IDQ

Redefining Security

SWISS QUANTUM

QUANTUM-SAFE SECURITY WHITE PAPER

Why Quantum Technologies Matter in Critical Infrastructure and IoT

V1.0
October 20th 2017

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

Table of content

1. Introduction 3
2. Crypto Security Requirements 3
3. Quantum Threats to Today's Cryptography 4
4. Quantum-Era Solutions for Quantum-Safe Security 5
5. Hardware Protections & Key Generation 5
6. Quantum Key Distribution 7
7. Quantum-Resistant Algorithms 7
8. Recommendations 8

ID Quantique SA

Ch. de la Marbrerie, 3

1227 Carouge

Switzerland

Tel: +41 (0)22 301 83 71

Fax: +41 (0)22 301 83 79

www.idquantique.com

info@idquantique.com

Information in this document is subject to change without notice.

1. Introduction

A nation's critical infrastructure provides the essential services that underpin our society and serve as the backbone of our country's economy, security and health. In most countries critical infrastructure comprises a number of sectors, with criticality being highest in electricity and water supply, banks, road and rail transport, telecommunications and information technologies. Defense of the country depends in a large part on protecting such assets, systems and networks, which underpin our liberal democracy and civilization.

Such systems and assets have developed into a networked Internet of Things, where machines talk to machines and devices to devices without human interaction. This is already the case for Supervisory Control and Data Acquisition (SCADA) and industrial control systems (ICS) which are moving online and towards modern standardized networking protocols. Examples include the electricity grid and train networks, where commands can now be sent over open transmission networks using IP-based protocols, such as MPLS; or the connections to smart meters deployed in millions of homes; or to the devices underpinning smart cities; or in the future to the millions of smart cars driving autonomously on our roads which depend on embedded IoT devices.

Such hyper-interconnected infrastructures present new defense challenges:

- **Rapid advancements in technology** will add new attack vectors which were not conceived of or which were not feasible at the time that the devices were originally deployed – especially given the long field lifetimes of critical infrastructure devices
- The **scalability of the attack vectors** is unprecedented, where a single successful hack could affect millions of devices[1]. So far such attacks have been relatively benign, but this could change. This means that many previously isolated or siloed systems and devices forcibly become part of a networked critical infrastructure. For example, in the past, if one car crashed it was a matter for the police and possibly an ambulance. However, in the world of ubiquitous IoT, if a hack can cause an entire smart city infrastructure to fail, or the entire self-driving car or rail network to go down, then it becomes an issue of national security[2].

2. Crypto Security Requirements

Many of the core requirements for security of modern critical infrastructures depend on cryptographic primitives. Clearly, cryptography is only a part of the whole but for the purposes of this paper, we will consider specifically the implications of the emergence of new quantum technologies on the cryptographic primitives - in the context of both creating new threat vectors, as well as providing some solutions. And the cryptography is crucial - If the underlying crypto primitives fail, then the security of the device(s) and the network fail as well.

[1] https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

[2] For this reason in the paper it is considered that ultra-networked IoT devices in certain industries form part of the nation's critical infrastructure, and the terms IoT and critical infrastructure are used interchangeably.

The US Department of Homeland Security[3] (DHS) recommends certain key tenets for what they term "Life Critical Embedded Systems" which neatly summarise the ubiquity of cryptography in machine to machine security.

- All interactions between devices MUST be mutually authenticated
- Continuous authentication SHOULD be used when feasible and appropriate
- All communications between devices SHOULD be encrypted
- Devices MUST NEVER trust unauthenticated data or code during boot-time
- Devices MUST NEVER be permitted to run unauthorised code
- Devices SHOULD NEVER trust unauthenticated data during run-time
- When used, cryptographic keys MUST be protected

Moreover, the report goes on to state that devices and systems MUST be built to include mechanisms for in-field update, and that devices and systems for managing updates MUST be mutually authenticated and secured: *"Threat models must recognize that some systems will need to be in place for decades, while others may refresh annually or more frequently….. Life critical embedded systems should be engineered to include enough compute capacity for stronger cryptographic and runtime protections that will need to be added within the lifetime of the systems."*

However, in-field update mechanisms may also bring about new attack vectors, as an attacker, who manages to enter the system will be able to update it according to their needs.

3. Quantum Threats to Today's Cryptography

Recent breakthroughs in quantum computing have brought about a credible threat to the widely used cryptographic primitives which underpin our infrastructures and networks – notably to public key cryptography, such as RSA, Elliptic Curve Cryptography & Diffie Hellmann. Scientists have known about this threat since 1994 when a mathematician, Peter Shor, published his now-famous quantum algorithm for factoring large numbers into primes and finding discrete logarithms much faster than any classical algorithm. These are precisely the mathematical problems underpinning the above-mentioned primitives. A quantum computer running Shor will therefore break all the cryptographic systems based on these primitives.

The exponential speed-up brought about by quantum computers stems from the fact that they act as massively parallel computers. This is made possible by a weirdness of quantum mechanics known as "superposition". Crudely put, it is the ability for a quantum bit (or qubit) to be both a one and a zero at the same time. Properly implemented (and this is by no means an easy task), this weird property extends to any numbers of qubits. Ultimately, the whole quantum computer can now be in a superposition state, which provides exponential computing power.

[3] DHS Security Tenets for Life Critical Embedded Systems https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

And quantum computers already exist – albeit with a restricted number of qubits. IBM has launched the first quantum computing cloud, which allows external users to experiment with a small number of qubits[4]. Google has set itself a target for proving quantum supremacy (the ability of a quantum computer to resolve certain problems faster than the best available conventional processors) by the end of 2017[5]. D-Wave was the earliest to market and has already launched its 2000Q System quantum computer which - luckily for today's security – uses a quantum computing process which cannot run Shor's algorithm.

So the question is: when will a universal quantum computer run Shor's algorithm (or any variation thereof) on enough qubits to be able to break today's crypto primitives? One estimation is provided by Dr Michele Mosca from the Institute for Quantum Computing in Canada, who also runs a quantum risk assessment practice[6]: he estimates that large-scale quantum computing is 10-15 years away, and that there is a 1 in 7 chance of crypto primitives being affected by quantum attacks in 2026, and a 1 in 2 chance by 2031.

This may sound a long time away, but given the timescales for developing and deploying many critical infrastructure devices – which are often in the field for 20+ years, it would be prudent to start preparations now.

4. Quantum-Era Solutions for Quantum-Safe Security

New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed "quantum-safe" and consist of both techniques based on quantum properties of light that prevent interception of messages (Quantum Key Distribution or QKD[7]), as well as new algorithms (known as Quantum Resistant Algorithms) that are resistant to known quantum attacks, like Shor's. Quantum technologies can also be used to improve the overall safety of critical infrastructure by improving cryptographic key generation. The devices are known as Quantum Random Number Generators, or QRNGs.

5. Hardware Protections & Key Generation

While the algorithms in devices may be upgraded remotely, the hardware aspects of the device must be secure from the outset, unless they are recalled physically for upgrade. Mission critical devices often have long lifetimes in the field – stretching over decades – so the hardware must be adapted or adaptable to counter future threats. This is particularly relevant for the multitude of field-deployed devices, where cost and size is a major factor and which today are frequently deployed without any

[4] https://www.forbes.com/sites/aarontilley/2017/03/06/ibm-quantum-computing-cloud/#b6b65e877a2c

[5] https://www.newscientist.com/article/2138373-google-on-track-for-quantum-computer-breakthrough-by-end-of-2017/

[6] http://globalriskinstitute.org/publications/3423-2/

[7] For more information on QKD see http://www.idquantique.com/quantum-safe-crypto/qkd-overview/

of the required security protections or upgrade paths. Again, while individually each device, sensor or actuator may not present a major threat, a single hacked device may provide an entry point to the whole system. Therefore, critical systems should already have implemented strong cryptographic protocols on all their components, with enough computing capacity built in for this to be upgraded in the future to address new crypto primitives and runtime protections.

Another aspect fundamental to security is the random number generator (RNG), essential to all crypto operations. Generating strong keys, based on true randomness, is the cornerstone of security – good keys must be unique, unpredictable and truly random. Having strong crypto algorithms with weak keys is akin to putting a huge padlock on your front door and then hiding the key under the mat[8]. Software-based RNGs are not sufficient, as the computer programs they run are purely deterministic and cannot generate true randomness without external entropy sources. Since many critical infrastructure and IoT deployments are in isolated locations with limited external interaction, such sources of external entropy are limited.

Therefore RNGs should be based on hardware, and the resulting crypto key should also be protected in hardware. This need for hardware-based root of trust, and hardware protection of the keys is recognized also in the DHS recommendations, which state "*Ideally life critical embedded systems would include a hardware root of trust and system integrity, as without such system hardening, updates could be unreliable or untrustworthy. "*

Moreover in critical infrastructures RNGs need to be able to withstand the extremely harsh environments in field deployments often over many decades without losing quality of the randomness. They should not degrade with time, and they need to withstand extremes of temperature, vibrations, and electromagnetic noise. Photonics-based quantum random numbers generators (QRNG) meet these requirements well. Firstly quantum systems are intrinsically random, and therefore do not need to accumulate entropy to generate secure keys – every bit has what is termed "full entropy". This is important to ensure adequate security during boot time and for the first trusted handshake with other devices. Secondly, photons (single light particles) are more resilient to external influences, such as heat and electromagnetic signals than other types of thermal-noise based RNGs . Photonics-based QRNGs are already used for transport encryption of critical infrastructures by vendors, such as ABB[9] , and a next generation of low cost, miniaturized QRNGs meet the requirements for widespread field-based deployments of IoT devices[10].

[8] A more scholarly version of this example is stated in Kerckhoff's principle: "A cryptosystem should be secure even if everything about the system, except the key, Is public knowledge". This encapsulates the importance of the encryption key in crypto systems.

[9] See the SECU1 Encryption card by ABB: http://new.abb.com/network-management/communication-networks/optical-networks/mission-critical-communications/security

[10] http://www.idquantique.com/random-number-generation/

6. Quantum Key Distribution

Wide-scale QKD is already being deployed on transport networks to provide quantum-safe protection to critical infrastructures in countries such as China. However, QKD is not yet adapted for edge or hyperconnected networks. Applications of QKD are currently restricted to specific cases, such as highly critical links between major infrastructure components rather than IoT field deployments. Therefore we will focus currently on the two key components for a quantum-safe solution in the IoT world – the secure key generation mechanism above, and Quantum Resistant Algorithms below.

7. Quantum-Resistant Algorithms

Quantum Resistant Algorithms (also known as Post Quantum Cryptography) refer to cryptographic primitives (such as lattice-base or code-based), that are thought to be secure against an attack by a quantum computer, or at least against known attacks such as Shor's.

Since such algorithms are not provably secure from a mathematical perspective (unlike QKD), they must be rigorously tested and analysed before being deployed. NIST, the American National Institute for Standards and Technology, has launched a solicitation and evaluation process[11] with the goal to standardize on one or more quantum resistant public key crypto algorithm. The process will take at least 5 years.

What is clear is that – while such quantum resistant algorithms are not yet ready for deployment – manufacturers and users must already start to prepare by implementing crypto-agility into their devices and systems today, so that these may be securely upgraded in a timely manner as the threat to today's asymmetric algorithms becomes relevant. This will similarly impact new technologies, such as Blockchain, which have huge potential for delivering authentication and integrity in IoT environments, but are in large part based on crypto primitives which will require a future upgrade to be quantum safe.

[11] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

8. Recommendations

In summary, the recommendations come in two different categories: Prepare Now, and Act Now.

Prepare Now:

- Understand and document the threat models which might affect your critical infrastructure deployments, including dependencies resulting from high interconnectivity between devices and (your and third party) systems.
- Build a process for continual evaluation for such threat models as new technologies and attack vectors emerge, based on an estimation of the lifecycle and field deployment conditions, as well as expected renewal rates.
- Prepare for the upcoming quantum era by investigating the impact of quantum technologies upon your devices, systems and deployment. Conduct a quantum risk assessment, specifically for the trust models based on cryptographic primitives, and how this will impact your devices and systems.

Act Now:

- Build crypto agility into your devices, systems and deployments to ensure an upgrade path in the future. Ensure the ability to conduct remote upgrades in a secure, timely and pro-active manner.
- Build hardware devices and systems with a view to long term security in the field, and notably with:
    - Spare computing power able to support upgraded crypto primitives and run time protections, and
    - Hardware based key generation for adequate security of cryptographic operations throughout the lifetime of the device, ideally based on quantum photonics for resilience to environmental influences.
- Demand these same security criteria from your suppliers and everyone in the value chain bringing your systems into field deployment.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com