Ordinateur quantique

Les défis de la cybersécurité pour la Suisse politique

Etat des lieux

La construction d'un ordinateur quantique pleinement opérationnel est l'un des défis scientifiques et techniques les plus passionnants de notre époque. La réalisation de cet objectif poursuivi de longue date aurait un effet très positif sur divers domaines scientifiques tels que l'intelligence artificielle et la bio-informatique. Les ordinateurs quantiques seront en mesure de résoudre certains problèmes nécessitant énormément de puissance beaucoup plus rapidement que les ordinateurs classiques. Toutefois, ils ne sont pas censés être utilisés comme ordinateurs polyvalents en remplacement des ordinateurs traditionnels.

La technologie de l'informatique quantique s'est développée rapidement ces dernières années. Les premiers ordinateurs quantiques sont déjà disponibles sur internet, de sorte que toute personne intéressée peut développer et essayer de nouveaux algorithmes quantiques.

Si les ordinateurs quantiques créent un nouveau paradigme pour la résolution de problèmes informatiques complexes, ils génèrent malheureusement aussi un nouveau risque sécuritaire. De nombreux algorithmes cryptographiques actuels à clés publiques se fondent sur des problèmes difficiles à résoudre par les ordinateurs traditionnels, mais peuvent être efficacement traités par les ordinateurs quantiques.

Recommandations

1. Même si de puissants ordinateurs quantiques ne sont pas encore disponibles, les organisations sont bien conseillées en matière de vérification des exigences de sécurité des bases de données et des systèmes à longue durée de vie. Cette évaluation devrait déterminer la feuille de route pour savoir comment et quand la norme cryptographique évolutive d'anti-hacking quantique sera adoptée.
2. Lors du développement ou de l'acquisition de nouvelles solutions logicielles, les principes d'agilité cryptographique doivent être respectés afin que les algorithmes cryptographiques utilisés puissent être facilement remplacés par des algorithmes d'anti-hacking quantique.

Défis

On ne peut que spéculer sur le moment où l'on disposera d'ordinateurs quantiques capables de craquer les cryptosystèmes actuels. Les estimations vont de 10 à 30 ans et plus. Le nombre de qubits est l'une des mesures permettant d'évaluer les performances d'un ordinateur quantique. En mécanique quantique, un qubit peut être considéré comme l'équivalent d'un bit classique. Une distinction est faite entre qubits logiques et qubits physiques. Un qubit logique nécessite environ 1000 qubits physiques pour assurer la stabilité, la correction des erreurs et la tolérance d'erreur nécessaires à un calcul fiable. Il est également admis que plusieurs milliers de qubits logiques sont nécessaires pour percer les cryptosystèmes actuels. Dans la pratique, on aurait donc besoin d'ordinateurs quantiques dotés de millions de qubits physiques. Les ordinateurs quantiques expérimentaux actuels ne possèdent actuellement «que» 50 à 100 qubits physiques.

Même s'il faudra encore un certain temps avant que de puissants ordinateurs quantiques soient disponibles, il existe déjà plusieurs méthodes cryptographiques d'anti-hacking quantique considérées comme sûres face aux attaques des ordinateurs quantiques. Celles-ci se fondent sur des problèmes complexes pour lesquels aucune solution quantique efficace n'est connue.

Divers efforts sont actuellement en cours pour normaliser la cryptographie d'anti-hacking quantique. Le plus remarquable est le processus développé par l'Institut national des normes et de la technologie (NIST). La normalisation est un processus exigeant et de longue haleine. On estime qu'une norme devrait être disponible dans les trois à cinq prochaines années.

Nécessité d'agir

Il existe des systèmes informatiques, p. ex. dans les centrales électriques ou les usines de production, qui ont une longue durée de vie et qui seront donc probablement encore utilisés le jour où de puissants ordinateurs quantiques seront disponibles. Il en va de même pour les données. Certaines bases de données, qui doivent être conservées pendant 10 ans ou plus (selon les prescriptions légales), pourraient devenir vulnérables aux attaques d'ordinateurs quantiques.

Références

- Institut national des normes et de la technologie (NIST): cryptographie post-quantique. 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
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

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

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
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, Verwaltungsrat und Berater | 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
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
Septembre 2020