakteristische Abweichungen von echten Fotos“, erklärt Jonas Ricker. Die hohen Frequenzen kommen bei künstlich erzeugten Bildern übermäßig häufig vor. Das lässt sich nachvollziehen, und die Bilder lassen sich anhand dessen von echten Fotos unterscheiden.

Jonas Ricker beschäftigt sich zurzeit mit einer anderen Klasse von Modellen zur Bilderzeugung, den sogenannten Diffusion Models. Während GANs schon 2014 vorgestellt

Künstliche Intelligenzen sind in der Lage, Bilder zu erzeugen, die Menschen nicht von Fotografien unterscheiden können. (Bilder: ms)

> LETZTLICH WIRD JEDES BILD VERDÄCHTIG UND AUCH VERNEINBAR, SOGAR BILDER ALS BEWEISE VOR GERICHT.
>
> Jonas Ricker

wurden, werden diese erst seit etwa drei Jahren erforscht, mit herausragenden Ergebnissen. „Das grundlegende Prinzip von Diffusion Models klingt zunächst verwunderlich“, so Ricker: „Ein echtes Bild wird Schritt für Schritt zerstört, indem zufälliges Rauschen hinzugefügt wird – daher der Name. Nach einigen hundert Schritten sind keine Bildinformationen mehr vorhanden, das Bild ist vollständig verrauscht. Das Ziel des Modells ist nun, diesen Prozess umzukehren, um das ursprüngliche Bild zu rekonstruieren – was ein schwieriges Problem darstellt.“

Der Schlüssel liegt darin, das Bild nicht direkt vorherzusagen, sondern wie beim Verrauschen Schritt für Schritt vorzugehen. Mit einer ausreichend großen Anzahl an Trainingsdaten kann das Modell lernen, ein verrauschtes Bild ein kleines bisschen weniger verrauscht zu machen. Durch die wiederholte Anwendung lassen sich dann aus zufälligem Rauschen komplett neue Bilder erzeugen. „Ein Schwachpunkt dieser Methode ist die lange Laufzeit aufgrund der mehreren hundert Schritte“, schränkt Jonas Ricker ein. „Allerdings wurden schon Techniken zur Optimierung vorgestellt, und die Forschung macht ständig Fortschritte.“

Zuletzt erregten Diffusion Models durch die sogenannte Text-zu-Bild-Generierung großes Aufsehen. Damit lassen sich Bilder auf Basis einer Texteingabe erzeugen, mit erstaunlichem Detailgrad. Trainiert werden diese Modelle mithilfe unzähliger Bild-Text-Paare aus dem Internet. Sowohl diese Datensammlung als auch das eigentliche Training ist extrem rechen- und damit kostenintensiv. Bis vor kurzem waren daher nur große Unternehmen wie Google (Imagen) und OpenAI (DALL-E 2) imstande, diese Modelle in hoher Qualität zu trainieren – und die halten die Modelle weitestgehend unter Verschluss.

Mit „Stable Diffusion“ gibt es jedoch nun ein frei zugängliches Modell, welches im Prinzip jeder selbst nutzen kann, vorausgesetzt der eigene Computer verfügt über genug Leistung. Die Anforderungen sind jedoch moderat, zudem gibt ▸

es inzwischen auch Webseiten, auf denen man sich Bilder zu eigenen Texten erstellen lassen kann.

Das Diffusion Model wird von einer Organisation vorangetrieben, die dank einer Spende über entsprechende Mittel und Rechenleistung verfügt. „Es ist schon jetzt sehr gut in der Erzeugung täuschend echter Bilder und wird sich künftig noch verbessern“, ist Jonas Ricker sicher. Das macht es noch schwieriger, echte Bilder von so erzeugten zu unterscheiden. Mittels Frequenzen klappt das hier schon mal weniger gut als bei GAN-Bildern. „Es gibt den Ansatz, die Reflexionen von Licht in den Augen für die Unterscheidung heranzuziehen – das klappt immerhin bei Bildern von Personen“, so Jonas Ricker. Er testet aktuell verschiedene Ansätze, die es erlauben, durch das Modell erzeugte Bilder von echten Fotos zu unterscheiden.

Ein universeller Detektor, der für alle möglichen GAN-Bilder funktioniert, funktioniert für diese Art von Bildern zum Beispiel eigentlich nicht – es sei denn, man stellt ihn durch ein gewisses Finetuning besser ein. Damit ist gemeint, dass man dem Detektor, der als Lernmaterial sehr viele echte und gefälschte Bilder mitsamt der dazugehörigen Information „echt“ oder „falsch“ zur Verfügung gestellt bekommt, zusätzliche Trainingsdaten gibt, um die Detektion für die neuen Daten zu optimieren. So kann er lernen, die mittels Diffusion Model erzeugten Bilder korrekt zu unterscheiden. Wie er das allerdings macht – das ist unklar.

Wichtig ist die Unterscheidung echter und gefälschter Bilder nicht nur, um Fake News zu enttarnen, die zum Beispiel als Video daherkommen, sondern auch, um Fake-Profile in Social Media dingfest zu machen. Sie werden in großem Stil eingesetzt, um zum Beispiel die öffentliche Meinung politisch zu beeinflussen. „Im Exzellenzcluster CASA geht es genau darum: großskalige Angreifer wie Staaten oder Geheimdienste zu enttarnen, die über die Mittel verfügen, mittels Deepfakes Propaganda zu machen“, so Jonas Ricker.

Die Erkennung gefälschter Fotos hat auch strafrechtliche Relevanz, etwa wenn es um unfreiwillige Pornografie geht, bei der Gesichter von Personen auf die Körper von anderen montiert werden. „Ganz allgemein führt die Masse künstlich erzeugter Bilder zu einem Schwund an Vertrauen, auch in seriöse Medien“, so Jonas Ricker. „Letztlich wird jedes Bild dadurch verdächtig und auch verneinbar, sogar Bilder als Beweise vor Gericht.“

Auch wenn Ricker daran arbeitet, dass gefälschte Bilder automatisch erkennbar werden, schätzt er, dass es letztlich auf etwas anderes hinauslaufen wird: „Ich glaube, am Ende wird es darum gehen, echte Bilder zu zertifizieren“, mutmaßt er. „Das könnte man sich zum Beispiel mit kryptografischen Methoden vorstellen, die schon in der Kamera des Fotografen eingebaut sein müssten und jedes echte Bild unzweifelhaft überprüfbar macht.“

md

> „DIE MASSE KÜNSTLICH ERZEUGTER BILDER FÜHRT ZU EINEM SCHWUND AN VERTRAUEN, AUCH IN SERIÖSE MEDIEN.“
>
> Jonas Ricker

Quiz

WELCHE **PERSONEN SIND ECHT?**

Jeweils eines der beiden Gesichter in jeder Gegenüberstellung ist echt, das andere ist mittels maschinellem Lernen erzeugt. Welche Bilder zeigen reale Fotos?
Die Lösungen finden sich auf Seite 62. Das Material stammt von der Seite whichfaceisreal.com.

1 a ◯

1 b ◯

2 a ◯

2 b ◯

3 a ◯

3 b ◯

4 a ◯

4 b ◯

5 a ◯

5 b ◯

6 a ◯

6 b ◯

Fuzzing

INTELLIGENTE **AFFEN**

Bochumer Forscher finden Sicherheitslücken in IT-Systemen besonders schnell. Ihr Trick: Sie konzentrieren sich auf das Wesentliche. Das Vorgehen erklären sie mithilfe des Theorems der endlos tippenden Affen.

Ein Programmcode ist ein bisschen wie ein Dschungel: komplex aufgebaut, schwer von außen einzusehen, mit unzähligen möglichen Wegen, die man nehmen kann. Schwachstellen in einem solchen Code zu finden ist wie Tiere zwischen den Bäumen im Urwald zu suchen: Man weiß, dass sie da sind, aber man sieht sie nicht direkt. Doktorand Tobias Scharnowski entwickelt daher neue Methoden, um im Dschungel der Einsen und Nullen effizient Programmierfehler aufspüren zu können. Er forscht am Lehrstuhl für Systemsicherheit des Horst-Görtz-Instituts der Ruhr-Universität Bochum, betreut von Prof. Dr. Thorsten Holz.

Die Forscher interessieren sich vor allem für eingebettete Systeme: „Wir versuchen, die Sicherheit von Computern zu erhöhen, von denen die meisten Menschen gar nicht wissen, dass sie überhaupt Computer sind“, beschreibt Scharnowski. Smarte Glühlampen, ans Internet angeschlossene Kühlschränke oder intelligente Thermostate sind ein paar Beispiele für die eingebetteten Systeme, die auf der Agenda der Systemsicherheitsforscher stehen. Diese Gegenstände enthalten elektronische Steuerungstechnik mit vielen Zeilen Programmcode, in die sich Fehler eingeschlichen haben können. Es geht den IT-Experten aber nicht nur um Gegenstände aus dem Haushalt. Vor allem interessieren sie sich für Steuerungssysteme in der Industrie, zum Beispiel aus dem Bereich der kritischen Infrastrukturen wie der Energieversorgung. Sicherheitslücken könnten hier besonders dramatische Auswirkungen haben.

Tobias Scharnowski und Thorsten Holz nutzen das sogenannte Fuzzing, um Fehler im Programmcode aufzuspüren. Als Fuzzer bezeichnet man Algorithmen, die die zu testende Software mit zufälligen Inputs füttern und prüfen, ob sie die Anwendung damit zum Absturz bringen können. Solche Crashs weisen auf Programmierfehler hin. Immer wieder variiert der Fuzzer den Input, um Schritt für Schritt möglichst viele Programmbestandteile zu erkunden.

EINGEBETTETE SYSTEME

Ein eingebettetes System ist eine Kombination aus einer Hardware und einer Software, die einen speziellen Zweck innerhalb eines größeren Systems erfüllt – zum Beispiel im Auto die elektronische Steuerung der Sitze. Eigentlich ist ein eingebettetes System ein Computer, der einem eng umgrenzten Zweck dient.

SOFTWARE, HARDWARE, FIRMWARE

Als Hardware bezeichnet man alle Geräte im Computerbereich – anders als Soft- und Firmware existiert sie also in der realen Welt, die mit den Händen angefasst werden kann. Software und Firmware hingegen sind Programme, die nur virtuell existieren. Die Firmware ist dabei eine spezielle Art von Software, die verwendet wird, um Hardware zu steuern; sie erfüllt also einen genau definierten Zweck für diese Hardware.

FUZZING

Fuzzing ist eine Methode zum Finden von Schwachstellen in Software. Dabei wird die Software mit vielen verschiedenen Inputs gefüttert und solange ausgeführt, bis eine Eingabe sie zum Absturz bringt. Ein Programmabsturz deutet auf einen Fehler hin.

Die beiden Forscher suchen nach Schwachstellen im Programmcode von Firmware, also von einer speziellen Software, die zur Steuerung von Hardware gebraucht wird.

Für bestimmte Anwendungsbereiche ist das Fuzzing bereits etabliert, zum Beispiel, um Betriebssysteme wie Windows oder Linux zu testen. Eingebettete Systeme hingegen wurden noch nicht ausgiebig damit untersucht; denn sie bringen einige Herausforderungen mit sich: Bei ihnen ist die Software – die sogenannte Firmware – in eine Hardware eingebettet, mit der sie interagiert. Über die Hardware und ihre Funktionsweise haben die Forscher aber in der Regel wenig Informationen. „Das ist wie eine Blackbox für uns“, beschreibt Thorsten Holz. Hinzu kommt, dass diese Blackbox in der Regel nicht besonders leistungsstark ist – oft haben die Systeme verhältnismäßig wenig Speicher und langsame Prozessoren. Ein Problem, wenn die Forscher das Fuzzing direkt im System durchführen wollen. Es würde viel zu lange dauern, alle möglichen Inputs durchzuprobieren und auf die Antwort des Systems zu warten.

Deswegen analysiert das Team die Firmware nicht direkt in der industriellen Steuereinheit oder in der Glühbirne. Stattdessen bauen sie die Hardware virtuell nach – emulieren nennt sich dieser Prozess. Der Emulator gaukelt der Firmware vor, sich in dem realen Gegenstand zu befinden. Dazu muss er genauso mit dem Programm interagieren, wie es die echte Hardware tun würde. „Wir müssen also alle Schnittstellen, die es zwischen Hardware und Firmware gibt, nachahmen“, erklärt Thorsten Holz. Gelingt das, können die Wissenschaftler die Firmware in einem leistungsfähigen System testen.

Trotzdem würde es lange dauern, wenn sie ihren Fuzzer alle theoretisch denkbaren Inputs ausprobieren lassen würden. Deswegen schalten die Forscher dem eigentlichen Fuzzing-Prozess einen weiteren Schritt vor, in dem sie die möglichen Inputs eingrenzen. Sie modellieren zunächst, in welchem Rahmen sich die Eingaben befinden müssen, um für die Firmware logisch zu sein. Ein Beispiel: Gehen wir davon es, dass es sich bei der Hardware um einen Kühlschrank mit einem Temperaturfühler handelt. Die gemessenen Temperaturen kann die Kühlschrank-Hardware an die Software ▸

> „WENN EIN SYSTEM NOCH NIE MIT FUZZING GETESTET WURDE, DANN GIBT ES DARIN AUCH UNENTDECKTE SCHWACH-STELLEN.“

Thorsten Holz

des Kühlschranks, also seine Firmware, melden. Realistischerweise können nicht alle möglichen Temperaturen auftreten, sondern nur ein gewisser Bereich. Daher ist auch die Firmware nur für einen bestimmten Temperaturbereich programmiert. Andere Werte könnte sie gar nicht verarbeiten, also muss man sie auch nicht im Fuzzing testen.

„Im Fuzzing-Prozess nutzen wir also nur die Inputs, die die Firmware auch erwartet und mit denen sie umgehen kann“, beschreibt Thorsten Holz und vergleicht den Prozess mit dem Infinite Monkey Theorem: „Dieses Theorem besagt, dass, wenn man Affen lange genug auf eine Tastatur drücken lassen würde, irgendwann auch Shakespeares Werke dabei herauskommen würden.“ So wäre es mit dem Fuzzer auch: Wenn man ihn lange genug probieren lassen würde, würde er durch Zufall irgendwann sinnvolle Inputs nutzen. Aber es würde lange dauern. „Wir wollen unsere Affen aber etwas intelligenter machen“, sagt Tobias Scharnowski. „Wir nehmen ihnen alle Tasten weg, die sie nicht brauchen, und versuchen sie dazu zu bringen, nur sinnvoll auf die Tasten zu drücken. Mit den Inputs, die übrigbleiben, können wir den Code trotzdem bis in die hintersten Ecken testen.“ Auf diese Weise wird das Fuzzing mit dem Bochumer System, Fuzzware genannt, besonders effizient.

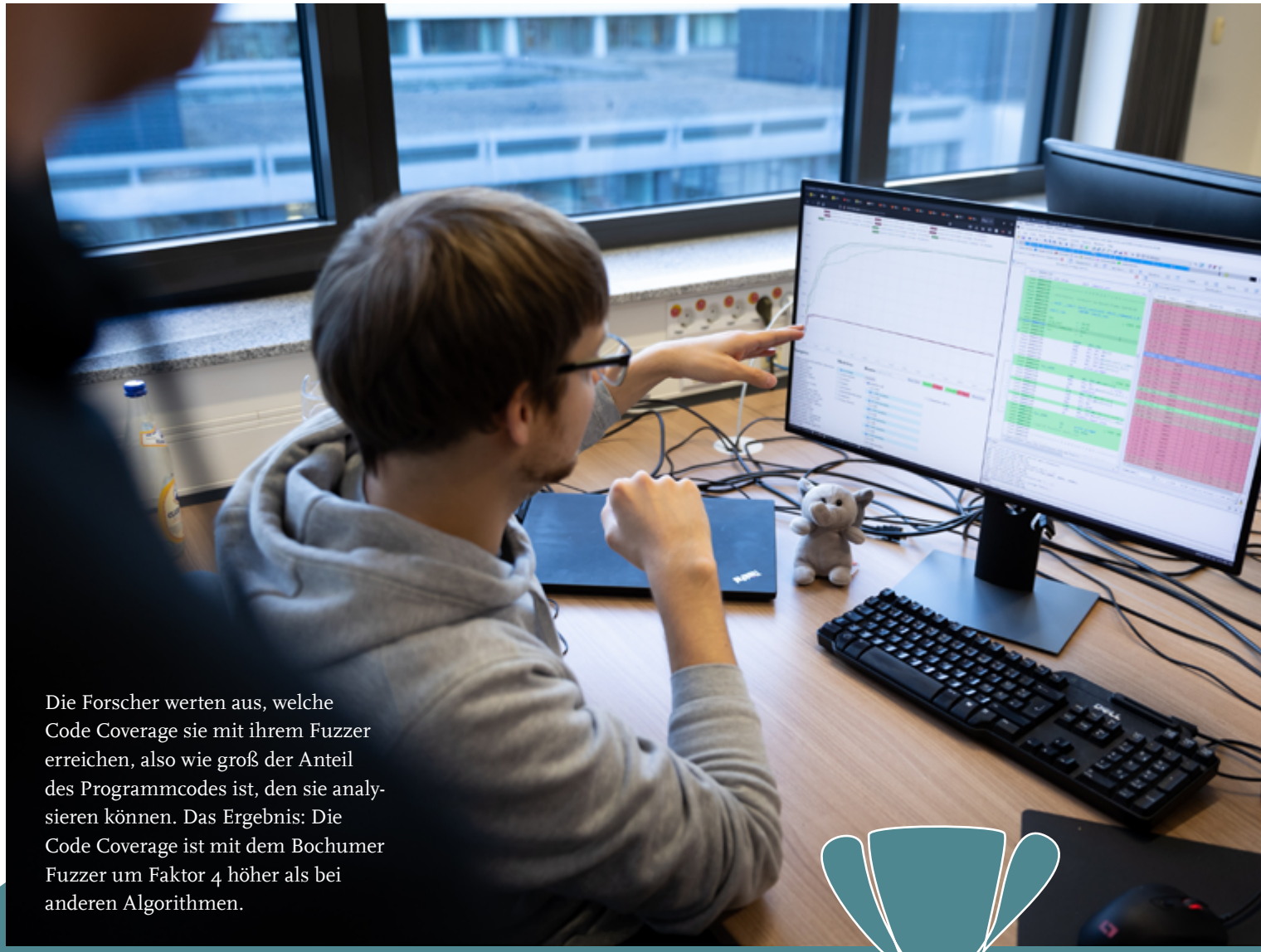
Zusammen mit Kolleginnen und Kollegen aus Santa Barbara und Amsterdam testete das Bochumer Team 77 Firmwares mit Fuzzware. Im Vergleich zu herkömmlichen Fuzzing-Methoden sortierten sie bis zu 95,5 Prozent der möglichen Inputs aus. Trotzdem gelang es ihnen, mit dem Fuzzware-System in der gleichen Zeit bis zu dreimal mehr von dem Programmcode zu checken wie mit herkömmlichen Verfahren. Dabei fand die Gruppe auch neue Schwachstellen, die mit anderen Fuzzing-Methoden unentdeckt geblieben waren.

„Man findet eigentlich immer was“, weiß Thorsten Holz. „Wenn ein System noch nie mit Fuzzing getestet wurde, dann gibt es darin auch unentdeckte Schwachstellen.“ Gerade bei eingebetteten Systemen ist es für Programmiererinnen und Programmierer nahezu unmöglich, einen perfekten Code auf die Beine zu stellen. „Um mit der Hardware von eingebetteten Systemen sprechen zu können, muss man eine Low-Level-Programmiersprache nutzen“, erklärt Tobias Scharnowski. Programmierer können in vielen Bereichen nicht auf Codeschnipsel zurückgreifen, die für andere Anwendungen entwickelt wurden. Sie müssen ihren Code von Grund auf neu aufbauen. Gerade Randfälle – Zustände, in denen sich das System selten befindet – werden dann eventuell nicht bedacht. „Für unsere Fuzzer sind diese Zustände aber leicht zu analysieren“, sagt Scharnowski. „Sie können daher helfen, die Systeme robuster zu machen.“ Gefundene Schwachstellen melden die Forscher an die Hersteller und tragen so zu mehr Sicherheit in Industrie, Glühbirnen, Kühlschränken und Co. bei.

Text: jwe, Fotos: ms

Tobias Scharnowski ist Doktorand am Horst-Görtz-Institut für IT-Sicherheit.

Thorsten Holz war viele Jahre einer der Principal Investigators des Exzellenzclusters CASA.



Die Forscher werten aus, welche Code Coverage sie mit ihrem Fuzzer erreichen, also wie groß der Anteil des Programmcodes ist, den sie analysieren können. Das Ergebnis: Die Code Coverage ist mit dem Bochumer Fuzzer um Faktor 4 höher als bei anderen Algorithmen.

Im Gespräch

„EIN RAUNEN GING DURCH DIE MENGE“

Softwarefirmen freuen sich, wenn Forschende Fehler in ihrem Code finden, bevor es Angreifer tun. Sie richten sogar Wettbewerbe für die Fehlersuche aus. Das Bochumer Team hat schon reichlich Preisgelder eingeheimst.

Herr Scharnowski, in Ihrem Bereich ist öfter mal von Bug Bounties die Rede. Was muss man sich darunter vorstellen?
Es ist eine Art Bonusprogramm von Softwareunternehmen für das Aufspüren von Schwachstellen. Je schwerwiegender die Schwachstelle ist, die man entdeckt, desto höher der Gewinn. Manche Hersteller schreiben sogar Wettbewerbe aus.

Haben Sie schon einmal teilgenommen?
2020 habe ich mit Kollegen beim Pwn2Own-Wettbewerb in Miami mitgemacht. Er wurde von verschiedenen Herstellern aus dem industriellen Sicherheitsbereich ausgelobt. Es ging um Geräte, die industrielle Anlagen steuern. Wir haben unter anderem das sogenannte DNP3-Protokoll angegriffen, das für die Kommunikation zwischen den Steuersystemen eingesetzt wird, beispielsweise im kritischen Energiesektor. Wir haben es als einzige geschafft, die höchste Kategorie für diese Aufgabe zu erreichen, und konnten komplette Kontrolle über das Programm gewinnen.

Das klingt nach einem besonderen Erfolg.
Ja, das war ein besonderes Erlebnis. Bei dem Wettbewerb waren verschiedene Ziele ausgelobt worden, und zu Beginn wurde verkündet, welches Team welches Ziel in Angriff nehmen würde. Als unsere Idee vorgestellt wurde, ging ein Raunen durch die Menge.

Und was war der Gewinn?
Wir haben zu dritt 87.500 US-Dollar Preisgeld bekommen. Das gibt uns nun die Freiheit, Software und Equipment für unsere nächsten Abenteuer dieser Art zu kaufen.

jwe

Im Gespräch

DATEN **ABGESCHIRMT VERARBEITEN** IN DER CLOUD

Cloud-Dienste nutzen ohne Ärger mit der Datenschutz-Grundverordnung – die Firma Edgeless Systems macht es möglich. Gründer Dr. Felix Schuster blickt zurück auf den nicht immer einfachen Einstieg in einen neuen Markt.

Felix Schuster und Thomas Tendyck feierten die Gründung ihrer Firma Edgeless Systems im Frühjahr 2020 während des Corona-Lockdowns zu zweit auf einer Parkbank. Gut zwei Jahre später haben sie ein 15-köpfiges Team, namhafte Kunden und einen repräsentativen Firmensitz in Bochum. Dennoch war der Start nicht immer einfach, berichtet Felix Schuster im Interview.

Herr Schuster, Sie wissen, wie man Cloud-Anwendungen zum Beispiel in den USA nutzen kann, ohne mit der Datenschutzgrundverordnung (DSGVO) in Konflikt zu geraten. Was genau bieten Sie Ihren Kunden?

Wir programmieren Software für sicheres Cloud-Computing – das Marketing-Schlagwort heißt Confidential Computing. Die Cloud hat das grundsätzliche Problem, dass Daten normalerweise im Klartext verarbeitet werden. Das heißt, Mitarbeitende von Cloud-Anbietern oder Behörden haben möglicherweise Zugriff darauf. Das hat zur Folge, dass Unternehmen aus der EU diese Cloud-Dienste, die meistens in den USA beheimatet sind, nicht nutzen können.

Wir sorgen dafür, dass man die Cloud nutzen kann wie einen eigenen Rechner. Voraussetzung dafür ist, dass die Hersteller von Prozessoren seit knapp zehn Jahren Funktionen in die Hardware einbauen, die es erlauben, Daten verschlüsselt zu verarbeiten. Bis dahin konnten die Daten zwar beim

Transport und auf der Festplatte verschlüsselt sein, mussten zur Verarbeitung aber entschlüsselt werden. Wir sorgen mit unserer Software dafür, dass die Daten die ganze Zeit über verschlüsselt bleiben, und dass das auch überprüfbar ist. Der Prozessor stellt dafür ein Zertifikat aus, das bescheinigt, was mit den Daten gemacht wurde, und dass sie zu keinem Zeitpunkt entschlüsselt wurden.

Für welche Art von Anwendungen ist das bedeutend?
Der typische Fall ist, dass eine Firma eine Anwendung lokal laufen hat, aber aus Ressourcengründen gerne in die Cloud will. Ein Beispiel dafür wäre etwa eine Personalverwaltungssoftware. Da geht es um personenbezogene Daten, die einem besonderen Schutz unterliegen. Oder ein Beispiel aus unserer Praxis: Unser Partner Bosch sammelt Daten vernetzter Autos. Da geht es um geistiges Eigentum, es können auch Bilder von Passanten dabei sein. Die Hardware der Cloud ermöglicht es, diese Daten sozusagen abzuschirmen und verschlüsselt zu verarbeiten. Aber da das nicht von alleine klappt, braucht es dafür eine Software wie unsere.

Kann dann jeder Kunde diese Funktionen ganz einfach nutzen oder muss jemand da sein, der IT-Expertise hat?
Unser Programm basiert auf Kubernetes, einer sehr gängigen Anwendung in Clouds, die beim Kunden meistens schon im Einsatz ist. Die Grundzüge sind daher den Anwendenden oft bekannt. Aber es muss schon jemanden vor Ort geben, der sich auskennt.

Sie haben Ihre Software zuerst unentgeltlich und quelloffen angeboten. Wie kann man sich davon finanzieren?
Das ist aktuell eher die Norm, dass man zunächst eine Art erweiterte kostenlose Testversion anbietet. Natürlich geht man ▸

i EDGELESS SYSTEMS

Die beiden Gründer der Firma Edgeless Systems haben sich beim Studium an der Ruhr-Universität kennengelernt. Die Gründung konnten sie mit Unterstützung des Gründungs-Inkubators Cube 5 vorbereiten. Cube 5 ist am Horst-Görtz-Institut für IT-Sicherheit sowie der Fakultät für Informatik der Ruhr-Universität angesiedelt und Teil des Worldfactory Start-up Centers. Aktuell hat die Firma 15 Mitarbeitende, davon zehn Festangestellte. Die Gründer suchen weitere Mitarbeitende, gerne aus der Ruhr-Universität, wo auch fast alle bisherigen ausgebildet wurden.

Die Firma programmiert Software für sicheres Cloud-Computing.

damit das Risiko ein, dass die Anwender damit zufrieden sind und dabei bleiben, oder dass die Konkurrenz das Programm kopiert. Aber der Vorteil ist, dass man ein sehr niedrigschwelliges Angebot für potenzielle Kunden hat. Der erste Schritt ist damit schon getan, und vielleicht kommt der Kunde auf uns zurück, um eine Enterprise-Version zu kaufen.

In einem so neuen Markt wie unserem ist das eine gute Möglichkeit zu sehen, wo die Kunden stehen. Es hilft auch, Kunden zu identifizieren und zu akquirieren. Ein Jahr nach dem ersten kostenfreien Angebot hatten wir viele schöne Anfragen. Anders als in den USA ist dieses Geschäftsmodell hier allerdings eher unüblich, und man stößt auf Unverständnis. Aber bei den Investoren sind wir damit wesentlich besser angekommen.

Wenn der Markt noch so jung ist, gibt es dann trotzdem eine nennenswerte Konkurrenz?

Ja, es gibt sogar viel Konkurrenz, vor allem in den USA. Aber unser Produkt ist am weitesten ausgereift. Das muss der Markt nur noch mitbekommen. Aktuell wissen die wenigsten Kunden, was sicheres Cloud-Computing ist – sie sehen zwar ihr Problem, kennen die Lösung aber nicht. Da gibt es viel Erklärungsbedarf.

Spielt Ihnen die DSGVO nicht in die Hände?

Das kann durchaus ein Treiber sein. Wir würden vor diesem Hintergrund auch gerne mehr mit europäischen Cloud-Anbietern zusammenarbeiten. Dann könnten wir einen Dienst auf Seiten des Anbieters entwickeln, und der Kunde müsste

> „AKTUELL WISSEN DIE WENIGSTEN KUNDEN, WAS SICHERES CLOUD-COMPUTING IST.“
>
> Felix Schuster

Das Team umfasst zurzeit 15 Mitarbeitende. Weitere werden gesucht.

gar nichts mehr selbst machen, sondern könnte einfach sicher sein, dass seine Daten geschützt sind.

Zurück zu den Anfängen von Edgeless Systems: War es schon immer Ihr Wunsch, Gründer zu werden?
Ich wollte schon zu Schulzeiten eine Softwarefirma gründen. Während des Studiums habe ich in einer kleinen Firma gearbeitet, da hat sich der Wunsch verfestigt. Der Hauptgrund für meine Promotion war auch die Suche nach spannenden Technologien als Basis für die Gründung.

Was prägt heute Ihre Arbeitstage?
Aus den technischen Details bin ich heute raus. Das ist das Spezialgebiet meines Mitgründers Thomas Tendyck. Ich kümmere mich weiterhin um die Produktvision und Teile der Architektur. Weitere Kernaufgaben sind Außendarstellung, Kundengewinnung, Mitarbeiterwerbung und Akquise von Investorengeldern. Dazu kommen viele andere kleinere Aufgaben aus den Bereichen Personal, Operations und Finanzen.

Haben Sie die Gründung je bereut?
Gelegentlich – es gibt immer Höhen und Tiefen. Aber im Allgemeinen war es eine gute Entscheidung. Es macht viel Spaß, ist aber sehr stressig. Ich habe gelernt, damit umzugehen.

Wenn Sie in die Kristallkugel blicken und fünf Jahre voraussehen könnten, was wünschen Sie sich zu sehen?
Wir sind als Unternehmen noch in der Phase, den Product Market Fit zu optimieren – perfekt ist der, wenn man zum Beispiel während einer Pandemie eine Impfung anbieten kann, also genau das Produkt hat, was der Markt gerade nachfragt. Wir versuchen gerade, diese Passung gut hinzubekommen. Wir lernen viel. Wir wollen die Plattform schlechthin für besonders sicheres Cloud-Computing werden.

In fünf Jahren sollten wir unser Geschäftsmodell skaliert und über 100 Mitarbeitende haben. Noch weiter in die Zukunft gesehen sollte ein Börsengang oder ein Verkauf der Firma stehen. Das sind die beiden Ziele für wagniskapitalfinanzierte Firmen, wie wir es sind.

Welchen Rat würden Sie sich selbst geben, wenn Sie zwei Jahre zurück gehen könnten?
Wir haben zu ingenieursmäßig angefangen, haben uns teils verzettelt, um das Risiko zu minimieren. Rückblickend würde ich sagen, wir hätten früher mehr Risiko eingehen und ein mögliches Scheitern in Kauf nehmen sollen. Und: Es ist ein spannender, aber auch schwieriger Markt. Beim nächsten Mal würde ich einen Markt wählen, der schon etwas weiter ist.

Das klingt, als wäre nach einem möglichen Verkauf der Firma eine weitere Gründung für Sie denkbar?
Auf jeden Fall. Vielleicht mit etwas Urlaub zwischendurch.

Text: md, Fotos: ms

Geheimdienste wollen so viel wissen wie möglich. Sie versuchen beispielsweise, Datenverschlüsselungen zu umgehen. Das kann Kollateralschäden verursachen, warnen Bochumer Forscher.

Absichtliche Schwachstellen in Verschlüsselungsalgorithmen scheinen Geheimdiensten und Strafverfolgungsbehörden verlockend – erlauben sie es doch, vermeintlich sichere Informationen mitzulesen. Über den Sinn und Unsinn solcher Hintertüren und ein sehr langlebiges Beispiel einer solchen Lücke berichten Prof. Dr. Gregor Leander und Dr. Christof Beierle vom Lehrstuhl Symmetrische Kryptografie sowie Dr. David Rupprecht vom Lehrstuhl für Systemsicherheit. Mit internationalen Kollegen konnten sie zeigen, dass aktuelle Smartphones die unsichere Handyverschlüsselung GEA-1 immer noch an Bord haben. Seit den 1990ern gibt es sie, seit 2013 sollte sie laut Mobilfunkstandards verschwunden sein.

Herr Professor Leander, Herr Dr. Rupprecht, Herr Dr. Beierle, Sie suchen nach geheimen Hintertüren. Was genau ist das eigentlich?

David Rupprecht: Eine Hintertür ist eine Art Sollbruchstelle im Verschlüsselungsverfahren. Man kann sie sich etwa so vorstellen wie einen Generalschlüssel, der gar nicht existieren dürfte. Physisch liegt sie im von uns untersuchten Fall in einem Chipsatz, der in Handys verbaut ist, also auf der Hardware.

Gregor Leander: In unserem Fall handelt es sich um symmetrische Kryptografie. Das bedeutet, dass alle legitim an der Kommunikation Beteiligten – hier Mobiltelefone und Mobilfunkmasten – denselben Schlüssel haben. Der zugrunde liegende Algorithmus ist sozusagen das Kochrezept für die Herstellung dieser Schlüssel.

David Rupprecht: Um den Schlüssel zu erzeugen, der übrigens bei jedem Kontakt zwischen Handy und Mast neu generiert wird, braucht man außerdem noch einen auf der SIM-Karte des Handys gespeicherten, geheimen Code. Ausgehend davon wird mittels Algorithmus der GEA-Schlüssel berechnet, und zwar sowohl vom Handy als auch vom Mobilfunkmast. Das Ergebnis bedeutet für die beiden: Wir sind Freunde, wir können kommunizieren.

Welche Daten sind von der Sicherheitslücke in GEA-1 betroffen?

Leander: Im Prinzip alle. Aber das ist nicht für alle Daten von Bedeutung. Denn wenn ich zum Beispiel Online-Banking nutze, werden die Daten von der Bank extra verschlüsselt, und zwar Ende-zu-Ende, sodass sie zwischendurch gar nicht entschlüsselt werden.

Christof Beierle: In den 1990ern, aus denen die GEA-Verschlüsselung stammt, war das allerdings noch nicht so.

Leander: Es geht bei solchen Hintertüren aber weniger um die Inhalte der Informationen, die hin und her geschickt werden, sondern um Metadaten, das wird oft unterschätzt. Es geht um die Information: Wer kommuniziert wann mit wem? Diese Metadaten sind von sehr großem Wert. Das lässt sich schon allein daran erkennen, dass der Facebook-Konzern Meta Platforms bei WhatsApp eine Ende-zu-Ende-Verschlüsselung eingeführt hat, ohne dass es seitens der Nutzenden großen Druck gegeben hätte. Das wirkt wie ein Widerspruch, denn Facebook lebt von Daten. Der Grund ist schlicht: Facebook sieht immer noch die Metadaten. Und das genügt.

Auf wessen Betreiben werden Hintertüren in Systeme eingebaut?

Leander: Solche Hintertüren sind natürlich im Interesse der Geheimdienste und Strafverfolgungsbehörden. Die Diskussion über Hintertüren für diese Zwecke ist immer da, wenn sie auch wenig sinnvoll ist. Im Fall von GEA-1 muss man sich vor Augen halten, dass es in den 1990er-Jahren entwickelt wurde. Damals galt Kryptografie als Waffe. Starke Kryptografie durfte nicht ins Ausland ausgeführt werden, da galten strenge Exportbeschränkungen. Handys wollte man aber natürlich auch ins Ausland verkaufen. Also musste man diese Exportbeschränkungen umgehen.

Beierle: Es gibt ein Dokument von 1998 zu den Anforderungen an die Chiffre. Eine war: Die Verschlüsselung muss exportfähig nach gängigen Richtlinien sein. Das bedeutet: Sie musste gerade so schwach sein, dass sie durchkommt, aber auch nicht zu schwach.

Wer legt solche Standards wie die zur Verschlüsselung fest?

Rupprecht: Im Fall von GEA war das die European Standard Organisation ETSI, so eine Art DIN-Institut auf europäischer Ebene. Darin sind zum Beispiel große Hersteller vertreten, Unternehmen wie die Telekom, aber auch Regierungsorganisationen. ▸

Im Gespräch

SICHERHEIT MIT **SOLLBRUCHSTELLE**

Gregor Leander, David Rupprecht und Christof Beierle (von links) befassen sich mit Hintertüren in Computersystemen.

Frühere Schwächen der Kryptografie sind heute bekannt und die Verfahren öffentlicher geworden.

Leander: Es ist nicht ausgeschlossen, dass da auch Angehörige von Geheimdiensten angestellt waren, damals.

Weiß man, ob die Hintertür in GEA-1 ausgenutzt worden ist?

Leander: Für GEA ist unbekannt, ob sie genutzt wurde oder nicht. In anderen Fällen ist es aber belegt, dass Hintertüren ausgenutzt wurden.

Rupprecht: Die Enthüllungen durch Edward Snowden haben zum Beispiel zutage gefördert, dass Angela Merkels Handy abgehört wurde. Wenn man sich fragt, wie das zustande gekommen sein kann, kommt man schnell auf Verschlüsselungsverfahren, die so ähnlich wie GEA funktionieren und für Voice-Telefonie verwendet werden. Auch hier war ein relativ schwacher Algorithmus eingebaut.

Herr Leander, Sie deuteten gerade an, dass Sie absichtlich eingebaute Hintertüren im Interesse von Behörden als nicht sinnvoll erachten.

Leander: Es gibt 1.000 legitime Gründe für die Strafverfolgungsbehörden und Geheimdienste, sich solche Hintertüren zu wünschen. Aber sie sind der falsche Weg. So ein Generalschlüssel kann auch von jemandem gefunden werden, der vielleicht kriminelle Interessen hat. Und ist die Lücke einmal da, ist sie immer da – man sieht ja, dass es bis heute nicht gelungen ist, GEA-1 zu beseitigen, obwohl das schon vor Jahren hätte passiert sein sollen.

Rupprecht: Ein weiterer Aspekt ist: Wenn alle wissen, dass nur schwache Algorithmen erlaubt sind, werden Verbrecher selbst eine sichere Verschlüsselung benutzen und sich so vor den Behörden verschanzen. Verbrecher kümmern sich nicht darum, dass Kryptografie verboten ist. Die switchen einfach um auf ein eigenes System. Hinzu kommen natürlich grundsätzliche Prinzipien der Demokratie wie der Schutz der Privatsphäre. Massenhafte Überwachung ist nicht mit demokratischen Werten vereinbar.

Wie kommt es, dass GEA immer noch in aktuellen Geräten ist, obwohl bekannt ist, dass die Verschlüsselung eine Hintertür hat?

Rupprecht: Die Herstellerindustrie ist riesig, da geht das vielleicht einfach unter, weil es in dem Moment keine Priorität hat.

Müssen wir also alle damit rechnen, dass in unseren Geräten Verschlüsselungsalgorithmen mit Hintertüren aktiv sind?

Leander: Nein. Wir gucken inzwischen gut hin.

Rupprecht: Nicht in Endgeräten. Das spielt sich inzwischen mehr in den Netzwerkprodukten ab, zum Beispiel Routern, auf denen das Internet basiert. Es gibt Beispiele für modernere Verschlüsselung mit Hintertüren. Ein aktuellerer Fall ist etwa die Manipulation von Zufallsgeneratoren durch den US-Geheimdienst NSA. Der Zufall ist bei Verschlüsselungsverfahren oft nötig, und wenn man dafür sorgt, dass überzufällig häufig Nullen statt Einsen erzeugt werden, kann man die Schlüssel vereinfachen. Im Fall der NSA war der manipulierte Algorithmus so langsam, dass ihn keiner haben wollte, daher wurden Firmen bezahlt, damit sie ihn einbauen.

Leander: Es gibt aber auch kryptografische Algorithmen ohne Hintertür.

Das Problem der Hintertüren bleibt für viele abstrakt, aber die Industrie-community ist gewillt zu handeln.

> „VERBRECHER KÜMMERN SICH NICHT DARUM, DASS KRYPTOGRAFIE VERBOTEN IST."
>
> David Rupprecht

Rupprecht: Seit den 1990er-Jahren gab es da einen Shift: Die damaligen Schwächen der Kryptografie sind mittlerweile bekannt, und die Verfahren sind öffentlicher geworden.

Beierle: Verdächtig ist immer, wenn Algorithmen nicht öffentlich sind. Der GEA1-Standard war zum Beispiel geheim.

Leander: Heute ist die Auswahl von Verschlüsselungsverfahren öffentlich und transparent. Forschende reichen Vorschläge ein, in einem mehrstufigen Verfahren werden diese bewertet. Wenn da auch nur ein Hauch von Unklarheit ist, fliegt der Vorschlag sofort raus. Es gibt also bei öffentlichen Verfahren keine absichtlichen Schwachstellen mehr. Das ist auch einer der Gründe, warum wir beim Exzellenzcluster CASA glauben, dass Schutz gegen Geheimdienste wie die NSA möglich ist: Es existieren mathematische Verfahren, die niemand auf der Welt brechen kann. Daher darf man hoffnungsvoll sein.

Was nehmen Sie sich in Ihrer Forschung in Zukunft noch vor?

Leander: Wir suchen weiter nach Hintertüren. Es gibt Hinweise, dass es sie gibt, das Problem ist nur, sie zu finden. Wir beschäftigen uns damit, strukturiert zu suchen. Wir schauen uns große Programme an, sieben die Kryptografie heraus und analysieren sie – insbesondere die, die wir noch nicht kennen. Manche sind auch geheim. Im Fall von GEA-1 hat uns ein Whistleblower einen Hinweis gegeben. So ist es auch in einem weiteren Fall, den wir gerade untersuchen.

Wie kommt es, dass in der Öffentlichkeit keine Empörung aufbrandet, wenn solche Entdeckungen gemacht werden?

Leander: Es gibt keinen Aufschrei der Nutzer, aber schon einen großen Widerhall in der Presse. Das Interesse ist da.

Beierle: Vielleicht war bei GEA keine so große Empörung, weil das Verfahren schon so alt ist und keine Gefahr mehr davon ausgeht.

Rupprecht: Man muss den Endnutzern klar machen, was auf dem Spiel steht. Aber das Problem bleibt für viele sehr abstrakt. Anders ist das in der Industriecommunity. Da will man wirklich etwas tun.

Leander: Man muss tatsächlich zwischen Nutzenden und Entscheidern unterscheiden. Endnutzer kümmern sich nicht um ihre Daten. Die Nutzung von Social Media ist das Gegenteil davon. Auch tolle Services im Internet zu nutzen für kein Geld – wie geht das? Nur durch das Sammeln von Daten. Aber das ist den Leuten egal. Die Entscheidungsträger müssen sich kümmern. Das ist wie beim Autofahren: Wäre der Gurt nicht Pflicht, würde sich niemand anschnallen.

Text: md, Fotos: ms

Kryptowährungen

VERTEILTE VERANTWORTUNG

Kryptowährungen unterliegen keiner zentralen Kontrolle. Die Community ist an der Macht. Aber sie kümmert sie sich schlicht nicht um alles, was nötig wäre. Dadurch könnte die Sicherheit des Geldes auf dem Spiel stehen.

Bitcoin, Dogecoin, Digibyte – die Liste der derzeit existierenden Kryptowährungen ist sehr lang. So lang, dass die Namen kaum noch lesbar wären, würde man versuchen, sie alle auf eine DIN-A4-Seite zu quetschen. Es existieren tausende virtuelle Währungen, und sie sind längst kein Nischenprodukt mehr. Millionen Menschen nutzen sie. Für sie spielt IT-Sicherheit eine besonders große Rolle. Denn Geld ist letztendlich nichts anderes als Daten, die wie alle Daten potenziell verwundbar durch Cyberattacken sind.

Die Frage, wie gut gesichert verschiedene Kryptowährungen sind, treibt Prof. Dr. Ghassan Karame um. Er ist Leiter des Lehrstuhls Information Security am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum und ein Befürworter von dezentral organisierten Plattformen, wie sie auch Kryptowährungen zugrunde liegen. Die Idee dahinter ist einfach: Die Macht ist nicht an einer zentralen Stelle gebündelt, zum Beispiel in einer Bank. Stattdessen muss es für Entscheidungen immer eine Mehrheit unter den Nutzerinnen und Nutzern geben. „In solchen Systemen wäre es sehr schwer für eine zentrale Stelle, Zensur auszuüben, und sie

Bitcoin zählt zu den bekanntesten Kryptowährungen. Der Quellcode ist frei verfügbar im Internet – und wurde vielfach kopiert. So entstanden zahlreiche neue virtuelle Währungen.

SLOSIGKEIT

sind robust gegenüber Fehlern und Fehlverhalten, weil eine große Community von Entwicklerinnen und Entwicklern über das System wacht", nennt Karame zwei Vorteile von dezentral organisierten Plattformen. „Die Idee ist großartig und wahrscheinlich ist sie die Zukunft", ergänzt er. Wie bei jeder IT-Technik kann es aber natürlich auch bei Kryptowährungen Sicherheitslücken geben.

Bereits 2012 entdeckte Karame zusammen mit Kolleginnen und Kollegen ein besonders schwerwiegendes Problem in der Bitcoin-Nutzung, das dazu führte, dass Leute dieselben Bitcoins mehrmals ausgeben konnten, um verschiedene Dinge damit zu bezahlen. „Es war, als könnte man mit einem Fünf-Euro-Schein erst einen Burger kaufen und denselben Schein dann noch mal nutzen, um ein Eis zu bezahlen", veranschaulicht der Forscher.

Im Jahr 2015 dokumentierte Karame mit seinen Kolleginnen und Kollegen einen weiteren schwerwiegenden Fehler, der auftrat, nachdem Bitcoin sein System an eine größere Nutzerzahl angepasst hatte. „Wir haben gezeigt, dass wir den Informationsfluss im gesamten Bitcoin-System zum Erliegen ▸

i KRYPTOWÄHRUNGEN

Für virtuelle Währungen gibt es keine Zentralbank, die das Geld verwaltet. Das tun die Nutzerinnen und Nutzer selbst. Geldbeträge sind bestimmten Personen zugeordnet, die diese in einer digitalen Brieftasche speichern können. Die wohl bekannteste Kryptowährung ist Bitcoin.

In Deutschland besitzen Menschen Kryptogeld vor allem aus Experimentierfreude, Spekulationsgründen oder als Teil ihrer Geldanlage. In autokratisch geführten Staaten hingegen sind die virtuellen Zahlungsmittel auch deswegen interessant, weil Krypto-Finanzflüsse sich staatlichen Kontrollen entziehen. In Ländern mit extremer Inflation können sie Menschen zudem finanzielle Stabilität bieten: Bricht die Währung eines Landes ein, ist die Kryptowährung davon nicht betroffen.

bringen könnten, wenn wir Kontrolle über einige Dutzend Laptops im System besitzen würden“, beschreibt Ghassan Karame die Schwere der Schwachstelle. Um beide Sicherheitslücken hat Bitcoin sich längst gekümmert.

Aber es gibt nicht nur Bitcoin, sondern auch viele Kopien davon. Bitcoins Quellcode ist frei verfügbar im Internet. Wer mag, kann ihn kopieren und seine eigene Kryptowährung an den Start bringen. Auf diese Weise entstand beispielsweise Dogecoin, heute die Nummer 1 der Kryptowährungen im Gaming-Bereich. „Es gibt so viele Kryptowährungen, dass wir noch nicht mal alle kennen, und wir wissen erst recht nicht, wer sie betreibt“, sagt Ghassan Karame, der einer der vier Hub-Leader im Exzellenzcluster CASA ist. Denn das ist die Krux bei dezentralen Systemen. Weil die Entscheidungsgewalt verteilt ist, ist es schwierig für die Forschenden, Sicherheitslücken zu melden.

In der IT-Sicherheit gibt es das ethische Gebot des „Responsible Disclosure“. Wird eine Sicherheitslücke gefunden und bestätigt, so müssen die Forschenden immer erst den Betreiber des betroffenen Produkts informieren und ihm ausreichend Zeit geben, den Fehler zu beheben, bevor er veröffentlicht wird. So soll sichergestellt werden, dass die Einfallstore geschlossen werden, bevor Angreiferinnen und Angreifer sie ausnutzen können.

Aber wem soll man in einem dezentral organisierten System die Fehler berichten, wenn manchmal gar nicht klar ist, wer das System betreibt? Oder wenn man gar nicht weiß, wie viele und welche Systeme überhaupt betroffen sind? Wer entscheidet in einer solchen Struktur, ob die Software aktualisiert werden muss, um Sicherheitslücken zu schließen? Und wie kann man kontrollieren, ob eine Schwachstelle behoben wurde? Auf diese Fragen gibt es bislang keine Antworten.

Im Fall der oben beschriebenen Sicherheitslücken waren Karame und seine Kolleginnen und Kollegen in Kontakt mit verschiedenen Bitcoin-Entwicklerinnen und -Entwicklern. „Die Leute dort haben sehr gewissenhaft und schnell reagiert“, erinnert er sich. Aber für die zahlreichen Kopien von Bitcoin gab es keine Vorwarnung. Ghassan Karame möchte herausfinden, welche Auswirkungen diese unklaren Strukturen in der Praxis haben. Mit seinem Team untersuchte er verschiedene virtuelle Währungen, die leicht abgewandelte Kopien von Bitcoin sind. Für diese Alternativen hat sich der Begriff „Altcoins“ etabliert. Die Wissenschaftlerinnen und Wissenschaftler überprüften, wie lange es gedauert hat, bis in diversen Altcoin-Quellcodes Sicherheitslücken nach ihrem Bekanntwerden geschlossen wurden – beispielsweise die 2015 veröffentliche schwerwiegende Sicherheitslücke, die Karames Team gefunden hatte.

„Um es kurz zu machen: Die Ergebnisse waren schockierend“, fasst Ghassan Karame zusammen. Während Bitcoin die Sicherheitslücke in nur sieben Tagen behob, brauchte Litecoin beispielsweise 114 Tage, Dogecoin 185 Tage und Digibyte fast drei Jahre. „Drei Jahre, in denen man mit einigen Dutzend Laptops das gesamte System der Kryptowährung zum Zusammenbruch hätte bringen können“, unterstreicht Ghassan Karame und vergleicht: „Man stelle sich vor, Visa

Ghassan Karame leitet an der Ruhr-Universität Bochum den Lehrstuhl Information Security.

Auf der Plattform GitHub steht der Quellcode vieler Anwendungen, auch von der Kryptowährung Bitcoin, offen zur Verfügung, sodass er leicht kopiert werden kann.

würde drei Jahre brauchen, um eine Sicherheitslücke bei der Kreditkartenzahlung zu beheben."

Das Ergebnis der Bochumer Analyse klingt simpel, aber der Weg zu den Zahlen war langwierig. Das liegt an dem Kopiermechanismus, mit dem der Bitcoin-Code von den Altcoin-Anbietern geklont wird. Der Quellcode von Bitcoin und alle Modifikationen davon sind im Internet frei verfügbar auf der Plattform „GitHub". Aus diesem öffentlichen Projekt können Aktualisierungen also leicht kopiert oder importiert werden. Wer zum Beispiel eine Bitcoin-Kopie, also eine Altcoin, erstellen will, kann den Quellcode in GitHub über einen einfachen Befehl in sein eigenes Projekt kopieren.

Steht ein Sicherheitsupdate für Bitcoin bereit, das eine Altcoin-Entwicklerin bei sich einspielen möchte, verwendet sie dafür typischerweise den Befehl „Rebase". So muss sie nicht den eigenen Code mühsam umschreiben, sondern kann die erforderlichen Informationen direkt vom Bitcoin-Code in den eigenen transferieren. Das Problem für die Forschenden: Normalerweise haben in GitHub alle Modifikationen einen Zeitstempel, aber durch Nutzung des Rebase-Befehls können diese Metadaten verlorengehen. Aus dem Quellcode ist nachher nicht mehr leicht ersichtlich, wann ein Sicherheitsupdate eingebaut wurde.

Das Team musste daher zunächst ein Tool entwickeln, mit dem es den Zeitpunkt eines Sicherheitsupdates in einem verzweigten Quellcode näherungsweise bestimmen konnte. Dieses Tool basiert auf einem bereits existierenden GitHub-Archiv, das alle Ereignisse für öffentliche Projekte nachhält, etwa Code-Modifikationen oder Rebase-Operationen. So konnten die Forschenden Aktualisierungen im Code mit dem jeweiligen Event im Archiv zusammenbringen, um die Zeitpunkte der Sicherheitsupdates zu schätzen.

Auf diese Weise analysierten die Forschenden 44 der schwerwiegendsten Sicherheitslücken, die für Bitcoin und Altcoins bekannt sind. Es ergab sich stets das gleiche Bild: Bei vielen Altcoins dauerte es eine drei- oder gar vierstellige Anzahl von Tagen, bis die Fehler behoben waren. „Wir glauben, dass einige Kryptowährungen gewisse Schwachstellen bis heute gar nicht gepatcht haben", so Karame. Er ist sicher, dass das Problem eigentlich noch viel größer ist, als es seine erste Analyse gezeigt hat. „Ich habe beinahe Angst, noch genauer hinzuschauen", sagt er. „Wir haben bislang sicher nur die Spitze des Eisbergs gefunden."

Daher mahnt der Forscher zur Vorsicht: „Leute müssen vorsichtiger bei der Auswahl von Kryptowährungen sein, und nicht nur basierend auf den Profitaussichten entscheiden. Es bringt ihnen nichts, einen Haufen Geld zu machen, wenn es durch eine Sicherheitslücke am nächsten Tag komplett verschwunden sein kann." Eigentlich sollte man also nur mit Kryptowährungen handeln, deren Betreiber sich um Sicherheitsupdates kümmern. Aktuell hat man als Nutzer aber kaum eine Chance herauszufinden, ob das der Fall ist. Es bleibt abzuwarten, ob diese Lücke geschlossen wird, wenn dezentrale Plattformen noch populärer werden.

Text: jwe, Fotos: ms

> „DIE ERGEBNISSE WAREN SCHOCKIEREND."
>
> Ghassan Karame

WENN DIE **HARDWARE** DIE **TÄTER** ERTAPPT

Hardware vor Manipulationen zu schützen ist bislang eine mühsame Angelegenheit – teuer und nur in kleinem Maßstab möglich. Der Einsatz von Antennen könnte das ändern.

Bezahlvorgänge, Geschäftsgeheimnisse, Dokumente, die für die nationale Sicherheit bedeutsam sind: Die großen Geheimnisse der Welt sind heute oft nicht mehr auf Papier gespeichert, sondern als Einsen und Nullen im virtuellen Raum. Wenn man sie in Gefahr wähnt, stellt man sich zumeist eine Bedrohung aus der Ferne vor – Angreiferinnen und Angreifer, die über Cyberattacken versuchen, vertrauliche Daten zu erbeuten. Aber es gibt auch noch eine andere Bedrohung, einen viel direkteren Weg, in fremde Systeme zu gelangen: nämlich indem man sich an der Hardware zu schaffen macht. Die wertvollen Informationen sind letztendlich nichts anderes als elektrische Ströme, die zwischen verschiedenen Computer-Bauteilen über Leiterbahnen wandern. Ein winziger metallischer Gegenstand, an der richtigen Stelle der Hardware platziert, kann ausreichen, um diese Datenströme abzugreifen. „Betrüger haben diese einfache Methode zum Beispiel genutzt, um Kreditkartendaten aus Kartenlesegeräten abzugreifen“, wissen Paul Staat und Johannes Tobisch. Die beiden promovieren am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum und forschen am Bochumer Max-Planck-Institut für Sicherheit und Privatsphäre. Im Team von Prof. Dr. Christof Paar entwickeln sie Methoden, die vor Hardware-Manipulationen schützen sollen. Dabei kooperieren sie mit Prof. Dr. Christian Zenger von dem aus der Ruhr-Universität ausgegründeten Unternehmen PHYSEC, der zu seiner Zeit als Forscher die Grundlagen für diese Technik legte und seit kurzem Juniorprofessor an der Fakultät für Elektrotechnik und Informationstechnik ist.

Natürlich gibt es bereits Mechanismen, die Hardware vor Manipulationen schützen soll. „In der Regel ist das eine Art Folie mit dünnen Drähten, in die die Hardware-Komponente eingepackt ist“, erklärt Paul Staat. „Wird die Folie beschädigt, schlägt das System Alarm.“ Auf diese Weise lassen sich allerdings nur kleine Komponenten schützen, nicht das ganze System. Man kann also nicht ein ganzes Computergehäuse in die Folie einwickeln, sondern zum Beispiel nur ein besonders wichtiges Bauteil wie ein Speicherelement oder einen Prozessor. Tobisch und Staat feilen jedoch an einer Technik, die ganze Systeme auf Manipulationen überwachen soll – und obendrein nicht so teuer wäre.

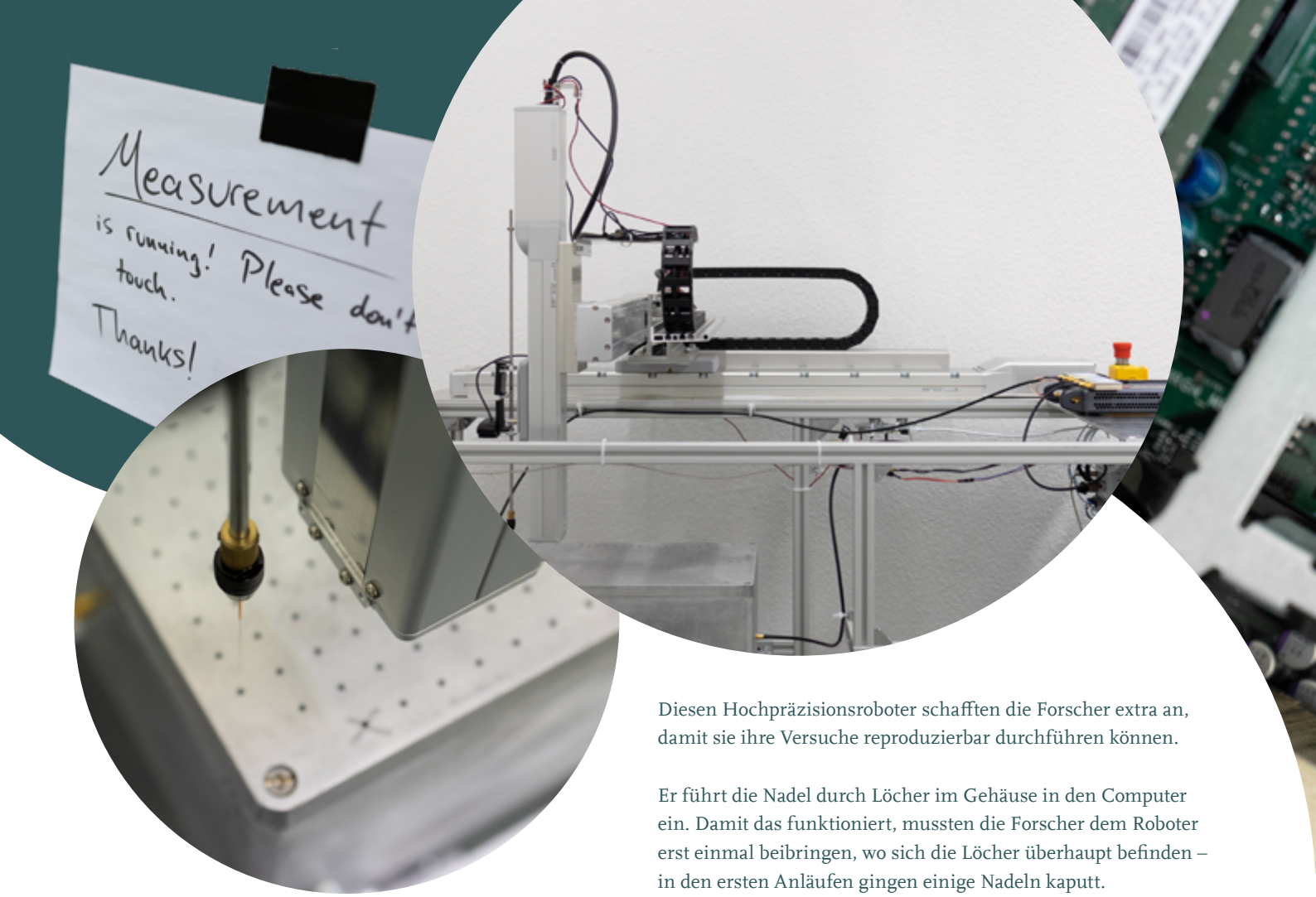
Dazu setzen sie auf Funkwellen. Sie verbauen in dem zu überwachenden System zwei Antennen: einen Sender und ei- ▸

Paul Staat (links) und Johannes Tobisch promovieren an der Ruhr-Universität und forschen am Bochumer Max-Planck-Institut für Sicherheit und Privatsphäre.

i MANIPULIERTE LESEGERÄTE

Forschende aus Cambridge haben schon 2008 gezeigt, wie leicht sich verschiedene Kartenlesegeräte manipulieren lassen – und das, obwohl die Hersteller sogar einen Manipulationsschutz eingebaut hatten. Dieser sichert aber nur einzelne Komponenten der Geräte, etwa den Prozessor. Auf den Leiterbahnen der Platine können die Daten dann aber doch abgegriffen werden: Es gelang den Wissenschaftlern, sowohl die Daten der eingeführten Karten als auch die eingetippten PINs auszulesen. Kriminelle Akteure gehen ähnlich vor und modifizieren Kartenlesegeräte sogar so, dass Daten ausgelesen und über Bluetooth übermittelt werden können. „Für solche Manipulationen gibt es einen regelrechten Markt“, weiß Paul Staat.

Mithilfe eines Hochpräzisionsroboters untersuchen Bochumer Forscher, ob sie mit ihrer Technik Hardware-Manipulationen aufspüren können.



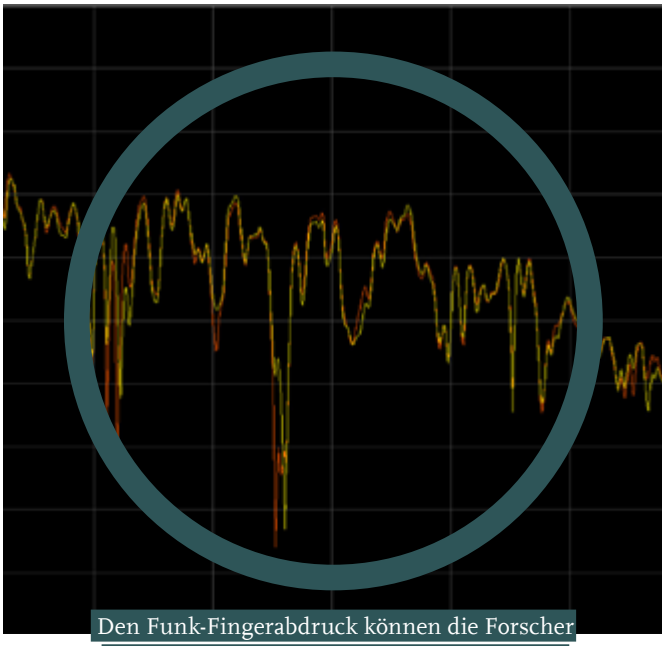
Diesen Hochpräzisionsroboter schafften die Forscher extra an, damit sie ihre Versuche reproduzierbar durchführen können.

Er führt die Nadel durch Löcher im Gehäuse in den Computer ein. Damit das funktioniert, mussten die Forscher dem Roboter erst einmal beibringen, wo sich die Löcher überhaupt befinden – in den ersten Anläufen gingen einige Nadeln kaputt.

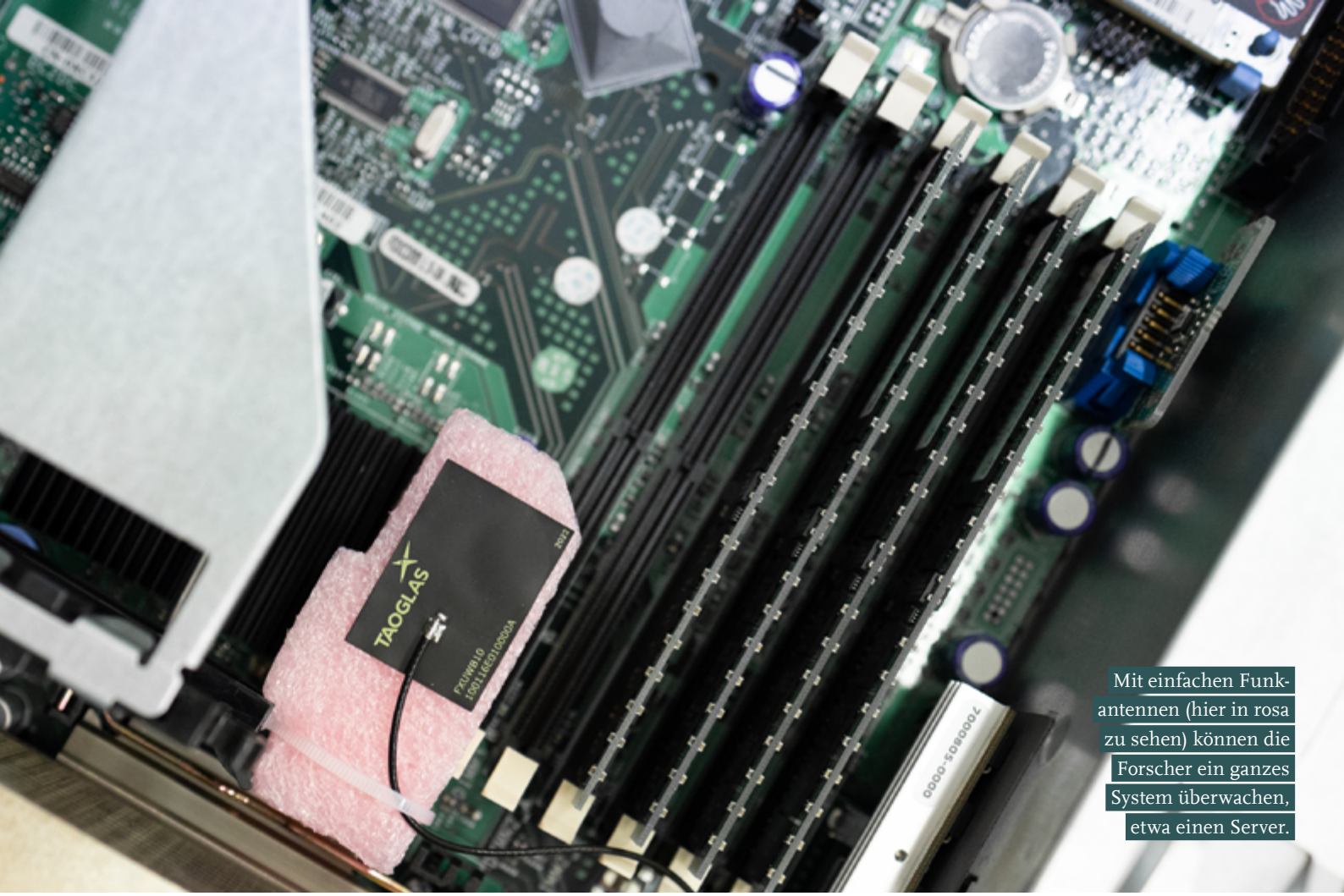
nen Empfänger. Der Sender schickt ein spezielles Funksignal in die Umgebung, das sich überall im System ausbreitet und an den Wänden und Computerkomponenten reflektiert wird. Durch all diese Reflektionen kommt beim Empfänger ein Signal an, das für das System so charakteristisch ist wie ein Fingerabdruck.

Winzige Veränderungen am System reichen aus, um den Fingerabdruck merklich zu beeinflussen, wie eine Demonstration der beiden Forscher zeigt: Ihre Funktechnik haben Paul Staat und Johannes Tobisch in ein altes Computergehäuse eingebaut. Das gemessene Funksignal machen sie auf einem Laptop als Kurve sichtbar, welche die Stärke des Signals bei verschiedenen Frequenzen in Echtzeit darstellt. Dann drehen sie aus dem überwachten Objekt eine der außen im Gehäuse sitzenden Schrauben ein kleines Stück heraus. Und schon reagiert die Frequenzkurve mit einem merklichen Ausschlag, der zuvor nicht da war.

Für ihre Forschung gehen Johannes Tobisch und Paul Staat die Untersuchungen aber systematischer an. Ihr Testobjekt ist ein herkömmlicher Computer, dessen Gehäuse sie in regelmäßigen Abständen mit Löchern versehen haben. Durch diese Löcher können sie eine feine Metallnadel in das Innere des Systems eindringen lassen und überprüfen, ob sie die Veränderung im Funksignal bemerken. Sie variieren dabei die Dicke der Nadel, die Position und die Eindringtiefe. Damit der Versuch unter kontrollierten und reproduzierbaren Bedingungen stattfindet, haben die beiden Forscher extra einen Hochpräzisionsroboter angeschafft, der die Nadel mi-



Den Funk-Fingerabdruck können die Forscher als Kurve sichtbar machen (rot). Sie zeigt die Stärke des Signals bei verschiedenen Frequenzen. Dringt die Nadel in das System ein, reagiert die Kurve mit merklichen Ausschlägen (gelb). (Bild: Paul Staat)



Mit einfachen Funkantennen (hier in rosa zu sehen) können die Forscher ein ganzes System überwachen, etwa einen Server.

krometergenau in das Gehäuse einführt. „Eine Besonderheit ist, dass wir den Versuch durchführen, während der Computer läuft“, sagt Tobisch. Das erzeugt allerhand Störungen. „Die Lüfter sind wie kleine Staubsauger und der Prozessor ist wie eine Heizung“, vergleicht Staat. Diese Schwankungen in den Umgebungsbedingungen beeinflussen das Funksignal. Solche Störungen müssen die Forscher messen und herausrechnen, um unterscheiden zu können, ob Schwankungen im Signal legitim sind oder durch Manipulationen zustande kommen.

Das Eindringen einer 0,3 Millimeter dicken Nadel können die Bochumer IT-Experten mit ihrem System ab einer Eindringtiefe von einem Zentimeter zuverlässig erkennen. Selbst bei einer Nadel von 0,1 Millimeter Dicke – etwa so dick wie ein Haar – schlägt das System noch an, allerdings nicht an allen Positionen. „Je näher sich die Nadel zur Empfangsantenne befindet, desto leichter ist sie zu detektieren“, erklärt Staat. Je dünner und weiter weg die Nadel, desto höher die Wahrscheinlichkeit, dass sie unbemerkt bleibt. Ebenso ist es mit der Eindringtiefe: Je tiefer die Nadel im System steckt, desto leichter ist sie zu erkennen. „Für die Praxis ist es also sinnvoll, sich genau zu überlegen, wo man die Antennen platziert“, resümiert Tobisch. „Sie sollten sich möglichst nah bei den besonders schützenswerten Komponenten befinden.“

Ihren Versuch ließen Johannes Tobisch und Paul Staat zehn Tage laufen und zeigten somit, dass das Messsystem über lange Zeit stabil ist. Später dehnten sie die Messdauer sogar auf einen ganzen Monat aus. Neben teurer, sehr präziser Messtechnik zum Aufzeichnen des Fingerabdrucks werteten sie das Funksignal zum Vergleich auch mit einfacher Technik aus, die für ein paar Euro zu haben ist. Das funktionierte ebenfalls, wenn auch mit einer etwas geringeren Trefferquote. „Es ist immer ein Kompromiss aus Kosten und Genauigkeit“, sagt Paul Staat.

Je nach Einsatzzweck müsste auch noch der Einfluss von Umweltfaktoren berücksichtigt werden. Denn wenn sich die Temperatur oder Luftfeuchtigkeit im Raum ändert, kann das auch den Funk-Fingerabdruck ändern. „Wir hoffen, solche Probleme in Zukunft mithilfe von Maschinellem Lernen angehen zu können“, blickt Johannes Tobisch voraus. Künstliche Intelligenz könnte selbstständig lernen, welche Veränderungen im Funksignal auf unkritische Umgebungsveränderungen zurückzuführen sind und welche auf Manipulationen – so die Idee.

„Prinzipiell steht einer breiten Anwendung der Technik nichts im Wege. Sie eignet sich sowohl für Hochsicherheitsanwendungen als auch für Alltagsprobleme“, sagt Christian Zenger, Gründer und Geschäftsführer von PHYSEC. Das IT-Unternehmen nutzt die Technik bereits, um unerlaubte Manipulationen an kritischen Infrastrukturkomponenten zu verhindern. „Weitere technische Systeme, die nicht nur vor Cyberattacken aus der Ferne, sondern auch vor Hardware-Manipulationen geschützt werden müssen, gibt es genug“, ergänzt er. „Beispielsweise Steuergeräte in Autos, Stromzähler, Medizingeräte, Satelliten und Serviceroboter.“

Text: jwe, Fotos: ms

Der menschliche Faktor

WIE SICHER SICH **MENSCHEN WELTWEIT IM INTERNET** FÜHLEN

Wer war schon von Cyberkriminalität betroffen? Was unternehmen Menschen, um sich davor zu schützen? Eine Umfrage zeigt Gemeinsamkeiten und Unterschiede zwischen verschiedenen Gruppen in aller Welt.

Im Internet gilt erst recht, was der Volksmund sagt: Das Böse ist immer und überall. Durch sicheres Verhalten können wir es Cyberkriminellen jedoch schwerer machen, Daten zu erbeuten oder anderen Schaden anzurichten. Aber was ist sicheres Verhalten? Was muss man tun, um sich vor Datendiebstahl und Co. zu schützen? „Darüber herrscht viel Unsicherheit, und zwar bei Menschen in aller Welt", hat Franziska Herbert herausgefunden. Die studierte Psychologin fertigt zurzeit ihre Dissertation im Exzellenzcluster CASA am Horst-Görtz-Institut für IT-Sicherheit an. Gemeinsam mit Prof. Dr. Markus Dürmuth, Prof. Dr. Angela Sasse und anderen Kolleg*innen hat sie eine große Umfrage durchgeführt, die den menschlichen Faktor in der IT-Sicherheit ausleuchtet.

Über 12.000 Menschen in zwölf Ländern haben an der Online-Umfrage teilgenommen, in der es darum ging, welches Verständnis Menschen von sicherem Verhalten im Cyberspace haben, welche Einstellung sie dazu haben und welchen Missverständnissen sie möglicherweise aufsitzen. Die Teilnehmenden stammten aus China, Deutschland, Großbritannien, Indien, Israel, Italien, Mexiko, Polen, Saudi-Arabien, Schweden, den USA und Südafrika. Sie repräsentieren 42 Prozent der Weltbevölkerung. Die Fragen drehten sich zum Beispiel um Ende-zu-Ende-Verschlüsselung, Surfen im WiFi, den https-Standard, Virtual Private Networks, kurz VPN, und Passwörter. „Es hat sich gezeigt, dass einige Risiken durchaus allen Teilnehmenden in aller Welt gleichermaßen bekannt sind", berichtet Franziska Herbert, die den Fragebogen selbst mit dem Team designt hat. Dazu gehört etwa das Phänomen des Shouldersurfing, bei dem Unbeteiligte private Daten durch den Blick über die Schulter eines Nutzers oder einer Nutzerin ausspähen.

Aber auch einige Missverständnisse sind offenbar weltweit verbreitet. „Es glauben zum Beispiel in allen Ländern, die wir in der Umfrage abdecken konnten, 80 Prozent der Menschen, dass es für die Sicherheit notwendig sei, ihr Passwort regelmäßig zu ändern", so Herbert. Diesen Rat haben IT-Sicherheitsspezialisten lange Zeit auch wirklich gegeben, bis sich erwiesen hat, dass dieses Vorgehen nichts Gutes bewirkt. „Die Passwörter werden dadurch nur immer unsicherer, weil man sie sich sonst nicht mehr merken kann. Besser ist es, wirklich starke Passwörter zu wählen, die nicht leicht zu knacken sind – dazu ist ein Passwort-Manager sehr hilfreich", sagt Herbert. „Dabei kann man dann aber auch bleiben, solange die Passwörter nicht in falsche Hände geraten."

Teilnehmende aller Länder stimmten auch der Aussage zu, dass ihr PC von Malware infiziert werden könne, wenn sie auf einen Link klicken. „Das trifft nur in wenigen Ausnahmefällen zu", so die Forschenden, „meistens braucht es dafür noch weitere Aktionen wie die Eingabe von Daten in die über den Link aufgerufene Webseite."

Was die Wissenschaftler*innen ebenfalls weltweit feststellen konnten, war eine generelle Unsicherheit in Bezug auf IT-Sicherheitsfragen. „Das zeigt sich darin, dass die Leute bei vielen Fragen auf einer Skala von absoluter Zustimmung bis zu kompletter Ablehnung genau die Mitte gewählt haben", sagt Franziska Herbert.

Abseits aller Gemeinsamkeiten konnten die Forschenden jedoch auch Unterschiede zwischen Teilnehmenden aus verschiedenen Ländern feststellen, vor allem in der Größenordnung der Einschätzungen. „Die größten Unterschiede haben wir hier zwischen westlichen und nicht-westlichen Ländern gefunden", so Franziska Herbert. Zu letzteren zählen die Forschenden China, Indien, Mexiko, Saudi-Arabien und Südafrika. „Im Vergleich zu den Deutschen hatten die Teilnehmenden in allen anderen Ländern eher falsche Vorstellungen in Bezug auf Malware, Gerätesicherheit und Passwörter", erklärt die Forscherin. Die deutschen Befragten stimmen falschen Aussagen am wenigsten zu – wenn auch immer noch in mittlerem Ausmaß der Skala zwischen voller Zustimmung und kompletter Ablehnung. Die größte Zustimmung zu missverständlichen Aussagen gab es von Teilnehmenden aus China und Indien.

In der Öffentlichkeit genügt ein Blick über die Schulter, um zum Beispiel Passwörter auszuspähen.

80 %

DER MENSCHEN GLAUBEN, DASS ES FÜR DIE SICHERHEIT NOTWENDIG SEI, IHR PASSWORT REGELMÄSSIG ZU ÄNDERN.

Zwei Beispiele aus dem Fragebogen:

„Es ist wahrscheinlicher, dass ich mir beim Besuch einer Pornowebseite Schadsoftware einfange, als wenn ich eine Webseite zum Thema Sport besuche." Diesem Missverständnis-Item stimmten in Deutschland etwa 49 Prozent der Befragten zu, während 75 Prozent aus Saudi-Arabien und 86 Prozent aus China dem Item zustimmten.

Der richtigen Aussage „Links in E-Mails können mich auf gefälschte Webseiten führen, um so meine Login-Daten abzufangen" stimmten 87 Prozent der deutschen Teilnehmenden zu, und 78 Prozent der chinesischen Teilnehmenden.

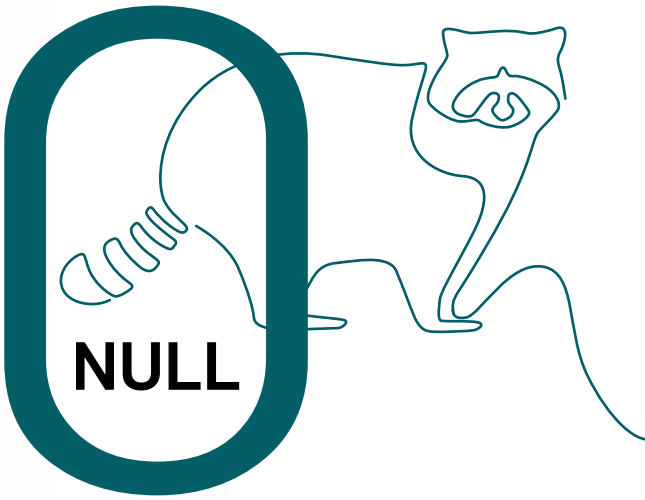
Alle befragten Gruppen hatten gemeinsam, dass sie in Familie und Freunden eher kein IT-Sicherheitsrisiko sehen. „Das sehen wir anders", sagt Markus Dürmuth. Gerade wenn man sich einen Computer teile oder Passwörter weitergebe, gebe es durchaus Risiken. Im Zusammenhang mit häuslicher Gewalt oder Stalking seien es oft gerade Menschen aus dem nahen persönlichen Umfeld, die ein Risiko darstellen. „Im Freundeskreis gibt es auch Scherze im weiteren Sinne, die für das Opfer gar nicht lustig sind", so der Forscher.

Text: md, Fotos: ms

Franziska Herbert will wissen, wie sicher sich Menschen im Internet fühlen und welche Erfahrungen sie gemacht haben.

Die Berechnungen für den Angriff namens RACCOON erfolgten auf der lehrstuhleigenen Cloud.

DIE VERRÄTERISCHE NULL



Angriffe auf TLS-Protokolle sind selten. Und höchst komplex. Doch die Verschlüsselungsexperten der Ruhr-Universität kommen ihnen immer wieder auf die Schliche.

Etwa tausend Seiten umfasst der dicke Wälzer, der alle technischen Details zum Verschlüsselungsprotokoll TLS enthält. Damit ist der TLS-Standard so dick wie drei Harry-Potter-Bände. „Es braucht viel Zeit und Krypto-Knowhow, um alle Features zu verstehen und zu überblicken“, weiß Dr. Robert Merget vom Lehrstuhl für Netz- und Datensicherheit am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum. Hier hat man sich schon vor Jahren auf die Transport Layer Security, kurz TLS, spezialisiert. Das kryptografische Verschlüsselungsprotokoll sorgt dafür, dass zum Beispiel Verbindungen zwischen Internetbrowsern und Servern oder zwischen verschiedenen E-Mail-Servern sicher sind. Merget und seine Kolleginnen und Kollegen kennen den Standard fast auswendig und beherrschen somit sämtliche Tricks und TLS-Verschlüsselungszauber. Seit 2015 entwickeln sie ein TLS-Analyse-Tool.

Das Tool ermöglicht Unternehmen, TLS möglichst fehlerfrei einzusetzen, sodass keine Sicherheitslücken für Angreifer entstehen. Fast täglich stoßen die Forschenden dabei auf Schwachstellen bei der Implementierung, sogenannte bugs. „Systematische Attacken auf den TLS-Standard hingegen sind eher selten geworden“, weiß Merget. Und doch kommen sie vor. 2020 entdeckte der Krypto-Experte einen hoch-spezialisierten Angriff auf einen spezifischen TLS-Algorithmus, und warnte die Fachwelt vor der gefährlichen RACCOON-Attacke, zu Deutsch Waschbär-Angriff.

„Wir verwenden leicht zu merkende Namen für die sonst recht technisch lautenden Schwachstellen. So können wir in der Community leichter darüber reden“, erklärt Merget. Die Community – das sind Forschungsinstitutionen, aber vor allem IT-Unternehmen wie etwa Google, Microsoft oder Cloudflare, die alle ein Interesse daran haben, dass TLS so sicher wie möglich ist, und fortwährend daran mitarbeiten.

Das Verschlüsselungsprotokoll TLS ist für alle öffentlich einsehbar. „Die Algorithmen sind öffentlich, aber die ▸

Schlüssel, die verwendet werden, sind geheim“, betont Merget. „Man muss sich das wie eine Geheimsprache vorstellen.“ Früher habe man bei Geheimsprachen häufig Buchstaben vertauscht. Wer das genaue Verfahren kannte, also wusste, welcher Buchstabe durch welchen ersetzt werden muss, konnte die Botschaft entschlüsseln. Verfahren geheim zu halten habe sich jedoch als schwierig und unsicher erwiesen. Darum geht man heute anders vor. „Moderne Algorithmen sind öffentlich, aber die Schlüssel für die Algorithmen sind geheim. Bei TLS funktioniert das genauso. Der Feind darf das Verschlüsselungsprinzip kennen, aber die Schlüssel werden geheim gehalten“, erklärt Robert Merget. Die TLS-Kryptografie soll vor allem verhindern, dass Dritte mitlesen. Das Protokoll hat darüber hinaus zwei weitere Eigenschaften: Zum einen dient TLS der Authentifikation, zum anderen der Integrität der Daten.

Etwa vier Milliarden Nutzerinnen und Nutzer weltweit verwenden heute TLS. Und alle haben unterschiedliche Wünsche und Ansprüche an das Verschlüsselungsprotokoll. Das erklärt, warum so viele Entwicklerinnen und Entwickler über Jahre am TLS-Standard getüftelt und gefeilt haben – und auch, warum das Protokoll mittlerweile als sicher gilt. Das war jedoch nicht immer so.

„Seit 1994, seitdem es TLS gibt, hat es etliche Angriffe auf das Protokoll gegeben. Vor allem zwischen 2011 und 2016 gab es viele Attacken“, berichtet Merget. Der Krypto-Experte betont dabei: „Das ist in der Regel nichts, was der nächste Nachbarschaftshacker machen kann. Das sind schon schwierige High-Tech-Angriffe, wie sie von Geheimdiensten ausgeübt werden könnten. Davor müssen normale Nutzerinnen und Nutzer in der Regel keine Angst haben.“ Seit 2018, seit der Einführung des modernisierten Standards TLS 1.3, seien die Angriffe deutlich weniger geworden. Und dennoch: Angriffe auf die TLS-Versionen von 1996 bis 2018 kommen noch immer vor. 2020 entdeckte Robert Merget besagte Schwachstelle, die er RACCOON taufte.

Der RACCOON-Angriff greift das sogenannte Diffie-Hellman-Schlüsselaustausch-Protokoll an, also einen ganz be-

i DIE ERFINDUNG DES TLS

Das Verschlüsselungsprotokoll TLS wurde 1994 von der Firma Netscape (heute: Firefox) entwickelt und hieß erst SSL (kurz für: Secure Sockets Layer). 1999 benannte die Internet Engineering Task Force SSL in TLS um, da man überzeugt davon war, dass das Protokoll zur Datensicherheit im Internet nicht in den Händen eines Unternehmens liegen darf.

Robert Merget hat sich in seiner Forschung auf das Verschlüsselungsprotokoll TLS spezialisiert.

Die Krypto-Experten der Ruhr-Universität Bochum haben den Netzwerkverkehr stets im Auge und arbeiten an TLS-Analyse-Tools.

> „SEIT 1994, SEITDEM ES TLS GIBT, HAT ES ETLICHE ANGRIFFE AUF DAS PROTOKOLL GEGEBEN.“
>
> Robert Merget

stimmten Algorithmus, der in TLS genutzt werden kann und der sicherstellen soll, dass zum Beispiel eine Bank und eine Bankkundin ein gemeinsames Geheimnis, einen gemeinsamen Schlüssel, austauschen können.

Ganz konkret nutzt der Angreifer eine Timing-Schwachstelle in der Schlüsselableitung aus, wenn der Diffie-Hellman-Algorithmus verwendet wird: Die Dauer der Schlüsselableitung und damit der kryptografischen Weiterverarbeitung des Geheimnisses gibt dem Angreifenden die Info, die er braucht, um die Daten zu entschlüsseln und damit die Vertraulichkeit des Protokolls zu verletzen.

„Die Zeit ist ein sogenannter Seitenkanal, einer von vielen, der es ermöglicht, Rückschlüsse über den geheimen Schlüssel eines Algorithmus zu ziehen und ihn möglicherweise zu knacken“, erklärt Merget. „Nehmen wir an, ich verschlüssle das Wort Hund oder das Wort Katze. Für das Wort Katze brauche ich länger, da es mehr Buchstaben hat. Ein Angreifer oder eine Angreiferin kann die Zeit, die ich zum Verschlüsseln brauche, messen und die gemessene Zeit wiederum nutzen, um Rückschlüsse zu ziehen auf das, was verschlüsselt wurde“, erläutert Merget. Neben der Zeit würden auch Temperaturanstiege oder der Stromverbrauch von Geräten Auskunft über die Rechenoperationen einer Verschlüsselung geben – auch das seien Seitenkanäle, die es Angreifenden unter Umständen ermöglichen, an Schlüssel zu gelangen.

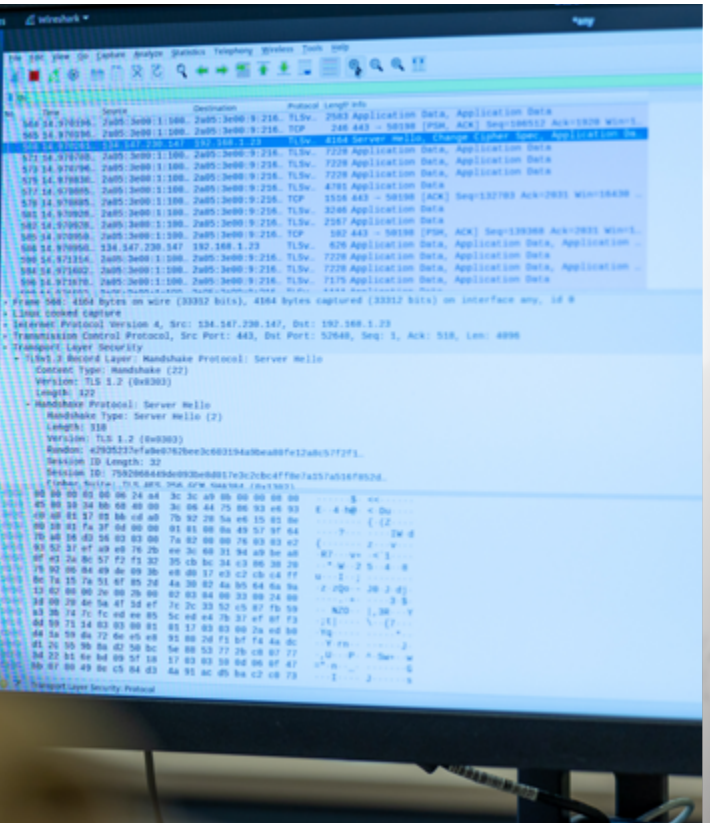
Das Konzept hinter dem Waschbär-Angriff sei leicht zu verstehen. „Ganz grob gesagt geht es beim Diffie-Hellman-Schlüssel immer um Rechnen mit Rest“, so Merget. In den knifflig en mathematischen Ableitungen des Diffie-Hellman-Schlüsselaustausches wird mit dem Rest ohne führende Nullen weiter gerechnet. „Kleinere Zahlen zu verarbeiten geht aufgrund der geringeren Datenmenge schneller. Das gibt dem Angreifer einen Vorteil: Er beobachtet, wie schnell eine Operation war, und schließt dann daraus, ob eine führende Null vorhanden war oder nicht“, erklärt der Forscher. Das ist die Schwachstelle, die der Angreifer ausnutzt. Aus den gesammelten Informationen kann er dann den geheimen Schlüssel rekonstruieren. „Dazu braucht es jedoch komplizierte mathematische Verfahren aus dem Bereich der Linearen Algebra“, weiß Robert Merget.

Um zu schauen, wie verbreitet die Schwachstelle ist, schickte Merget über eine spezielle Internetleitung Datenpakete an etwa 100.000 Server, die TLS nutzen. „Drei Prozent des weltweiten Internets antworteten und waren von dieser anfälligen TLS-Konfiguration betroffen“, so Merget.

„Wir haben zunächst alle Entwicklerinnen und Entwickler von wichtigen TLS-Implementierungen angeschrieben und gewarnt. Außerdem haben wir den Fall dem Bundesamt für Sicherheit in der Informationstechnik gemeldet und dieses gebeten, uns bei dem sogenannten Responsible-Disclosure-Prozess zu unterstützen“, berichtet der Wissenschaftler. Bei diesem in der IT-Sicherheit etablierten Verfahren zur Offenlegung von Sicherheitslücken geht es darum, die Hersteller umgehend über Schwachstellen zu informieren sowie Updates und Korrekturen bereitzustellen, bevor die Öffentlichkeit davon erfährt.

Wie lässt sich die Schwachstelle beheben? „Die beste Gegenmaßnahme ist es, die neueste und sichere Version von TLS zu verwenden, TLS 1.3“, so die Empfehlung Mergets. Insgesamt, davon ist er überzeugt, sei das TLS-Protokoll aber sehr sicher: „Es ist äußerst schwierig, noch Schwachstellen zu finden.“

Text: lb, Fotos: ms



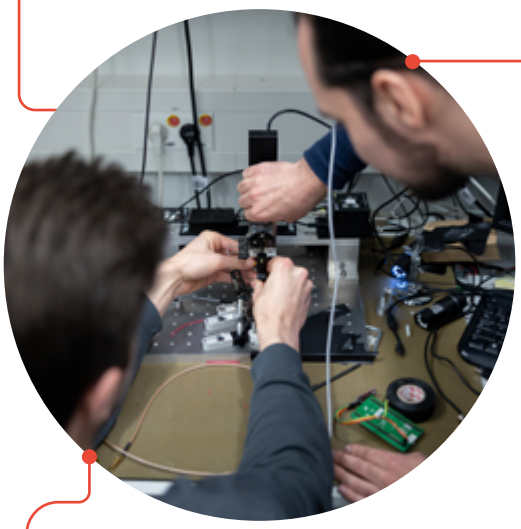
Knifflige Berechnungen: Beim Entschlüsseln kommen mathematische Verfahren aus dem Bereich der Linearen Algebra zum Einsatz.

Seitenkanalangriffe

WENN DEM **CHIP** DER KOPF RAUCHT

Viele Verschlüsselungsalgorithmen sind mathematisch bewiesen hundertprozentig sicher. Trotzdem können sie geheime Daten manchmal nicht schützen. Weil Verschlüsselung eben nicht nur in der Theorie passiert.

Mit einem elektronischen Chip ist es ein bisschen wie mit einem Menschen, der unter Zeitdruck eine komplizierte Aufgabe lösen muss. Viele kennen sicher das Gefühl, wenn einem der Kopf vor lauter Denksport raucht und richtig warm wird. Eventuell kommt Heißhunger auf etwas Süßes hinzu, weil man den Eindruck hat, mehr Energie zu brauchen. In Gedanken versunken fängt man vielleicht sogar an, etwas vor sich hinzumurmeln. Ganz ähnlich macht es auch ein elektronischer Chip, der den Job hat, Daten zu verschlüsseln. Während er seine Aufgabe vollbringt, kann er warm werden, sein Stromverbrauch kann steigen, und er kann akustische Signale von sich geben. Und das kann ein



Im Labor können die Forschenden Seitenkanalangriffe nachstellen.

Sicherheitsrisiko sein. Nämlich dann, wenn die Veränderungen in den physikalischen Parametern etwas über die Daten verraten, die der Chip gerade verschlüsselt.

Dass das der Fall sein kann, wurde längst mehrfach gezeigt. Forschende sprechen in diesem Fall von Seitenkanalangriffen, weil nicht der Verschlüsselungsalgorithmus selbst geknackt wird, sondern Begleitinformationen herangezogen werden, um die geheimen Daten auszulesen. Allein schon die Zeit, die es braucht, um gewisse Daten zu verschlüsseln, kann etwas über den Inhalt der Daten selbst aussagen. ▸

Das Forschungsteam: Nicolai Müller, Pascal Sasdrich, David Knichel und Amir Moradi (von links)

„Solche Angriffe sind gar nicht so aufwendig“, sagt Dr. Pascal Sasdrich vom Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum. „Das ist nichts, was nur Organisationen wie die NSA können. Theoretisch kann jeder Seitenkanalangriffe aus seiner Garage durchführen. Das Equipment dafür kostet nur rund 200 Euro.“ Betroffen sein können Funkautoschlüssel, Kartenlesegeräte, Smart-Home-Techniken und vieles mehr.

Pascal Sasdrich forscht an der Fakultät für Informatik in der Emmy-Noether-Nachwuchsgruppe „Computer-Aided Verification of Physical Security Properties“, kurz CAVE. Gemeinsam mit weiteren Kollegen aus der Arbeitsgruppe Implementation Security von Prof. Dr. Amir Moradi beschäftigt er sich mit der Frage, wie man herausfinden kann, ob ein elektronisches Bauteil vor Seitenkanalangriffen sicher ist – und wie man eine sichere elektronische Schaltung bauen kann. „Bei der Implementierung von kryptografischen Verfahren geht es Herstellern oft darum, dass Chips möglichst klein, möglichst effizient oder möglichst schnell sind“, weiß Pascal Sasdrich. Die Sicherheit steht dabei in der Regel nicht an erster Stelle. Hinzu kommt, dass ein einziger Flüchtigkeitsfehler bei der Implementierung der Verschlüsselungstechnik reicht, um ein Einfallstor für Angreiferinnen und Angreifer zu öffnen. Das Bochumer Team entwickelt daher Tools, die Hersteller bei der Implementierung von Verschlüsselungstechnik unterstützen sollen.

Dazu muss man zunächst einmal herausfinden können, ob eine vorhandene elektronische Schaltung sicher ist oder nicht. Amir Moradi hat dafür das sogenannte SILVER-Verfahren entwickelt. Die Abkürzung steht für Statistical Independence and Leakage Verification. Der Name verrät bereits, was der Schlüssel zum Erfolg ist: statistische Unabhängigkeit. SILVER überprüft, ob die beobachtbaren physikalischen Parameter wie Stromverbrauch oder Temperatur während der Verschlüsselung statistisch unabhängig von den Daten sind, die verschlüsselt werden. Liegt eine statistische Unabhängigkeit vor, erlauben die physikalischen Parameter keine Rückschlüsse auf den Inhalt der Daten.

„Früher wurden andere Kriterien für die Verifikation von sicheren Schaltungen herangezogen, nicht die statistische Unabhängigkeit“, sagt Sasdrich. „Die Methoden beruhten auf Annahmen oder Schätzungen und haben teils falsch negative Ergebnisse erzeugt.“ Verfahren wurden also als unsicher eingestuft, obwohl sie es in der Praxis gar nicht waren. Diese Fehler passieren mit dem SILVER-Verfahren nicht.

„SILVER ist hundertprozentig sicher, weil es auf einer sehr umfangreichen Analyse basiert“, unterstreicht Amir Moradi, schränkt aber ein: „Es funktioniert allerdings noch nicht für größere Schaltungen, weil der Aufwand dann explodieren würde.“ Für große Schaltungen nutzen die Bochumer Forschenden derzeit simulationsbasierte Methoden, die auch für komplexe Systeme effizient sind. „Allerdings sind sie nicht hundertprozentig sicher“, so Moradi. Sein Team sucht nun nach Möglichkeiten, die Sicherheit von größeren Schaltungen mit einer hohen Zuverlässigkeit überprüfen zu können.

Könnte man die komplexeren Systeme nicht einfach in mehrere Bestandteile zerlegen und diese einzeln überprüfen? „Man kann einzelne Teile anschauen und beweisen, dass sie sicher sind. Wenn man sie dann zusammenfügt, heißt das aber nicht, dass die gesamte Schaltung auch sicher ist“, erklärt Pascal Sasdrich. Denn an den Schnittstellen der Bestandteile können sich Einfallstore für Angreifer ergeben.

An Lösungen für dieses Problem arbeiten David Knichel und Nicolai Müller, ebenfalls aus der Bochumer Arbeitsgruppe Implementation Security. Die IT-Experten entwickeln Bausteine für elektronische Schaltungen, die sich sicher miteinander kombinieren lassen, sodass auch die zusammengesetzte Schaltung garantiert resistent gegen Seitkanalangriffe ist. Die einzelnen Module bezeichnen sie als Gadgets. „Man benötigt gar nicht viele verschiedene Gadgets, um eine Schal-

i BITS

Ein Bit ist die kleinste Informationseinheit, mit der herkömmliche Computer arbeiten. Es kann die Werte „null“ und „eins“ annehmen. Komplexe Informationen bestehen aus vielen verschiedenen Bits, die bei der Verarbeitung im Computer durch logische Operationen miteinander verknüpft werden.

Die Forschenden entwickeln Tools, welche Hersteller dabei unterstützen, elektronische Schaltungen sicherer zu machen.

tung zu realisieren“, erklärt David Knichel. Die Gadgets bilden zum Beispiel bestimmte logische Operationen ab, etwa die Multiplikation von zwei Bits, die häufig benötigt wird. Würde man allerdings für jede logische Operation, die in der Schaltung passieren muss, ein eigenes Gadget einsetzen, würde das Konstrukt extrem viel Platz verbrauchen. Denn im Verschlüsselungsprozess müssen viele Bits miteinander multipliziert werden. David Knichel und seine Kollegen arbeiten daher daran, den Funktionsumfang einzelner Gadgets zu erweitern, beispielsweise so, dass ein Gadget gleich mehrere Bits parallel multiplizieren kann. Das würde die Schaltung schneller und kleiner machen.

Die Gadgets des Bochumer Teams liegen allerdings nicht als real existierende Bauteile vor, sondern in Form von Code. „Wir nutzen eine spezielle Hardware-Beschreibungssprache“, sagt Knichel. Damit liefern er und seine Kollegen quasi eine Bauanleitung für Hersteller.

Allerdings ist es eine mühsame Angelegenheit, elektronische Schaltungen manuell vor Seitenkanalangriffen zu schützen. „Wir haben daher ein Tool namens AGEMA entwickelt, das auf Knopfdruck eine ungeschützte Schaltung in eine beweisbar sichere Schaltung überführen kann“, erklärt Nicolai Müller. AGEMA steht für Automated Generation of Masked Hardware. Das Tool checkt, welche logischen Operationen in einer Schaltung vorhanden sind, und ersetzt unsichere Bestandteile durch die sicheren Gadgets. „Wir können dabei auch gewisse Wünsche berücksichtigen, also die Schaltung zum Beispiel im Hinblick auf Geschwindigkeit oder Größe optimieren“, so Müller.

Noch handelt es sich bei den entwickelten Tools um erste Schritte in der Grundlagenforschung, nicht um industriell einsetzbare Lösungen. Denn zum automatisierten Schutz von elektronischen Schaltungen gegen Seitenkanalangriffe wird weiterhin sehr viel geforscht. Die Bochumer IT-Experten werden ebenfalls intensiv an optimierten Lösungen arbeiten . Manchmal sicher auch, bis ihnen die Köpfe rauchen.

Text: jwe, Fotos: ms

> „THEORETISCH KANN JEDER SEITENKANAL-ANGRIFFE AUS SEINER GARAGE DURCHFÜHREN.“
>
> Pascal Sasdrich

Wie ein Baukasten sollen die Gadgets des Bochumer Teams funktionieren und als Basis für sichere elektronische Schaltungen dienen.

WIE MAN **IT-SICHERHEIT UND PRODUK-TIVITÄT** UNTER EINEN HUT BEKOMMT

Uta Menges und Jonas Hielscher wollen IT-Sicherheitsmaßnahmen aus der nervigen Ecke herausholen und besser in den Alltag bringen.

IT-Sicherheit – bei der Vokabel verdrehen viele innerlich gleich die Augen. Natürlich ist allen klar, dass das Thema wichtig ist. Die spektakulären Angriffe auf IT-Systeme von Organisationen in den vergangenen Jahren sind beängstigend, ganze Universitäten oder Stadtverwaltungen waren teils wochenlang vom Netz. Und die gelungenen Angriffe sind nur die Spitze des Eisbergs, denn versuchte Angriffe sind an der Tagesordnung. Aber was tun Unternehmen und Organisationen dafür, dass ihre IT sicher ist? Letztlich muss jede und jeder Einzelne diese Sicherheit mittragen – warum klappt das nicht gut und wie könnte es klappen?

Diese Frage treibt Uta Menges und Jonas Hielscher um. Die beiden bilden ein Tandem im Forschungskolleg SecHuman – Sicherheit für Menschen in Cyberspace. Gemeinsam arbeiten sie hier an ihrer Doktorarbeit. Dabei könnten ihre fachlichen Hintergründe kaum unterschiedlicher sein. Während Jonas Hielscher in Magdeburg Informatik studiert hat, ist Uta Menges studierte Wirtschaftspsychologin. Ihren Master hat sie in der Ehe-, Familien- und Lebensberatung absolviert und auf diesem Gebiet auch gearbeitet. Wie passt das zusammen?

„Das geht erstaunlich gut zusammen“, sagt sie. „Ich kann das dort Gelernte prima auf den Bereich der IT-Sicherheit übertragen.“ Denn im Fokus steht auf beiden Gebieten der Mensch. „Die technischen Maßnahmen für die Sicherheit eines IT-Systems können noch so gut sein – ohne die Mit- ▸

Im Büroalltag gibt es viele Fallstricke, die die IT-Sicherheit gefährden. Doch wie an alles denken und die eigentliche Arbeit nicht beeinträchtigen? (Foto: ms)

FORSCHUNGSKOLLEG SECHUMAN

Seit 2016 forschen Doktorandinnen und Doktoranden an der Ruhr-Universität Bochum im Forschungskolleg „SecHuman“ zur Sicherheit im Cyberspace, das vom NRW-Ministerium für Kultur und Wissenschaft gefördert wird. Im Kolleg arbeiten Doktorandinnen und Doktoranden nicht nur mit Forschenden aus anderen Disziplinen zusammen, sondern auch mit Akteuren aus der Praxis. Das Forschungskolleg SecHuman, kurz für „Schöne neue Welt: Sicherheit für Menschen im Cyberspace“, ist am Bochumer Horst-Görtz-Institut für IT-Sicherheit angesiedelt und auch eingebunden in das Exzellenzcluster CASA – Cybersicherheit im Zeitalter großskaliger Angreifer.

Jonas Hielscher (links) und Uta Menges wollen wissen, wie sich IT-Sicherheit so in den Arbeitsalltag integrieren lässt, dass sie nicht hinderlich ist. (Foto: CASA, Caroline Schreer)

> „DAS SCHAFFT IN EINEM NORMALEN ARBEITSTAG KEIN MENSCH."
>
> Uta Menges

arbeit der Nutzenden funktionieren sie nicht“, sagt auch Jonas Hielscher. Aber wie man Organisationen dazu bringt, ihre Mitarbeitenden bei der Umstellung zu sicherem Verhalten zu unterstützen und nicht alle Last einfach bei den Endnutzer*innen abzuladen, dazu sind die Forschungsergebnisse bislang rar. Und mit der Praxis sind Menges und Hielscher auch nicht sehr glücklich. „Viele Firmen beauftragen Anbieter zum Beispiel damit, gefakte Phishingmails an ihre Mitarbeitenden zu senden, um das Team für Angriffe zu sensibilisieren“, erzählt Jonas Hielscher. „Aber solche einmaligen und eindimensionalen Maßnahmen bringen nicht viel.“ Im Zweifel hat jemand, der drauf hereingefallen ist, das Gefühl, den Schwarzen Peter zu haben. Damit ist niemandem geholfen.

Die beiden Forschenden stellen ganz andere Fragen: Wie machbar ist IT-Sicherheit für Mitarbeitende eigentlich? Wissen die Mitarbeitenden genau, was sie zu tun haben? Lassen sich Maßnahmen wirklich umsetzen oder ist dafür im Arbeitsalltag gar keine Zeit? Stehen die IT-Sicherheitsmaßgaben in Konkurrenz mit Dingen, die zu erledigen sind? „Stichwort: Lesen Sie jede Mail ganz genau und prüfen Sie sie auf Indizien für einen Phishing-Angriff“, gibt Uta Menges ein Beispiel. „Das schafft in einem normalen Arbeitstag kein Mensch.“

Neben solchen Fragen, die unter dem Begriff „productive security“ zusammengefasst sind, fassen die beiden Promovierenden auch die Kommunikation über IT-Sicherheit ins Auge. Wie reden die Leute darüber? Die Macher sind oft Ingenieure. Sie sprechen über Technik und holen die nicht technisch versierten Kolleginnen und Kollegen damit nicht ab. Diese kommunikative Hürde führt zu Missverständnissen und trägt nicht zu einem vertrauensvollen Miteinander bei. Genau das halten die Forschenden aber für unverzichtbar. „Wenn jemand eine Phishingmail geöffnet hat und in die Falle getappt ist, darf er oder sie keine Angst haben, diesen Vorfall zu melden“, sagt Uta Menges. „Und es muss klar sein, bei wem.“ Sie fordert eine gute Fehlerkultur: Niemand darf an den Pranger gestellt werden, weil er oder sie einen Fehler gemacht hat. Es braucht klare Anweisungen. Allzu oft würden Mitarbeitende aber mit unklaren Regelungen allein gelassen. Zur Kommunikation gehört auch die Antwort eines Helpdesks. Ist sie unpersönlich, bleibt IT-Sicherheit abstrakt.

Kommunikationsprobleme stellen die beiden auch zwischen IT-Sicherheitsprofis und dem Management von Institutionen fest. „Profis wollen über Produkte reden. Für das Management ist das Risiko viel interessanter, das es einzudämmen gilt. Aber dafür, wie sicher oder unsicher sich Mitarbeitende verhalten, gibt es bisher kein Maß“, erklärt Jonas Hielscher. Er und Uta Menges wagen sich auf ein weitgehend unerforschtes Terrain. „Man müsste die Leute befragen, ihr Verhalten beobachten, ihr Feedback einholen, Vorfälle auswerten. Aber das ist alles noch nicht gemacht worden, auch weil es so kompliziert ist“, sagt er.

Auf Basis ihrer Expertise als Psychologin unterstreicht Uta Menges: Soll IT-Sicherheit in Organisationen gelingen, ist vor allem die Selbstwirksamkeitserwartung der Menschen wichtig. Mit anderen Worten: IT-Sicherheit muss zu bewältigen sein. Und sie muss wirken. „Das klingt vielleicht selbstverständlich, aber das jahrzehntealte Narrativ, dass alles ohnehin immer schlimmer wird und man sowieso nichts machen kann, steckt in vielen Köpfen“, sagt Uta Menges. „Wer das verinnerlicht hat, hat es schwer, Maßnahmen zu ergreifen, weil er nicht an sie glaubt.“

Mit verschiedenen Praxispartnern tasten sich Uta Menges und Jonas Hielscher an das Thema heran. Gemeinsam mit einem großen Industrieunternehmen aus Nordrhein-Westfalen bilden sie über ein Dutzend aktueller Auszubildener zu Botschaftern für IT-Sicherheit aus. Sie haben den Chief Information Security Officer kennengelernt und seine Handynummer bekommen. Ziel ist es, ein Netzwerk zu schaffen über die vielen Standorte des Unternehmens mit über 20.000 Mitarbeitenden hinweg. So soll IT-Sicherheit ein Gesicht bekommen. Seit November 2021 stehen die beiden in Kontakt mit einer Gruppe von 28 schweizerischen Chief Information Officers von verschiedenen Firmen. Sie gestalten hier unter anderem Workshopinhalte mit und bleiben auf dem Laufenden über Alltagsprobleme in den Unternehmen.

„Diese Doktorarbeit entwickelt sich erst, während wir sie erarbeiten“, sagt Jonas Hielscher. Beide sind jedoch fasziniert von ihrem Forschungsfeld. „Es ist Pionierarbeit und nicht planbar – es sind halt Menschen, die im Mittelpunkt stehen“, sagt Uta Menges. Forschungsfragen drängen sich noch jede Menge auf. Das Forschungsfeld Human Centered Security ist noch jung, erst um 2000 herum kam das Thema auf. „Aber es werden immer mehr Professuren, es ist ein wachsendes Feld“, freut sich Jonas Hielscher. „Und unsere Ergebnisse werden sicher nicht auf taube Ohren stoßen.“

md

i SCHÄDEN DURCH IT-ANGRIFFE

Wie groß der wirtschaftliche Schaden durch IT-Angriffe ist, kann niemand genau beziffern, da es in Deutschland für solche Vorfälle keine Meldepflicht gibt. Die vom Branchenverband Bitcom veröffentlichte Zahl, die sich auf rund sechs Prozent des Bruttoinlandsprodukts beläuft, ist daher auch nur eine Schätzung, die Jonas Hielscher für zu hoch hält.
Ransomware-Angriffe, bei denen IT-Systeme von außen verschlüsselt werden, um ein Lösegeld zu erpressen, treffen oft mittlere Unternehmen, deren Schutz häufig unzureichend ist.

REDAKTIONSSCHLUSS

Die Hasen im CASA Universe sind aufgeschreckt: Der scheinbar gut gesicherte Zugang zum Karottenvorrat von Hase Mark wurde gehackt und alle Wintervorräte geraubt. Die mutige Häsin Betty macht sich daraufhin auf die Suche nach Unterstützung im nahegelegenen CASA Hub C – einem geheimnisvollen Ort, der Lösungen für digitale Sicherheit bereithalten soll. So beginnt das Abenteuer von Häsin Betty, der Protagonistin des ersten Wissenschaftscomics des Exzellenzclusters CASA. Gemeinsam mit Betty lernen die Leserinnen und Leser bei ihrem Streifzug durch den Research Hub die Forschungsschwerpunkte und Herausforderungen kennen, mit denen sich die Wissenschaftlerinnen und Wissenschaftler im Forschungsbereich Hub C „Sichere Systeme" tagtäglich beschäftigen. Wie Sie alle Comics der Reihe kostenlos lesen können, erfahren Sie unter:

↗ *casa.rub.de/outreach/wissenschaftscomics*

Auflösung
DEEPFAKE-QUIZ
Folgende Gesichter sind echt:
1a, 2a, 3b, 4a, 5b, 6a

IMPRESSUM

HERAUSGEBER: Exzellenzcluster CASA und Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Lisa Bischoff (lb)

FOTOGRAFIE: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: 0177/3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

BILDNACHWEISE INHALTSVERZEICHNIS: Michael Schwettmann

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

DRUCK: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Tel.: 0231/90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

AUFLAGE: 4.700

BEZUG: Die reguläre Ausgabe von Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden. Die Sonderausgabe 2023 ist erhältlich beim Horst-Görtz-Institut für IT-Sicherheit. Interessierte können sich per E-Mail an hgi-presse@rub.de melden.

ISSN: 0942-6639

CaSa im Podcast Exzellent Erklärt

„Unsere Daten werden verschlüsselt, wenn wir im Internet surfen oder eine Nachricht per Messenger schicken. Bis jetzt sind viele dieser Verfahren recht sicher – wenn aber der Quantencomputer kommt, ist es mit dieser Sicherheit vorbei.

Daher hat das Exzellenzcluster CASA Verschlüsselungsmethoden entwickelt, die sogar Quantencomputern standhalten können. Außerdem wird erforscht, wie die IT-Sicherheit so umgesetzt werden kann, dass sie für Anwender*innen verständlicher und einfacher in der Anwendung wird. Im Gespräch mit Podcasterin Larissa Vassilian sprechen Prof. Eike Kiltz und Prof. M. Angela Sasse über ihre Forschung“

Der Podcast

57 Exzellenzcluster, 1 Podcast. Regelmäßig berichtet „Exzellent erklärt“ aus einem der Forschungsverbünde, die im Rahmen der Exzellenzstrategie des Bundes und der Länder gefördert wird. Die Reise geht quer durch die Republik, genauso vielfältig wie die Standorte sind die Themen: Von A wie Afrikastudien bis Z wie Zukunft der Medizin. Seid bei der nächsten Folge wieder dabei und taucht ein in die spannende Welt der Spitzenforschung! Wenn Euch der Podcast gefallen hat, abonniert „Exzellent erklärt“ bei dem Podcast-Anbieter Eurer Wahl.

Hier reinhören:

CASA
Cyber Security In the Age of Large-Scale Adversaries

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM
RUB

Kennen Sie schon unseren HGI Newsletter?

Hier informieren wir regelmäßig über News aus der Bochumer IT-Sicherheits-Forschung, Events und Outreach-Projekte.

Zur Anmeldung geht es hier:

RUHR UNIVERSITÄT BOCHUM RUB

HORST GÖRTZ INSTITUT