PREPARING YOUR ORGANIZATION FOR THE QUANTUM THREAT TO CRYPTOGRAPHY

FEBRUARY 2021 **ITSAP.00.017**

Cryptography is an effective way to protect the confidentiality and integrity of information and to protect IT systems from cyber threat actors. Quantum computing threatens to break much of the cryptography we currently use. Quantum computers will use quantum physics to efficiently process information and solve problems that are impractical to solve using current computing capabilities. Quantum computers that are available now are not powerful enough to break cryptography, but a threat actor could take advantage of a sufficiently powerful quantum computer in the future to decrypt, read, or access sensitive information.

HOW IS YOUR CYBER SECURITY AFFECTED?

Your organization's cyber security is at risk as quantum computing advances. Although quantum computers are currently not powerful enough to break cryptography, a sufficiently powerful device could be available by the 2030s.

Cryptography provides security to information and IT systems in three main ways: encryption, integrity, and authentication.

Encryption is used to protect the confidentiality of information being transmitted or stored on a device (e.g. smartphones, USB drives).

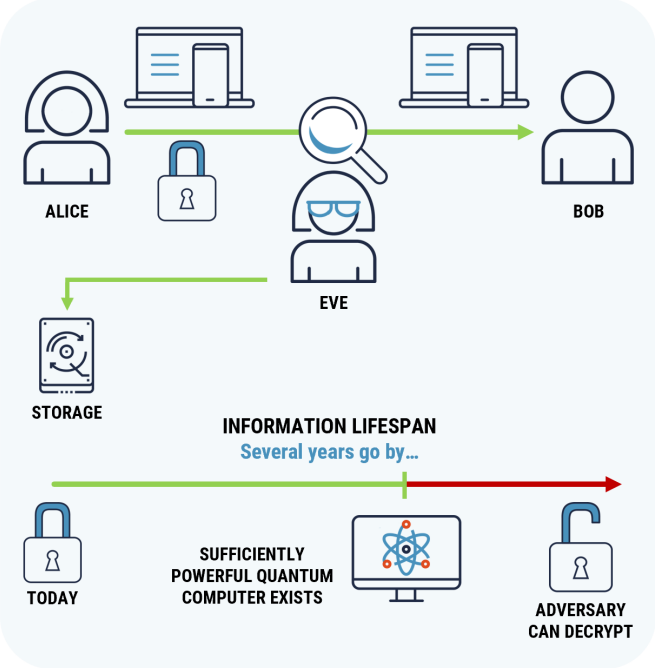
Currently, threat actors can store encrypted information to decrypt in the future, when a sufficiently powerful quantum computer exists. Information with a medium or long lifespan (i.e. it will still require protection in 10 or more years) could be at risk of decryption.

Lifespan refers to the timeframe for which information held by an organization requires protection (e.g. to protect privacy or intellectual property).

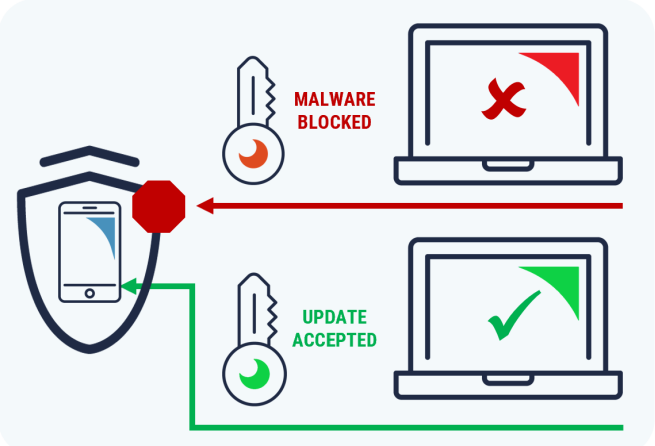
Integrity and authentication provides assurance that information has not been altered while in transit or in storage (e.g. accidentally or intentionally); and that the information originated from the correct source.

Threat actors could use a sufficiently powerful quantum computer to impersonate trusted systems (e.g. app store or trusted vendor) to deliver fake software updates and gain access to systems of interest. Unlike confidentiality, integrity and authentication will only be at risk when a sufficiently powerful quantum computer is available.

THREAT ACTOR STORES ENCRYPTED DATA FOR FUTURE DECRYPTION:



THREAT ACTOR DELIVERS FAKE SOFTWARE UPDATES TO GAIN ACCESS TO SYSTEMS:



AWARENESS SERIES

HOW ARE YOUR IT SYSTEMS AFFECTED?

Any information with a medium or long lifespan held by your IT systems may be at risk. While systems used to provide authentication and data integrity are not at risk today, in the future, these systems could be attacked by a threat actor.

Your organization should develop and budget for a transition plan to upgrade IT systems and deploy standardized quantum resistant cryptography when available. Practitioners should ask vendors about their plans to securely upgrade software and hardware to quantum resistant cryptography. As a part of this transition, software upgrades and system patches should be delivered to systems using cryptography to ensure the security of the upgrade and to authenticate the source.

In developing this plan, sensitive information with a long lifespan (e.g. intellectual property, tax data, medical records) should be prioritized.

IS THERE A QUANTUM SOLUTION?

Future, quantum technology and quantum key distribution (QKD) may be used to protect sensitive information. Research on the security and scalability of QKD is progressing, and the development of QKD is still maturing. QKD is not a replacement for current applications of cryptography, but it could be a way of securely communicating in the future.

WHAT IS CYBER CENTRE DOING?

The Canadian Centre for Cyber Security (Cyber Centre) is promoting awareness on the impact quantum computers pose to cryptography and the steps that can be taken to prepare for the transition to quantum-resistant cryptography when available.

The Cyber Centre is working with National Institute for Standards in Technology[1] (NIST) and other partners to evaluate the next generation of quantum-resistant cryptography, to replace current cryptographic applications.

The Cyber Centre is actively participating in international standards bodies including the International Standards Organization and the Internet Engineering Task Force to ensure the cryptographic security and privacy needs of Canadians are being met in new standards for quantum-resistant cryptography.

HOW CAN ORGANIZATIONS MANAGE THE RISKS?

We recommend your organization takes the following steps to help manage the risks associated with quantum computing advancements and to plan the transition to quantum-resistant cryptography:

1. Evaluate the sensitivity of your organization's information and determine its lifespan to identify information that may be at risk (e.g. as part of ongoing risk assessment processes).
2. Review your IT lifecycle management and develop plans to transition to quantum-resistant cryptography when available.
3. Budget for potentially significant software and hardware updates, as the timeframe for necessary replacement approaches.
4. Educate yourself and your teams on the emerging quantum threat and future quantum technologies.
5. Ask your vendors about their plans to implement quantum-safe cryptography (e.g. do vendors plan to include quantum-safe cryptography in future updates, or will you need to acquire new hardware or software?).
6. Ensure that your vendor is using standardized, validated cryptography (e.g. Federal Information Processing Standards [FIPS]).
7. Determine how and when you will be able to implement post-quantum algorithms in your life-cycle plan.
8. Update and patch systems frequently.

Contact the Cyber Centre by email at contact@cyber.gc.ca or by phone at 1-888-CYBER-88 for further recommendations.

REFERENCES:

The Cyber Centre and NIST[1]: *Post-Quantum Cryptography.* February 2020.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**