Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Daten langfristig schützen – selbst vor der NSA

Forscher bereiten IT-Sicherheit auf Zukunft mit Quantencomputern vor

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Silke Paradowski
Tel. 06151 16 - 32 29
Fax 06151 16 - 41 28
paradowski.si@pvw.tu-darmstadt.de

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

Darmstadt, 7. 4. 2014. Geheimdienste wie die NSA interessieren sich für zukünftige Superrechner, sogenannte Quantencomputer. Sie können nämlich auf einen Schlag große Teile der weltweit gängigen IT-Sicherheit unwirksam machen. Der Darmstädter Informatiker Johannes Buchmann arbeitet deshalb an quantencomputer-resistenten Sicherheitsverfahren, die Daten auch in Zukunft schützen können – vor Hackern und vor Geheimdiensten.

„Es gibt große internationale Forschungsanstrengungen, leistungsstarke Quantencomputer zu bauen“, sagt Johannes Buchmann, Informatikprofessor an der TU Darmstadt und Vizedirektor des LOEWE-Forschungszentrums CASED. „Wenn sie Erfolg haben, sollten wir eine gute Alternative bereithalten. Online-Shopping? Software-Updates? Internetgestützte Fahrzeugelektronik? Das alles wäre in der heutigen Form schlagartig nicht mehr sicher“, schätzt er die Folgen ein. Von Herstellern wie IBM wurden bereits erste Quantencomputer mit noch geringer Rechenkapazität vorgestellt. Es überrascht nicht, dass nach neuesten Berichten auch die amerikanische Sicherheitsagentur NSA für zukünftige Spähangriffe auf die Superrechner setzt und die Entwicklung vorantreibt.
Wie aber kann es sein, dass für Besitzer von Quantencomputern sensible Daten leicht zugänglich würden und elektronische Signaturen einfach zu fälschen wären? „Die Mehrzahl der heute eingesetzten Verschlüsselungen und elektronischen Signaturen nutzt das sogenannte RSA-Verfahren“, erklärt Buchmann. Dabei verschlüsselt der Sender die Nachricht mit einem bekannten, öffentlichen Schlüssel, und nur der Empfänger kann sie mithilfe eines zweiten, privaten Schlüssels wieder entschlüsseln. Die digitale Signatur funktioniert andersherum: Der Autor einer Nachricht nutzt seinen geheimen Schlüssel als Unterschrift, die jeder mit einem öffentlichen Schlüssel überprüfen kann. Unverzichtbar, um zum Beispiel sichere Software-Updates von gefährlichen Fälschungen zu unterscheiden.
Das RSA-Verfahren ist sicher, weil die Berechnung des geheimen Schlüssels aus dem öffentlichen die Lösung eines extrem schwierigen Problems nötig macht: die beiden Primfaktoren einer mehr als 300-stelligen Zahl zu finden. Dies würde auf den besten Computern der Welt Jahrtausende dauern. Überraschenderweise konnte der Mathematiker Peter Shor 1994 beweisen, dass Quantencomputer die Faktoren in sehr kurzer Zeit finden können. „Uns wurde klar, was ein Quantencomputer in der schnell wachsenden Internetgesellschaft anrichten würde. Deshalb haben wir bereits vor zehn Jahren angefangen, neue kryptographische Verfahren zu entwickeln, die gegen derartige Angriffe resistent sind – so genannte Post-

Quantum-Kryptoverfahren“, erklärt Buchmann. Einen ersten Erfolg können die Darmstädter Forscher bereits verbuchen: In einem von der Deutschen Forschungsgemeinschaft geförderten Projekt haben sie das vielversprechende Post-Quantum-Signaturverfahren XMSS entwickelt.
Das besondere an XMSS: seine Sicherheit kommt ohne die Schwierigkeit des Faktorisierungsproblems oder eines vergleichbaren Problems aus. XMSS ist sicher, solange ein Grundbaustein aller Signaturverfahren sicher ist: die verwendete Hashfunktion. Die Sicherheitsanforderungen sind also minimal. Bleibt die Frage, ob Hashfunktionen auch vor Quantencomputerangriffen sicher sind: „Sicherheit lässt sich mathematisch nur sehr selten beweisen. Aber eins ist klar: solange es überhaupt ein sicheres Signaturverfahren gibt, bleibt XMSS sicher. Darum können wir uns auf XMSS konzentrieren“ ist sich der Kryptologe sicher.
Zusammen mit dem deutschen Unternehmen genua werden die Darmstädter ihr Verfahren für konkrete Anwendungen anpassen und standardisieren. Wenn leistungsstarke Quantencomputer Realität werden sollten, könnten dann zumindest bestehende Signaturverfahren durch sichere ersetzt werden.
Weltweit forschen nur eine Handvoll Experten auf diesem komplexen Gebiet. Buchmann hat mit seiner Gruppe in den letzten zehn Jahren die Postquanten-Kryptographie durch Workshops und Konferenzen vorangetrieben. Neben der Entwicklung hash-basierter Kryptographieverfahren arbeiten die Wissenschaftler auch mit gitterbasierter und multivariater Kryptographie. 2008 erhielt der Kryptologe zusammen mit Kollegen den hochdotierten IT-Sicherheitspreis der Horst Görtz-Stiftung.

Weitere Informationen

Quantencomputer-resistente Signaturverfahren für die Praxis
In einem 2014 startenden Transferprojekt kooperiert die Gruppe von TU-Informatikprofessor Johannes Buchmann mit der genua mbh, einem Spezialisten für IT-Sicherheit. Ziel ist es, ein marktfähiges quantenresistentes Verfahren zu entwickeln. Die Deutsche Forschungsgemeinschaft fördert die praxisnahe Umsetzung an der TU Darmstadt mit etwa 231.000 Euro für 36 Monate. Die genua mbh mit Hauptsitz in Kirchheim bei München ist Hersteller von Firewall- und VPN-Produkten im Hochsicherheitsbereich.

Homepage CDC: https://www.cdc.informatik.tu-darmstadt.de/cdc/
Veröffentlichung zu Signaturverfahren XMSS:
http://eprint.iacr.org/2011/484.pdf

MI-Nr. 27/2014, Anne Grauenhorst