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

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

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