Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Ein Rezept gegen die Macht der Quantencomputer

Signaturverfahren aus Darmstadt könnte bald weltweit Updates absichern

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20018
Fax 06151 16 - 23750
feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 11. Juni 2018. Ein vor Quantencomputern sicheres Verfahren für digitale Signaturen, das ein Team um Professor Johannes Buchmann von der TU Darmstadt entwickelt hat, ist nun ein allgemeiner Internet-Standard.

Dramatische Fortschritte bei der Entwicklung von Quantencomputern lösen Besorgnis über die künftige Sicherheit des Internets aus. Denn die superschnellen Rechner könnten gängige Verschlüsselungen und digitale Signaturen in Windeseile knacken. Weltweit entwickeln Forscher daher neue Sicherheitsverfahren, die immun gegen einen Angriff mit einem Quantencomputer sein sollen, so genannte Post-Quanten-Kryptographie. Ein an der TU Darmstadt entwickeltes Post-Quanten-Verfahren ist jetzt fertig für den weltweiten Einsatz. Die letzte Hürde für die allgemeine Verwendung im Internet, die IETF-Spezifikation (Internet Engineering Task Force; ein internationales Gremium, das sich mit der technischen Weiterentwicklung des Internets befasst), hat die Methode eines Teams um Professor Johannes Buchmann namens XMSS (eXtended Merkle Signature Scheme) nun genommen.

„Ohne sichere digitale Signaturen müsste man das Internet abschalten“, betont Buchmann die Wichtigkeit dieser Urheberschaftsnachweise. Bei Updates etwa sichern digitale Signaturen, dass die neue Software nicht verändert wurde und man sich nicht statt einer Aktualisierung des Virenscanners einen böswilligen Trojaner einhandelt.

Bisherige Verfahren basieren auf komplexen mathematischen Problemen, die zwar für einen herkömmlichen Computer nur in Jahrmilliarden zu knacken sind, für einen künftigen Quantencomputer aber binnen Minuten. Zusätzlich bauen alle bisherigen Verfahren auf die Sicherheit von Hashfunktionen. Diese sind wie individuelle Fingerabrücke von digitalen Dateien.

XMSS hingegen beruht ausschließlich auf der Sicherheit von Hashfunktionen. Es kommt ohne zusätzliche mathematische Hürden aus, deren Unknackbarkeit immer nur eine Annahme bleibt. Buchmann ist diese Unabhängigkeit besonders wichtig. „Niemand weiß heute, ob alternative mathematische Hürden, die heute noch als sicher vor Quantencomputern

gelten, nicht einmal doch von einem solchen schnell gelöst werden können“, sagt der Mathematiker.

Das nun verfügbare Verfahren erfüllt weitere wichtige Anforderungen. Sichere Hashfunktionen garantieren, dass keine zwei Dokumente den gleichen Fingerabdruck liefern. Bei XMSS ist diese „Kollisionsfreiheit“ zentral. Sicherheitslücken schließt Buchmann ebenfalls aus. „Wir konnten mathematisch beweisen, dass unser Verfahren sicher ist, solange es die Hashfunktion ist“, betont der Forscher. Anwendbar bleibt XMSS aber auch dann, wenn die eingesetzte Hashfunktion von Hackern geknackt werden sollte. Derlei kommt vor. Doch es gibt nicht nur eine Hashfunktion, sondern viele. XMSS ist eine Art Container, in die eine neue Hashfunktion eingesetzt werden kann, falls eine alte nicht mehr sicher ist.

Buchmanns Team begann vor 15 Jahren mit der Entwicklung von XMSS und brachte es bis zur Praxisreife. Maßgeblichen Anteil an der ursprünglichen Erfindung von XMSS hatte Buchmanns ehemaliger Doktorand Andreas Hülsing (TU Eindhoven) in einem ehemaligem Projekt der Deutschen Forschungsgemeinschaft (DFG). Im neuerem DFG-Transferprojekt „squareUP“ kooperierte Denis Butin (TU Darmstadt) mit der Münchener Firma genua. Bei der Spezifikation von XMSS waren außer den squareUP-Partnern auch die TU Eindhoven, die Radboud University Nijmegen, und die US-Firma Verisign involviert.

In einzelnen Anwendungen setzt genua XMSS schon ein. Doch um es im allgemeinen Internetverkehr benutzen zu können, bedurfte es noch der Standardisierung durch die IETF, ein internationales Gremium. Sie hat für XMSS nun einen „Request for Comments“ (RFC) herausgegeben, was bedeutet, dass das Verfahren eine „offizielle“, von einer breiten Öffentlichkeit unterstützte Methode ist. Allerdings rechnet Buchmann damit, dass die Integration der Methode in alltägliche Anwendungen noch Jahre dauern wird. Er mahnt, schon damit anzufangen. Denn manche Physiker rechnen bereits in zehn bis fünfzehn Jahren mit ersten Quantencomputern, die stark genug sind, um heute gängige digitale Signaturverfahren zu knacken.

Hintergrund:

IT-Sicherheit zählt zu den herausragenden Forschungsthemen der TU Darmstadt: Im Profilbereich CYSEC arbeiten Wissenschaftlerinnen und Wissenschaftler an zentralen Fragestellungen der Cybersicherheit und des Schutzes der Privatheit. An CYSEC sind derzeit insgesamt 33 Fachgebiete aus acht Fachbereichen der TU Darmstadt beteiligt (Informatik, Physik, Elektrotechnik und Informationstechnik, Gesellschafts- und Geschichtswissenschaften, Biologie, Humanwissenschaften, Maschinenbau,

Rechts- und Wirtschaftswissenschaften). In seinen vielfältigen Verbund- und Einzelprojekten betreibt CYSEC auf international anerkanntem Niveau Spitzenforschung in zahlreichen Bereichen der Cybersicherheit. www.cysec.tu-darmstadt.de

MI-Nr. 30/2018, Christian J. Meier