PRESSEINFORMATION

Kryptografie wird jetzt zukunftssicher gemacht

genua und Partner starten Projekt zu quantenresistenter Kommunikation

Kirchheim bei München, 5. Dezember 2019. Fortschritte bei der Entwicklung leistungsfähiger Quantencomputer haben zuletzt Google in die Schlagzeilen gebracht, auch die Kryptografie hält in diesem Wettlauf das Tempo mit: genua und Partner entwickeln im Projekt QuaSiModO (Quanten-Sichere VPN-Module und Operantionsmodi) Verschlüsselungsverfahren zur Kommunikation via Internet, die der neuartigen Rechenleistung von Quantencomputern standhalten. Denn viele der heute gängigen Krypto-Verfahren werden unsicher, sobald Quantencomputer marktreif sind. Das Ziel des Forschungsprojekts: bis 2022 praxistaugliche Verschlüsselungsverfahren zur sicheren Kommunikation in der aufziehenden Ära der Quantencomputer entwickeln. Projektpartner sind der Netzwerkausrüster ADVA Optical Networking SE, das Fraunhofer-Institut AISEC, die Ludwig-Maximilians-Universität München (LMU) und der IT-Sicherheitshersteller genua GmbH als Konsortialführer.

Quantencomputer setzen neue Maßstäbe. Sie funktionieren nach den Regeln der Quantenphysik und damit grundsätzlich anders als konventionelle Computer, die mit binären Bits und Bytes arbeiten. Dadurch können Quantencomputer einige komplexe Aufgaben um ein Vielfaches schneller berechnen. So hat Google nach Meldungen im September mit einem Quantencomputer eine schwierige Mathe-aufgabe mit Zufallszahlen in drei Minuten und 20 Sekunden gelöst, für die ein konventioneller Superrechner rund 10.000 Jahre gebraucht hätte. Die neuartigen Computer versprechen großes Potenzial, sind für die Kryptografie aber ein Problem: Alle heute im Internet gängigen Public-Key-Krypto-Verfahren basieren auf komplexen mathematischen Aufgaben, die Quantencomputer innerhalb kürzester Zeit berechnen können.

Kryptografie jetzt auf Quantencomputer vorbereiten

Derzeit befinden sich Quantencomputer noch im experimentellen Stadium und sind nicht marktreif. Angesichts des Potenzials fließen jedoch erhebliche Investitionen in die Entwicklung dieser Computertechnologie. „Einige Experten schätzen, dass praxistaugliche Quantencomputer in zehn bis 15 Jahren kommen werden. Da die Entwicklung und anschließend die Verbreitung neuer Verschlüsselungsverfahren aber viel Zeit kostet, ist es wichtig, das Projekt für quantensichere Kommunikation jetzt zu starten“, sagt Alexander von Gernler, Forschungsleiter bei genua.

Bewährte Protokolle mit quantenresistenten Verfahren erweitern

Die Forscher haben für das Projekt die Kommunikationsprotokolle IPsec und MACsec ausgewählt. IPsec und MACsec bzw. deren Schlüsselaustausch-Protokolle IKEv2 und MKA sollen mit quantenresistenten Verfahren erweitert werden. Beide ermöglichen verschlüsselte Kommunikation via Internet und werden häufig eingesetzt, um den Datenaustausch via VPN (Virtual Private Network) zwischen verteilten Unternehmensstandorten oder die Anbindung mobiler Mitarbeiter an Firmennetze abzusichern.

Experten für alle Forschungsbereiche

Die Projektarbeit teilen sich die Partner gemäß ihrer Expertise: genua konzentriert sich auf das Protokoll IPsec/IKEv2, ADVA auf MACsec/MKA, die LMU leistet grundlegende Forschung für das gesamte Projekt und Fraunhofer AISEC testet mit Attacken im Cyber-Labor die Sicherheit der entwickelten Verfahren. Das Projekt läuft bis 2022 und erhält eine Förderung vom Bundesministerium für Bildung und Forschung.

Bildunterzeile:
Forschungsleiter Alexander von Gernler: „Die Kryptografie muss jetzt auf die Entwicklung bei den Quantencomputern reagieren.“ / Bildquelle: genua GmbH

Über genua

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Das Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen und Netze im Behörden- und Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen, die zuverlässig verschlüsselte Datenkommunikation via Internet, Fernwartungs-Systeme sowie Remote Access-Lösungen für mobile Mitarbeiter und Home Offices. Alle Produkte werden von genua in Deutschland entwickelt und produziert. Regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) belegen die Produktqualität. Zahlreiche Kunden aus der Industrie und dem öffentlichen Bereich setzen auf die Erfahrung und Lösungen des 1992 gegründeten Unternehmens, das am Hauptsitz in Kirchheim bei München sowie an den Standorten Berlin, Köln, Leipzig und Stuttgart über 250 Mitarbeiter beschäftigt. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

Weitere Informationen:

genua GmbH
Dietmar Bruhns
Domagkstr. 7
85551 Kirchheim bei München
tel +49 89 991950-169
dietmar_bruhns@genua.de
www.genua.de