PARTNER CONTENT DON HAYFORD, BATTELLE

THE FUTURE OF SECURITY: ZEROING IN ON UN-HACKABLE DATA WITH QUANTUM KEY DISTRIBUTION

mikecogh/Flickr

Thieves steal data constantly, so protecting it is an ongoing challenge. There are more than 6,000 banks with 80,000 branches in the United States, nearly 6,000 hospitals and thousands of insurance companies, all with data that we want to be kept private. Traditionally, their valued data is protected by “keys,” which are transmitted between sender and receiver. These secret keys are protected by unproven mathematical assumptions and can be intercepted, corrupted and exposed if a hacker “eavesdrops” on these keys during transmission. Specific problems with current encryption technology include:

- Potential backdoors inserted into at least one of the recommended random number generators, (which can be fixed by following the NIST recommendation of no longer using the suspect method)

- Improvements in quantum computing, which will nullify the security of all approved encryption key transfer methods
- At least two different types of side channel attacks on the most popular key exchange methods that can break key exchange methods as powerful as RSA-40963

Standard methods for exchanging cryptographic keys are in jeopardy. RSA-1024, once commonly used to exchange keys between browsers and web servers, has probably been broken; it's no longer regarded as safe by NIST, though RSA-2048 is still approved. This and other public-key infrastructure technologies perhaps haven't been broken yet but soon will be by bigger, faster computers. And once quantum computers are mainstream, data encrypted using existing key exchange technologies will become even more vulnerable.

Researchers are working on methods to improve the security of software-based key exchange methods using what is known as post-quantum cryptography — methods that will continue to be effective after quantum computers are powerful enough to break existing key exchange methods. These are all based on the unprovable assertion that certain numerical algorithms are difficult to reverse. But the question that remains is — difficult for whom? How do we know that an unpublished solution to these exact problems hasn't been discovered? The answer is — we don't.

Quantum cryptography is the only known method for transmitting a secret key over long distances that is provably secure in accordance with the well-accepted and many-times-verified laws that govern quantum physics. It works by using photons of light to physically transfer a shared secret between two entities. While these photons might be intercepted by an eavesdropper, they can't be copied, or at least, can't be perfectly copied (cloned). By comparing measurements of the properties of a fraction of these photons, it's possible to show that no eavesdropper is listening in and that the keys are thus safe to use; this is what we mean by "provably secure". Though called quantum cryptography, we are actually only exchanging encryption keys, so researchers prefer the term "quantum key distribution", or QKD, to describe this process. The no-cloning theorem is one of the fundamental principles behind QKD, and why we think that this technology will become a cornerstone of network security for high value data.

While products based on QKD already are being used by banks and governments in Europe — especially Switzerland — they have not been deployed commercially in the United States to any great extent. Current technological breakthroughs are pushing the distance over which quantum signals can be sent. Trials using laboratory-grade hardware and "dark fibers" — optical fibers laid down by telecommunications companies but lying unused — have sent quantum signals three hundred kilometers, but practical systems are currently limited to distances of about 100 kilometers. A scalable architecture that includes a Trusted Node to bridge the gap between successive QKD systems can both extend the practical range of this technology and allow keys to be securely shared over a wide ranging network, making large scale implementation possible and practical. Cybersecurity is making progress toward the future reality of sending data securely over long distances using quantum physics.

As an example, my team at Battelle, together with ID Quantique, has started to design and build the hardware required to complete a 650-kilometre link between Battelle's headquarters and our offices in Washington DC. We are also planning a network linking major U.S. cities, which could exceed 10,000 kilometers and are currently evaluating partners to work with us on this effort. For the past year, we have used QKD to protect the networks at our Columbus, Ohio headquarters. But we're not alone when it comes to quantum-communication efforts. Last month, China started installing the world's longest quantum-communications network, which includes a 2,000-kilometre link between Beijing and Shanghai.

Many nations acknowledge that zeroing in on un-hackable data security is a must, knowing that even the best standard encryption that's considered unbreakable today will be vulnerable at some point in the future — likely the near future. QKD is the best technically feasible means of generating secure encryption. Yes, it has its challenges, but continued innovation is tackling these issues and bringing us closer to the reality of long-distance quantum rollouts and truly secure and future-proofed network technology.

Does this mean that software-based methods won't have any value for network security applications? Of course not. One must always evaluate the cost of the protection against the cost associated with the loss of your data. But part of that evaluation must include the certainty of the security solution. So, while post-quantum cryptography and QKD may both be secure enough for a particular application, we use QKD when we want to “know” that our data is secure, without having to rely on unproven assumptions that it is.

In the long run, we envision an integrated network that includes software-based methods, which we call Tier III (cost conscious), alongside higher-security and commercially viable QKD (Tier II) solutions that use quantum methods with Trusted Nodes to distribute keys, but conventional encryption (AES, for example) to protect actual data. In this vision, there is also one higher level — Tier I (very secure, very expensive) — that uses quantum repeaters to transmit long, quantum-based keys and one-time-pad encryption to protect our highest value data, mostly government and military information.

QKD is an attractive solution for companies and organizations that have very high-value data. If you have data that you want to protect for years, QKD makes a lot sense. I think you’ll see this distributed across the country to protect that high-value, long-duration data. This is the future.

Don Hayford is a senior research leader in National Security Global Business at Battelle.