ETSI/IQC Quantum Safe Cryptography Workshop 2019

Executive Highlights - November 5-7, 2019 - Seattle, WA

Quantum computing and risks to cybersecurity are gaining notoriety.

Quantum is becoming a prominent issue as more and more people outside of the quantum technology field are becoming aware of the concerns associated with a post-quantum reality as it pertains to crippling today's cybersecurity, said Michele Mosca, Institute for Quantum Computing while summarizing the 3 day conference that occurred at Amazon Web Services HQ in Seattle.

Donna Dodson from NIST highlighted the need for business managers need to start working on plans to migrate to PQC algorithms very soon and this migration needed to be presented as a business imperative and not just as a cryptographic and security requirement.

Jay Baloo from KPN (Dutch Telco Provider) explained that China currently spends an equivalent of €10B a year on Quantum research whereas Europe will spend €1B over the next 10 years and it is a serious concern that quantum computers could break our existing crypto systems.

And while many companies struggle to determine when quantum computing will emerge, Michele Mosca pointed to a new report has been published by the Global Risk Institute https://globalriskinstitute.org/publications/quantum-threat-timeline/ "Quantum Threat Timeline" that surveyed 22 quantum computing experts and reported on their predictions of time to break cryptography. Michele Mosca predicts there is a 1 in 5 chance in 10 years that today's public key cryptography could be broken.

But before companies worry about implementing post quantum cryptography, IBM highlighted the need to first define a basic strategy for managing their cryptographic assets/processes. Michele Mosca explained that 90% of the transition effort lies in the planning, and companies need to start sooner rather than later, adapting their approaches as capabilities and timelines begin to coalesce into something more definite in terms of when the quantum threat will become a reality.

The workshop wrapped up with a set of actions for attendees that included feedback to NIST on real-world, business-centric PQC requirements, and engagement with regulators to determine the role they could play in preparing their respective industries for quantum cybersecurity threats.

Quantum cybersecurity standards progressing well, but have a long way to go.

Global standards have made a lot of progress this past year, participants from various governments on a panel that included Michael Groves from the National Cyber Security Centre (NCSC) in the UK, Lily Chen from NIST, Manfred Lochter from the German BSI and Bridget Walshe from the Canadian Centre for Cybersecurity, indicated that it was unlikely changes to standards or protocol designs will be mandated, but instead would be encouraged to move as quickly as possible by incubating early research activities through sponsorship.

Both Cloudflare and IBM highlighted the importance of key agreement to widely used security protocols such as SSH and TLS, and there was also a need to upgrade digital signatures with a number of standardization efforts noted that were underway. Most important is to upgrade secure software updates in the near term, so that future upgrades can be reliably pushed out to endpoints and devices.

Dustin Moody from NIST gave an update on the post quantum selection process, it will be entering it's 3rd round selection stage in June 2020 and is expected to last 12-18 months. NIST is also planning to release an HBS-focused SP800 document by the end of 2020. Martin Ward of ETSI gave updates on the ISG for QKD which is continuing standardization efforts throughout 2020. Matthieu Legre of the ITU updated that work is being done on QKD, QRNGs within their SG13 and SG17 groups. Lily Chen from NIST who participates in ISO mentioned that ISO is trying to standardize Quantum-resistant cryptography via WG2 and their Standing Document 8 initiative.

Cryptanalysis of Post Quantum Cryptography is an important ingredient to security.

Quantum cryptanalysis is continuing to evolve and mature as it becomes more of a discipline. The hope is that this will lead to more groups/individuals becoming involved in the field, which should help to continue pushing the boundaries and improving the techniques and results.

Traditional mathematical analysis on algorithms continues to be needed, but new quantum analysis methods are emerging where techniques are being researched to apply new quantum algorithms to new classes of cryptography. In addition, Vlad Gheorghiu of IQC summarized a number of optimizations that are underway to reduce the number of qubits needed to apply existing quantum algorithms like Shor's method to break RSA and ECC, that reduce quantum computing requirements to break today's public key cryptography.

Efficiencies in PQC are also being actively researched including energy-/computational-efficiency of the various NIST round 2 PQC candidates on IoT style processors such as the Cortex-M4 platform and FPGAs. Experimentation in the embedded processor realm has resulted in improvements to a further understanding of potential side-channel security risks of running PQC on various hardware platforms, since some algorithms can be identified based solely on their distinctive power consumption signatures, indicating that these algorithms will likely be subject to traditional side-channel attacks that are one of the primary concerns of smart-cards and HSM vendors.

Transitioning to post-quantum, hybrid is the prevailing approach.

Hybrid approaches appear to be the prevailing choice when it comes to the best way to deal with the transition from classic to post-quantum methods. This sentiment was echoed by a number of companies doing real-world experiments, as well as the standardization bodies (e.g., NIST, BSI, etc.). Technology vendors warned that once these hybrid schemes are adopted as a method of transition, they might not go away once the transition is complete, resulting in future vulnerabilities where systems still accept weak cryptographic methods, long after the transition period when quantum computing has arrived. Regardless, Bob Blakely from CITI Group explained that companies still need to start a transition plan now, given that past technology transitions such as Y2K as well as cryptographic migrations have taken upwards of 10 years of planning.

An industry panel of companies including Amazon Web Services, Microsoft, IBM and Cloudflare that have been experimenting with TLS have been pleasantly surprised that the protocol is able to handle new PQC algorithms without many failures and a number of hybrid certificate techniques are available to support unsafe and quantum-safe protocol variants at the same time to ease a period of transition.

Ken Beer from Amazon Web Services announced the availability hybrid key agreement as part of the AWS Key Management Service APIs and is soliciting feedback on timing and message sizes in real-world customer environments running on AWS.

With having already been through the need migrate cryptographic algorithms in the past, questions have been posed as to why cryptographic agility has not been considered before. Bob Blakely from CITI reminded attendees that in the late nineties, "crypto agility" was considered "crypto with a hole" and therefore not exportable. For this transition to post-quantum, the industry needs to assume that there will be more transitions in the future, and ensure that new regulations foster and encourage future secure cryptographic transitions.

2020 Workshop

There will many new developments to report in autumn 2020. Planning for the 2020 event is taking into account the global impact of COVID-19. Further details will be available at etsi.org.