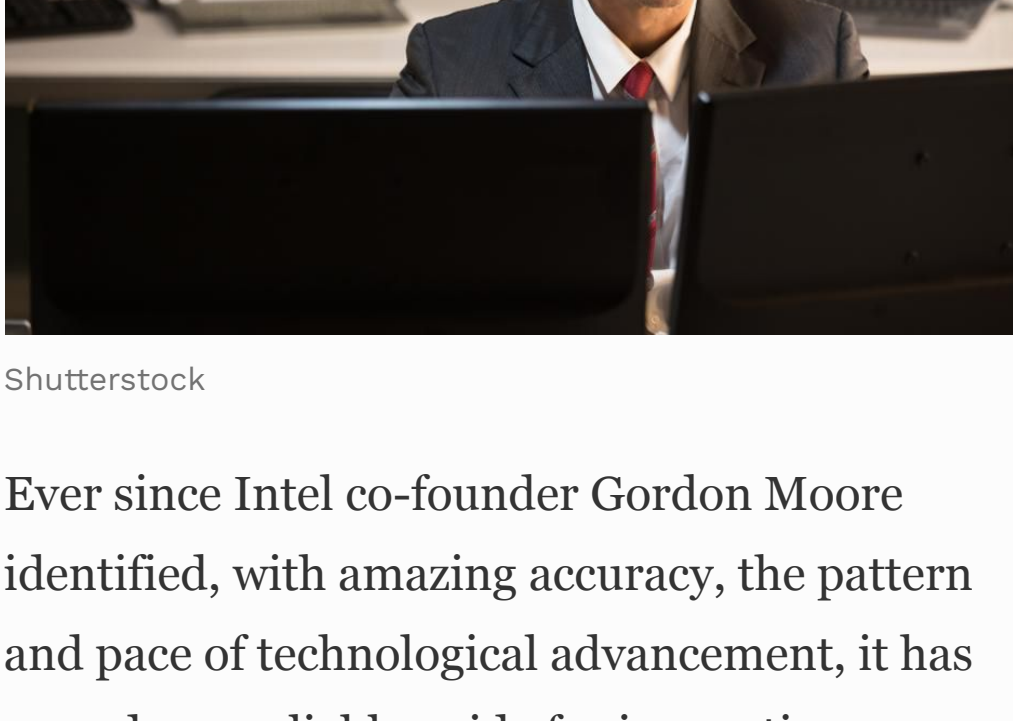
1,431 views | Mar 13, 2018, 08:45am

Moore's Law At Warp Speed: The Global Security Risks Of A Post-Quantum World

Michael Xie CommunityVoice
Forbes Technology Council CommunityVoice

POST WRITTEN BY
Michael Xie
Founder, President and CTO at Fortinet, overseeing the technology vision and strategy for the global network security leader.



Shutterstock

Ever since Intel co-founder Gordon Moore identified, with amazing accuracy, the pattern and pace of technological advancement, it has served as a reliable guide for innovation. Moore's Law, which states that the number of components per integrated circuit doubles every 18 months, has been the standard measurement and projection for long-term planning and research and development.

But now that storage has been achieved at the atomic level, it could be argued that we have reached the ultimate, intractable limit for Moore's Law.

Perhaps.

Another possibility, though, is that Moore's Law will soon hit warp speed -- driving certain innovations and breakthroughs at polynomial speeds -- thanks to the rapidly approaching reality of quantum computing.

While it may strike some as strange to be discussing an acceleration of Moore's 18-month timeline by a technology that even the most aggressive estimates predict will not be a reality for more than a decade, the impact of quantum will be seismic. And the fact is, nobody really knows exactly how quickly it will be felt or how it will be applied.

But just going by predictive models and research, it is clear that quantum's power is beyond comparison to anything we have today. Though the applications for quantum computing will certainly be limited at first, there are also clear certainties of how its power can be applied, particularly in the fields of AI, genetic research, engineering and economics -- challenges that are known as optimization problems.

For anyone tasked with securing critical infrastructure (bridges, dams, electrical grids, nuclear facilities, critical manufacturing, communications systems and financial services), this is why the arrival and power of quantum computing might be keeping them up at night.

Because of all the optimization problems, the low-hanging fruit that quantum computing will be able to pick is, unfortunately, a critical fundamental of cybersecurity: encryption.

This should give some indication of quantum's power, because encryption -- the process of encoding information so only those authorized to access it are able -- has proved to be a remarkably resilient and powerful tool to protect all types of digitally transmitted and accessible data. How resilient? If a hacker were to try to launch a brute-force attack against the common 128-bit AES key, using a sophisticated computer that could check one key per second, it would take approximately 149 trillion years to crack the encryption (the universe itself is only about 13.75 billion years old).

Before breathing a collective sigh of relief, though, consider that some have estimated that a quantum computer could theoretically improve the efficiency of a brute-force crypto attack significantly.

That is cause for concern -- but not alarmism. Significantly, there have been several studies that support the theory that simply doubling the key length could be quite effective against quantum. It is theorized that the time it would take a quantum computer to crack a 256-bit key is comparable to the time it would take today's computers to crack 128-bit keys.

Regardless, Shor's algorithm and Grover's algorithm -- the basis for quantum attacks -- are considered effective against common public-key algorithms in use today, including RSA, Diffie-Hellman and elliptic curve cryptography. However, symmetric encryption methods such as AES seem to be mathematically resistant to brute-force attacks, at least today. Significant research has shown that just a small increase in the key length of these symmetric algorithms seems to be able to fend off rather big improvements on the computing power side, better than public key-based algorithms such as Diffie-Hellman.

A simple start and absolute imperative is to begin upgrading to longer key lengths. While 128-bit symmetric keys are still considered unbreakable today, public keys -- the kind we all use on a day-to-day basis for shopping, banking and communicating online -- are far more vulnerable. To a savvy hacker, even a 256-bit public key is of little to no protection. The minimum recommendation is now 512 bits, with longer bits recommended for valuable or confidential information.

For critical infrastructure stored in governmental and global security organizations, though, the situation is much more of a crisis -- for all of us -- because the devastation of an attack on the networks of critical infrastructure facilities does not remain within the walls or confines of an organization. Breaching an electrical grid, the controls of a dam or a nuclear reactor could trigger a horrific catastrophe.

And this is where we get a chilling glimpse of the dangers of Moore's Law at warp speed, long before quantum computing is a reality. Because not only are increasingly sophisticated attacks on critical infrastructure facilities a possibility in the very near future -- they have already happened, though few people are aware of it.

House, Republicans finalized their tax plans, the Harvey Weinstein scandal still commanded headlines and Roy Moore refused to concede the election in Alabama?

Something far more significant happened that day as well.

In an unprecedented attack, online hackers breached the important safety systems for the control units used in nuclear, oil and gas plants. The attackers, suspected to be state-sponsored, used sophisticated malware called Triton to take control of a workstation. The system responded by going into a failsafe mode and shutting down, averting a possible disaster.

For the time being anyway. Though the immediate impact of that attack was not felt, authorities believe that may not have been the attackers' goal anyway. They were primarily interested in learning how the safety systems operated and how to shut them down during a future attack. And as more than 50 years of Moore's Law has proved, the future is arriving faster every day, so we need to start preparing now.

Forbes Technology Council is an invitation-only community for world-class CIOs, CTOs and technology executives. ***Do I qualify?***

Founder, President and CTO at Fortinet, overseeing the technology vision and strategy for the global network security leader.

30,458 views | Oct 15, 2018, 05:26pm

One Year After #MeToo, UNICEF Is Fighting Sexual Assault Worldwide

Sarah Ferguson Brand Contributor
UNICEF USA BRANDVOICE

Sarah Ferguson Brand Contributor
Follow

Sarah Ferguson is a writer and critic whose work has appeared in The Guardian, Elle, Vogue, New York Magazine, Mother Jones and The New York Times Book Review, among other publications.