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

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

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