RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE

IT-SICHERHEIT

Wie sich künstlich erzeugte Bilder verraten

Drei harte Nüsse für Quantencomputer

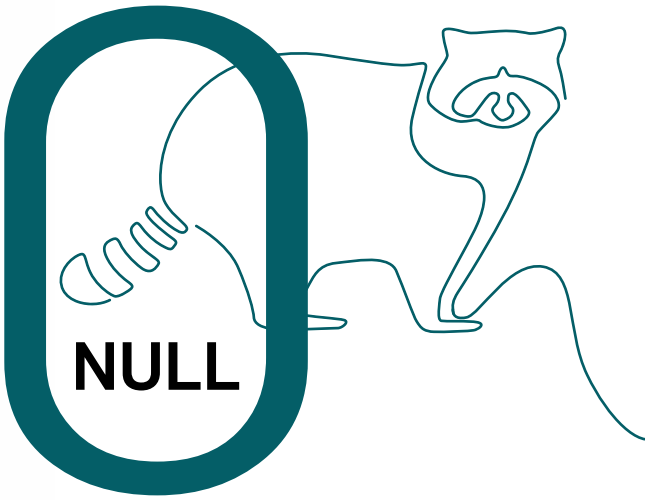
Start-up: Fit für die neue Mobilfunkgeneration

#33 Jahrgang

Sonderausgabe 2023

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.

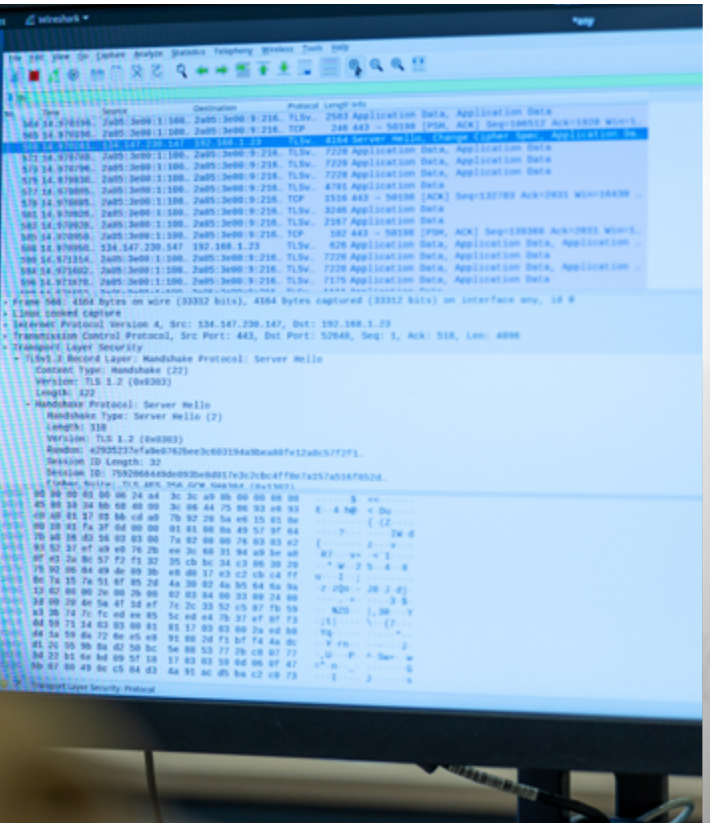
Das Konzept hinter dem Waschbär-Angriff sei leicht zu verstehen. „Ganz grob gesagt geht es beim Diffie-Hellman-Schlüssel immer um Rechnen mit Rest“, so Merget. In den knifflig en mathematischen Ableitungen des Diffie-Hellman-Schlüsselaustausches wird mit dem Rest ohne führende Nullen weiter gerechnet. „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.

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