Member News

LUXTRUST AND SNT COLLABORATE TO RESEARCH NEW TECHNOLOGIES IN SECURING DATA

1 June 2021 – LuxTrust S.A. and the University of Luxembourg's Interdisciplinary Centre for Security, Reliability and Trust (SnT) engage in a collaborative research partnership to investigate new cryptographic algorithms, which are resistant against the impact of quantum computers.

FORESEEING THE CHALLENGES OF TOMORROW

Quantum computers are a completely new type of computer that exploit physical phenomena of quantum mechanics. According to the engineering progress made during the last few years, it is very likely that large-scale quantum computers will be built within the next decade. When this happens, quantum computers will achieve a computation power that goes far beyond that of any classical super computer in the world can perform today.

It has already been shown in the past that quantum computers will be able to easily break any type of currently used public key cryptography, based on algorithms of RSA (Rivest, Shamir and Adleman) or on elliptic curves. Even augmenting key sizes for those algorithms will not help due to the exponentially growing computation power of quantum computers compared to classic computers that rely on the electrical effects of semi-conductors.

RESEARCH AREAS FINDING APPLICABILITY

New quantum-computing resistant cryptography and particularly new public key algorithms that LuxTrust needs to ensure continuity of its Trust Services, like creation of Electronic Signatures, have already been proposed by researchers. They are currently analysed by various international experts and institutions like NIST (National Institute of Standards and Technology of the United States).

LuxTrust and SnT join their resources and share their expertise to analyse the most promising PQC (Post-Quantum Cryptography) algorithms and to prepare the transition from the core mechanisms of LuxTrust's currently used technology to the post-quantum era. This joint engagement will ensure seamless continuity of the trust services and the security provided by LuxTrust, so that online banking and electronic contract signing will remain safe when quantum computers arrive.

"Being able to innovate and invest in research are vital to stay relevant and to offer state-of-the-art digital solutions. We are confident that thanks to the expertise of SnT researchers we will deliver practical solutions or answers to real industry challenges that will further benefit clients using our digital services", explains Fabrice Aresu, Chief Executive Officer, LuxTrust.

"*Developing resistant cryptography – in preparation for when quantum computers become more widely available – is a challenge that a lot of industries now face as a priority. We are very enthusiastic to help LuxTrust in this endeavour, and enable them to maintain their impeccable standards of customer security into the next era of computing,*" says Carlo Duprel, Head of the Technology Transfer Office at SnT.

Press contact LuxTrust:

Emilia Leonescu

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

About SnT

The Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg conducts internationally competitive research in information and communication technology. In addition to long-term, high-risk research, SnT engages in demand-driven collaborative projects with industry and the public sector through its Partnership Program. The resulting concepts present a genuine, long-lasting competitive advantage for companies in Luxembourg and beyond.

www.snt.uni.lu

About LuxTrust

With 15 years of experience in providing electronic identity and trust services, LuxTrust equips clients and businesses with complete, tailor-made digital solutions to digitize processes and enhance overall efficiency. We offer a wide range of services based on compliance, security and user convenience from the creation and provision of electronic identity, electronic signature, electronic seal, to authentication and timestamping.

As an eIDAS Qualified Trust Service Provider published in EU Trusted List and a Certification Authority, we are compliant with the latest European and industry regulations, and we guarantee the highest level of reliability and trust for our services.

www.luxtrust.com