PRESS RELEASE

Cryptography is Now Being Made Future-Proof
genua and its Partners Start a Project for Quantum-Resistant Communication

Kirchheim near Munich, December 5, 2019. Advances in the development of powerful quantum computers have placed Google in the headlines recently. Cryptography is also keeping up in this race: By means of the project QuaSiModO (Quanten-Sichere VPN-Module und Operationsmodi – Quantum-safe VPN Modules and Operation Modes), genua and its partners are developing cryptographic procedures for communication via the Internet that keeps up with the new computing power of quantum computers. Because many of today’s common crypto procedures will become insecure as soon as quantum computers are ready for the market. The goal of the research project is to develop a practical encryption procedure for secure communication in the looming era of quantum computers by 2022. The project partners are network supplier ADVA Optical Networking SE, the Fraunhofer Institute for Applied and Integrated Security (AISEC), the Ludwig Maximilian University of Munich (LMU), and IT security provider genua GmbH as the consortium leader.

Quantum computers set new standards. They function according to the laws of quantum physics, and are therefore fundamentally different to conventional computers, which use binary bits and bytes. This allows quantum computers to handle complex tasks significantly quicker. According to reports in September, Google used a quantum computer to solve a mathematical task with random numbers in three minutes and 20 seconds. The same problem would have taken a conventional supercomputer around 10,000 years. This new type of computer promises a great deal of potential, but presents a problem for cryptography: All public-key crypto procedures commonly used in the Internet today are based on complex mathematical tasks, which quantum computers can solve within a short period of time.
Getting Cryptography Ready for Quantum Computers Now

Quantum computers are currently still in an experimental stage and are not yet market-ready. However, due to their potential, significant investment is being channeled into the development of this computer technology. “Some experts estimate that practical quantum computers will be available in 10 to 15 years. However, because the development and subsequent distribution of new encryption procedures are extremely time-consuming, it is important to start the project for quantum-safe communication now,” says Alexander von Gernler, Head of Research at genua.

Extending Proven Protocols with Quantum-Resistant Procedures

The researchers selected the IPSec and MACsec communication protocols for the project. IPsec and MACsec and their key exchange protocols IKEv2 and MKA are to be extended with quantum-resistant procedures. Both allow encrypted communication via the Internet and are often used to secure data exchange via VPN (Virtual Private Network) between distributed company locations or the connection of mobile employees to company networks.

Experts for All Research Areas

The project activities are divided up according to the partners’ areas of expertise: genua is concentrating on the IPsec/IKEv2 protocol, ADVA on MACsec/MKA, the LMU is conducting basic research for the entire project, and Fraunhofer AISEC is testing the security of the procedures developed by means of attacks in the cyber laboratory. The project runs until 2022, and receives funding from the Federal Ministry of Education and Research.

Captions:
Research Director Alexander von Gernler: “Cryptography needs to respond to developments in quantum computing now.” / Picture source: genua GmbH
About genua

genua GmbH is a German IT security specialist. Its business activities range from securing sensitive interfaces in public authorities and industry to connecting highly critical infrastructure, reliably encrypting data communication over the Internet and providing remote maintenance systems for industry and remote access solutions for mobile users and home offices. All genua products are developed and produced in Germany. Product quality is ensured by regular certification and approval by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik). genua was founded in 1992 and now has over 250 employees at its main site in Kirchheim near Munich and subsidiaries in Berlin, Cologne and Stuttgart. Over the years, numerous customers from industry and government have come to rely on the experience and solutions provided by the company. genua is a member of the Bundesdruckerei Group.

Further information:

genua gmbh
Dietmar Bruhns
Domagkstr. 7
85551 Kirchheim near Munich
Germany
phone +49 89 991950-169
dietmar_bruhns@genua.eu
www.genua.eu