REPORT REPRINT

Move over, Heisenberg: QuintessenceLabs brings key generation into the quantum realm

GARRETT BEKKER, PATRICK DALY

30 OCT 2017

The vendor is applying quantum physics to data security by generating encryption keys based on quantum physical states rather than deterministic algorithms.

THIS REPORT, LICENSED TO QUINTESSENCELABS, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

451 Research®

©2017 451 Research, LLC | WWW.451RESEARCH.COM

Encryption and key management is complicated enough, and the injection of quantum mechanics into the discussion is enough to make most folks' heads spin. Mainstream quantum computing is likely still several decades away, but there is already a small group of companies applying quantum technology to cryptography to deliver true random number generators based on the physical states of particles rather than pseudorandom numbers generated by algorithms. QuintessenceLabs is one of the few vendors tapping into the power of quantum physics for random number generation, with an offering the vendor claims to generate completely random encryption keys, along with advanced key and policy management features that give customers complete control over the lifecycle and use of encryption keys.

THE 451 TAKE

By combining the added security of encryption keys based on quantum random numbers, advanced key lifecycle management and an HSM for protecting those keys, QuintessenceLabs has developed a compelling offering for those enterprises and agencies with a need for the highest level of data security. While the technical advantages of quantum-based key generation are clear, the near-term obstacle is most likely 'good enough' security from practitioners that are willing to live with the theoretical and practical limitations of pseudorandom key generation until the threats from quantum computing are more tangible.

CONTEXT

QuintessenceLabs was founded in 2008 as a result of work done by founder and CEO Vikram Sharma with the Australian National University's Quantum Optics Group. The company is based in Canberra with a foothold in North America through its office in San Jose. Headcount is about 40 employees. The company has received an undisclosed amount of funding in June 2015 and January 2017 from its largest investor, Westpac, one of Australia's 'Big 4' banks. Although QuintessenceLabs has been in existence for nearly a decade, commercial shipments of its products didn't begin until 2014 and today it has several customers in the aviation and defense, legal and financial services industries.

TECHNOLOGY

Entropy is a quantitative measure of the 'randomness' of data, and with many cryptographic processes, higher entropy implies greater security. Many security functions, including encryption but also authentication, code signing, one-time passcodes and others depend on randomness. Most encryption keys are currently based on pseudorandom numbers, which are quickly and easily generated using deterministic mathematical algorithms. However, pseudorandom numbers are not completely unpredictable because they are generated from a relatively small set of initial seed numbers. And if they are not completely unpredictable, then they can be predicted – or hacked, at least in theory. For example, if certain factors can be predicted or guessed, such as the time of day or system information, the algorithm can be reverse engineered and the keys can be guessed. In short, poor-quality random numbers effectively reduce the strength of the encryption algorithms used. However, generating completely random numbers is a more difficult task that historically has taken longer, potentially reducing the usefulness of encrypting data. New quantum technologies applied to the randomness problem have resulted in generation of true random numbers 'fast enough' for large-scale enterprise use.

The company's qStream offering generates random data by measuring 'quantum tunneling noise.' The essential idea is that voltage is applied to a diode that contains a barrier, and the number of charged particles that are able to cross the barrier creates random fluctuations in the current flowing through the diode. These fluctuations can be measured, digitized and digitally processed to generate ultra-high-bandwidth (1Gbps) random numbers that can be used in any cryptographic application.

PRODUCTS

QuintessenceLabs offers a key generation and management platform referred to as the Trusted Security Foundation (TSF). TSF is a single, rackable hardware appliance that consists of three distinct technologies that can also be purchased separately and integrated into third-party products: a random number generator (qStream), an encryption key and policy manager (qCrypt) and an embedded hardware security module (HSM) to protect encryption keys.

The qStream component is a true random number generator that QuintessenceLabs claims can generate 1Gbps of random numbers for use as encryption keys with 100% entropy; i.e., complete randomness. This is a fundamental aspect of QuintessenceLabs' value proposition because achieving true random numbers at high speed increases the security of encryption keys. QuintessenceLabs offers qStream as a stand-alone one-rack server hardware appliance and also in conjunction with its key manager, as well as in the TSF platform.

The second component of TSF, qCrypt, can centrally manage cryptographic objects and meets current NIST standards for encryption key lifecycle management. It can perform synchronous replication of keys for increased redundancy, so customers can still access data if one site fails. Customers can purchase qCrypt with the qStream random number generator fully integrated, and like qStream, it is also offered with an SDK to allow customers to integrate QuintessenceLabs' key management capabilities. Fully compliant with the Key Management Interoperability Protocol (KMIP) standard, qCrypt can also export logs into SIEM tools for monitoring and analysis.

The final TSF component is a FIPS 140-2 level 3 compliant embedded HSM delivered through a third party to secure a company's cryptographic keys. QuintessenceLabs offers qProtect, a one-time pad encryption device that generates keys using quantum random numbers and then destroys the keys once the data is encrypted, ensuring that data and keys are never stored on the same device.

QuintessenceLabs also provides a fully KMIP-compliant qClient SDK with the TSF product suite, as well as a standalone product for third-party vendors to integrate into existing encryption and key management offerings.

One of the potential challenges of quantum-based random number generators is they are not as fast as current pseudorandom number generators, which could limit their applicability for implementations that are latency-sensitive, such as in healthcare, government or financial services. Many quantum random number generators are based on detection of a single photon, which limits throughput. However, qStream's current maximum throughput at 100% entropy is 1Gbps. Still, even at 1Gbps, QuintessenceLabs' true random number generator is theoretically slower than a pseudorandom number generator, although the vendor claims that if a higher rate is required, several qStream quantum random number generators can be used concurrently, and for low-latency situations, random can be pooled. For situations where pseudorandom generation is acceptable, qStream can be used to seed the pseudorandom generator to obtain significantly higher entropy than with conventional seeding techniques.

STRATEGY

OEM is a big part of QuintessenceLabs' go-to-market and its products have been designed to easily integrate into other systems. QuintessenceLabs has several partnerships, most notably with PKWARE. TSF is integrated with PKWARE's Smartcrypt Enterprise Manager to deliver key generation, management and storage, and implement encryption directly on endpoint devices. VMware is deploying the qClient SDK as a white-label offering that allows VMware customers to interface with key management products through a KMIP interface. Cloud storage provider NetDocuments integrates TSF to secure sensitive data stored in the cloud, with the option of deploying TSF devices on-premises for full control of their keys and protection from government subpoenas.

COMPETITION

QuintessenceLabs may face general competition from encryption and key management heavyweights such as Thales Vormetric, Gemalto/SafeNet, Micro Focus (HP/Voltage) and IBM, although as was the case with PKWARE, some of the latter could also be potential partners.

QuintessenceLabs will likely face its most direct competition from a handful of vendors that have focused specifically on quantum encryption and key management. Whitewood Security is a Boston-based quantum encryption vendor that also uses a true random number generator and has worked with Los Alamos Laboratory in developing its offering. SecureRF and ID Quantique are both also tackling the threat posed by quantum computers, with SecureRF focusing on algorithmic approaches, and ID Quantique on quantum key distribution in contrast to QuintessenceLabs' primary goal of strengthening encryption using quantum-generated random numbers and strong key management.

SWOT ANALYSIS

STRENGTHS

High-speed true random number generation combined with centralized key management and HSMs is a solid value proposition for companies across a variety of markets that need to ensure the highest levels of data security.

WEAKNESSES

QuintessenceLabs does not yet have a large market presence or brand recognition in North America. Even at 1Gbps, qStream is slower than a pseudorandom number generator, and may not be suitable for certain latency-sensitive environments, although several qStreams can be used concurrently, or alternatively used to 'seed' a pseudorandom number generator to achieve much higher entropy.

OPPORTUNITIES

QuintessenceLabs can more aggressively market to vertical markets that have a heightened need for stronger data security, including healthcare and financial services.

THREATS

One of QuintessenceLabs' biggest obstacles may be 'good enough' security. Attacks frequently take advantage of poorly implemented crypto rather than attack the crypto algorithms directly, itself, although QuintessenceLabs can address poorly implemented random number generators.