satw

Quantum Computing

Cybersecurity – challenges for political Switzerland

State of the art

Building a fully functional quantum computer is one of today’s most exciting scientific and engineering challenges. Accomplishing this long-sought-after goal would have a very positive effect on such areas of science as artificial intelligence and bioinformatics. Quantum computers will be able to solve certain performance-demanding problems much faster than traditional computers. However, they are not expected to be used as general-purpose computers replacing traditional computers.

Quantum computing technology has evolved rapidly over the past few years. First quantum computers are available on the Internet already today, allowing everybody interested in to develop and try out new quantum algorithms.

While quantum computing creates a new paradigm for solving complex computing problems, unfortunately it also creates a new security risk. Many of today’s public key cryptographic algorithms are based on problems that are difficult to solve by traditional computers but can be efficiently tackled by quantum computers.

Recommendations

1. Even though powerful quantum computers are not available yet, organizations are advised to assess the security requirements of data assets and systems that have a long lifetime. The assessment should drive the plan of how and when to adopt the evolving quantum-safe cryptography standard.
2. When developing or acquiring new software solutions, cryptographic agility principles should be adhered to so that deployed cryptographic algorithms can be easily replaced with quantum-safe ones.

Challenges

It can only be speculated by when quantum computers will be available that are able to break current crypto systems. Estimates range from 10 years up to 30 years and more. A measure to assess the power of a quantum computer is the number of qubits. A qubit can be seen as the quantum mechanical analogue of a classical bit. It is differentiated between logical and physical qubits. A logical qubit requires about 1000 physical qubits to provide stability, error-correction and fault tolerance as needed for reliable computing. Furthermore, it is suggested that several thousands of logical qubits are needed to break today's crypto systems. Hence, in practice, one would need quantum computers with millions of physical qubits. Current experimental quantum computers "only" have between 50 and 100 physical qubits.

Although it will take some time until powerful quantum computers will be available, already today there are several cryptographic schemes that are considered quantum-safe, i.e., secure against attacks by quantum computers. They are based on difficult problems that are not known to have efficient quantum solutions.

Various efforts are currently underway to standardize quantum-safe cryptography. The most notable is the standardization process initiated by the National Institute of Standards and Technology (NIST). Standardization is a challenging and time-consuming process. It can be expected that within the next three to five years a standard will be available.

Need for action

There are IT systems such as devices used in, e.g., power plants or production factories that have a long lifetime. Systems deployed today may still be in use at the time powerful quantum computers are available. The same applies to data. Some data assets have to be archived for 10 and more years for regulatory compliance reasons and could get prone to quantum computer attacks.

References

- National Institute of Standards and Technology (NIST): Post-Quantum Cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography
- Computing Community Consortium: Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility, CCC Workshop, Feb. 2019. https://cra.org/ccc/wp-content/uploads/sites/2/2018/11/CCC-Identifying-Research-Challenges-in-PQC-Workshop-Report.pdf

Contact

Nicole Wettstein
Head of priority programme Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-challenges

Impressum
Swiss Academy of Engineering Sciences SATW
Expert contributions
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Editing and graphics
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

The views expressed here are those of the members of the SATW Cyber Security Advisory Board and do not necessarily reflect the official position of SATW and its members.

www.satw.ch
September 2020