Mitglieder News

LUXTRUST UND SNT ENTSCHLÜSSELN NEUE TECHNOLOGIEN ZUR DATENSICHERUNG

Juni 2021 – LuxTrust S.A. und das Interdisciplinary Centre for Security, Reliability and Trust (SnT) der Universität Luxemburg gehen eine gemeinsame Forschungspartnerschaft ein, um neue kryptographische Algorithmen zu erforschen, die resistent gegen die Auswirkungen von Quantencomputern sind.

DIE HERAUSFORDERUNGEN VON MORGEN VORAUSSEHEN

Quantencomputer sind eine völlig neue Art von Computern, die sich auf die physikalischen Effekte der Quantenmechanik stützen. Allerdings ist es sehr wahrscheinlich, dass nach den technischen Fortschritten der vergangenen Jahre innerhalb des nächsten Jahrzehnts hochwertige Quantencomputer gebaut werden. Wenn dies geschieht, werden Quantencomputer eine Rechenleistung erreichen, die weit über das hinausgeht, was jeder Supercomputer der Welt heute leisten kann.

Es wurde bereits in der Vergangenheit bewiesen, dass Quantencomputer zu diesem Zeitpunkt in der Lage sein werden, jede Art von derzeit verwendeter Public-Key-Kryptographie, basierend auf Algorithmen von RSA (Rivest, Shamir und Adleman) oder auf elliptischen Kurven, leicht zu brechen. Selbst die Vergrößerung der Schlüsselgrößen für diese Algorithmen helfen in diesem Fall aufgrund der exponentiell wachsenden Rechenleistung von Quantencomputern im Vergleich zu klassischen Computern, die auf die Verarbeitung binärer Zustände in Halbleitern beruhen, nicht weiter.

FORSCHUNGSBEREICHE- ANWENDBARKEIT FINDEN

Neue quantencomputing-resistente Kryptographie und insbesondere neue Public-Key-Algorithmen, die LuxTrust benötigt, um die Kontinuität seiner Trust Services zu gewährleisten, wie z.B. die Erstellung elektronischer Signaturen, wurden bereits von Forschern vorgeschlagen. Sie werden derzeit von verschiedenen internationalen Experten und Institutionen wie NIST (National Institute of Standards and Technology of the United States) analysiert.

LuxTrust und SnT bündeln ihre Ressourcen und teilen ihr Fachwissen, um die vielversprechendsten PQC-Algorithmen (Post-Quantum Cryptography) zu analysieren und den Übergang von den Kernmechanismen der derzeit verwendeten Technologie von LuxTrust in die Post-Quanten-Ära vorzubereiten. Dieses gemeinsame Engagement wird die nahtlose Kontinuität der Vertrauensdienste von LuxTrust und der Sicherheit, die sie bieten, gewährleisten, damit Online-Banking und elektronische Vertragsunterzeichnungen auch dann sicher bleiben, wenn die Quantencomputer auf den Markt kommen.

„Innovationen und Investitionen in Forschung sind unerlässlich, um innovative und moderne digitale Lösungen anzubieten. Wir sind zuversichtlich, dass wir dank der Expertise von SnT-Forschern praktische Lösungen oder Antworten auf echte Herausforderungen der Branche liefern werden, von denen unsere Kunden durch die Nutzung unserer digitalen Dienstleistungen weiter zugutekommen werden", so Fabrice Aresu, CEO bei LuxTrust.

„Entwicklung widerstandsfähiger Kryptographie – in Vorbereitung auf den Fall, wenn Quantencomputer in größerem Umfang verfügbar sind – ist eine Herausforderung, die für viele Branchen inzwischen Priorität hat. Wir sind begeistert, LuxTrust bei diesem Vorhaben zu unterstützen und ihnen zu ermöglichen, ihre hohen Standards bei der Kundensicherheit auch in der nächsten Ära des Computing beizubehalten", erklärt Carlo Duprel, Leiter des Technologietransferbüros bei SnT.

Pressekontakt LuxTrust:

Emilia Leonescu

Marketing and Communication Department emilia.leonescu@luxtrust.lu
(+352) 26 68 15 – 888

Über SnT

Das Interdisciplinary Centre for Security, Reliability and Trust (SnT) der Universität Luxemburg betreibt international wettbewerbsfähige Forschung

im Bereich der Informations- und Kommunikationstechnologie. Zusätzlich zur klassischen Grundlagenforschung arbeitet das SnT über sein Partnership Programm auf Nachfrage auch an gemeinsamen Projekten mit der Industrie und dem öffentlichen Sektor. Die daraus entstehenden Konzepte sind ein echter, dauerhafter Wettbewerbsvorteil für Unternehmen in Luxemburg und darüber hinaus.

www.snt.uni.lu

Über LuxTrust

Mit 15 Jahren Erfahrung in der Bereitstellung elektronischer Identitäts- und Vertrauensdienste stattet LuxTrust Kunden und Unternehmen mit kompletten, maßgeschneiderten digitalen Lösungen aus, um Prozesse zu digitalisieren und die Gesamteffizienz zu steigern. LuxTrust bietet eine breite Palette von Dienstleistungen an, die auf Compliance, Sicherheit und Benutzerfreundlichkeit basieren- von der Erstellung und Bereitstellung elektronischer Identitäten, elektronischer Signaturen, elektronischer Siegel bis hin zur starken Authentifizierung von Benutzern und Zeitstempeln.

Als eIDAS Qualified Trust Service Provider, eingetragen in der EU Trusted List und als Zertifizierungsstelle, ist LuxTrust konform mit den neuesten europäischen und branchenspezifischen Vorschriften und garantiert ein Höchstmaß an Zuverlässigkeit und Vertrauen für unsere Dienstleistungen.

www.luxtrust.com