IS QUANTUM COMPUTING A THREAT TO CRYPTOGRAPHY ?

Quantum computing has become a very hot topic the last few years, promising the kind of speed and compute power that some believe could make encryption obsolete. If true, that would obviously present a clear and present danger to existing security solutions. Many security vendors that use single layer encryption have responded to this worry by stating that their products are safe from a quantum attack, without offering the requisite proof. Unlike other vendors, at TrustWrx, our solution is built around a unique three-layer cryptography that defeats decryption attacks. Not only do we believe our present solution is safe today from quantum attacks, we can prove it.

Furthermore, new quantum-immune encryption algorithms are in the works and will be available long before quantum computers become commercially viable. When the new algorithms become available, they will easily plug into the TrustWrx architecture. For the past few years the pundits have predicted that commercially available quantum computing is about a decade away, and nobody has yet predicted a shortening of that timing - many consider it too aggressive.

The primary virtue of quantum computing is that it promises to be orders of magnitude faster than standard CMOS computing. However, quantum processor speed alone is not enough; other considerable technical constraints get in the way of quantum computing being a threat to present and future forms of cryptography.

Here are the primary reasons why quantum computing is not a near-term or long-term threat to cryptography.

1. **Rudimentary Hardware Platforms** A true quantum computer does not yet exist at commercial scale. The **D-Wave 2000Q** is the only commercially available "quantum computer" on the market today. However, it is more precisely described as an early stage "quantum annealer", a primitive first step towards true quantum computing. (Quantum annealing will never be able to run Shor's algorithm, which purportedly breaks common forms of contemporary cryptography.) Obviously, owning and operating such a computer is beyond the means of most organizations.

   The D-Wave 2000Q This technology cannot crack any encryption.

   a. Cost: A cool US $15 million.
   b. Size: A ten-foot cube, requiring more than 1,000 cubic feet.
   c. Processor capacity: 2,000 qubits (The industry believes that commercial viability will require upwards of one million qubits.)
   d. Operating environment: The D-Wave 2000Q processor resides in a high vacuum environment in which the pressure is 10 billion times lower than atmospheric pressure and operates at a temperature that is approximately 180 times colder than interstellar space.
   e. Management: Requires a front-end silicon-based CMOS server, with standard operating systems, code and operating speeds.

2. **Quantum mechanics is imprecise – but cryptography demands bit-level precision. This issue is the main impediment to decryption attacks from quantum computing.**

   Qubit computations are highly unstable and error-prone, limiting them to short and simple calculations; producing imprecise results. Reliable error correction techniques will require large quantities of qubits; have proven to be elusive and have yet to overcome quantum noise and other quantum-decoherence phenomena to produce reliably repeatable results. As a consequence, quantum computing remains **probabilistic rather than deterministic.**

   However, cryptography must be 100% bit-perfect; a one-bit deviation anywhere will fail a key match to an encrypted file or finding the prime factor of an integer (Shor's algorithm attack). The fundamental nature of quantum mechanics will keep qubit-error rates above zero percentile acceptable levels for a decryption attack, simply because the shift of a single bit, or qubit, in the encrypted file, the test key or the calculation, will render the test key a no-match to decrypt the encrypted file. It is therefore statistically unlikely that a quantum-based key test against an encrypted file will ever return a 100% deterministic result.
   Without bit-level precision all quantum cryptography attacks will fail.

3. **No quantum-speed memory or circuitry** Quantum persistent memory and quantum-speed circuitry does not exist and is anticipated only theoretically. The reality is that long term memory persistence and quantum decoherance are mutually exclusive. This means that all quantum computation must swap data and code commands through standard CMOS memory and circuitry, constraining quantum processes to snippets of quantum-chip-resident code and data, and performance dependent on classical network I/O and CMOS execution speeds, while trying to overcome the noise and decoherance of quantum mechanics. To date, the predicted fast performance of quantum calculations have remained largely theoretical, with limited real-world proof.

4. **CPU performance constraints** The primary quantum threat to cryptography is the high-speed brute-force testing of guessed keys against an encrypted file, or finding the prime factor of an integer. This is an automated process that succeeds only when the test returns plain text. This CPU data-intensive analysis problem exceeds the capacity of current quantum processors by orders of magnitude, requiring constant off-board CMOS memory and standard operating system I/O processes. Therefore, the data swap performance constraints will throttle the testing of keys or the search for the prime factor of an integer.

Post Quantum Cryptography

In anticipation of quantum cryptography attacks, many Post Quantum Cryptography initiatives have sprung up to develop advanced encryption algorithms that will be quantum immune. A recent NIST program has solicited proposals for new algorithms and is considering 26 candidates; all that purport to be immune to quantum attacks. When these new methods become standards, TrustWrx will simply adopt them and imbed them within our technology.

CONCLUSION -- NO THREAT

Quantum computing remains largely theoretical and is advancing at a pace constrained by extreme operating environments, high costs, the total lack of equivalent-speed memory and circuitry, dependency on slow front-end CMOS management, and the imprecise nature of quantum computing results. Many very expensive and very serious R&D operational and equipment challenges have yet to be overcome. After more than ten years of extremely expensive research and development the best technology to date is a 2,000-qubit processor that operates in an environment 100 times more hostile than deep space and costs $15 million. The gorilla in the problem is the probabilistic, rather than deterministic, nature of quantum mechanics that **may well exclude quantum computing from being effective at cracking current or future cryptography.**

George Sidman, CEO