Quantum Computing and the End of Computer Security As We Know It.

I know that I don't have much to give
But I can open any door
Everybody knows the secret
Oh, everybody knows the score
— Eric Clapton, Presence of the Lord

On May 4, 2022, the Biden Administration released "**NATIONAL SECURITY MEMORANDUM/NSM-10**." NSM-10 addressed both the coming promise and the indeed real threat that quantum computing represents. The document "**identifies key steps needed to maintain the Nation's competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation's cyber, economic, and national security**." While quantum computing represents an enormous forward leap in the amount of data that can be processed at one time and the calculations derived from that data, such capacity and alacrity of processing will render today's password security model moot.

Although in many ways, "quantum computing" is simply a buzzword to denote new and faster computing methods, quantum computing does have common accepted definition. **AT&T defines quantum computing as**:

> **Quantum computing focuses on developing computer technology based on principles that describe how particles and energy react at the atomic and subatomic levels. Today's computers encode information in 1's and 0's. Quantum computing says that information can be encoded simultaneously in more than one place.**
>
> **While the science is a bit muddy for those who are not quantum theory experts, we can all agree that quantum computing is faster than any other computing technology. In fact, the quantum computer that is in development at Google is 158 million times faster than the world's fastest computer today.**
>
> **Digital transformation has already spurred an increase in demand for web designers and developers, and web development is one of the fastest-growing career fields in the United States right now. In the future, quantum computing has the potential to contribute to finance, military intelligence, pharmaceutical development, aerospace engineering, nuclear power, 3D printing, and so much more.**

Along with the technological advances promised by quantum computing come real challenges to our current computer security model of encrypted passphrases to verify the identity of a user requesting network access. Although **quantum computers promise revolutionary benefits for many industries, they also pose an existential threat to all sensitive digital information, past and present**.

> **Due to their incredible computing power, these machines will be able to break through the public key encryption standards (RSA and Elliptic Curve cryptography) relied on today by virtually every organization, device and end-to-end encryption service. That's a big problem for businesses and governments alike.**
>
> **Public key cryptography relies on two different types of keys for encryption and decryption. A quantum computer could gain access to the secret key**

> **corresponding to any public key, use that access to forge the signature of a software update and push that to a corresponding piece of hardware.**

One reason quantum computers can break a password exponentially faster has to do with **nature of quantum mathematics**.

> **Breaking a symmetric code like AES is a matter of searching all possible key combinations for the one that works. With a 128-bit key, there are 2128 possible combinations. But thanks to a quantum computer's ability to probe large numbers, only the square root of the number of combinations needs to be examined -- in this case, 264. This is still a huge number, and AES should remain secure with increased key sizes.**

Nevertheless, organizations should begin to transform their security protocols to adjust to what will soon be an even more challenging security environment. Although it is estimated that the ability of quantum crooks to easily overcome today's password protocols in maybe 20 years, changes in computing power tend to accelerate with each new advancement. **One method organizations could implement now is to employ an access key regime where the key is replaced more frequently.** "**Every key, of course, requires a fresh cracking effort, as any success with one key isn't applicable to the next**."

What the future holds for all of us computer users, whether we are members of a larger global network, or simply Grandma wanting to Facebook with the grandkids, is a world where "**cybersecurity experts are racing to roll out a new form of cryptography that would defend against quantum hacks. This is known as post-quantum cryptography, or PQC**." One reason security experts are pushing for a speedy rollout of PQC is that crooks are stealing encrypted data today on the grounds that at some time in the near future that encrypted data will be easily decrypted and read and distributed.

> **Compounding this risk is what researchers call the "catch now, exploit later" threat. Nefarious hackers might intercept secure messages today and then hold onto them until tomorrow, whenever quantum computers are advanced enough to decrypt them.**
>
> **"This is why we need to push for the adoption of post-quantum cryptography as early as possible," said Evan Peet, associate economist at RAND and coauthor of the report. "Some encrypted communications don't lose their value over time."**
>
> **Simply put, the longer that PQC is not in place, the greater the amount of today's encrypted information that is at risk of being exposed tomorrow.**

Although there exists many position papers by various expert individuals and organizations, there is no common agreement on what post-quantum cryptography would look like. **Microsoft is working on four different tracks to find the best path to PQC**. **Yet, there are some significant roadblocks to development and implementation of PQC.** Currently, it is estimated that only 2% of organizations that could develop and implement PQC protocols today are doing so. PQC solutions are more costly to implement, and until sufficient quantities of scale are reached, the cost of implementing PQC will be prohibitive. Second, since PQC is technology meant to mitigate against future threats, testing PQC protocols cannot be done in a real world environment. Another barrier to greater adoption of PQC security techniques is the tremendous amount of computing power required by PQC. This is both an issue of costs and practicality. It is costly both in terms of money and time to implement. It is not practical for many entities to retool their networks to accommodate the required investment in hardware, nor do organizations lacking depth of pockets and people have the time or the means to implement new security protocols to counter an unknown future threat. **As McKinsey Digital consulting concluded:**

> **Given the risks and costs outlined here, most organizations should take a wait-and-see approach to PQC solutions. The exceptions are organizations and uses for which the stakes for security are particularly high, such as in the defense industry, where even provisional PQC protection for some high-value systems or for data with long lifetimes outweighs trade-offs in cost or performance. Another exceptional circumstance is when it would be more costly or impractical—or impossible—to access and retrofit high-value systems in the future compared with installing some protection today.**

Certainly, adoption of PQC is nothing for computer users at the consumer level to be to worried about at least at the time of this writing. Nonetheless, each advancement to computer technology tends to impact consumers more and more quickly. An organization has been formed that is attempting to address the challenges of identity verification for average consumers. Formed by Google, Apple, and Microsoft, Fast Id Online (FIDO) seeks to find alternatives to the traditional passwords that could be implemented today. **The organization is called the FIDO Alliance.**

The alternatives to passwords proposed by the FIDO Alliance center around **4 technologies that go beyond the traditional password**. These alternative technologies are:

✓ SECURITY KEY like A USB device that contains the key.

✓ FACIAL RECOGNITION

✓ FINGERPRINT

✓ VOICE

You can learn more about this initiative among the major technology companies to address the problems with passwords and the need right now to implement security protocols that go beyond the traditional password, go to **The FIDO Alliance**.

Wait a minute something's wrong baby,
Lord, have mercy, this key won't unlock this door, something's goin' on here.
I have a bad bad feeling that my baby don't live here no more.
That's all right, I still got my guitar
Look out now

— Jimi Hendrix, Red House

Back to Top

Gerald Reiff

Back to Top ← next post previous post →