Member News

LUXTRUST ET SNT COLLABORENT DANS LA RECHERCHE DE NOUVELLES TECHNOLOGIES POUR LA SÉCURISATION DES DONNÉES

1er juin 2021 – LuxTrust S.A. et l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) de l'Université du Luxembourg s'engagent dans un partenariat de recherche collaboratif pour étudier de nouveaux algorithmes cryptographiques, qui seront résistants à l'impact des ordinateurs quantiques.

PRÉVOIR LES DÉFIS DE DEMAIN

Les ordinateurs quantiques sont un type d'ordinateurs complètement nouveau, qui repose sur les effets physiques de la mécanique quantique. Cependant, au vu des progrès d'ingénierie réalisés au cours des dernières années, il est très probable que des ordinateurs quantiques de qualité adaptée à la production soient construits au cours de la prochaine décennie. Lorsque cela se produira, les ordinateurs quantiques atteindront une puissance de calcul dépassant celle

de n'importe quel super ordinateur dans le monde d'aujourd'hui.

Comme cela a déjà été prouvé dans le passé, les ordinateurs quantiques seront à ce stade en mesure de déchiffrer facilement tout type de cryptographie à clé publique actuellement utilisée, sur la base des algorithmes de RSA (Rivest, Shamir et Adleman) ou des courbes elliptiques. Même l'augmentation des tailles de clés pour ces algorithmes ne sera pas utile dans ce cas, en raison de la puissance de calcul à croissance exponentielle des ordinateurs quantiques par rapport aux ordinateurs classiques, qui dépendent des effets électriques des semi-conducteurs.

DOMAINES DE RECHERCHE AYANT UNE APPLICABILITÉ

De nouveaux algorithmes de cryptographie résistants aux ordinateurs quantiques et en particulier de nouveaux algorithmes à clé publique, dont LuxTrust a besoin pour assurer la continuité de ses services de confiance, comme la création de signatures électroniques, ont déjà été proposés par les chercheurs. Ils sont actuellement analysés par divers experts et institutions internationaux, comme le NIST (Institut national des normes et de la technologie des États-Unis).

LuxTrust et SnT joignent leurs ressources et partagent leur expertise pour analyser les algorithmes PQC (cryptographie post-quantique) les plus prometteurs et pour préparer la transition des mécanismes fondamentaux de la technologie actuellement utilisée par LuxTrust vers l'ère post-quantique. Cette collaboration garantira la continuité sans faille des services de confiance de LuxTrust et la sécurité qu'ils fournissent, afin que les opérations bancaires en ligne et la signature de contrats électroniques restent sûres à l'arrivée des ordinateurs quantiques.

« Il est vital d'être en mesure d'innover et d'investir dans la recherche pour rester pertinent et offrir des solutions numériques de pointe. Nous sommes convaincus que, grâce à l'expertise des chercheurs du SnT, nous fournirons des solutions pratiques et des réponses aux défis réels de l'industrie, qui bénéficieront encore davantage aux clients utilisant nos services numériques », explique Fabrice Aresu, CEO de LuxTrust.

« *Développer une cryptographie résistante, en préparation du développement d'ordinateurs quantiques de plus en plus largement disponibles, est un défi prioritaire auquel beaucoup d'industries sont désormais confrontées. Nous sommes très enthousiastes à l'idée d'aider LuxTrust dans cet effort, et de leur permettre de maintenir leurs normes de sécurité client impeccables dans la prochaine ère de l'informatique* », déclare Carlo Duprel, directeur du service de transfert de technologie au SnT.

Contact presse LuxTrust:

Emilia Leonescu

Marketing and Communication Department emilia.leonescu@luxtrust.lu

(+352) 26 68 15 – 888

À propos du SnT

L'Interdisciplinary Centre for Security, Reliability and Trust (SnT) de l'Université du Luxembourg mène des recherches concurrentielles au niveau international dans le secteur des technologies de l'information et de la communication. Outre la recherche sur le long terme et à haut risque, le SnT s'engage dans des projets collaboratifs à la demande de l'industrie et du secteur public à travers son programme de partenariats. Les concepts qui en résultent présentent un véritable avantage concurrentiel durable pour les entreprises du Luxembourg et du monde entier.

www.snt.uni.lu

À propos de LuxTrust

Avec 15 ans d'expérience dans la production d'identité électronique et de services de confiance, LuxTrust équipe les clients et les entreprises de solutions numériques complètes et sur mesure, destinées à numériser les processus et d'améliorer l'efficacité globale. Nous proposons une large gamme de services basés sur la conformité, la sécurité et la commodité de l'utilisateur, allant de la création et la production d'identité électronique, de signature, de cachet électronique, à l'authentification et l'horodatage.

En tant que fournisseur de services de confiance qualifiés selon le règlement eIDAS en vigueur, figurant sur la liste de confiance de l'UE et en tant qu'autorité de certification, nous nous conformons aux dernières réglementations européennes et industrielles et nous garantissons le plus haut niveau de fiabilité et de confiance pour nos services.

www.luxtrust.com