Information Security Thought Paper

Quantum Cryptography

Background

New technologies always have exciting implications for the ways they can be used in homes and workplaces of the citizens of British Columbia. Unfortunately, these technologies can create new risk and disrupt accepted security practices.

In the past half-century, study of Quantum Physics has revealed a variety of strange phenomena that allow possibilities that are outside of the conventional rules of our everyday reality. For the most part, this strange behaviour is limited to only the smallest of scales that we are capable of studying, leaving our day-to-day lives untouched. As our understanding of Quantum Physics has improved, we also have developed methods of using Quantum phenomena in our computers through the study of Quantum Computing.

Consequences

While there are exciting implications for technology development, there are also consequences to the security landscape. Quantum Physics allow us to go outside the usual limitations of computing, allowing hackers to break classical safeguards. In particular, this technology threatens the security of modern public key encryption.

Public key cryptography relies on complex mathematics being computationally difficult in order to be secure. Classical computers require an impractical amount of time to calculate the primes (more than a decade); however quantum computers could crack it in a matter of minutes or seconds. The solvability of this problem determines which cryptographic codes can be cracked, and what codes cannot be cracked.

Laboratory prototypes already exist that prove that this is practically achievable. It is just a matter of time before the technology is refined and achieves widespread use. When that happens, public key cryptography will be compromised. Currently, public key cryptography use is widespread in technologies such as SSL/TLS, Blockchain, and SSH. Without countermeasures to quantum decryption, the impact would be catastrophic to security. These vulnerable technologies underlie a wide array of security technologies used to protect personal information, business information, national security, and more.

Approaches to building quantum-secure cryptography can be sorted into two general categories:

Post-Quantum Cryptography

Work has already begun on building new cryptographic algorithms based on different mathematical principles. The aim is to develop math-based encryption that is not easily solvable by quantum computers. The benefit of this approach is that it would work on currently existing hardware and infrastructure. The downside is it is still unknown how many

complex algorithms a quantum computer is capable of solving quickly.

Quantum Cryptography

An alternative approach is to use quantum principles themselves as the basis for new cryptography. The advantage of these approaches is that they would not rely on difficult mathematical computation, only immutable properties of physical reality. The downside is that it would require widespread quantum repeaters to be built to form quantum channels for quantum information to be sent and received.

One of the most well developed methods of Quantum Cryptography is **Quantum Key Distribution (QKD)**. It uses quantum channels to distribute keys and establish a secure connection, and future communication would operate on classical channels.

Recommendations

Organizations will have to accept that modern cryptographic methods will soon be obsolete. Though quantum cryptography is theoretically unbreakable, it will likely have vulnerabilities based in imperfect physical implementations. Despite this, vulnerabilities in quantum systems carry significantly less risk than the current models that are completely vulnerable to attacks from Quantum Computers.

Organisations should conduct a risk management evaluation to create an inventory of organisational assets and determine what cryptographic technologies will need to be replaced. Performing a risk assessment will allow organisations to properly prioritize risks when transitioning to technologies that are secure against quantum threats.

Organisations need to begin developing a medium-term plan to evaluate emerging quantum-safe technologies and work with educational authorities to ensure there are security professionals who understand these new Quantum tools and methods. Transitioning from the current encryption paradigm will be difficult and new technologies and skill-sets will be necessary.

Currently, it is too early to begin physically transitioning systems to any particular quantum safe model, though the resulting solutions will likely involve both quantum-secure approaches. Quantum Cryptography and Post-Quantum Cryptography are still years away from feasible implementation, and deploying a global network of quantum repeaters will take time.

Resources:

- **The Global Risk Institute** has already released a Methodology for Quantum Risk Assessment, in order to provide and initial roadmap of what organisations can to prepare for the consequences of quantum computers:

  https://globalriskinstitute.org/publications/3423-2/

- **Quantum-Safe Canada** is an initiative that works to prepare Canadian leaders for the security threats posed by quantum computing. They host a series of resources for professionals looking to learn more about the topic:

  https://quantum-safe.ca/