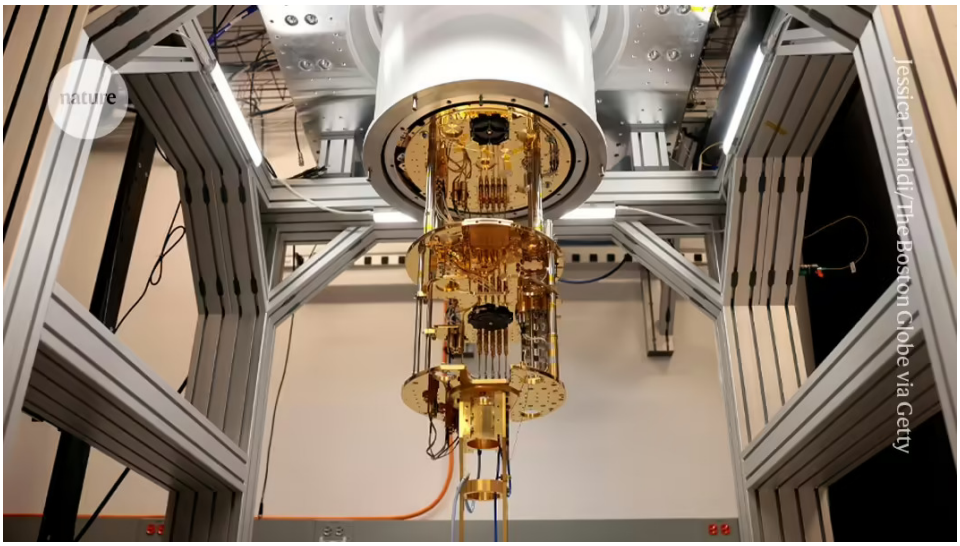
Quanten-Hacking droht - aber ultrasichere Verschlüsselung steht zum Einsatz bereit

Mit den neuen Verschlüsselungsstandards für die Kommunikation im Internet schützt sich die US-Regierung vor zukünftigen Angriffen durch Quantencomputer. Erfahren Sie mehr über die Maßnahmen und die Auswirkungen auf die Cybersicherheit weltweit.



Die Cybersicherheit steht vor einer umfassenden Überholung. Die US-Regierung hat einen Satz von Standards finalisiert, um Internetkommunikation vor Angriffen durch zukünftige Quantencomputer zu schützen, die die meisten aktuellen digitalen Schutzmaßnahmen wirkungslos machen könnten.

Die Richtlinien umfassen einen Algorithmus zur sicheren Kommunikation durch Verschlüsselung und zwei Algorithmen für digitale Signaturen, die verhindern, dass Hacker einen bekannten Benutzer oder ein bekanntes Gerät nachahmen. Es wird erwartet, dass sie global übernommen werden. Das US-

amerikanische National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland, hat die drei Algorithmen durch einen Prozess ausgewählt, der 2016 begann und die Hilfe von Kryptographiespezialisten weltweit in Anspruch nahm. NIST hatte eine vorläufige Auswahl von vier Algorithmen im Jahr 2022 angekündigt und hat jetzt die Standards für drei von ihnen finalisiert.

„Es ist großartig zu sehen, dass sie endlich veröffentlicht wurden“, sagt Peter Schwabe, ein kryptografischer Ingenieur am Max-Planck-Institut für Sicherheit und Datenschutz in Bochum, Deutschland, der drei der vier Systeme entworfen hat.

„Diese finalisierten Standards enthalten Anweisungen zu deren Integration in Produkte und Verschlüsselungssysteme“, sagt Dustin Moody, ein Mathematiker bei NIST, der die Standardisierungsbemühungen leitet. „Wir ermutigen Systemadministratoren, sofort mit der Integration in ihre Systeme zu beginnen, da die vollständige Integration Zeit in Anspruch nehmen wird.“

Daten sicher halten

Digitale Kommunikation und Transaktionen wie Online-Shopping basieren fast universell auf einem kleinen Satz von Algorithmen für Public-Key-Kryptographie. Diese Systeme ermöglichen es zwei Parteien, Informationen sicher auszutauschen. Jede Partei hat einen eigenen öffentlichen Schlüssel, eine Sequenz von Zahlen, die sie jedem geben, der ihnen eine Nachricht senden möchte. Der Empfänger kann die Nachricht dann mit einem privaten Schlüssel entschlüsseln, den nur er kennt.

Aber aktuelle Public-Key-Systeme sind bekannt dafür, anfällig für Entschlüsselung mit einem von Peter Shor, einem Mathematiker, der heute am Massachusetts Institute of Technology in Cambridge tätig ist, entwickelten Quantenalgorithmus zu sein. Im Jahr 1994 – zu einer Zeit, als nicht einmal die rudimentärsten Quantencomputer existierten und als die Internetkommunikation

gerade erst begann, mainstream zu werden – zeigte Shor, dass solche Maschinen schnell in der Lage sein würden, die beliebtesten Public-Key-Systeme zu knacken. Dadurch könnten auch Geräte wie Kreditkarten und Sicherheitspässe einem Hackingrisiko ausgesetzt sein.

Dreißig Jahre später haben die Bemühungen, Quantencomputer zu bauen, große Fortschritte gemacht, aber die Maschinen sind immer noch mindestens ein Jahrzehnt davon entfernt, Shors Algorithmus auf etwas anderes als Zahlen mit einigen Stellen auszuführen. Dennoch haben Shor und andere vor Complacency gewarnt.

Der von NIST ausgewählte neue Verschlüsselungsalgorithmus heißt CRYSTALS-Kyber. Schwabe und seine Mitarbeiter haben ihn aus einer Technik entwickelt, die erstmals 2005 von dem Informatiker Oded Regev an der New York University vorgeschlagen wurde. Schwabe sagt, dass die Bereitstellung in den Anwendungen, die den meisten Benutzern vertraut sind – Internet-Browsing und Smartphone-Apps -, relativ reibungslos verlaufen sollte. „Browser werden schnell migrieren, ebenso wie Messaging-Apps und Videokonferenzsysteme“, sagt er. Es könnte länger dauern, bis die Entwickler kleiner Internet- oder WiFi-verbundener Geräte aufholen, fügt er hinzu.

Obwohl CRYSTALS-Kyber gegen Angriffe von Quantencomputern resistent sein sollte, sind keine der bestehenden Public-Key-Algorithmen – einschließlich der drei von NIST ausgewählten – mathematisch als vollständig sicher erwiesen, und Forscher werden weiter an Alternativen arbeiten, für den Fall. NIST selbst evaluiert „zwei weitere Algorithmengruppen, die eines Tages als Backup-Standards dienen könnten“, sagte das Institut in einer Erklärung.

Obwohl die NIST-Ankündigung dies nun offiziell gemacht hat, gibt es „post-quantum“-Algorithmen schon seit Jahren. Einige Unternehmen wie Cloudflare und IBM haben bereits begonnen, sie in ihre Systeme zu integrieren, während andere langsamer

waren, sich anzupassen. „Viele Organisationen haben die Arbeit an der post-quantum-Migration noch nicht begonnen und verweisen auf den Mangel an Standards – **eine Situation, die als Kryptoprokrastination bezeichnet wurde**“, schrieb Bas Westerbaan, ein Mathematiker bei der Internetdienstleistungsfirma Cloudflare, in einem Blogbeitrag im letzten Jahr. Sicherheitsspezialisten hoffen, dass die NIST-Ankündigung die meisten anderen Organisationen nun dazu bewegen wird, mit dem wahrscheinlich langwierigen und komplizierten Übergang zu beginnen.

Besuchen Sie uns auf: natur.wiki