How Quantum Computing Impacts Long-Term Encryption

Alarming headlines in regard to the topic keep invading the internet, and it seems like there is no escaping the approach of a new era where quantum computers will replace our current devices, exposing us to a new series of cyber threats. But is there truth to all the info you find online? As worrying as the subject is, enough time is left until quantum computers will become a commonality, which means that there is plenty of time to develop and move to encryption algorithms that are quantum-safe.

Quantum computing 101

Quantum mechanics already play a major role in our lives and most of us don't know about it. From the transistors in our smartphone to the MRI machines in hospitals, quantum mechanics are what make the world work as it does from many perspectives. Nevertheless, the constant development is opening up new doors as it doesn't rely on the classic 1's and 0's, providing a more complex computing manner using qubits that can occupy a state of both 1 and 0, and can influence each other through the process of entanglement.

What does quantum computing bring new to the table, you ask? Algorithms will be able to execute faster to a greater extent as opposed to current performance on computers. To get a better picture of how big the difference will be, think about it this way – a process that would normally take days is only going to take a few seconds.

What does it mean for long-term encryption?

Quantum computing is desirable as it promises to solve what current computers cannot fix regarding encryption security, a grave issue at the moment as it affects VPNs, database storage, online banking, and so forth. Solving these problems presents a worrying issue as data currently stored and transmitted with existing protocols is exposed when the change occurs as an automatic shift in protocols follows immediately.

How you should handle your projects

Check your projects to see if long-term encryption might be an issue or if they will span over a long period of time. With the inevitable change of protocols, your work is left exposed to new vulnerabilities and attacks. Luckily, there is ongoing research on creating protocols that are quantum resistant. Woefully, we have to hope that these protocols will be open source and not have any restrictions regarding intellectual property. Consequently, the best course of action when designing products and applications at the moment is to consider an eventual move to a different protocol.

With the scene looking as it does today, even the strongest security measure and protocol set in place would not be able to resist a '*quantum attack*'. An estimated five to thirty more years will pass until this becomes a realistic problem, but handling it ahead of time is the correct course of action, by far. At the moment, the closest we come to viable protection is Lattice cryptography, a form of encryption that resists these attacks, but not impervious to them so far. When it comes to encoding data, it's your best guess by far.

Does too much focus on the negatives help?

Caution is the fundamental key to a successful transition regardless of the situation, but focusing on the negatives exclusively leads to an outbreak of paranoid behavior among people that isn't beneficial as it doesn't solve the issue at hand. For big companies and banks, the situation is even direr as the trend is to overspend time and money on security measures for fear of breaches. Nonetheless, the interesting characteristics that come with this wave of change will make all the impending threats worth the hassle of protecting against them as **quantum search applicable in the security field** will allow an unprecedentedly complex gathering of data during malicious attacks.

How would the worst case scenario look like?

This threat, no matter the perspective, constitutes simply an economic problem. Ultimately, viable computers, when they appear as a full-functioning product, will be expensive and limited in their power, which means that governments will be the only ones able to afford them. There's no point of digging into any conspiracy theory regarding what a government would do with the technology as espionage and fight over power are topics for a different story.

As time will pass and the technology will become available to the masses, threats will come at a more ‘intimate' level as occurrences including blackmailing companies, selling sensitive data, and even transaction falsification will be an issue. Concurrently, a realistic estimate of how much time passes until the wrong people get their hands on this technology is about two or three decades from now. By that time, it’s likely that current algorithms will disappear and encryption won't be as exposed as it is at the moment.

So, a small reality check before we end, the internet won't break, missiles won't launch randomly, and banks won't lose your funds, at least not at any point in the near future, and while multiple threats are on the way, explicitly regarding exposure to attacks, there are efforts to prevent them as well. Evolution won’t cease regardless of how many scary headlines flood websites each day, and it's our duty to stay informed so that we reap only the benefits of what's to come.