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

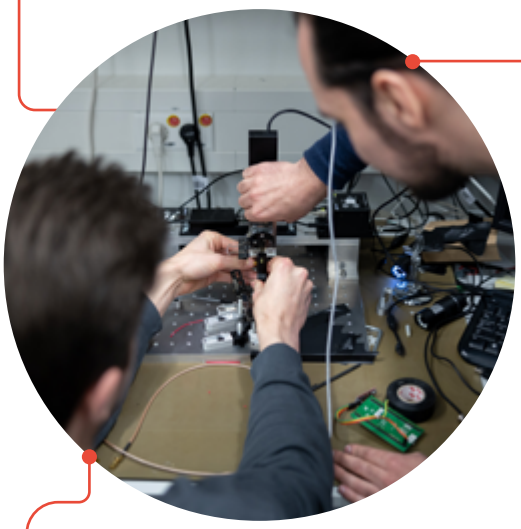
Sonderausgabe 2023

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.

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