Real Random

Securing Ecommerce in the Era of Quantum Computing

Doug Hill is passionate about creating a worldwide business that will improve digital security. His core values are integrity, inclusiveness, and innovation for all. He is the Founder of Real Random and has solved the puzzle of creating true random numbers from a reliably unpredictable physical source to protect people.

Doug Hill ▪ *Founder* ▪ Real Random

Quantum computing represents the next evolution in how we use computers to solve complex problems, as it holds great promise for advancing the speed at which data can be analysed in useful and harmful ways.

As an ecommerce operator, it will affect your industry in both positive – e.g. the ability to rely upon more accurate data and faster processing of transactions across different platforms – and potentially negative ways. The primary negative aspect is the threat to the current methods of securing transactions, the private/public key pairs, and the commonly used encryption algorithms. In addition, the timing of the availability of quantum computing is a moving target. Several factors such as the market demand, technological advancements, and the cost to purchase or gain access to a quantum computer will influence the outcome. But there are things you can do to prepare for what is sometimes called ‘Q-Day’, the day when quantum computers will be available for commercial purposes, including nefarious organisations and nation-state actors.

Let’s talk about quantum computing

To better understand this phenomenon, let’s begin with how today’s computerised systems operate and why quantum computing systems are the next major step in advancing computing power.

Nowadays’ binary-based computing systems operate in a linear fashion. This means that we input data or commands and expect a result built on the processor’s ability to receive and carry out the instructions for any given type of input. Processing time and results are based on the available computing power and network access speeds.

While useful now and in the future, linear computing is much slower than quantum because of the way data is processed. As a practical example, imagine a maze puzzle – the kind we have all tried at some point – and think of this puzzle as the keys used to secure your computerised networks. As humans, we take a linear or binary approach to solving the puzzle: we try a pathway and continue trying until we solve for the maze. However, the method of trial and error is effective but not efficient. Now, imagine the ability to try all combinations simultaneously, a la quantum. The outcome of both approaches is the same, but the difference is the time and computing power needed to solve the problem.

Securing transactions: what to take into account

The first thing to consider is how long the equipment or process you are using to secure transactions and communications will last. Is it less than 5 to 7 years? If the answer is yes, according to industry experts, your level of concern is low. If it is longer, then you should consider taking steps to reduce your risk by creating a long-term plan with incremental steps to mitigate the factors within your control.

One approach is to develop solutions with equipment providers that include dynamic encryption in the form of one-time passcodes. Imagine a unique key that is used for each transaction, making it traceable and ineffective if captured in transit. This method of authentication is also useful in evading attackers that can gain access to the static or fixed keys in use today. Given that most of the communication in the authentication process is in a machine-to-machine environment, you must consider the unknown access that is typically undetected until you are facing a major financial loss due to a breach.

➔

The second question is: how long do you need to secure the sensitive data that passes over your networks? If the answer is more than 10 years, then you need to begin planning for a post quantum world.

The secure storage of the vast amount of data collected in ecommerce is becoming an increasing concern for operators, customers, and governments. One must consider the ramifications of a breach from the loss of funds, angry customers, to fines levied by government bodies.

Protecting your data begins with understanding your current methods and future opportunities to enhance your security. Is your method of encryption reliant upon technologies that use pseudo random numbers to generate the keys that secure your networks? Most likely the answer is yes, because that is considered sufficient to prevent an attacker from using linear computing to break the key in less than 100 years or more. Yet, consider quantum computers and the ability to simultaneous try all possible key combinations: the result is that the time to break the key shrinks to only a few hours.

The solution to implementing a quantum-resistant solution is still evolving. We are reliant upon engineered algorithms to generate secure keys; we must realise that anything that is engineered can be reverse engineered. One approach is to rely upon random numbers that are generated from a physical process that is impossible to guess or predict. Keys created from physical sources of randomness like dice or weather are the solution to being secure in the quantum age. This approach avoids the inevitable supply chain attack that is a growing threat to operators from bad actors and nefarious organisations that are harvesting data while waiting for ‘Q-Day’.

real random

realrandom.co

Real Random’s mission is to improve digital security by providing true random numbers for real security. In modern cryptographic systems, security is largely based on algorithms that can be reverse engineered, making them increasingly vulnerable to threats as technology advances. The company’s API solution provides a reliable source of true random numbers.